Why All Drives Should Be Self-Encrypting

Robert Thibadeau, Ph.D.

SVP & Chief Scientist

Wave Systems Corp.

Why? Use Cases

Drive is gone. What is the level of assurance that the data on the drive will not be harvested?

More subtle question… loss of control

How can I achieve regulatory compliance?

…. But Let's Go a few Steps Further

News from the land of Cyberwar

The device boots (and runs) from Storage

An insidious level of attack is upon us…

- **The Advanced Persistent Threat (APT) is migrating to attacks at a level much closer to foundational hardware**
  - These attacks occur before the operating system loads on the PC
  - Invisible to current anti-virus and anti-malware solutions
- **These attacks are designed to;**
  - Steal information to achieve economic, political and strategic advantage[1]
  - Establish and maintain an occupying force in their target's environment, a force they can call on at any time
- **Attacks can target key infrastructure including;**
  - Government
  - Utilities
  - Transportation
  - Communications
  - Banking
  - National Security
- **APT attacks may cause core infrastructure to be un-useable or offline for extended periods of time**

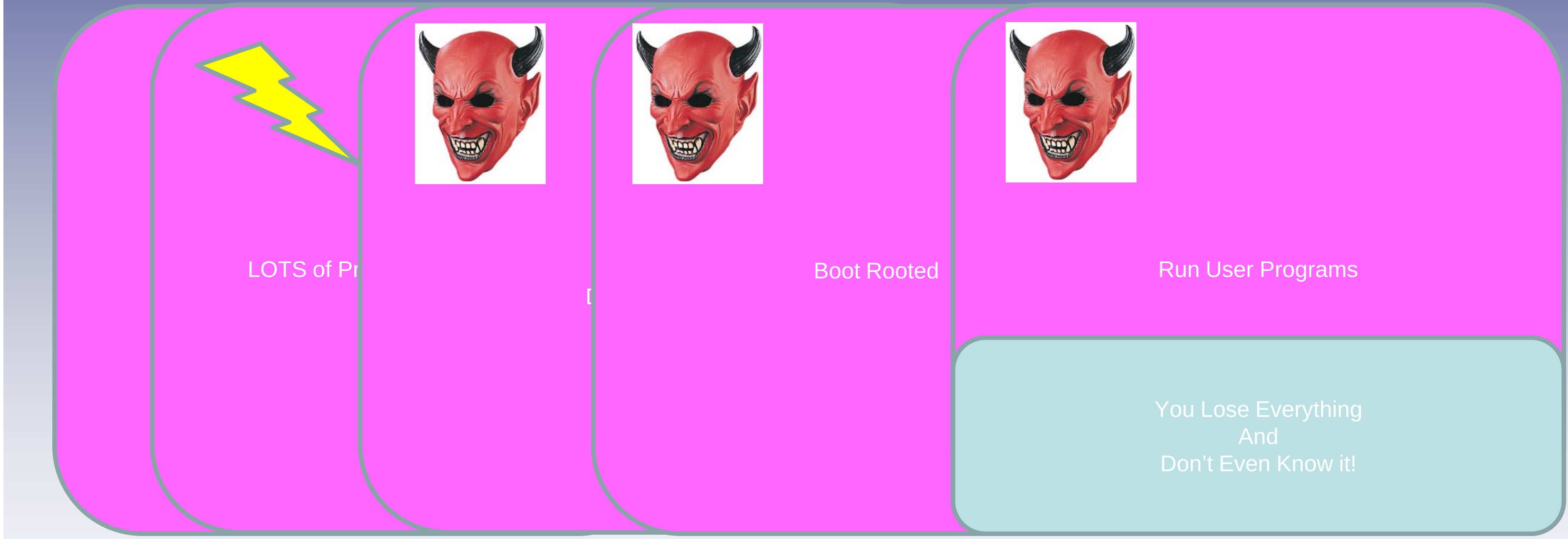
We can no longer hope or expect that a PC or Phone is running a good BIOS
It must be based on a trusted foundation

[1] http://kohi10.wordpress.com/2010/02/07/google-adobe-hacking-event-follow-up-apt-malware/

Non-Fiction Story -- The TPM and SED

- **Advanced Persistent Threats in Preboot**
  - It doesn’t get any worse than this!!!
  - The laptop that can’t even be repaired by wiping the disk
  - Yes, This is real
- **The Self-Encrypting Drive**
  - Self-Protecting
  - Self-Healing
  - IT Management to Prove you are (still) OK

“Rootkit” Attacks (For Long History, Google it).



