# Beyond the TPM: Other Trusted Computing Technologies

Ariel Segall
ariels@alum.mit.edu

Day 1

Approved for Public Release: 12-2749.
Distribution unlimited

# License

All materials are licensed under a Creative Commons “Share Alike” license.

- http://creativecommons.org/licenses/by-sa/3.0

**You are free:**

**to Share** — to copy, distribute and transmit the work

**to Remix** — to adapt the work

to make commercial use of the work


**Under the following conditions:**

**Attribution** — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

**Share Alike** — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

# What We'll Be Covering

- The Roots of Trust for Measurement (RTMs)
- Trusted Network Connect
- What else is out there (in brief)

# Core Concept: Chain of Trust

Measurements in trusted computing are based on the idea of a *chain of trust*.

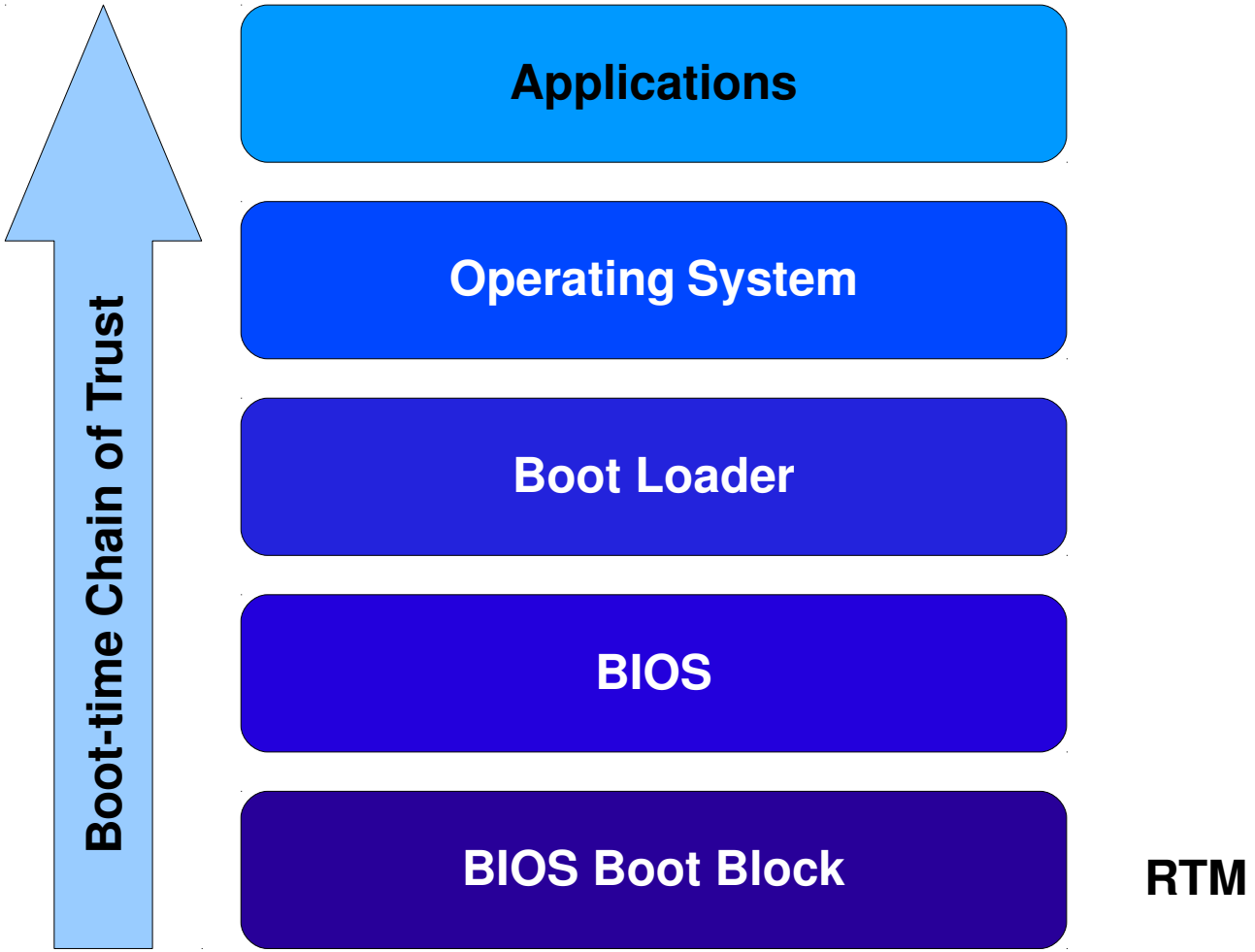
- Component A measures component B; stores that measurement
- Component A then launches component B
- Verifier: "If I trust A, then I can believe the measurement of B is accurate, and use the measurement to decide if I trust B."
- Chains: A measures B, B measures C, C measures D....

