RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

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

RIFT RECON

Tampering: The “Evil Maid”

Security is like a layer-cake…

RIFT RECON

…Take out the foundations for house of fail

RIFT RECON

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- Hardware security measures relatively weak and outdated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

RIFT RECON

Attacker can bypass software protections

RIFT RECON

Types of attacks

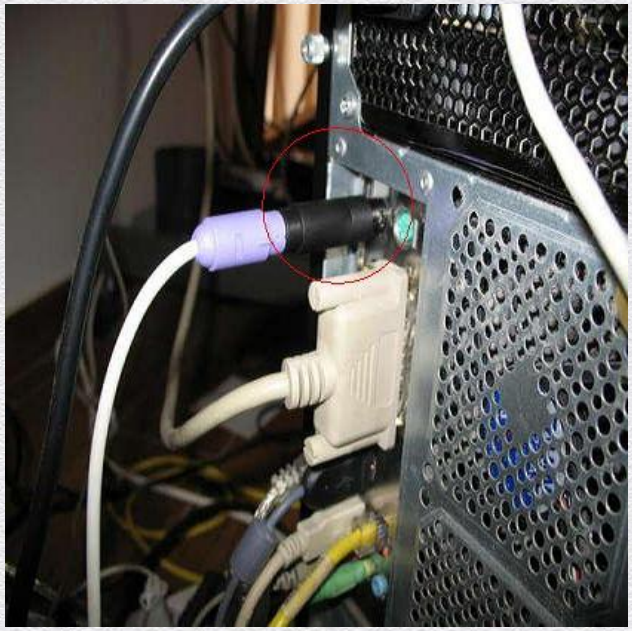
- Forensic imaging
- Hardware implants
- “Evil Maid”

RIFT RECON

Forensic Imaging

RIFT RECON

Hardware Implants



RIFT RECON

The “Evil Maid”

RIFT RECON

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Tampering:
In the real world

