Compass Security 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
Black Hat USA 2013

Document Name:	blackhat_2013_v1.0.docx
Version:	v1.0
Authors:	Sascha Herzog, Compass Security AG
	Thomas Roethlisberger, Compass Security AG
Date of Delivery:	27. August 2013
Classification:	PUBLIC

Introduction

Black Hat USA is the most famous conference for IT security professionals and hackers around the globe. The highly skilled speakers provide insights into their ongoing research and release their brand new tools. Of course, the spectacular location at Caesars Palace in Las Vegas contributes to the popularity of this conference as well. This year's event was particularly special for us because Cyrill Brunschwiler, CTO of Compass Security and passionate penetration tester, was honored to contribute his own talk about the security of the upcoming wireless metering protocol. Thomas Röthlisberger and Sascha Herzog, IT Security Analysts and penetration testers of Compass Security, accompanied his journey and, as the authors of this paper, report about the newest trends and their conclusion of the Black Hat USA 2013.

On one hand, this year's talks did not necessarily reveal revolutionary topics or many new vulnerabilities. Especially in well-known areas like web security, the conference leaves the feeling that we kind of reached the zenith. On the other hand, the known attacks are enhanced with new creative exploiting techniques and helpful tools, which penetration testers will love. Furthermore, topics like hardware hacking and digital forensics have been very popular this year.

Keynote – NSA Director

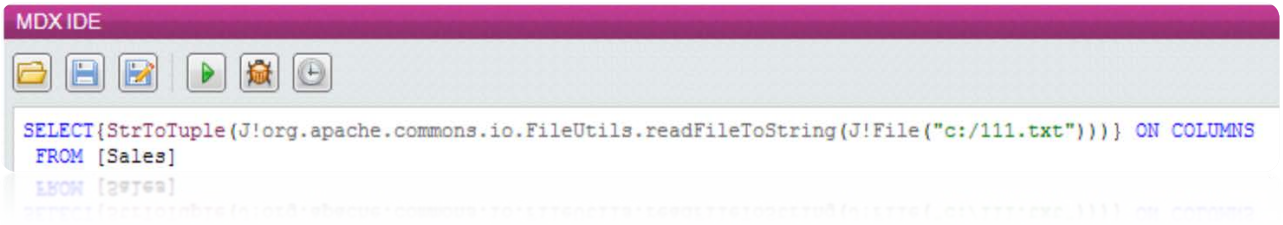
Presented by: Gen. Alexander

General Alexander was facing the skeptical crowd of hackers, knowing that this audience is probably not a big fan of the NSA surveillance program PRISM.

This man tried to persuade the audience that there is no such thing as a US based mass surveillance and instead highlighted the positive aspects of the program, which was involved in half of the 54 successfully prevented terror attacks since its introduction. The general as a speaker was surprisingly very charismatic, authentic and even did some jokes on the stage. However, it was obvious that not everybody in the audience believed him ;)

Compass Security 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

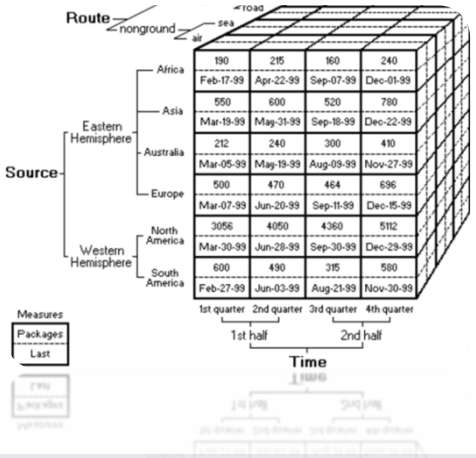


Big Data – Exploiting of MDX Injection

Presented by: D. Chastuhin, A. Bolshev

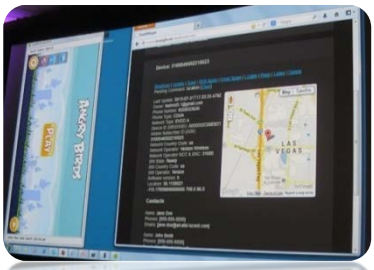
After a quick explanation of the differences between traditional SQL queries on Online Transaction Processing (OLTP) databases and multi-dimensional MDX queries on Online Analytical Processing (OLAP) warehouses, Dmitry and Alexander jumped right into a series of live hacking demos. The audience was challenged to follow a rapid sequence of several exploiting techniques already known from other web based attacks, but now shown in the context of MDX. They showed that finding the vulnerability is often not the challenge. Not surprisingly, several data warehouse products have been developed without a sense for security. "It feels like web application security back in 2000" they said. More exciting is the way they exploited it. Besides reading arbitrary data, they used external functions to call Java methods, which allow exporting files from the file system. Finally they compromised the server because of an OS command injection vulnerability in one of the Java libraries on the server.

