Lessons Learned from Physical Tamper-Response Applied to Client Devices

SESSION ID: MBS-F01

Ryan Lackey
Founder and CEO
CryptoSeal. Inc.
@octal @cryptoseal

Eric Michaud
CEO
Rift Recon, inc.
@ericmichaud @riftrecon
Overview

- What is tampering
- Who/what is vulnerable and where?
- Specific countermeasures
- Framework to evaluate countermeasures
- Lessons learned
Tampering: The “Evil Maid”
Security is like a layer-cake…
…Take out the foundations for house of fail
Attacks on the hardware substrate

- Attacks depending on **physical access**
- Bypass many conventional software security measures
- Hardware security measures relatively weak and outdated
- Invalidate assumptions about scope of system
Attacker can bypass software protections
Types of attacks

- Forensic imaging
- Hardware implants
- “Evil Maid”
Forensic Imaging
Hardware Implants
The “Evil Maid”

Lemme borrow some scissors.
Tampering: In the real world
Major targets

- Laptops
- Cellphones
- Tablets and other electronics
- Non-electronics
Travel is a major vulnerability

- Increased exposure
- Less defense
- Potentially different laws
International Borders
International Borders
Hotels
Luggage
But not only travel

- Unattended offices
- “Interdiction”
- Journalists
- Search incident to arrest
Conventional security measures are a baseline

- Screenlockers/access control
- Full disk encryption
- Transport encryption for traffic
- Virtual private networks
- (Mobile) device management
- Backups, user training, …
Many vendors of many products
Travel security policies

- Minimize what you take
- Pre and post trip wipe
- “Download-it-there”
- Dedicated travel pool of equipment
Physical security

- Difficult in travel environments
- Generally ineffective against powerful (State) threats
- Expensive to maintain
- Insider threats
Hotel safes
Door locks
Under the door tool
After-hours access
Government solutions
Tamper-evidence and Tamper-response
Passive tamper evidence vs. active tamper response

- Passive
  - Seals
  - Stickers

- Active
  - “Trusted Computing”
  - Smartcards
  - HSM
Seals
Seals
Stickers and improvised seals
Passive seals

- Low cost
- Relatively unobtrusive to users
- Infrequently verified
- Can be defeated vs. field verification
DOE VAT Seal Results

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mean</th>
<th>Median</th>
</tr>
</thead>
<tbody>
<tr>
<td>defeat time for 1 person</td>
<td>1.4 mins</td>
<td>43 secs</td>
</tr>
<tr>
<td>cost of tools and supplies</td>
<td>$78</td>
<td>$5</td>
</tr>
<tr>
<td>marginal cost of attack</td>
<td>62¢</td>
<td>9¢</td>
</tr>
<tr>
<td>time to devise successful attack</td>
<td>2.3 hrs</td>
<td>12 mins</td>
</tr>
</tbody>
</table>

- Half of these seals are in use for "critical" opportunities.
- At least 19% are in use and under consideration for nuclear safeguards.
Forensic analysis
Active tamper-response: TCG/Trusted Computing
PIN processors
Smartcards
Hardware Security Modules
Threats
Threats
Active tamper-response drawbacks

- Expensive
- Specialty hardware
- Can be bypassed, don’t protect entire computing device
- Impractical for “office automation” uses
Automatic verification of seals
Active seals exist
Active seal drawbacks

- Expensive
- Specialty hardware
- Still highly vulnerable
- Generally designed for large cargo containers
Smartphone validation of seals
Smartphone software validation of passive seals

- Inexpensive and practical: “Blink comparison”
- Existing hardware (cellphones running iOS or Android)
- Non-suspicious hardware (“arrested in China for spying”)
- Applicable to a range of hardware
- Many difficult technical challenges (image processing, coatings, integration with enterprise IT)
Lessons Learned
Major lessons of 2013

- Users in the field are exposed to many threats
- Must be unobtrusive to users, but not “click yes to proceed”
- “Travel naked”: equipment setup in-country
- Separate infrastructure from low-threat defaults
- Seal technology, especially when machine-verified, very promising
2014 goals

- Integration of the machine-verification technique into enterprise IT tools (VPN, mail, DLP, …)
- Improvement of seal coatings (pearlescent paint? anti-tamper?)
- Production-quality client software
- Application of smartphone validation to non-computer seals
Contact Us

- Eric Michaud <eric@riftrecon.com> www.riftrecon.com
- Ryan Lackey <ryan@cryptoseal.com> www.cryptoseal.com