Bypassing Self-Encrypting Drives (SED) in Enterprise Environments

black hat EUROPE 2015

Daniel Boteanu
Kevvie Fowler

November 12th, 2015

Who are we ?

Daniel Boteanu

- Forensic Technology and eDiscovery, KPMG Canada
- M.Eng., M.Sc. – Information Security
- Background
  - IT Security (MCP, MCTS, CSSLP)
  - Penetration Testing (GPEN)
  - Forensic Technology (CHFI, GCFA, EnCE)
  - Security Research
- Organiser of nsec.io – 48h CTF + InfoSec conference

Who are we ?

Kevvie Fowler, GCFA, CISSP

- Partner, National Cyber Forensics Leader, KPMG Canada
- Author and co-author to multiple Security and Forensic books
- Developer of database forensic tools
- SANS Lethal Forensicator

Agenda

What are SEDs ?

Typical SED Enterprise Deployments

Attack Scenarios

- What / How / Demo
- Mitigations

Detection of Past Exploitation

Real-World Implications

What are SEDs ?

The state of data encryption

- Encryption related vulnerabilities have made recent headlines
  - Open-source & commercial encryption software
- Concerns over governments ability to bypass data encryption
- Public breach disclosures involving encrypted data
- SED's are referred to by many as a solution to data loss problems

http://www.computerweekly.com/feature/Self-encrypting-drives-SED-the-best-kept-secret-in-hard-drive-encryption-security

What are SEDs ?

Classical Full Disk Encryption (FDE)

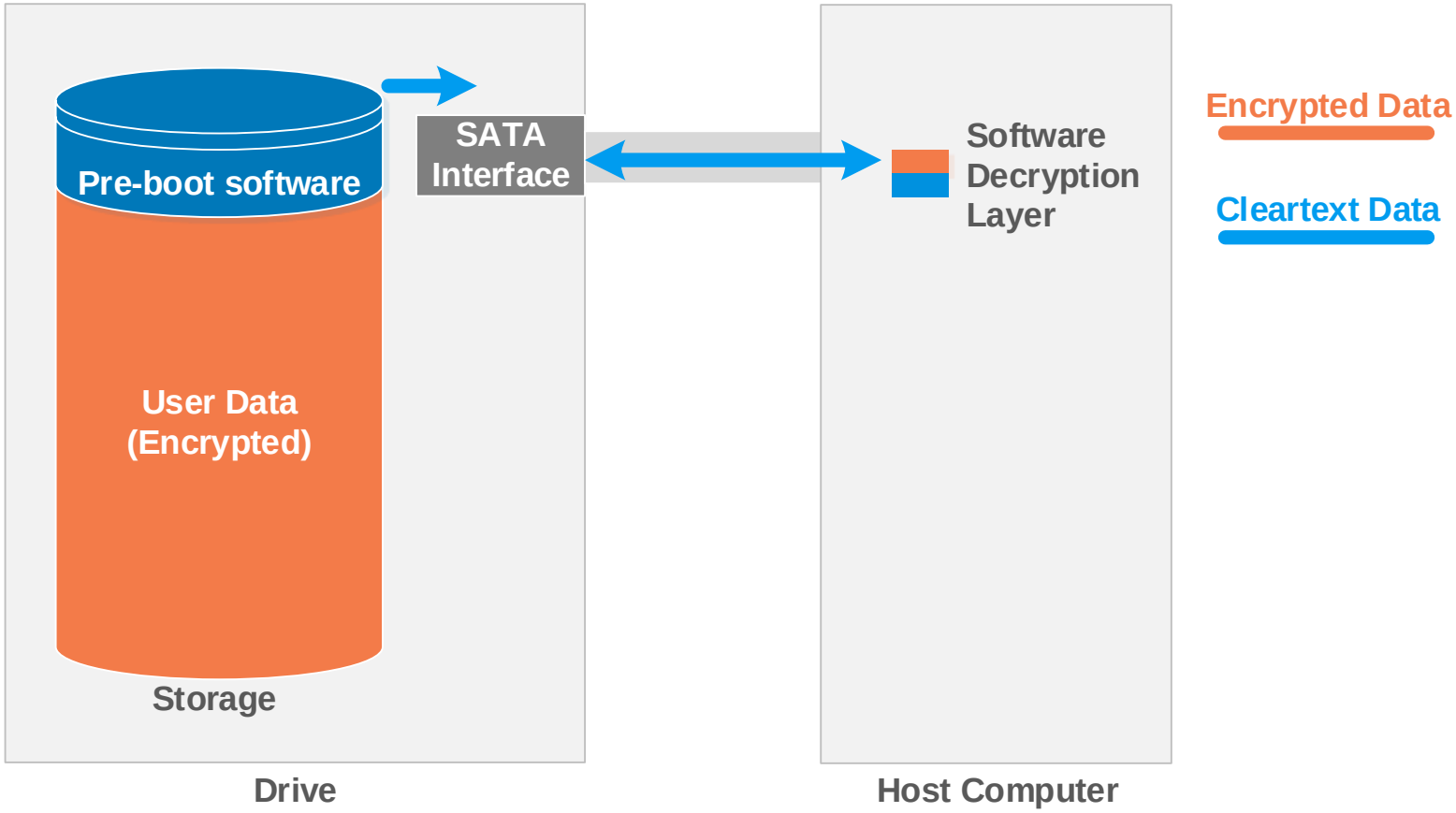
- Software-based
- Encryption performed by the OS
- Advantages
  - Hardware agnostic
  - Transparent for applications
- Disadvantages
  - Slow in-place encryption
  - Performance overhead*

*Hardware acceleration possible (ex: AES-NI)

What are SEDs ?

Classical Full Disk Encryption (FDE)

