/dev/random
Can't sleep, hackers will eat me!

Hack.lu 2015 Wrap-Up Day #2

October 21, 2015 22:58 | 14 Comments | Xavier

Here we go with my wrap-up for the second day. After some coffee and pastries, the day started hardly with a very technical talk. Samuel Chevet & Clément Rouault presented their research about Windows local kernel debugging. Kernel debugging does not mean always being used for the bad, it can also be used for good purposes. When? For reverse engineering, exploit or driver development or for low level interaction with the system.

How to access the debugger? Via the network cable, USB, a serial cable, serial over USB or locally. This was this last way that we covered in Samuel and Clément's talk. By running the debugger locally, it means that the debugger is running on the computer as any other program => No break point possible of course! But you can dump memory, search for interesting stuff in memory or, better, modify this memory. They explained how to use WinDbg, the debugger provided by Microsoft. After a description of the standard features, they explained how to use Python to interact with the local debugger.

Honestly, the rest of the presentation was way to technical for me. The demos they presented looked impressive how to (ab)use the Windows kernel and memory. If you're interested in this field, have a look at their slides.

Then, we focused on the "*Security of Virtual Desktop Infrastructures*" by Maxime Clementz and Simon Petitjean. VDI technologies are more and more deployed in big organizations for multiple reasons: cost, ease of use, maintenance but, in some case, definitively not for security reasons! During a penetration test, they discovered multiple vulnerabilities in the deployment of a Teradici solution.

Follow Me

Upcoming Events

Here is a list of events that I will attend and cover via Twitter and wrap-ups. Ping me if you want to meet! The list is regularly updated.

Recent Posts

The Truth is in Your Logs!

Physical Access == Pwn3d!

[SANS ISC Diary] Unity Makes Strength

Managing Palo Alto Firewalls Custom URL Categories

[SANS ISC Diary] Enforcing USB Storage Policy with PowerShell

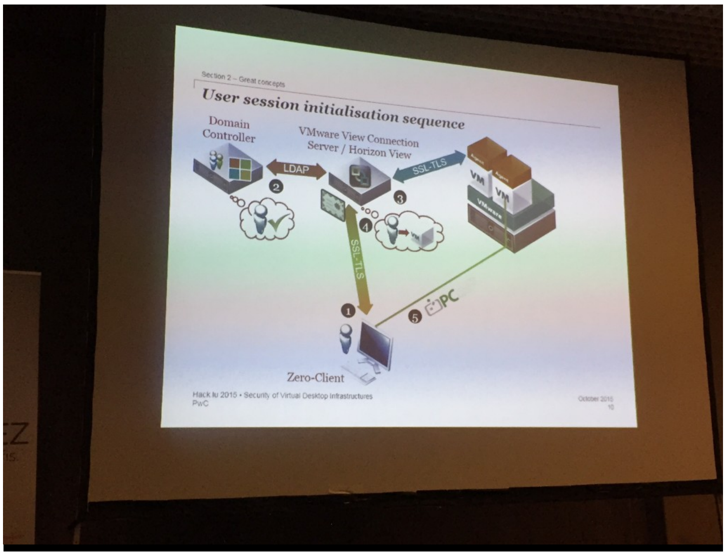
Popular Posts

The Truth is in Your Logs!
2,043 views

Physical Access == Pwn3d!
361 views

Managing Palo Alto Firewalls Custom URL Categories
206 views

Show me your SSID's, I'll Tell Who You Are!



Section 2 – Great concepts

User session initialisation sequence

Hack.lu 2015 • Security of Virtual Desktop Infrastructures
PwC

October 2015
10

The solution is based on the PCoIP protocol and zero-client. In a first step, they explained how sessions are initiated and how, from a security perspective, it looks a good approach (no local storage, "*empty shell*", etc). But, when they gave more focus in the PCoIP management console, they started to find interesting stuff: many open ports, vulnerable software components, default passwords, data stored in clear text in databases. About those databases, they found an non-protected page which allowed to download previous backups ("BackupDBDownload.php"). The URL being based on EPOCH timestamps, it was easy to get back in time and to find a valid backup file. Backup are encryption but in a bad way (an hard coded password). They also found a vulnerable ProFTPd server vulnerable to CVE-2015-3306. About passwords, Teradici was using postal address as password for SSH, fail! All those findings put together, they demonstrated a Python script written to pwn a management console and play MitM. The client being disconnected and reconnected to a rogue server. The talk was a good opportunity to explain how they applied the process of responsible disclosure. They reported the findings to Teradici via the CIRCL and it was quickly fixed.

