Design and Implementation of a Security Architecture for Critical Infrastructure Industrial Control Systems in the Era of Nation State Cyber Warfare

David Safford, Bill Smith, Monty Wiseman
GE Global Research Center

LSS, 2016

Imagination at work.

Controls broad reach

GE:

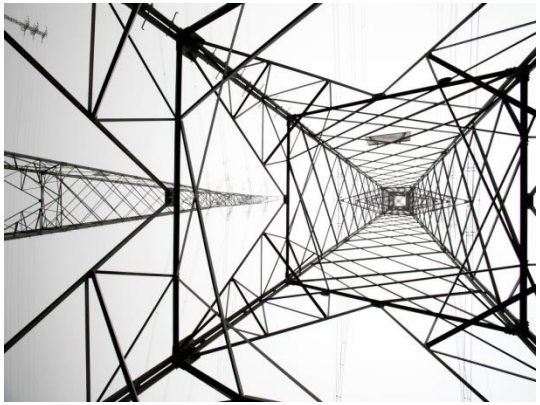
- **Half of the world's installed Power Generation (PG) base is from GE**
  - 10,000 gas and steam turbine generating units
  - Over 1,000,000 megawatts of installed capacity in 120 countries.
  - https://powergen.gepower.com/products/heavy-duty-gas-turbines.html
- **40% share of the worldwide market for new PG equipment.**
  - http://www.statista.com/statistics/381088/global-market-share-of-power-generation-equipment-manufacturers/
- **Largest supplier of Transmission & Distribution (T&D) equipment in the United States, top three worldwide.**
  - http://microgridmedia.com/ge-becomes-globa-utility-td-powerhouse/
  - https://medium.com/@GE_Grid/a-vision-to-power-the-world-74349a3c98a6#.ehjw5t7v8

Controls in The Era of Nation State Cyber Attacks

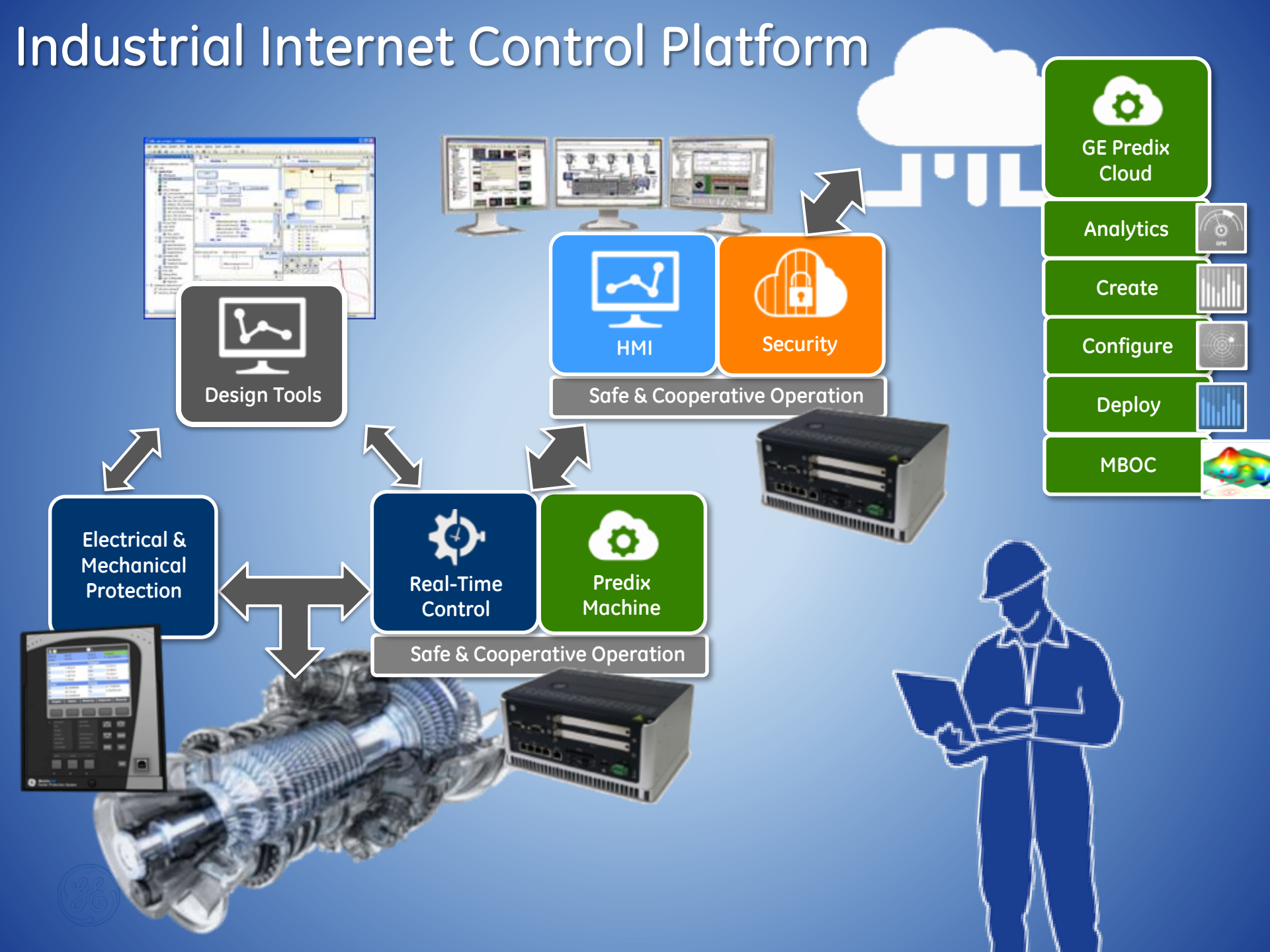
At RSA 2016, **Admiral Michael Rogers**, head of the NSA and the US Cyber Command, told delegates during his keynote address at RSA 2016 that the number one thing that keeps him awake at night is a cyber attack against US critical infrastructure, which is only a matter of when, not if, it will happen.
http://www.theregister.co.uk/2016/03/01/nsa_boss_three_security_nightmares/