Major targets

- Laptops
- Cellphones
- Tablets and other electronics
- Non-electronics

RIFT RECON

Travel is a major vulnerability

- Increased exposure
- Less defense
- Potentially different laws

RIFT RECON

International Borders

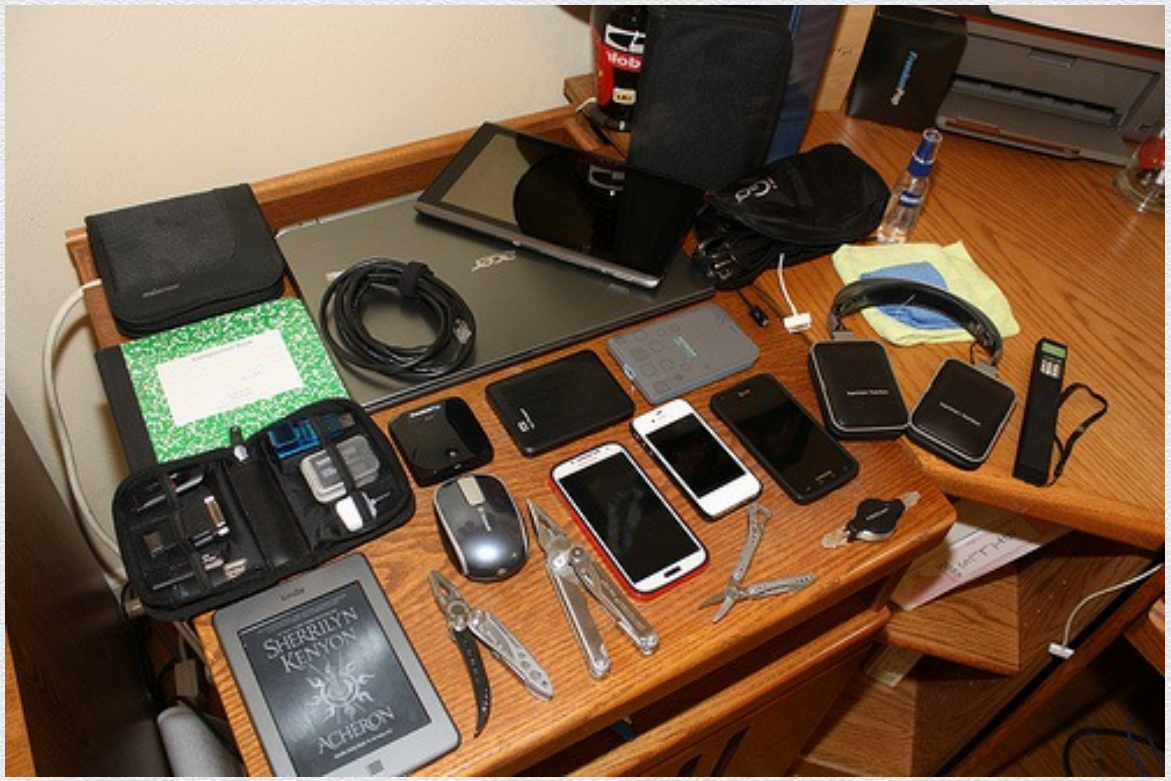
RIFT RECON

International Borders

Hotels

RIFT RECON

Luggage



RIFT RECON

But not only travel

- Unattended offices
- “Interdiction”
- Journalists
- Search incident to arrest

RIFT RECON

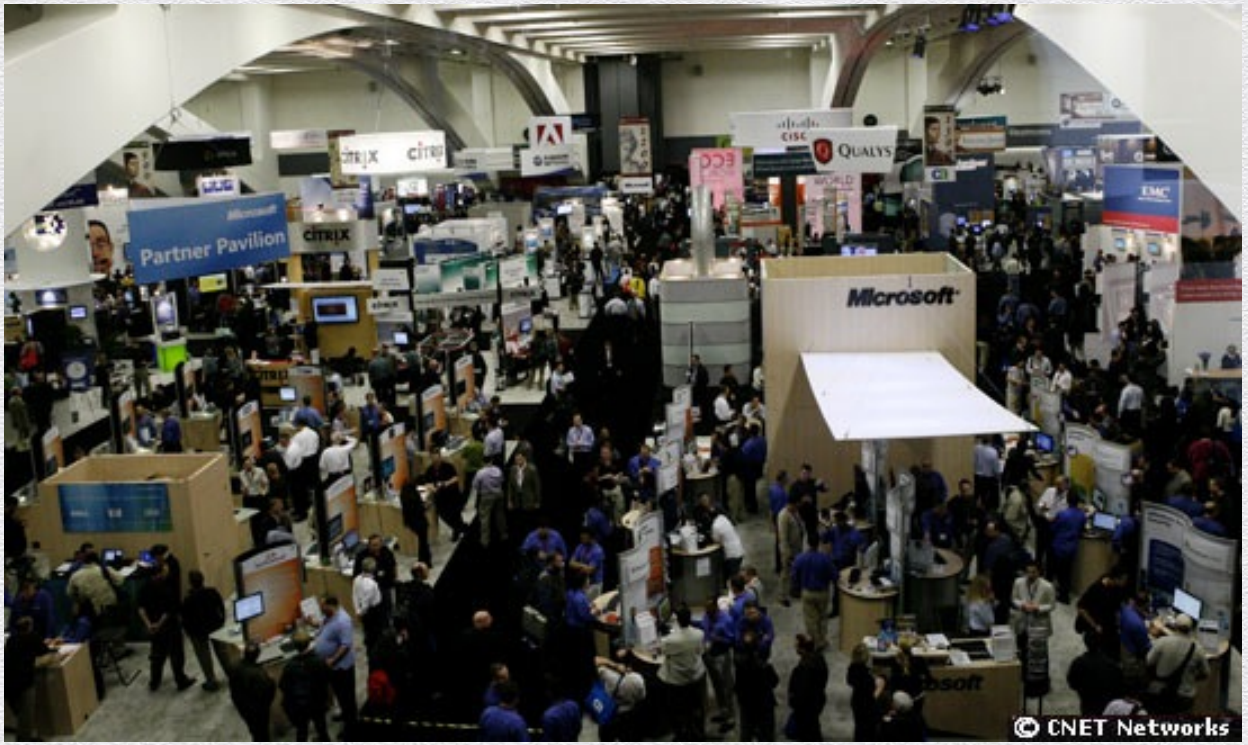
Countermeasures

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, …

RIFT RECON

Many vendors of many products



RIFT RECON

Travel security policies

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

RIFT RECON

Physical security

- Difficult in travel environments
- Generally ineffective against powerful (State) threats
- Expensive to maintain
- Insider threats

RIFT RECON

Hotel safes

RIFT RECON

Door locks

RIFT RECON

Under the door tool

RIFT RECON

After-hours access

RIFT RECON

Government solutions

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Tamper-evidence and Tamper-response

Passive tamper evidence vs. active tamper response

- Passive
  - Seals
  - Stickers
- Active
  - “Trusted Computing”
  - Smartcards
  - HSM

