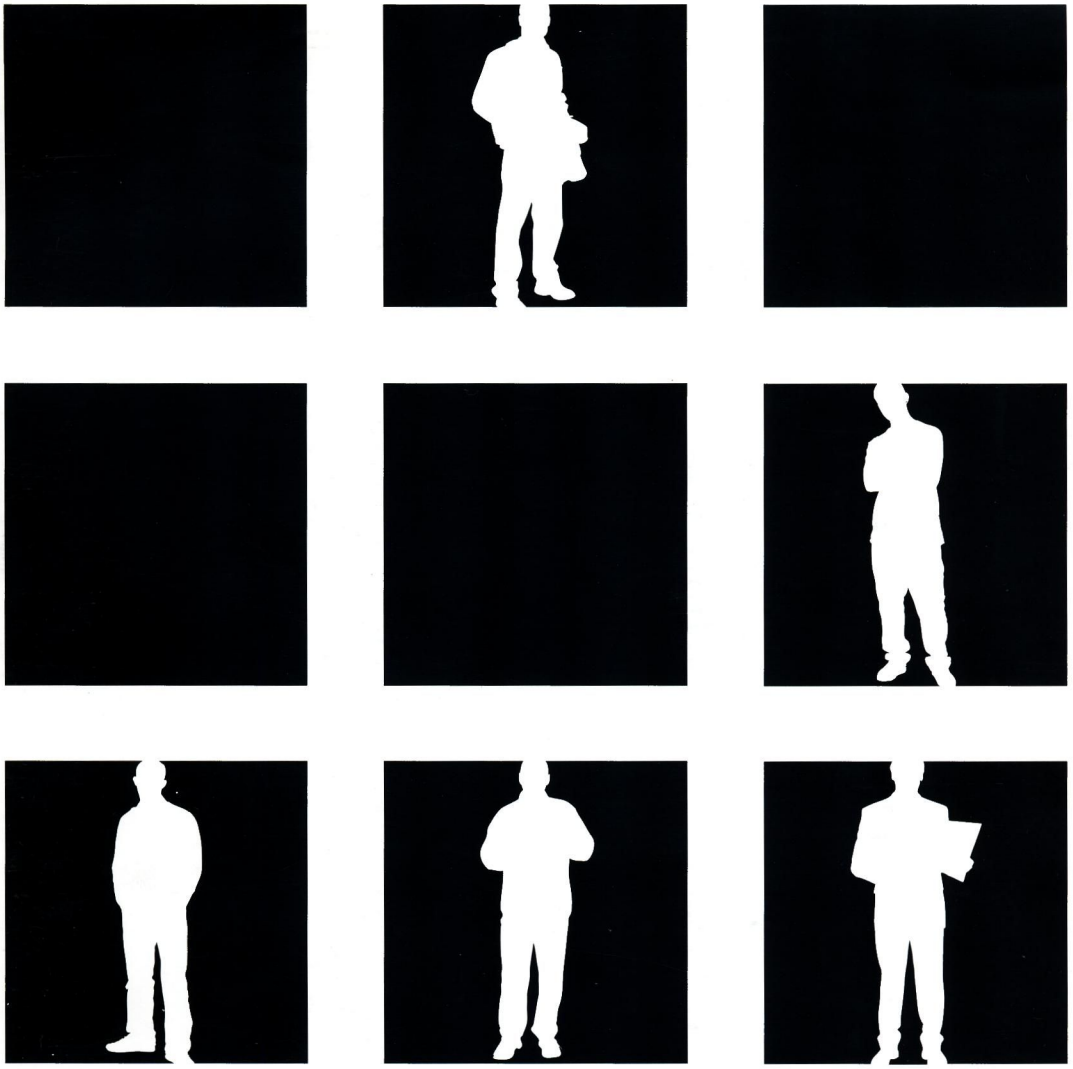


HACKTIVITY

2011. Budapest

...ptember 17–18., Millenáris

Közép-Európa legnagyobb hackerkonferenciája

...gest Hacker Conference in Central and Eastern Europe

Kötélen táncolunk...

Aggódnom kellene?

Igen

Biztos benne, hogy bizalmas vállalati információi megfelelően védettek?

A biztonsági fenyegetettségek és a támadási módszerek kifinomultságának növekedésével egyre fokozódó igény van kiemelkedő tudással és tapasztalattal rendelkező biztonsági szakértőkre. A Deloitte az információbiztonsági tanácsadás vezető szakértőjeként mély technológiai tudással rendelkezik az informatikai biztonsági kontrollok elemzéséről, tervezéséről és ellenőrzéséről. A részletekért látogasson el a ***www.deloitte.hu/security*** weboldalra.

Deloitte.

Gyémánt / *Diamond*

Deloitte.

Arany / *Gold*

kancellar.hu

BalaBit IT Security

Cyber-Ark
Security That Empowers People™

Wi-Fi

ARUBA networks

biztributor

FORTINET

GFI

gemalto
security to be free

websense
ESSENTIAL INFORMATION PROTECTION

Ezüst / *Silver*

WEBSHARK

rrc THINK VALUE.

Technikai / *Technical*

SILENT SIGNAL
VÉSZJELZÉS HELYETT...

xemeti
DIGITAL MARKETING

Bronz / *Bronze*

NOREG
Információvédelmi Kft.

hp

Sabretooth Global

intel

eset

vodafone

További támogató / Futher Sponsors

SZVT

KISKAPU

FORMULA MÉRNÖKIRODA

Kiemelt médiapartnerek / Special Mediapartners

Haking
All About IT Security

IT café

it business

Médiapartnerek / Mediapartners

BIZTONSÁGPORTÁL

PC WORLD

SZÁMÍTÁSTECHNIKA COMPUTERWORLD

hwsw
www.hwsw.hu

HUP

BITPORT

techline.hu

PC dome

PRIM ONLINE

mysec

BEYOND security

ASVA.INFO

BuheraBlog

ClubHACK

itSHOP
www.itshop.com

Szakmai partnerek / Professional Partners

Hungarian Autonomous Center for Knowledge

netACADEMIA

CISCO
TO BE ON THE SAFE SIDE

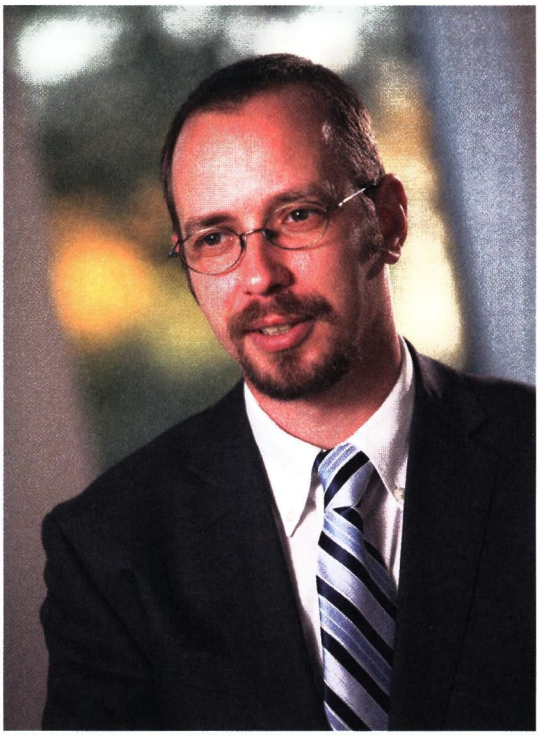
ISACA
Budapest Chapter

IVSZ

ZMNE

INFORMATIKUSOK EGYESÜLETE

Szakmai programszervezők: Tiborcz József, Bártfai Attila, Tóth László, Spala Ferenc
PR, marketing, szponzoráció: Szutor Bernadette
Ügyvezetés: Csere Attila, Mikecz Dalma
Operatív szervezés: Mikecz Dalma, Keresztesi Rita,
Arculat: Keresztesi Rita
All in: Papp Péter
Kapcsolat: info@hacktivity.com



előszó

Vállalati információbiztonsággal foglalkozó szakemberként számtalan olyan helyzettel találkoztam, amely megfelelő tervezéssel és felkészüléssel megelőzhető lett volna. Az információ érték, amelynek védelme átgondolt stratégiát kíván: a Deloitte-nál éppen ezért komoly nemzetközi, nagyvállalati tapasztalattal rendelkező szakértői csapat dolgozik azon, hogy ügyfeleink adatai, informatikai rendszerei biztonságban legyenek.

Azért döntöttünk úgy, hogy főtámogatóként veszünk részt a Hacktivity konferencián, mert a tapasztalatcsere és új ismeretek megszerzése szerintünk nélkülözhetetlen ahhoz, hogy együtt jobb válaszokat találjunk a különféle támadások, fenyegetések ellen. Az ördög nem alszik, ezért legyünk mi is ébren.

Antal Lajos,
a Deloitte Zrt. Informatikai biztonság és adatvédelem üzletágának vezetője

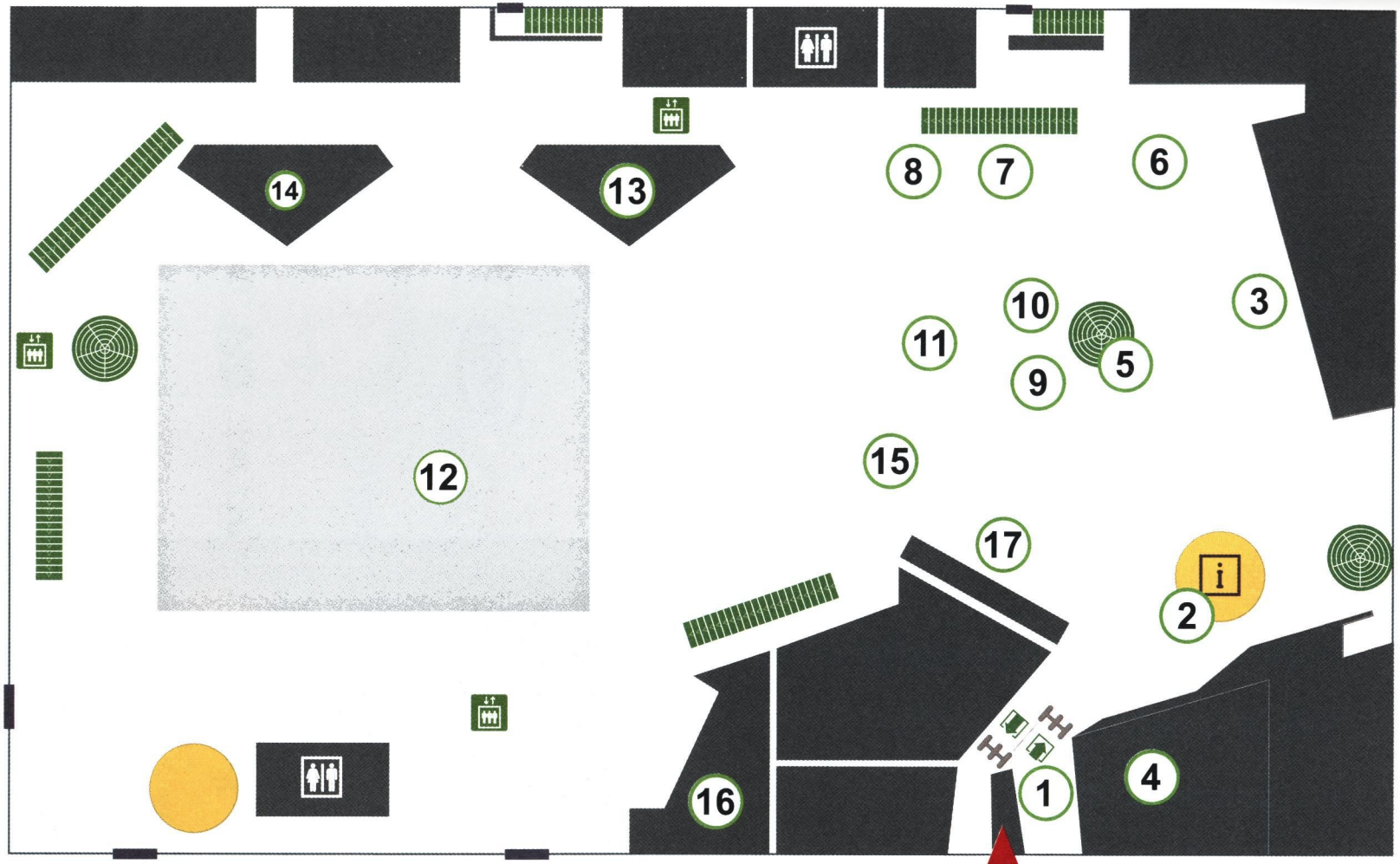
preface

As a corporate IT security expert I have come across a number of situations which could have been avoided by careful planning and preparation. Information is valuable and protecting it requires a well-developed strategy, which is why we at Deloitte work with a team of experts who possess a wealth of experience with multinational corporate clients to ensure the security of the data and IT systems of our clients.

The reason we have decided to come on board as the main sponsor of Hacktivity was that we believe exchanging ideas and obtaining new knowledge are essential for finding the right responses to the various types of attacks and threats. The devil never sleeps, which is why we should also be alert.

Lajos Antal,
Deloitte Hungary's Security and Privacy service line leader

HACKTIVITY TÉRKÉP földszint / MAP ground flour



1. BEJÁRAT / *ENTRANCE*
2. INFORMÁCIÓ / *INFORMATION*
3. ÉTTEREM / *RESTAURANT*
4. CYBER LYPICS
5. FELJÁRAT A HELLO WORKSHOPHOZ / *ENTRANCE TO THE HELLO WORKSHOP*
6. EGYEDI PÓLÓNYOMÁS / *T-SHIRT PRINT*
7. KANCELLAR.HU STAND
8. MYSEC STAND
9-10. KÖNYVSTANDOK / *BOOK STANDS*
11. LEISURE ZONE
12. PIPACS TEREM / *PIPACS HALL*
13. H.A.C.K.TEREM / *H.A.C.K. ROOM*
14. LOCKPICKING TEREM / *LOCKPICKING ROOM*
15. BIZTRIBUTOR STAND
16. ORVOSI ÜGYELET / *MEDICAL SEVICE*
17. BALABIT STAND - SZOMBAT ESTE / *SATURDAY NIGHT*

HACKTIVITY TÉRKÉP emelet / MAP first flour

1. SILNET TEREM / *SILENT HALL*
2. DELOITTE STAND
3. RRC STAND
4. TÖRTÉNETI KIÁLLÍTÁS / HISTORICAL EXHIBITION
5. KANCELLAR.HU & CYBER ARK VIP ROOM
6. SAJTÓ SZOBA / *PRESS ROOM*
7. ESET STAND
8. BÜFÉ / *BUFFET*
9. SABRETOOTH STAND
10. NOREG STAND
11. BALABIT STAND
12. INTEL STAND
13. CAPTURE THE FLAG

HACKTIVITY - SZOMBAT

	PIPACS terem	SILENT terem
08:00–09:00	Regisztráció	
09:00–09:15	MEGNYITÓ	
09:15–10:15	**Szőr Péter / Keynote–Küzdelem a kártékony kódok ellen**	
10:15–10:25	SZÜNET	
10:25–11:10	Barta Csaba – Az NTDS.DIT forensic vizsgálata	Illési Zsolt – Informatikai bizonyíték, bizonyítás igazságügyi szakértői szemmel
11:10–11:15	SZÜNET	
11:15–12:00	Joe McCray – Van rá progi: mobilalkalmazások pentesztje	Peszleg Tibor – Mit tegyünk, ha bekövetkezett a baj?
12:00–12:05	SZÜNET	
12:05–12:50	Alexander Kornbrust – Oracle-forensic	Alexin Zoltán – Nagy magyar egészségügyi adatbázisok
12:50–13:30	EBÉDSZÜNET	
13:30–14:15	Subecz Ákos & Zánthó Csaba – Lockpicking – a zárnyitás művészete	Leitold Ferenc & Horváth Botond – Dobozba zárt internet
14:15–14:20	SZÜNET	
14:20–15:05	Ertunga Arsal – Rootkitek és trójaik az SAP alkalmazásrendszerekben	Kovács Győző – Válogatott kalandozásaim Informatikában
15:05–15:10	SZÜNET	
15:10–15:55	Tóth László – Majdnem láthatatlan álca az Oracle-adatbázisban, avagy a nem dokumentált ismét segít minket	Muszka Dániel – Kalmár-korszak Szegeden
15:55–16:15	SZÜNET	
16:15–17:00	Georgi Geshev – A fal ledöntése / Mission: Impossible	Veres-Szentkirályi András – Hacking hardware for fun and profit
17:00–17:05	SZÜNET	
17:05–17:50	Felix Schuster – Egy extra titkosítási réteg tervezése és implementálása a Skype-hoz	Otti Csaba & Őszi Arnold – Ujjlenyomat-azonosító rendszerek, biztonság vagy biztonsági rés
17:50–17:55	SZÜNET	
17:55–18:40	Kerekasztal: Léderer Sándor, Földes Ádám, Bodoky Tamás, Csörgő László - Wikileaks: infoszabadságharc vagy infoterrorizmus?	Gara-Tarnóczi Péter – Publikus exploitok testre szabása

HACKTIVITY - VASÁRNAP

	PIPACS terem	SILENT terem
09:00–09:45	Paulik Tamás – Ki lakik a routeremben? A beágyazott eszközök botnetbe szervezésének kivitelezhetőségéről	Hornák Zoltán, Kerényi Kristóf, Kispál István – Cryptochipek biztonsága / passzív-aktív kombinált támadások
09:45–09:50	SZÜNET	
09:50–10:35	**Raoul Chiesa / Keynote – Kiberbűnözés, információs hadviselés és kiberháború: mi ez az egész? Tévhitek és igazságok a hacker nézőpontjából**	
10:35–10:50	SZÜNET	
10:50–11:35	Vivek Ramachandran – Nagyvállalati Wi-Fi-férgek és -botnetek	Bodor Péter – Social engineering és pszichológia
11:35–11:40	SZÜNET	
11:40–12:25	Pavol Luptak – Kriptoanarchia 19 évvel a Kriptoanarchista kiáltvány után	Oroszi Eszter – Social engineering – amikor fellebben a fátyol
12:25–13:20	Ebédszünet	
13:20–14:05	Balázs Zoltán – IPv6 shipworm + My little windows domain pwnie	Bíró László – Stuxnet – valóban az első?
14:05–14:10	SZÜNET	
14:10–14:55	Gyöngyösi Péter & Illés Márton – Tűzfalak és támadások	Yaniv Miron – SCADA-szomorúság vagy bumm-bumm SCADA
14:55–15:10	SZÜNET	
15:10–15:55	Michele Orru – Dr. Strangelove, vagy: Hogyan tanultam meg nem aggódni és a BeEF-et szeretni	Yaniv Miron – SCADA Hacking & Security Workshop
15:55–16:00	SZÜNET	
16:00–16:45	Major Marcell & Zágon Mihály – A legújabb webes támadási lehetőségek	Beregnyei Balázs – Szilícium layouttól a kapcsolási rajzig
16:45–16:50	SZÜNET	
16:50–17:35	Kabai András – Malware-analízis, tippek és trükkök	
17:35–17:50	Konferencia zárás	

HACKTIVITY - *SATURDAY*

	PIPACS Hall	SILENT Hall
08:00–09:00	Registration	
09:00–09:15	OPENING	
09:15–10:15	**Peter Szor / Keynote – Fighting Computer Malware**	
10:15–10:25	*break*	
10:25–11:10	Csaba Barta – Forensic analysis of NTDS.DIT	Zsolt Illési – IT as evidence from forensics perspective
11:10–11:15	*break*	
11:15–12:00	Joe McCray – There's An App For That: Pentesting Mobile Applications	Tibor Peszleg – What to do when the problem is on board?
12:00–12:05	*break*	
12:05–12:50	Alexander Kornbrust – Oracle Forensic	Zoltán Alexin – Big Hungarian Health Databases
12:50–13:30	*launch break*	
13:30–14:15	Ákos Subecz & Csaba Zánthó – Lockpicking / the finest art of opening locks	Ferenc Leitold & Botond Horváth – Internet in the sandbox
14:15–14:20	*break*	
14:20–15:05	Ertunga Arsal – Rootkits and Trojans on Your SAP Landscape	Győző Kovács – My Assorted Wanderings in IT
15:05–15:10	*break*	
15:10–15:55	László Tóth – Almost invisible cloak in Oracle databases or the "undocumented" helps us again	Dániel Muszka – The Kalmár Era in Szeged
15:55–16:15	*break*	
16:15–17:00	Georgi Geshev – Breaking The Wall – Mission: Impossible	András Veres-Szentkirályi – Hacking hardware for fun and profit
17:00–17:05	*break*	
17:05–17:50	Felix Schuster – Design and implementation of an additional layer of encryption for Skype	Csaba Otti & Arnold Őszi – Fingerprint identification systems, security or security leak
17:50–17:55	*break*	
17:55–18:40	Roundtable: Sándor Léderer, Ádám Földes, Tamás Bodoky, László Csörgő – Wikileaks: info-freedom fight or info-terrorism?	Péter Gara-Tarnóczi – Customizing Public Exploit

HACKTIVITY - *SUNDAY*

	PIPACS Hall	SILENT Hall
09:00–09:45	Tamás Paulik – Who's living in my router? About the feasibility of botnet construction from embedded devices	Zoltán Hornák, Kristóf Kerényi, István Kispál– Crypto-chipset Security / Passive Active Combined Attacks
09:45–09:50	*break*	
09:50–10:35	**Raoul Chiesa / Keynote – Cybercrime, Information Warfare and CyberWar: what's this all about? False myths & true facts, from an hacker's perspective.**	
10:35–10:50	*break*	
10:50–11:35	Vivek Ramachandran – Enterprise Wi+Fi Worms, Backdoors and Botnets	Péter Bodor – Social engineering and psychology
11:35–11:40	*break*	
11:40–12:25	Pavol Luptak – Cryptoanarchy after 19 years since Crypto Anarchist Manifesto	Eszter Oroszi – Social Engineering - when the veil lifted
12:25–13:20	*launch break*	
13:20–14:05	Zoltán Balázs – IPv6 shipworm + My little windows domain pwnie	László Bíró – Stuxnet – Really the first one?
14:05–14:10	*break*	
14:10–14:55	Péter Gyöngyösi & Márton Illés – Firewalls and Exploits	Yaniv Miron – SCADA Dismal, or bang-bang SCADA
14:55–15:10	*break*	
15:10–15:55	Michele Orru – Dr. Strangelove or: How I Learned to Stop Worrying and Love the BeEF	Yaniv Miron – SCADA Hacking & Security Workshop
15:55–16:00	*break*	
16:00–16:45	Marcell Major & Mihály Zágon – Modern Browser Attack Vectors	Balázs Beregnyei – From silicon layout to circuit diagram
16:45–16:50	*break*	
16:50–17:35	András Kabai – Malware analysis, tips and tricks	
17:35–17:50	*Conference closure and farewell*	

CTF – Capture the Flag

A tavalyi nagy sikerű versengés után idén újra CTF! Annyit változtatással, hogy idén már kétfordulós a verseny, a 28 órás netes előselejtezőt szeptember 2-án tartottuk, s a Hacktivityn a legjobb 10 csapat méri össze az erejét. A Capture the Flag feladatra jelentkezett maximum 3 fős csapatoknak tíz órájuk lesz – a hagyományos Wargame-től szeparált hálózatban – távolról megszerezni az irányítást számítógép(ek) fölött, melyek a gyakorlatban is előforduló, sebezhető konfigurációkkal lesznek ellátva.

A játék döntőjének versenyideje: szombat 11.00 – vasárnap 15.00-ig.
Eredményhirdetés vasárnap 17.35-től a Pipacs teremben, konferencia záráskor!

A nyertes értékes tárgynyereményeket és a „2011-es Hacktivity legjobb hackercsapata" címet, és a hozzá járó vándordíjat viheti haza magával.

GLOBAL CYBERLIMPICS!

A világ első, az ENSZ cyber biztonsági szervezete (IMPACT) által támogatott nemzetközi csapatos etikus hackbajnoksága!