LOTS of Pr

[

Boot Rooted

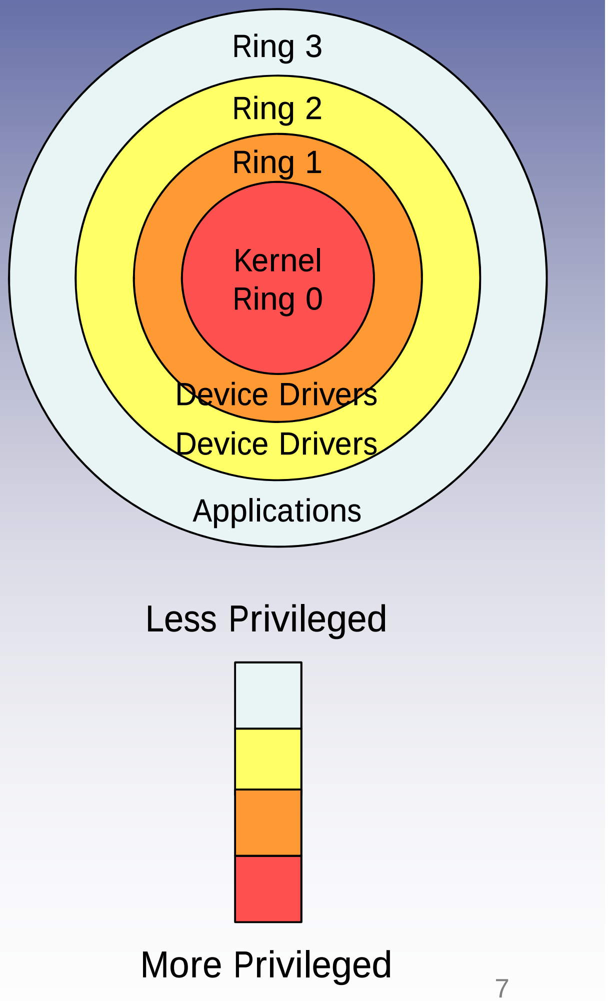
Run User Programs

You Lose Everything
And
Don’t Even Know it!

Advanced Persistent Threat!

Rootkit attacks allow continued privileged access
while hiding from administrators

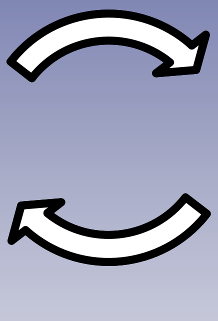
- **Attacks at the core have the highest privileges and are hardest to discover**
- **Option ROM – Drivers (Pre-boot firmware programs) are attack vectors**
  - Multiple vendors include code on machine
  - Video, NTFS, USB interface, etc.
- **Master Boot Record Program ("MBR" on Boot Drive) is the most common attack vector – 512 Byte Program…**
- **Virus checkers cannot check kernel**