# The Two RTMs

There are two Roots of Trust for Measurement:

- Static
  - Part of BIOS
  - Runs automatically as part of system boot
  - Used to create "boot-time" chain of trust
- Dynamic
  - Part of CPU (signed code from manufacturer)
  - Run by entering special secure CPU mode
  - Used to create "late-launch" chain of trust
  - Can be used to measure and launch anything!

# Static RTM Chain of Trust



# Static RTM Tradeoffs

Pros:

- Already there, already working
- Free, no need to change any software

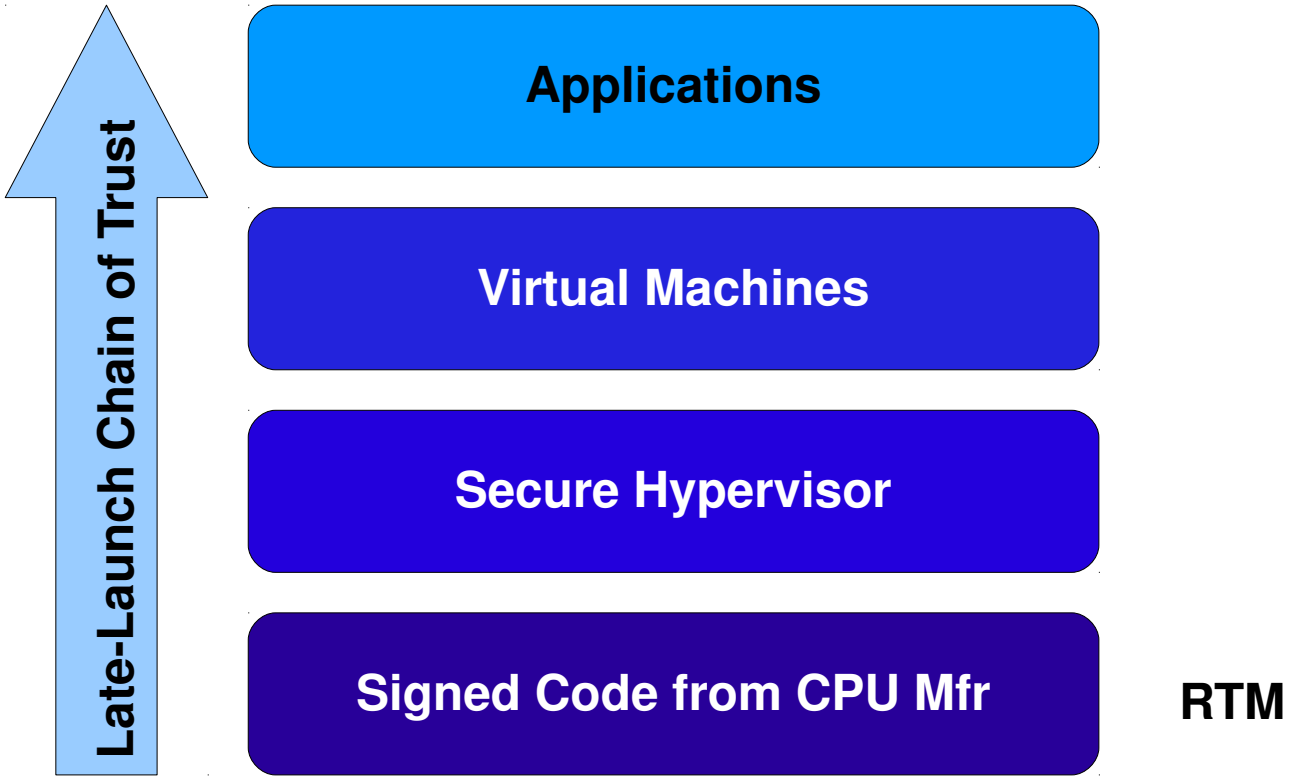
Cons:

- How much do you trust your BIOS? Your BIOS vendor?
- Today, measurements are *extremely* variable and cryptic
  - Work ongoing on standardizing, but not rolled out yet
- BIOS "bootkits" exist.

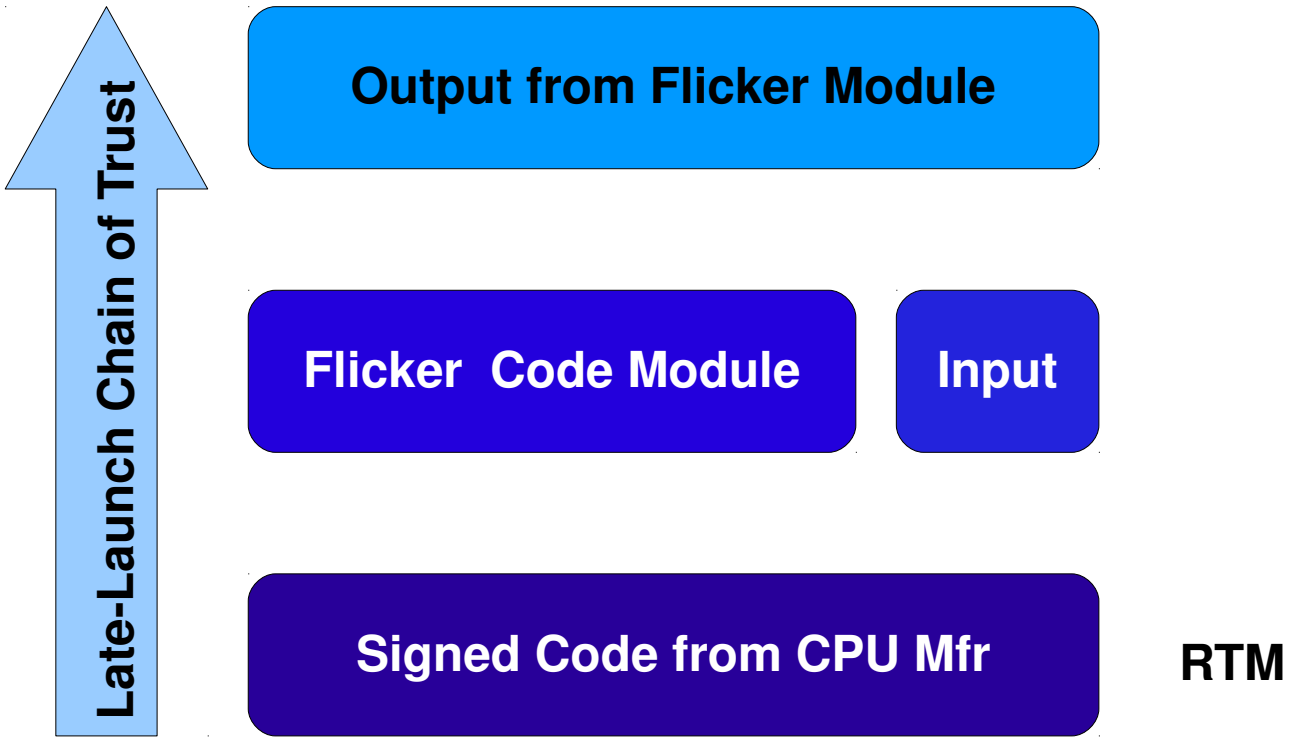
# DRTM: How It Works

- Special command sent to processor, along with designated region of memory
  - SINIT (Intel's TXT) or SKINIT (AMD's SVM)
- All processing on machine shut down except for special code module
  - Stored in firmware, signed by CPU manufacturer
  - Signature verified before execution
- Code module (DRTM) hashes contents of memory region, stores in TPM
  - Memory region may include both data and executables
- Passes control to specified location in memory
- Direct chain of trust from CPU root to any program user chooses
- Has special locality, and PCRs only it can write to
  - Can also be used to constrain keys or data
- Often referred to as *Late Launch*

# DRTM Example: Virtualization Chain of Trust



# DRTM Example: Flicker Chain of Trust



# DRTM Tradeoffs

Pros:

- Very flexible; measure anything you need to
- Trust CPU, not BIOS or boot loader
- Much shorter chains of trust

Cons:

- Requires non-trivial implementation

Mixed:

- Can be done repeatedly; only most recent verifiable

# When Should You Care About RTMs?

System design or integration:

- You want your system to be remotely evaluatable via TPM.

Application:

- You want your app to be measurable.
  - Unless using Flicker-style application-specific DRTM, you just need to know which component should measure your app.
- You are evaluating another system's trustworthiness, and thus need to know which RTM they use.
- That's it! Otherwise, you can pretty much ignore.

# What We'll Be Covering

- The Roots of Trust for Measurement (RTMs)
- Trusted Network Connect
- What else is out there (in brief)

# Trusted Network Connect Overview

- TCG's architecture for network access control (NAC)
- Not really a technology; a suite of protocols and architectures
- Probably the most supported TCG product
- **Does not actually require use of the TPM**
  - Part of the reason adoption has been rapid
  - Architecture flexible and abstract– roots of trust optional!
  - **Not all implementations of TNC can meaningfully be trusted**
- Uses fairly standard NAC abstractions

Core idea: Machines seeking network access present evidence about their state, which is evaluated based on policy before the machine is admitted.

# TNC Vocabulary

AR **Access Requestor**: machine seeing network access

PEP **Policy Enforcement Point**: Gateway, or other resource that can allow or deny access