Stuxnet compromised the control systems for Iran's nuclear centrifuges, rendering them useless. It attacked them successfully despite a state of the art air-gap defense.
http://threatjournal.com/archive/tj12072013.html

Ukraine's electric grid was shut down for 8 hours by a cyber attack, which wiped all control system computers, and bricked critical control interfaces.
https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/



Industrial Internet Control Platform



How Much Security Do We Need? Strength of Mechanism Level (SML)

Risk

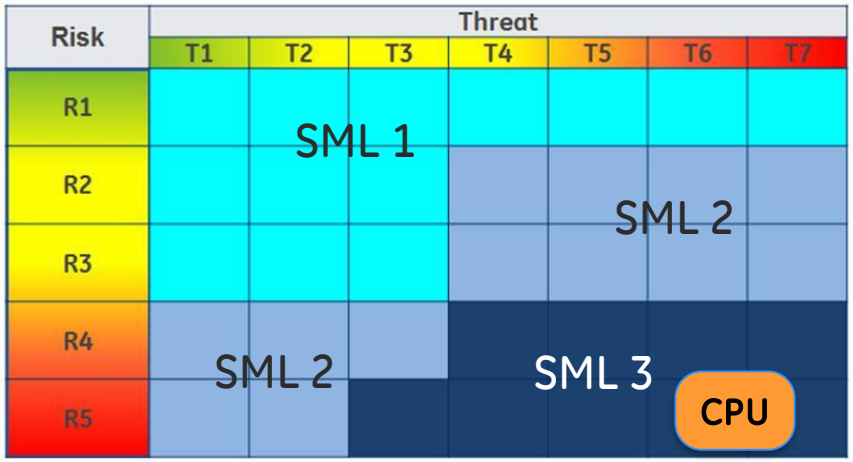
R1 Negligible consequences.

R2 **Minimal damage** to security, safety, financial posture, or infrastructure.

R3 **Some damage** to the security, safety, financial posture, or infrastructure.

R4 **Serious damage** to the security, safety, financial posture, or infrastructure.

R5 Exceptionally **grave damage** to the security, safety, financial posture, or infrastructure.



Threat

T1 Inadvertent or accidental events.

