Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Compass Security AG

BSidesLV, Black Hat & DEF CON 2014

27. August 2014

Document Name:	blackhat_2014_paper_v1.0.docx
Version:	v1.0
Authors:	Alexandre Herzog, Compass Security Schweiz AG
	Dobin Rutishauser, Compass Security Schweiz AG
Date of Delivery:	27. August 2014
Classification:	Public

Compass Security AG

By Alexandre Herzog [alexandre.herzog@csnc.ch] & Dobin Rutishauser [dobin.rutishauser@csnc.ch]

Introduction

As each year, a couple of Compass analysts have the opportunity to travel to Las Vegas and take part at the mythical Black Hat and DEF CON security conferences. This year's schedule also allowed us to attend the first day of BSides Las Vegas, which also happened to be combined with the Passwords14 conference. This first day at the Tuscany Suites & Casino was followed by two days at Black Hat USA 2014, located for the first time at the Mandalay Bay. Finally, we attended DEF CON 22 – which took place for the last time at the Rio Hotel & Casino.

BSidesLV 2014 & Passwords14

Opening Keynote – Beyond Good and Evil: Towards Effective Security

Presented by Adam Shostack - video

Inspiring keynote which stated that efficiency is the main issue in our business, leading to personal dramas of people due to burn outs. Currently companies address issues around APT / 0day protection, compliance and implementation of best practices. Bu t there is little to no scientific approach or feedback loop, especially around the (hardly) learnt lessons after an incident. While recent US laws force enterprises to disclose data breaches, the hacker community only gets the "what happened" about the incident, but not the information "how it happened". Without this information, it is hard to decide if research and investments are well spent.

It is a common believe that sharing data about successful attacks harm the company in question, by affecting for example the stock price or due to lost customers. In fact, no evidences exist which proves such an impact over medium or long term. On the contrary, transparency tends to increase public trust in the company.

Adam suggests bringing in some science in this field by establishing a matrix listing controls which may-, or should, detect incidents. Feedbacks from incidents can then feed into this document and allow correlation (e.g. sites with Microsoft EMET never felt victim of 0day attacks so far). Results should be shared, enabling us in the information security industry to leverage proven efficient solutions for today's challenges.

SHA-1 backdooring and exploitation

Presented by Jean-Philippe Aumasson - video - website

Swiss-based Jean-Philippe started his presentation by recalling the research done on SHA-1. This hashing function is considered from an academic perspective to be broken since 2005 as attacks allow creating collisions in an order of 2^{60}. The presented research is the result of a team effort done by Jean-Philippe, fellows from Graz University of Technology, Austria and Ange

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Albertini – who is well known in the community for "corkami" and his schizophrenic files. By altering 4 32-bit constants defined in SHA-1, they found exploitable collisions in an order of 2^{48}. An illustration of their work is based on two related JPEG files which display completely different pictures and also have other sizes. These files in fact both contain two images, similarly constructed to Ange's schizophrenic files, but some tweaks in the file structure make one or the other images appear in the reader. The delta between both files is ironed out by well-chosen SHA-1 constants.

The tuning applied to the algorithm's constant is partially file format dependent and doesn't work for all type of files. While they were unable to create SHA-1 collisions for ELF or EXE files, they found collision possible for e.g. COM, Bash scripts or RAR files.

Tuning the constants of SHA-1 is, according to the speaker, a common practice for some vendors, looking for proprietary tools and verification mechanisms. Such alterations should therefore be questioned in light of these recent results.

Allow myself to encrypt… myself

Presented by Evan Davison - video

The speaker states we transitioned from a state of connectivity (we could have online access) to constant connectedness, where everything is connected and always online. In such a world, trying to constantly keep the bad guy out is getting harder and harder. His suggested approach is to minimize the available plain text data by integrating encryption in the standard IT stacks and thus reduce exposure. From an OSI layer perspective, he reckons that encryption should be integrated in the presentation layer, creating layer "6.5". Keys should also be bound to roles or groups, making data only available to a limited amount of people.

What Microsoft would like from the Password Hashing Competition

Presented by Marsh Ray and Greg Zaverucha

Microsoft is the only big "industry" stakeholder in the currently running Password Hashing Competition (PHC). While the presentation was not officially endorsed by the company, it presented various use cases and requirements where the winning algorithm might be used in the future. Several of the expressed requirements where aimed at simplifying as much as possible the life of developers, ensuring their implementation of the solution would be easy and similar to PBDKF2.

Protecting Data – How Cultural-Political Heritage Shapes Security Approaches

Presented by Malte Pollmann

The speaker, a German CEO of a company building e.g. Hardware Security Modules (HSMs), presents his over 10 years of experience and observations about how data protection and security are perceived in the US and Europe. The first comparison is between Carcassonne, a French medial town surrounded by guarded walls and a plain grid town structure common in the US. By its history, Europe relies on a trust model where the community (e.g. people behind the walls) takes a big place versus the individual focus of Americans.

Laws in Europe tend to be much less specific, usually referring to "state of the art" practices where US laws would clearly require encryption of data. This leads to unexpected results in his experience, as e.g. much less US companies seem to implement pre-boot authentication than in

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Europe, arguing that the data is already encrypted by another mechanism on the device.

His talk also evoked the focus or data protection (EU) versus system protection (US), or the Preska case, where a US judge ruled that US company Microsoft must hand over to the US justice emails stored in Ireland and considered to be protected by the Safe Harbor framework.

Tradeoff cryptanalysis of password hashing schemes

Presented by Alex Biryukov, Johann Großschädl & Dmitry Khovratovich – video

The team analyzed three candidates in the password hashing competition. These competitors should be memory-hard alg orithms, as memory in hardware is expensive and slow. Therefore creating hardware based password brute forcing chips will be expensive too. They showed that two of the algorithms could be efficiently implemented in hardware, despite looking complex in their design. The method used is similar to normal cryptanalysis. Their own proposed algorithm did withstand their own analysis.

Using cryptanalysis to speed-up password cracking

Christian Rechberger – video

The speaker advocates improving the inter-disciplinary work between crypto analysis and practical password cracking. A good example is hashcat, where the developer integrates many cutting edge cryptographic research results for effective brute forcing.