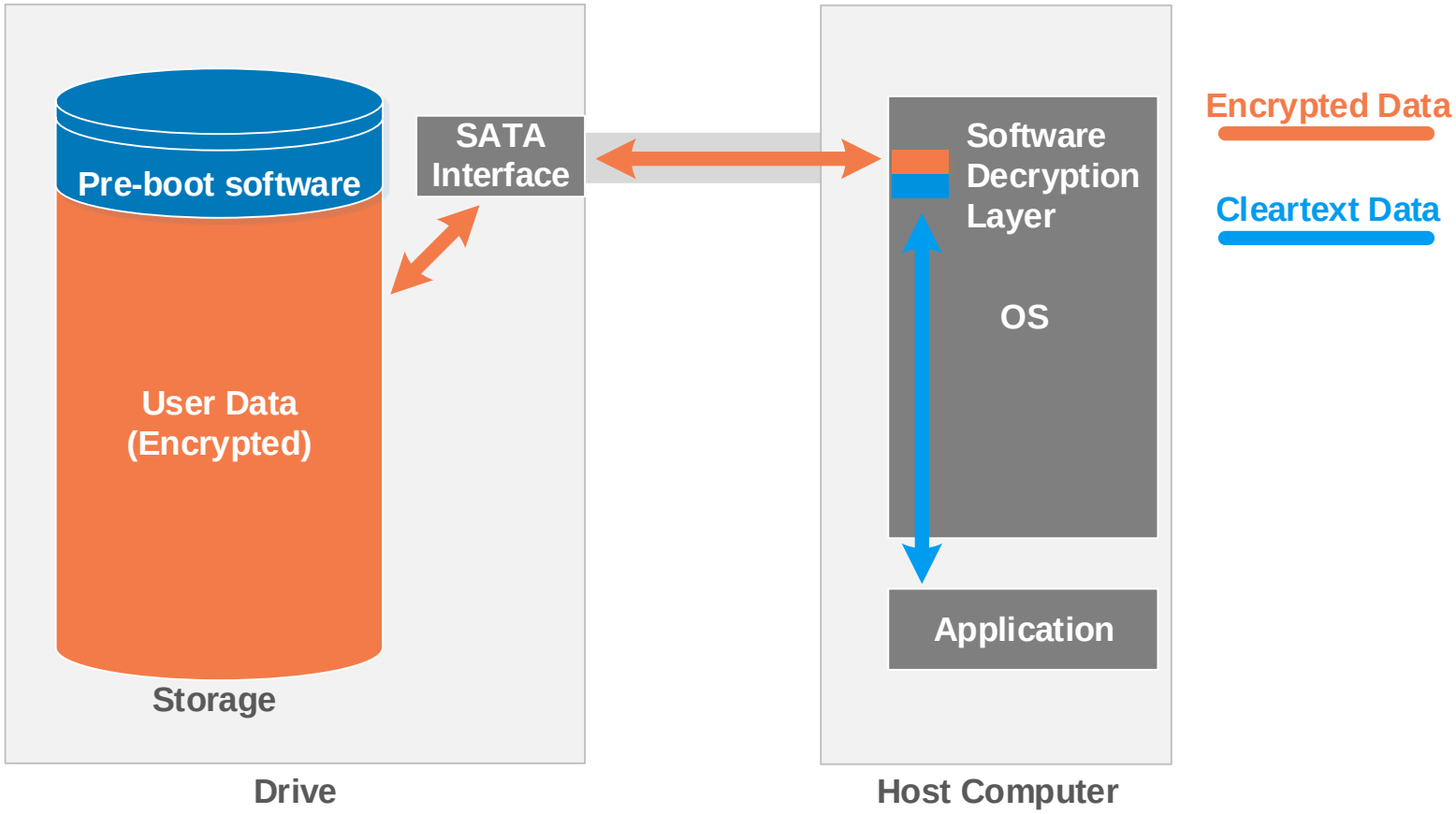
- Boot process



What are SEDs ?

Classical Full Disk Encryption (FDE)

- Accessing encrypted data



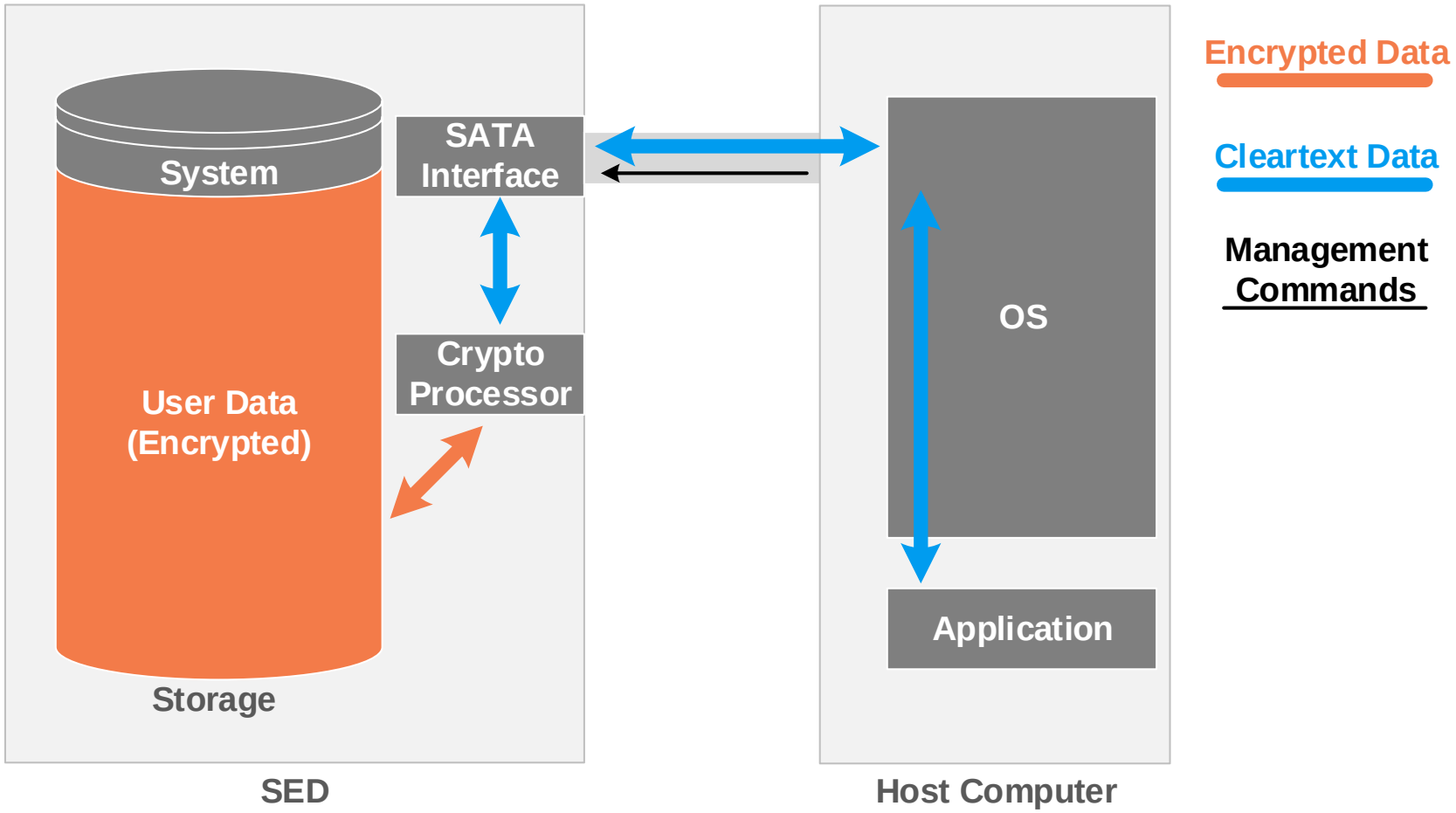
What are SEDs ?

Self-Encrypting Drives (SED)

- Hardware-based encryption
- Encryption performed by the drive controller
- Advantages
  - No performance overhead
  - Instant in-place encryption
  - Transparent for applications and OS
- Requirements
  - Compatible motherboard + drive + management component
- Disadvantages ?

What are SEDs ?

Self-Encrypting Drive (SED)



What are SEDs ?