The coffee break was welcome before the next presentation: Frédéric Jacobs about "*Advances in Secure Messaging*". Within the first slides, Frédéric reviewed the story of well known protocols:

- 1991: mail box protocol (ARPANET), no auth, no encryption
- 1982: SMTP
- 1984: POP
- 1991: PGP, IMAP v3 (still plaintext authentication)
- 1994: OTP and Kerberos support in IMAP/POP
- 1995: Auth in SMTP, SSLv2
- 1997: SMTPS

MALWARE ANALYSIS
PROFESSIONAL SECURITY TRAININGS
SYSTEM AND NETWORK FORENSICS
REVERSE ENGINEERING
INDICATORS & INFO SHARING
INCIDENT RESPONSE
CYBERSECURITY
CIRC
PARC HOTEL

179 views

Sending Windows Event Logs to Logstash
126 views

dns2tcp: How to bypass firewalls or captive portals?
125 views

Forensics: Reconstructing Data from Pcap Files
87 views

Vulnerability Scanner within Nmap
77 views

Keep an Eye on SSH Forwarding!
75 views

Email Tracking for Dummies
68 views

Recent Tweets

#CCC is alive! src_ip="151.217.0.0/16" -> 245 hits in my logs since 26th Dec… 11 hours ago

Usually, we're looking for a password… Here, I found one and I'm looking to who it belongs ;-) 13 hours ago

Any idea why all cmds return "Rex::TimeoutError Operation timed out" in a valid #Meterpreter session!? #LazyTweet 16 hours ago

xortool.py: a tool to guess the key length and key of a XOR'd file (kitploit.com/2013/02/xortoo…) 19 hours ago

Anybody has access to a #Barracuda spam firewall? I've a question… (Please RT) 2 days ago

Follow Me on Twitter

Time Machine

Time Machine

Select Month ▾

"SecurityFocus Vulnerabilities"

Vuln: Google Chrome Prior to 47.0.2526.106 Multiple Remote Code Execution Vulnerabilities

Vuln: libxml2 CVE-2015-7500 Denial of Service Vulnerability

Vuln: Mozilla Firefox Multiple Security Vulnerabilities

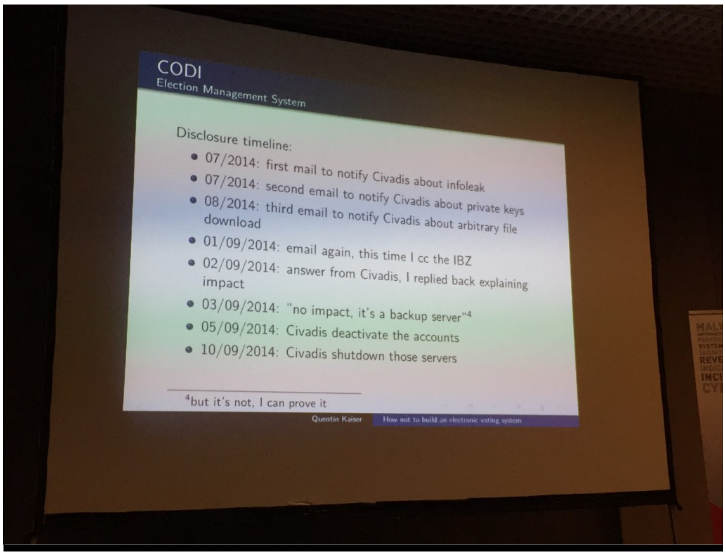
Thanks to the Snowden story, today more and more people takes care of their privacy. This is especially true in messaging applications. A fact reported by Frédéric: today the adoption of SMTP remains bad (only a few percents of the total mail traffic). There exists solutions to encrypt data (PGP and friends like S/MIME) but they suffer of multiple problems:

- They work in asynchronous environment
- They lack of forward / future secrecy
- They lack of deniability
- They are complex to deploy and use!

Today, the experience of users regarding messaging applications is changing: it is based on multiple devices, they need ability to message offline users and the use of groups keeps growing. We are facing message protocols VS session protocols. The second part of the talk focused on the description of modern protocols used in messaging applications.