Mit érdemes tudni róla? Először is, hogy 2 fordulós. Az európai, régiós döntő a Hacktivityn kerül megrendezésre, majd a legjobb csapat Amerikába megy a döntőre! Csapatsport, legalább négy, legfeljebb hat játékossal zajlik. Minden csapat tagjai azonos nemzetiségűek kellenek legyenek, akárcsak az olimpián. A csapat feladata lesz megvédeni a saját hálózatát, míg mások támadják azt, valamint átvenni az irányítást a többi csoport rendszerei fölött – védekezz és támadj!

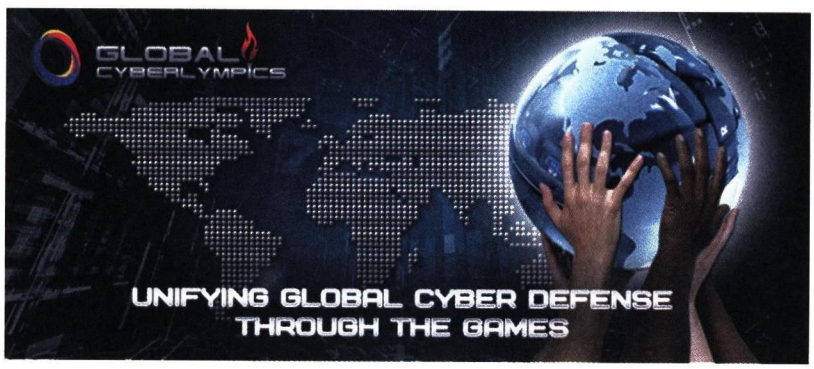
A verseny két fő részből és összesen 6 feladatból áll majd:

Támadók
- Webes alkalmazások támadása
- Operációs rendszerek kompromittálása
- Exploit vadászat
- Lock picking

Védekezők
- Szolgáltatásüzemeltetés
- Tartsd távol a támadókat!

A játék versenyideje: szombat 10.00–18.00-ig.
Eredményhirdetés: vasárnap 12.25-kor az ebédszünet előtt!

Az európai győztes csapat részt vehet az amerikai döntő bajnokságon 2012-ben és nyereményeket kap több mint 30 000 $ értékben!



WARGAME – előtérben a webes sérülékenységek

A játékpálya megalkotója a Webshark Kft. és a Silent Signal Kft. A játék egy szimulált betörési tesztgyakorlat-sorozat, mely különböző nehézségű pályákból áll. Minden szint teljesítésekor a versenyző egy jelszót kap, melyet az értékelési rendszerbe felvezetve jelzi a pálya teljesítését. Figyelj! Az idei játékban több feladatot social engineering alkalmazásával is leküzdhetsz! A legtöbb pályát teljesítő versenyző a nyertes. Minden versenyző saját laptopot használ.

Néhány dolog, amit ne tegyél:

* Ne támadd a versenyző társaidat!
* Ne DOS-olj!
* Ne támadd az értékelő rendszert!
* Ne tedd elérhetetlenné a játékot, ha valamelyik szerveren admin jogot szereztél!

A fentiek megsértése a játékból való kizárást vonhatja maga után!

Díjazás: értékes tárgynyeremények!

A játék versenyideje: szombat 12.00–vasárnap 12.00 között.
Eredményhirdetés vasárnap 17.35–től a Pipacs teremben, konferencia záráskor!

Wall of the Sheep - Birkafal

FIGYELEM: Ez egy HACKERkonferencia! Ha bekapcsolod a számítógépedet, számolj vele, hogy feltörhetik, finoman szólva is ez egy ellenséges környezet! Hogy tovább erősítsük a résztvevők biztonságtudatosságát, a Független Magyar Tudásközpont (H.A.C.K.) támogatásával felállítottunk egy kijelzőt az előtérbe, ahol regisztráltatok, ahová folyamatosan kitesszük a Wi-Fi hálózatokon talált felhasználóneveket és jelszavakat (jelszavakat csillagozva) :)

Hardver workshop 2 teremben!

1.LOCKPICKING TEREM: LOCPICKING WORKSHOP a locpicking blog szervezésében

Fordult már veled elő, hogy nem tudtál bejutni a lakásodba, mert elhagytad a kulcsot? Láttad, hogy mennyi idő alatt törik a zárat a zárnyitók? 5 másodperc? A roncsolásmentes zárnyitás ennél trükkösebb és nagyobb kihívás. A feladat ugyanaz: bejutni, csak most a zár törése nélkül. Nem lehetetlen, de sok gyakorlást és tanulást igényel. A konferencián mindkettőre lesz lehetőség, lesz lockpicking előadás, és berendezünk egy szobát, ahol folyamatos szakmai segítség mellett gyakorolhatod a zárnyitás művészetét.

2. HACKERSPACE (:
Programozható mikrokontroller workshop a Hackerspace szervezésében

Forraszd össze a saját arduino-dat és utána együtt programozzuk fel. Továbbá lesz megint a nagysikerű 3D nyomtatóhackelés és burnstation 2.0.

A workshopon részt vevőknek biztosítunk metaboard jellegű arduino klon kiteket (http://metalab.at/wiki/Metaboard), melyeknek önköltségi ára: 4000 Ft.

Hackelj és bulizz!

Leisure Zone

Pihenés, kellemes beszélgetések, könyvek és Szőr Péter könyvdedikálás – szombaton 12.50–13.50 között a könyvsarokban! Idén kiemelt hangsúlyt kap a Hacktivityn a networking és a kikapcsolódás. A földszinten kellemes beszélgetéseknek helyet adó kényelmes babzsáktér, kávézó és a legújabb szakkönyvekkel teli könyvsarok vár benneteket. És kapható lesz Szőr Péter vírusbibliája is, amit nem csak megvásárolni, de dedikáltatni is lehet majd 12.50–13.50 között ugyanitt!

Hacker tanösvény

Járd végig a HP Hacker tanösvényt és szerezd meg a CERTIFIED HACKER ROAD PARTICIPANT PROFESSIONAL MINŐSÍTÉST!:)
A tanösvény egy olyan kiépített gyalogút, amin végigsétálva megismerkedhetsz a konferencia különböző helyszíneivel és EGYIDEJŰLEG MAGASAN KÉPZETT HACKERRÉ FOGSZ VÁLNI.

A tanösvényt teljesített és jelen levő túrázók között vasárnap záráskor (17.35) kisorsolunk 3 darab fél terrás hordozható merevlemezt a HP jóvoltából.

Az induláshoz kérd el a menetlevelet az RRC standján!

Kiállítói programok – *Történelem a lábunk, akarom mondani a Hacktivity alatt!*

Tudod, mi az az M-3? Na nem a metróra gondolunk, hanem az első magyar elektronikus (elektroncsöves), digitális, programvezérelt, automatikusan működő számítógépre. Kíváncsi vagy, milyen lehetett, hogy működött? Milyen körülmények között épült? Szívesen beszélnél azzal, aki építette? Igen?!

Az emeleten a Szegedi Informatikai Történeti Múzeum Alapítvány gyűjteményének köszönhetően felélesztett ősrégi számítógépek és néhány ritkaság vár Benneteket! Lesz működő telexgép, itt lesz Muszka Dániel és az általa megalkotott szegedi elektronikus katicabogár másolata (ami máig is az egyetlen hazai műállat, bogár-formájú feltételesreflex-modell), és látható lesz többek között egy IBM 3270-es terminál is! És ha tetszett a kiállítás, ülj be a történeti szekciónk 2 előadására szombaton 14.20-15.55-ig a Silent terembe!

14:20–15:05 – Kovács Győző - Válogatott kalandozásaim Informatikában
15:10–15:55 – Dr. Muszka Dániel – Kalmár-korszak Szegeden

ÉS EZÚTON IS SZERETNÉNK KÖSZÖNETET MONDANI A TÖRTÉNETI SZEKCIÓ SZAKMAI PARTNERÉNEK:
Az NJSZT Informatikai Történeti Fórumnak

Étel- és italfogyasztás

Az ebéd árát a konferencia díj nem tartalmazza, de a helyszínen két büfé is vár Benneteket finomságokkal és meleg étellel. És mára már hagyomány, hogy a szponzorok játékokkal és ingyenes finomságokkal is várnak, kényeztetnek Bennünket! Mi várható idén?

Ingyen sör a Noreg Kft. támogatásával! Keresd a folyamatosan mobil SegWay-es Noreg hostesseket és kérj tőlük sörkupont, amit aztán beválthatsz a büfékben!

Ingyen pizza az RRC és disztribútorai jóvoltából! Keresd a pizza tálcát az RRC standon!

Ingyen kávé a Sabretooth Globál jóvoltából! Keresd a standjukat a kuponért és vigyél névjegyet!

Szombat esti Kontinens Party – a Balabit támogatásával

Tavaly egy résztvevő azt mondta többet tanult az este alatt folytatott beszélgetésekből, mint egy komplett 5 napos tréningen. A szombat esti party a Balabit támogatásával 19.00-tól indul a konferencia helyszínén a földszinti Leisure Zone-ban! Lazulj el, találd meg az előadót, akinek legjobban tetszett a prezentációja, mutass neki jobbat, ellenkezz vele – légy részese az estének! „Láttál" valami érdekeset az elmúlt 1 évben – készülj, az este megmutathatod – kivetítőt biztosítunk! Mindehhez idén Dj adja az aláfestő jó zenét!

Keresd a csomagban található RRC kérdőívet, töltsd ki és hozd magaddal az emeleti standunkra, hogy megvendégelhessünk egy pizzaszeletre!

Find the RRC questionnaire in the package, fill it in, bring it with you to our stand on the first floor and be our guest for a slice of pizza!

rrc THINK VALUE.

cisco | IronPort Email and Web Security

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

rrc education

SONICWALL

VASCO THE AUTHENTICATION COMPANY

splunk>

TippingPoint

hp

CTF - Capture the Flag

Last year's highly successful CTF continues in a slightly changed format. This year the competition has two rounds: the 28-hour online qualifying round was held on September 2. In the finals the top 10 teams will compete at Hacktivity. The teams of maximum 3 people participating at the Capture the Flag game will have ten hours to remotely achieve control over computer(s) with vulnerable configurations found in the real world (on a network separated from the traditional Wargame).

Date of the finals: Saturday from 11.00 to 21.00.
Results will be announced at 12:50 on Sunday before lunch in the Pipacs Hall.

The winner will receive valuable prizes, the title „Best Hacker Team at Hacktivity 2011" and the challenge cup.

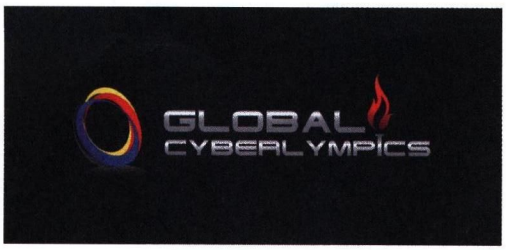
GLOBAL CYBERLIMPICS! *The world's first international team ethical hacking championships endorsed by the cyber security executing arm of the United Nations (IMPACT).*

What do you need to know? There are 2 rounds. The European regional finals will be held at Hacktivity and the best team will travel to the US for the finals. It's a team sport where a team will consist of at least four players and no more than six players. All members of the team must be of the same nationality just like at the Olympics. The team will be responsible for defending their own network under attack and trying to gain control over the other teams' systems – defend and attack! The registration fee is $ 100 per team.

The Championship will be made up of two parts and a total of 6 tasks:

Attackers
- Attacking web applications
- Compromising operating systems
- Exploit hunting
- Lock picking

Defenders
- Service uptime
- Keeping attackers out



Date of the Championship: Saturday from 10.00 to 18.00
Results will be announced: Sunday 12.25 before lunchbreak

The European winner team will participate at the finals in the US in 2012 and will receive prizes worth over $ 30,000!

WARGAME – Web Vulnerabilities in the Focus

The designer of this game is Webshark Kft. and Silent Signal Kft. The game is a series of simulated penetration tests made up of courses of different difficulty levels. When a level is completed the player will receive a password which must be entered into a scoring system to confirm the completion of the course. Please note that this year you can do several tasks by using Social Engineering! The player completing the highest number of courses will win. All players will use their own laptops. Date of the finals: Saturday from 12.00 to Sunday 12.00. Results will be announced on Sunday.

Things you shouldn't do:
* attack other contestants
* use DOS
* attack the scoring system
* make the game unavailable if you have gained admin rights on one of the servers.

Violating the above may lead to disqualification from the game!

Prizes: valuable gifts!

Date of the finals: Saturday from 12.00 to Sunday 12.00
Results will be announced at 17:35 p.m. on Sunday at the closing ceremony in the Pipacs Hall.

Wall of the Sheep - Birkafal

PLEASE NOTE: this is a HACKER conference! If you switch on your computer you can count on it being hacked in this hostile environment, to say the least. To improve participants' security awareness a display will be set up with the help of the Hungarian Autonomous Centre for Knowledge (H.A.C.K) to show all user names and passwords (marked by asterisks) found on Wifi networks :)

Hardware Workshops in 2 Halls!

1. LOCKPICKING HALL: Lockpicking Workshop Organized by Lockpicking Blog

Have you ever lost your key and couldn't get into your apartment? Did you see how long it took the locksmith to break the lock? 5 seconds? Lockpicking without breaking is a trickier and bigger challenge. The task is similar: entering but without breaking the lock. It's possible but it requires plenty of practice and learning. You will need both at the conference where you can listen to a lecture on lockpicking and there will be a room where you can practice the art of lockpicking under ongoing professional assistance.

2. HACKERSPACE (H.A.C.K.) HALL: Programming Microcontrollers Workshop Organized by Hackerspace

Weld you own arduino and let's do some programming. We will have the highly successful wall of lame, 3D printer hacking and burnstation 2.0 again.
Participation is free of charge. We provide participants with metaboard arduino clone kits (http://metalab.at/wiki/Metaboard) which cost HUF 4,000.

Leisure Zone

Relaxation, pleasant conversation, books, book-signing by Peter Szor on Saturday between 12.50 and 13.50 in the book corner! Networking and relaxing will have a special place at Hacktivity this year. On the ground floor a bean-bag area suitable for pleasant chats, a café and a book corner full of the latest specialist books will be available for visitors. Peter Szor's anti-virus Bible will also be available for sale and for signing between 12.50 and 13.50 in the book corner.

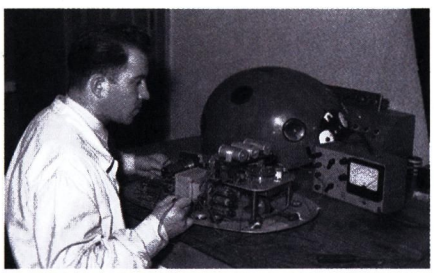
Hacker Road

Walk the HP Hacker Road and get the CERTIFIED HACKER ROAD PARTICIPANT PROFESSIONAL CERTIFICATE :) If you hike along the road you can get to know the different locations of the conference and will become a highly qualified hacker.

Hikers who walked along all the roads will have the chance to win one of the three 500Gb external HDDs at 17.35 on the stage in the large hall.

To start hiking get your passport at the RRC stand!

Exhibitor's Programme / *History at Hacktivity*



Do you know what M-3 is? No, we don't mean the metro line but the first electronic, digital, programmed and automated computer (with electron tubes). Do you want to know what it looked like and how it worked? How was it built? Would you like to talk to the guy who built it? Yes?!

On the top floor an exhibition of ancient computers reborn and other rarities will be held thanks to the collection of the Szeged Computer Science Museum Foundation. There will be a telex machine in working order, Dániel Muszka and a copy of the electronic ladybird he had created in Szeged (the only Hungarian artificial animal up to now, a bug-shaped conditioned reflex model) as well as an IBM 3270 terminal. If you liked the exhibition come and listen to the 2 lectures of the Historical Section held on Saturday between 14.20 and 15.55 in the silent room!

14:20 - 15:05 - Győző Kovács – My Assorted Wanderings in IT
15:10 - 15:55 - Dr. Dániel Muszka – The Kalmár Era in Szegeden

WE WOULD LIKE TO THANK OUR PARTNER IN THE HISTORICAL SECTION: the Forum of Information Technology History at the John von Neumann Computer Society

Hack and Party

Food and Drinks

Lunch is not covered by the conference charge but there will be two bars providing delicious snacks and hot food at the conference venue. And it is now a tradition that visitors are spoilt by games and free food and drinks offered by the sponsors! What can you expect this year?

Free beer, sponsored by Noreg Kft. Find the Noreg hostesses riding on SegWays and ask them for a beer coupon that you can redeem at the snack bars.

Free pizza, sponsored by RRC and its distributors. Look for the pizza tray at the RRC stand!

Free coffee, sponsored by Sabretooth Global. Find their stand to get a coupon and bring a business card with you!

Saturday Night Continent Party – Sponsored by Balabit

Last year a participant told us that he learnt more from the conversations he had during the evening than at a 5-day training course. The Saturday night party, sponsored by Balabit, will start at 18.00 in the Leisure Zone on the ground floor at the conference venue. Chill out, find the speaker whose presentation you liked best, show him something better, confront him – be part of the night! Did you „see" something interesting last year – get ready, you can show us – a projector will be waiting for you. This year a DJ will be giving us good music.

Szőr Péter / keynote

Küzdelem a kártékony kódok ellen

Fighting Computer Malware

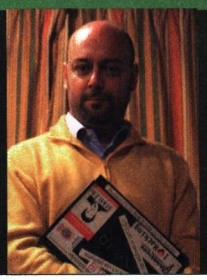
A személyi számítógépes vírus mint probléma az idén 25 éves. Látni fogjuk, hogy a legkorábbi számítógépes kártékony fenyegetések közül sok az antivírustermékek elleni küzdelemben rejtőzködési és később alakváltó technikákat vetett be. A modern fenyegetések a múltból ismert technikákra épülnek. Ezek a régi technikák az idők folyamán fejlődtek kifinomult rootkitekké és az új platformokon kihasználható technikákká, amelyeket az olyan botnetek is használnak, mint a TDSS, napjaink egyik legelterjedtebb botnete. Az előadás részletesen tárgyalja az alakváltási technikák fejlődését, hogy bemutassa, az évek során hogyan tudott a kártékony technológiák középpontjában maradni. Az előadás szemléltetni fogja, hogy az új technikák milyen gyorsan fejlődnek az olyan új platformokon, mint a mobil-kártékonykódok, és hogyan változik a kártékony kód környezete vele együtt. Képet kapunk a támadó motivációiról is, a pénzszerzési módszerekről. Friss példákat láthatunk, mint a Google Engine Poisoning által terjesztett FakeAV, példákat gyanús cégekről és tevékenységeikről, olyanokról, amelyek a kártékony kódok fejlesztőit és társaikat fizetik, hogy világszerte terjesszék a támadásaikat. Ezek a cselekmények szintén kapcsolódnak a rootkitekhez, amelyek egyre nagyobb mértékben támadnak biztonsági termékekre. Szó lesz a legújabb rootkittechnikákról, mint az új DKOM technikák, az általános biztonságitermék-gyilkos technikák, ahogy azt mostanában a Max++ és TDSS-variánsok implementálták. A közelmúltban nagyon kifinomult támadásokat láthattunk, ezért az előadás az ICS (Industry Control Systems – ipari ellenőrző rendszerek) történetére is kitér, külön kiemelve a Stuxnet férget, amelyet évekbe telt megépíteni, bemutatva annak támadási technikáit és rootkittechnológiáját. Milyen a Stuxnet utáni világ?

Számos antivírus-keresőmotoron dolgozott az elmúlt évtizedben, a Pasteur, F-PROT, AVP, Norton AntiVirus és mostanában a McAfee VirusScan motorján. Péter a vírusazonosítás és behatolásvédelem területén több mint 40 találmány szerzője. 1997-ben felkérték, hogy csatlakozzon a CARO-hoz (Computer Antivirus Researchers' Organization). Többek között a Virus Bulletin, az RSA és Usenix Security konferenciák gyakori előadója. Az elmúlt évek során Péter szívesen dolgozott számos biztonsági kutatóval a Data Fellowsnál (F-Secure), a Symantecnél és a McAfee-nél. Ő a szerzője a 2005-ben az Addison Wesley gondozásában megjelent „The Art of Computer Virus Research and Defense" bestseller technikai könyvnek. A könyvet a lengyel, cseh, kínai és magyar mellett egyéb nyelvekre is lefordították. Péter szabadidejében „vallásosan" szeret szörfözni.

The PC computer virus problem is 25 years old this year. We will learn, that many of the earliest computer malware threats introduce stealth capacities and later on polymorphic techniques to fight back against Antivirus products. These old techniques evolved over the years to sophisticated Rootkits and exploitation techniques on new platforms, which are utilized by botnets, such as TDSS, that are very prevalent today. The presentation will detail the evolution of polymorphic techniques to show how it remains the center of the malware technology over the years. It will be demonstrated how quickly new techniques evolve on new platforms such as mobile malware, and how the environment of the malware changes rapidly accordingly. We will also learn about the motivation of the attackers, targeting money. Recent examples such as FakeAV distributed by Google Engine Poisoning will be discussed, with examples of shady companies, and their operations behind it, which pay malware authors and affiliates to distribute their attacks globally, all around the world. Such operations are also connected to rootkits, which increasingly fight back against security products. Recent techniques from rootkits will be discussed, such as new DKOM techniques, generic security product killing techniques, as implemented by recent Max++, and TDSS variants, to name a few. There are very sophisticated attacks, which happened in the recent past, and the presentation will also show the history of ICS (Industry Control Systems) attacks, with highlights from the Stuxnet worm, which took years to build, showing its exploitation techniques and its rootkit technology. How the world looks like after Stuxnet?

He worked on various anti-virus scanning engines over the last decade including Pasteur, F-PROT, AVP, Norton AntiVirus, and recently McAfee VirusScan. Peter is the author of over 40 inventions on computer virus detection, and intrusion prevention. He was invited to join CARO, the Computer Antivirus Researchers' Organization in 1997. He is a frequent speaker at Virus Bulletin, RSA and Usenix Security conferences among others. Over the years Szor enjoyed working with many security researchers at Data Fellows (F-Secure), Symantec, and McAfee. Hi is the author of best selling technical book "The Art of Computer Virus Research and Defense" published by Addison Wesley in 2005. The book has been translated to several languages, including Polish, Czech, Chinese and Hungarian. As a "religion", Peter enjoys surfing in his free time.

Raoul Chiesa / keynote



Kiberbűnözés, információs hadviselés és kiberháború: mi ez az egész? Tévhitek és igazságok a hacker nézőpontjából

[vagy más néven: „Az öreg hackerek csupa szentek voltak napjaink történései fényében":( ]

Cybercrime, Information Warfare and CyberWar: what's this all about? False myths & true facts, from an hacker's perspective.

[a.k.a. „Old times hackers were just saints, compared to nowadays' scenarios":( ]

Ez a Keynote bevezeti a hallgatóságot napjaink kiberháborújába vagy más néven információs hadviselésébe, eloszlatva a különböző terminológiák használata körüli félreértéseket, más néven, mi számít információs hadviselésnek, és mi nem.

Az előadó a hackelés kezdeteitől indítva követi végig az utat egészen napjaink kiberbűnözéséig, majd röviden elidőzik a Stuxnet „incidensnél", mielőtt továbbugrik a „munkaeszközökre", végül az Irán elleni támadást mint kiindulást felhasználva „hasonlítja össze a fegyvereket", és mit jelent hadifogolynak lenni háborús és IT-biztonsági/IT-s környezetben.

Az előadás befejező része a világ különböző katonasági és kormányai által nem igazán felismert úgynevezett „paradigmaváltást" veszi közelebbről szemügyre.

Megjegyzés: a prezentáció Mr. Jart Arminnal (CyberDefcon, HostExploit) közös munka eredménye.

This Keynote will bring the audience into today's "Cyber War" aka Information Warfare, clearing out those misunderstandings on the terminologies to be used, i.e. "what is" and "what is not".

In order to run this path, the speaker will start from the hacking roots up to today's cybercrime, then will briefly focus on the Stuxnet "incident", jumping to the "Tools of the Trade", then taking the Iran's attack as a starting example in order to run a "Comparison of Weapons", from a military environment PoW 'till InfoSec & IT PoW.

The last part of the talk will analyze the so-called "Paradigm Shift" that Mils and Govs from all over the world are not fully realizing (yet).