MDX as well makes use of XML as a data transfer standard called XML for Analysis (XMLA) also known as mdXML. The speakers showed that this allows the same famous xml-based attacks, like XML External Entity (XXE), we all love. Last but not least some of the data warehouse products even provide web interfaces that are prone to Cross-Site Scripting (XXS) attacks via MDX queries. However, it was good to hear that Microsoft's answer to data warehousing, the Microsoft SQL Server Analysis Services (SSAS) does not allow using external functions since version 2003 SP1 and does not provide an error prone web interface like it seems to be the case with many other products.



How to Build a SpyPhone

Presented by:
K. McNamee



Interesting, but not ground breaking – He showed that android phones do not have a robust certificate check in place, concerning third party apps (apks not from Google PlayStore). This allows the following:

- Change any valid APK (here AngryBirds) and integrate the Trojan
- SelfSign the new APK via Jarsigner
- Deploy on the phone via webpage or physical access

As a PoC they developed DroidWhisper a Trojan that is able to read any information from the phone (phone book, SMS, data, GPS coordinates, etc.), can listen to phone calls and taps the microphone and video camera.

Compass Security 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

Million Browser Botnet

Presented by: J. Grossman, M. Johansen

With HTML5 a lot of new powerful features have been introduced to modern web browsers. The research of Michael Schmidt, the presentation of Thomas Röthlisberger at the Swiss IT security conference "Swiss Cyber Storm 3" in 2011 and several Black Hat talks of previous years already showed that these new features introduce several new threats as well.

Jeremiah and Matt impressively demonstrated a powerful Denial-of-Service attack using millions of hijacked browsers. To achieve this, they used the new HTML5 Web Workers feature to run asynchronous JavaScript code, which opens hundreds of connections in the background to attack the target server. But the real clue of this attack was the way they distributed the malicious code. They managed to bypass the validation stage of advertising networks easily and were able to embed any malicious JavaScript in their Ad. This Ad, and of course the malicious JavaScript code, was then automatically hosted on several trustful web sites, infecting hundreds of innocent visitors.

They even found a way to bypass the maximum connection limit on Firefox by using the FTP protocol handler instead of HTTP. But the origin attack was so successful that they not even had to pull this trigger. The test apache servers have already gone down immediately by the normal attack, which by the way did not make use of any vulnerabilities in any of the browsers. It purely uses the power of the W3C compliant HTML5 behavior of modern browsers. "The web is supposed to work like that" they said.

- Compass Security "HTML5 Web Security"
  Video:
  www.youtube.com/watch?v=Eju4e5mhEN0
  Slides:
  http://www.jug.ch/events/slides/130528_HTML5_v1.1_handout.pdf
  Paper:
  http://media.hacking-lab.com/hlnews/HTML5_Web_Security_v1.0.pdf

Maltego Tungsten as a collaborative attack platform

Presented by: R. Temmingh, A. MacPherson

Cool presentation. New Maltego editions with new capabilities. Maltego TUNGSTEN can be used to conduct reconnaissance with Maltego in a collaborative way (chatting, task execution on other systems, etc.), involving many team members. Maltego Teeth is a weaponized Maltego, including tools as sqlmap, metasploit framework and nessus.

- Maltego Blog & Tool:
  http://maltego.blogspot.de/2013/08/vegas-feedback-tungsten-release-teeth.html

Compass Security 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

Energy Fraud & Orchestrated Blackouts

Issues with Wireless Metering Protocols (wM-Bus)
Presented by: Cyrill Brunschwiler
CTO of Compass Security AG

For many in the audience this was probably one of the new topics. However, the wireless M-Bus protocol got Cyrill's attention very early. He started his master thesis in autumn 2012 and soon realized that the security of M-Bus is insufficient. The BSI came to the same conclusion in March 2013.

