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 2011
October 17th, 2011

Document Name:	BlackHat_2011_v1.0.docx
Version:	v1.0
Author(s):	Roger Blum, Compass Security AG
	Michael Schmidt, Compass Security AG
Date of Delivery:	October 17th, 2011
Classification:	PUBLIC

By Roger Blum and Michael Schmidt

Introduction

Black Hat 2011 USA in Las Vegas; one of the biggest IT-Security conferences located in the Caesars Palace at Las Vegas and Compass has attended. Two security analysts participated at Black Hat this year and learned about the newest trends in IT-Security. A great many things are going on in IT-Security and for Compass it is more important than ever to keep in touch with the newest technological evolutions going on. Researchers have presented their results the first time to the public, new vulnerabilities and attacks were described, new tools and mythologies were introduces and vendors have explained their innovative and new products.
Quite lot briefings were given in nine parallel tracks so it wasn't possible to hear all interesting speakers. However, this paper summarizes some of the most interesting talks the Compass employees have visited and indeed, they are very interesting. We encourage you not only to read this summary but to go online and watch the videos ...

Abstract

No more attacking as usual. Security providers have developed security products that protect us and make attacks as usual, as we have seen them the last years more and more difficult. Therefore the attacks are also moving to more and more dedicated-, customized- and creative ways. Clearly, new technologies, such as mobile devices and HTML5, will affect IT security. But also the "old stuff" compromised in new creative methods, such as identifying you only based on a profile picture or exploiting DNS by making use of cosmic radiation. Hackers showed their creativity in hacking systems even if they seem to be secure; if a computer is secure, try to hack it through its battery!

Bit-squatting: DNS Hijacking without exploitation

Artem Dinaburg's talk about bit-squatting was for us one of the highlights of this year's Black Hat.
Bit-squatting is the same as typo-squatting but for bits. Due to heat, electrical problem's, cosmic rays and defects about 600'000 bit errors occur every day on the whole world.
Artem analyzed the bit-squatting errors in domains. So he took well known domains such as facebook.com, converted them into binary, flipped a bit, and converted them back. As an example facebook.com leads in fadebook.com. He then registered all these domains and configured a DNS zone and also a web server which responds on these requests. For measuring the occurred bit-squatting he chose only URLs that are never entered by a human to exclude typos.
It is unbelievable how many "wrong" requests, containing valid session information, Artem was able to catch! One of his real world examples was p**b**ofile.ak.fbbdn.net (Facesbooks Farmville). Here a bit error in one of the Zynga server farm occurred. This resulted in 2555 requests from 1227 unique IPs to Artems registered domains. A simple attack with a great profit.

USB – Undermining Security Barriers

Andy Davis talk was about vulnerabilities in USB drivers on different platforms and devices. He did some research in how these vulnerabilities can be identified. In a first step, he built its own USB-Fuzzer based on an Arduino board. Unfortunately he was unhappy with the results and he decided to buy a product called Packet Master USB 500 AG. With the included tool, called GraphicUSB, it is possible to record USB traffic and replay it afterwards. A disadvantage of this tool is, that there is no API for manual scripting. Finally Andy found Frisbee, a tool which can modify the captures and send them to GraphicUSB via Phyton's SendKeys library.

As a conclusion: There are still plenty of vulnerabilities in USB device drivers and an Endpoint Security solution will not protect us of these attacks. If you want to be aware, disable the USB port in the BIOS.

Battery Firmware Hacking

The talk of Charlie Miller was an eye-opener to us. We'd never thought that there is such intelligence in a laptop's battery!

Charlie heard that every battery in an Apple's MacBook has a chip, which can be controlled if the password is known. Unfortunately Apple uses the same password for all batteries which where produced. With a reverse engineering of the Battery Firmware Update Utility, Miller was able to gather this password. But, what can we do now? As an example, we can tell the battery to don't stop charge after it's fully charged. In the worst case, the battery could explode! To counter this attack, Charlie developed a small tool which let's you change the chip's password.