Note: this presentation has been designed along with Mr. Jart Armin (CyberDefcon, HostExploit).

Raoul „Nobody" Chiesa Olaszországban, Torinóban született 1973-ban. Miután a 90-es években (1986–1995) az első olasz hacker volt, elhatározta, hogy hivatalosan is InfoSeckel fog foglalkozni, ezért 1997-ben megalapította a @ Mediaservice.net Srl gyártófüggetlen és jól ismert biztonsági tanácsadócéget. Raoul egyike a CLUSIT – Olasz Informatikai Biztonsági Szövetség – alapító tagjainak, és az ISECOM, CLUSIT, OWASP olasz fejezetének, az Italian Privacy Observatory (AIP/OPSI) igazgatótanácsainak tagja. 2003 óta az UNICRI (United Nations Interregional Crime and Justice Research Institute) ENSZ-ügynökséggel dolgozik együtt a HPP (Hackers Profiling Project) projekten. Mostanában az UNICRI-ben Senior Advisor, Strategic Alliances and Cybercrime Issues Technical Contact Officer pozíciót tölt be. 2010 februárjában Rault Európa legjobb 30 biztonsági szakértője közé választották, aki az ENISA-igazgatókat segíti 2012-ig.

Raoul "Nobody" Chiesa was born in Torino, Italy, in 1973. After being among the first italian hackers back in the 90's (1986-1995), Raoul decided to move to professional InfoSec, founding in 1997 @ Mediaservice.net Srl, a vendor-neutral and well known security consulting company. Raoul is among the founder members of CLUSIT – the Italian Information Security Association – and he is a Board of Directors member at ISECOM, CLUSIT, OWASP Italian Chapter, Italian Privacy Observatory (AIP/OPSI). Since 2003 he started its cooperation with the UN agency "UNICRI" (United Nations Interregional Crime and Justice Research Institute), working on "HPP", the Hackers Profiling Project. Nowadays his role at UNICRI is "Senior Advisor, Strategic Alliances and Cybercrime Issues Technical Contact Officer". On February 2010, Raoul has been selected among the 30 European top security expert to assist the ENISA Director until 2012.

Barta Csaba

Az NTDS.DIT forensic vizsgálata

Forensic analysis of NTDS.DIT

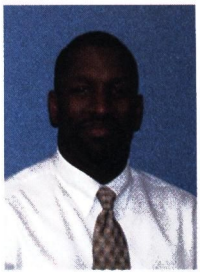
Az előadó bemutatja saját fejlesztésű forensic keretrendszerét, amely a Microsoft Windows- tartományok (Active Directory) központi adatállományának (NTDS.DIT) vizsgálatát segíti a benne tárolt értékes információk kinyerésével. Ennek az információforrásnak a vizsgálatára a szakma eddig nem rendelkezett megfelelő eszközökkel. Az előadó olyan bizonyítékok kinyerését is bemutatja, amelyek csak ebben az adatállományban találhatóak meg. A bemutatandó eszközkészlet különböző moduljai másmás vizsgálandó adatokat képesek rendezett, feldolgozható formában kinyerni.

The presentation introduces a software framework developed by the speaker for the forensic analysis of NTDS.DIT which is the main database of Microsoft Active Directory. Until now the forensic field did not have the appropriate tools for processing this information source. The speaker will also show how to obtain information stored nowhere else, but NTDS.DIT. The tools are capable of extracting different information in a form that is suitable for further processing and analysis.

Csaba menedzserként dolgozik a Deloitte informatikai biztonság és adatvédelem üzletágában, több mint 6 év tapasztalattal. Számos konfiguráció- és forráskódelemzésben, binárisalkalmazás-tesztelésben, illetve külső és belső betörési tesztben vett részt. Mielőtt a Deloitte-hoz csatlakozott volna, Csaba 2 és fél évig dolgozott egy másik „big 4" cégnél hasonló területen. Karrierjét az OTP Bank Nyrt.-nél kezdte, az információbiztonsági főosztályon, szoftverfejlesztőként. Munkái során mély szakmai ismeretekre tett szert a kriptográfia, a reverse engineering, a hálózati biztonsági protokollok, a vezeték nélküli technológiák (Wi-Fi, Bluetooth) és a biztonságos szoftvertervezési és implementációs megoldások terén. Kiemelt szakterületei a betörési tesztek, a computer forensics és az incidensreagálás. Csaba Computer Hacking Forensic Investigator (CHFI) és hivatalos CHFI-oktató. Számos hazai és nemzetközi konferencián tartott előadást. Több publikációja is megjelent computer forensic és malware research témában.

Csaba is currently employed as a manager at the Security & Privacy group of Deloitte Hungary's Enterprise Risk Services service line with over 6 years of experience. He has worked on a number of projects involving configuration analysis, source code audits, analysis of binary applications and external and internal penetration tests. Prior to joining Deloitte, Csaba had been working for another Big4 company in a similar area for 2 and a half years. He began his career at the Information Security Department of OTP Bank NyRt. as a software developer. During the course of his work he has acquired deep technical expertise in the areas of cryptography, reverse engineering, network security protocols, wireless technologies (Wi-Fi, Bluetooth) and secure software design and implementation methods. His main areas of expertise include penetration testing, computer forensics and incident response. Csaba is a Computer Hacking Forensic Investigator (CHFI) and a certified CHFI instructor. He has held seminars at numerous conferences both in Hungary and worldwide. In addition, he has published research papers on computer forensics and malwares.

Joe McCray



Van rá progi: mobilalkalmazások pentesztje

There's An App For That: Pentesting Mobile Applications

A Wikipédiából: „Az okostelefon egy olyan mobiltelefon, ami napjaink általános telefonjaiban elérhető funkciókhoz képest fejlettebb számítási és kapcsolattartási képességeket kínál. Az okostelefonokra és a hagyományos mobiltelefonokra úgy is gondolhatunk, mint egy kézi számítógépekre integrált mobil telefonálási lehetőséggel. De amíg a hagyományos mobiltelefonok JavaME-hoz hasonló platformon képesek alkalmazásokat futtatni, addig az okostelefonok rendszerint megengedik a felhasználónak, hogy sokkal bonyolultabb alkalmazásokat telepítsenek és futtassanak. Az okostelefonok teljes értékű operációs rendszert futtatnak, az alkalmazásfejlesztőknek biztosított platformmal együtt. Így ezek a kamerás telefonok és a PDA-k funkcióit ötvözik." Szerezzünk egyet, és építsünk egy Android/iPod/iPhone/iPad környezetet, használjuk az Android/iPod/iPhone/iPadet mint egy pentest platformot, fejtsük vissza az Android/iPod/iPhone/iPad alkalmazásokat, törjünk Android/iPod/iPhone/iPad alkalmazásokat, támadjunk webes szolgáltatásokat Android/iPod/iPhone/iPad alkalmazásokon keresztül.

Joe részt vett több mint 150 magas szintű pentestben, és sikerült néhány jelentősebb hacket végrehajtania, amelyek tapasztalatait az ügyfeleivel és a diákjaival örömmel osztja meg. Széles körű tapasztalata és alapos tudása – s mindez könnyed stílussal keverve – az egyik leginkább keresett előadóvá tette az iparágban. Joe előadásokat és szemináriumokat tart az IT-biztonsági közösség legnagyobb eseményein, mint a Black Hat, Defcon, BruCon, Hacker Halted és így tovább. Joe megkapta a 2009-es EC-Council Instructor Circle of Excellence és a 2010-es EC-Council Instructor of the Year díjat. Alapítója és vezérigazgatója a http://strategicsec.com informatikai biztonsági tanácsadócégnek, amely részletes technikai hálózati és webes alkalmazásbiztonsági elemzéseket, valamint jogszabályi előírásoknak való megfelelésvizsgálatokat végez.

"A smartphone is a mobile phone that offers more advanced computing ability and connectivity than a contemporary feature phone. Smartphones and feature phones may bethought of as handheld computers integrated with a mobile telephone, but while most feature phones are able to run applications based on platforms such as Java ME, asmartphone usually allows the user to install and run more advanced applications. Smartphones run complete operating system software providing a platform forapplication developers. Thus, they combine the functions of a camera phone and a Personal digital assistant (PDA)." Let's own one shall we..... * Building the Android/iPod/iPhone/iPad environment * Using Android/iPod/iPhone/iPad as a Pentest Platform * Reverse Engineering Android/iPod/iPhone/iPad Apps * Exploiting Android/iPod/iPhone/iPad Apps * Attacking Web Services via Android/iPod/iPhone/iPad Apps

Joe has been involved in over 150 high level penetration testing engagements and has some major hacking accomplishments that he can share with his students and clients. His extensive experience and deep knowledge, mixed with his comedic style has lead Joe to be one of the most highly sought after speaking experts in the industry. Joe makes speaking appearances and gives seminars at major events in the security community such as Black Hat, DefCon, BruCon, Hacker Halted and more. Joe is the recipient of the 2009 EC-Council Instructor Circle of Excellence Award and the 2010 EC-Council Instructor of the Year Award. Joe is the founder and CEO of http://strategicsec.com an IT Security consulting firm that provides in-depth technical security assessments of your network, web application, and regulatory compliance gap analysis.

Alexander Kornbrust

Oracle-forensic

Oracle Forensic

Az előadás az Oracle-forensicsről és arról szól, hogyan tud egy ember mély adatbázis-szakértelem nélkül forensicelemzést végezni. Az adatbázis-forensic két legnagyobb nehézsége az adatbázisok bonyolultsága (mi és hol került tárolásra), és hogy az SQL-t „anyanyelvi szinten" kell ismerni. A sikerességhez az outer join, self join halmazműveletek, az adatok importálása jelen állás szerint szükséges, hogy (jó) eredményt érjünk el. Az adatok exportjának hagyományos módja az SQL*Plusban a spoolfile-lal éles helyzetben olyan, mint tűt keresni a szénakazalban.

Bevezetés, az Oracle-forensic aktuális helyzete (adatok gyűjtése, könyvek, ajánlások)
Oracle-forensic-problémák (hogyan kell elemezni a begyűjtött adatokat?)
Rendelkezésre álló eszközök
Új, fejlett megközelítés
Fejlett adatgyűjtés
Tipikus minták

Alexander Kornbrust az Oracle-biztonsággal foglalkozó Red-Database-Security cég alapítója. A világ minden táján végez Oracle-biztonsági auditokat, biztonsági oktatást és tanácsadói tevékenységet. Kornbrust emellett az „SQL Injection Attacks and Defense" című könyv társszerzője is. Kornbrust 1992 óta foglalkozik az Oracle termékeivel, fő szakterülete az Oracle-adatbázisok biztonsága és a biztonságos szoftverarchitektúrák. Az elmúlt 6 évben Kornbrust több mint 350 biztonsági programhibát jelentett az Oracle-nek, és számos informatikai biztonsággal foglalkozó konferencián – pl. Black Hat, Defcon, Bluehat, HITB stb. – tartott előadást. Kornbrust a Passaui Egyetemen szerzett M. A. fokozatot számítástechnikából.

One of the biggest problems in database forensics so far is the complexity of the databases (what is stored where) combined with the need to "speak" SQL. Knowing and using stuff like Outer joins, Self joins, Set operators and data import are at the moment necessary to get (good) results. The traditional approach to export data using SQL*Plus with a spoolfile is normally not helpful in the real world and is more finding the needle in the haystack.

Introduction
Current status of Oracle forensic (artifact collection, books, recommendations)
Oracle Forensic problems (how to analyze the collected artifacts)
Available tools
New advanced approach
Advanced Artifact collection
Typical patterns

Alexander Kornbrust is the founder of Red-Database-Security a company specialized in Oracle security. He provides Oracle security audits, security training and consulting to customers worldwide. Alexander is also the co-author of the book "SQL Injection Attacks and Defense ". Alexander has worked since 1992 with Oracle and his specialties are the security of Oracle databases and secure software architectures. In the last 6 years Alexander has reported more than 350 security bugs to Oracle and gave various presentations on security conferences like Black Hat, Defcon, Bluehat, HITB, etc Alexander holds a masters degree in computer science from the University of Passau, Germany.

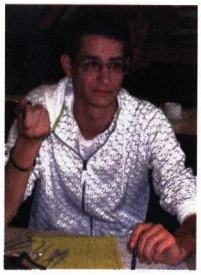
Come work with Vodafone!

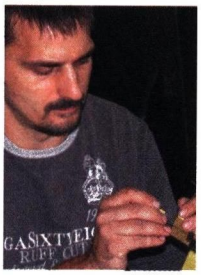
Career at a multinational company? International assignments? Leading edge IT security technologies & solutions? Long term development path & training opportunities?

Vodafone Operations Centre Hungary is looking for qualified professionals for the following roles:

- **Network or EndPoint Security Engineer (e.g. CISSP, CCIE etc.)**
- **Ethical Hacking Specialist**
- **Security Appliance System Administrator**
- **Project Manager or Service Management Specialist**

APPLY here: **careercentre.hu@vodafone.com**
www.vodafone.com/operationscentre





Subecz Ákos, Zánthó Csaba

Lockpicking – a zárnyitás művészete

Lockpicking – the finest art of opening locks

Előadásomban a lockpicking alapjaival szeretném megismertetni a hallgatókat. Idetartozik a zártípusok és felépítésük rövid bemutatása, valamint azok támadhatósága. Be kívánom mutatni az alapvető szerszámokat és említésszerűen az alaptechnikákat (bővebben pedig a workshopon). Négy kategóriába csoportosítom a zárakat a biztonsági szintjüknek megfelelően, majd végül felhasználási, alkalmazási javaslatot adok, bemutatva a legmodernebb védekezést a finomnyitás, azaz a lockpicking ellen. Az előadásban animációk segítik a működés és a technikák könnyebb megértését, ami által a prezentáció végén már egy kezdő is képzett lockpickernek gondolja magát :-).

Ákos 22 éves egyetemi hallgató, lockpicker. Tavaly kijutott a német SSDeV bajnokságra, ahol a B finálé 5. helyén végzett kézi nyitás versenyszámban. A Buhera blogról tévedt anno a lockpick.blog.hu internetes oldalra, ahol ez a hobbitevékenység felkeltette az érdeklődését. Azóta aktívan űzi a lockpickinget mint sportot. 2010 augusztusában megtartották az első magyar lockpic-king találkozót, ahol kialakult egy törzscsapat. Így most már közösségileg tudnak tapasztalatot cserélni és egymást segítve előrehaladni a magyar lockpicking hobbi népszerűsítésében. Szintén 2010 augusztusában bekerült a lockpick.blog.hu szerkesztői csapatába, ahol a Nyitva! lista rovatszerkesztője, de más cikkekkel is emeli az oldal színvonalát. Tavaly kijutottak a német SSDeV bajnokságra, ahol a B finálében végzett kézi nyitás versenyszámban. A Buhera-sörözésen tartották az első nyilvános előadásukat, és mivel ez a visszajelzések alapján jól sikerült, szeretnének továbbra is kapcsolatot tartani az IT-biztonság területével.

Csaba 36 éves, foglalkozása eredetileg épületgépész, melyben aktívan tevékenykedik. Lockpickinggel tavaly március óta foglalkozik aktívan, több országos találkozón vett részt, és a német bajnokságon is a magyar csapatot erősítette, B finálé 3. helyezettként.

In my presentation I will introduce the audience to the basics of lockpicking such as lock types, short explanation of their design and vulnerabilities. I'm going to show the most fundamental tools and we will take a cursory look at the basic techniques as well (for more details see the workshop). I classify locks into 4 different classes by their security levels. Then I will give application and usage advice by showing the latest protections against lockpicking. Animations will help the audience to undestand operation and techniques so that at the end of presentation even a beginner lockpicker fancies himself an expert :-)

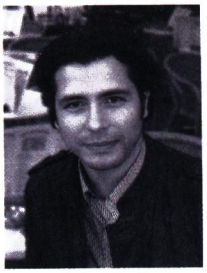
I'm a 22-year-old university student who is engaged in lockpicking for several years. I stumbled upon lockpick.blog.hu blog from buhera's site which raised my interests in this hobby. Since then lockpicking transfered from a hobby to a sport activity. We held the first Hungarian lockpicking meeting in August 2010, where a core lockpicker community was formed. This core team can help and inspire each other to advance lockpicking in Hungary. I was invited to lockpick.blog.hu as editor also in August 2010 where I'm in charge of editing Open! list.

Csaba is 36-year-old and works as building engineer. He is engaged in lockpicking since last March. Since then he participated in nationwide venues and was the member of the Hungarian team at German lockpicking championship where they hit the third place in finals B.

Ertunga Arsal

Rootkitek és trójaik az SAP alkalmazásrendszerekben

Rootkits and Trojans on Your SAP Landscape



Az SAP rendszerek számos vállalkozásban játszanak központi szerepet. A legtöbb üzletkritikus funkció SAP alkalmazáson fut, és ezeknek az alkalmazásoknak a bonyolultsága nagyon nehézkessé teszi a támadók elleni védekezést. Az alapértelmezett beállítások, az elfelejtett, nem megvalósított biztonsági beállítások, a kevésbé „fontos" rendszereken alkalmazott gyenge jelszókezelési és változáskezelési eljárások a teljes SAP alkalmazásrendszer kompromittálásához vezethetnek. A jogi következmények, az elveszett/sérült üzlet és hírnév a támadás fajtájától függően akár katasztrofális is lehet. Amíg a legtöbb cég sokat költ az SAP rendszerek üzletifolyamat-szintű biztonságára, például a hozzáférési rendszer koncepciójának megtervezésekor, a feladatok szétválasztásának megvalósításával vagy GRC-rendszerek (Governance Risk and Compliance) használatával, addig a technikai szintű biztonságra nem fordítanak figyelmet. Előadásomban bemutatok számos támadási módot, amelyek a technikai szintű konfigurációs gyengeségeket használják ki, és egy rendszer támadásától a teljes SAP alkalmazásrendszer és végül az egész vállalati hálózat támadásáig vezethetnek. A konfigurációs gyengeségek elleni különböző, kreatív támadások bemutatásával mindenkit az SAP rendszerek technikai szintű védelmére kívánok ösztönözni.

Ertunga Arsal az alapítója az ESNC, az SAP®-biztonságra szakosodott cégnek, ahol az SAP-rendszerek biztonsági és forensic vizsgálatára is folyik szoftverfejlesztés. Ertunga a Tech Data (Nasdaq: TECD) biztonsági tanácsadója volt 5 évig, ahol az EMEA régióban az SAP és az alkalmazások biztonságáért volt felelős. A biztonsági incidenskezelő csoport tagjaként személyesen vezetett több vizsgálatot. Ertunga számos SAP-biztonságihibát jelentett, a közepestől egészen a rendkívül kritikus hibákig. Jelenleg a Sabanci Egyetemen oktat rendszer- és hálózatbiztonságot végzősöknek.

SAP systems are the heart of many enterprises. Most critical business functions run on SAP Applications and the complexity of these systems makes it very difficult to protect against attackers. Default setups, forgotten/unimplemented security configurations, weak password management and change processes that apply to one 'unimportant' system can result in complete compromise of the SAP landscape. The legal consequences, lost/damaged business and reputation can be disastrous depending on the type of the attack. While companies invest a lot to secure SAP systems at business process level for example by designing authorization concepts, implementing separation of duties or by using GRC (Governance Risk and Compliance) tools, the security at technical level mostly lacks attention. In this lecture I present several attack paths exploiting configuration weaknesses at technical level, leading to attack potential to single systems, to whole SAP landscapes, and finally the whole enterprise network. By demonstrating creative exploit variants of configuration weaknesses, I motivate the necessity to safeguard a SAP system at technical level.

Ertunga Arsal is the founder of ESNC, a company specialized in SAP® security. ESNC develops software for security audits and forensic examinations of SAP systems. Previously, he worked with Tech Data (Nasdaq: TECD) for five years as a security consultant and was responsible of SAP and applications security of the EMEA region. Being part of the incident response team, he took lead on several investigations. Ertunga has reported numerous security vulnerabilities in SAP systems ranging from medium to extremely critical. He currently lectures Systems and Network Security at Sabanci University grad school.

Tóth László

Majdnem láthatatlan álca az Oracle-adatbázisban, avagy a nem dokumentált ismét segít minket

Almost invisible cloak in Oracle databases or the "undocumented" helps us again

László az eddigi előadásaiban már bemutatta, miként lehet az Oracle-adatbázisok mélylélektanát manipulálni egy sikeres támadás után (post-exploitation). A mostani előadásban László továbbmegy és bemutatja, hogy az Oracle adatbázis memóriájának változtatásával hogyan lehet néhány beépített detektív kontrollt megkerülni vagy operációsrendszer-parancsot futtatni. A bemutatásra kerülő módszerek közül sok a „nem dokumentált" oradebug parancsot használja amely jól ismert mint hibafelderítő eszköz, de – mostanáig – kevésbé mint "hackereszköz". Minden 64bit-es platformon lesz bemutatva és – ahol lehetséges – élő demóval. Mellékesen a résztvevők betekintést nyerhetnek a 64 bites Linuxon történő bináris nyomkövetésbe és kódinjekciós technikákba.

In previous talks László has already shown some ways to play with Oracle database internals after a successful attack (post-exploitation). In this presentation László goes further and shows how Oracle memory can be manipulated to avoid some detection controls and run operating system level commands. Moreover some of the techniques will use the "undocummented" oradebug command which is well known as a troubleshooting tool, but until now it was less known as a hacker tool. Everything will be presented on 64 bit platform and - if possible - with online demos. As a side effect the attendees will get a glimpse into the world of 64 bit Linux binary debugging and code injection techniques.

Tóth László jelenleg a Deloitte Magyarország informatikai biztonság és adatvédelem üzletágának nemzetközileg elismert szakértőjeként dolgozik, és több mint 10 éves tapasztalattal bír. Ezek alatt az évek alatt számtalan biztonsági betörési tesztet és felülvizsgálatot végzett különösen érzékeny környezeteken. László az írója a woraauthbf eszköznek, mely kiadásakor az egyik leggyorsabb Oracle-jelszótörő program volt. Több cikket is publikált az Oracle-authentikáció sérülékenységeivel kapcsolatban. Több Oracle által kiadott CPU-ban is szerepelt.

László Tóth works as an internationally acknowledged consultant at Deloitte Hungary's Security and Privacy service line and has more than 10 years experience in this field. He conducted numerous security penetration tests and reviews in highly sensitive environments. László is the developer of the woraauthbf tool which was one of the fastest Oracle password crackers at the time of its publishing. He released several papers about vulnerabilities of Oracle authentication protocols. His name was mentioned in several CPUs released by Oracle.

Georgi Geshev

A fal ledöntése – Mission: Impossible

Breaking The Wall – Mission: Impossible

Az egyszerű, minimalista és totálisan megerősített szerverplatform, az Openwall GNU/Linux-disztribúció könnyen érthető áttekintése. Az előadás a disztribúció biztonsági mechanizmusainak és tulajdonságainak széles skáláját érinteni fogja, mint például a támadási felület jelentős csökkentése (SUID-fájl-mentes alapinstalláció, biztonságikód-elemzés, least-privilage elv kikényszerítése stb.). Proaktív Linux-kernel 0day exploits protection mechanizmusok (címrandomizálás – ASLR), adatvégrehajtás-megelőzés (DEP), Null pointer hivatkozásvédelem, korlátozott kernelmemória-hozzáférés stb. Egyéb védelmi mechanizmusok (stack smash védelem, fordítási idejű bufferellenőrzés, részleges/teljes RELRO stb.). Erős jelszavas kriptográfia.

Georgi Geshev másodéves informatikai hallgató. Emellett független biztonságihiba-vadász és szenvedélyes FOSS-evangelista, aktív közreműködője különböző ingyenes és open source szoftverprojekteknek, az OWASP-ot, az Openwall- és Mozilla-projektet is beleértve.

An easy to understand overview of the Openwall GNU/Linux distribution which is a simple, minimalistic and utterly strengthened server oriented platform. The talk will cover a wide range of security mechanisms and features of the distro., such as Strongly reduced attack surface (SUID files free default install, source code review for security flaws, enforcing the least privilege principle, etc.) Proactive Linux kernel 0day exploits protection mechanisms (address space layout randomization (ASLR), data execution prevention (DEP), Null pointer dereference protection, restricted kernel memory access, etc.) Miscellaneous protection mechanisms (stack smash protections, compile time buffer checks, partial/full RELRO, etc.) Strong password cryptography

Georgi Geshev is a second year CS student. He is also an independent security bug hunter and a passionate FOSS evangelist, actively involved in various free and open source software projects including the OWASP, the Openwall Project and the Mozilla Project.

