Computer Security in 2015: Where are we? What to expect? How does it affect science / HEP?

Sebastian Lopienski
CERN Deputy Computer Security Officer

CHEP 2015
Congratulations!

4.7 magnitude earthquake
134 km from Itoman,
Okinawa, Japan

2 days ago
UTC time: Sunday, April 12, 2015 02:49 AM
Your time: Sunday, April 12 2015 11:49 AM
Delete any YouTube video

1. Send this:

   POST live_events_edit_status_status_ajax?action_delete_event=1
   Host: www.youtube.com

   event_id: ANY_VIDEO_ID
   session_token: YOUR_TOKEN

2. Receive this:

   {
     "success": 1
   }

3. Report to Google and get $5’000 bounty

Blunders happen to everyone

... but better to be ready to react fast
Security on the Internet?

https
Apple’s “goto fail” SSL bug (late 2012 – Feb 2014)

```c
if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(ctx,
    ctx->peerPubKey,
    dataToSign,
    dataToSignLen,
    signature,
    signatureLen);

if(err) {
    sslErrorLog("SSLDecodeSignedServerKeyExchange: sslRawVerify 
                returned %d\n", (int)err);
    goto fail;
}

fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
```
Heartbleed bug (OpenSSL)
SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).

User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server’s master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "ColHeRaSt". User Arber requests pages.

From http://xkcd.com/1354/
Software and protocols we all rely on are vulnerable
A simple mistake...
but honest or intentional?

goto fail;
goto fail;
Software and protocols we all rely on are sometimes made or kept vulnerable.
Code from 2004, running as root

```perl
foreach my $f (<$_[0]/.*\.out>){
    my $nf="$f.cut";  # files are in /tmp
    system "
      head -100 $f > $nf;
      echo "----CUT----" >> $nf;
      tail -100 $f >> $nf"
;}

Two root privilege escalation vulnerabilities:
- $f tainted (name of user-created file, can include shell commands)
- $nf controlled by user (can be a symbolic link to system files)
```
Code from 2004, still running as root

Reported by a user:

“I was in a usual boring meeting and just did ps aux in lxplus :)”
We often rely on very old code

... but who knew secure coding back in 2004?
DRAM rowhammer bug => kernel exploit

Access repeatedly a row of DRAM memory

codela:

```assembly
mov (X), %eax // Read from address X
mov (Y), %ebx // Read from address Y
clflush (X) // Flush cache for address X
clflush (Y) // Flush cache for address Y
jmp codela
```

This can cause bit flips in neighboring rows

Proof-of-concepts: privilege escalation exploits

- e.g. modifying page table entries (PTEs)
- goal: gain write access to its own page table
- result: gain read-write access to all of physical memory

http://googleprojectzero.blogspot.fr/2015/03/exploiting-dram-rowhammer-bug-to-gain.html
Attack techniques are highly sophisticated

... and they only get better
Prepare for your day and stay in touch.

Job Changes

[Profile picture] has a new job.
Now Senior Software Engineer at [Company Name]

Say congrats

Work Anniversaries

[Profile picture] is having a work anniversary.
1 year this April at [Company Name]

Say congrats

[Profile picture] is having a work anniversary.
4 years this April at CERN.

Say congrats
Exploit kit infection chain

Source: Trend Micro
Attacking is so much easier than defending

... and cheaper, too
Your personal files are encrypted by CTB-Locker.

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press ‘View’ to view the list of files that have been encrypted.

Press ‘Next’ for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View  95:58:56  Next >>
Bitcoin mining: $250 K / month

Click fraud: $2.8 M / month
Opportunistic attacks

Criminals are just after the money, so they usually chose the “easy targets”
PLEASE DO NOT LOG ONTO YOUR PC EQUIPMENT OR COMPANY WIFI UNTIL FURTHER NOTICE

For update information contact CSD via ext. 3459
Sony Pictures Entertainment breach

Warning:
We’ve already warned you, and this is just a beginning. We continue till our request be met.
We’ve obtained all your internal data including your secrets and top secrets.
If you don’t obey us, we’ll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM (GMT).

Data Link:
https://www.sonympicturesstockfootage.com/SPEData.zip
http://dmiplaewh36.spe.sony.com/SPEData.zip
http://www.ntcnt.ru/SPEData.zip
http://www.thammasatpress.com/SPEData.zip
http://moodle.universidadebematech.com.br/SPEData.zip
Targeted attacks
Much harder to protect against, much more devastating
... but who is really behind this attack?
8 months

“Average time between intrusion and detection”
Two types of organisations:

those that know they’ve been hacked
and those that don’t know
“We are currently experiencing the largest DDoS attack in github.com's history [...] we believe the intent of this attack is to convince us to remove a specific class of content.” Mar 27
Target: BBC and NYTimes on Github

The Dalai Lama's visit to Japan, "the right to pass human happiness"

The Dalai Lama's visit to Japan since 1967, the beginning of the interval and sometimes as long as 10 years, almost a year after the 1998 visit to Japan, also twice a year in some years, excluding Japan, he visits in turn, has made a special visit to Japan has been at least 19 times.
Man-on-the-side attack

