-*- Computer Security News -*-

Rémi Mollon

CERN Computer Security Team

HEPiX Spring 2012

Prague, Czech Republic

23-27 April 2012

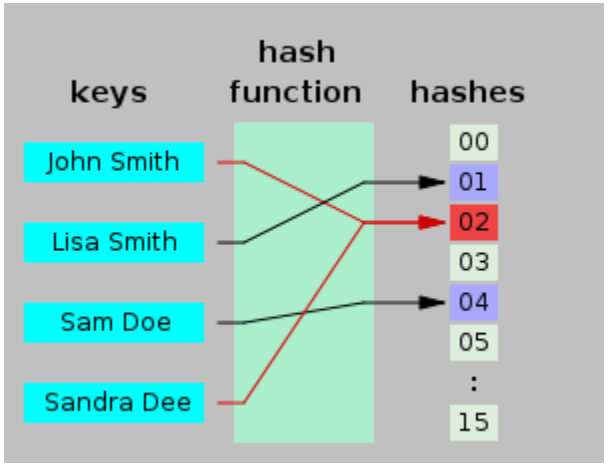
CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Outline

- Interesting Vulnerabilities
- Hacktivity
- Trustworthiness
- From the Internet

PHP (Fail) Story

- PHP hash table collisions CPU usage DoS issue (CVE-2011-4885)
  - Alexander “alech” Klink & Julian “zeri” Wälde at 28C3
  - Most of popular web programming languages
  - Use of simple hash function (djb2) instead of cryptographic ones (eg. SHA256)
  - Realistic efficiency
    - ~70-100kbits/s → keep one i7 core busy
- Disclosure: November, 1st 2011
- Fix release: January, 11th 2012



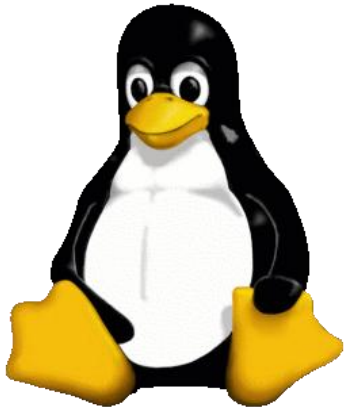
** NOT THAT BAD! But... **

PHP (Fail) Story

- PHP remote code exec flaw introduced in the CVE-2011-4885 hashdos fix (CVE-2012-0830)
  - Stefan Esser
  - Previous fix back-ported to all maintained versions
  - Flaw in the new '*max_input_vars'* directive
  - Much worse vulnerability
- Disclosure: February, 1st 2012
- Fix release: February, 2nd 2012

** BE CAREFUL WHEN FIXING BUGS **

Tough time for Linux...



- Insufficient permission checking of /proc/<pid>/mem (CVE-2012-0056)
  - Root escalation vulnerability
- Debugging actions enabled by default in xkeyboard (CVE-2012-0064)
  - Screen locking application killed by key combination
- Format string flaw in SUDO (CVE-2012-0809)
  - Root escalation vulnerability

What about Macs?

- Apple's Smart Cover security bug
  - Break into any iPad 2
  - Can't open any apps, but can access an app open before locking
- Flashback Trojan
  - Harvest information from Web activities (eg. logins/passwords)
  - 600,000+ infected devices (!?)
    - >1% of Macs
    - Comparable to Conficker worm for Windows
  - Drive-by vulnerability in Java (CVE-2012-0507)
  - Delayed patching of Java for Mac OS X
    - Patched in February 2012 by Oracle
    - Distributed in April 2012 by Apple

Are Macs safer than PCs?

- According to Apple and Mac users: YES!
  - Based upon BSD with built-in security model
  - Homogeneity of the overall system ensured by Apple
    - May add overhead in some cases (eg. Java updates)
- Historically much less targeted by viruses/trojans/worms than Windows
  - Attacks directly related to user community size
    - Apple victim of its success
  - Mac users are less aware and experienced on security
    - No protection software, less careful with updates