Hogy üzenete célba érjen

Fordítás, tolmácsolás

Az INTERLEX Communications Kft.® alakulása, 1997. óta meghatározó tényező a minőségi fordítás, tolmácsolás és más kommunikációs szolgáltatások piacán. A cég – a részvevők által képviselt számos szakterület ötvözésével – egy helyen kínálja az összetett feladatok megoldását, az ügyfelek igényeit a lehető legmagasabb szinten elégítve ki, teljeskörű megoldást kínálva minden olyan feladatra, mely a megbízó saját szervezeti keretei között nehezebben lennének elvégezhetők. Az INTERLEX Communications Kft.® név 1999. óta bejegyzett védjegy. A minőségi szolgáltatásnyújtás elkötelezett híveként cégünk 2002. decemberében MSZ EN ISO 9001:2001 minőségirányítási rendszert vezetett be és tanúsíttatott.

Az INTERLEX Communications Kft.® professzionális fordító- és tolmácsirodaként a fordító-és tolmácságazat teljes területét lefedő szolgáltatásokat kínál ügyfelei részére. A társaság tulajdonosai és munkatársai szakfordítók, tolmácsok illetve több idegennyelvet beszélő magasan képzett és elismert szakemberek, akik munkájuk során a szolgáltatás minőségét és az ügyfél-elégedettséget tartják a legfontosabbnak, a cég filozófiájával összhangban. A cég kiterjedt nemzetközi és hazai partnerhálózata révén (i2i GROUP, ProFord) szinte minden nyelvi viszonylatot és szakterületet lefedve nyújtja magas szintű szolgáltatásait, melynek színvonalát jelzi az ágazatban még igen ritka ISO minősítés, kiterjedt ügyfélkörünk és referenciáink, valamint az, hogy szolgáltatásaink minőségéért garanciát vállalunk.

Ügyfeleink között tudhatunk számos államigazgatási és kormányszervet, külképviseletet, valamint több vezető hazai és multinacionális vállalatot. Ügyfeleink elégedettségét több megnyert pályázat, számos sikeres projekt és referencia támasztja alá; tevékenységünkről, referenciáinkról további információt a **www.interlex.hu** weboldalon talál.

Az INTERLEX Communications Kft.® cégfilozófiája minőségi szolgáltatások nyújtása ügyfeleinek, az összetett igényekre átfogó megoldásokat kínálva, folyamatosan alkalmazkodva a megrendelő konkrét elvárásaihoz. Célkitűzésünk, hogy minőségtudatos, ügyfélorientált kommunikációs szolgáltatóként a piac meghatározó szereplői legyünk.

INTERLEX – „A Megoldás Egy Helyen"

Szakképzett anyanyelvi fordítók és lektorok, ISO minősítés, teljeskörű szolgáltatás, minőségi garancia, kormányzati referenciák – ez az INTERLEX Kft.

INTERLEX Communications Kft.®
H-1013 Budapest, Attila út 6. félemelet 2.
Tel.: +36 1 487-0660; Web: www.interlex.hu

INTERLEX Communications Kft.®

Felix Schuster

Egy extra titkosítási réteg tervezése és implementálása a Skype-hoz

Design and implementation of an additional layer of encryption for Skype

Kétségkívül a Skype a leghíresebb és legelterjedtebb hang- és video-chat szolgáltatás az interneten. Philippe Biondi and Fabrice Desclaux a 2006-os BlackHat-előadásukban („Silver Needle in the Skype") már leírták, hogy a Skype Ltd., a Skype hálózat CA üzemeltetője gyakorlatilag minden egyes hívást képest lehallgatni a Skype hálózatban. Bár az nem világos, vajon ezt a képességet ténylegesen használják, vagy akár eladták kormányzati szervezeteknek. Ahhoz, hogy csökkentsük ezt a súlyos titokvédelmi problémát, pár hónapos munkával egy tool lett kifejlesztve, amely a legújabb windowsos Skype-klienst egészíti ki egy ellenőrizhetően biztonságos és lehallgatásbiztos, Skype-hálózaton keresztüli P2P-hívási képességgel. A biztonságot minden új hívás előtt a két módosított Skype-kliens közötti hitelesített kulcscsere növeli. A biztonságosan cserélt kulccsal utána egy további titkosítási réteg kerül felépítésre, amely minden IP-csomagot elfed, ami a két fél között közlekedik. A fejlesztett eszköz biztonsága a Microsoft Cryptography API és a már bizonyított Off-The-Record Library (libOTR) köré épül. Ezzel a Skype-felhasználóknak nem kell többé a Skype Ltd. megbízhatóságával foglalkozniuk, sem a Skype-kliensek titkosítási implementációjának hatékonyságával és helyességével. Az előadás bemutatja a legnagyobb kihívásokat, amelyek az eszköz megvalósítása során felmerültek, és áttekinti az eszköz felépítését. Emellett egy rövid betekintést nyújt, hogy történt a Skype-kliens egyes részeinek reverse engineeringje.

Felix jelenleg biztonsági tanácsadóként dolgozik a bécsi székhelyű SEC Consult cégnél. Ezt megelőzően IT-biztonságot tanult, és részmunkaidőben a Zynamicsnál (azóta már a Google része) dolgozott, ahol többek között a BinNavi reverse engineering toolhoz debugging modul fejlesztésén dolgozott. A FluxFingers nemzetközileg sikeres CTF-csapat tagja, és különösen élvezi a reverse engineering és egyéb alacsony szintű kihívásokat.

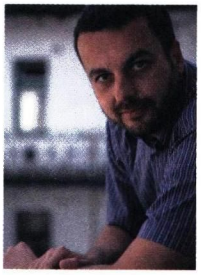
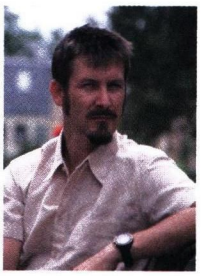
Without doubt, Skype is the most famous and widely used service for voice and video-chats over the internet. Philippe Biondi and Fabrice Desclaux already described in their BlackHat 2006 talk "Silver Needle in the Skype" how Skype Ltd., as the operator of the CA of the Skype network, is virtually capable to easily eavesdrop on every single call made in the Skype-Network. Though it is unclear, whether this capability is really made use of or is maybe even sold to governmental organisations. To mitigate these severe privacy issues, a tool was developed in several months' work, that extends the latest Skype-Clients for Windows with functionality for making verifiable secure and eavesdrop-safe P2P calls over the Skype-Network. The security-gain arises from an authenticated key-exchange that is performed for each new call between the involved extended Skype-Clients. The securely exchanged key is then used to establish an additional cryptographic layer that covers every IP-packet that is exchanged between the involved parties of a call. At its cryptographic heart the developed tool uses the proven Off-The-Record Library (libOTR) as well as Microsoft's Cryptography API. This way Skype-users do neither need to rely any longer on the trust-worthyness of Skype Ltd.'s central CA nor on the correctness and effectiveness of the Skype-Clients' own cryptographic implementations. The planned presentation will describe the major challenges that had to be taken during the implementation of the tool and give an overview on its architectural details. Beside that, a short insight will be given on how parts of the Skype-Client for Windows were reverse engineered.

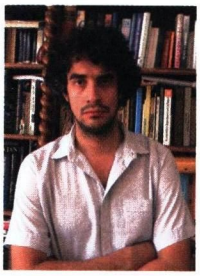
Felix currently works as security consultant for Vienna-based company SEC Consult. Before that he studied IT-Security and worked part-time for zynamics (now part of Google), where he among other things programmed debugging modules for the reverse engineering tool BinNavi. He is an active member of the internationally successful CTF-Team FluxFingers and especially enjoys reverse engineering and other low-level challenges.

Wikileaks: infoszabadságharc vagy infoterrorizmus? – kerekasztal beszélgetés

Wikileaks: info-freedom fight or info-terrorism? – roundtable discussion

Résztvevők: Bodoky Tamás, Csörgő László, Földes Ádám, Léderer Sándor



Az elmúlt években nagy viharokat kavart kiszivárogtató oldallal kapcsolatban kétféle szélsőséges véleményt szokás hangoztatni. Szimpatizánsai szerint a Wikileaks információs szabadságharcot folytat a politikai és gazdasági hatalmasságok ellen, leleplezi sötét ügyeiket, ezért működtetői szabadsághősök, akik átveszik a médiától a demokrácia őrkutyájának szerepét, megteremtik a valódi transzparenciát és sajtószabadságot. A másik oldal viszont úgy véli, hogy amit a Wikileaks művel, az közönséges infoterrorizmus, lopott adatokkal, üzleti titkokkal való felelőtlen és rendkívül káros visszaélés. A Wikileaks megítélése hasonlít a hackerekére, akiket szintén forradalmároknak vagy bűnözőknek szokás láttatni. Pedig ha van etikus hacker, akkor biztos, hogy van etikus leaker is, a kérdés az, hogy ezt a határvonalat hol lehet meghúzni.

There are two quite extremist opinion about the most debated info leaking site. According to his supporters Wikileaks fights and info freedom fight against political and economic powers, unveils their dire business, therefore, its operators take over the role of democracy's watchdog from media and establish the genuine transparency and freedom of press. However, its opponents claim that what Wikileaks is doing is plain info-terrorism an irresponsible abuse of stolen data and business secrets. Opinion about Wikileaks resembles that of hackers who are depicted as either freedom fighters or criminals. But if there exists such thing as ethical hacker then it must surely exists ethical leaker. The questions is how to draw the line.

***Dr. Bodoky Tamás Richárd** (1971–) szabadúszó újságíró. 1995-ben diplomázott a Gödöllői Agrártudományi Egyetem Mezőgazdaságtudományi Karán, 1995–1996-ban tudományos segédmunkatárs volt az MTA Állatorvostudományi Kutatóintézetében. 1996–2001 között szabadúszó újságíró, a Magyar Narancs és az Internetto tudományos-technológiai újságírója, szerkesztője. 2001-től az Index tudományos-technológiai rovatvezetője, főszerkesztő-helyettese (2001–2006), főmunkatársa (2006–2010). 2003–2010 között a Pécsi Tudományegyetem bölcsészkarán működő Társadalmi kommunikáció program doktorandusz hallgatója, „A hírportál mint tömegmédium – tájékozódás és médiahasználat az interneten" című PhD-értekezését 2010-ben cum laude védte meg. A Médiakutató kommunikációelméleti szaklap szerkesztőbizottságának 2005 óta tagja, több tudományos publikáció szerzője, társszerzője. A 2006. őszi tüntetések és zavargások során történt rendőri túlkapásokról szóló cikksorozatáért 2008-ban Gőbölyös Soma-díj*

***Tamás Bodoky** is freelance investigative journalist based in Budapest, Hungary. He covers science and technology, environmental and human rights issues, corruption and organized crime cases, misuse of power and police brutality, and green politics. Bodoky has been a journalist since 1996. Before joining Index.hu, where he worked 9 years in different journalistic and editorial positions, he was science and technology journalist at the Magyar Narancs weekly. Bodoky has won the Gőbölyös Soma Prize for investigative journalism in 2008, and the Szabadság Prize in 2009 for his articles on Hungary's 2006 unrest and police brutality. His first book (Tresspasses, 2009) covers the issue of riot police brutality in 2006. Bodoky has won the Iustitia Regnorum Fundamentum and the Hungarian Pulitzer Memorial Prize for his investigative articles on corruption cases. Bodoky holds an MSc degree in Agricultural Sciences and a PhD degree in Language Sciences. He is editor of hungarian media studies quarterly Médiakutató, and teaches journalism at*

ban, 2009-ben pedig Szabadság Díjban részesült. Az MVM-től offshore cégekhez került milliárdokról szóló cikksorozatáért 2009-ben elnyerte a Minőségi Újságírásért Díjat. A tizedik leggazdagabb magyarnak tartott Kovács Bence János zavaros múltjáról szóló cikkéért 2010-ben ismét elnyerte a Minőségi Újságírás Díjat. Tényfeltáró újságírói munkásságáért 2010-ben megkapta a Pulitzer-emlékdíjat, közérdekű adatigényléses pereiért pedig az adatvédelmi biztos által adományozott Justitia Regnorum Fundamentum díjat. A 2006-os rendőri brutalitásról szóló cikksorozata könyvben is megjelent, magyarul „Túlkapások", angolul „Tresspasses" címmel. 2009 óta a Károli Gáspár Református Egyetem Bölcsészettudományi Kar kommunikáció és médiatudomány tanszékének oktatója, egyetemi adjunktus. A Marshall Memorial Fellowship transzatlanti csereprogram és az Organized Crime and Corruption Reporting Project nemzetközi oknyomozó újságírói hálózat tagja.

***Csörgő László** (1974–) szabadúszó újságíró, marketing/PR- és IT-szakértő. A Tényező.hu főszerkesztője. Publikációi jelentek meg a következő médiumokban: Index, Népszabadság, Médiatechnika, FotoVideo, CHIP, Computer Panoráma, Computerworld stb. Részt vett az Információs Társadalom- és Trendkutató Központ Információs Társadalom Klubjának a munkájában is. Az első Hacktivity konferencia előadója.*

***Földes Ádám** 2003-ban szerzett jogi diplomát az ELTE ÁJK-n, és 2004-ben végzett szociológusként az ELTE TÁTK-n. 2003 óta emberi jogi területen dolgozik, közérdekű érdekérvényesítést, jogfejlesztést, kutatásokat végez az információszabadság és a személyes adatok védelme területén. Mielőtt a Transparency International Magyarországhoz csatlakozott, 2008 szeptembere és 2009 áprilisa között a madridi székhelyű Access Info Europe-nál dolgozott, előtte majd öt évig a Társaság a Szabadságjogokért adatvédelmi és információszabadság-program vezetője volt. Tapasztalatokkal rendelkezik jogi reform-, minisztériumi és parlamenti szinten jogszabálytervezetek, jogszabályjavaslatok véleményezése, közérdekű adatok nyilvánosságának monitorozása és stratégiai pereskedés területén. A TI Magyarország munkájában már 2009 előtt is részt vett, a NIS kormányzati korrupcióellenes szervezetekről szóló fejezetét írta, valamit a közérdekű bejelentők védelméről szóló törvénykoncepció elkészítésében segített.*

***Léderer Sándor** 2006-ban végzett a Budapesti Corvinus Egyetem nemzetközi tanulmányok szakán. Ezt követően hozta létre két társával a K-Monitor Közhasznú Egyesületet, amelynek célja a közpénzek elköltésének folyamatos nyomon követése és a korrupció elleni küzdelem. Az egyesület által létrehozott adatbázis, illetve honlap a sajtó ilyen témájú cikkeit rögzíti és dolgozza fel. A K-Monitor bejelentőfelületet is működtet, illetve részt vesz számos kutatásban. Léderer Sándor 2002–2004 között tagja volt a Corvinus Egyetemen működő Társadalomelméleti Kollégiumnak, 2009 óta pedig az ELTE történelem szak doktori iskolájának hallgatója. Folyékonyan beszél angolul és németül.*

Károli Gáspár University, Budapest. Bodoky is Marshall Memorial Fellowship alumni, and member of the international investigative journalism network „Organized Crime and Corruption Reporting Project".

***László Csörgő** is freelance journalist, marketing/PR & IT specialist. Editor-in-Chief of Tényező.hu. Publications have appeared in the following media: Index, Népszabadság, Médiatechnika, Nemzeti Sport, FotoVideo, CHIP, Computer Panoráma, Computerworld, etc. Participated in the work of Information Society Club of Information Society Research Institute. Speaker of the first Hackivity conference.*

***Ádám Földes** holds a J.D. from ELTE University, Budapest, where he wrote his thesis on video surveillance. He also holds a Master's degree in Sociology from ELTE University, Budapest and studied sociology and law at the Humboldt University in Berlin on a Copernicus Scholarship (2001-2002). Ádám has been working in the field of human rights since 2003. He conducts research, advocacy and policy development to promote and defend the right of access to information. In addition to the right of access to information, he specializes in issues relating to protection of personal data and state secrecy. Prior to joining Transparency International Hungary, Ádám led the Freedom of Information and Personal Data Protection Program of the Hungarian Civil Liberties Union (HCLU) between 2004 and 2008. He has extensive experience of engaging in law reform, providing expert opinions at ministerial and parliamentary level, monitoring levels of access to information in practice, and managing strategic litigation and campaigning. Before joining the organisation Ádám has also contributed to the work of TI Hungary in the field of whistleblower protection as well as re Anti-corruption agencies in the frame of the NIS. He also provided expertise on right to information issues in a number of countries in Central and Eastern Europe (including Bulgaria, Czech Republic, Moldova, Macedonia, Poland, Serbia, and Slovakia) as well Chile. He had acted as an expert for the OSCE (Organization for Security and Cooperation in Europe) and participated in debates in Brussels on the European Union Access to Documents Regulation and on transparency of lobbying. He participated as a civil society observer in two International Conferences of Information Commissioners (Manchester 2006, New Zealand 2007).*

***Sándor Léderer** holds an MA in international studies and is a co-founder of K-Monitor Institute. Sándor graduated from Corvinus University Budapest in 2006 after which he immediately started working with K-Monitor. The association was founded as a „watchdog" organization with the aim of drawing constant attention to issues of corruption in Hungary. K-Monitor seeks to bring a new level of transparency in the field of governance for the purpose of fostering democracy and the rule of law. The association has created a website that makes all the corruption-related articles of online Hungarian media accessible, searchable and analyzable. The database is permanently updated with new articles and archive information as well. K-Monitor also has a whistleblowing blog and the association takes part in several researches. Sándor has started his PhD in History at Eötvös Loránd University Budapest in 2009 and was a member of College of Social Sciences between 2002 and 2004. He's fluent in English and German.*

szakmai workshopok
a kommunikációs stratégiaalkotás új dimenziója

...a hagyományokon túl

koncepcionális események
a prémium célcsoport új eventmarketingje

ict-kommunikációs ügynökség
ict-ügyfelek kommunikációs feladatainak ellátása

piackutatások
viselkedés alapú, egyedi piackutatások lefolytatása

Illési Zsolt

Informatikai bizonyíték, bizonyítás igazságügyi szakértői szemmel

IT as evidence from forensics perspective

A különböző jogágak más-más bizonyítási „világképpel" bírnak. Amikor egy informatikai ügy büntető-, polgári, munkajogi bíróság elé kerül, akkor jó tudni, hogy mik azok a sajátosságok, amelyekre vádlóként vagy a védelem oldalán figyelni kell/érdemes, hogy a vád/védelem eredményes legyen. A problémát elsősorban informatikai igazságügyi szakértői szemszögből szeretném ismertetni, de a vonatkozó jogi körítést sem tudom nélkülözni, mivel erre épülnek a szakjogágak bizonyítással kapcsolatos jellegzetességei – pl. büntetőügyben minden kétséget kizárólag természetes személy(eke)t kell vádolni, ezzel szemben polgári ügyben elég a valószínűség; munkajogi ügyekben megfordul a bizonyítási teher: a munkavállaló állít valamit, és a munkáltatónak kell annak az ellenkezőjét bizonyítani... Az előadás alapvetően elméleti jellegű (semmi billentyűzetmágia), de tartalmaz hazai és nemzetközi jogeseteket az ismertetett problémák illusztrációjaként.

Illési Zsolt jogi szakokleveles informatikus, a Dunaújvárosi Főiskolán, a Pécsi Tudományegyetemen, a Veszprémi Egyetemen és a Kodolányi János Főiskolán műszaki, informatikai, tanári, jogi és szakfordítói tanulmányokat folytatott. 1993-óta foglalkozik hivatásszerűen informatikával, üzemeltetői, rendszergazdai, tervezési, biztonsági, kockázatkezelési és oktatási területen szerzett tapasztalatokat. 1999-óta vállalkozó, jelenleg is saját cégében, a Proteus Consulting Kft.-ben partnerként és vezető tanácsadóként dolgozik. 1996-óta tagja az ISACA-nak, 1998-ban CISA, 2004-ben CISM minősítést szerzett; 2000 óta informatikai igazságügyi szakértő, főleg büntetőügyek informatikai szakértésével foglalkozik. 2007 óta a Zrínyi Miklós Nemzetvédelmi Egyetem PhD-hallgatója, kutatási területe az információs terrorizmus kriminálttechnikai vizsgálata. 2011-től a Dunaújvárosi Főiskola Informatikai Intézetének oktatója.

Different areas of law have different "picture of the world". As accuser or defendant it is good to know the special characteristics of the law to be considered for achieving effective defence or accusation when an IT case brought to the civil, criminal or labour court. I will introduce the key issues from the perspective of an IT forensics expert. However the related legal garnish cannot be omitted because of the specialities of the different areas of law are built on these – in criminal cases for example the indubitable determination of liability of a natural person is required, but in civil cases reasonable level of probability can be sufficient; in labour law the burden of proof reversed: the employee states something and the employer have to provide information that this is not the case... Basically the presentation will be theoretical (no keyboard-based magic), but it will provide domestic and international cases as the illustration of the issues to be addressed.

Zsolt Illési is the co-founder of Proteus Consulting Ltd., an IT risk management company providing complex IT professional consulting services. In 2011 he started his academic carrier in the Institute of Informatics of at College of Dunaújváros as an assistant professor. Prior to founding his company, Zsolt spent a number of years in the fields of IT operation, system administration, security and risk management, also in system development, and in education. Zsolt studied technical sciences, informatics, teaching, law and translation, and graduated at the Polytechnics of Dunaújváros, University of Pécs, and at Kodolányi János University of Applied Sciences. In 2007 he went to Zrínyi Miklós National Defense University, and his PhD research focuses on cyber terrorism and applicable IT forensics methods and techniques.

Peszleg Tibor

Mit tegyünk, ha bekövetkezett a baj?

What to do when the problem is on board?

Előadásomban szeretném bemutatni, hogy mit tegyen egy szervezet abban az esetben, ha informatikai rendszerébe jogosulatlanul behatoltak, és nem elégszik meg annyival, hogy kijavítja a hibákat, működőképessé teszi a rendszerét, hanem szeretne utánamenni annak, hogy ki volt a támadó, és jogi lépéseken is gondolkodik. Ilyenkor milyen alapvető IT-kriminalisztikai elveket kell követnie ahhoz, hogy szükség esetén akár belső vagy polgári, netán büntetőeljárás során felhasználható bizonyítékokat gyűjtsön, adhasson át a hatóságoknak. Előadásomban felvázolnám, hogy milyen információkra van szükség egy ilyen vizsgálat során, azokat hogyan kell megfelelő módon rögzíteni, dokumentálni és tárolni. Kik végezzék az adatok biztosítását, elemzését? Milyen vizsgálatokat célszerű lefolytatni annak eldöntésére, hogy házon belül rendezzük, vagy a hatóságok segítségét kérjük az ügy tisztázásához? Mit érdemes mérlegelni a döntéshozónak egy incidens után lefolytatott vizsgálat utáni döntésnél – üzleti, fegyelmi, polgár-, munka- vagy büntetőjogi szempontból?

Peszleg Tibor rendőrtisztként a bűnügyi nyomozás különböző területein dolgozott. 2002-től a magyar rendőrség internetes egységének létrehozásában, majd munkájában tevékenykedett a kezdetektől. Különböző, internettel összefüggő bűncselekmények nyomozásában vett részt, illetve irányította a nyomozást. Több éven keresztül az informatikai bűncselekmények nyomozását tanította a Rendőrtiszti Főiskolán és a Nemzetközi Rendészeti Akadémián (ILEA). 2004-től a Pécsi Tudományegyetem Doktori Iskolájának kutatója informatikai bűncselekmények témájában. Tanít a PTE jogi karán, illetve az infokommunikációs szakjogászok képzésén.