1. A web site you visit loads http://hm.baidu.com/h.js (Baidu analytics)

2. Your browser requests this JavaScript file from Baidu, but gets a response from elsewhere (!)

1. The injected, malicious script hammers two github projects

```javascript
Github didn’t give in... this time.
“Superhuman” espionage malware

Equation group victims map

High infection rate
- Iran
- Russian Federation
- Pakistan
- Afghanistan
- India
- China
- Syria
- Mali

Medium-level infection rate
- Lebanon
- Yemen
- United Arab Emirates
- Algeria
- Kenya
- United Kingdom
- Libya
- Mexico
- Qatar
- Egypt

Low infection rate
- Turkey
- Somalia
- Myanmar
- Germany
- South Africa
- Nigeria
- United States
- Venezuela
- Sudan
- Palestinian
- Morocco
- Malaysia
- Kazakhstan
- Iraq
- Brazil
- Uganda
- Switzerland
- Singapore
- Philippines
- Peru
- France
- Ecuador
- Belgium
- Bahrain

© 2015 Kaspersky Lab
Reprogramming HDD firmware

From: Kaspersky Lab
What else is out there, that we don’t know about yet?
Is it possible to repel government-sponsored attacks?
What to do when criminals or hacktivists of tomorrow use the same attacks techniques as governments of today?
How is HEP affected?

From https://ideas.lego.com/projects/94885
Resources, assets
Motivations

- **criminals**: motivation: profit
- **hacktivists**: motivation: ideology, revenge
- **governments**: motivation: control, politics
“OK, so can someone make money from hacking HEP? ”
Bitcoin mining by a rouge sysadmin

*Inspired* (issue 18, Feb 2015)


“[..] substantial amounts of mining jobs were submitted over the 2013 Christmas holidays before being discovered in early January. The user had attempted to masquerade the mining activities as legitimate production jobs and also tried to hide his traces by planting false evidence of external attacks on the job submission machine. He failed and was caught.”
Computing power == money
“We just do fundamental research – how can this motivate an attacker?”
CERN, “a fun real-world example”

Hacking CERN - Exploiting python-lz4 for Particles and Profit

TL;DR

Editor's Note: The TL;DR of this long technical report can be summarized as:

- LZ4 was always critically vulnerable whether in Kernel or User-land
- Exploitation is easy regardless of the attack used (16MB or 2+MB)
- PoCs are written for python2.7 on 32bit ARM/x86 (scroll to the end)
- Updating is critical for all consumers of LZ4, not just python-lz4

Additional Note: The author of LZ4 claims that the PoC presented in the blog below was written against some ghostly alternative version of LZ4. For further proof of exploitation, the sample payload generated by the script at the end of this blog post will also crash python-lz4 (versions prior to r119) directly. The CERN software was simply used as a fun real-world example because their package depends on python-lz4. To test, call the Python bindings directly with:

http://blog.securitymouse.com/2014/07/hacking-cern-exploiting-python-lz4-for.html
LHC start-up? Death threats

#CultOfSiduri #OpDamageControl

Send email to update those at CERN who may be in danger:

April 3rd 2015. Re: Death threats posted on dark net regarding upcoming CERN high energy experiment

Dear Dr. [Name],

I regret to inform you that your life may be at risk for higher energy particle collision experiments.

Due to warnings by prominent theoretical physicists, some anonymous individuals have become convinced that the only way to save our universe from destruction is to kill these 7 men, of which, unfortunately, you may be one.

SIDURI retweeted

JimRothschild @LordJimRoth · Apr 3
@mrtnbenigno @AnonOpAcc

Yeah, #CERN are risking our Universe to play God. Even if the risk is small they shouldn't do it! >0% = TOO RISKY!!!
“But black hole fears aside, why would someone specifically target HEP?”
Welcome to the CERN Internet eXchange Point

The CERN Internet eXchange Point (CIXP) is a carrier-neutral exchange point based at CERN in Geneva, Switzerland.

Our partners are telecom operators and ISPs in Switzerland and France, as well as national and international research network operators. The service is provided jointly by CERN and Equinix's data-centres in Geneva and Zurich.
The URL?

The URL?
https://zenodo.org

From https://zenodo.org/policies
We never do “just HEP”
Windigo operation

- Spammers send spam emails containing malicious links to potential victims.
- Victims click on the links, leading to a setup process.
- A DNS redirect is performed, directing traffic to a C&C server.
- The C&C server configures a reverse proxy for further communication.
- Malware is delivered, infecting both Windows and Linux systems.
- Infected systems are used to exfiltrate sensitive information.

Source: ESET
Country 'X' infection
how Regin stays under the radar

Control over infected machines in the targeted organizations is implemented through one node (an infected machine in an educational institution) connected to C&C in India.

The attackers can either issue commands to all the victims or command one victim through another (e.g. work with president’s office via the bank network). This strategy allows the attacker to stay under the radar.
Watering hole attacks
We may be *not* the primary target

... but we may still be attacked
Security - it’s just as with earthquakes

Risks are there, whether we like it or not
Addressing them means investing in protection and preparation
Including security early is the only option
We need awareness and education on all levels

Additionally, our systems and outside threats constantly evolve