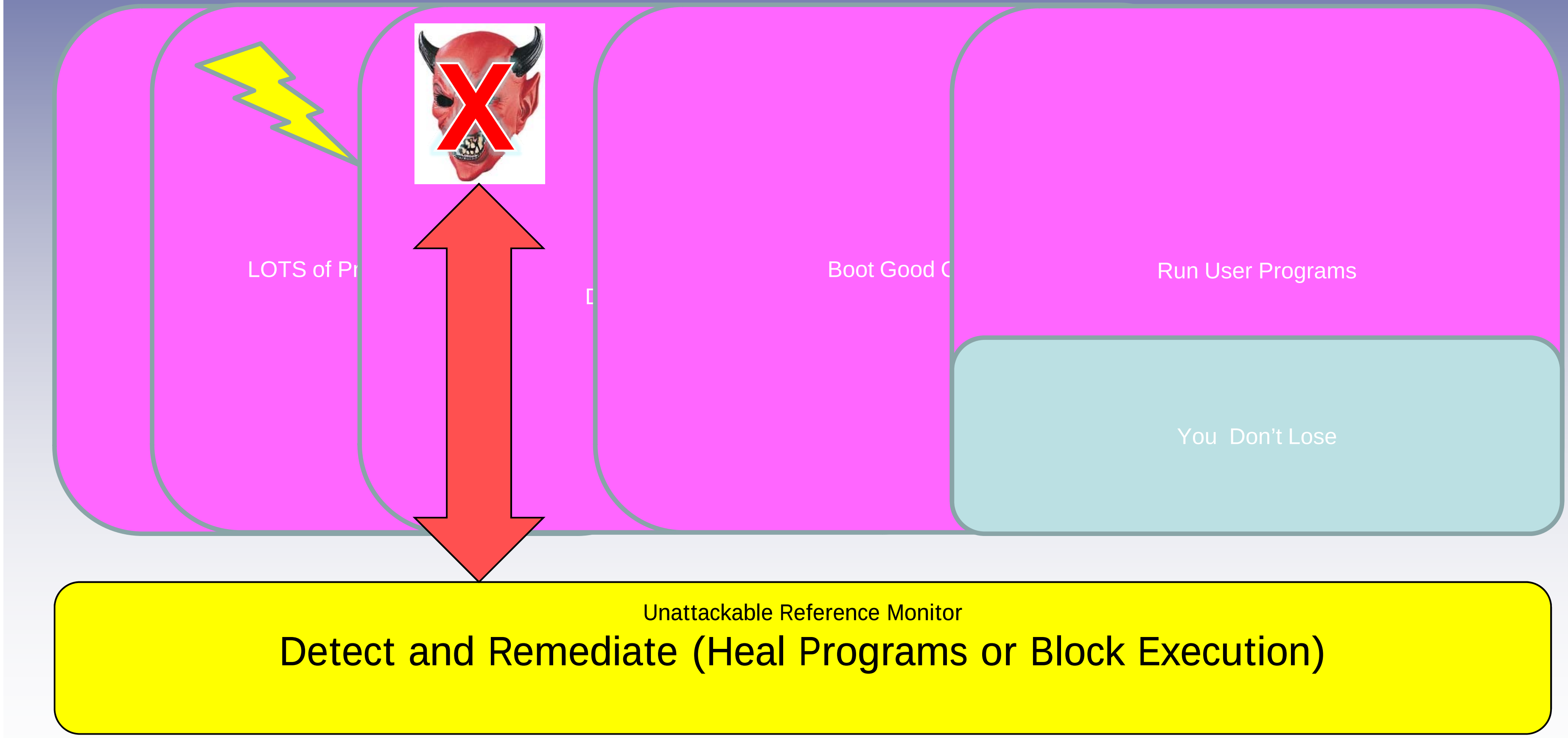
Two classes of Preboot threats are really bad and worse

- **Parasitic Infected Firmware**
  - Can operate clandestinely (below the “security radar”)
  - With an ongoing mission
    - data theft
    - corruption or destruction
    - infection propagation
    - identity theft
    - password theft; or other exploit
  - Persistence is of particular concern; not detectable by today's tools
  - Even if detected by higher level tools there is no way to neutralize the infected firmware, and the exploit would re-propagate each time the firmware was executed
- **Fatal Infected Firmware**
  - Renders the host system permanently unusable, or "bricked"
  - The impacted host could require physical repair, potentially necessitating costly and time-consuming component replacement at a manufacturer’s repair facility

Re-infection



“Reference Monitor” (For Long History, Google it).