This presentation will show you what steps should an organisation take after an unauthorised intrusion into their IT system. If you aspire for more than just troubleshooting and making the system work, if you want to identify the attacker to take legal action. I will explain what basic IT criminalistic principles should be followed in order to collect usable evidence for internal, civil or criminal procedures to be able to hand them over to authorities.
I will outline what information is needed for such an inquiry, how should this information be recorded, documented and stored. Who should secure and analyze the data. What inquiries will help decide whether the case should be handled in-house or authorities should be requested to help.
Points of consideration will be given for decision makers that can help to make a decision after an incident related inquiry – aspects on business, discipline, civil law, labor law, criminal law.

As a police officer Tibor Peszleg worked in various fields of criminal investigation. Created the cyber-crime unit of the Hungarian Police and worked in it since the beginning in 2002. Participated and led various internet related criminal investigations. For several years participated as instructor of internet related crime investigation at the Police College and at the International Law nforcement Academy in Hungary (ILEA). From 2004 takes part in a PhD Program at the University of Pécs, as a researcher in the field of IT crime. Teaches at the University of Pécs Faculty of Law and at a specialized lawyer-school in infocommunications.

Alexin Zoltán

Nagy magyar egészségügyi adatbázisok

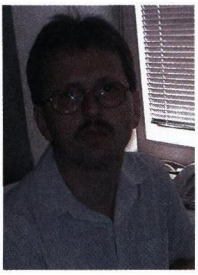
Big Hungarian Health Databases

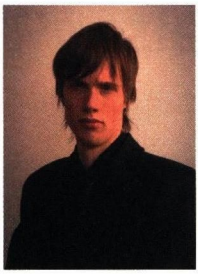
Az egészségügyi adatok a különleges személyes adatok közé tartoznak, ezért kitüntetett figyelemben és védelemben kell részesülniük. Be kell valljuk, hogy ma Magyarországon a nagy egészségügyi adatbázisok előzetes tájékoztatás nyújtása és hozzájárulás kérése nélkül működnek. Vajon mi a helyzet az intézményi védelmi intézkedésekkel? Az előadás ismertet néhány nagyobb adatbázist: az igénybe vett társadalombiztosítási ellátások adatbázisa, tételes egészségügyi adatbázis (TEA), a Nemzeti rákregiszter, a Veleszületett rendellenességek országos nyilvántartása (VRONy), a védőoltás-regiszter, az újszülöttek vérmintáit tároló országos adatbázis, valamint az Országos szűrési regiszter (OSzR). Az előadás feltárja a rájuk vonatkozó fontosabb jogszabályokat, a tárolt adatok körét, az adattovábbítások rendjét és az adatokhoz való hozzáférés jelenlegi helyzetét. Meg kívánom vizsgálni az adatbázisokat kezelő egészségügyi szervezetek működését, a tárolt adatokon végzett kutatási tevékenységek kockázatait és ennek az állampolgárok magánéletére gyakorolt hatását, továbbá rámutatok az adatkezelés etikai vonatkozásaira. A magyar viszonyok bemutatásával párhuzamosan külföldi megvalósítási példákat is be kívánok mutatni.

Alexin Zoltán 1985-ben szerzett diplomát a Szegedi József Attila Tudományegyetem matematikus szakán. Jelenleg a Szegedi Tudományegyetem TTIK szoftverfejlesztési tanszékén dolgozik egyetemi adjunktusként. 2003-ban PhD. fokozatot szerzett a Szegedi Tudományegyetemen. 2004 óta foglalkozik adatvédelemmel, azon belül is kifejezetten az egészségügyi adatok védelmével. 2006-ban meghívott szakértőként részt vett az Európai Bizottság által támogatott EuroSOCAP kutatási projektben, 2007-ben pedig meghívást nyert a The European Privacy Institute projekt tudományos tanácsadótestületébe; 2009. január 1-jétől a Dél-Alföldi Regionális Humán Orvosbiológiai Kutatásetikai Bizottság tagja. 2009 és 2011 között az NFÜ által támogatott TÁMOP 4.2.2-08/1/2008-0008 számú, Szenzorhálózat-alapú adatgyűjtés és információfeldolgozás projektben a University of Central Lancashire, Egyesült Királyság intézettel közös tudományos kutatást folytatott a személyes adatok védelme témakörében. 2010-ben elkészítette „A személyes adatok védelmének jogi, etikai és informatikai kérdései" című egyetemi jegyzetet. 2009-ben adatvédelmi szakértők közreműködésével létrehozták a Tisztességes Adatkezelésért Egyesületet.

Medical data belong to the special categories of personal data. Therefore particular attention shall be paid to ensuring their protection. It should be confessed that currently the big Hungarian health databases are working without providing preliminary data protection information and obtaining consent. What about the institutional protection measures? The presentation enumerates several bigger databases, like: the consumed health insurance services database, the itemized health database (TEA), the National Cancer Registry, the Congenital Developmental Disorders database (VRONy), the vaccination database, the newborns' blood database and the newly designed National Screening Registry (OSzR). The author presents the legal framework that governs them; kinds of data stored in particular databases, the routine data transfer between the databases, and the data access regime. The author examines the functioning of the data processor government bodies, the risks of research activities being done on the stored data and its effects on the privacy of patients. The talk pays attention to the relevant medical ethics issues and proposes several foreign implementation examples.

Zoltán Alexin earned his degree in 1985 at József Attila University of Szeged as a mathematician. Currently he is senior lecturer at the Department of Software Engineering at the University of Szeged. He got his PhD. in 2003 at the University of Szeged. Since 2004 he deals with personal data protection, especially with medical data protection. In 2006 he was invited to become an expert in the EuroSOCAP research project funded by the European Commission. In 2007 he became member of the scientific advisory committee of The European Privacy Institute project; since 2009 he is member of a Regional Medical Research Ethics Committee. Between 2009 and 2011 he carried out research on personal data protection within the framework of TÁMOP-4.2.2-08/1/2008-0008 „Sensor based data collection network and information processing" project supported by the National Development Agency in cooperation with the University of Central Lancashire, United Kingdom. In 2010 he wrote a lecture notes: Legal, ethical and informatics questions of personal data protection. In 2009 together with data protection experts they founded the Association for Fair Data Processing.





Leitold Ferenc & Horváth Botond

Dobozba zárt internet

Internet in the sandbox

Manapság a legtöbb kártevő kártékony URL-ken, kártékony oldalakon keresztül terjed. Ezeknek az oldalaknak a tartalma folyamatosan változik: megjelennek, eltűnnek, esetleg megváltozik a tartalmuk. A kártevők aktivitását így nagyon nehéz követni, esetenként csak néhány hétig, napig vagy óráig elérhetők. Az előadásban az utóbbi időben fejlesztett „malware proxy server" kerül bemutatásra, amely képes arra, hogy weboldalak tartalmát archiválja és a forgalmat egy későbbi időpontban megismételje. A tanulási fázisban a „malware proxy server" a weboldalak tartalmát tárolja, majd képes arra, hogy a klienseknek visszajátsszon egy adott időpontra vonatkozó tartalmat.

Leitold Ferenc a Budapesti Műszaki Egyetemen diplomázott 1991-ben. 1997-ben ugyanitt készítette doktori disszertációját, melynek témájául a számítógépes vírusok szolgáltak. Jelenleg a Dunaújvárosi Főiskola Informatikai Intézetének tanára. Kutatási területe a számítógépes vírusok köre: a számítógépes vírusok matematikai modellezése, a számítógépes vírusok vizsgálatának automatizálása. A Veszprog Kft. Checkvir projektjének keretében különböző antivírustermékek tesztelését végzi. 2004 októbere óta a Journal in Computer Virology szerkesztőbizottságának tagja, részt vesz az EICAR, illetve az AMTSO szervezetek munkájában is.

Horváth Botond jelenleg a Dunaújvárosi Főiskola mérnök-informatikus szakára jár. Részt vett a főiskola informatikai intézetében működő víruskutató labor elindításában, és jelenleg is itt végzi kutatásait. Kutatási területe a számítógépes kártevők terjedésének elemzése, informatikai rendszerek és hálózatok biztonsági megközelítése, valamint önszabályzó biztonsági rendszerek fejlesztése. 2010-ben a főiskolai TDK-versenyen a „Kártevők intelligens keresése és begyűjtése az interneten" című előadásával 3. helyezést ért el.

Nowadays most malware incidents are related to malicious URLs and malicious sites. The content of these sites are continuously changing. They can appear, they can disappear and they can change their content as well. It is very difficult to follow malware activities, they are available only for weeks, days or hours. In this paper the concept and the experiment of the recently developed malware proxy server will be presented which is able to archive the content of URLs and it is possible to repeat the traffic later. In the learning phase the malware proxy server stores the content of the requested URLs and it can provide the content of the stored URLs to clients that are related to a certain date and time.

Ferenc Leitold graduated from Technical University of Budapest in 1991. He received his Ph.D. at Technical University of Budapest too, in 1997 in the theme of computer viruses. Currently he teaches in the Institution of Informatics at College of Dunaújváros. His research interest is based on computer viruses: mathematical model of computer viruses, automatic methods for analyzing computer viruses. According to the CheckVir project of Veszprog Ltd. he is dealing with the testing of anti-virus software products. From October 2004 he is a member of the editorial board of the Journal in Computer Virology. He is working int he organizations of EICAR and AMTSO too.

Botond Horváth is currently a student of College of Dunaújváros and he is learning Computer Engineering. He took part at the set up of the virus research laboratory at the Institute of Informatics, and he is still doing his research work there. His main topics include the examination of spreading computer malware, informatics system and networks safety as well as self-contain security systems development. In 2010 he got the 3rd place at college's Scientific Students' Associations with his paper: Intelligent search and capture of malware on the net.

Kovács Győző

Válogatott kalandozásaim Informatikában

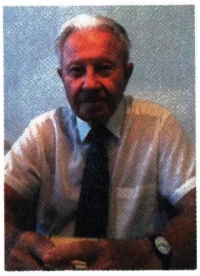
My Assorted Wanderings in IT

Azt hiszem, szerencsés voltam, hogy a szüleim a születésem időpontját úgy időzítették, hogy éppen akkor induljon el mérnöki karrierem, amikor betöltöttem a 24. évemet, és Tarján Rezső kitartó munkálkodásának köszönhetően a Magyar Tudományos Akadémia eldöntötte, hogy a Kibernetikai Kutató Csoport megépíthet egy elektronikus számítógépet. A világon kevés önálló számítógép-alkotó volt, elsősorban John Vincent Atanasoff, Neumann János, Alan Turing, Kozma László, Josef Kaufmann (Temesvár), A. Lebedjev (SzU), Jánosi Marcell – a felsorolás folytatásához elég lenne a két kezünk. Mi – a többiek – másoltunk, ami nem volt bűn, hanem dicsőség. Neumann János például, amikor az IAS gépet tervezte, szinte laponként küldte el a terveit azoknak az intézeteknek, amelyek számítógépet akartak építeni. A számítógép nem valakié, hanem az egész emberiségé! – mondta. A terveket még a washingtoni szovjet nagykövetségnek is postázta, akik érdeklődtek a munkája iránt. Ennek a paradicsomi állapotnak – a hatvanas években – a politika és a hidegháború vetett véget. Erről fogok beszélni.

Kovács Győző villamosmérnök, 1957 és 1967 között az MTA kibernetikai kutatócsoport, majd a számítástechnikai központ osztályvezetője. Az első magyar elektronikus számítógép (M-3) egyik szülőatyja. Részt vett a számítógépes távoktatás indításában (TVBASIC), a Mikroklub mozgalom szervezésében. NJSZT-főtitkár, majd -alelnök, a Számalk távtanulási vállalatának igazgatója, több száz tudományos publikáció szerzője, író. Munkásságát többek között Neumann János-emlékéremmel (1979), Wilhelm Exner-éremmel (1988), a Magyar Informatikáért Érdeméremmel, Neumann János Számítógép-tudományi Társaság Életműdíjjal (2003) és a Magyar Köztársasági Érdemrend lovagkeresztje kitüntetéssel (2004) ismerték el.

I think I was lucky that my parents timed the date of the my birth in a way that my career as an engineer started when I turned 24 and when owing to Rezső Tarján's persistent efforts the Hungarian Academy of Sciences agreed to the Cybernetics Research Group building a computer. There were just a few people in the world who independently built computers such as John Vincent Atanasoff, John von Neumann, Alan Turing, László Kozma, Josef Kaufmann (Timisoara), A. Lebedjev (Soviet Union), Marcell Jánosi, and no more than a dozen others. We (the others) just copied them but it was no sin but glory.For instance when John von Neumann designed the IAS machine he sent his designs almost page by page to institutes that wanted to build computers. Computers are for mankind not just for individuals, he said. He even posted his designs to the Soviet embassy in Washington interested in his work. This paradise was ended (in the 1960s) by politics and the Cold War. This is what I will speak about.

Győző Kovács, Electrical Engineer. Head of the Cybernetics Research Team, then the Computer Sciences Centre at the Hungary Academy of Sciences. One of the fathers of the first Hungarian electronic computer (M3). Participated in the launch of distant computer learning (TVBASIC) and the organization of the "Mikroklub" movement. Secretary, then Vice President of John von Neumann Society, Director of SZÁMALK Distance Learning Company, author of hundreds of scientific publications, writer. Awarded the John von Neumann Medal (1979), the Wilhelm Exner Medal (1988), the Medal for "Hungarian Information Technology", the Life Achievement Award of the John von Neumann Society (2003) and the Knight of Cross from the Order of Merit of the Hungarian Republic (2004).



Muszka Dániel

Kalmár-korszak Szegeden

The Kalmár Era in Szeged

Kalmár László világhírű matematikus 1955-ben kezdett érdeklődni a kibernetika, és az elektronikus „számológépek" iránt. 1956-ban megtervezte a róla elnevezett logikai gépet. Megszervezte a programozóképzést a szegedi egyetemen, majd 1963-ban létrehozta a Kibernetikai Laboratóriumot, ahol vezetésével kibernetikai, a matematikai logika és alkalmazásai, a számítógépes programozás területén folytak kutatások, melyek jelentős eredményeket hoztak. E munka nemcsak úttörő volt, de világszínvonalú is. Ezt bizonyítja a számára 1996-ban posztumusz odaítélt Computer Pioneer Award díj is. Kalmár László nemcsak tudós és kiváló pedagógus, hanem nagyszerű ember, remek vezető és atyai jó barát is volt. Számtalan közös élményünk közül szeretnék néhányat elmondani, melyek segítségével bemutathatom őt, felidézhetem bölcsességét és sziporkázó humorát.

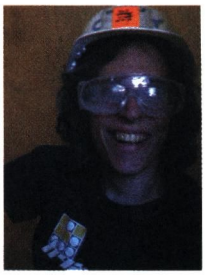
Muszka Dániel matematikus, a magyar informatika korai szakaszában, az 50-es és 60-as években Kalmár László tanítványaként, majd munkatársaként számos jelentős kutatásban és fejlesztésben vett részt. Kalmár László tervei alapján ő építette meg az azóta Kalmár-féle logikai gép néven ismert jelfogós berendezést, valamint ő tervezte és építette meg a szegedi elektronikus katicabogarat, amely máig az egyetlen hazai műállat (bogár formájú feltételesreflex-modell). A Szegedi Tudományegyetem kibernetikai laboratóriumában végzett munkái közül (pl. közlekedéskibernetikai kutatások, ipari és mezőgazdasági célú automatikus berendezések fejlesztése stb.) 11 témában elért eredménye kapott szabadalmi oltalmat. Vezetője volt az első vidéki, a szegedi egyetemi számítógépközpontnak, amelyben M-3, majd Minszk 22 és végül R-40 gépek telepítését, üzemeltetését szervezte és vezette.

László Kalmár, world-famous mathematician, took an interest in cybernetics and electronic „computing" machines in 1955. In 1956 he designed the logical machine named after him. He organized the education of programmers at the University of Szeged, then in 1963 set up the Cybernetics Laboratory where he led research projects into cybernetics, mathematical logic and its applications and computer programming, with important results. His work was not only pioneering but also world-class. This is confirmed by the Computer Pioneer Award he received posthumously in 1996. László Kalmár was not only a scientist and a great teacher but also a wonderful man, a brilliant leader and a father figure. I'd like to share some of our common experience which help me present him, evoke his wisdom and sparkling humour of sense.

Dániel Muszka, Mathematician. Took part in several important research and development projects as a follower and colleague of László Kalmár in the early period of Hungarian information technology in the 1950s and 60s. Based on the plans of László Kalmár he built the relay equipment known as "Kalmár's logic machine" and designed and built the electronic ladybird of Szeged, the only artificial animal in Hungary up to know (bug-shaped conditioned reflex model). 11 of his projects conducted in the Cybernetics Laboratory of the University of Szeged (e.g. transport cybernetics research, development of automated equipment for industry and agriculture, etc.) were granted patent protection. Head of the first computer centre outside Budapest, at the University of Szeged where he was responsible for organizing and managing the installation and operation of M-3, Minszk 22 and R-40 computers.

Veres-Szentkirályi András

Hacking hardware for fun and profit



Amikor szoftverek gyors felépítése a cél, a legtöbb hacker reflexből kedvenc eszköztárába nyúl, előkerül a Python, Perl, esetleg Ruby-script, megspékelve néhány Unix-eszközzel, így percek alatt kész a proof-of-concept kód. De mi a helyzet, ha kilépünk a szoftver világából, és ugyanezt a hardverrel tennénk meg? Korábban ez a terület tömött bajszos villamosmérnökök drága laborjainak sajátja volt, néhány halva született próbálkozást leszámítva az egyszeri buherátor azzal szembesült, hogy az ingyenes interpreterek és fordítók helyett ezen világ meghódítása komoly pénzbe került. Ezt a status quót rendezte át az Arduino megjelenése, mely alaposan megváltoztatta a terepet, lehetőséget adva a gyors prototípusok olcsó elkészítésére, komoly beruházás nélkül, bárkinek. Az előadás során bemutatom a platform világát és működését, majd az érdeklődők betekintést nyerhetnek abba is, milyen problémákat és hogyan tudtam megoldani a segítségével az elmúlt években.

When the goal is to build a software quickly most hackers resort to their favourite tools like Python, Perl, maybe ruby scripts with some unix tools so that they can build a proof of concept prototype in a matter of minutes. But what about if we'd like to achieve the same but with hardwares? In former times it was the privilege of eletrical engineers equiped with expensive labor devices. Besides some hopeless attempt the plain hacker had to realise that hardware hacking requires a round sum of money. The appearance of Ardunio has changed this status quo by enabling cheap prototyping without big investment. In my lecture I show Ardunio's ecosystem and I talk about real-life problems which I was able to solve by using Ardunio.

Veres-Szentkirályi András 2009 decemberében szerezte meg diplomáját a BME-VIK mérnök-informatikus BSc-képzésén, rendszerfejlesztés ágazaton, jelenleg ugyanitt mesterképzésen vesz részt, valamint adatbázislaboron harmadévesek méréseit vezeti. A Silent Signal Kft. és a Független Magyar Tudásközpont alapító tagjaként érdekli a hackelés szoftveres, hardveres és néhány egyéb területe. 2004 óta részt vesz a Hacktivity rendezvényeken, 2008 óta előadóként is.

András Veres-Szentkirályi received his BSc degree as an engineer and IT specialist, specializing in system development, at the Faculty of Electrical Engineering at the Budapest University of Technology and Economics in December 2009. He is now an M.A. student and oversees the tests of third-year students in the database laboratory. As a founding member of Silent Signal Kft. and the Hungarian Autonomous Center for Knowledge, he is interested in software, hardware hacking and other areas of hacking. He has attended Hacktivity since 2004 and has been a speaker since 2008.

Otti Csaba & Őszi Arnold

Ujjlenyomat-azonosító rendszerek, biztonság vagy biztonsági rés

Fingerprint identification systems, security or security leak

Egy ujjnyomat-azonosító rendszer átveréséhez nekünk csak annyi a dolgunk, hogy egy a tulajdonostól származó ujjnyomatról másolatot készítsünk, és előhívassuk a mintát egy rugalmas anyagra. Most biztos azt gondolják, hogy ez azért nem olyan egyszerű feladat... Nos, ez nem így van. Sokkal könnyebb, mint azt hinnénk, ezt fogjuk bemutatni. A tulajdonos számos helyen hagyja ott az ujjnyomatát, például poháron, fényképen, számítógépegéren stb. Minden olyan helyen, amely sima felülettel rendelkezik. A rendőrség által is alkalmazott eljárás a legegyszerűbb és leggyorsabb: a felületet grafitporral szórjuk meg, majd egy ecsettel lesöpörjük a felesleget. Ezután egy átlátszó, ragadós felületű fóliával lehúzzuk a mintát, amely fehér háttér előtt már mutatja is a személy ujjának barázdaelrendezését. Ezt a mintát számítógép segítségével javítjuk, eltüntetjük a zajokat, és elkészítünk egy nyomtatásra alkalmas képet. Miután létrehoztuk a rugalmas másolatot, már le is húzható az azonosítón, és hozzáférhetünk a védett anyagokhoz. Megoldás a többfaktoros azonosítás vagy egyéb biometrikus rendszerek használata, de mindenképpen a kockázatok ismerete. Egyéb biometrikus alternatívák lehetnek a kézgeometria-, kézerezet- vagy ujjerezet-azonosító eszközök. Jövőre majd ezeket hackeljük meg...

If we want to trick a fingerprint reader we need to make a copy of a person's finger then create the sample with the help of a flexible material. Now, people may think this is not that easy. Well, that's not true. It is much easier than you may think! This is going to be presented now. People leave their fingerprint in many places, for example glasses, photographs, computer mouses etc... Anything may do that has a smooth surface. The process used by the police is the easiest and fastest: sprinkle the surface with graphite powder and then brush away the excess. Then we put a transparent adhesive film on the sample surface. After pull it off, the fingerprint is seen on a white background. This pattern can be improved by a photo manipulating software that removes the noise and creates a picture suitable for printing. After creating the flexible fake sample we can immediately access to protected materials. The solution against this is multi factor identification or other biometric systems, but the most important thing is to know the risks we take by using these systems. Further alternative is biometric hand geometry, hand or finger vein recognition systems. Next year we will hack these...

Otti Csaba a Login Autonom Kft. ügyvezetőjeként 12 éve többek közt biometrikus, biztonsági és felhasználóazonosító rendszerek tanácsadójaként dolgozik. Ezen időszakban több nagyvállalat biztonsági koncepciójának elkészítésében vett részt. Megismerte a gyakorlatban elérhető biometrikus eszközök nagy többségét, és részt vett a tesztelésükben. Számos cikket és tanulmányt publikált a gyakorlati biometrikus megoldások témakörében. Vendégelőadóként részt vesz a hallgatók oktatásában a Zrínyi Miklós Nemzetvédelmi Egyetemen és az Óbudai Egyetemen.

Csaba Otti is working as a biometric, security and employee identifier systems consultant and has 12 years experience in this field. He has been involved in the preparation of the security concepts of several large companies during this period. He studied and participated in testing of most biometric devices available. Csaba published several articles and studies concerning biometric solutions in practice. He is also acting as a Guest lecturer at the Zrínyi Miklós National Defense University and the University of Óbuda.

Őszi Arnold az Óbudai Egyetem doktorandusza. A biztonságtechnika területén 6 éves szakmai tapasztalattal rendelkezik. Jelenleg az Óbudai Egyetem Biztonságtechnikai Laboratóriumában végez demonstrátori és kutatói tevékenységet. Leginkább a biometrikus azonosítás és azon belül az ujjnyomat-azonosítás a fő kutatási területe. A biztonságtechnika területén számos cikket publikált már.

Arnold Őszi is a PhD student of Obudai University. He has 6 years experience in safety and security engineering. At present he is a researcher and demonstrator in the Safety and Security Laboratory of Óbuda University. The biometric identification and the fingerprint identification are the main topics in his researches. He released several articles concerning Safety and Security.

Gara-Tarnóczi Péter

Publikus exploitok testre szabása

Customizing Public Exploits

Akad köztük olyan, amely számos különböző környezetben is ellátja feladatát, és olyan is, amely szerencsés csillagállásnak köszönheti sikeres alkalmazását. Az exploit futtatójának szemszögéből nézve ez utóbbi épp annyira elégséges lehet, mint egy közel tökéletes kód, számára az a lényeges, hogy az adott helyzetben működik. Egy másik felhasználó eltérő környezeti feltételek mellett kénytelen jobb kódot keresni vagy a meglévőt módosítani. Előadásomban példákon keresztül mutatom be, hogyan lehet publikus exploitok kódját javítani, általánosabbá tenni. Annak ajánlom megtekintését, aki legalább elméleti síkon tisztában van egy veremtúlcsordulásos sérülékenység kihasználásának menetével. Megértésében előnyt jelent alapszintű C-, Perl-, Python- vagy Ruby-programozási ismeret, na meg jó barátom, x86 Assembly iránti fogékonyság.

