More security or something..

Tomas Forsman <stric@cs.umu.se>
2016-11-24
Who am I?

- SysAdm at CS since 1999
- SysAdm at ACC since 1998
- Tinkering with computers since I was ~5
- I like to investigate things
- Mostly Linux/Unix around computers
- Homebrew IoT stuff at home
Mail from Amazon 2 years ago

- Dear AWS Customer,
- We're contacting you as the security of your account appears to be compromised as your bill for August 2014 now exceeds $77,000.00 and is increasing by over $1,000.00 each hour.

... 

- We would very much like to speak to you regarding this matter and help you fix this situation.
GitHub

• Don't check in passwords/keys (like Amazon) on GitHub. If you do, and "immediately remove it" with a new commit, it's still there and someone has already seen it. Change/regenerate.

• People do this by accident. People get bills.
Public clouds

- What do you want to store there?
- NSA is listening
- The hardware owner might be listening
- Other customers might be doing bad things
- PUL
- Box vs Dropbox vs … rules, laws and agreements
Public clouds

• How to make it secure?
  – Encrypt all traffic!
    • .. where is the key stored?
  – Encrypt the disk!
    • .. where is the key stored that is needed when the machine boots?

• If someone else has full control over your reality and all communication, security is hard
Public clouds

- Timing attacks against virtualization
  - Checking cache hits/misses to determine code path used in OpenSSL, revealing the private key
- Network abuse from neighbor customers
Virtual Machines

- Virtual machines on physical hardware

![Diagram](image.png)
Deduplication

- If memory page A and B contains the same thing, store 1 copy and point both there

- Saves memory/space.
- (OS makes a) copy on write
Rowhammer

- Manipulating physical properties of DRAM by reading excessively, draining charge in neighboring memory cells between refresh cycles
Virtual Machines

• Virtual machines on physical hardware
Virtual Machines

• Deduplication time!
Virtual Machines

• Deduplication time!

1234

RAM chip

1234

1234

1234
Virtual Machines

- Hammer time!

![Diagram of virtual machines with a hammer and RAM chip]
Virtual Machines

- Hammer time!
Java Deserialization

- If you use Java serialization to exchange data between components...
- If you allow the world to send data there..
- If there's a library in your classpath that maybe isn't even used...
- If that library has a security hole..
- Java can load it for you and run.
- Apache Commons Collections < 3.2.2, InvokerTransformer for example
- Found 419 sets of it here at CS
Network traffic

• How do you know that you're talking to the right server / component?

• A server authenticates the client by asking for username and password. How does the client authenticate the server?

• (SSL/)TLS is one way
  – Remember to verify the certificates. Samsung fridges don't. How to get updates?
  – Certificates are generated by a CA, which most often wants money (and/or requires time) → people invent their own stuff.
Verify certificates

- Bootstrap problem
- Mail.google.com certificate, expires 2017-01
  - Google Internet Authority G2, expires 2018-01
    - GeoTrust Global CA, expires 2022-05
- What should the fridge do after that?
- How often do you update the firmware in your fridge?
DNSSEC

- DNSSEC
- DNS-Based Authentication of Named Entities (DANE)
Hello!

Username?

Adam

Password?

SnailSoup44

<kind act>

<malice>

Man-in-the-middle
Man-in-the-middle

- Base the traffic/encryption on some secret that the server has, through asymmetric encryption
- How do you get hold of the public key?
- PKI, trusted CA's, chain of trust
Crypto

• Diffie Hellman, previous wisdom said that you can pick any good large prime, so almost everyone picked the same. Reduces the attack cost immensely.

• SHA-1, used in TLS etc, consider it broken
  – Leaves older software out in the dust
  – Cut-off is in action
Time

- All components should preferrably have the same time
  - Prevent replay attacks etc
Statistics

- One of our servers in Luleå, fail2ban had crashed last year
  - November 1st to November 8th; 42768 failed attempts to login as root over ssh.
  - One every 4 seconds.
  - Multiply by how many ssh servers there are in the world.
Scanning all of IPv4

- Roughly 4 billion addresses
- How long does a port scan take from a single (optimized) machine?
Scanning all of IPv4

- Roughly 4 billion addresses
- How long does a port scan take from a single (optimized) machine?
  - About 5 minutes.
DDoS

• In september, some people didn’t like FreeNode IRC network (used by Dark Army in mr.Robot).
• ACC in Samhällsvetarhuset has a server
• NorduNet got about 400Gbit/s heading our way, and re-routed ACC via Chicago instead
• A few days later, a world record of 1.5Tbit/s hit OVH – driven by ~150k IP cameras
• Many parts of the internet broke around that time
RFC5961

- Improving TCP's Robustness to Blind In-Window Attacks
RFC5961

• Improving TCP's Robustness to Blind In-Window Attacks
• Due to "lack of luck when thinking", it enables people to:
  – Find out, from a distance, whether A and B are communicating (10s of work)
  – Disrupt their traffic
  – Inject traffic
• Implemented 2012 in Linux v3.6, fixed Summer 2016.
• All machines running versions inbetween are vulnerable.
Security with IoT

1/x: So I bought a surveillance camera
Security with IoT

1/x: So I bought a surveillance camera

8/x: Actually, it took 98 seconds for first infection
RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis