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 2012
November 16th, 2012

Document Name:	blackhat_2012_paper_v1.0.docx
Version:	v1.0
Author(s):	Riccardo Trombini, Compass Security AG
	Martin Loher, Compass Security AG
Date of Delivery:	November 16th, 2012
Classification:	PUBLIC

Introduction

Black Hat USA in Las Vegas is one of the biggest IT security conferences in the world. Every year, thousands of security-interested people attend the conference that is held in the infamous Caesars Palace, the heart of Las Vegas. And as every year, two security analysts of Compass have participated the conference to learn about the latest trends in IT security. Black Hat easily combines the transfer of the latest top-class security know-how and networking among the attendees with a social frame around the conference. The sponsored Rapid7 Party in the Palms Hotel is just one example, how to combine "work" with pleasure. The Defcon conference takes place right after Black Hat and focuses more on the "geeky" audience.

This paper summarizes some of the most interesting talks we've attended during these five days (Black Hat and Defcon). We encourage you not only to read this summary but also to go online and take a closer look at the videos or the slides.

Abstract

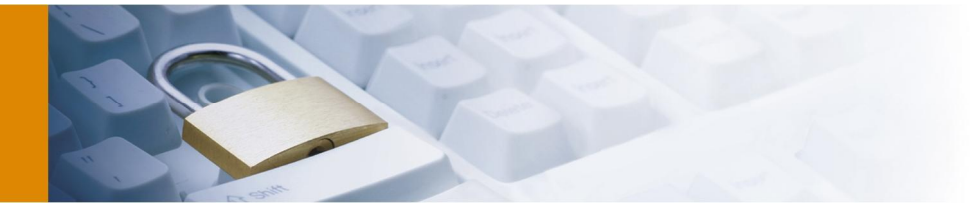
In our daily work, we register a rising interest in mobile technologies such as iOS or Android App reviews. And similar to our experience, the Black Hat schedules focus more and more on mobile technologies. Another topic, which is currently hyped, is Near Field Communication. A lot of research is going on in this area, especially since the number of NFC payments is increasing more and more. Besides focusing on mobile technologies, Black Hat is also getting more into the topic of defending the own network, which is highly related to knowing your enemy and knowing his targets. Besides these technical talks, Defcon always has some funny, off-topic talks in its schedule.

Advanced Software Exploitation on ARM Microprocessors by Stephen Ridley & Stephen Lawler

This talk gained our interest because our work with the iOS platform and the application reviews we are doing every day. Analyzing code on the assembler level gets more and more relevant as the developers won't provide us with the source code of their binaries. In this talk, Stephen and Stephen share their experience of developing the "Practical ARM Exploitation" training that was also given at the Black Hat 2012 and all the obstacles they had to overcome. The training focused on teaching how to reverse engineer ARM binaries and some techniques to exploit buffer overflows. A really cool detail besides the topic itself is the hardware platform they used in the training to develop and teach exploiting. The Gumstix are basically a low powered PCs with an ARM chip. This little stick contains the complete tool chain you need to develop the exploits and solve the exercises. I am really looking forward to order one of these and play around. The rest of the talk was a detailed discourse about different exploiting techniques.

Probing Mobile Operator Networks by Collin Mulliner

Collin Mulliner's talk was about scanning the Mobile Operator Networks for other clients and the results he gathered over time. Already in the past, Collin highlighted the risk of running jailbroken iPhones with the default SSH password in his blog, what would later be exploited by the Ikee.A/B worm. Based on this experience, Collin continued scanning the Mobile Operator Networks to disclose if other devices exist with security implications. Simply connecting to the network via a 3G modem and start scanning turned out to be no valid option. He experienced various problems like inter-client connectivity,



slow connections, different operators and other problems. Consequently, he had to completely overthink his approach. He began searching for mobile networks in public databases like RIPE. It helped that some operators label their networks with its use like "GPRS". After some research he had enough IP address ranges to start scanning with a custom Python script that simply probed TCP connect's on various services. The rest of the talk was all about the results and statistics what services he found. Some of the more interesting devices were: GPS tracking devices returning coordinates, devices for power system automation, smart meters and surveillance cams.