T2 Passive, casual adversary with minimal resources (e.g., **listening**, ...).

T3 Adversary with minimal resources; willing to take significant risk (**hackers**, ...).

T4 Sophisticated adversary with moderate resources; little risk (**organized crime**, ...).

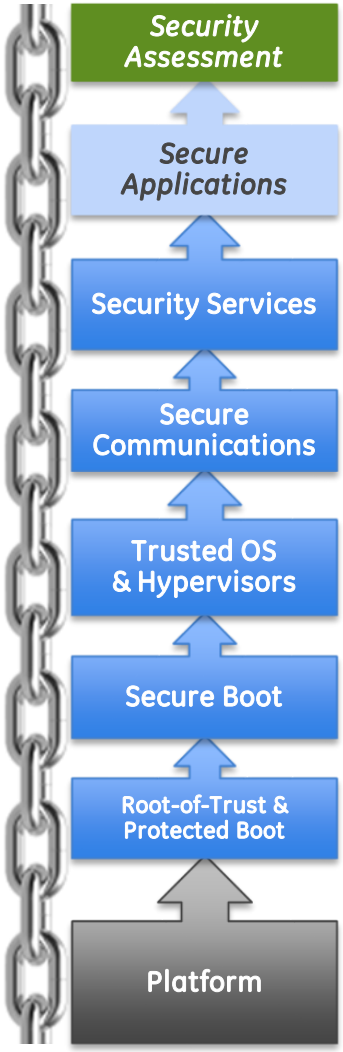
T5 Sophisticated adversary with moderate resources; significant risk (**terrorists**, ...).

T6 Extremely sophisticated adversary with abundant resources; little risk appetite (e.g., **nation-state**, ...).

T7 Extremely sophisticated adversary with abundant resources; will to take extreme risk (e.g., **nation-state** in time of crisis).

* Information Assurance Technical Framework, section 4.5, Release 3.1, National Security Agency, September 2002

A Hardware rooted Security Architecture for SML 3



Generic Security Feature	Example Instantiation
Certification, Penetration Testing of the entire system	
Secure Development Life Cycle (SDLC) for all applications	SDLC
Directory Services, Attestation, Public Key Infrastructure, Security Management	Predix, IMA Attestation Server, Signing Server
Data-in-motion encryption, based on Hardware Protected Keys	OpenSSL, TPM Keys
Encrypted Disk, Integrity Measurement and Appraisal, Hardware Protected Keys	LUKS, TPM-LUKS, IMA, IMA Client, Trusted Keys
Protected, Verified, Measured Boot Firmware	UEFI secure boot, Trusted Grub 2, tboot
Security Hardware for Hardware roots of trust for boot and key management	TPM-1.2/2.0 (e.g. Infineon SLB-9670)
Selection of processors with specific security features (DRTM, IOMMU, Virt), trusted supply chain	AMD Steppe Eagle (DRTM, IOMMU support)

There is no single security technology – It must be built into all layers

Specific Types of "Secure Boot"

- **Protected Boot (e.g NIST SP-800-147, SPI-HPM, ROM'ed bootloader…)**
  - Boot firmware is write protected so it cannot be modified
  - Essential base for all other boot versions

- **Verified Boot (e.g. UEFI Secure Boot, "locked" bootloaders, appraisal…)**
  - Digital signature verification of boot sequence
  - Active Defense: blocks system boot on verification failure

- **Measured Boot (SRTM, DRTM)**
  - Collection of cryptographic hashes/signatures associated with boot environment
  - Requires a measurement root-of-trust
  - Provides audit trail and basis for attestation of platform integrity
  - Passive Detection: does not block system from booting
  - Seal & protect platform secrets based on platform integrity

Instantiating the Chain of Trust Across Platforms:

- Intel/AMD
  - UEFI
  - Chipset based Protected Boot
  - LPC TPM
- ARM, ARM + FPGA (TI, Freescale, Xilinx…)
  - U-boot
  - CPU/ROM based secure boot (sometimes requiring NDA)
  - SPI TPM
- PPC (Freescale…)
  - U-boot
  - CPU/ROM based secure boot
  - SPI TPM
- Virtualized
  - KVM + swtpm + seabios
  - Containers