Quentin Kaiser talked about electronic voting system used in my country: Belgium. During the last elections, the system in place suffered of a major bug which forced authorities to count against votes manually. The problem was so big that the e-vote has been suspended by authorities. It was two years ago and this (bad) story gave ideas to security researchers who try to understand how the system works. It was introduced as a test in 1991 in two townshops. In 2012, the Smartmatic system was introduced. Building an e-voting system is very complex: It must have:

- Confidentiality
- Non repudiation
- Authenticity
- Integrity
- Audit trails
- and simplicity!



CODI
Election Management System

Disclosure timeline:

- 07/2014: first mail to notify Civadis about infoleak
- 07/2014: second email to notify Civadis about private keys
- 08/2014: third email to notify Civadis about arbitrary file download
- 01/09/2014: email again, this time I cc the IBZ
- 02/09/2014: answer from Civadis, I replied back explaining impact
- 03/09/2014: "no impact, it's a backup server"[4]
- 05/09/2014: Civadis deactivate the accounts
- 10/09/2014: Civadis shutdown those servers

[4] but it's not, I can prove it

Quentin Kaiser How not to build an electronic voting system

Quentin focused on the CODI system, based on magnetic cards. He explained in details, how the magnetic card layout was designed and used. He also explained how it was possible to bypass the fraud detection mechanism. I'll not give details here (have a look at his slides) but the talk contained a lot of fact that made the audience laugh… (or cry?)

- Basic encryption (XOR!)
- Old technologies used (floppy disks)
- Clear text communication between components
- Password disclosed online
- …

Quentin's conclusions: The CODI system was broken starting for day 1 and needs a strong audit!

After a lunch and some drone flights, back to the main room to listen to Marie Moe who came back on stage to present a more detailed version of her research about pacemakers (see my yesterday wrap-up). About the future, we'll have to trust machines more and more. Like the example given by Marie: an animal heart fully controlled by sensors:

Vuln: Libxml2 'xmlParseConditionalSections()' Function Denial of Service Vulnerability

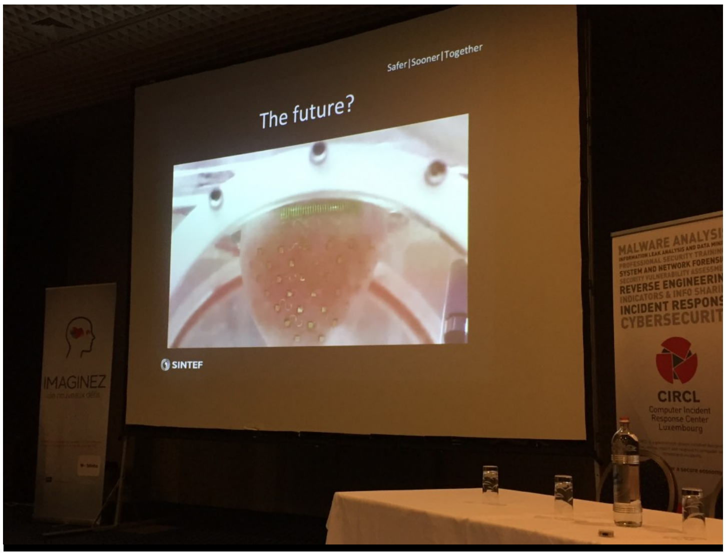
Bugtraq: [oCERT 2015-012] Ganeti multiple issues

Bugtraq: WebKitGTK+ Security Advisory WSA-2015-0002

Bugtraq: libtiff bmp file Heap Overflow (CVE-2015-8668)

Bugtraq: libtiff: invalid write (CVE-2015-7554)

More rss feeds from SecurityFocus



The Internet of Medical "things" is real… Marie gave several fail examples like a medical company contacting their cloud provider to ask why they can't monitor some patients for a while… and giving all the details in the mail body! A presentation full of emotions and where Marie was really congratulated by a huge amount of applause! To conclude, I noticed this tweet from Regiteric:

> @xme There is a stress test function in pacemaker that panic heart to see if device can recover the heart. You can activate it remotely…

The next time slot was assigned to Ange Albertini and his famous malicious files! Ange's vision about files and formats is unique. Can we trust them? "*Yes, I'm writing files by hands and I open them in hex editors*".