LOTS of Pr

D

Boot Good C

Run User Programs

You Don’t Lose

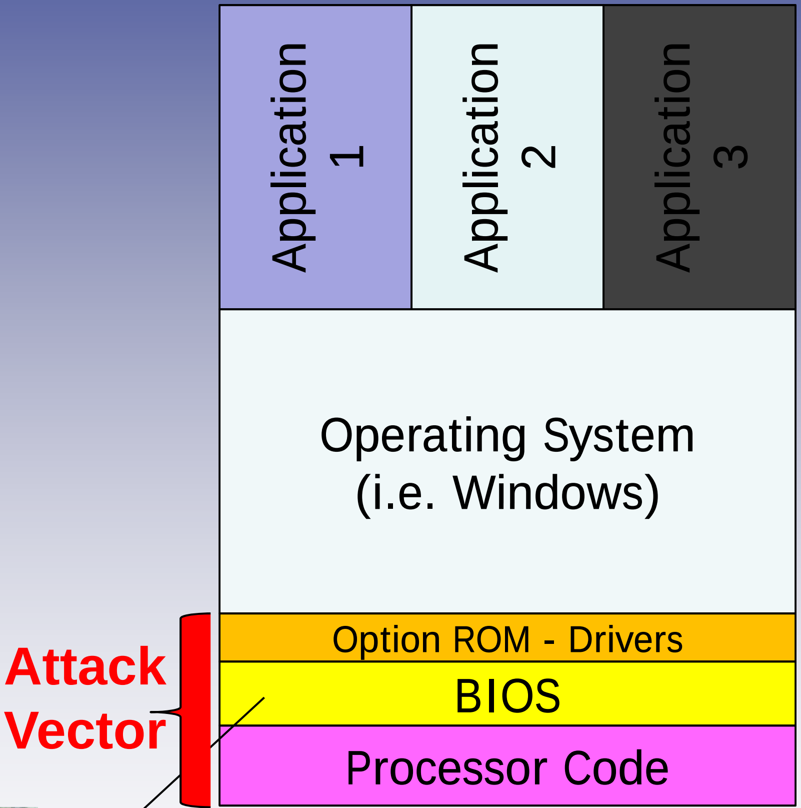
Unattackable Reference Monitor

Detect and Remediate (Heal Programs or Block Execution)

The Trusted Computing Group (TCG) Trusted Platform Module (TPM) with TCG BIOS IS A REFERENCE MONITOR

BIOS (Basic Input Output System)

- First code run by a PC when powered on
- The primary function of the BIOS is to configure the hardware and load and start an operating system
- The first job for the BIOS is to initialize and identify system devices such as the video display card and keyboard
- BIOS then loads software (OS) held on a peripheral device such as a hard disk
- BIOS firmware is stored on a non-volatile ROM



Platform Configuration Register (PCR) Values

- Computed by measuring platform firmware and BIOS configuration settings during the boot process (before the OS loads).
- PCRs 0-11 are relevant to the boot process.
- Stored and protected by the TPM
- Can be used to verify the integrity of the BIOS and MBR on the platform when it is powered on
- A quoting key is used to verify the identity of the platform which generated the measurements
- Reporting of PCR measurements uses public key cryptography, called “quoting,” to guarantee that the measurements are not spoofed

PCRs Computed by the TPM on My Laptop (Dell 6400)

PCR #	PCR Value	PCR Use
PCR 0:	f1fbb8971bc33115a6ccec5c9ef9794db595c7dc	CRTM, BIOS and Platform extensions
PCR 1:	a89fb8f88caa9590e6129b633b144a68514490d5	Platform and Motherboard configuration and data
PCR 2:	a89fb8f88caa9590e6129b633b144a68514490d5	Option ROM code
PCR 3:	a89fb8f88caa9590e6129b633b144a68514490d5	Option ROM configuration and data
PCR 4:	ea20c275a11010f64f414376e55875fe4e0497f8	MBR code
PCR 5:	401877b9c4988f1505a230cb1857d62a25ffdf35	MBR partition table
PCR 6:	a89fb8f88caa9590e6129b633b144a68514490d5	State transition and wake events
PCR 7:	a89fb8f88caa9590e6129b633b144a68514490d5	Computer manufacturer specific
PCR 8:	565a823e67f584d082932616cf9c40df36633c70	NTFS sector
PCR 9:	03c2d5f225d1cce23825ee4d42379c85b855a549	NTFS boot block
PCR 10:	f069d16800fd22b6a66103fc2d49934bd1b7e6de	Boot Manager
PCR 11:	2a6d6d4124b1ec83a4d5a69111fb23711e36170f	BitLocker Access Control
PCR 12:	a2986b03fdb883d4636240721fad43f67a751caf	Defined for use by the static operating system
PCR 13:	0000000000000000000000000000000000000000	Defined for use by the static operating system
PCR 14:	0000000000000000000000000000000000000000	Defined for use by the static operating system
PCR 15:	0000000000000000000000000000000000000000	Defined for use by the static operating system
PCR 16:	0000000000000000000000000000000000000000	Used for debugging
PCR 17:	ffffffffffffffffffffffffffffffffffffffff	Dynamic CRTM
PCR 18:	ffffffffffffffffffffffffffffffffffffffff	Platform defined

Getting back to basics - In an enterprise environment, legitimate firmware is absolutely necessary