After explaining the basics of Smart Metering with its main components Meter, Relay and Collector, he explained what the wireless M-Bus protocol was designed for. The fact that the protocol is not only used for reading meter values, but as well allows to make configuration changes on a device and send control instructions like "open / close valve" certainly gained the crowd's attention. He explained that on the Application Layer (prEN 13757-3), none of the specified encryption modes 1 – 5 is sufficient to prevent meter readings from being eavesdropped in any circumstance. Furthermore, because the protocol in general lacks of integrity protection, he was able to demonstrate that the payload can be manipulated by an adversary acting as a malicious Collector. He showed live how he sends valid commands to the vulnerable meter and so changed the name of the meter. Conceptually it would even be possible to open or close a valve.

- Compass Security "Wireless M-Bus Security" Blog:
  http://blog.csnc.ch/2013/06/compass-crew-member-speaking-at-black-hat-usa/
  Slides:
  http://www.csnc.ch/misc/files/2013/energy_fraud_and_blackouts.pdf

Breaking Home Security Systems

Presented by: D. Porter, S. Smith

This talk was not related to IT at all, but it was good old hardware fun. Drew and Stephen showed several ways to bypass common sensors of Home Security Systems. E.g. they used a large magnet to prevent the switch from closing the circuit in case someone opens a door or they used a lighter to "blind" the IR sensors which are supposed to detect the bad guy moving around your house.

Compass Security 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

Pass-The-Hash 2: The Admin's Revenge

Presented by: A. Duckwall, C. Campbell

As a sequel to their PTH talk on last year's Black Hat, Alva and Chris explained that the specific PTH attack isn't Microsoft's main problem. In fact Microsoft always had several credential management issues.

Windows excessively caches credentials in memory for later use in all forms of single-sign-on scenarios. "Because you know, they could be used... sometime... somewhere... somehow... maybe?" the speakers were joking. (Un)fortunately, these credentials are easy to recover in plain text. Thanks to Benjamin Delpy and his tool Mimikatz this is an easy task today. Then of course there are the local account hashes stored in the SAM (Security Account Manager). The bottom line is, that if an attacker has SYSTEM privileges on your server, it is only a matter of time he as well has compromised your domain controller.

In the meantime, with Group Policy Preference Settings, a new feature introduced with Windows Server 2008 to deploy local accounts on every workstation of a domain, Microsoft made it even worse. The speakers demonstrated how easy it is to recover such local account passwords, if they are pushed to the machines using GPP. Since the last Black Hat talk in 2012 they also released a pass-the-hash toolkit for Linux, which is very useful for penetration testers if they do not want to use native Windows tools like WCE to perform pass-the-hash attacks.

Windows System Administrators might wonder how they can fix that? Alva and Chris also explained that there is no easy solution for these problems. E.g. there is no patch that can be applied. It is more about a clever and restrictive server administration strategy where you try to minimize the amount of Domain Administrators in your network and don't use dangerous features like GPP.

- PTH Toolkit: http://passing-the-hash.blogspot.ch/
- CSNC Blog about GPP: http://blog.csnc.ch/2012/04/exploit-credentials-stored-in-windows-group-policy-preferences/
- Tool – Mimikatz: http://blog.gentilkiwi.com/mimikatz
- CSNC Blog about Mimikatz: http://blog.csnc.ch/2012/11/asfws-mimikatz/
- Tool – WCE: http://www.ampliasecurity.com/research/windows-credentials-editor/

Malicious iOS Charger

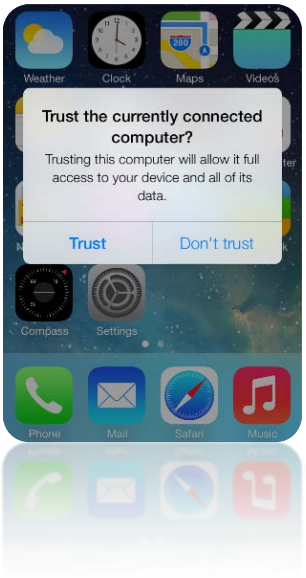
Presented by: B. Lau, Y. Jang, C. Song

Three researchers of the Georgia Institute of Technology held a presentation with the very promising title "Injecting Malware into iOS Devices via Malicious Chargers". Unfortunately, mobile device and iOS security specialists in the audience have been disillusioned by the fact that as a precondition for the attack, the passcode of the iPhone / iPad needs to be entered at least once while the malicious charger is attached to the device.