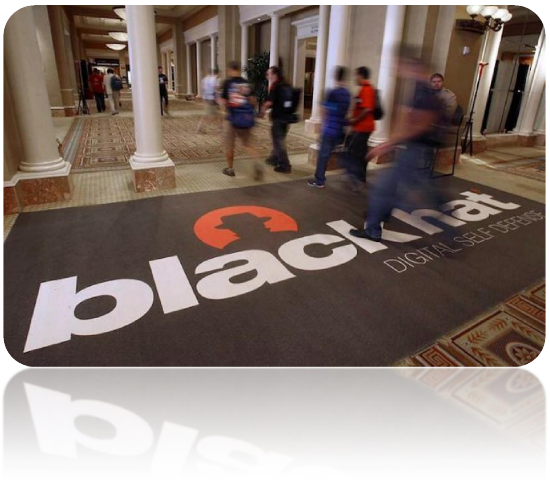
Don't Stand So Close To Me: An Analysis of the NFC Attack Surface by Charlie Miller

Since my first glimpse on the Black Hat 2012 schedule, it was clear that we had to attend this talk. NFC gets more and more into our focus and earned our interest. Security related issues in the protocol or the implementation would have a huge impact and will raise high waves among the general public. In fact, we currently register a rising interest of local medias in this topic.

After some introduction about NFC, Charlie dives right into fuzzing the NFC stack on Android smartphones. The most difficult part of the fuzzing was to present his fuzzed data to the smartphone. He put some real effort in finding the best solution. Finally, he found a way to emulate a card or a tag that responded with his fuzzed data while on the phone, the NFC service has to be restarted for every new test case. Charlie highlighted some crashes he provoked, but did not focused too much on the low-level results. Instead he continued showing off issues he disclosed on higher-level apps, which he called the most exciting part of his research. One thing that really got me thinking was the possibility to open a browser on the phone without the users interaction. As a matter of fact, the proof of concept Charlie and his team showed was an exploit where you end up getting an interactive shell on the device, simply by touching the phone with a manipulated NFC tag. Pretty amazing.

NFC Hacking: The Easy Way by Eddie Lee

Unlike Charlie Miller's talk, Eddie Lee focused more deeply on analyzing the protocol between NFC cards and payment terminals. To support his work he started implementing an NFC proxy, which is the main topic of his talk. The proxy is designed to help with protocol analysis by providing a proxy for the communication between RFID tag and a reader. The software runs on two Android phones that built up a TCP connection among each other. The NFC data is simply forwarded from one phone to the other, which does emulate the card or terminal. While in transmission, the data can be analyzed or even manipulated to test how the terminal reacts. Pretty simple approach, nevertheless it is a great idea and I can imagine using it in the future by myself.

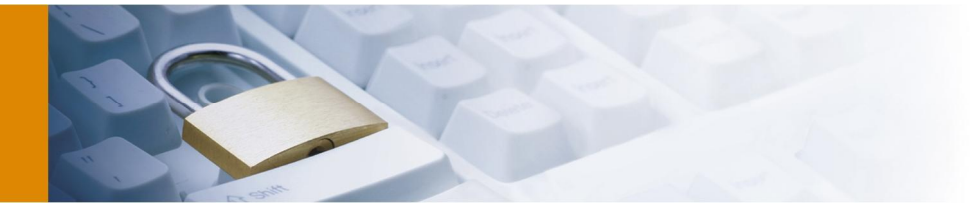


KinectasploitV2: Kinect Meets 20 Security Tools by Jeff Bryner

From a security perspective, there is really not much to say about this talk, except that it may be the coolest thing pentesting has ever seen. Kinectasploit is basically a mashup of popular pentest tools like Nmap, Metasploit and a 3D first person shooter game environment. The best way to think about Kinectasploit is for sure Tom Cruise in Minority Report. You can control supported tools with simple gestures while standing in front of Microsoft's Kinect controller. It brings the fun back into routine scanning work and I am still trying to free up some time to set up Kinectasploit.