The Wave solution provides a trust infrastructure for remotely managed PCs

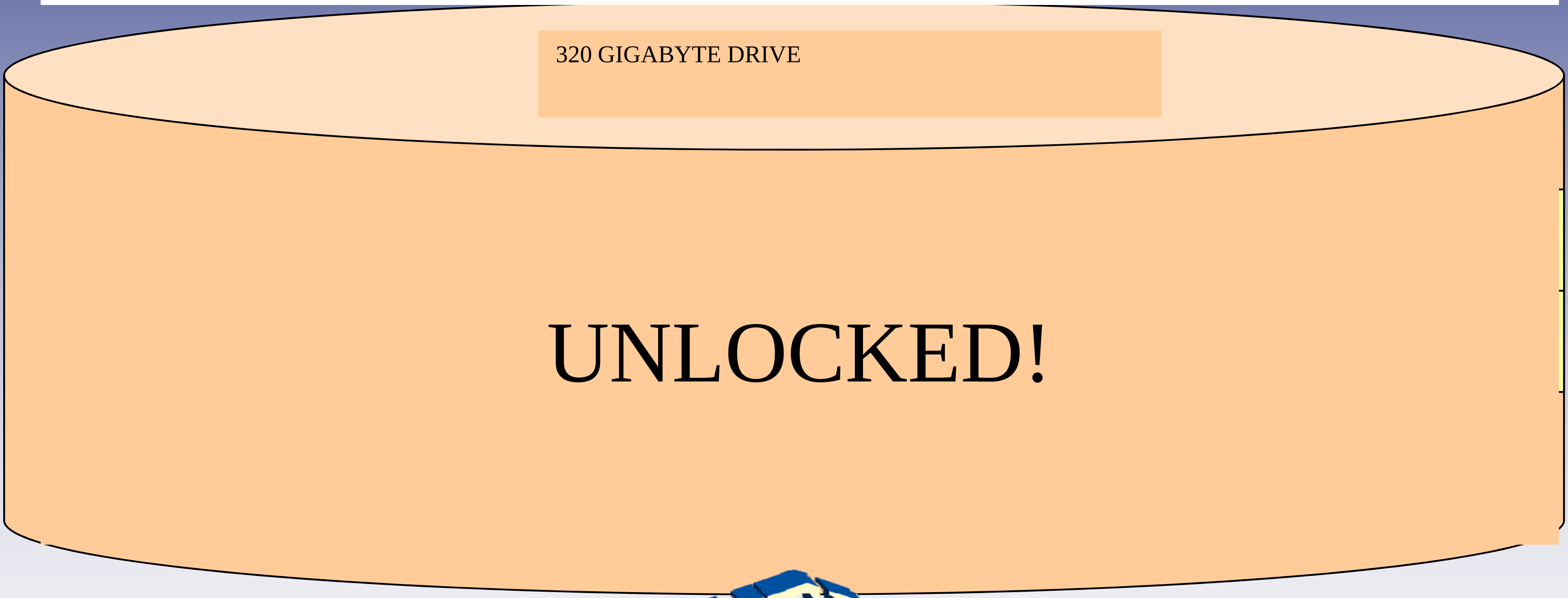
- **TPM-based: provides a hardware root of trust**
- **Strong machine identity: ensures it is a “known” device**
- **PC integrity measurements: ensures that the device is in a known state before the OS loads**
- **Self-Encrypting Drives can Self-Heal APTs**

Self-Encrypting Drive

- **FAST IN LINE HARDWARE :**
  - Encrypts all data onto Storage Media
  - Decrypts all data from Storage Media
- **Media Encryption Key Never Leaves Drive**
- **Generate new Media Encryption Key -- > Instant Erasure of a Terabyte!**

SED is Secure for Data at Rest

OS MBR CHECKED/FIXED, now BOOT HYPERVISOR/OS



320 GIGABYTE DRIVE

UNLOCKED!

POWER UP!