** EVERY SYSTEM IS VULNERABLE **

Outline

- Interesting Vulnerabilities
- Hacktivity
- Trustworthiness
- From the Internet

Anonymous

- Anonymous: “Hacker Collective”
  - Several sub-groups: Lulzsec, Antisec, …
- [...]
- December, 24th 2011: Stratfor hack
  - Stratfor Global Intelligence: Security “Think Tank”
  - Clients like Defense Department, Bank of America, …
  - Theft of credit card data
    - Donation of $500,000 to charities
  - Around 1000 stolen mails
    - Given to Wikileaks and other organizations

Anonymous

- February, 28th 2012: 25 Suspected Anonymous Hackers Arrested
  - Across Europe and South America
- March, 6th 2012: LulzSec's top members arrested
  - Based on LulzSec's leader (“Sabu”) cooperation

NASA hack

- December 2010: Computers at NASA's Jet Propulsion Laboratory hacked
  - Damage estimated to be around $580,000
- November 2011: Robert Butyka is arrested and admitted the hack
- January 2012: 3-year suspended prison sentence from the Romanian authorities
- United States hopes to get him
  - Up to 10 year prison sentence

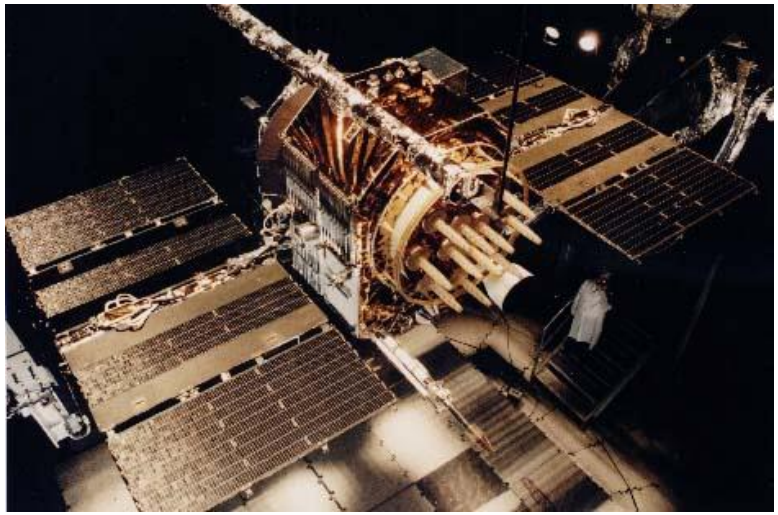
Outline

- Interesting Vulnerabilities
- Hacktivity
- Trustworthiness
- From the Internet

To trust or not to trust...

- People?
  - Social Engineering
  - What about a Policeman?

- Technologies?
  - 100% security doesn't exist...
  - What about a GPS device?



GPS and Financial Institutions

(Analysis from Todd Humphreys from the University of Texas)

- Dependency on highly-precise timing (microsecond) via GPS
- Consequences of a sabotage
  - Black out of the market if detected
  - Timing advantage for unscrupulous people/organisations
- Spoofers/Jammers are on the market
- Low probability + very high impacts
  - Not negligible for risk management

Outline

- Interesting Vulnerabilities
- Hacktivity
- Trustworthiness
- From the Internet

IPv6

- IPv6 is coming...
  - Official launch day on 6 June 2012
  - New security challenges
  - Lack of expertise/experience
    - Confusion and configuration problems
    - Inappropriate monitoring tools

- IPv6-related incidents are rare
  - First IPv6 DDoS in February 2012
  - More and more will come with deployments advance

Great Firewall of China

- Great Firewall of China
  - Censorship + Blocking of Tor Anonymity Network
  - Live deep packet inspection
    - Identifying Tor cipher list in TLS connections
  - Active scanning of suspected Tor bridges
    - Blocking of IP:Port in case of successful scan
- Cryptic probes from random Chinese IPs on port 22
  - Garbage scanning
    - Random binary data to TLS hosts
    - Not targeted to Tor
    - Unknown purpose !?

"How China Is Blocking Tor", Philipp Winter and Stefan Lindskog

http://www.cs.kau.se/philwint/pdf/torblock2012.pdf

Conclusion

- Every OS can be vulnerable
  - Protection software is a must-have
- Trust will remain a big issue...
- Cyberwar (or not)
  - Buzz-word
  - More and more groups like Anonymous
  - Governments are also in the field
- IPv6 is going to generates lots of incidents

Thanks you!

Questions?

Rémi Mollon

Remi.Mollon@cern.ch