Bridging the Air Gap: Cross-Domain Solutions

Presented by Patrick Orzechowski - video

The speaker starts by presenting requirements which state that document of a given classification domain (e.g. secret or top-secret) can only be processed on devices and networks located within the same classification. No logical connection is allowed between networks of different classification and data exchange occurred historically by scanning documents or burning CD-ROMs.

New systems called Cross-Domain Solutions (CDS) emerged, which serve as exchange point between these networks of different classification. The CDS are pulling data from the networks, acting each time as client and implement Mandatory Access Control (MAC) based e.g. on SELinux or Trusted Solaris, ensuring all data received on a network is labelled accordingly.

Interestingly enough, CDS solutions are not sold by companies specialized in software but by contractors such as Boeing. Some solutions propose the aggregation of connections from unclassified, secret and even top-secret networks on one box. Several CDS solutions are based on open source software and get built on unclassified networks. A future project of the speaker is OpenCDS, an open source CDS project.

This talk was the last attended on this first day of conferences. We took this opportunity to socialize with other peers. We therefore missed the final Passwords14 talk "Surprise talk + advisory

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

release" of our Swiss friend Dominique Bongard. This talk turned out to be the spot where he presented "Offline bruteforce attack on WiFi Protected Setup" (presentation & video), disclosing the weaknesses in the randomness of the nonce he discovered in the implementation of the WiFi WPS protocol of several access point vendors.

Black Hat USA 2014

Keynote – Cybersecurity as Realpolitik

Presented by Dan Geer – transcript – video

The opening keynote of Black Hat was truly fascinating and cannot be resumed in a few paragraphs. I therefore warmly encourage you to take time to read the transcript or watch the video where Dan Geer exposes groundbreaking legislation ideas to improve cyber security. These ideas include mandatory reporting (and voluntary announcements, see Adam Shostack's opening keynote as BSidesLV), depicted an interesting choice for ISPs about net neutrality, recommends source code liability and discussed consequences of its abandonment or government funded vulnerability finding programs (see Stefan Frei's presentation at Area41).

The beast wins again: why TLS keeps failing to protect HTTP

Presented by Antoine Delignat-Lavaud – slides, paper, and video of the demos

The speaker demonstrated several attacks on TLS implementations, which are based from a network perspective. The first attack, named cookie cutter, relies on the fact that TLS implementations will accept truncated messages sent over an abruptly interrupted TCP connection, allowing an attacker to reset the stream before e.g. additional cookie settings (such as flag "secure") has been received by the client. The same attack could be used to bypass HSTS by truncating the headers (the client gets a HSTS time of 10 instead of 10'000 seconds as the communication is reset immediately).

Several attacks based on virtual host confusion were also demonstrated, e.g. by abusing the default virtual host or with SPDY, which multiplexes communications to different web sites in the same TCP connection if the web sites are all hosted on the same IP address. Flaws in the TLS specifications – such as for the triple handshake attack – were also uncovered, and are currently being address by the adequate working group.

As conclusion, clients and servers should always reject content which cannot be parsed or which is malformed. Additionally, don't base security on explicit declarations but specify it implicitly to avoid attacks such as the truncation of the httpOnly or Secure cookie flags.

Bringing Software Defined Radio to the penetration testing community

Presented by Jean-Michel Picod, Jonathan-Christofer Demay & Arnaud Lebrun – slides – video – paper

The root of the presented project is the steady increase of embedded and mobile devices such as smart meters. While there are several tools out there to analyze specific protocols (e.g. Ubertooth for Bluetooth, rfCat or Api_Mote for Zigbee), today's CPU can (almost) handle the load to perform all tasks in software instead of relying on dedicated hardware. The only requirement is to possess the hardware to acquire the signal before passing it to the software stack.

The presented software stack is a combination of two existing tools: GNU Radio and Scapy, the famous packet manipulation program. GNU radio

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

can do some analysis on blind signals to identify the adequate parameters, while Scapy already supports many protocols and has native fuzzing capabilities. The binding between these two projects was named scapy-radio and will be available within the next release of Scapy. Communication between Scapy and GNU radio is done over UDP, as it allows the setup of cluster to scale up to catch high frequencies. The tool was used to analyze Z-Wave, a Bluetooth Low Energy e-cigarette or XBee. Their software is available on Bitbucket and the authors also provided detailed step-by-step instructions on how to add new protocols and enhance the tool.

Governments as malware authors: the next generation

Presented by Mikko Hypponen

It was a pleasure seeing Mikko on stage, as he delivered (yet another – see his TED talks) convincing and engaged presentation about the current situation of malware, especially those written by state nations. While his talk did not contain revelations or new facts (especially if you follow him on Twitter - @mikko), he linked recent revelations together in a great and entertaining story.

Mikko also stated several assertions, which surfaced in other talks heard during our week in Las Vegas. As already said by Adam Shostack in his opening keynote of BSlidesLV, no company ever went bankrupt due to a data breach – aside Dutch Diginotar, which had trust as its only business model. He also made several parallels between cyber and nuclear weapons. Nuclear deterrence worked because all other parties knew a country had the technology for nuclear bombs. Capabilities of countries about cyber weapons are on the other hand a high secret – although several countries were listed by Mikko (including e.g. Sweden, which is not a NATO country).

Article 52 of the Geneva Conventions states that: "In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.". While nuclear weapons are exclusively the matter of the military, civilian information security practitioner are daily in contact with tools which may qualify as potential cyber weapons and may therefore be a target of war…

Finding and exploiting access control vulnerabilities in graphical user interfaces

Presented by Collin Mulliner – slides – paper

While shatter attacks against Windows services date back to 2002 as a way to escalate privileges, they are nowadays fixed with the various restrictions implemented in the operating system. Still, many user-land applications are tempted to implement their own access control. An application implementing its own ACLs will likely have a hidden GUI to manage these permissions.

The threat model presented in this talk is against applications which implement their own user management, thus not relying on the operating system. Three types of bugs were identified: unauthorized callback execution, information disclosure and information manipulation. The speaker first demonstrated how to use WinSpy++ (published on catch22.net, including the source code) to activate a disabled button in the UI. He then demonstrated his GEM Miner System, which automates the discovery process of hidden GUIs. The tool uses Win32 API calls such as sendMessage, enumCildWindows and enableWindow, which can also uncover .NET apps GUIs. The tool is therefore a good indicator to see

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

if the application is developed in a serious way and to find backdoors.