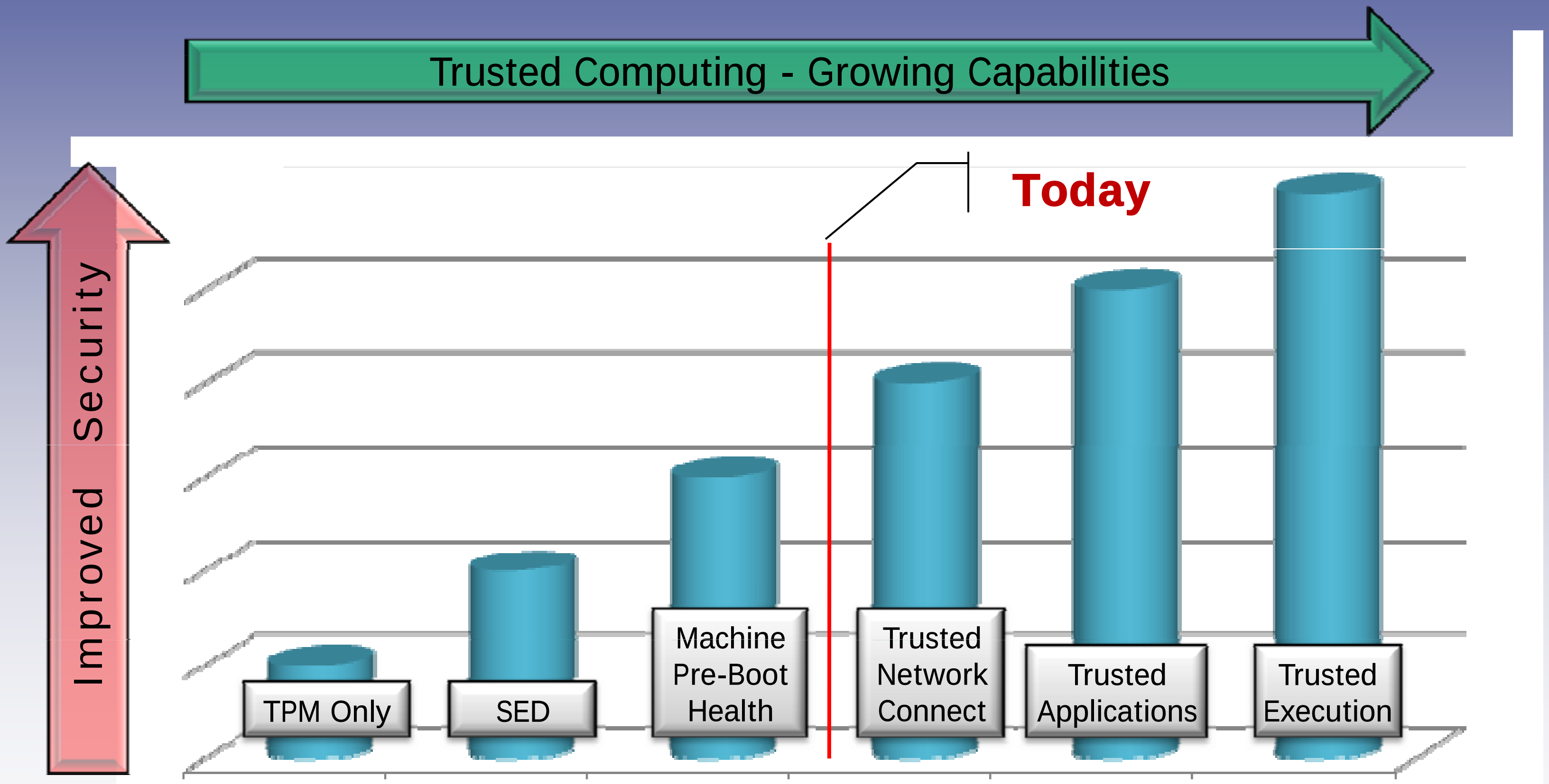
Self-Healing : User Notices Nothing…although Enterprise IT gets informed!

- **READ ONLY MBR runs and checks OS BOOT MBR**
- **If it is infected: Replace it with the Right MBR**

Smart Phones and Preboot Attacks… You know them already!

- Smart phones are just little PCs, but are **always on**
- Jailbreak iPhone, rooted Android…
- Phones
  - Should be slaved to lock after a few minutes,
  - Should encrypt sensitive data until unlocked,
  - Should log encryption state with server
  - Should use non-spoofable device identity and preboot measurement to alert if device is rooted.