Linux/Platform Gaps/Issues

- TPM 2.0 Support – (Thursday Evening BoF)
  - Resource management (kernel and user space)
  - Getting the boot log to the kernel (was acpi) -> UEFI table, Device Tree?
  - Agreeing on APIs
- Measured and verified boot in UEFI Grub2 with TPM2 (Matthew Garrett)
- Container Filesystem - User Namespace support (James Bottomley)
- Containers - IMA Namespacing (Yuqiong Sun)
  - Separate policies, measurement lists, vTPMs
  - Hierarchical, easy to delete
- Hypervisor (KVM/QEMU) support for vTPM
  - Support for measured and verified boot in UEFI/Legacy guest firmware.

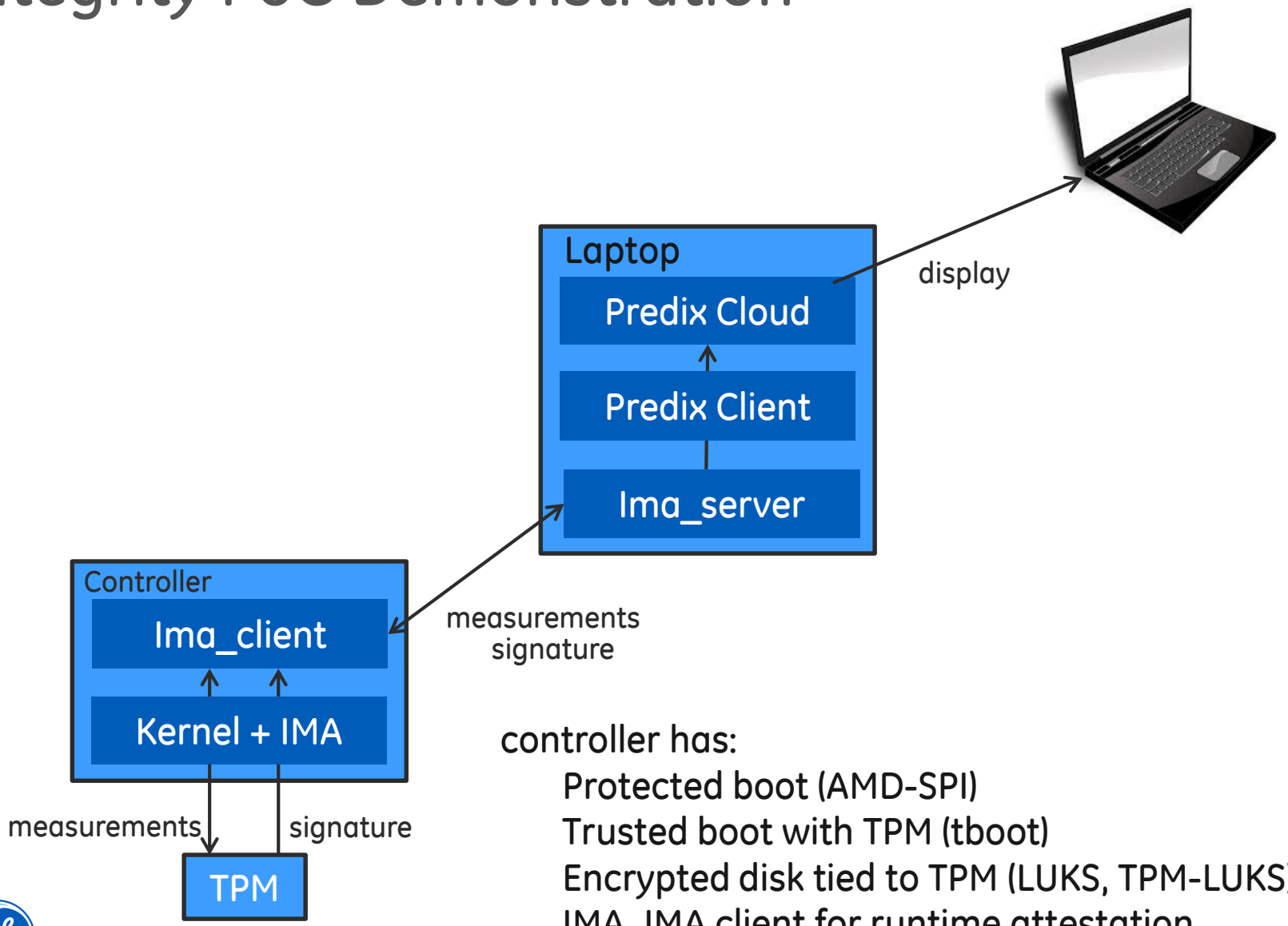
Linux/Platform Gaps/Issues

- SPI TPM driver in Linux (4.8RC) and u-boot (?)
- LUKS and Systemd support for Kernel Key Ring (e.g. from trusted keys)
  - Or ext4 encryption?
- CPUs without public documentation on their processor based verified boot
- CPUs with binary blobs in: SMI, ME, trustzone
- Package signing tools
- Key management for third party signed files (less critical in embedded)

Contributions

- tboot: (Safayet Ahmed)
  - Security, Bug fixes
  - AMD port with full DRTM

Integrity PoC Demonstration



controller has:

- Protected boot (AMD-SPI)
- Trusted boot with TPM (tboot)
- Encrypted disk tied to TPM (LUKS, TPM-LUKS)
- IMA, IMA client for runtime attestation

Situation Normal

Predix Seed

localhost:9000/about

Apps IBM dave News Google Gmail Google Maps BluePages CUPS » Other bookmarks

Predix

Integrity Summary

Controller Integrity Status GOOD

```
Appraised File Summary: Number of Files, Keys used to sign
      1019   /etc/keys/ima/local_x509-signed.der

Signature Errors:

      Unsigned:           0

      Invalid signature:  0

      Missing key:        0

Actual Integrity Value
     PCR-10: 2F 37 C6 AD 33 1D F5 24 FE 21 E2 F7 A8 59 9D A1 39 89 94 52
Reported Integrity Value