CONGRATULATIONS!
YOU OPENED A CORKAMI PDF!
NO WORRIES,
IT'S JUST A STANDARD FILE ;)
For some reason, many people are not motivated to open any files coming from me, so I made this to reward them :)
IMAGINEZ

His talk was a suite of enumeration of funny proof-of-concept… Ange says "*A file has no intrinsic meaning*" It can be opened by multiple programs and have multiple behaviours. Files are not used in the same way:

- End-users: view external files, use it, save it
- Developers: rely on the specs
- Archivists: want to make sure that his data will be re-usable later.
- Attackers: try to craft dangerous files
- Defenders: want to prevent it from happening

Nice talk, but here again, difficult to resume in a few words… Have a look at Ange's website to have a better idea of his research: pe.corkami.com.

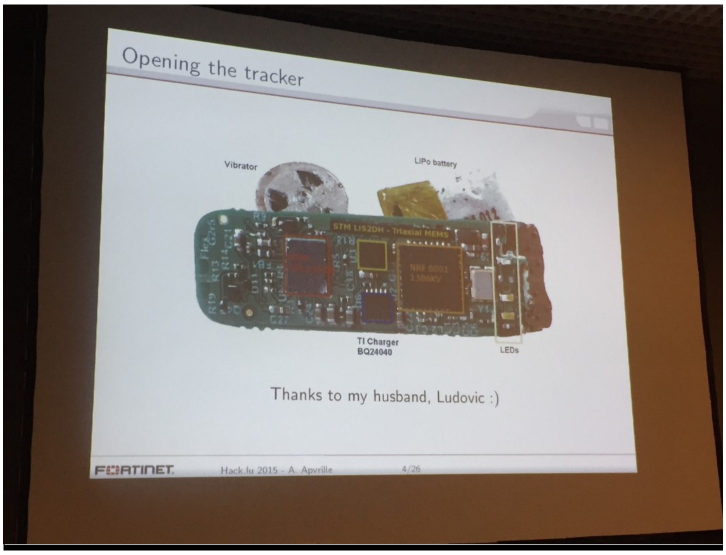
The next talk was not technical but tried to gave a political view of the Internt in Iran… Mahsa Alimardani's talk was "*How mobile applications are redefining information controls inside of Iran*". In this country, the Internet is called "Filternet" because it is completely filtered and controlled. The Iran's internet is the infrastructure of control TCI ("Telecom Company Iran"). All traffic is routed to TCI. It started in 2001 and, in 2012, the Supreme Leader established the "Supreme Council of Cyberspace".

Over there, Internet is a national security issue. Authorities implemented several types of control:

- Shallow inspection at ISP level
- Firewall and traffic shaping boxes
- IP based filtering
- Random packets dropping!

They also push for a imitated and controlled Internet called "*Halal Internet*" where classic sites are replaced by local solutions. Example the Iranian version of Instagram is called Lenzor. Masha then focused on the mobile devices and the applications used by people in Iran. Like everywhere new technologies have been adopted by citizens and, here again, authorities are trying to control them. This talk was interesting and opened my eyes about what's happening over there!

Axelle Apvrille presented her research results about Fitbit trackers. I had the opportunity to see a first version of this talk at Hack in Paris in June. In a first phase, Axelle explained what is the tracker, what are its features and how it works. The best way to learn is to open/dissect the device. It is based on a vibrator, a LiPo battery, an accelerometer, a Bluetooth LE chipset and some LEDs.



Opening the tracker

Thanks to my husband, Ludovic :)

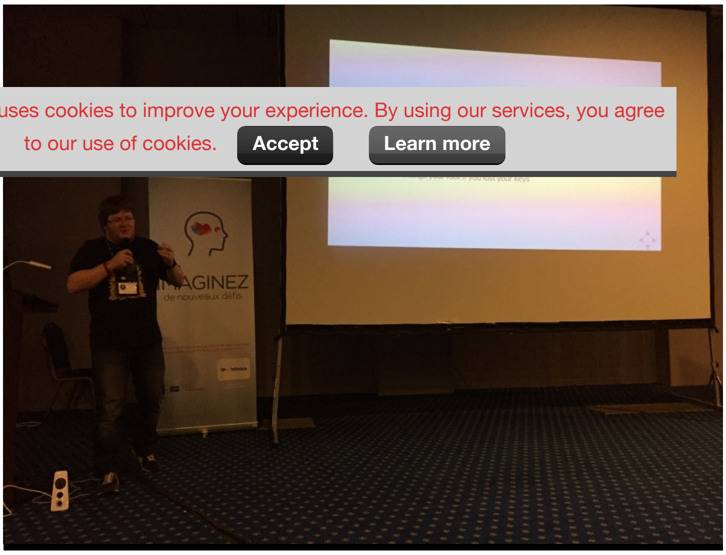
FORTINET Hack.lu 2015 - A. Apvrille 4/26