Responsible disclosure roundtable: you mad Bro?

Moderated by Trey Ford

Several aspects of a bug bounty programs where discussed during this roundtable, highlighting the fact that a company starting such an incentive program must prepare itself beforehand. Not only the legal aspects must be prepared, but also several operational tasks must be clarified to handle the 10 fold multiplication of reports the company is likely to get just after the start of the bounty program.

Other discussions were oriented on how to handle security advisories for cloud providers. While customers do not need to take any actions in such cases, they expect transparency from their provider as in the case of Heartbleed. About disclosure of security issues to ICS vendors, participants pointed out ICS vendors are now well geared and reactive to incoming notifications. The issue is no more the vendors but the operators of SCADA systems, who do not yet have a culture of patching their ever running systems.

This topic becomes a business as some participants founded or were employed by startups managing bug bounty programs on the behalf of their customers. The corporate world integrates now information security and is capable of well reacting to issues such as e.g. Heartbleed. Individuals unfortunately remain largely unaware of these topics and do not take events such as the recent end of life of Windows XP seriously.

I know your filtering policy better than you do: external enumeration and exploitation of email and web security solutions

Presented by Ben Williams – slides

The speaker is the author of WebFEET and MailFEET, two tools to automate the audit of web and email content filters. Using these tools, the author was able to quickly get an overview of the currently applied web proxy filtering policy in a company and detect device limitations or policy misconfigurations.

Flaws in the web content filters include verbose HTTP headers added by the appliance, issues in the handling of invalid SSL certificates or representation of error messages within the Same Origin Policy as the filtered website. The timing of the blockage (when the request is sent or after the response was examined) can also reveal details about the policy, as a blocked URL will be blocked upfront while a content scanning failure will only occur after a given delay.

The mail content filter assessment can be done without any insider knowledge if inexistent emails bounce. All an attacker needs to do is sent various emails with specific content. Applied filters, email architecture and product information might be deduced by the attacker based on email bounces (or the absence of error notification in case of a filtered email with malicious content).

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

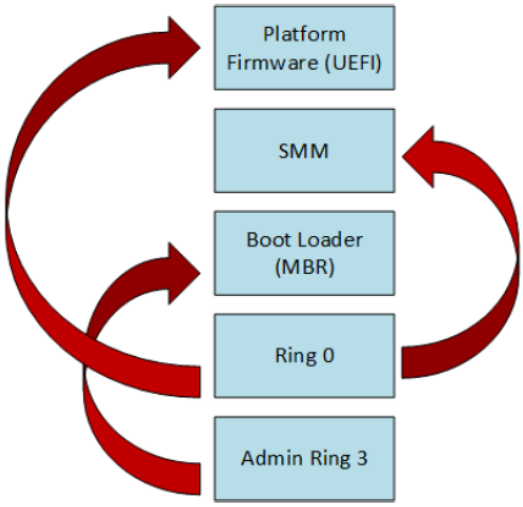
T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Extreme privilege escalation on Windows 8 / UEFI systems

Presented by Corey Kallenberg, Xeno Kovah & Samuel Cornwell – slides – paper

Nowadays, an attacker able to gain local administrator rights on a machine remains restricted by the operating system to ring 3 execution (user space). While kernel execution might be possible abusing further flaws (e.g. the recent exploitation of a digitally signed VirtualBox driver), even ring 0 access does not provide access to UEFI related components such as SMM.

The speakers therefore focused on attacks on UEFI from admin ring 3. Once UEFI is compromised, they would then be able to subvert all the underlying components (SMM, MBR and kernel). Administrators can, in Windows 8, interact directly with the UEFI by setting environment variables (SetFirmwareEnvironmentVariable).



These user-defined values are parsed and executed by the UEFI on the next boot. By analyzing the open source reference implementation of UEFI, they found two new attacks. The first issue was found in the coalescing phase (PEI) of the UEFI firmware update process, which allows the injection of code before its integrity is checked. The second issue is during the DXE phase, while the envelope of the UEFI firmware update is parsed.

As both issues were found in early boot phases, the relevant UEFI registers are not yet locked at this point in time. These flaws can therefore be abused to defeat SecureBoot, make a SMM rootkit, subvert the hypervisor, … – all of this independent of an reinstallation of the operating system. An exploit was presented where the UEFI of a machine running Windows 8 was exploited and an OS independent SMM rootkit was installed. This SMM Watcher continuously scans the memory and executes code as soon as a given signature is found. Assembly payload can therefore be executed in a platform independent way by the rootkit using several means, e.g. by processing a ping request, visiting a web page or receiving an email. The demo finished by a payload which would overwrite the first four bytes of the boot instructions.

The disclosure was done with Intel, but the coordination for the fix across all manufacturers caused to be troublesome. It is yet unclear if all vendors patched their UEFI and released patches. This kind of issues should become easier as a new CERT for UEFI Security Response Team (USRT) is being created and starts on September 1st, 2014.

Abusing Microsoft Kerberos: Sorry you guys don't get it

Presented by Alva Duckwall & Benjamin Delpy - slides

Despite Microsoft's updates to improve credential protection in May 2014 (see KB 2871997), pass-the-hash still works on the vast majority of systems. What are the options open to an attacker if the NTLM provider is disabled or the new "protected users" feature is in use? The answer is

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

"Kerberos", as tickets can be stolen and reused. In Microsoft's implementation of Kerberos, valid tickets are all based on encryption material derived from passwords: the KDC long-term secret key – used for the Ticket Granting Ticket (TGT) – is truly the domain key while the client long-term secret is derived from a user's password. Finally, the target/service key is also derived from another password for a given Ticket Granting Service (TGS).

Depending on the functional level of the Windows domain, elderly cipher primitives are used to encrypt the tickets. Furthermore, the domain key only changes when you upgrade your domain from functional level Windows 2000 to Windows 2003. This domain key, represented in fact by the password of domain user krbtgt, is never changed afterwards. An attacker able to compromise a domain controller (DC) can therefore steal this domain secret and use it to craft arbitrary Kerberos tickets – and this long after the compromise has been detect and remediated.