     PCR-10: 2F 37 C6 AD 33 1D F5 24 FE 21 E2 F7 A8 59 9D A1 39 89 94 52
```

Signed Measurements Show Attempt

Predix Seed

localhost:9000/about

Apps | IBM | dave | News | Google | Gmail | Google Maps | BluePages | CUPS | Other bookmarks

Predix

Integrity Summary

Controller Integrity Status WARNING

```
Appraised File Summary: Number of Files, Keys used to sign
      1059   /etc/keys/ima/local_x509-signed.der

Signature Errors:

      Unsigned:            1
            /usr/bin/trojan_nosig

      Invalid signature:   1
            /usr/bin/trojan_badsig

      Missing key:         0

Actual Integrity Value
     PCR-10: 5D 32 5C EF A8 41 79 BE C7 FD 3E 9B 9D 2D 62 D1 FF 14 78 25
Reported Integrity Value
     PCR-10: 5D 32 5C EF A8 41 79 BE C7 FD 3E 9B 9D 2D 62 D1 FF 14 78 25
```

TPM Signature Catches the Kernel Compromise

Predix Seed

localhost:9000/about

Apps | IBM | dave | News | Google | Gmail | Google Maps | BluePages | CUPS | Other bookmarks

Predix

Integrity Summary

Controller Integrity Status COMPROMISED

```
Appraised File Summary: Number of Files, Keys used to sign
      212   /etc/keys/ima/local_x509-signed.der

Signature Errors:

      Unsigned:           0

      Invalid signature:  0

      Missing key:        0

Actual Integrity Value
     PCR-10: AF F1 3C 1C 6E 96 F0 36 62 9F 7D CB 62 EB 34 E3 CE AD 44 6F
Reported Integrity Value
     PCR-10: 82 2F 6D 0D 7E C1 31 7B 18 20 7E 1B 62 AC BC 7D 37 F6 45 27
```

Summary

- Nation State threat model
- Air Gaps keep you from knowing you've been hacked
- Industrial Control Systems Security Architecture
  - Security from hardware through cloud
  - Secure Hardware for multiple architectures (X86, ARM, PPC)
  - Protected, Verified, Measured Boot
  - Trusted OS
  - Security Services
  - Cloud based Attestation/Verification
  - A Lot of Work Remaining