SED Operating Modes

1. ATA Security
   - Subset of ATA Command Set
   - Managed by BIOS / EFI or low-level drive software (ex: hdparm)
   - Encryption schemes non-standardized
   - Generally
     - Data encrypted with Media Encryption Key (MEK)
     - MEK encrypted with Key Encryption Key (KEK) and stored on drive
     - KEK generated from ATA User Password

What are SEDs ?

SED Operating Modes

2. Trusted Computing Group (TCG) Storage Security Subsystem Class : **Opal**
   - New commands defined by the Opal standard
   - Managed by software
   - Pre-boot authentication software available through MBR shadowing
   - User Data always encrypted
     - Data encrypted with Media Encryption Key (MEK)
     - MEK encrypted with Key Encryption Key (KEK) and stored on drive
     - KEK generated from user password/management software

What are SEDs ?

SED Operating Modes

3. Microsoft Encrypted Drive (eDrive)
   - Opal + IEEE 1667 + UEFI 2.3.1
   - Managed by Bitlocker
   - Operation similar to Opal
4. Custom / Proprietary implementation
   - Typically USB hard drives and thumb drives
   - Managed by software or hardware interface (ex: pinpad)

Typical SED Enterprise Deployments

SED Operating Mode

- Opal

BIOS Lockdown

- Sometimes

Available Power States

- S0 – On
- S3 – Sleep
- S4 – Hibernate
- S5 – Off

Previous Work

Software Encryption

- Recovering encryption key (ex: Cold Boot, Side-channels)
- Bypass Windows authentication (ex: DMA, BHEU15?)
- Evil Maid Attack

ATA Security

- Hot Plug Attack (Müller et al)

Custom Implementation

- Targeted research & vulnerabilities (ex: Alendal et al., SySS)

Previous Work

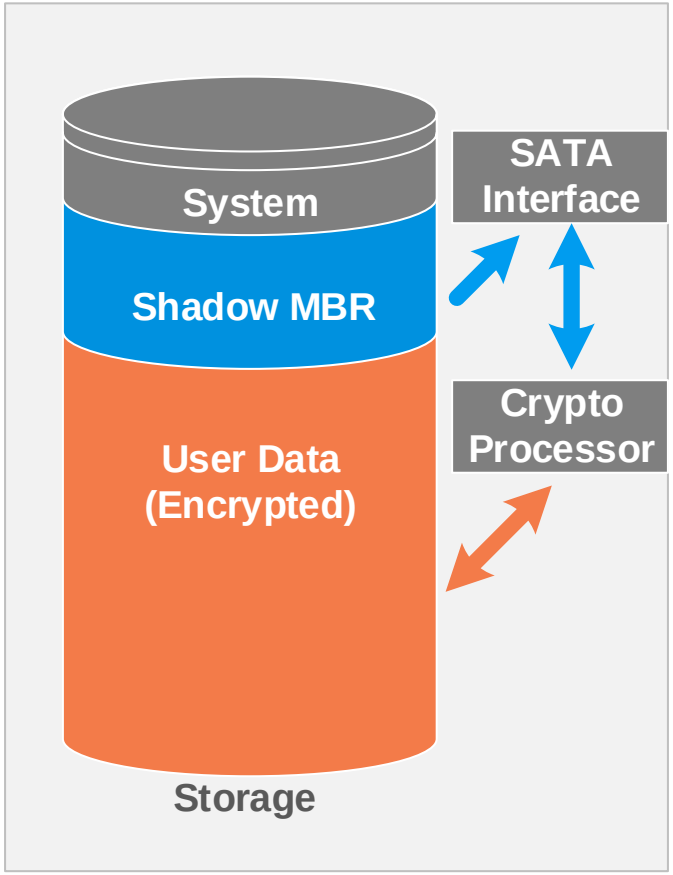
Our research

- Research on SEDs in Opal & eDrive modes
- Industry-wide problem
- Typical SED enterprise deployments
- Focus on laptops - applicable to other devices

Opal SED

Storage Contents

- System Area
  - TCG tables (encrypted MEK, settings, etc.)
- Shadow MBR
  - Pre-boot environment, cleartext
- User Data Area
  - Always encrypted, with MEK
  - Potential for multiple zones with different keys