The first demo performed by Benjamin, author of mimikatz, showed how to inject stolen Kerberos tickets on an un-joined computer. By default, a standard user cannot access his TGT but only the issued TGS. This setting can be overridden in the registry and a local administrator will continue to be able to dump the TGT and TGS of all the users currently connected on the machine. Another demo showed how the credentials of user krbtgt, stolen on a DC could be used to craft arbitrary Kerberos tickets. The only other requirement is the knowledge of the domain's name and SID, information accessible to any domain user.

As Kerberos tickets contain all the information required for a user to authenticate, it's thus possible to create fake but valid tickets containing arbitrary group memberships. It is also possible to include user related SIDs in the membership section of the ticket, granting access to this user's privileges. Windows machines will even accept tickets issued for inexistent username and still allow authentication.

The library of Sparta

Presented by David Raymond, Greg Conti & Tom Cross – slides – paper

The speakers discussed military doctrine in context of computer security. Relevant documents are for example Field Manual (FM) 3-0 (Operations), FM 5-0 (The operations process), and FM 6-0 (Mission command). The word OPSEC "Operations Security" mainly means the protection of information. OPSEC failed for Stuxnet, because it was distributing itself widely, which led to detection routines from anti-viruses. Some of the modules were also used for Duqu, which was the reason for its detection. The KILLCHAIN describes the process of "find, fix, track, target, engage and assess". In asymmetrical warfare, this can be used as advantage, as each stage can be identified by the defender. "Cyber terrain analysis" uses the OCOK concept: "observation, cover and concealment, obstacles, key terrain, avenues of approach". Here too, the defender has an advance, as for the attacker it is difficult to correctly map the terrain. The word "denial" was described as "hinder or deny the enemy the knowledge of an object, by hiding or disrupting the means of observation". In IT security, this can mean the use of deception and canaries in all forms. "Exploiting the human" is not only the weakest link for the defender, but also in the attacker. On risk analysis, it was mentioned that "the more you know of an attacker, the greater the risk of let the adversary continue". Because at first one should study the attacker, but when you know enough you should stop the attack. After that, the famous OODA loop was recited (observe, orient, decide, act). It means to operate at a faster tempo or rhythm than the

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

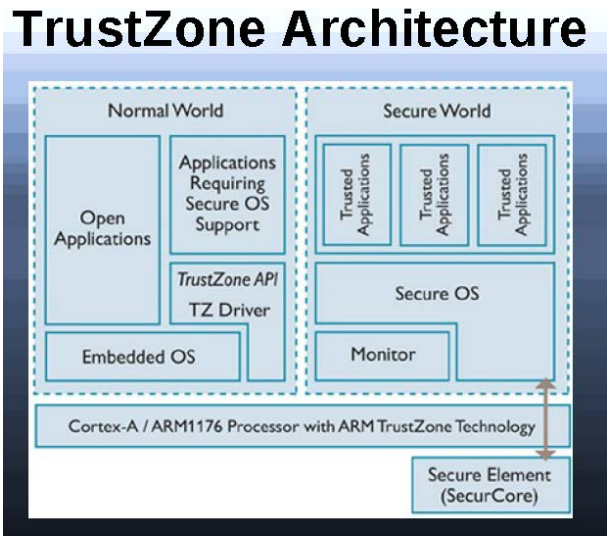
T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

adversaries. "Targeting" can be described quickly as "decide, detect, deliver, assess". Last but not least, the military has centuries of know-how in attack and defense, and the IT security industry could learn a lot of it. Examples are the cycle of military operation planning, the "design" aka the way of creating and thinking of problems, and the heavy use of graphics and symbology.

Network attached shell: N.A.S.TY systems that store network accessible shells

Presented by Jacob Holcomb

The talk discussed several vulnerabilities of numerous tested NAS (Network Attached Storage) systems of different vendors. 100% of the tested products were exploitable, 50% of them without authentication. This is problematic, as the same software is being used in low-end products as in high-end products. These systems offer a lot of unnecessary services over the network. The most common vulnerability is the "command injection". But also several backdoors (hardcoded accounts) and directory traversal vulnerabilities could be identified. A vendor used the current time in microseconds in hex as cookie value, or used the HTTP referrer header information as security token.



The beast is in your memory: return-oriented programming attacks against modern control-flow integrity protection techniques

Presented by Daniel Lehmann & Ahmad-Reza Sadeghi

The speakers presented an introduction into anti-ROP exploitation measurements first. It is assumed that the attacker knows the memory layout, is able to hijack the control flow and also has access to gadgets. The usual defense against ROP is called "Control flow integrity" (CFI), which has several problems like coverage, accessibility to debug symbols or performance overhead. EMET is an example of a "Coarse-grained" CFI. It hooks critical functions (like syscalls) to check if the call stack comes from a valid originating function. The speakers analyzed the EMET CFI implementation, and showed that it is possible to circumvent all protection measurements by simply using ROP gadgets of kernel32.dll (which is mapped by default by all processes). This was mainly achieved by selecting "good" gadgets, and a very long "NOP gadget". As a proof of concept, they show a demonstration of an older PDF exploit, where the Acrobat Reader process was protected using all EMET 4.1 features. In the Q&A, they said that EMET 5.0 introduced no big changes and that their technique still works with this version.

Reflections on Trusting trustZone

Presented by Dan Rosenberg – slides

In this talk, the speaker analyzed the TrustZone implementation of Qualcomm (Qualcomm secure execution environment - QSEE - used by Samsung S4, S5, Nexus 4/5 and many more devices). The TrustZone is a special mode in the ARM CPU, which executes code loaded from the firmware (or from disk). This code is then called "trustlet", and is stored in a protected memory

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona
T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

location, not writable by non-Trustlets. The attack surface consists of the secure monitor call (SMC), hardware exceptions, the shared memory interface (MobiCore), the eMMC flash (used by secure boot), and Trustlet-specific calls. The author identified a buffer overflow in the Qualcomm Secure Channel Manager (SCM), the Linux Kernel Driver used to interact with the QSEE via SMC. The SMC has to check if the destination memory address is not in the protected (Trustlet-specific) memory area. The check can be circumvented by a clever exploit (but requires the ability to execute kernel code), and the protected memory made writable. This allows full access to the complete protected memory. As Motorola implements their locking/unlocking in the TrustZone, it was possible to implement an exploit relying on this technic which reliably unlocks Motorola phones. But it is also possible to access any secrets stored in the TrustZone, and execute any code in it.

