

Trusted Computing for High- Consequence Missions

John McDermott
Naval Research Laboratory

Trust

“Trust is the expectation that a device will behave in a particular manner for a specific purpose.”

TCG Specification Architecture Overview rev. 1.2

Core Root of Trust

- CRTM/S/R or equivalent is necessary for vendor software privacy and DRM
- If challenge or reporting protocols for management of CRT use ciphertext then
 - CRT can be exploited to encrypt intruder activities
 - If CRT is present then IDS must accept the presence of ciphertext on the network
 - It is not even necessary to break CRT to exploit the encryption
- This is not an issue of vendor/OEM intent
- The existence of key tags to designate *storage keys* and *bind keys* suggests a potential problem.

Lack of Authoritative Design Information

- Need public disclosure of TC **use cases**
- Need public disclosure of TC **trust model**
 - What **purpose** is associated with each trust relationship?
 - What **behavior** is associated with each trust relationship?
- Need public disclosure of TC security **assumptions** and **assertions**

Certification Infrastructure

- Quality, assurance level, and motivation of certifiers of software.
 - The present level of practice hardly seems suitable for high-consequence applications
 - What is the meaning of EAL 4 and above, protected by EAL 3 TC ?
 - Transfer of responsibility / risk away from vendor and certifier
- Will there be alternative certifications?
- What would the credential and key structures for alternatives look like?

Tunable Security

- Security should be proportional to risk.
- Will TC security be tunable?
- TC *protected capabilities* will be determined by TCG members.
- Will there be TC Common Criteria Protection Profiles for higher levels of assurance?

Fail-Stop Technology

- TC provides fail-stop security
- Fail-stop security does not support reconfiguration
- Many high-consequence applications require fail-report security
- Denial-of-service attack: **create new platform owner**
- Loss of data recorded in proprietary formats.

End-User Management

- If a TPM is compromised how is a new EK issued?
- Buy new hardware?
 - The “Best Buy” algorithm is not scalable
- Buy a new TPM?
- How are measurements updated? What if there is no update protocol in place?

Aggregation of End-Point Information

- Points where large amounts of end-point information are stored
- Exposes information about internal networks
- User's "private" information is often corporate information in high-consequence systems.
- What constitutes "reasonable protection" for this data varies with value or criticality of the data.

Higher-Assurance Enhancements for Small Markets

- Virtual machine monitor?
- Host-based IDS?
- Higher-assurance cryptographic peripherals?

Data-Owner Roots of Trust

User Data Protection in High-Consequence Systems

Trust

“Trust is the expectation that a device will behave in a particular manner for a specific purpose.”

TCG Specification Architecture Overview rev. 1.2

“Trust in these components is derived from good engineering practices, manufacturing process and industry review.

Evidence of engineering practice and industry review is contained in the Common Criteria (CC) certification results ... “