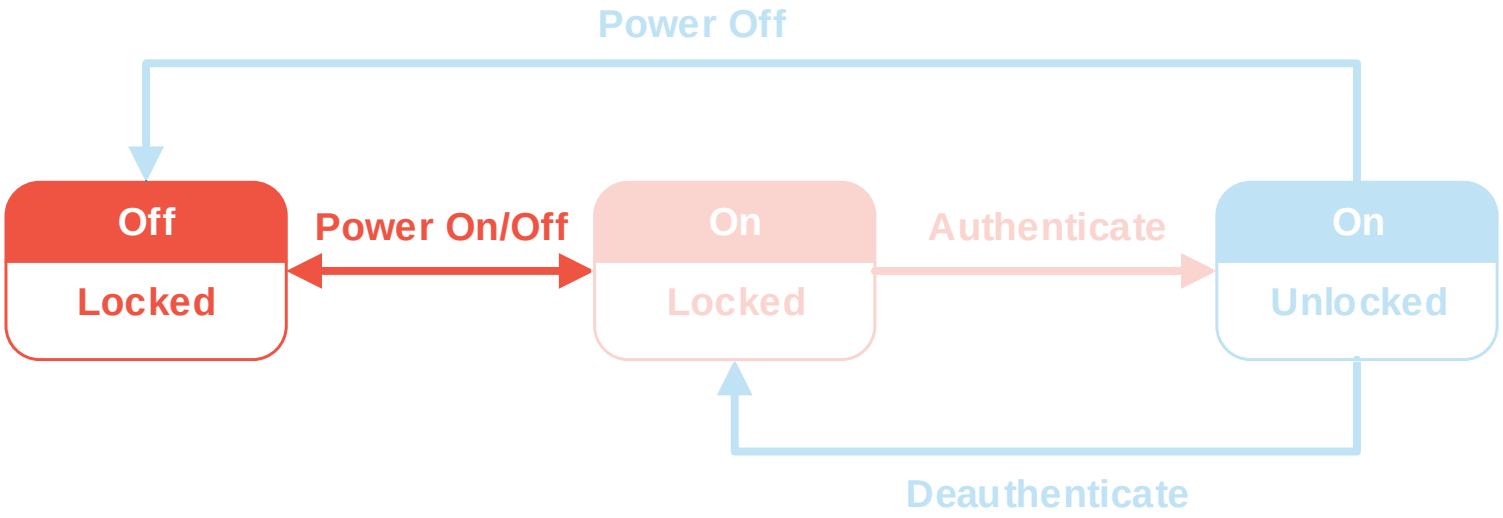


Opal SED

Opal SED – Drive States

Off – Locked

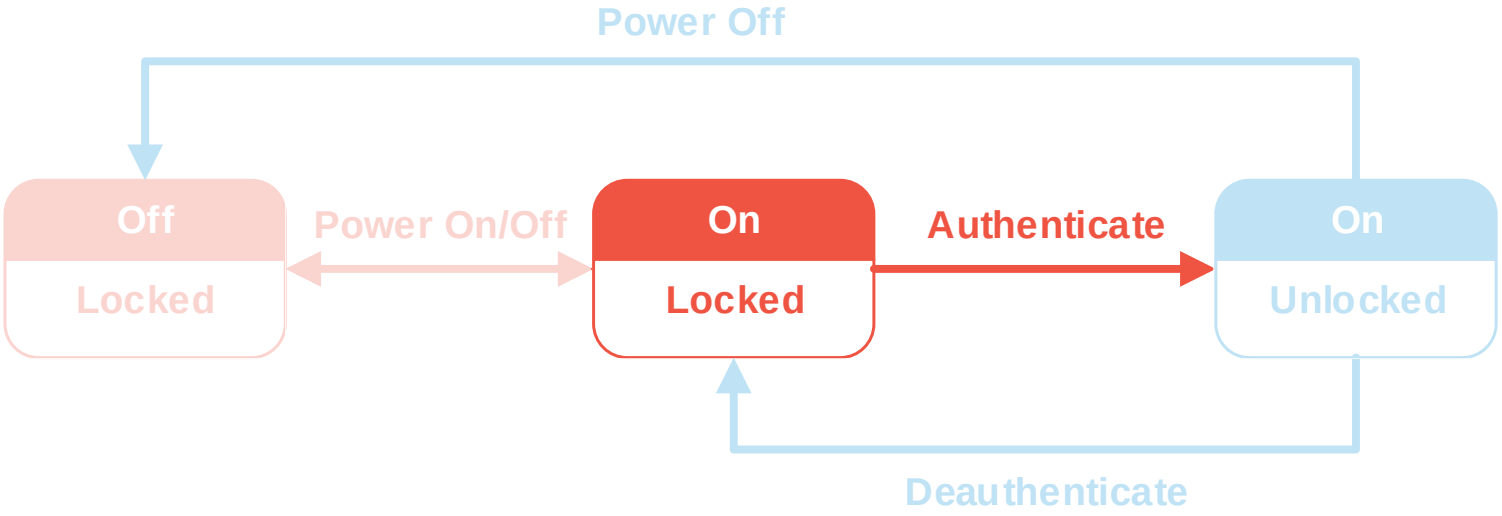
- Drive always gets locked when power cycled



Opal SED – Drive States

On – Locked

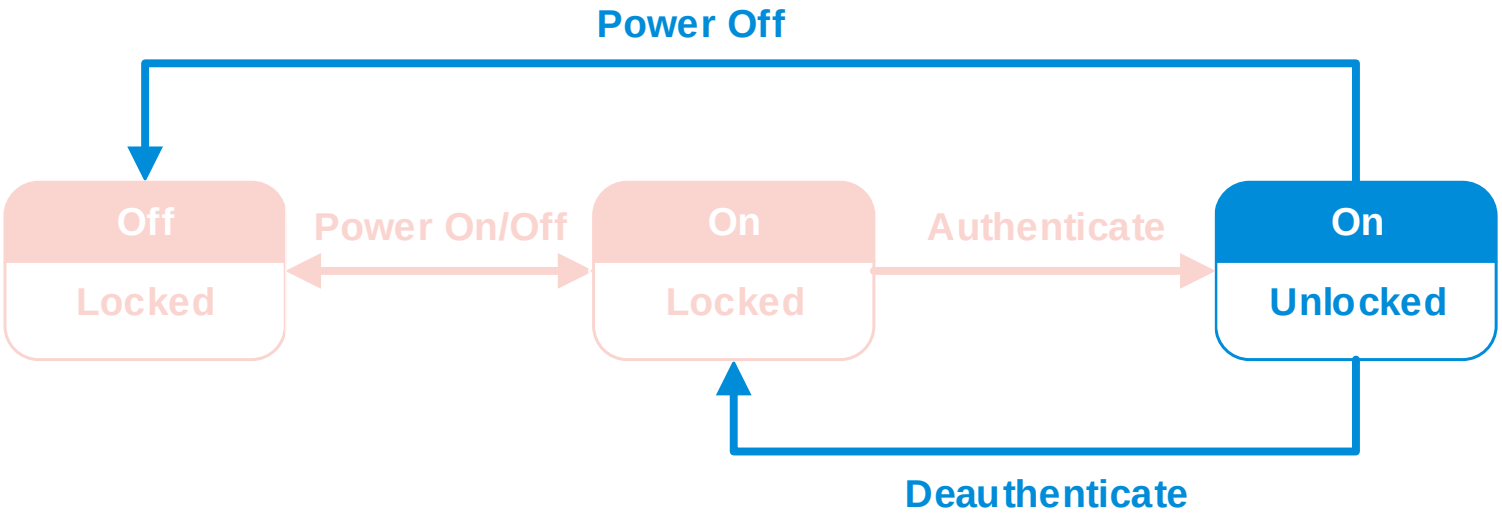
- Only Shadow MBR is visible, read-only
- Boot process
  - Pre-boot environment loads, user authenticates
  - Drive decrypts MEK, triggers boot from User Data



Opal SED – Drive States

On – Unlocked

- Encryption transparent to OS
- Only User Data is visible
- **Drive remains Unlocked until power cycle or Deauth**



Opal Specs version 2.01

2.1 Opal SSC Use Cases and Threats

Protect the confidentiality of stored user data against unauthorized access once it leaves the owner's control (involving a power cycle and subsequent deauthentication)

Tested Configurations

Combination of

- Drives
  - Samsung 850 Pro, SSD, 1 TB, P/N MZ7KE1T0
  - Samsung PM851, SSD, 256GB, P/N MZ7TE256HMHP – 000L7
  - Seagate ST500LT015, HDD, 500 GB, P/N 1DJ142-500
  - Seagate ST500LT025, HDD, 500 GB, P/N 1DH142-500
- Laptops
  - Lenovo ThinkPad T440s, BIOS version 2.32
  - Lenovo ThinkPad W541, BIOS version 2.21
  - Dell Latitude E6410, BIOS version A16
  - Dell Latitude E6430, BIOS version A16

Tested Configurations

Combination of

- Management Software
  - Microsoft Bitlocker eDrive, version 8.1 Enterprise, Build 9600
  - Wave EMBASSY Security Center (ESC), version 2.11.1
  - WinMagic SecurDoc, version 6.4.0.117-HF1
- Laptop Power State
  - S0 – On
  - S3 – Sleep

Agenda

What are SEDs ?

Typical SED Enterprise Deployments

Attack Scenarios

- What / How / Demo
- Mitigations

Detection of Past Exploitation

Real-World Implications

Previous Work

Software Encryption

- Recovering encryption key (ex: Cold Boot, Side-channels)

★Bypass Windows authentication (ex: DMA, BHEU15?)