Mac EFI Rootkits by Loukas K

This Talk sounded really interesting in the booklet but also very technical. We weren't disappointed. Loukas K had a closer look the EFI (Extensible



Firmware Interface), which is basically the successor of the BIOS. Since Apple introduced Intel chips in its computers, they run an EFI. Because there are development kits available and the interfaces are publicly known, malware authors have a new playground. Loukas showed different sorts of malware, which could be placed inside the EFI. One example is a keystroke logging software. Because Apple's Whole-Disk Encryption File Vault takes place in the EFI-pre-boot environment, it is possible to sniff the keystrokes using a manipulated driver. As a highlight of the talk, Loukas showed how to deploy malware onto the computers. PCI devices, such as the newly introduced Thunderbolt-to-Ethernet adapter, contain a PCI expansion ROM that can store drivers on them. In this example he deployed a malware onto this adapter. By booting the system with the adapter plugged in, the MacBook got automatically infected. This looks like an interesting attack in an environment, where a lot of Apple devices are used. The attacker only has to "lose" his adapter and wait until a victim plugs it into his computer.

Off Grid Communications with Android – Meshing the Mobile World by Josh Thomas and Jeff Robble

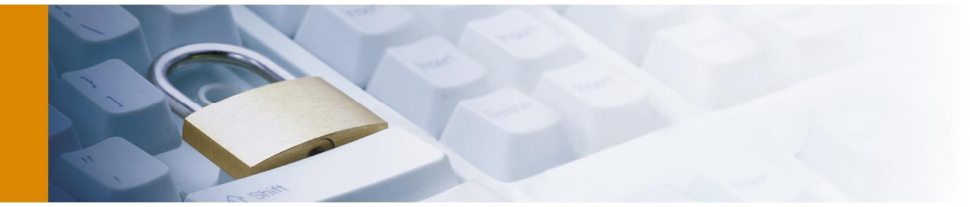
In case of natural disasters or political events, mobile networks tend to fail in case of breakdowns or censorship by authorities. Thus, it is important to introduce a backup network to keep communication up and running, while ideally operating headless (no single point of failure) between independent mobile clients. In their talk, Josh Thimas and Jeff Robble share the work they put into a framework called SPAN that replaces the network stack of a smartphone to setup a mesh among mobile clients, without touching the upper layers. As a result, developers of third-party apps don't have to touch their code to support the framework. The framework currently runs on the Android OS. Problems they had to solve are pretty complex: Routing traffic among mobile clients, power limitations of devices, tunneling traffic through other networks.

SexyDefense - Maximizing the Home-field Advantage by Iftach Ian Amit

The keynote of Shawn Henry, former FBI Executive Assistant Director, and the talk of Iftach Ian Amit had a lot in common. They both talked about the threats our networks face everyday. One of the main statements was that we have to get to know the adversary and what assets are at risk. A company should specifically protect these goods. If the target is known and the adversary is identified, the defender is able to find tools, which are used by the attacker and specifically protect against these attacks. Traps can be put in the network to mislead the attacker and think, that the attack was successful. What we also have to be aware of is that there is no 100% protection. Successful attacks happen and there is nothing you can do about it. The point is what you do about it. People have to be trained how to react in case something happened.

Intrusion Detection Along the Kill Chain: Why Your Detection System Sucks and What to do About It by John Flynn

John Flynn is a Security Engineer at Facebook with a special interest in Intrusion Detection. In his talk, he described some very interesting ideas about the topic of IDS systems. He found out that of all the attacks against larger organizations, only about 5% are detected by fraud detection systems. Third parties detect most of the frauds. Possible explanations for this phenomenon are thresholds, which are set by system administrators. Nobody wants to be woken up at night by a triggered alarm, only to see, that automated scans are ongoing. (These people wouldn't get any sleep anymore). The talk then introduced a workflow, which could be used to get more reliable results instead of setting any thresholds. The new concept is based on the fact that intrusion events are not binary. Several events are correlated along the different steps of a successful attack. This correlation of the events



allows the system to get a better understanding about these events and a more reliable statement if an attacks is ongoing or not.