RIFT RECON

Seals

Seals

RIFT RECON

Stickers and improvised seals

Passive seals

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

RIFT RECON

DOE VAT Seal Results

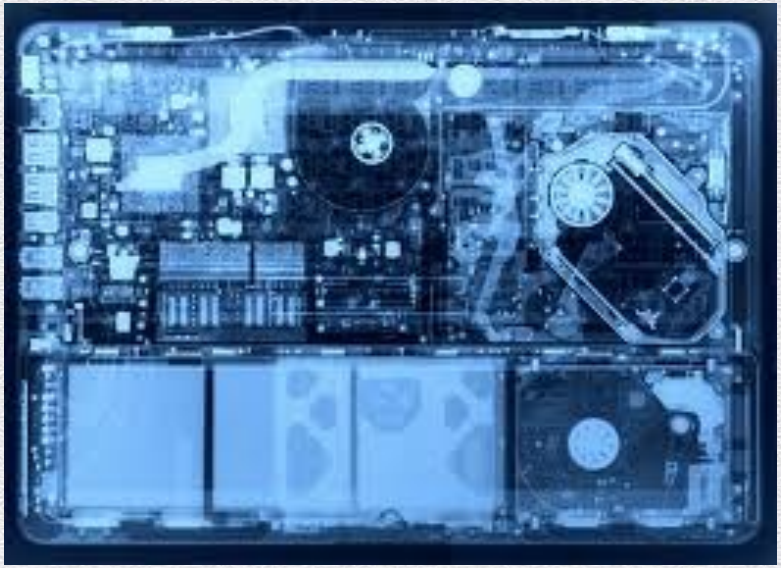
Results for 244 Seals

Parameter	Mean	Median
defeat time for 1 person	1.4 mins	43 secs
cost of tools and supplies	$78	$5
marginal cost of attack	62¢	9¢
time to devise successful attack	2.3 hrs	12 mins

- Half of these seals are in use for "critical" opportunities.
- At least 19% are in use and under consideration for nuclear safeguards.

RIFT RECON

Forensic analysis



RIFT RECON

Active tamper-response: TCG/Trusted Computing

TRUSTED COMPUTING GROUP™

RIFT RECON

PIN processors

RIFT RECON

Smartcards

RIFT RECON

Hardware Security Modules

RIFT RECON

Threats

RIFT RECON

Threats

RIFT RECON

Active tamper-response drawbacks

- Expensive
- Specialty hardware
- Can be bypassed, don’t protect entire computing device
- Impractical for “office automation” uses

RIFT RECON

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Automatic verification of seals

Active seals exist

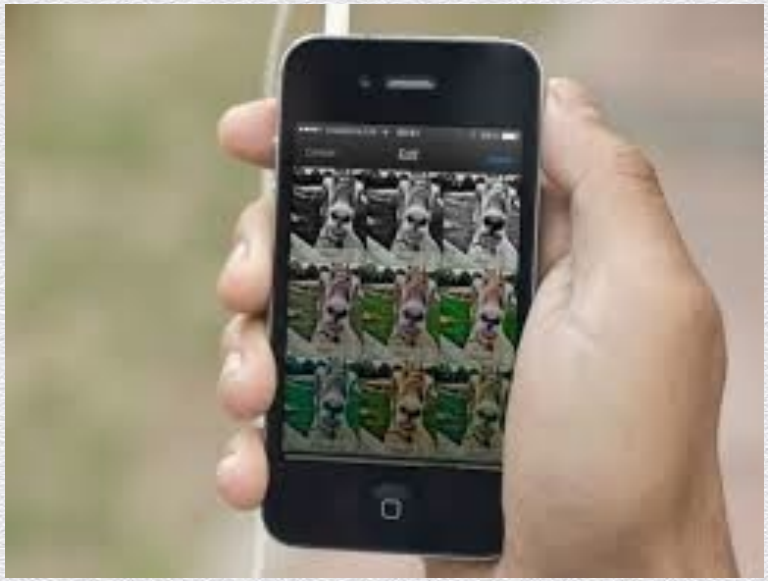
RIFT RECON

Active seal drawbacks

- Expensive
- Specialty hardware
- Still highly vulnerable
- Generally designed for large cargo containers

RIFT RECON

Smartphone validation of seals



RIFT RECON

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)

RIFT RECON

RIFT RECON

RIFT
RECON

#RSAC

RSACONFERENCE2014

RIFT
RECON

#RSAC

RSACONFERENCE2014

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

RIFT RECON

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

RIFT RECON

Contact Us

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

RIFT RECON