★Evil maid attack

★ **Also applicable to Opal and eDrive**

ATA Security

★Hot Plug Attack (Müller et al)

Custom Implementation

- Targeted research & vulnerabilities (ex: Alendal et al., SySS)

Attack Scenarios – Hot Plug Attack

Details

- Steps

	Drive State
1. If laptop is On (S0), put to Sleep (S3)	Off-Locked
2. Remove drive	Off-Locked
3. Install SATA data + power extension	Off-Locked
4. Wake up from Sleep (S3)	On-Locked
5. Management software unlocks drive	On-Unlocked
6. Switch SATA data to attacker machine	On-Unlocked

Attack Scenarios – Hot Plug Attack

Demo

Attack Scenarios – Hot Plug Attack

Vulnerable

- All 12 tested Opal & eDrive configurations

Not Vulnerable

- None

For ATA Security SEDs

- Müller et al. - modern Lenovo laptops not vulnerable
- Confirmed

Attack Scenarios – Hot Plug Attack

Mitigations

- Users: Power-off or Hibernate laptop when unattended
- IT Administrators: Disable Sleep Mode (S3)
  - Already recommended by some management software
- Laptop manufacturers: Detect drive unplug in Sleep Mode
  - Hard-reset on tamper
- SED manufacturers: Detect SATA data disconnect
  - Lock SED on tamper

Attack Scenarios

Hot Plug Attack

Forced Restart Attack

Attack Scenarios – Forced Restart Attack

Details

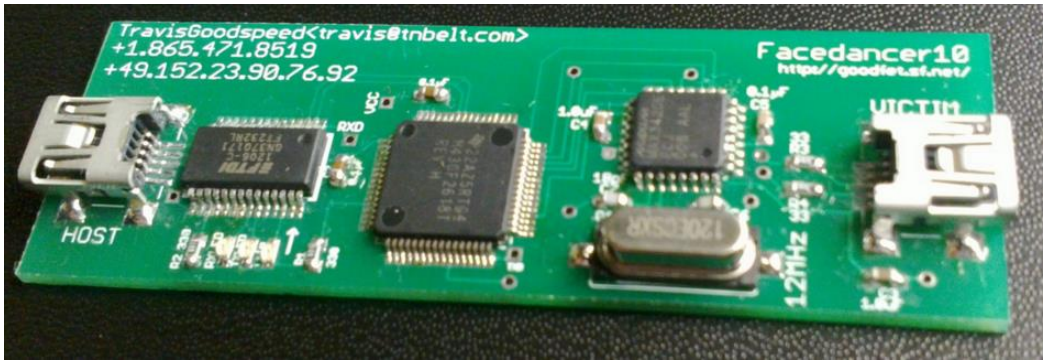
Steps	Drive State
1. If laptop is in Sleep (S3), wake up (S0)	**On-Unlocked**
2. Trigger soft-reset	**On-Unlocked**
3. Boot from alternative OS	**On-Unlocked**

Attack Scenarios – Forced Restart Attack

How to trigger soft-reset ?

By default, Windows soft-resets on BSOD

- Facedancer – umap – BH Asia 14

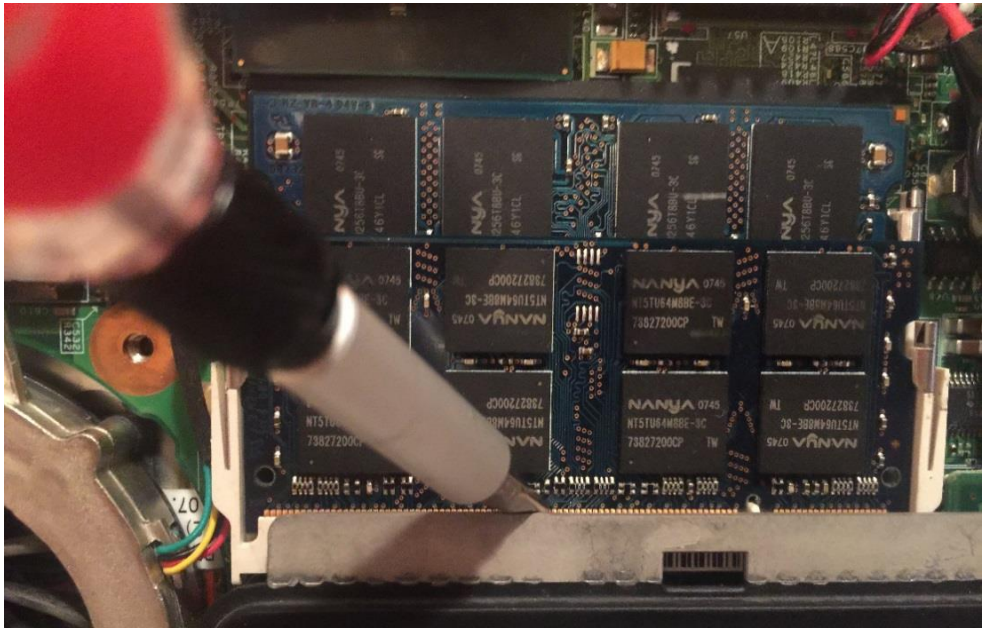


Attack Scenarios – Forced Restart Attack

How to trigger soft-reset ?

By default, Windows soft-resets on BSOD

- Facedancer
- Short memory pins



⚠ Potential hardware damage

Attack Scenarios – Forced Restart Attack

How to trigger soft-reset ?

By default, Windows soft-resets on BSOD

- Facedancer
- Short memory pins
- Unlucky hardware mix
- Keyboard – for testing

Attack Scenarios – Forced Restart Attack

Demo

using BSOD by Facedancer

Attack Scenarios – Forced Restart Attack

Vulnerable

- All 8 tested Opal configurations

Not Vulnerable

- Modern Lenovo laptops with eDrive SEDs

Attack Scenarios – Forced Restart Attack

Mitigations

- Users: Power-off or Hibernate laptop when unattended
- IT administrators: Disable automatic restart on BSOD
- IT administrators: Lock-down BIOS/EFI
  - Prevent boot from external media
- Laptop manufacturers: Power-cycle SED on restart
- OS developers: Reconsider fixing local access BSOD

Attack Scenarios

Hot Plug Attack

Forced Restart Attack

Hot Unplug Attack

Attack Scenarios – Hot Unplug Attack

Details

- Hot Plug Attack on steroids
- Bypasses potentially disabled Sleep (S3) or Tamper Detection
- Steps
  1. Expose SATA data and power pins