PDP Policy Decision Point: Machine which evaluates access requests

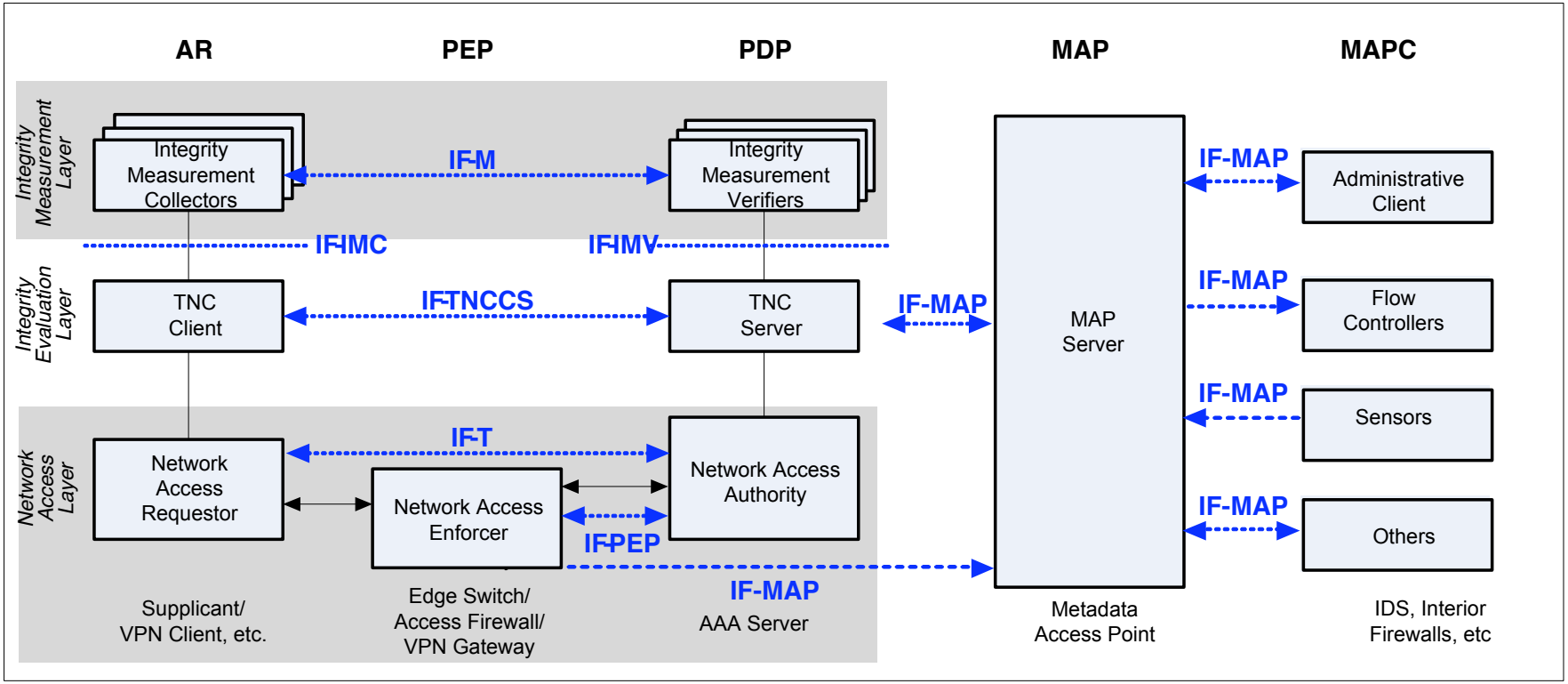
MAP Metadata Access Point: Stores and provides information about ARs