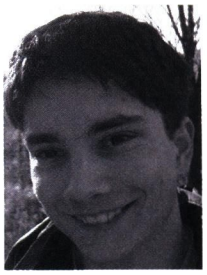
Some of them can be executed perfectly in different environments, others operate well at a special constellation. Getting the expected result who runs the exploit can appreciate the latter one. Another user – in different environmental conditions – forced to look for a better code or modify the existing one. In my presentation, I show you how to improve and make more general public exploits. If you know how a stack buffer overflow can be exploited, you can enjoy the content of the presentation. Basic skills of programming in C, Perl, Python or Ruby and x86 Assembly is an advantage.

Péter 1998-ban szerezte programtervező matematikusi diplomáját az Eötvös Loránd Tudományegyetem Természettudományi Karán. Több mint 10 éve dolgozik informatikai biztonsági területen, CISSP és GCIH Gold minősítésekkel rendelkezik. Eddigi Hacktivity-fellépéseinek összefoglalója: 2007 – Windowsos webes kliensek biztonsága (a kliensoldali támadások számos részletre kiterjedő, érdekes, de nem annyira mély bemutatása), 2009 – Windowsos shellkódok kártékony alkalmazásokban (a shellkódok felépítésének az alapok elmagyarázásával történő mély, technikai prezentációja), 2010 – Adatmentés rendhagyó módon (esettanulmány egy nem bootoló titkosított merevlemez adatainak megmentéséről).

Peter graduated as a programmer mathematician from the Faculty of Science at Eötvös Loránd University. He has worked in IT Security for more than ten years. He hold CISSP and GCIH Gold certifications. His earlier Hacktivity presentations: 2007: Web Client Security in Windows 2009: Shellcodes in Windows Malware 2010: Data Rescue in a Different Way.


WEBSHARK™
A profik velünk úsznak!
AMIT FONTOSNAK TARTUNK ELMONDANI MAGUNKRÓL...
• büszkék vagyunk az „Év honlapja“elismeréseinkre
• több munkánkat díjazták eFesztiválokon
• CMS rendszereket fejlesztünk
• vállalatok irányításához is kínálunk megoldást
• profi és biztonságos hosting szolgáltatást nyújtunk
• közösségi marketing terén is segítünk
HOGYAN KAPCSOLÓDUNK A HACKTIVITY-HEZ?
• 2009 és 2010 évben 2. helyezést ért el csapatunk a Wargame játékban
• 2011-ben részt vettünk a Wargame játék kialakításában
• fejlesztői és üzemeltetői vagyunk a Hacktivity weboldalának
MILYEN SZOLGÁLTATÁSOKAT VEHETSZ IGÉNYBE NÁLUNK?
Webfejlesztés • HOSTING• Vállalatirányítás • Webmarketing
Úgy gondoljuk, nem mindig lehet csomagokról beszélni. Ahány Ügyfél, annyi igény.
Vedd fel velünk a kapcsolatot weboldalunkon – www.webshark.hu – és mi mindent
megteszünk, hogy elégedett legyél a szolgáltatásainkkal!
w3b$h4r|{
H-9700 Szombathely, Semmelweis Ignác u. 2. • Postacím: H-9701 Pf. 486. • Tel: +36 94/514-333 • Fax: +36 94/514-339
E-mail: info@webshark.hu

Paulik Tamás



Ki lakik a routeremben? A beágyazott eszközök botnetbe szervezésének kivitelezhetőségéről

Who's living in my router? About the feasibility of botnet construction from embedded devices

A technika fejlődésével és a széles sávú internet meghonosodásával irodáinkban, háztartásainkban ugrásszerűen megnőtt azon eszközök száma, melyek állandó hálózati és internetkapcsolatot igényelnek. A szolgáltatások palettájának szélesedése új frontokat nyitott az eszközök támadása terén. Az egyik ilyen támadási forma a Cross Channel Scripting (XCS), mely megadhatja az esélyt arra, hogy egy támadó saját, egyedileg módosított firmware-ét töltse fel a sebezhető eszközre. Az előadás során kitérek arra, hogy milyen előnyei, hátrányai lehetnek a beágyazott eszközök botnetbe szervezésének, valamint bemutatásra kerül egy sikeres XCS-támadás, továbbá egy olyan rendszer, mely alkalmas arra, hogy hatékonyan és automatizáltan állítson elő egyedileg módosított firmware-eket, támogatva az XCS-támadást, így megteremtve a beágyazott eszközök botnetbe szervezésének lehetőségét.

Végzős mérnök-informatikus MSc-hallgató a Budapesti Műszaki és Gazdaságtudományi Egyetem hírközlő rendszerek biztonsága szakirányán. Érdeklődése még a BSc-képzés során fordult a privátszféra-védelem és a hálózatbiztonság területei felé. 2009-ben a Hacktivityn egy saját fejlesztésű, privát szférát erősítő technológiát mutatott be, melyre alapozott kutatásait azóta tudományos körökben is elismerték. Jelenleg a Crysys Laboratóriumban a beágyazott eszközök sebezhetőségeinek vizsgálata és azok botnetépítésre történő felhasználása a fő kutatási területe.

By the advancement of technology and the spread of broadband Internet access, the number of Internet-connected devices is quickly increasing in our homes and offices. The widening of their service palette opened new fronts and created new vulnerabilities to attack these devices. Cross Channel Scripting (XCS) is one of the new attack techniques, that makes it possible for an attacker to upload his own, modified firmware to vulnerable devices. During the presentation I'm going to talk about the advantages and disadvantages of constructing botnets from embedded devices, demonstrate a successful XCS attack and a system which is able to build modified firmwares in a fast and automated way, providing a good support for the XCS attack, creating the possibility of effective embedded botnet building.

He is before MSc graduation at the Budapest University of Technology and Economics specialized in Security of Telecommunication Systems. During his BSc studies his interest turned towards the topics of privacy and network security. At the Hacktivity 2009 he introduced Blogcrypt, a Privacy Enhancing Technology developed by himself, and his researches based on his application are scientifically admitted. Currently he is researching at Crysys Laboratory, investigating the vulnerabilities of embedded systems and the feasibility of constructing botnets from such devices.

Vivek Ramachandran

Nagyvállalati Wi-Fi-férgek és -botnetek

Enterprise Wi+Fi Worms, Backdoors and Botnets

Előadásomban azt járjuk körül, hogy hasznos funkciókat, mint a Wi-Fi-hostolt networkot a Windows 7-en kártékony módon is fel lehet használni, rombolásra! Látni fogjuk, hogy egy támadó létre tud hozni WiFi-wormot, -backdoort és -botnetet különböző technikák felhasználásával és a WPA2-PSK-t használó Windows 7-kliens támadásával. Ezek a rosszindulatú szoftverek a saját magán Wi-Fi-hálózatukat fogják használni, hogy továbbterjedjenek és a támadóval, illetve egymással kommunikáljanak. Azt is látni fogjuk, hogyan készíthető proxylánc a Wi-Fi-kliensek felhasználásával, és azt is, hogy ezzel a technikával a támadó kilétét felderíteni szinte lehetetlen. Ki tudja, a következő Stuxnet talán a Wi-Fi-terjesztést fogja használni a pendrive helyett.

In this talk, we will explore how perfectly legitimate and useful features like the Wi-Fi Hosted Network on Windows 7 can be abused by malware to wreck havoc! We will see how an attacker could create Wi-Fi worms, backdoors and botnets using different techniques and attack Windows 7 clients using WPA2-PSK networks. These malware will use their own private Wi-Fi network to propagate and communicate with the attacker, and each other. We will also look at how to create proxy chains using Wi-Fi clients and how this technique makes it almost impossible to trace back the attacker! Who knows, the next Stuxnet may just use Wi-Fi for propagation over USB :-)!

Vivek Ramachandran 2003 óta foglalkozik a Wi-Fi biztonságával. A témáról olyan konferenciákon adott elő, mint a DefCon, a Toorcon, és ő a Caffe Latte-támadás kiötlője. 2007-ben a DefConon nyilvánosan törte fel a WEP Cloakingot, egy WEP biztonsági sémát. Vivek a szerzője a 2011 augusztusában megjelenő „Wireless Penetration Testing using BackTrack 5" könyvnek. Egyike a Cisco's 6500 Catalyst sorozatú switchek 802.1x protokoll és Port Security funkciók fejlesztőinek. Megnyerte az Indiában 65 000 résztvevővel megtartott Microsoft Security Shootout versenyt. A hackerközösségen belül a SecurityTube.net alapítójaként ismert, ahol rendszeresen tesz közzé videókat a Wi-Fi biztonságáról, az Assembly-programozásról, az exploitírási technikákról. A SecurityTube.netnek több mint 100 000 egyedi látogatója van havonta. Vivek wirelessbiztonsági területen végzett munkáját idézte a BBC online, az InfoWorld, a MacWorld, a The Register, az IT World Canada és még sok más hírforrás. Ebben az évben előad vagy oktat az alábbi konferenciákon: Blackhat, DefCon, Hacktivity, 44con, HITB-ML, Brucon, Derbycon, HashDays, SecurityByte and MIT, Boston.

Vivek Ramachandran started working on Wi-Fi Security since 2003. He has spoken at conferences such as Defcon and Toorcon on Wireless Security and is the discoverer of the Caffe Latte attack. He also broke WEP Cloaking, a WEP protection schema in 2007 publically at Defcon. Vivek is the author of the book "Wireless Penetration Testing using BackTrack 5" due for release in August 2011. He was one of the programmers of the 802.1x protocol and Port Security in Cisco's 6500 Catalyst series of switches. He was one of the winners of Microsoft Security Shootout contest held in India among a reported 65,000 participants. He is best known in the hacker community as the founder of SecurityTube.net where he routinely posts videos on Wi-Fi Security, Assembly Language, Exploitation Techniques etc. SecurityTube.net gets over 100,000 unique visitors a month. Vivek's work on wireless security has been quoted in BBC online, InfoWorld, MacWorld, The Register, IT World Canada etc. places. This year he is either speaking or training at Blackhat, Defcon, Hacktivity, 44con, HITB-ML, Brucon, Derbycon, HashDays, SecurityByte and MIT, Boston.

Pavol Luptak

Kriptoanarchia 19 évvel a Kriptoanarchista kiáltvány után

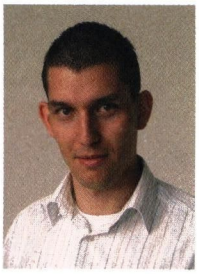
Cryptoanarchy after 19 years since Crypto Anarchist Manifesto

A teljesen anonim cryptopénz, a Bitcoin mára kimagasló átváltási árfolyamot ért el azzal, hogy több mint 8 dollárt ér 1 Bitcoin. Ezzel a világ legerősebb pénzneme. Az anonim, ingyenes, nem szabályozott piacok, beleértve a lenyomozhatatlan kábítószerpiacot, folyamatosan növekednek. Letéti szolgáltatások, mint a ClearCoin és a jó hírnévre alapuló rendszerek, mint a Bitcoin OTC nagyon fontossá váltak az anonim kereskedelem kockázatainak kiküszöbölésében. A Timothy C. May által 19 évvel ezelőtt megjósolt kriptoanarchia rideg valósággá válik.

Pavol számítógép-tudományból szerzett egyetemi diplomát. A CISSP, CEH és OWASP szlovákiai fejezetének vezetője. Ügyvezetője és tulajdonosa az IT-biztonsággal foglalkozó Nethemba Kft.-nek, amely elsősorban teljes körű behatolásteszteléssel és biztonsági audittal foglalkozik, valamint a VOIP-megoldások és a fürtözés területén nagy biztonságú megoldások kidolgozását végzi, és biztonsági tanácsadást, biztonsági oktatást is végez.

Completely anonymous cryptocurrency Bitcoin today reached a peak exchange rate - with more than 8 USD per 1 bitcoin it became the strongest currency in the world. Anonymous free non-regulated markets including untraceable drug markets are expanding. Escrow services like ClearCoin and reputation systems like Bitcoin OTC become very important in risk elimination of anonymous trade. Cryptoanarchy that was predicted 19 years ago by Timothy C. May becomes cruel reality.

MSc degree in Computer Science. CISSP, CEH and OWASP Slovakia Chapter Leader. Owner, CTO and Lead Security Consultant of the security-based company Nethemba s.r.o. focused on comprehensive penetration tests and security audits, proposing ultra secure solutions, VOIP solutions, clusters, consulting & training in security areas.



Balázs Zoltán

IPv6 shipworm + My little windows domain pwnie

Egy vállalati hálózat a célpont. A bejövő hálózati kapcsolatok tiltottak, nincs internetről elérhető szerver. Ismert egy adminisztrátor, aki a legfrissebb Linuxot használja, friss böngészőt, Javascript tiltva. A támadás első lépését az adja, hogy az adminisztrátor engedélyezi az IPv6-ot a munkaállomásán, és ezzel tudtán kívül az internetről elérhetővé teszi a munkaállomást. A probléma legalább 2001 óta ismert... A támadó triviális módszerekkel megszerzi az adminisztrátor IPv6-címét, majd felhasználói jogot szerez a munkaállomásra (pl. SSH brute force segítségével). A második hiba: a Linux alá fel van csatolva a Windows-rendszerpartíció. Így a támadó könnyedén megszerezheti a lokális Windows-rendszergazda-jelszó hasht. A harmadik hiba: ugyanaz a lokális Windows-rendszergazda-jelszó egy Windows-domainadminisztrátor munkaállomásán. A régi bevált pass-the-hash támadás alkalmazásával (1997 óta ismert) először rendszergazdai jogokat szerzünk a domainadminisztrátor munkaállomásán, majd megszerezzük a domainadminisztrátor jogosultságait. Befejezésül hasznos és kevésbé hasznos tanácsok hallhatók, melyek segítségével elkerülhető a fenti szituáció.

Balázs Zoltán a BME-n végzett 2006-ban, az infokommunikációs rendszerek biztonsága szakirányon. Néhány hónapig a Citigroup Threat Assesment Centerben dolgozott IT-biztonsági elemzőként. 2006 és 2010 között IT-biztonsági szakértőként dolgozott az Erste Bank Hungarynél, majd 2010 óta IT-biztonsági csoportvezetőként, szintén az Ersténél. Főbb szakterülete a biztonsági felügyelet, az adatbázis-biztonság és a behatolástesztelés. Zoltán egyik hobbija az ún. hacking challenge-ek megoldása vagy készítése.

The target is a company network, where inbound traffic is denied, no internet accessible server is hosted. The target administrator uses latest Linux, updated Browser, JS disabled. The first mistake: the administrator enables IPV6 on the client workstation. This will connect the workstation to the IPv6 network, bypassing the inbound firewall filtering (known since 2001). After the attacker knows the global accessible IPV6 address, the client workstation can be owned via usual ways (e.g. SSH brute force). The second mistake: the Windows partition is mounted to the Linux workstation, so attacker can extract the local Windows admin hash. Third mistake: the Windows local admin password is the same on a Windows domain administrator workstation. Via pass-the-hash (known since 1997) attacker can gain local administrator privileges on the target Windows workstation, then via token impersonation or via pass the hash attacker can gain domain admin privileges. The presentation will be closed with effective and not so effective countermeasures against these attacks.

Zoltán Balázs graduated at the Budapest University of Technology and Economics, finishing the Security of Infocommunication Systems special in 2006. Worked for some months at Citigroup Threat Assessment Center as IT Security Analyst. From 2006-2010 he worked as an IT Security Expert at Erste Bank Hungary, and from 2010 he works as an IT Security team leader, still at Erste. His main experts are Security Monitoring, Database Security, Penetration Testing. One of Zoltán's hobbies is to solve and create hacking challenges.

Gyöngyösi Péter & Illés Márton

Tűzfalak és támadások

Firewalls and Exploits

Napjainkban komoly biztonsági problémának számít bármely szervezetnél, ha nem védi tűzfal. Éppen ezért ma már gyakorlatilag minden hálózaton valamilyen szintű tűzfal – csomagszűrő, inspekciós modul, alkalmazásszintű proxy – használatban van. Ugyanakkor akár a Youtube-on, akár a népszerű hackerkonferenciákon számos izgalmas, a legújabb trükköket alkalmazó támadásokat, meterpreter shelleket és más csodákat lehet látni. A legtöbb bemutató a sebezhetőségek kihasználására, illetve a többszintű támadásokra fókuszál, míg a tűzfalakat csak mellékesen vagy egyáltalán nem említik meg. Pedig a tűzfalak ott vannak, és úgy néz ki, hogy ezek sebezhetőségeit is ki lehet használni. Vajon okoznak-e egyáltalán bármiféle fejfájást a támadók számára a tűzfalak? Milyen módon tudják megnehezíteni a támadók életét? Lehet okosabb és jobb módon használni ezeket, vagy a háborúnak már rég vége? Az előadás során egy kicsit a dolgok mélyére nézünk, hogy kiderítsük, mit lehet tenni a tűzfalak segítségével annak érdekében, hogy megállítsuk a támadásokat vagy legalábbis megnehezítsük a támadók életét.

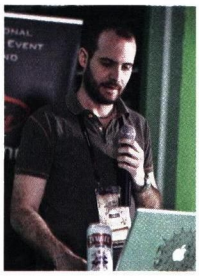
It is a serious security problem if an organization is unprotected by a firewall. As a result practically all networks are equipped with some kind of firewall (packet filter, inspection module, application-level proxy). At the same time numerous exciting attacks based on the latest tricks, meterpreter shells and other wonders can be seen on Youtube or at popular hacker conferences. Most of the presentations focus on the exploitation of vulnerabilities and multi-layer attacks, only mentioning firewalls in passing or not at all. Yet the firewalls are in place and it looks like their vulnerabilities can be indeed exploited. Do firewalls cause a headache for hackers at all? How can they make the attackers' job more difficult? Can we use them in a cleverer and better way or is the war long over? My presentation will include some in-depth investigation to find out what to do with firewalls to stop the attacks or at least make life more difficult for hackers.

Péter dolgozott cirkuszi medvéket szállító vállalatnál, írt blogot pénzért kenyérpirítókról, és elemzett high-tech digitális dobókockákat, közben szép lassan elvégezte a Műegyetem infoszakán a biztonságtechnikai szakirányt, és kikötött a BalaBitnél, ahol negyedik éve fejleszt security szoftvereket. Diplomáját naplóüzenetek statisztikai alapú elemzéséből írta, többször adott elő webes rendszerek biztonságáról, és már akkor bringával (és olajos nadrágszárral) járt Pesten, amikor a Critical Mass még sehol sem volt.

Illés Márton 30 éves életművész, polihisztor. Termékmenedzserként a BalaBit IT Security oszlopos tagja, a Shell Control Box és a syslog-ng Store Box termékek ötletgazdája és fejlesztési vezetője. A meghatározó hazai és külföldi konferenciák állandó előadója. Nem mellesleg a Kispál és a Borz zenekar fő rajongója.

Péter worked as a developer for a company transporting circus bears, made money by writing a blog about toasters, analyzed high-tech digital dices and finally received his degree in security technology at the IT Department of the Budapest University of Technology and Economics. He then joined BalaBit where he has developed security software for four years. His wrote his thesis about the statistics-based analysis of log messages, gave several presentations about the security of web systems and already rode a bicycle in Budapest (with oil on his trouser legs) when Critical Mass was nowhere to be found.

Márton Illés, 30-year old bon vivant and polyhistor. Product manager and stalwart of BalaBit IT Security, creator and development manager of Shell Control Box and syslog-ng Store Box. Frequent speaker at major Hungarian and foreign conferences. Also, number one fan of the band Kispál és a Borz.



Michele Orru

Dr. Strangelove, vagy: Hogyan tanultam meg nem aggódni és a BeEF-et szeretni

Dr. Strangelove or: How I Learned to Stop Worrying and Love the BeEF

A böngészőbiztonság még mindig az egyik legtrükkösebb kihívás. Rengeteg erőfeszítés történt már, hogy csökkentsék a böngészők sérülékenységét a heap és stack overflow-val, a pointer dereference és egyéb, memóriát érintő hibákkal szemben. És mégis létezik egy szinte teljesen feltáratlan terület. Az X-Frame-Options, X-XSS-Protection, Content Security Policy, DOM sandboxing jó kiindulási pontok az XSS-csapás kezelésére, de még mindig nem kerültek széles körben implementálásra. Látni fogjuk, hogy az olyan keretrendszerek, mint a BeEF, segítségével a böngészők security contextjével vissza lehet élni. Mivel lehetőségünk van a DOM kedvünk szerinti módosítására a webalkalmazások 95%-ában, egy triviális reflected DOM-alapú XSS elég, hogy a böngészőt a BeEF-hez csatoljuk és teljes egészében ellenőrzésünk alá vonjuk. Az előadás az alábbi fő területeket fogja érinteni a sok közül. Cutting: rejtőzködő tevékenységek, célfelderítés és -vizsgálat, általános modul automatikus futtatása. Devouring: belső hálózati ujjlenyomatképzés JS-en keresztül, belső szolgáltatások kihasználása a böngészőn keresztül, billentyűnaplózás, böngésző pwnage, autopwn. Digesting: perzisztencia, tunneling sqlmap/Burp BeEF proxyn keresztül, XSS Rays-integráció.

Michele Orru, más néven antisnatchor egy olasz IT-biztonsági srác, aki a varsói székhelyű Royal Bank of Scotland Groupnál dolgozik mint penetrationtesztelő. Fő kutatási területe a webalkalmazások biztonsága. A black, gray, white hat hackelés iránti csúnya szenvedélye és a BeEF (aktív committer a Ruby port kezdete óta) mellett szereti a Macjét egyedül hagyni, amíg a sós vízben horgászik és Kubrick feltámadásáért imádkozik.

Browser security is still one of the trickiest challenges to afford nowadays. A lot of efforts has been spent on mitigating browser exploitation from heap and stack overflows, pointers dereference and other memory corruption bugs. On the other hand there is still an almost unexplored landscape. X-Frame-Options, X-XSS-Protection, Content Security Policy, DOM sandboxing are good starting points to mitigate the XSS plague, but they are still not widely implemented. We will see how a framework like BeEF can be used to abuse the security context of a browser. As we are able to manipulate the DOM for fun and profit in 95% of web applications, a trivial reflected or DOM-based XSS is enough to hook a victim browser to BeEF and control it completely. The presentation will cover the following main areas, between the many: Cutting: stealth activities, target enumeration and analysis, comman module autorun. Devouring: internal network fingerprint via JS, exploiting internal services through the browser, keylogging, browser pwnage, autopwn. Digesting: persistence, tunneling sqlmap/Burp through BeEF proxy, XSS Rays integration.

Michele Orru' a.k.a. antisnatchor is an IT and ITalian security guy who works as a Penetration Tester for The Royal Bank of Scotland Group in Warsaw, Poland. He mainly focus his research on web application security. Besides his nasty passion about black, gray, white hat hacking and BeEF (being an active committer since the Ruby port started), he enjoys to leave alone his Mac while fishing on salted water and preys for Kubrick resurrection.

Major Marcell & Zágon Mihály

A legújabb webes támadási lehetőségek

Modern Browser Attack Vectors

Az előadás fókuszában a jelenlegi böngészőket érintő fejlesztések és exploitírási lehetőségek elemzése áll. Az elterjedtebb böngészők fejlesztői tervezik vagy már megvalósították a „sandbox" technológiát, hogy a böngészőket biztonságosabbá tegyék. A HTML5-kompatibilis böngészők számos új funkciót valósítanak meg az audio- és videolejátszás, illetve a 3D-renderelés grafikus processzorral történő támogatása terén. A WebGL javascript segítségével lehetővé teszi a grafikus hardverre történő közvetlen rajzolást és „shader" kód futtatását a GPU-n. A HTML5 szabvány lehetővé teszi nagy mennyiségű adat kliensoldalon történő tárolását a böngésző helyi tárolójában vagy az élő sessionhöz rendelt tárolóban. A Microsoft az Internet Explorerhez a „Protected Mode" sandboxot, a Google Chromium „Sandbox" projektjét pedig a Google Chrome böngésző és az Adobe Acrobat Reader alkalmazza. A sandbox koncepciót az egyes gyártók különbözőképpen valósították meg. Léteznek elméleti és gyakorlati gyengeségei, melyek biztonsági sebezhetőségekhez vezetnek.