Drive State

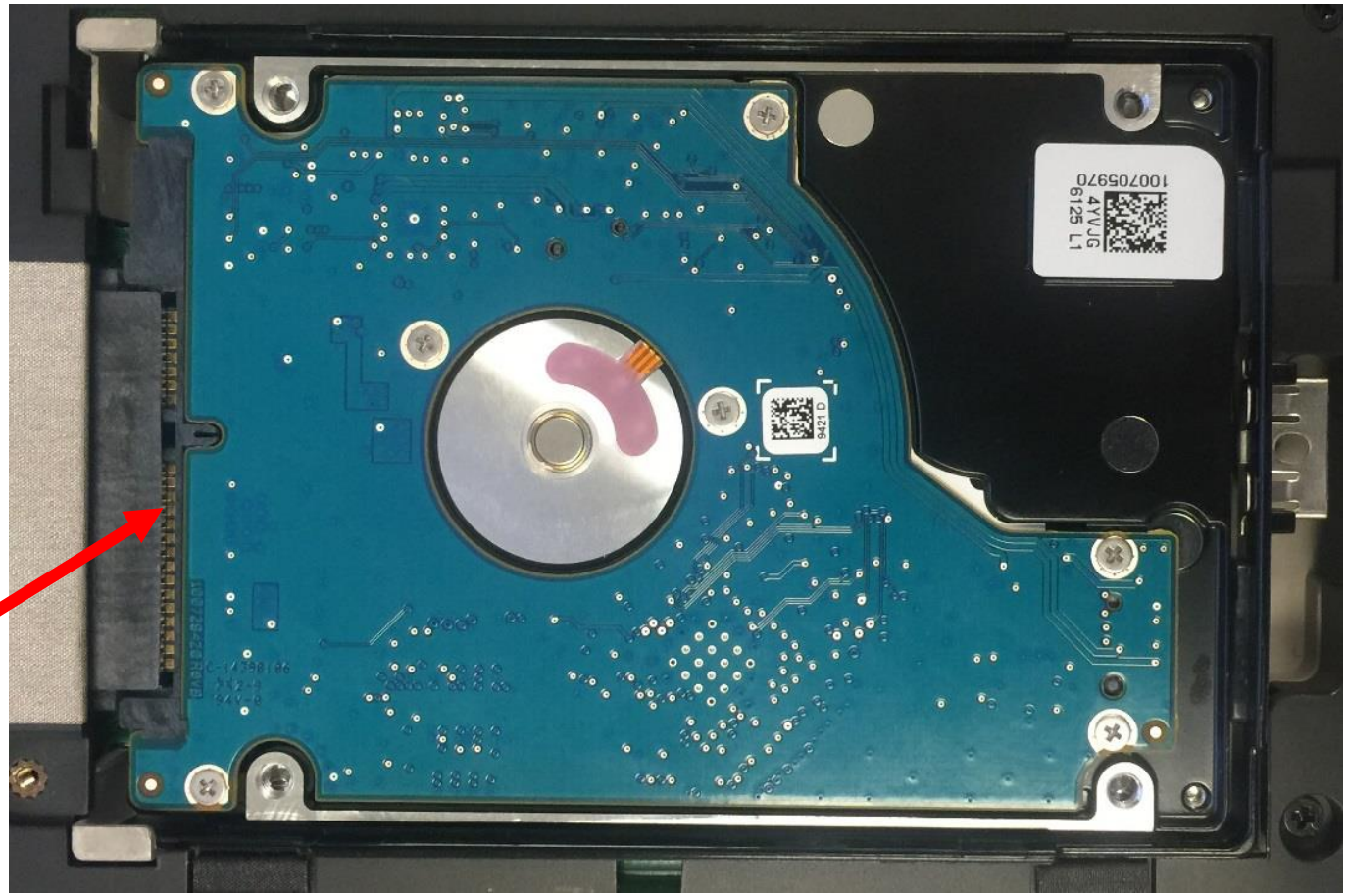
On-Unlocked

Attack Scenarios – Hot Unplug Attack

SED in laptop compartment

Attack Scenarios – Hot Unplug Attack

SED with SATA pins exposed



Attack Scenarios – Hot Unplug Attack

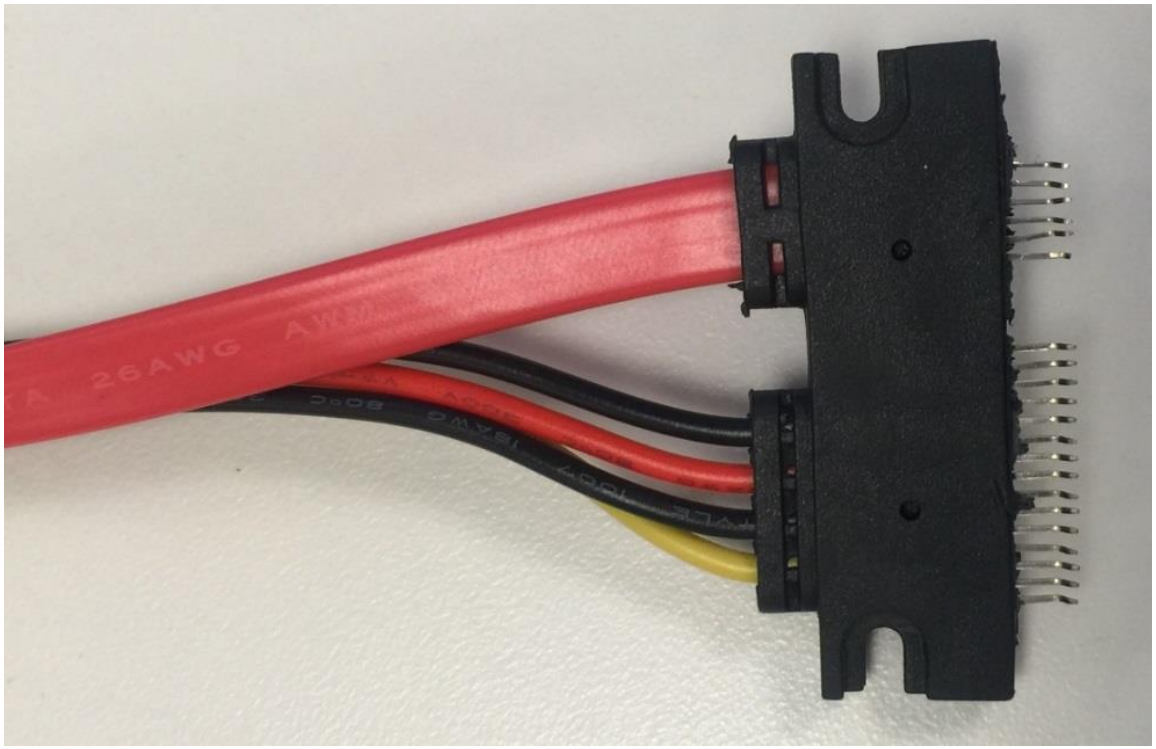
Hot Unplug Attack

- Hot Plug Attack on steroids
- Bypasses potentially disabled Sleep (S3) or Tamper Detection
- Steps

	Drive State
1. Expose SATA data and power pins	**On-Unlocked**
2. Force-supply SATA power on pins	**On-Unlocked**