Of course, everything is proprietary and undocumented. After reversing the Bluetooth protocol between the devices and the laptop/mobile phone, Axelle was able to write a tool to interact with her wrist. It started with funny thinks like making the LEDs blink. Another idea was to use the wrist as a random number generator. Since her talk in Paris, Axelle improved her presentation and added a nice feature to the Fitbit wrist: why not use it to (un)lock your computer when you're away? She explained how to achieve this and make a nice live demo! The next (ab)use was to inject some data into the wrist and send them to the connected computer. If it's working fine, the major limitation is the size of the data: Maximum 17 bytes can be sent. It's a big limitation but, as said Axelle, 4 bytes were enough to crash a Pentium processor in 2004! Axelle released all the scripts used in her presentation.

The next speaker was Yaniv Balmas with his talk about KVM's! They are everywhere, on every desktop, in every datacenter. From the 1990's version (an A/B switch) to the modern ones with thousands of ports, they also evolved and today they can be considered as complete computers. And computers are made to be abused right?

As they are designed to process keystrokes, they are good candidates to run keyloggers. Yaniv explained how to tried to reverse the firmware of a KVM. It was challenging and the researchers had to bypass multiple issues. Each scenario was explained in a funny way by Yaniv and step by step how the firmware was successfully reversed! During this process they also found that some piece of code was dedicated to a keyboard emulation. Wait? Does it mean that the KVM can act as an USB Rubber Ducky? Challenge accepted again! The presentation ended with an awesome demo of injecting a malware into an air-gapped computer connected to a KVM… This was for sure my favourite talk of the day! Good speaking, good topic, awesome demo… The conclusion to this talk: KVM are computers and do not share KVM's between zones of different security level!

Why not remain in the same field and continue to abuse hardware? After Fitbit wrists and KVM's, Damien Cauquil presented his research about smart locks. If some vendors were disclosed during the day (see the VDI talk above), here Damien did not disclose the vendor name. It's a fact that today mechanical logs are weak and not very convenient. As an example, if you loose your key, you must change your lock. We need a credential dematerialisation. Keys are now data and, with smart locks, we can assign, revoke keys or have multiple keys for one lock. It is so convenient to grant access to some people only at specific times.



Damien's target was a smart lock available in US and EU. It can be used with NFC tags and Bluetooth LE. What could possibly go wrong asked Damien… So many things! The rest of the presentation was dedicated to the detail about how the device can be abused. Using a Bluetooth sniffer, Damien was able to reverse the protocol and write his own tools to abuse the lock. The most entertaining was the "*Blueman in the Middle*" where he made a fake smart lock able to collect keys and they replay them against the real lock to… unlock it!

The last presentation of the day was performed by Laura Vidal. The talk was more a reflection about how to improve the communications between "techies" and other people. Technical guys are good to find critical issues, to write tools to exploit/fix them but they simply can't talk about them to non-technical people. The idea of the talk was interesting and lot of questions raised from the audience turning the talk in some kind of round table.

As a tradition, the Belgian infosec crew had the Belgian dinner with good food and interesting discussions… It’s now time to get a few hours of sleep before the third day. See you tomorrow!

Like Share 0 Tweet

- Stu

Pin It

Posted in: Security, Event | Tagged: Security, Event, hack.lu, Luxemboug

Profile

Sign in with Twitter Sign in with Facebook
or

Comment

Name

Email

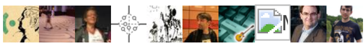
Not published

Website

Post It

- 14 Replies
- 0 Comments
- 14 Tweets
- 0 Facebook
- 0 Pingbacks

Last reply was 2 months ago



... and 4 more

← Previous Post Next Post →

Theme Chiron by WPJournals · WordPress