Marcell jelenleg a Deloitte Magyarország IT-biztonsági csapatának tagja. Több mint 6 éves tapasztalattal rendelkezik betörési tesztek és informatikai biztonsági vizsgálatok terén. Tanulmányait a Széchenyi István Egyetem és a Budapesti Műszaki és Gazdaságtudományi Egyetem műszaki informatika szakain végezte, a szoftverfejlesztésre és az informatikai biztonságra fókuszálva. Tapasztalatokat szerzett az alkalmazások biztonsági tesztelése, a reverse engineering, a kriptográfiai algoritmusok és protokollok megvalósítása terén.

Mihály IT-biztonsági tanácsadóként dolgozik, alapvetően „black-box" belső betörési tesztekre specializálódott, de exploitfejlesztésben és webes/bináris alkalmazások tesztelésében is szerzett tapasztalatot. A különböző problémák megoldása közben szereti automatizálni azt, amit automatizálni lehet, hogy arra koncentrálhasson, ami kreativitást igényel.

The presentation is focusing on the analysis of the new features in current browser developments and the possibilities of creating exploits. Major browser vendors are considering or already implemented sandbox technology to improve browser security. There are numerous new features implemented in the HTML5 compatible browsers to support audio and video playback or graphic processor support for 3D rendering. WebGL features enable drawing directly to the graphic hardware and executing shader code on the GPU from javascript code. HTML5 enables storing large amount of data in browser local storage or session related data for the lifetime of the session. Microsoft implemented the "Protected Mode" for Internet Explorer and Google implemented the "Sandbox" in the Chromium projects which is used in Google Chrome and Adobe Acrobat Reader. There are theory behind sandboxing and different implementations from vendors. There are theoretical and practical weaknesses which can lead to security vulnerabilities.

Marcell is currently working for the IT security group in Deloitte Hungary. He has more then 6 years of experience in penetration testing and information security audits. He attended Széchenyi István University and Budapest University of Technology and Economics specialized in software development and information security. He has experience in application level security penetration testing, reverse engineering and implementing cryptographic protocols and algorithms.

Mihály is working as an IT security consultant, he primarily specialized himself on network level black-box penetration testing, but gained experience in exploit development and in web / binary application testing as well. He prefer to automate what can be automated, so he can concentrate on the creative part of the problems.

Kabai András

Malware-analízis, tippek és trükkök

Malware analysis, tips and tricks

Nap mint nap találkozunk kártékony kódokkal, de a belső lelki világukról annál kevesebbet tudunk, működésükről és tevékenységükről pedig általában egy-egy felkapott cikk során értesülünk. Az előadás keretén belül bemutatom, hogy miként szerezhetünk részletesebb információkat, és vehetjük fel magunk a harcot ezen programok ellen a működésük és kódjuk analizálásával, valamint rejtőzködő és védelmi mechanizmusaik kicselezésével.

Több mint 10 éve foglalkozik az IT-biztonság különböző területeivel, ezek közül is kiemelten behatolásteszteléssel, sérülékenységkereséssel és exploitok írásával, valamint kártékony kódok elemzésével. 2004 óta a PTA CERT-Hungary Nemzeti Hálózatbiztonsági Központ vezető IT Security-specialistája.

Malwares are part of our lives but our knowledge of their inner workings is scarce. We get to know them what they are doing and how from media coverage only. In this lecture I demonstrate how to elicit detailed information about malwares and how can we fight back by analyzing their code, functionality and their protective and stealth mechanisms.

He is working on various fields of IT security for more than 10 years now. His main interests are penetration testing, searching for vulnerabilities, exploit writing and analysing malwares. He works as a senior IT security specialist at PTA CERT-Hungary National Cybersecurity Center since 2004.

ethical hacking

C|EH™ Certified Ethical Hacker

Legyél Te is Certified Ethical Hacker!

Vegyél részt a Hacktivity után induló online CEHv7 képzésen!

2011-ben az EC-Council útjára indította a világszerte elismert ethical hacking képzés legújabb verzióját, a CEHv7-et. Most itt a lehetőség, hogy kedvezményesen elvégezd online, és Te is Certified Ethical Hacker minősítést szerezz.

Kezdési időpont: 2011. szeptember 26.

Képzés díja: 420.000 Ft + Áfa

15% kedvezmény Hacktivity résztvevőknek
Jelentkezéskor tüntesd fel a következő promóciós kódot, és kapsz 15% kedvezményt:
▶ **c48fe831**

Online bemutató a Hacktivity után!
Találkozz velünk szerdán online (szept. 21.)!
Bemutatjuk a Cross Site Sripting szépségeit.

További infó a bemutatóról és a képzésről:
www.ethicalhacking.hu

Become a Certified Ethical Hacker!

Attend Our Online CEHv7 Course Right After Hacktivity!

In 2011 EC-Council released the most advanced ethical hacking training program in the world, the CEHv7, and now you have the chance to take it online for a special Hacktivity price and become a Certified Ethical Hacker.

Start Date: 26 September 2011

Training Free: 1490 EUR ex. VAT

15% Discount for Hacktivity Participants
To get 15% discount, use the following promotional code at registration:
▶ **c48fe831**

Online Demo After Hacktivity!
Come and meet us online on Wednesday (21 Sept)!
We will show you the beauty of Cross Site Sripting.

More Info about the Demo and Training:
www.ethicalhacking.hu



Hornák Zoltán, Kerényi Kristóf, Kispál István

Cryptochipek biztonsága – passzív-aktív kombinált támadások

Crypto-chipset Security – Passive Active Combined Attacks

A cryptochipek megvalósításának legnagyobb kihívása, hogy a rejtjelkulcsok titkosságát olyankor is garantálniuk kell, amikor a támadó hozzáfér az elektronikai áramkörhöz, képes annak működését megfigyelni, befolyásolni, sőt akár a chipet módosítani is tudja. A prezentáció célja a biztonsági chipek elleni legújabb fizikai és logikai támadások és az ellenük való védekezési módszerek bemutatása. Passzív-aktív kombinált támadási módszereket RSA, DES és AES implementációs példákon keresztül mutatjuk be.

A Search-Lab tulajdonosa és ügyvezetője, Zoltán a Budapesti Műszaki Egyetemen szerzett diplomát. Nyolc évet töltött az antivírusiparban mint a VirusBuster fejlesztési vezetője, valamint biztonsági tanácsadóként dolgozott. A Budapesti Műszaki és Gazdaságtudományi Egyetem oktatója, és világszerte tart biztonságos kódolási képzést. CISA, az ISACA tagja, a SAFECode és a Neumann János Számítógép-tudományi Társaság tagja.

A Budapesti Műszaki és Gazdaságtudományi Egyetem befejezését követően néhány szemesztert Németországban és az USA-ban töltött, majd K+F projekteken dolgozott, valamint termékbiztonsági auditokban vett részt. Kristóf CISA, tagja az IEEE-nek és a Neumann János Számítógép-tudományi Társaságnak, valamint tapasztalt biztonságosprogramozás-oktató. Fő területe a set-top dobozok és hasonló technológiák.

István a Budapesti Műszaki és Gazdaságtudományi Egyetemen számítógép-tudományból szerzett diplomát. Fő érdeklődési területe a számítógépes látás és a képfeldolgozás. Jelenleg a Search-Labnál a szoftverfejlesztési tevékenységekért felel.

The biggest challenge in crypto chip-sets is to preserve the secrecy of cryptographic keys even when adversaries have access to the electrical circuitry, are able to observe all physical behavior of the chip, influence its operation or even modify it. The presentation aims to discuss the latest advances in physical and logical attacks against security chips and possible countermeasures. The very powerful passive active combined attacks (PACA) are introduced through practical examples of RSA, DES and AES implementations.

The owner and managing director of SEARCH-LAB, Zoltán completed his degree at the Technical University of Budapest. He spent eight years in the anti-virus industry as the development director of VirusBuster, and then worked as a security consultant. He is a lecturer at the Budapest University of Economics and Technology and gives secure coding courses worldwide. He is a CISA, a member of the ISACA, the SAFECode and the John von Neumann Computer Society.

After graduation at the Budapest University of Economics and Technology, spending some semesters in Germany and in the USA, Kristóf started working in R&D projects and product security audits. Kristóf is a CISA, a member of the IEEE and the John von Neumann Computer Society and an experienced secure coding trainer. Focusing on of set-top-boxes and related technologies.

István graduated from the Budapest University of Technology and Economics in Computer Science. His main interests are computer vision and image processing. Currently he is responsible for software development activities at SEARCH-LAB.

Bodor Péter

Social engineering és pszichológia

Social engineering and psychology

A hackelést lehetséges elkülöníteni a technical engineering és a social engineering aspektusaira, annak alapján, hogy az információk nem hagyományos úton történő megszerzése elsődlegesen 1.) a technikai eszközök vagy 2.) a társas intézmények és a bennük tevékenykedő személyek ismeretén alapul. Az előadás a social engineering gyakorlata és a pszichológia mint tudományos diszciplína kapcsolatát, azonosságát és különbségeit vizsgálja. Saját perspektívám a pszichológus nézőpontja lesz, s nem a gyakorló hackeré, ám e külső, némileg „detached" nézőpont érdekes belátásokkal kecsegtet. A social engineering és a pszichológia kapcsolatának tárgyalása során három tézist vetek fel. Érveket hozok fel a mellett, hogy a social engineering több, mint a pszichológia (>), egyenlő a pszichológiával (=), kevesebb, mint a pszichológia (<). E három tézis természetesen ellentmond egymásnak, ám az ellentmondások olykor termékenyek lehetnek. Néhány olyan pontot kívánok tehát felmutatni, ahol a social engineering és a pszichológia egymást kölcsönösen megtermékenyíthetik, azaz, ahol a pszichológia tanulhat a social engineeringtől, és viszont, ahol a social engineering tanulhat a pszichológiától.

Bodor Péter *pszichológus, az ELTE oktatója. A rövidebb külföldi meghívásokon túl oktatott egy szemesztert az Egyesült Államokban, az American Universityn, és éveken át vendégoktató volt Ausztriában, a bécsi egyetemen. Vizsgálódásai a szociálpszichológia és a fejlődéslélektan kérdéseire összpontosulnak, de a pszichológia filozófiai és történeti problémái is foglalkoztatják. A pszichológia társas konstruktivista irányzatának követője. Számos magyar nyelvű publikációt készített. Az utóbbi időben folytatott kutatásai az identitás diszkurzív konstrukciójára vonatkoznak, melyekben kísérletet tesz arra, hogy a mindennapi beszélgetéseket folytató egyének különféle nyílt és burkolt identitásállításait rekonstruálja. Ugyancsak végez kutatásokat a nézés társas konstrukciójának témájában, melynek során a látás társas és társadalmi determinánsainak eyetracker felhasználásával történő empirikus vizsgálatára törekszik.*

Within hacking, techniques can be classified as either „technical engineering" or „social engineering" ones. In the former case information is primarily acquired by using technical devices while in the latter case social constructs and knowledge about people in them is employed. The presentation examines the relation between social engineering's practice and psychology as scientific discipline, explores their similarities and differencies. My perspective is of a psychologist and not a practicing hacker, but this outsider, slightly "detached" angle promises interesting insights. In the discussion of the relation of social engineering and psychology I propose three theses. I bring up arguments that social engineering is more than psychology (>) equals with psychology (=) and less then psychology (<) It is no doubt that these three theses contradicts each other, but contradiction can be fertilizing sometimes. I'd like to show some areas where social engineering and psychology can learn from each other.

Péter Bodor*, psychologist, lecturer at Eötvös Lorand University. In addition to short invitations abroad, he taught a semester at the American University in the US and was a guest lecturer for several years at the University of Vienna, Austria. He is a follower of social constructivism. His area of research covers the common ground of psychology and the use of language. He has numerous publications in Hungarian. His recent research focuses on the discursive construction of identity, attempting to reconstruct the various open and hidden identity statements of people in casual conversation. He also conducts research into the social construction of looking, doing an empirical analysis of the social factors of visual conduct using an eyetracker device.*

Oroszi Eszter

Social engineering – amikor fellebben a fátyol

Social Engineering - when the veil lifted

A social engineering technikákkal, azaz az emberi tényezőt kihasználó támadási formákkal már mindannyian találkozhattunk – jobb esetben csak egy előadás keretein belül, és nem áldozatként :-). Előadásomban a korábban elhangzottakkal ellentétben azonban nem pusztán az alkalmazott támadási technikákat szeretném bemutatni, hanem azokat a helyzeteket és emberi tulajdonságokat is, melyeknek köszönhetően olyan elképesztő dolgokra lehet rávenni az embereket, mint például egy bizalmas fájl kiküldetése egy külső, ismeretlen e-mail címre vagy egy jobb érdemjegy beíratása az egyetemi tanulmányi rendszerbe telefonon keresztül. Hihetetlennek hangzik, ezek azonban mégis megtörtént esetek. De miért is sikerülhet egy ilyen támadást kivitelezni? Sőt, miért fordulhat elő, hogy néhány esetben még kezeskednek is a támadóért? Ezekre a kérdésekre keresvén a választ ismertetem a kihasználható emberi tulajdonságokat és ezek pszichológiai hátterét, valamint bemutatom a célszemélyek azon csoportjait, akikre munkavégzésükből kifolyólag ezek a tulajdonságok kifejezetten jellemzőek, s éppen ezért bizonyos típusú támadásoknak nagyobb valószínűséggel vannak kitéve. Előadásomban megpróbálok arra is választ adni, milyen következtetéseket vonhatunk le például a közösségi portálon megjelenő adatokból vagy éppen a szemetes tartalmából… És, ha mindez még nem lenne elég, hogyan teremthetünk olyan körülményeket, hogyan hajthatunk végre olyan kombinált támadásokat, melyeknek köszönhetően megkönnyíthetjük a célszemélyek átverését, és még egy kellően biztonságtudatos felhasználót is tőrbe csalhatunk. De persze minden titkot nem árulhatok el… ;-)

We all might have met with social engineering techniques. The lucky ones only in a lecture settings and not as a victim :-) In my lecture my focus will shift from the already presented case show of SE techniques to describing situations, and human traits which together makes people behave and act so extraordinaly things like sending a confidental file to an external, unknown email address or to get a better mark at the university via a phone call. I will share unbelievable, yet true stories. I will describe the background of exploitable human traits and their roots in psychology. I will explain how the circle of potential victims is narrowed, how to test if somebody posesses said attributes. In my lecture I'm going to show what type of and level of inference can be drawn from the information gathered in social network sites or garbage bins. And top of all of this I will show how one can create a situation which makes the human attack more likely to succeed even in case of an alert human. But not all of my cards will be played, of course:-)

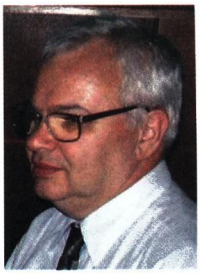
Oroszi Eszter social engineeri pályafutása alatt már több területen is szakdolgozatírásra adta a fejét, valódi diplomáját azonban 2009-ben szerezte meg a Budapesti Corvinus Egyetem gazdaságinformatikus (BSc) szakán. (És nem, nem közgazdász! :-)) Ezen sorok írásakor – nehogy kijöjjön a gyakorlatból – épp az MSc-s verzió megszerzésén mesterkedik, illetve már csak arra vár, hogy átadják az oklevelét. Jelenleg a kancellár.hu Zrt.-nél dolgozik mint információbiztonsági tanácsadó. A social engineering auditok mellett biztonságtudatossági oktatásokat is tart, valamint külsős óraadó egykori egyetemén.

Eszer Oroszi is a social engineer, who has dubbed herself as graduate student several times but in real life has graduated only in 2009 as Bsc in Business Informatoin System at Corvinus University of Budapest (definitely not economist! :-) By writing this bio, in order not to be out of practice, she is fiddling with getting her Msc degree, or to be more precise she is waiting for the ceremony only. She is working for kancellár.hu Zrt. as IT security consultant. Beside social engineering audits she is IT security awareness trainer and give lectures at Corvinus.

Bíró László

Stuxnet – valóban az első?

Stuxnet – Really the first one?



A Stuxnet által az iráni dúsítóüzemben okozott kár ráirányította a figyelmet az ipari vezérlőrendszerek (SCADA -- Supervisory Control And Data Acquisition) téves működése által okozható károkra. A kártékony információ átjutott az eltérő architektúrájú rendszerek védelmein, kellően hosszú ideig rejtve maradt ahhoz, hogy kellően sok helyre beépüljön, majd aktivizálódva komoly károkat okozott. A hatásmechanizmus nagyon hasonló volt ahhoz, mint ami 1983. december 15-én történt a transzszibériai gázvezetékkel: a rendszert valami módszeresen túlterhelte. Bár a történelem legnagyobb kémiai robbanását kiváltó ok akkor nem került nyilvánosságra, a vezérlés általi túlterhelhetőséggel már 1983-ban foglalkoztak a magyar Központi Gázdiszpécsernél. Még korábban, 1977-ben a magyar villamosenergia-rendszer és különösen Budapest áramellátása került az összeomlás hatására egy, a tévében elhangzó, akkor játékosnak tűnő ötlet hatására. Az ilyen típusú támadások még a rendszerek programozói előtt is rejtve tudnak maradni, azonban érdemes megismerni a működésmódjukat.

1972-ben szerzett műszaki tanári oklevelet. Műszerfejlesztő a Telefongyárban, rendszerprogramozó, programozási vezető, majd CIO a budapesti Zöldértnél. 1984-től 1994-ig programozási osztályvezető, majd CIO a BHG-ban. 1994-től 2000-ig CIO az ELMŰ-nél, majd IT-biztonsági vezető az Allianz Hungáriánál. 1997-től CISA, 2004-től CISM, 2009-től pedig CGEIT minősítése van. 1982-ben szabadalmat kapott digitális jelfeldolgozású elektrokardioszkóp témában. Rádióamatőr, hívójele HA5YAR. Hobbiként elektronikus és Hammond-orgonákat javít.

The damage in Iran caused by the Stuxnet moved the focus to damages can be done with malfunctioning industrial process control systems (SCADA, supervisory control and data acquisition). The malicious information ran through different architectures, protections and remained hidden for enough time to be infiltrated sufficiently to the system. Then, it started to work and destroy. The way the Stuxnet worked was very similar to the case of Trans-Siberian Gas Pipeline in 15th of December, 1983. That time the SCADA systematically overloaded the system and induced the largest chemical explosion of the history. Though that time the real reasons remained hidden in 1983 there were calculations about similar overloads at the Hungarian Central Gas Control Station. A couple of years before in 1977 the National Grid and especially the electricity supply of Budapest got close to the collapse by a playful idea was told in the TV. These attacks are extremely dangerous because those can remain hidden even for the SCADA programmers so it's useful to learn how that type of attacks can work.

Graduated in 1972 as Theacher of Technical Rudiments. Developer of measuring instrument in Terta, then systems programmer, head of Programing Dept., and CIO at Budapest Züldért. Between 1984-1994 Head of Prog. Dept and later CIO at BHG. From 1994 tp 2000 CIO at Budapest Electricity, then IT Security Officer at Allianz Hungaria. Qualifications: 1997 – CISA, 2004 – CISM, 2009 – CGEIT. Patent: ECG with digital signal processing, 1982. HAM, callsign is HA5YAR. As a hobby repairs electronic and Hammond organs.

Yaniv Miron

SCADA-szomorúság vagy bumm-bumm SCADA

SCADA Dismal, or bang-bang SCADA

Víziközmű, olaj, nukláris energia, elektromos hálózat, a levegő, amit belélegzel. Nem lenne vicces meghackelni? Az előadásban meg fogom mutatni, hogy az életünket kontrolláló SCADA (Supervisory Control And Data Acquisition) rendszereket milyen könnyű meghackelni, milyen gyengék a protokolljaik és milyen gyengén vannak telepítve. Ha szeretnék a nagy fiúk rendszereivel játszani, gyere és halgasd meg a SCADA-hekkelés előadást.

Yaniv Miron informatikai biztonsági tanácsadó és kutató, jelenleg az IL Hacknél nagy szervezetekkel dolgozik mint biztonsági tanácsadó és kutató. Senior oktató az Európában hackelési tanfolyamokat tartó IL Hack Institutenál. Yaniv a legnagyobb izraeli hacking összejövetel, az IL.Hack alapítója. Megszerezte a CISO minősítést az Izraeli Technológiai Intézettől, valamint minősített lakatos. A világ minden táján ad elő biztonsági és hackelési rendezvényeken (BlackHat/SyScan/CONFidence/HackerHalted/OWASP/IL.Hack stb.). Magasan képzett penetration tesztelő és biztonsági kutató, aki számos biztonsági hibát talált (Microsoft/Oracle/IBM stb.).

Water, Oil, Nuclear, Electric, The air you breathe, wouldn't it be fun to hack into it? In this presentation I will show you the ease of hacking into the systems that runs our lives (SCADA - Supervisory Control And Data Acquisition), how weak are their protocols and how lame they are deployed. If you wanna play with the big boys systems - be in this SCADA hacking talk. (A new tool will be reveled in the talk).

Yaniv Miron is an information security consultant and researcher currently working at "IL Hack" as a security consultant and researcher for major organizations. Yaniv is a senior instructor at the "IL Hack Institute" that teaches hacking classes in Europe. Yaniv is the founder of the largest Israeli hacking convention - IL.Hack. Yaniv is certified as a CISO from the Israel Institute of Technology and a Certified Locksmith. Yaniv spoke at security and hacking conferences all around the world (BlackHat/SyScan/CONFidence/HackerHalted/OWASP/IL.Hack...). Yaniv is highly skilled with hands on penetration testing and security research and found many security vulnerabilities (Microsoft/Oracle/IBM...).

SCADA Hacking & Security Workshop

A résztvevők a SCADA (Supervisory Control And Data Acquisition) rendszerek hackelésének alapjait fogják megismerni. Szó lesz a SCADA protokollokról, a gyengeségeikről és a SCADA biztonságáról is. Látni fogjuk, hogyan kell egy SCADA-hálózatot telepíteni, hogyan kell pentesztelni, hogyan lehet meghakkelni, hogyan lehet a gyenge hálózati protokolljait átverni, és milyen a biztonsága úgy általában. Kötelező penteszterek, hackerek és biztonsági szakértők számára.

The participants will learn the basics of hacking into SCADA (Supervisory Control And Data Acquisition)systems, about SCADA protocols and their weakness and about SCADA security. We will learn how to deploy a SCADA network, how to pentest it, how to hack into it, how to trick the weak protocols of it and about it's security in general. It's a must training for penetration testers, hackers and security experts.

Beregnyei Balázs

Szilícium layouttól a kapcsolási rajzig

From silicon layout to circuit diagram

Az informatikai eszközeink működéséhez szükséges integrált áramkörökre általában fekete dobozként tekintünk. Egy chip adatlapját letölthetjük, fogyasztását, kimeneteit és bemeneteit, azok időzítéseit és protokolljait megismerhetjük, blokkvázlat szintjén áttekinthetjük a működését, de ennél részletesebb információt nem tudunk beszerezni a gyártótól. Ahhoz, hogy tranzisztor szintű kapcsolási rajzhoz jussunk, reverse engineering módszereket kell alkalmazni. Egy régi 8 bites processzor, a 6502 visszafejtésének példáján mutatom be, hogy viszonylag olcsó eszközökkel is lehet érdekes eredményeket elérni. Egy szemléletes módszer, a vízanalógia segítségével megtudhatjuk, hogyan működnek a legegyszerűbb tranzisztoros logikai kapcsolások, így azok számára is érthetőbbé válik egy processzor belső működése, akik kevésbé jártasak az elektronikában. A layoutfejtés grafikus szabályainak ismertetésével pedig az is kiderül, hogy az adott kapcsolások pontosan hogyan néznek ki a szilíciumon.