Abusing performance optimization weaknesses to bypass ASLR

Presented by Byoungyoung Lee, Yeongjin Jang & Tielei Wang

Some browsers use memory addresses as index key in hash tables. Depending on the implementation, this can be used to leak up to 12 bits of pointer addresses which can then be misused to guess valid memory pages despite enabled Address Space Layout Randomization (ASLR) protection.

Write once, pwn anywhere

Presented by Yang Yu

In JavaScript 5.8, the internal representation of strings was called a "bstr", which contained its length and a pointer to the string itself. If it is possible to change the length of the string, the memory after the end of the string buffer could be read, which was immensely helpful for exploitation purposes. Sadly for exploit writers, IE9 uses JavaScript 9, which is now immune again this kind of attack. Nevertheless, using special tricks, it is still possible to get the JavaScript 5.8 implementation "back" - featuring the old, vulnerable behavior. In JavaScript 9, ArrayData is the new bstr-like data leaker. It is even better as its predecessor, as its implementation allows writes instead of reads. After code execution is achieved through an exploit, one needs to break out of the IE sandbox. The author described his technique as "vital point strike", where overwriting a single byte puts the browser into "God mode". From there it is possible to download a malicious DLL, which is then stored in the temp folder. By creating a "System32" directory and moving the DLL into it, it is possible to create a new process with VBS object "Shell.Application" which does not prompt the user for any confirmation dialog. After that, a second technique called "interdimensional execution" is used. By looking for the PE header in memory, the import section can be found, and therefore the base address of kernel32.dll. With GetProcAddress emulated in JS, all necessary functions like VirtualProtect or NtContinue can be called. With this succession of steps, it is possible to create an exploit nearly entirely in JavaScript.

A practical attack against VDI solutions

Presented by Daniel Brodie & Michael Shaulov – paper – slides

The talk was primarily on attacks against VDI solutions for mobile phones (like RDP, VNC). Multiple ways of capturing keystrokes and implement screen scraping were demonstrated.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

RAVAGE - Runtime Analysis of Vulnerabilities And Generation of Exploits

Presented by Xiaoran Wang & Yoel Gluck – slides – blog article

First the speaker talked about the advantages and disadvantages of dynamic and static code analysis. The main problem with static analysis is the amount of false negatives, and with dynamic analysis the amount of false positives. He modified the Java runtime environment to perform taint analysis on application server based web applications. The results are very impressive, as more vulnerabilities have been found in several Open Source software than by other dynamic code analysis tools, while returning just 1/10 of the false positives.

Yet the current solution still needs a work to make it really usable. The main issue is the rule set, which indicates the sources and sinks, but also sanitation functions. The speaker told me after the presentation that further improvements in the GUI are coming, and that the community is expected to come up with complete rule sets.

Call to arms: a tale of the weaknesses of current client-side XSS filtering

Presented by Martin Johns, Ben Stock & Sebastian Lekies – paper – slides

Current browsers implement anti-XSS measurements on the client side, which should prohibit XSS attacks. The speakers analyzed Chrome's XSS Auditor, and made a detailed presentation about its inner workings. The algorithm Google decided to implement is somehow cumbersome, and it was easy to circumvent it in different ways. It is possible to simply hinder the XSS Auditor to start, by not using certain constructs or chars, using partial injections, trailing content or double injections. The main issue is that the XSS Auditor is implemented for speed, not for complete security. After the talk, I have seen representants of Mozilla and Microsoft siege the speakers. But their main focus was Chrome, whereas the Anti-XSS features of the other Browsers was not analyzed in detail, but could be summarized as "worse than Chrome".

Unwrapping the truth: analysis of mobile application wrapping solutions

Presented by Ron Gutierrez & Stephen Komal – slides

Here the wrapping of mobile apps of a couple of unnamed MDM solution providers has been analyzed by the speaker. He examined the difference between wrapped and unwrapped Apps in both iOS and Android, and found some interesting things. On iOS the binary was hooked with LC_LOAD_DYLIB, especially file operations to perform encrypt/decrypt of data. Also a URL scheme was added. In Android, there are a lot more imports in the DEX files, API's modified and IPC stuff added. He found that the encryption was not really based on the user's password, but just on a key stored in the file system. In another case, the password was derived with the PBKDF2 function, but no salt was used. Very interesting was the finding, that a piece of code used to store the key in a ByteArray, and then created a string object from the array. This led to a decrease in entropy because of charset encoding, as it was interpreted as UTF-8, which ignored invalid chars. Several important API calls were not wrapped, for example iOS KeyChain API. Therefore data was stored without additional encryption. At the end he had a look at the IPC mechanism, which proved to be very hard to implement correctly. The communication between the wrapped Apps and the main MDM App was often unauthenticated and unencrypted.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

DEF CON 22

Due to the multitude of talks, we will shorten the summary of the DEF CON talks. Feel free to contact us (or have a chat at an upcoming OWASP / Beer on Tuesday event) if you wish further details!

Domain Name Problems and Solutions

Presented by Paul Vixie

As first talk for DEF CON, we could attend a neat summary of the current situation and challenges posed by the Domain Name System (DNS). It represents the only true map of the current Internet and is too cheap and quick to meter and thus is open to abuses. As solutions he suggests the usage of DNS history databases such as DNSDB (primarily to be able to monitor fast-flux C&C networks) and the introduction of delays during the creation of a new DNS zone or entry. A 10 minute delay in the DNS creation would already affect spammer and malware writer in their race against the clock before being caught on blacklists. Finally, he reminded everyone operating a public DNS to implement Response rate Limiting (RRL) to avoid misusage of the server for Distributed Denial of Services (DDoS). An interesting side note is that registrars are happy about domain takedown requests, as they earn twice.

From root to SPECIAL: Pwning IBM Mainframes

Presented by Philip "Soldier of Fortran" Young – website

The target of this talk is z/OS, which is a kind of dedicated world as it's hard to get the relevant hardware. Fortunately, it's possible to learn about the platform by using RDz, a tool which runs on Linux – just ask your IBM sales for a demo version of it. After some explanations about the platform, the speaker showed us several ways to compromise a mainframe and then elevate our privileges. If FTP is available, you can upload a JCL script and by specifying a given SITE command, the file will automatically get executed on the mainframe. Privilege escalation can then be performed by e.g. exploiting setuid REXX scripts. Finally the RACF.DB file can be copied and all its passwords, stored using DES, cracked. Several resources and tools are referenced on his website.