Trusted Computing is an Industry Standardized Solution based on hardware and device identity



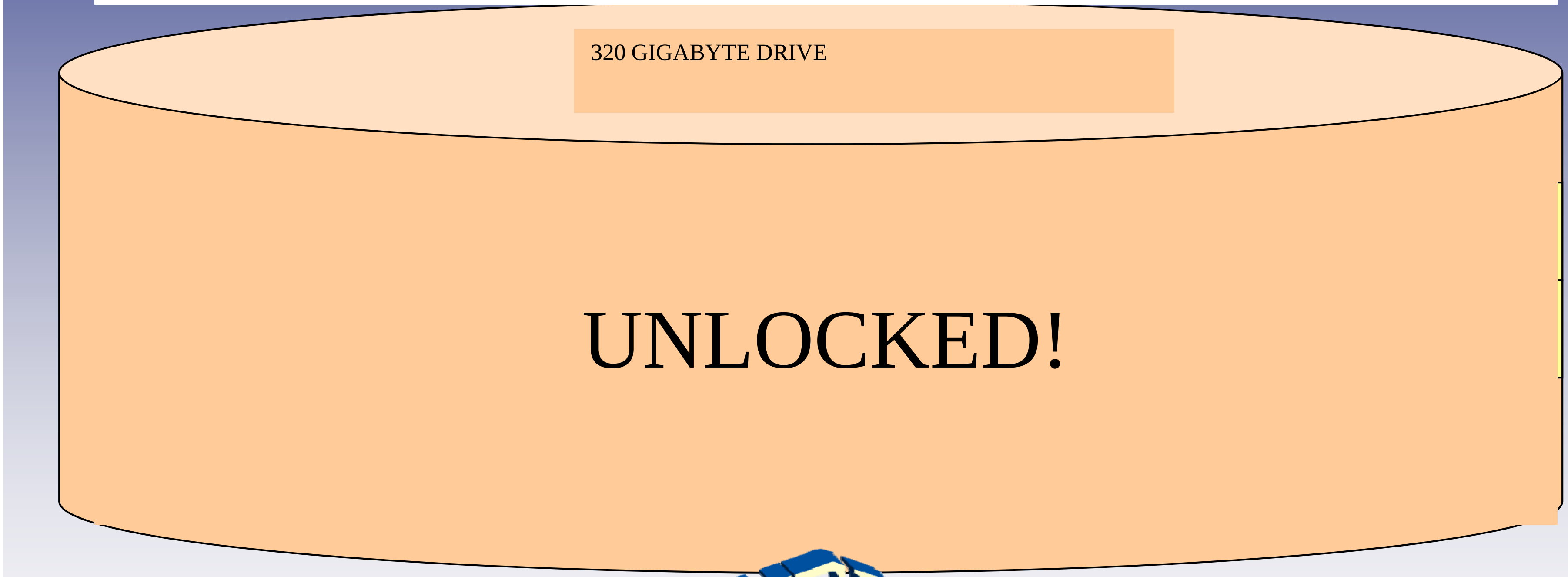
The Wave solution

Progression from Identification to Network Enforcement

Threat Types	Master Boot Record (MBR) and other major boot attacks. Fundamental changes to the BIOS or MBR are made that may involve violations of IT security policies. Boot configuration changes are made against organizational policy.		PC Spoofing attacks, Potential Denial of Service attack.	A machine that has been attacked boots onto the network. Network access is dependent on PCR Health and ID (AIK).
Mitigation/Solution	INFORM/ALERT PCRs 0-11 captured, put in a central database. Alert IT on specified PCRs (default 0, 2 and 4).	RISK ANALYSIS Analyze PCR data in order to diagnose the source of PCR changes. Perform analysis of enterprise PCR data. Audit for other kinds of boot attacks Report PCR data for PCRs 0-11s on demand.	ATTESTATION Use Endorsement Key to construct AIK for quoting. Create EK and AIK certificates where needed. This verifies the quotes and the PCR values are actually originating within a known TPM.	CONTROL/PREVENTION Network Access Control which can prevent a PC from having general network access until health is checked and approved. We are likely to interface with standard products from Microsoft or Juniper, etc., for the NAC specific functionality.

SED is Secure for Data at Rest

OS MBR CHECKED/FIXED, now BOOT HYPERVISOR/OS



320 GIGABYTE DRIVE

UNLOCKED!

POWER UP!