Beregnyei Balázs a Budapesti Műszaki és Gazdaságtudományi Egyetemen végzett 2004-ben mikrorendszerek és moduláramkörök főszakirányon és szoftvertechnológia mellékszakirányon. 2001-ben a tudományos diákköri konferencián „Mikroprocesszorok: layouttól a kapcsolási rajzig" című dolgozatával első díjat nyert. Jelenleg egyéni vállalkozóként többek között egyedi készülékek, elektronikák, nyomtatott áramkörök tervezésével, prototípus-építéssel, beágyazott Linux-rendszerek fejlesztésével foglalkozik.

Integrated circuits required for the operation of IT devices are usually considered as black-boxes. We can download a chip's data sheet and get to know its inputs, outputs, energy consumption, timing and protocol. We can even understand its internals at a block level, but manufacturers don't reveal more details. In order to get to a transistor level circuit diagram we have to use reverse engineering techniques. I will demonstrate using an old 8 bits processor as an example that one can achieve interesting results with fairly cheap devices. By contrasting the operation of the simplest logic circuits to water even those who have no expertise in eletronic can understand the inner working of a processor. By understanding the graphical rules of circuit layouts the audience will understand how they look like on the silicon.

Balázs Beregnyei has graduated at the Budapest University of Economics and Technology in 2004. His paper "From microprocessor to circuit diagram" has been awarded the first prize in Scientific Student's Conference in 2001. Nowdays he is working as a freelancer who designs individual devices, electronics and circuits, builds prototypes and develops embedded linux systems, among other things.

HELLO WORKSHOP

A workshopok kezdési időpontja az előadások kezdő időpontjához van igazítva. Minden workshop összesen háromszor lesz megtartva. Egyszerre 16 ember tud részt venni egy workshopon. A workshopokra a regisztráció a kezdés előtt pár órával lesz az információs pultnál. Mivel a workshopoknál nem lesz szinkrontolmácsolás, ezért a workshopleírásokban fel lett tüntetve, hogy milyen nyelven fognak folyni.

The starting time of the workshops is aligned with the starting time of the lectures. Each workshop will be held 3 times and 16 people can participate at the same time at a workshop. To register for the workshop go to the information stand a few hours prior to the starting time. There will be no simultaneous translation at the workshops. The workshop description will always show which language will be used.

1. nap, szombat / szeptember 17.		
	Eneterprise terem	*Voyager terem*
10:25–11:05	Szakály Tamás – Hello RCE (reverse code engineering)	Georgi Geshev – Hello packet capture / EN
11:50–12:50	nincs workshop	nincs workshop
13:30–14:10	Kovács Zsombor – Hello pendrive recovery	Egyed Péter – Hello loganalízis, avagy hatékony támadásdetektálási módszerek
15:15–15:55	Tomcsányi Domonkos – Hello Wi-Fi	Szatmári Gergely & Nagy Tibor – Hello PKI
16:15–16:55	Timur X. kHrotko – Hello password practice	Sebők Nándor – Hello mobilbiztonság
17:10–17:50	Kovács Zsombor – Hello pendrive recovery	Szakály Tamás – Hello RCE (reverse code engineering)
18:00–18:40	Egyed Péter – Hello loganalízis, avagy hatékony támadásdetektálási módszerek	Timur X. kHrotko – Hello password practice
2. nap, vasárnap / szeptember 18.		
	Eneterprise terem	*Voyager terem*
09:00–09:40	Szatmári Gergely & Nagy Tibor – Hello PKI	Szakály Tamás – Hello RCE (reverse code engineering)
10:50–11:30	Sebők Nándor – Hello mobilbiztonság	Tomcsányi Domonkos – Hello Wi-Fi
11:45–12:25	Georgi Geshev – Hello packet capture / EN	Egyed Péter – Hello loganalízis, avagy hatékony támadásdetektálási módszerek
13:20–14:00	Timur X. kHrotko – Hello password practice	Sebők Nándor – Hello mobilbiztonság
14:15–14:55	Szatmári Gergely & Nagy Tibor – Hello PKI	Kovács Zsombor – Hello pendrive recovery
15:15–15:55	Georgi Geshev – Hello packet capture / EN	Tomcsányi Domonkos – Hello Wi-Fi

Hello RCE (reverse code engineering)

Előadó: Szakály Tamás OSCE

Időpont: 09.17. 10:25–11:05, 17:10–17:50, 09.18. 09:00–09:40
Workshop nyelve: magyar

Leírás: A reverse code engineering az a folyamat, melynek során egy futtatható bináris fájlt „szétcincálunk" annak érdekében, hogy megfejtsük, mit és hogyan csinál. A legtöbb ember, aki ilyesmivel foglalkozik, másolásvédelmek törésével kezdte, de az RCE-nek vannak legális felhasználási területei is. Például malware-eket gyakran fejtenek vissza, hogy megértsék a veszélyt, amit jelentenek, illetve megtudják, hogyan lehet védekezni ellenük. Exploit írása közben is gyakran szükségünk van a hibás program visszafejtésére. A workshop bemutatja a Win32 reverse code engineering alapjait. Az előadás során a résztvevők megismerik az RCE során használt eszközöket, alaptechnikákat.

Módszer: A workshop első fele elméleti bemutató lesz a PE fájlformátumról, az IA-32 assemblyről, illetve az RCE során használt eszközökről. A második részben egy egyszerű crackmet fogunk visszafejteni, rögtön kétszer: először az OllyDbg nevű ingyenes Win32 ring3 debuggert használva, utána pedig az IDA Pro disassembler/debugger segítségével.

Feltételek: A workshophoz szükséges OS és programok egy VirtualBox/VmWare képfájl formájában kerülnek átadásra a résztvevőknek, így mindenkinek szüksége lesz egy számítógépre telepített VirtualBox/VmWare szoftverre.

Szakály Tamás 1985. augusztus 21-én született Szombathelyen. Jelenleg az ELTE Informatikai Karán végzi tanulmányait programtervező informatikus szakon. Mellette a PR-AUDIT Kft.-nél dolgozik informatikai biztonsági szakértőként és programozóként. 2008-ban előadóként vett részt a Hacktivity konferencián, ahol egy CUDA architektúrára írt MD5 hash törőt mutatott be. A 2010-es évben tagja volt a csapatnak, amely megnyerték a Hacktivity Capture the Flag versenyét. 2011-ben OSCE minősítést szerzett.

Tamás Szakály was born on the 21st of August, 1985. at Szombathely. He is now a student of the Faculty of Informatics of the Eötvös Loránd University. Besides that, he is working for PR-AUDIT KFt. as an IT security consultant and programmer. He gave a presentation about an MD5 hash cracker written for CUDA architecture at Hacktivity 2008. In 2010, he was member of the team that won the Hacktivity Capture the Flag contest. He acquired the OSCE certificate in 2011.

Hello pendrive recovery

Előadó: Kovács Zsombor penetration tester

Időpont: 09.17. 13:30–14:10, 17:10–17:50, 09.18. 14:15–14:55
Workshop nyelve: magyar.

Leírás: A workshopon a pendrive adattárolásának működéséről lesz szó. Ezzel kapcsolatban az alábbi témákat fogjuk körüljárni:
Hogyan működik az adattárolás?
Blokkméretek, slack, fragmentálódás, MFT. Mi történik, ha letörlök egy fájlt?
Disk image elmélet.

Módszer: Ezenkívül közösen elvégeznénk egy pendrive image-elést és az image szétcincálását foremosttal vagy autopsyval (az idő függvényében).

Feltételek: Nincsenek.

Kovács Zsombor legfőbb hobbija gyerekkora óta az, hogy szétszed dolgokat, és aztán szerencsétől függő mértékben összerakja őket – betörési tesztelőként így megtalálta álmai állását. Dolgozott mindenféle munkán Wi-Fi-s hálózattöréstől kezdve protokollanalízisen és social engineeringen át webalkalmazások teszteléséig, de legszívesebben fizikai betörési teszteket végez, amikor olyan helyeken kell járnia, ahová nem lenne szabad betennie a lábát.

Since his childhood Zsombor Kovács's favourite hobby has always been to take things apart and put them together again if luck was on his side – so as a penetration tester he has found the job of his dreams. He worked in all kind of projects from breaking into wi-fi networks through protocol analysis and social engineering to testing web applications. He prefers physical penetration testing which makes him visit places where he shouldn't be.

Hello Wi-Fi

Előadó: Tomcsányi Domonkos IT-biztonsági szakértő

Időpont: 09.17. 15:15–15:55, 09.18. 10:50–11:30, 15:15–15:55
Workshop nyelve: magyar

Leírás: A workshopon a Wi-Fi-hálózatok titkosítási módszereibe és a titkosítások törésének lehetőségeibe kapnak a résztvevők betekintést.

Módszer: WEP-hálózat törése (a WEP működése és a törés elmélete).
WPA–TKIP-hálózat törése (a WPA működése nagy vonalakban, illetve a Beck–Tews-féle WPA–TKIP attack ismertetése).
WPA2–AES-hálózat törése (miben különbözik a WPA-tól, illetve a legújabb CCMP known plain-text attack ismertetése).

Feltételek: Backtrack 5-kompatibilis, injectionre képes WLAN-kártya (szinte minden kártya, kivéve Hermes-, Aironet- és Marvell-alapúak, valamint a Broadcom BCM4321, 4322).

Középiskolai tanulmányaimat Magyarországon, Ausztriában és az Egyesült Államokban végeztem. 2006 óta foglalkozom etikus hackeléssel, IT-biztonsággal. Fő szakterületem a rádiós eszközök, azon belül is a Wi-Fi hálózatok feltörése, tesztelése. Ebben a témában eddig összesen nyolc cikket publikáltam, melyek közül egy, a 2008-ban felfedezett WPA-hibákat elemző esszém (melyet Fóti Marcellal közösen írtam) az ethicalhacking.hu-ra is felkerült. 2011 áprilisában kidolgoztam egy új támadás elméletét a WPA2-AES titkosítás és hitelesítés ellen. Az elméletet egy német programozóval közösen implementáltuk, a neve CCMP known plain-text attack, az ötletet a NetAcademia Ethical Hacking ösztöndíjjal tüntette ki. / http://domonkos.tomcsanyi.net

Attended high-school in Hungary, Austria and USA and went to college this September. Started dealing with ethical hacking and IT-security in 2006. His main area of interest is radio hacking, especially WiFi network cracking, testing. He published eight articles in this topic in Hungarian, one of them about the Beck-Tews attack (co-authored with Marcell Foti) was featured on the website of the Hungarian Ethical Hacking Community (http://ethicalhacking.hu). In April, 2011 he researched WPA2-AES and invented a new method for cracking the network key for such networks. Later he co-implemented the attack with the author of Pyrit, Lukas Lueg, and the idea was awarded with NetAcademia's Ethical Hacking Scholarship. / http://domonkos.tomcsanyi.net

Hello password practice

Előadó: Timur X. kHrotko

Időpont: 09.17. 16:15–16:55, 18:00–18:40, 09.18. 13:20–14:00
Workshop nyelve: magyar

Leírás: A workshopon röviden áttekinteném, hogy ma milyen irányadó ajánlások vannak jelszavakra, milyen eszközöket lehet igénybe venni szoftver, szolgáltatás és token tekintetében. Az előadás lényege pedig egy hüvelykujjszabály-rendszer lenne arra, hogyan lehet ezeket a rendelkezésre álló eszközöket és követendő iránymutatásokat minimális ráfordítással használni és betartani, azaz élhetőbb jelszókezelési praktikát használni, közben növelve a saját biztonságunkat. Ez az ajánlás nem független attól, hogy manapság jellemzően milyen operációs rendszereket, alkalmazásokat és szolgáltatókat használunk, ahol passwordözésre van szükség.

Módszer: Előadás és gyakorlati bemutató.

Feltételek: Nincsenek.

Timur a Cloudbreaker Company tagja. Az informatikai biztonságot egy emberi, szervezeti, társas ügynek tekinti. Tiimur PhD-jelölt, aki 2010-ben túlesett a védésen is a Budapesti Corvinus Egyetemen. Ugyanitt MSc fokozatot szerzett üzleti és IT-menedzsmentből 1993-ban, és pénzügyből 2000-ben. Budapesti születésű orosz.

Timur is a member of the Cloudbreaker Company. He treats information security as a human, organizational and societal matter. Timur is a defended PhD candidate at Corvinus University of Budapest (2010), where he also earned MSc degrees in Business IT Management (1993) and Finance (2000). He is a Budapest-born Russian.

Hello loganalízis, avagy hatékony támadásdetektálási módszerek

Előadó: Egyed Péter CISA

Időpont: 09.17. 13:30–14:10, 18:00–18:40, 09.18. 11:45–12:25
Workshop nyelve: magyar

Leírás: A workshop során szeretnék válaszokat adni egy rövid elméleti előadás keretein belül az alábbi kérdésekre:
- Mit jelent ma a loganalízis, és mire lehet használni?
- Hogy néz ki ma egy tipikus loganalízis-rendszer?
- Milyen szempontokra figyeljünk a logelemző architektúra bevezetésénél?
- Milyen szempontokra figyeljünk a korrelációs szabályrendszer létrehozásánál?

Módszer: Az elméleti részt követően szeretném a gyakorlatban is bemutatni a korrelációs szabályok létrehozását, amelyeket közös gondolkodással állítok össze a résztvevőkkel. Az összeállítást követően ki is próbáljuk a létrehozott szabályok hatékonyságát.

Néhány tipikus eset:
- Brute force detektálás.
- Portscan detektálás.
- Hozzáférés érzékeny fájlokhoz.
- Privilégiumok módosulása.
- Naplóállományok törlésének detektálása.

Feltételek: A gördülékeny workshophoz laptop és ezen előre telepített MS office / Open office és egy virtualbox javasolt.

Péter az Óbudai Egyetemen, az informatikai biztonsági szakirányon szerezte meg BSC képesítést, jelenleg pedig a Corvinus Egyetem, Gazdaságtudományi Kar, gazdasági informatika szakon tanul. A bankbiztonság területén többéves biztonsági adminisztrátori tapasztalattal rendelkezik.

Péter has graduated at Budapest Tech, John von Neumann Faculty of Informatics, BSC in Computer Sience and Egineering, IT security department, currently he is attending Corvinus University, MSc in Business Information Systems. He has several years of experience in banking security as IT security administrator.

Hello packet capture

Speaker: Georgi Geshev

Time: 17.09. 10:25–11:05, 18.09. 11:45–12:25, 15:15–15:55
Workshop language: English

Description: This workshop aims to be a gentle introduction to packet capture formats and network protocol analyzers. Participants will be taught on how to perform, manipulate and replay packet captures according to a certain predefined criteria. Some basic file extraction techniques will be demonstrated as well.

Method: : Participants will perform a live packet capture with one of the aforementioned protocol analyzers, preferably Wireshark/Tshark or TCPdump.
They'll need to extract some objects/files from the already saved packet capture file. One of the successfully extracted files will contain further instructions on how to perform a basic live packet replay attack.

Prerequisites: All the workshop participants will need a laptop with a fully functional wireless network interface card.

Georgi Geshev másodéves informatikai hallgató. Emellett független biztonságihiba-vadász és szenvedélyes FOSS-evangelista, aktív közreműködője különböző ingyenes és open source szoftverprojekteknek, az OWASP-ot, az Openwall- és Mozilla-projektet is beleértve.

Georgi Geshev is a second year CS student. He is also an independent security bug hunter and a passionate FOSS evangelist, actively involved in various free and open source software projects including the OWASP, the Openwall Project and the Mozilla Project.

Hello PKI

Előadó: Nagy Tibor, Szatmári Gergely

Időpont: 13:15–13:55
Workshop nyelve: magyar

Leírás: Az internet széles körű üzleti felhasználásának alapja, hogy a kommunikációban érintett felek egymást kölcsönösen azonosítani tudják. E nélkül nem lehetne biztonságosan bankolni, online fizetni, de akár e-mailjeink olvasása sem lenne ugyanaz. Mindezeket egy kevéssé értett és kevés figyelmet kapó technológia teszi lehetővé: a PKI. A workshop gyakorlati példákon keresztül ismerteti meg a résztvevőket a PKI alapfogalmaival, a tanúsítványok mibenlétével és használatával. A workshop végére tudni fogjuk, miért lopnak SSL-kulcsokat, és mire figyeljünk böngészéskor.

Módszer: A bemutató során kitérünk arra, mi is az a tanúsítvány, hogyan igényeljünk és használjunk SMIME-tanúsítványokat a levelezés biztonságának fokozására.
Elektronikusan aláírt levél küldése során betekintést nyújtunk az aláírás, tanúsítvány-ellenőrzés működésébe. Megmutatjuk a titkosított elektronikus levelek küldésének lehetőségét mobileszközön is.
A workshop befejező részében SSL-tanúsítványok kezelésével foglalkozunk. Megnézzük, melyek a lényeges különbségek a felhasználó számára kiadott SMIME-tanúsítványok és a szerver számára kibocsájtott SSL-tanúsítvány között. Megvizsgáljuk, hogy a szerver oldalának megnyitásakor milyen tanúsítványt kapunk, és validáljuk azt, illetve kitérünk arra, hogy egy esetleges man in the middle támadásnál mikre érdemes odafigyelnünk.

Feltételek: A workshophoz saját laptop szükséges, amelyre Mozilla Thunderbird 6 levelezőprogram van telepítve konfigurált, működő e-mail fiókkal, a levelezőszerverhez SMTP + IMAP/POP3-csatlakozással konfigurálva. (A Gmail account + IMAP megfelelőségét teszteltük.) Opcionálisan Android okostelefon Android 2.1 vagy későbbi operációs rendszerrel, Android Market-hozzáférés.

Nagy Tibor 14 éve dolgozik a nagyvállalati számítástechnika területén, ebből az elmúlt 9 évben az IT-biztonság számos területén szerzett széles körű tapasztalatokat. Jelenleg a HP Informatikai Kft. IT-biztonsági üzletágának munkatársa, ahol vezető konzultáns a PKI, az azonosság és központi hozzáférés-kezelés szakterületeken. CISA és CISSP minősítése van. Tibor 1992-ben végzett az ELTE matematika–fizika szakán, 1996-ban ugyanitt szakinformatikusi diplomát szerzett. Korábban a HP jogelődjeinél, a Compaq és a Digital Magyarország Kft.-nél töltött be különböző beosztásokat a rendszer- és alkalmazásintegráció területén.

Gergely Infokommunikációs rendszerek biztonsága szakirányon végzett a BME-n 2006-ban. Azóta a Hewlett Packard Informatikai Kft. IT-biztonsági részlegén dolgozik mint IT-biztonsági tanácsadó.
Mint PKI-rendszer-szakértő behatóan foglalkozott tanúsítványokkal, a titkosított levelezés lehetőségeivel az évek során. Mindezek mellett nagy tapasztalatot szerzett jogosultságkezelő rendszerek bevezetésén keresztül hiteles felhasználói adatok előállításával, megfelelő jogosultságok kialakításával és azok online integrációjával a tanúsítványkiadó rendszerek felé. Technikai ismeretein melett felülhitelesített PKI-rendszerek megvalósításán keresztül szakértelmet szerzett a megfelelő tanúsítványkiadási, -használati folyamatok és szabályzatok létrehozásában is.

Nagy Tibor has been working in the field of enterprise IT for 14 years. He has gained expertise in various areas of IT security in the last 9 years. Nowdays he works at the IT security division of HP Informatikai Ltd. where he is a senior PKI constulant of identity and centralized access management. He has received CISA and CISSP certifications. Tibor has graduated from ELTE as mathematics and physics teacher in 1992. In 1996 he received Msc in informatics from ELTE. In former times he worked for HP's predecessor companies Compaq and Digital Hungary Ltd. in various positions in the fields of system and application integration.

Gergely graduated from BME at faculty of infocommunication systems security in 2006. Since then he works for Hewlett-Packard Hungary Ltd. at IT security division as IT security consultant.
As PKI systems expert he has delved into certificates and opportunities of email encrpytion over the years. Beside all of these by implementation of authorisation management systems he has gained deep knowledge of authentic user data production, implementation of proper user rights and online integration of those with public key infrastructure systems. His expertise is not limited to technical issues because by implementation of certified PKI systems he knows how to develop policies and processes necessary to certification issuance and usage.

Hello Mobilbiztonság

Előadó: Sebők Nándor

Időpont: 13:20–14:00
Workshop nyelve: magyar

Leírás: 2011-ben 280 millió Android operációs rendszert futtató okostelefon eladásával számolnak, így egyre nagyobb az esélye, hogy az Ön zsebében is egy ilyen készülék lapul. Belegondolt már, mi történne, ha például elveszítené, és mások kezébe kerülnének a rajta tárolt adatok? A workshop során végigjárjuk a rendszer gyenge pontjait, valamint a gyakorlati részben telefonunk védelmét szolgáló alkalmazásokat is kipróbálhatnak a résztvevők.

Módszer: Az elméleti részben bemutatott védelmi eszközök közül egy fájltitkosító alkalmazás, valamint egy komplex védelmi megoldás is kipróbálásra kerül, mely során lehetőség lesz kipróbálni, hogy milyen lehetőségeink vannak állományaink védelmére, ill. mit tehetünk ha elveszítettük telefonunkat.

Feltételek: A workshophoz csupán egy Androidot futtató okostelefon és az Android Market elérése szükséges.

Nándor a Noreg Információvédelmi Kft. rendszermérnöke, előzőleg a Citibank globális sérülékenyégelemző csoportjának tagjaként dolgozott. 1976. szeptember 5-én született Pécsett. Jelenleg a Noreg Információvédelmi Kft. rendszermérnöke, ahol különböző IT-biztonsági rendszerek bevezetését és üzemeltetését végzi. Előzőleg a Citibank globális IT-biztonsági csoportjának tagjaként a világ egyik legnagyobb vállalati hálózatán végzett sérülékenységelemzést. 2006-ban CISSP minősítést szerzett.

System engineer from Noreg Kft, formerly member of global vulnerability assessement group of Citibank. Sebők Nándor was born in Pécs, Hungary, 1976. Currently he works for Noreg Kft as a system engineer. He is responsible for installing and operating different IT security systems. Formerly as a member of global IT security team, he was responsible for vulnerability assessment and scanning within one of the largest enterprise network. He obtained CISSP certification in 2006.

JÁRD VÉGIG A HP HACKER TANÖSVÉNYT ÉS SZEREZD MEG A CERTIFIED HACKER ROAD PARTICIPANT PROFESSIONAL MINŐSÍTÉST!

WALK THE HP HACKER ROAD AND GET THE CERTIFIED HACKER ROAD PARTICIPANT PROFESSIONAL CERTIFICATE!

A tanösvény egy olyan kiépített gyalogút, amin végigsétálva megismerkedhetsz a konferencia különböző helyszíneivel és **EGYIDEJŰLEG MAGASAN KÉPZETT HACKERRÉ VÁLHATSZ.**

*If you hike along the road you can get to know the different locations of the conference and will become a **HIGHLY QUALIFIED HACKER.***

Az összes tanösvényt teljesített túrázó között vasárnap 17.35-kor kisorsolunk a konferencia zárásakor **3 db 500 gigás hordozható merevlemezt** a Pipacs teremben a HP és az RRC jóvoltából. Az induláshoz kérd el a menetlevelet az **RRC standján!**

*Hikers who walked along the road and are present at the closing ceremony (5.35 pm) on Sunday will have the chance to win one of the **three 500Gb portable hard drives** thanks to HP and RRC. To start hiking get your passport at the RRC stand!*

rrc THINK VALUE.

Szeretnél egy aranyrudat?!

Ugye megkaptad az e-mailünk és megszerezted a **Cyber-Ark** egyedülálló digitális páncélszekrényből a **kancellar.hu** kódmondatát?

Keresd meg a **kancellar.hu standját** és váltsd be a névjegyeddel együtt egy **aranyrúdra!**

A Cyber-Ark egyedülálló technológiája megvédi a benne tárolt dokumentumokat (Sensitive Information Management Suite) és jelszavakat (Privilege Identity Management Suite) és a hozzájuk kapcsolódó audit (Privileged Session Management Suite) információkat.

kancellar.hu
AZ INFORMATIKAI BIZTONSÁG SZAKÉRTŐJE