Introducing: SIRA Semi-automated iOS Rapid Assessment by Justin Engler, Seth Law, Joshua Dubik & David Vo

As a result of several security reviews of iOS application Justin Engler, Seth Law, Joshua Dubik and David Vo felt the need of a framework, to provide the automation of repeating steps of iOS application reviews. The result of this is a framework called SiRA (Semi-automated iOS Rapid Assessment). The framework can be installed on any Backtrack system. In combination with a jailbroken iPhone that is connected via SSH the analyst is now able to perform several steps of an app review in an automated way. This includes the download of the app from the App Store, decrypting the app, taking snapshots of the underlying iOS file system, taking screenshots as well as an export of the Keychain. The snapshots can be analyzed automatically for stored credentials or any other sensitive data. Although the tool is available in a very early version and has still some bugs, it is a good starting point for the review of an app.

Hacking Humanity: Human Augmentation and You by Christian 'Quaddi' Dameff and Jeff 'r3plicant' Tully

In this talk the two students Christian Dameff and Jeff Tully talked about hacking the human body. The talk sounded very futuristic. However, body-hacking is already part of our everyday normal life. There are already prostheses, which help disabled people to walk again. Swallowing pills can boost concentration. So the talk focused on ethical problems and possibilities about boosting our body in the future and the risk they see.

Hellaphone: Replacing the Java in Android by John Floren

In this talk John Floren from Sandia National Labs showed some of the problems we have with today's smartphones. While Apple and Microsoft develop closed-source operating systems, Android gives developers insight into the code. But the code is large and not very well documented. In addition to that everything is wrapped in Java, so the apps are always executed in a Virtual Machine, which means performance loss. During his works, John had the idea of stripping the whole Java layer from the Android platform and build the OS on a plain Linux system. They ported the Inferno OS to the Android platform with an adapted UI. While the system is not really useable for every day tasks, because of several drawbacks (e.g. there is no multi-touch), they had some very interesting ideas for the new solution. For example phone calls can be made from the terminal: "echo 'dial 15551234567' > /phone/phone". The phone could be programmed to wipe the SD card, if the accelerometer reads more than 10G. This could be used to destroy sensitive data in emergency cases. Hellaphone seems like fun to try it on a rainy weekend, but I think you should not rely on it for your everyday phone OS.

Black Ops by Dan Kaminsky

Dan Kaminsky is known for very entertaining talks. It was really funny to listen to his talk, which went through several different areas of the IT security world. First of all he talked about today's encryption is often flawed because of bad random number generators. Computers nowadays often use hardware, like keyboards, mice or hard disks as sources for entropy. However most of this hardware is not available on virtualized server environments. After presenting a hack to get good entropy, Dan went on to injection flaws, like SQL injection. He hypothesized, that often developers do not use secure code, because it is to much work to build secure code. Most developers are happy, if their code compiles and fulfills functional requirements. The goal must be to provide frameworks and languages, which force the user to write secure by making it easier to write secure code than insecure code. He all talked about section of censorship and certificate replacement in the web environment. It was a lot of stuff covered in the talk. In my opinion it was a bit too much for a talk that started on 4pm and after a whole day of lot impressions from other talks.

About the Authors

Martin Loher, IT Security Analyst at Compass Security.
Martin Loher completed his studies for a BS in Computer Sciences at the end of 2007. During his studies he put high emphasis on subjects like software engineering, knowledge-based systems and Internet security. In several student research projects as well as in his diploma thesis on "Webbased Lifecycle Management" he expanded his knowledge in the environment of large web applications.
Martin Loher has been working as a security analyst for Compass Security AG since January 2008.

Riccardo Trombini, IT Security Analyst at Compass Security.
Riccardo Trombini completed his studies for a BS in Computer Science at the beginning of 2009. During his studies he focused on the major subjects of Internet technologies as well as network and IT security. After his studies he worked as a software developer for a renowned online shop and was able to apply and expand his knowledge of web application security.
Since November 2009 he has been working full time for Compass Security AG.

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 25 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 PenetrationTests, 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/