The $env:PATH less Traveled is Full of Easy Privilege Escalation Vulns

Presented by Christopher Campbell – slides

Package managers are already common in the Linux world and are emerging on Windows platform thanks to PowerShell. OneGet or Chocolatey are two of them which got analyzed from a security perspective. Malware could be identified in some of the packages available in those repositories. This can be explained as no manual review is done on submissions. Furthermore, these tools had either insecure installation configurations (e.g. all users could overwrite binaries or drop malware in folder of the global path) or were vulnerable to some race conditions. Additionally, the download of packages was not secured with SSL/TLS.

Bypass firewalls, application white lists, secure remote desktops under 20 seconds

Presented by Zoltán Balázs - slides

The speaker presented a scenario on how to compromise a secure RDP server. His first tool allows send automatically keystrokes to a server, which allows writing any kind of text files remotely with high speed. He used this tool to type

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

automatically a VBA macro within a Word document to bypass the installed application whitelist– VBA macros being by default out of scope of AppLocker. Arbitrary execution of code was done by creating and injecting a custom DLL into Office. Privilege escalation was done over a vulnerable service binary which could be changed and overwritten by any user. Exfiltration of data over a "hardware firewall" was achieved by misusing an existing kernel driver. The presentation raised several points of incomprehension, as e.g. the definition and capabilities of the "hardware firewall" remain unclear or existing tools such as rdp2tcp were not leveraged.

[Skytalks] Civilianization of War-Paramilitarization of Cyberspace and it's Implications for Civilian Information Security Professionals

Presented by Rod Soto

Skytalks are a dedicated track at DEF CON presented in an old-school way: neither recording nor cameras are authorized and any publication should be agreed with the speaker – which I forgot to secure in this case.

Acquire current user hashes without admin privileges

Presented by Anton Sapozhnikov – GitHub

Getting the user's password on a Windows machine is nowadays trivial if you have admin privileges. But how can malware get the credential of the user who just got infected? If no privilege escalation is possible, it is still possible to attempt to phish the user via a dedicated popup box. The other option, chosen by the speaker, was to leverage the existing Security Support Provider Interfaces (SSPI) of Windows. By simulating a NTLM speaking client and server within the same process, it is possible to capture NTLM hashes which can be cracked offline by the attacker. As there are several possible authentication schemes, the attacker should use the one which is the easiest to crack. The code is available on the author's GitHub and should be soon available in Metasploit too.

Mass Scanning the Internet: Tips, Tricks, Results

Presented by Robert Graham, Paul McMillan, & Dan Tentler

The speakers shared some experiences about mass scans they run on a regular basis to e.g. assess the number of remaining vulnerable Heartbleed servers (he found that around 300'000 hosts are still vulnerable). Using masscan, it is possible to scan the entire Internet on one port in less than an hour – provided you have enough bandwidth. A one gigabit pipe is theoretically able to send 1.5 million packets each second. Practically it will be around 500'000. A cooperative ISP is also a must, as you will anyway get abuse letters. Be prepared to answer them and exclude their IP ranges of future scans. The big advantage of masscan, compared to nmap, is the scaling if you want to audit millions of hosts. It is also possible to perform IP spoofing, and therefore send the packets from a colocation and receive the answers on an Android phone. For smaller target groups, stick with nmap. The demo showed a live scan of VNC servers accessible anonymously on Internet. Some of the results are being shared on Dan Tentler's Twitter account.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Bug Bounty Programs Evolution

Presented by Nir Valtman

The speaker presented us his feedback of crowdome, a now closed startup providing secure bug bounty program, which he co-founded. Many things evolved since the first bug bounty was published by Netscape in 1995 – which did not focus on security bugs only. The current popularity of bug bounties imply increased costs for the company starting such a program: several internal teams will have an increased workload while legal and technical aspects – such as handling additional load – have also to be dealt with. His point is that outsourcing the bug bounty may have several advantages, such as a clearer legal aspect, less pressure on internal teams and the ability for the external third party to shape the traffic by using dedicated network equipment such as WAFs. He also expects more professionals coming onboard such programs, such as business analysts which may easier find workflow based security issues.

Summary of Attacks Against BIOS and Secure Boot

Presented by Yuriy Bulygin, Oleksandr Bazhaniuk , Andrew Furtak & John Loucaides – slides – BlackHat Arsenal slides dedicated to CHIPSET

The four speakers, all working for Intel, gave us additional insights into UEFI attacks. They recapitulated the history of security relevant bugs or misconfigurations, which can all be diagnosed using their toolset "chipset". This tool can e.g. be used to diagnose if CSM is active (a BIOS legacy emulation above UEFI), or if the SMI lock (preventing SPI overwrites) or SMRAM lock (allowing bypassing SecureBoot with TPM) are set. They also remembered everyone that DMA attacks are not only possible from available extension ports, but could be triggered from network or graphic cards if a vulnerable firmware is exploited. A very dense presentation (we could only read a fraction of each slide before a next topic was evoked) and good looking toolset which clearly deserves further attention.

Secure Random by Default

Presented by Dan Kaminsky

Dan made again the show during this two-session long presentation about hardware dependencies, secure pseudo random generators, Distributed Denial of Services (DDoS), the NSA and of course other stuff as well. He started by talking about his (quite expensive) research about hard drive rootkits. Each CPU embedded into this hardware trusts the others completely. He mentioned that it is possible to flash the hard disk firmware from user space, which allows code running on the disk to access all RAM over DMA. The same problem also exists in our phones, which include a myriad of components and dedicated CPUs for specific tasks. Are all these components truly secure? According to Dan, "The best things hackers break are assumptions".