MAPC MAP Client: Clients which read or write MAP state data about ARs

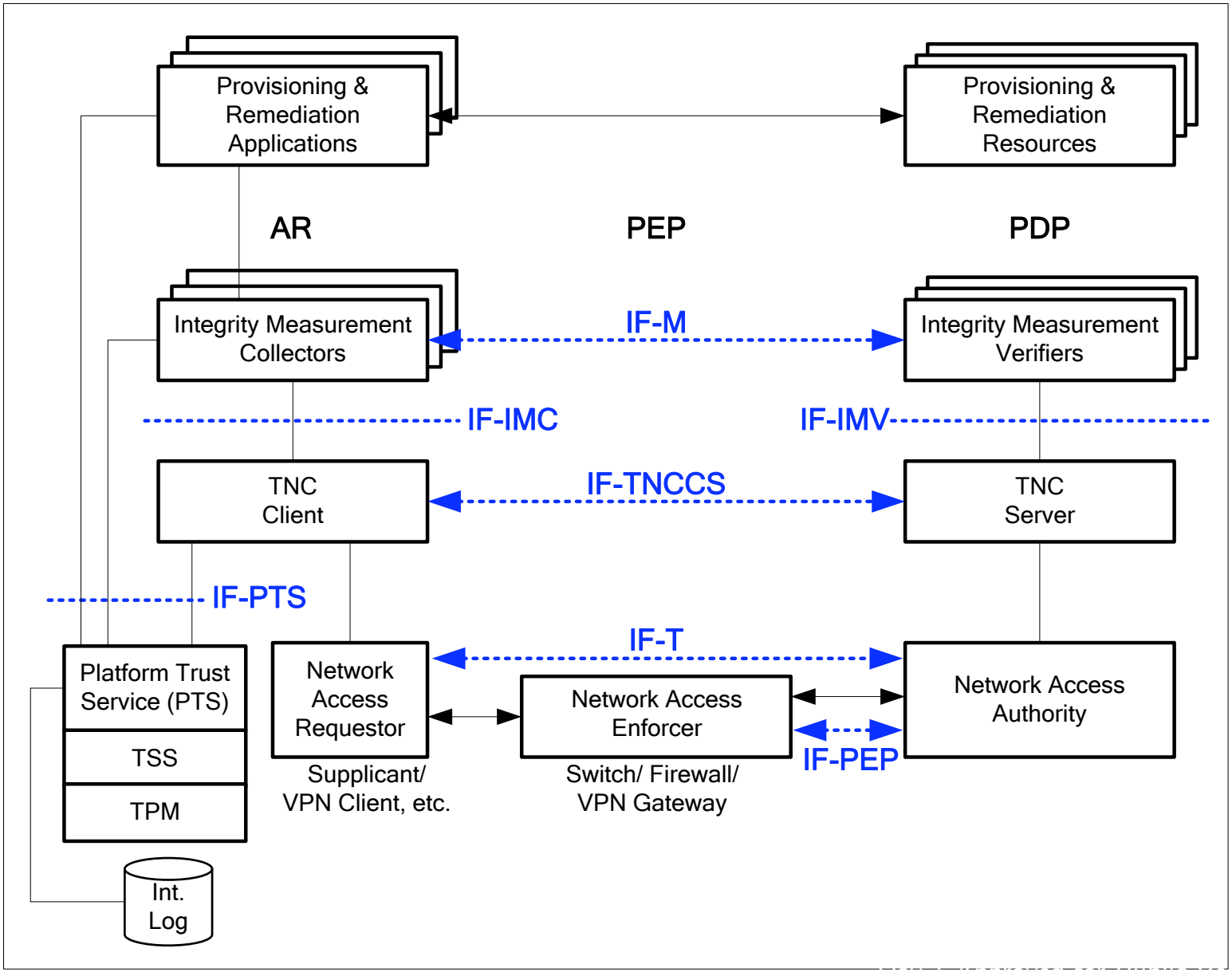
PTS Platform Trust Services: AR software interfacing between TNC and TPM.

Only bold roles actually required.

# TNC High-Level Visual



# TNC: Where the TPM Fits In



# Some Words of Warning

- The TNC protocol designers were not TPM experts.
  - **It is not safe to deploy their PTS to IF-M binding in an enterprise that plans to use any other attestation technologies.**
  - There is a **man-in-the-middle attack** if quotes are used elsewhere on the network.
- TNC alone does not give you real trust; it defines how components communicate
- You can buy TNC products today; always ask whether they use the TPM, and if so, how.

# What We'll Be Covering

- The Roots of Trust for Measurement (RTMs)
- Trusted Network Connect
- What else is out there (in brief)

# Other Trusted Computing Technologies: Storage

- High-security drives designed with trusted computing in mind
- Self-encrypting
  - Designed for high speed encryption and decryption
- Generally support user authentication
- Future possibilities: machine authentication or attestation

# Other Trusted Computing Technologies: Protocols

Generally, TCG's protocols are focused on taking advantage of low-level technologies.

- Integrate TPM quotes into high-level reporting standards
- Certify TPM keys and trusted platforms
- Add TPM data to various handshakes or channel establishments
- **Not all TCG protocols are appropriate for enterprise use!**
  - Serious flaws have been found in at least one TCG protocol (PTS Binding to IF-M)
  - Assumed it would be the *only* protocol on the network using the TPM
  - All TCG protocols should be evaluated against enterprise needs before use

# Other Trusted Computing Technologies: Near Future

- Mobile Trusted Module
  - Streamlined TPM-like functionality for cellphones
  - Allow providers more ability to control, verify software
  - Support cellphone-as-wallet usecase with real security
- TPM 2.0
  - Next version of TPM
  - Much like today's, but more flexible and more capable
  - Better crypto algorithms
  - More standards-compliant
- Trusted Virtualized Platform
  - Using TPMs to establish trust in virtualized workstation or cloud
  - Virtual TPMs for identifying VMs and protecting VM data