Security in 2015
LIP PhD Seminar

Arnaud Lefray

January 20, 2015
Some Security Areas

- Physical Security
- Software Security
- Social Security
- Cyber Security
Some Security Domains

- Cryptography
- Biometrics
- Image processing
- Privacy
Some 2014 Stories (1) - Dropbox password leaks

Hackers claim having retrieved 7 millions account credentials

Some Dropbox login:password
Some 2014 Stories (2) - Apple Goto Fail

```c
static OSSstatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
   uint8_t *signature, UInt16 signatureLen)
{
  OSSstatus err;
  ...

  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;
  ...

fail:
  SSLFreeBuffer(&signedHashes);
  SSLFreeBuffer(&hashCtx);
  return err;
}
```
Some 2014 Stories (3) - Heartbleed

```diff
--- a/ssl/t1_lib.c  b/ssl/t1_lib.c
@@ -2588,16 +2588,20 @@
    unsigned int padding = 16; /* Use minimum padding */

-/* Read type and payload length first */
- hbtype = *p++;
- n2s(p, payload);
- pl = p;
- if (s->msg_callback)
-     s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
-         &s->s3->rrec.data[0], s->s3->rrec.length,
-         s, s->msg_callback_arg);

+/* Read type and payload length first */
+ if (1 + 2 + 16 > s->s3->rrec.length)
+     return 0; /* silently discard */
+ hbtype = *p++;
+ n2s(p, payload);
+ if (1 + 2 + payload + 16 > s->s3->rrec.length)
+     return 0; /* silently discard per RFC 6520 sec. 4 */
+ pl = p;
+
+ if (hbtype == TLS1_HB_REQUEST)
+     { unsigned char *buffer, *bp;

OpenSSL source code
```
## Fun Stats about Threats

### Verizon 2011 Data Breach Investigations Report

Table 8. Top 15 Threat Action Types by number of breaches and number of records

<table>
<thead>
<tr>
<th>Category</th>
<th>Threat Action Type</th>
<th>Short Name</th>
<th>Breaches</th>
<th>Records</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Malware</td>
<td>Send data to external site/entity</td>
<td>SNDATA</td>
<td>297</td>
<td>1,729,719</td>
</tr>
<tr>
<td>2 Malware</td>
<td>Backdoor (allows remote access/control)</td>
<td>MALBAK</td>
<td>294</td>
<td>2,065,001</td>
</tr>
<tr>
<td>3 Hacking</td>
<td>Exploitation of backdoor or command and control channel</td>
<td>HAKBAK</td>
<td>279</td>
<td>1,751,530</td>
</tr>
<tr>
<td>4 Hacking</td>
<td>Exploitation of default or guessable credentials</td>
<td>DFCRED</td>
<td>257</td>
<td>1,169,300</td>
</tr>
<tr>
<td>5 Malware</td>
<td>Keylogger/Form-grabber/Spyware (capture data from user activity)</td>
<td>KEYLOG</td>
<td>250</td>
<td>1,538,680</td>
</tr>
<tr>
<td>6 Physical</td>
<td>Tampering</td>
<td>TAMPER</td>
<td>216</td>
<td>371,470</td>
</tr>
<tr>
<td>7 Hacking</td>
<td>Brute force and dictionary attacks</td>
<td>BRUTE</td>
<td>200</td>
<td>1,316,588</td>
</tr>
<tr>
<td>8 Malware</td>
<td>Disable or interfere with security controls</td>
<td>DISABL</td>
<td>189</td>
<td>736,884</td>
</tr>
<tr>
<td>9 Hacking</td>
<td>Footprinting and Fingerprinting</td>
<td>FTPRINT</td>
<td>185</td>
<td>720,129</td>
</tr>
<tr>
<td>10 Malware</td>
<td>System/network utilities (PsTools, Netcat)</td>
<td>UTILITY</td>
<td>121</td>
<td>1,098,643</td>
</tr>
<tr>
<td>11 Misuse</td>
<td>Embezzlement, skimming, and related fraud</td>
<td>EMBZZL</td>
<td>100</td>
<td>37,229</td>
</tr>
<tr>
<td>12 Malware</td>
<td>RAM scraper (captures data from volatile memory)</td>
<td>RAMSCR</td>
<td>95</td>
<td>606,354</td>
</tr>
<tr>
<td>13 Hacking</td>
<td>Use of stolen login credentials</td>
<td>STLCRED</td>
<td>79</td>
<td>817,159</td>
</tr>
<tr>
<td>14 Misuse</td>
<td>Abuse of system access/privileges</td>
<td>ABUSE</td>
<td>65</td>
<td>22,364</td>
</tr>
<tr>
<td>15 Social</td>
<td>Solicitation/Bribery</td>
<td>BRIBE</td>
<td>59</td>
<td>23,361</td>
</tr>
<tr>
<td><strong>Honorable Mention at #16</strong></td>
<td><strong>Hacking</strong> (SQL Injection)</td>
<td>SQLINJ</td>
<td>54</td>
<td>933,157</td>
</tr>
</tbody>
</table>

*Source: Verizon 2011 Data Breach Investigations Report*
Fun Stats about Threats (2)

Figure 19. Malware infection vectors by percent of breaches within Malware

- Installed/Injected by remote attacker: 81%
- Web/Internet (auto-executed/drive-by/infection): 4%
- Web/Internet (user-executed or downloading): 3%
- Installed by other malware: 3%
- Network propagation: 2%
- Portable media & devices: <1%
- Coded into existing program/script (i.e., a logic bomb): <1%
- Unknown: 10%
2014 Cost of Data Breach Study: Global Analysis (Sponsored by IBM)

Company average cost: $3.5 million, 15% more than last year.

"Companies estimate that they will be dealing with an average of 17 malicious codes each month and 12 sustained probes each month. Unauthorized access incidents have mainly stayed the same and companies estimate they will be dealing with an average of 10 such incidents each month."
What is a Cloud?
Cloud Infrastructure and Virtualization

Common preconception: Virtualization = Isolation = Security
Hacking the Cloud (Amazon EC2)

"Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", Ristenpart et. al., 2009.

1. How to find out where the target is located?
2. How to be co-located with the target in the same (physical) machine?
3. How to gather information about the target?
(1) Mapping the Cloud

Using IP addresses

100 vms with Account A. After 39 hours, 100 vms with Account B.
(2) Determining co-residency

Using RTT (Round Trip Time)

Co-resident: 0.242 ms — Otherwise: [0.436-1.187] ms
(3) Placing co-resident Virtual Machine

How to be co-located with the target in the same machine?

**Brute-force strategy**
1. Launch multiples VMs (e.g., 100+)
2. Determine co-residency using RTT
   - Success rate: 8.4%

**Smarter strategy**
1. Launch ”just after” the target
2. Determine co-residency using RTT
   - Success rate: 40.0%
(4) Exploiting co-residency

Same physical machine = same hardware

- DoS attack
- Traffic rate
- Keystroke timing
- Side-channels
  - Measure latency of cache loads
My Thesis

How to help the user to **specify** his security requirements?

How to **automatically enforce** those security requirements?
Questions?