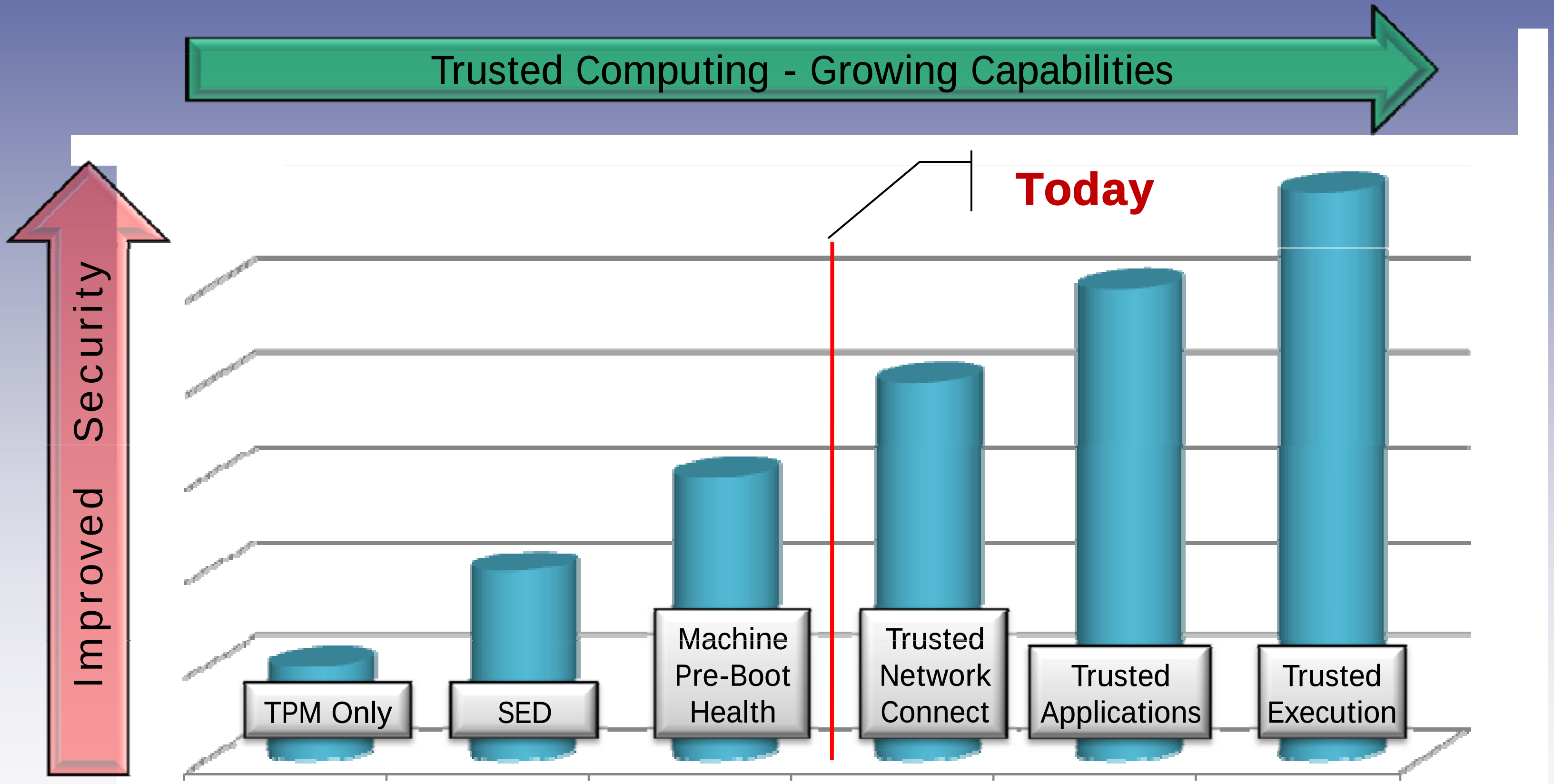
Self-Healing : User Notices Nothing…although Enterprise IT gets informed!

- READ ONLY MBR runs and checks OS BOOT MBR
- If it is infected: Replace it with the Right MBR

Smart Phones and Preboot Attacks… You know them already!

- Smart phones are just little PCs, but are **always on**
- Jailbreak iPhone, rooted Android…
- Phones
  - Should be slaved to lock after a few minutes,
  - Should encrypt sensitive data until unlocked,
  - Should log encryption state with server
  - Should use non-spoofable device identity and preboot measurement to alert if device is rooted.

Trusted Computing is an Industry Standardized Solution based on hardware and device identity


Trusted Computing - Growing Capabilities
Improved Security
Today
TPM Only
SED
Machine Pre-Boot Health
Trusted Network Connect
Trusted Applications
Trusted Execution