Attack Scenarios – Hot Unplug Attack

SATA power and data* pins

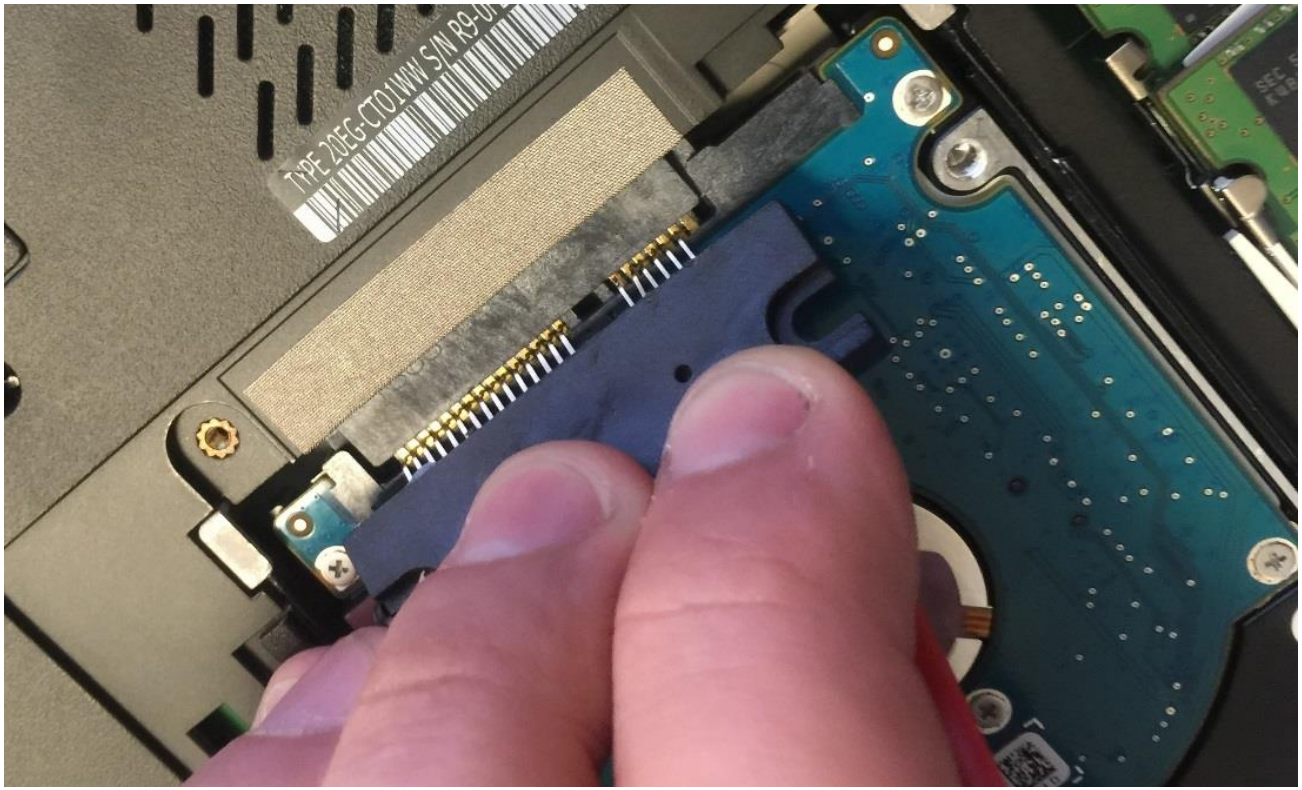


* Pin 1 (ground) broken by accident, no impact due to redundant Pin 4 and Pin 7

Attack Scenarios – Hot Unplug Attack

SED with forced-supplied power

- Only SATA power connected at the other end of extension



⚠ Potential hardware damage

Attack Scenarios – Hot Unplug Attack

Hot Unplug Attack

- Hot Plug Attack on steroids
- Bypasses potentially disabled Sleep (S3) or Tamper Detection

- Steps

	Drive State
1. Expose SATA data and power pins	**On-Unlocked**
2. Force-supply SATA power on pins	**On-Unlocked**
3. While maintaining power, remove drive	**On-Unlocked**
4. Connect SATA data to attacker machine	**On-Unlocked**

Attack Scenarios – Hot Unplug Attack

Vulnerable

- 1 tested eDrive configuration
- Expected all Opal and eDrive configurations to be vulnerable

Not Vulnerable

- None

Attack Scenarios – Hot Unplug Attack

Mitigations

- Users: Power-off or Hibernate laptop when unattended
- Laptop manufacturers: Detect drive enclosure opening
  - Power-cycle SED on tamper
- SED manufacturers: Detect SATA data disconnect
  - Lock SED on tamper

Attack Scenarios

Hot Plug Attack

Forced Restart Attack

Hot Unplug Attack

Key Capture Attack

Attack Scenarios

Key Capture Attack

- Theoretical, untested
- In Sleep Mode (S3), replace SED with tampered drive with custom firmware
  - Capture authentication commands
  - Replay authentication to SED
- Alternatively, sniff SATA bus for authentication commands