A top 10 eCommerce website handles in average 7 authentication requests per second. Why do we still rely on low entropy passwords while we would have more than sufficient calculation power to make more secure (and thus expensive) computation? Dan mentioned as another example of poor entropy Dominique Bongard's closing talk held at Passwords14, which ripped apart WPS implementations. According to Dan, the information security community spends a lot of time talking about the security SHA1 while in the field no (or only poor) crypto is engaged in many cases. Usually security does not fail because of insecure algorithms, but because of insecure random number generation. One of his current projects is to enhance the usage of passwords for end user, providing a way to use passphrases with

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

higher entropy while keeping their usage for the end user easy (or even entertaining).

Another topic of Dan is the current state of security in browsers. He acknowledged the incremental security enhancements made within Chrome and Internet Explorer, citing as example Microsoft's work to break various links in the chain of browser exploitation and eventually affecting the reliability of the final exploits. Only Firefox seems to be unable to implement security in their browser. He also mentioned that he will buy redirection attacks affecting Safari as finally Apple acknowledged that automatically redirecting a user to his AppStore if a mobile app is available was perhaps not a good idea.

His figures about DDoS were also impressive – while in 2013, only one attack had a bandwidth of more than 100 Gbps, this number increased alone this year to 114 attacks. The traffic from these attacks is not coming from botnets, but misconfigured DNS and NTP servers. He therefore urges all sysadmins to ensure their configurations are safe and enable RRD on authorative DNS servers. If nothing is done in the near future, Dan fears that such attacks will be able to disconnect entire regions or even countries from Internet. Finally, Dan makes the statement that we don't need the NSA to subvert cryptography; we as an industry are good enough to screw it up on a regular basis. He concludes about ECC P-curves, which should for him be considered as broken, and suggests using only the K-curves.

Abusing Software Defined Networks

Presented by Gregory Pickett – slides

The introduction of what Software Defined Networks (SDN) is mainly focused on the separation between the control and the data plan, which are now processed by two different entities: the data plan is handled by a commodity switch while the control plan is processed by a controller. His analyze focused on OpenFlow, one of the many SDN protocols. This protocol is supported in several implementations and the speaker had a look at two open source projects: Day Light and Flood Light. While the initial version 1.0 OpenFlow protocol specifications were quite secure – e.g. requiring a TLS channel for the switch-controller communication, requirements has been relaxed in version 1.1. A full support for TLS in the switches, controllers and in the implementation is rare and the security of the implementations are a concern. Using his SDN-Toolkit, he made an impressive demo where he enumerated SDN components and then exploited weaknesses in the web administration console of one of the implementation. By connecting to tcp/6633 or tcp/6653, he was able to anonymously trigger a Xml External Entity weakness in the application running as root. Using these privileges, he then reconfigured the whole network to his desires. Summarized, the SDN software is mostly unauthenticated, unencrypted and contains remote code execution vulnerabilities. The speaker also hinted that once these web weaknesses are fixed, the attacks may switch to e.g. the switch's debug port.

Getting Windows to Play with Itself: A Hacker's Guide to Windows API Abuse

Presented by Brady Bloxham – slides – Throwback on GitHub

While Metasploit is a great tool for pentesters, the speaker suggests that the information security community needs more than one tool for post-exploitation purposes. The main issues with metasploit and meterpreter are that they are widely known, and are quite extensive in size. He therefore developed a new tool named Throwback, which uses similar technics as current malware to gain and keep a foothold in a network. The tool is composed of a Windows client

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

developed in Python, and of a command-and-control server developed in PHP, all available on GitHub.

Old Skewl Hacking: Porn Free!

Presented by Major Malfunction

This last talk of day 2 of DEF CON was about MHEG, also known as ISO standard 13522-5. The initial idea was to provide a teletext-like interface for information and added value content for the television, referred as "Red button" in the UK. The implementation is based on ASN1 encoded programs streamed aside the TV signal and executed by the TV itself. Despite this and having no native cryptographic capabilities, this format got used in the UK to provide pay-per-view adult entertainment. The speaker first demonstrated how it was possible to capture such TV streams on a Linux computer using a humax or a TV dongle. After some manipulation of the TV client, he was able to hook the string comparison method, thus dumping to the console the expected PIN for a given challenge. Another manipulation of the client consisted of simply disabling the lock screen, thus allowing directly viewing the TV feed.

Weaponizing Your Pets: The War Kitteh and the Denial of Service Dog

Presented by Gene Bransfield – video

Very entertaining talk on how the speaker (mis-) used a cat and a dog as electronic scouts. While the cat was equipped for war-driving the surroundings, the dog was setup to act as a denial of service dog by turning off TVs in the area and broadcast with Karma a free WiFi access point which would rick-roll anyone who connected to it. The lessons are that pets, especially cats are very hard to work with. A second is that with miniaturization and open source components, you can achieve quite a few things, such as fit all equipment in a cat's collar.

[Wall of Sheep] Abusing Microsoft Kerberos: Sorry You Guys Don't Get It (Black Hat Encore Talk)

Presented by Alva Duckwall and Benjamin Delpy - slides

The speakers presented their Black Hat talk, with a new feature coded by Benjamin Delpy the night before: it is now possible to set the validity timeframe of a golden ticket via command line instead of having to edit the source code.

NSA Playset : GSM Sniffing

Presented by Pierce & Loki – slides

The speakers first presented a good recapitulation about the possibilities offered nowadays by Software Defined Radio as well as a history of attacks against the GSM A5 protocol. While A5/3 is seen as secure, it's seldom if ever seen deployed in the wild. The website gsmmap.org is referencing such implementations. The point of the speakers is that nothing will change in the GSM security unless existing attacks get broadly known. They aim is therefore to create a framework – called NSA Playset – which a 10 year old kid should be able to use to carry out such attacks. The authors released an initial version of their

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona
T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

project, which takes the form of a custom Kali installed on a 16GB USB 3.0 key.

Playing with Car Firmware or How to Brick your Car

Presented by Paul Such 0x222 & Agix – slides

Paul, founder SCRT - our Swiss colleagues based on Lausanne – first presented how to get hold of the firmware of his daily car. While you might be lucky using Google, he found an update with the GPS upgrade shipped per CD-Rom. The analyzed image is a UNIX file system and Paul was able to browse files such as /etc/passwd, which contained the personal accounts (and salted passwords…) of various VW engineering and subcontractors who obviously engineered the system. The hosts file also contained several internal entries a company may not want to leak out. It also seemed that the firmware contained all the features for higher class models, and that those we just disabled via a software flag. Once analyzed, Paul made a few changes to the firmware and applied them to his car. For a yet unknown reason, one of these changes broke some integrity check and basically broke all the multimedia and other options (e.g. door lightning or seat heating) of his car. It was only after the replacement of the hard drive – located in the hand glow compartment – that these features worked again.