Hacking .NET Applications – The Black Arts

This talk was about how to crack .NET applications. Jon McCoy started his presentation with explaining the two main attacks on .NET applications: attacking on Disk and attacking in Memory/Runtime. Same to both is the difficulty of identifying the weak spot. The main steps (simplified) for attacking on the disk (decompiling) he explained are: Flip The Check, Cut The Logic, Return True, Access Value, Set Value is "True". This may be done with setting a simple check to always true, crack complex math or fake a server call.

For attacking .NET application in runtime Jon McCoy developed an own tool for injection objects in to a .NET program at runtime. This tool he presented in a live demo and hacked a .NET application.

Finally he explained of how programmers can learn from attacking .NET Applications. In knowing of how an application can be attacked it is easier to build it secure.

Analyzing SPDY

Thomas Roth talked about SPDY, an alternative to the common HTTP protocol, invented by Google. As many of us don't know, if you're using Google's Chrome browser and surfs to a Google web site, such as Gmail, Docs, search engine, you already talk SPDY!

The difference of SPDY to HTTP is, that SPDY uses one single TCP connection which is hold open for the whole visit to the web application. This open connection is called "session" where the single requests inside

are called "frames". A great advantage of this session is, that now real push notification from the server to the client are possible. There is no longer a need to poll the server every few seconds to e.g. get notified about new mails in und webmail client.
Unfortunately, Thomas RothsRoth's luggage was lost and he didn't had is laptop to make some demos at the end of the talk.

Hacking Google ChromeOS

The presentation of Matt Johanson and Kyle Osborn was about hacking the Google ChromeOS. They both work for an IT security company and had the opportunity to join the ChromeOS beta test program.
In ChromeOS, all applications run in the browser and are comparable to small web applications.
They analyzed the ScratchPad app, which was delivered by Google itself, and found a Cross-Site Script vulnerability that allows injecting code in other users' browser.

Apple iOS Security Evaluation

Din Dai Zovi's talk about his analysis of the Apple iOS was very interesting but also a little bit complex. He reverse-engineered the top ten of the free apps in the AppStore to analyze if they are vulnerable to buffer overflow and other attacks. Due to the fact that all application in the AppStore are signed, and the AppleMobileFileIntegrity kernel module checks this signature, most of the applications are save, unless you jailbreak your iPhone and also install apps from other sources.

Server-Side JavaScript Injection

Attacking NoSQL and Node.js. Client-Side JavaScript injection (XSS) and the danger of this attack is mostly known. In the meanwhile JavaScript is also used on server-side - Server-Side JavaScript (SSJS) is integral to many NoSQL databases such as MongoDB and Neo4j. Bryan Sullivan presented the dangers of such Server-Side JavaScript code injection which can beused to write, upload and execute arbitrary files on the web server.
He compared the Server-Side JavaScript attacks with XSS and showed that the attacks are very similar. He made some demos of how XSRF can be launched, SQL-Injection, bypassing Firewalls and Port-Scanning attacks.
The presentation was finished with some recommendations of how the Server-Side JavaScript injection can be mitigated. The most important: Same old story, different words: Do input validation …

Reverse Engineering Browser Components: Dissecting and Hacking Silverlight, HTML5 and Flex

RIA – Rich Internet Applications will be more and found in the Internet. Web applications are full of new HTML5 features, Flash, Silverlight extended DOM and numerous third party libraries. Traditionally the web applications only needed to be protected on the server side; today protecting the client is important as well.
Shreeraj Shah presented reverse engineering mythologies to determine potential weaknesses. Some of his attacks he presented were:

- Malware and Worms leveraging XHR and WebSockets
- Exploiting HTML5 presentation features like CSS-opacity, sandboxed Iframes, Canvas etc. for potential abuses like ClickJacking and Spoofing
- Reverse engineering Silverlight components to discover vulnerabilities and business logic secrets
- Hacking and attacking Flex or Flash components via DOM
- Protocol reverse engineering and injections AMF, WCF, JSON etc.
- DOM injections and pollution to gain execution capabilities
- Cross widgets and component hacking and architecture reverse engineering

He covered these attacks and their variants along with some real life cases and demonstrations. He also introduced of how these types of vulnerabilities can be discovered and which tools can be used for this.

Don't Drop the SOAP: Real World Web Service Testing for Web Hackers

Web application penetration testing is not all about attacking the web interface. A modern web application is composed out of many parts that all together form a web application. One of these parts are SOAP web services. It is a common practice to load data from external servers using provided web services.