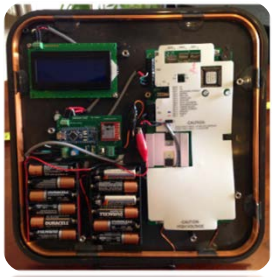
Compass Security AG
Werkstrasse 20
Postfach 2038
CH-8645 Jona

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

On one hand, having an USB connection established on an unlocked iOS device means that you completely own the device. You can steal data from the device using the backup feature or just Jailbreak it. On the other hand, they showed that a successful attack does not always need rocket-science-break-thru-technology. Inspired by the fact that the common mobile device user anyway enters the passcode to read incoming messages or browse the internet, while the device is charging (e.g. on a nice public charging station), they engineered a little charging device, which in fact is a little computer, plugged in to your iOS device. The charger first establishes the USB connection to the device (pairing) and second installs a provisioning profile for app developers. This finally allows installing a malicious app on the device, without having the device jailbreaked. This is not necessary, because the app is correctly signed by the provisioning profile. The victim does not notice anything, because the iOS does not show any message to the user throughout the whole process. Furthermore, the app can be hidden by using apple's built in functionality. Once more, this is an attack based on default functionality rather than using a new vulnerability.



Good to see is that apple seems to be aware of this problem, because they already mitigated this issue in iOS 7 BETA2 by prompting the user to decide if he trusts the connected device or not.



RFID Hacking: Live Free or RFID Hard

Presented by: F. Brown

This was not much about learning the technical details about RFID hacking. It was more a systematic approach for penetration testers on how to get into a RFID protected building.

Francis Brown explained the procedure in three main steps. First, you need to extract and steal the card data from an employee of your target company. Second, you need to clone the card. And finally you need to walk into the building. Sounds simple, right? The talk mainly addressed problem number one. Francis showed the audience how he solved the challenge by building a long range RFID scanner to steal the information from approximately three feet distance. Up to now, others usually recommended using a normal antenna and grabbing the information directly from someone else's back pocket (also known as "A$$ GRABBING").

But the chance is bigger to end up in jail for sexual harassment instead of really picking up the card data. Therefore, Francis' long range scanner is built out of a long range antenna from one of the well-known vendors and a custom PCB board to extract and store the data on a SD card. All the information how to build such an "extraction device" and the Fritzing-Files for the PCB board is now publicly available: http://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/.

Compass Security 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

About the Authors

Sascha Herzog, IT Security Analyst at Compass Security Deutschland GmbH.

Sascha Herzog worked for various companies in the development sector and performed penetration tests at financial service providers and in the hotel industry. As from 2008, Sascha Herzog worked as a security consultant for atsec information security GmbH in Munich exclusively in the penetration testing area and conducted assessments and ethical hacking workshops for governmental institutions, banks, the military and telecommunication providers in Europe and the USA. Since June 2010 Sascha Herzog has been working as Security Analyst for Compass Security (since 01.01.2013 with Compass Security Deutschland GmbH).

Thomas Röthlisberger, IT Security Analyst at Compass Security AG.

Thomas Röthlisberger started work as an IT Security Analyst for Compass Security AG in January 2010. Before that he was working as a .NET Software Engineer for 4 years. He first began in 2006 with Swisscom IT Services AG where he developed web applications in the field of resource management and SOX certification. After that he was working for 3 years at UBS AG where he was responsible for the analysis, design and implementation of middleware and web applications for the processing of SWIFT- and XML-messages in the Global Asset Management. Thus he was able to gain wide specialist knowledge in the banking sector. Additionally, as a software engineer, he was in charge of the design and the further development of the MS SQL databases. In early 2006, Thomas Röthlisberger completed his IT studies at the University of Applied Sciences in Rapperswil with majors in "Internet communication and applications" and "information systems".

About Compass Security AG

Compass Security Network Computing 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 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

References

- Image Credits: http://www.flickr.com/photos/blackhatevents/sets/72157634860935639/
- Black Hat USA 2013: http://www.blackhat.com/us-13/
- Compass Security Website: http://www.csnc.ch
- Compass Security Blog: http://blog.csnc.ch/

Compass Security 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