[Skytalk] SQL-Gestalt: A MS-SQL Rootkit Framework

Presented by Rob "whitey" Beck" – talk announcement

While officially no recording or camera is allowed in Skytalks, the speaker gave me his approval to transcript the content of his presentation. His talk is all about post-exploitation technics to keep a foothold in a network once the initial penetration succeeded. While rootkits on operating systems are well documented, his approach was to target the database server - Microsoft' SQL Server in this case. Some of the presented technics will leave no file on the file system, as the payload will be stored within the database itself. Xp_commandshell is far from the only feature to audit or look at – code can be kept in (extended) stored procedures, assemblies and within the SQL Server Agent. OLE automation provides a convenient shell to execute various types of script – not only wscript. While extended stored procedure will have to reside on disk as a dll, .NET assemblies are stored entirely in the database. Calls to unsafe or external methods will require the trustworthy flag to be enabled on the database, or a valid code signing certificate. The job part of the SQL agent can be misused to execute any kind of operations, including arbitrary OS commands and PowerShell scripts. The presentation was concluded by a demo of a rootkit which had 3 points of persistence: in the agent, in assemblies and within an extended stored procedure. The sources of the tool should be released soon.

Elevator Hacking - From the Pit to the Penthouse

Presented by Deviant Ollam & Howard Payne – slides

If you think physical security can be achieved by leveraging elevators, this talk is likely to be mind-blowing. The speakers admirably demonstrated why elevators and badge controls implemented in elevators are a weak link in physical security – while they are great at safety. Two types of calls exist for lifts: hall-calls are emitted when you order a lift while car-calls are details about a ride, once in the cabin (e.g. "I want to go to floor 7"). A cabin can be turned into independent service mode, which then ignores all the hall calls. In this mode, you have to provide each command to the elevator, such as "open door", "close door",

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

"move 1 level up" etc. This mode can (at least in the US elevators) be triggered from within the lift and is a perfect hide out for an attacker waiting for offices to empty themselves before accessing the desired floor. Other modes also exist, such as the VIP call (car is dedicated to the VIP until released), the firefighter or the inspector mode – which are the two most powerful roles in use. The switches to activate all these commands are within the elevators. While access to these controls is mostly protected by a key, this doesn't guarantee anything. In this review of US based lifts, several shown examples had either no key at all, or easily lockpick-able keys. When the lock is of good manufacture, it's biting is the same across the same vendor or, for privileged keys such as for firefighters, it's the same across the US state you're in. The only requirement to gain access to these controls and bypass any physical security mechanism (e.g. badge reader in the car) is to get the matching key. Here again, the speakers showed us that while the design of several emergency keys is protected by law, the same law provides the biting code! In other cases, the information is either leaked by documentation, buying the key is allowed for the general public or at least buying the cylinder is unrestricted. Cloning such keys is therefore trivial and the only recommendations provided by the authors are to ensure you don't rely on elevators for physical security – and ensure you log what happens in your lifts.

DEF CON Closing Ceremonies

It's amazing how quickly time flies – it's has been 6 intense days of conferences here in Las Vegas. This edition is also the last to be held in the Rio: from next year on, DEF CON moves to the Paris and Bally – as the growth in popularity requires two casinos to host all the participants. Book your hotel accordingly for 2015!

Conclusion

It was a pleasure to attend these different conference, each with its atmosphere and focus. This diversity is all packed into a single (busy) week, which definitely makes the travel to Las Vegas a must at least once for any security professional.

About the Authors

Alexandre Herzog, CTO at Compass Security Schweiz AG

Alexandre Herzog started his career in Information Technology in 1998 as an IT system administrator in the largest trading room in the Geneva region. Between 2004 and 2007 he attended the University of Applied Sciences Western Switzerland in Sierre. During his studies in computer science and business he co-founded the start-up BananaSecurity.com together with four other students. The company is still active today under the name of KeyLemon.com. In 2008 Alexandre moved to New Zealand and was hired as a Development Consultant. He essentially worked on a Microsoft based technology stack as a contractor for the fastest growing bank of the country. Aside from development tasks and second/third level support for the Internet Banking solution, he acted as an internal security expert. He was also heavily involved in the setup and deployment of a fully rewritten version of the Internet Banking solution based on the latest available Microsoft technologies.

After two years down under Alexandre Herzog returned to Switzerland in 2010 and started working as an IT security analyst for Compass Security AG in Rapperswil-Jona. His predilections in terms of fields of expertise mainly include Microsoft based technologies, from the operating system up to the C# code of (ASP).NET solutions.

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch

Alexandre is also interested in Web Security in general and is the author of several security advisories concerning products from, e.g., Microsoft to SAP and AdNovum.

Alexandre Herzog, now CTO of Compass Security, recently finished his MAS studies in Information Security at the University of Applied Sciences of Lucerne. His master thesis consisted of an analysis of cryptographic mechanisms in Windows and .NET.

Dobin Rutishauser, IT Security Analyst at Compass Security Schweiz AG

Dobin Rutishauser finishes his Bachelor in Computer Science in 2010 at the Zurich University of Applied Sciences/ZHAW. In 2011 he joined Compass Security AG as Security Analyst. His interests include web application security, network protocols, Unix systems and exploit development.

About Compass Security Schweiz AG

Compass Security Schweiz AG is a Swiss enterprise, based in Jona SG, which specializes in security assessments in the field of information technologies. The company has been established in 1999 by Walter Sprenger and Ivan Bütler and has grown to over 20 employees since then.

Meanwhile, Compass Security continuously improved and nowadays offers comprehensive services in the field of Computer- and Network-Security. Amongst others, these services cover Penetration-Tests, Web-Application-Tests, Security Reviews and Computer Forensics. Moreover, Compass Security offers several trainings in the mentioned areas.

More information at http://www.csnc.ch

Compass Security Schweiz AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

T +41 55 214 41 60
F +41 55 214 41 61
team@csnc.ch
www.csnc.ch