Responsible Disclosure

We disclosed findings with TCG on July 15th

- TCG agreed to disseminate info to all Storage Work Group members

Coordinated disclosure with CERT

- Assigned VU#631316 / CVE – pending assignment

Lenovo contacted us to discuss details and potential mitigations

Detection of Past Exploitation

Hot Plug/Unplug Attack

- Traces similar to power failure or forced power off

Forced Restart Attack

- BSOD error code (event logs, memory dump)
- Attacker can clean-up traces

Key Capture Attack

- Potentially no traces

Real-Word Implications

Yesterday's laptop risk

263 laptops stolen each year per organization

$49,256 in loss for each stolen laptop

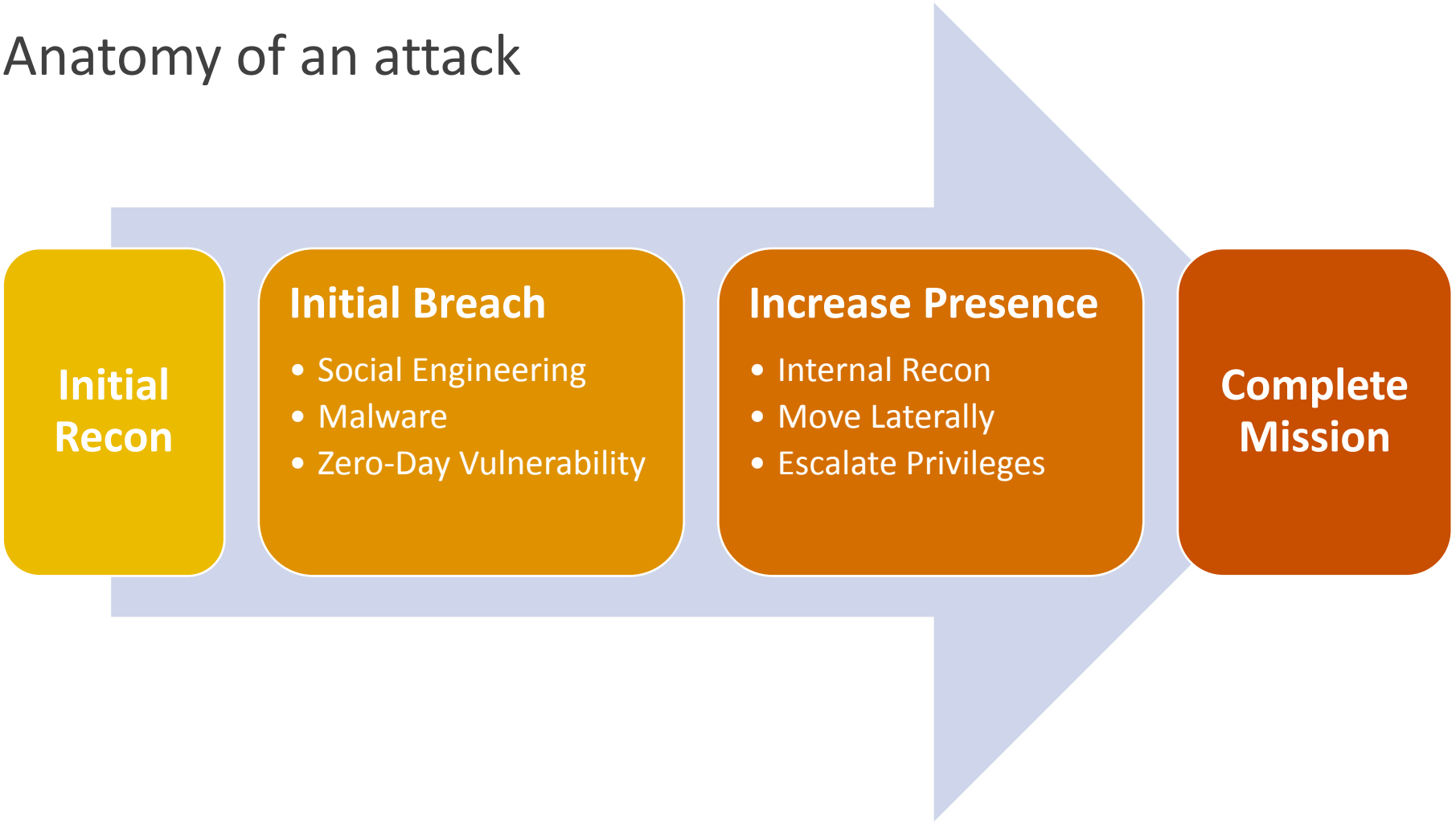
The SED bypass vulnerability and today's threat landscape increase laptop risk

- Increased number of laptop thefts and cost/impact per incident:
  - Size of disks and data stores
  - Value of sensitive information
  - Breach notification legislations
- Revisiting past laptop theft/loss incidents
- Increased number of criminals targeting laptops as part of an elaborate attack

Source: "The billion dollar lost laptop problem" Ponemon & Intel

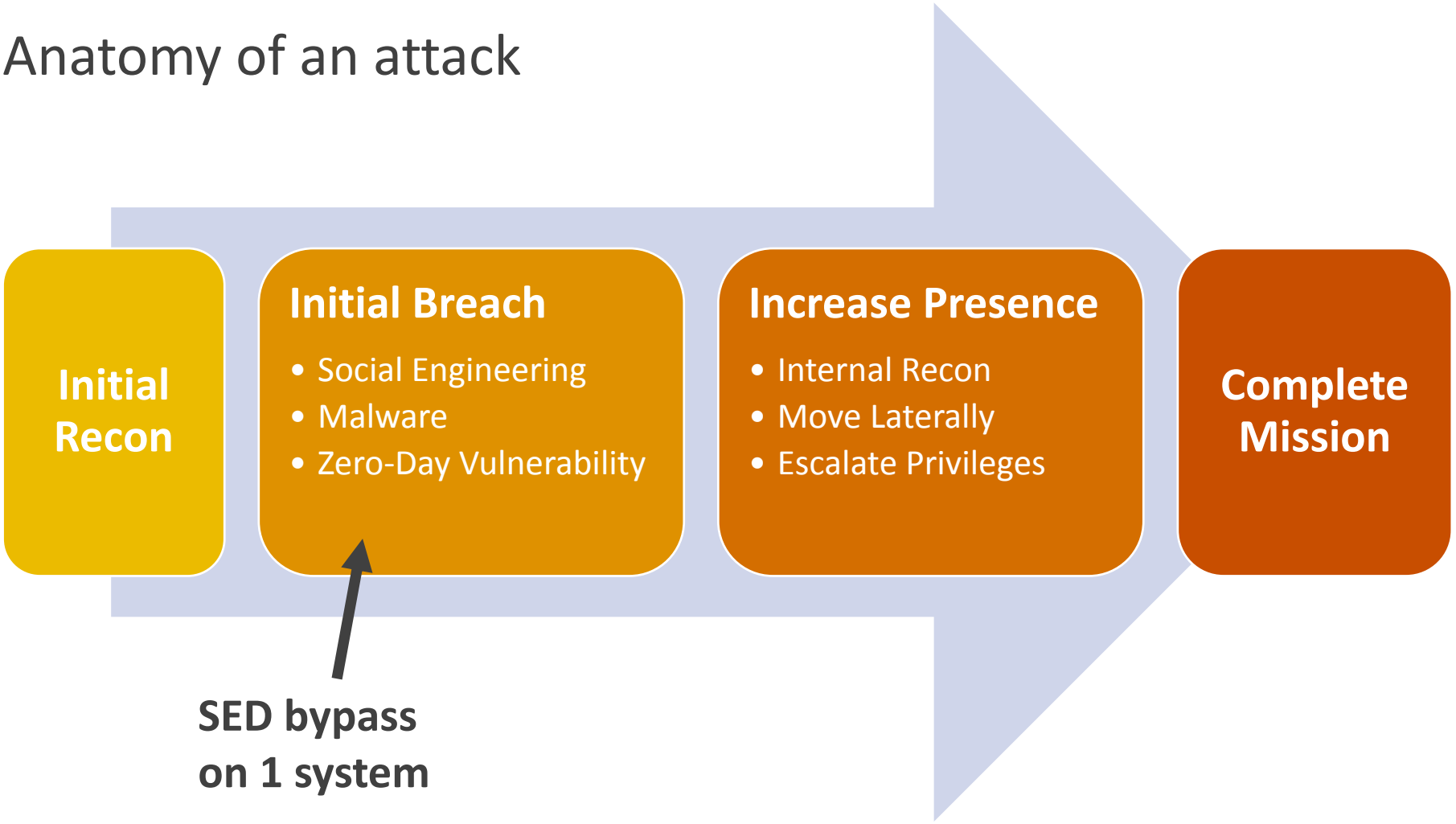
Real-Word Implications

Anatomy of an attack



Real-Word Implications

Anatomy of an attack



Black Hat Sound Bytes

SEDs are insecure by-design when laptop is On (S0) or in Sleep Mode (S3)

Hardened deployments can mitigate the risk

Difficult / impossible to detect attacks after the fact

Bypassing SEDs in Enterprise Environments

Q&A

Thank you

Daniel Boteanu

dboteanu@kpmg.ca

@DanielBoteanu

https://ca.linkedin.com/pub/daniel-boteanu/21/800/bbb