Kevin Johnson, Tom Eston and Joshua Abraham reminded to not forget these SOAP interfaces. They described the problems in testing SOAP interfaces using standard approaches to testing web application. Many of the tools and mythologies are not adequate and useable for web services. They introduced a combined solution by using SoapUI and BURP. SoapUI is used for interpreting the WSDL and creating valid XML SOAP messages and BURP is used to manipulate and resend them.

Finally they talked about their research about SOAP and how it will be included into the OWASP Testing Guide 4.

SSL And The Future Of Authenticity

Moxie Marlinspike gave a well presented talk about SSL-Authenticity and the problems. Who do you trust? The whole trust of our SSL-Authenticity is based on the Certificate-Authorities imported. Moxie talked about some break-ins to CAs and the bad reactions of these CAs.

The victim may not notice that a CA is hacked. This has the result that he trusts a Man-in-the-Middle and the attack will be completely transparent. His main critic points are: 1. There are too many CAs 2. There are a few bad apples 3. There's a mixed scope. We are not able to not trust VeriSign or Comodo because we will not be able to access the Internet anymore (certificate warnings will appear for nearly all HTTPS sites).

As a solution Moxie introduced a notary concept. The idea behind this idea is, that you do not trust CAs anymore. You decide which notary you will trust and for how long. When requesting a website two requests are made: one to the target website and one to the notary. The notary then attests to the user that the website is really the one it claims to be.

Lives On The Line: Defending Crisis Maps in Libya, Sudan, and Pakistan

We hear about Social Networks such as Facebook and YouTube mostly bad news if we talk about security. A different view gave George Chamales to this topic. He described how open source intelligence (such as Twitter, Facebook, YouTube news reports) and direct messages (SMS; email) can be used during disasters to create crisis maps in earthquakes and civil unrests. Deployments of crisis mapping technologies are used to gather information about a crisis to be able to send help.

He explained how the platforms can be used and how people can report. Out of this information humanitarian organizations are able to better coordinate their direct aid and save lives.

However, crisis maps also have problems. How to implement the platform, how to organize, which platform to be used, where to locate the platform, which messages should be collected, how should the messages processed, how the reports presented. Additionally crisis maps are exposed to specific attacks such as someone not wanting a crisis map to be deployed. Therefore George Chamales asked the audience and hacker community for help. Any ideas for attacking and improving crisis maps that they can be used more secure and accurate are welcome!

Faces Of Facebook - Or, How The Largest Real ID Database In The World Came To Be

What's the problem if I post my picture on Facebook? What's the problem of social networks? Nobody will ever be able to find me! Alessandro Acquisti demonstrated that this is not true. He developed a program that makes it possible to find you in social networks only based on a photo of you.

He investigated the privacy implications of combining publicly available images of persons with off-the-shelf face recognition. Therefore he downloaded and processed pictures and the attached personal information of many social communities. Then he made an experiment: He asked students on the campus to participate by only letting them being photographed. This photo was processed on a cloud computing service and a face matching was made. All the previously collected data was combined and checked whether a face match was recognized. In many cases he was able to find out the name and other personal details about his participants.

Finally he presented an iPhone application that can be used to do this on-the-fly. He used his iPhone to take a photo of a person and after some seconds he knew the name and address. So, next time you want to flirt in a bar, use his application and you already know the name…

About the Authors

Roger Blum, IT Security Analyst at Compass Security.
Roger Blum works for Compass Security AG since September 2007. First, he worked as a part-time employee before he started his work as a full-time security analyst in October 2008. During his study in computer science at the University for Applied Sciences in Rapperswil, he focused on network technologies as well as security. He also got certified as a Cisco Certified Network Associate.

Michael Schmidt, IT Security Analyst at Compass Security.
Michael Schmidt completed his studies in the field of computer science and media in mid 2007. The main focus of his studies was in the fields of software development and security where he also conducted several study projects. His diploma thesis he wrote with UBS AG in Zurich in the area of system modeling. Parallel to his studies he worked as a freelancer at Mosaiq Media as a developer for complex Web applications. He has been working as an IT security analyst for Compass Security AG since October 2007.

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/