Foundations of Computer Security

Lecture 76: Certification

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Buying Security Products

Ideally, buying security products should involve:

1. assessing needs to determine requirements;
2. identifying the product that will meet those requirements;
3. purchasing the product and deploying it.

The problem: most customers don't have the expertise to perform these steps effectively.

A solution: provide a standardized process of independent evaluation by expert teams to provide a certified level of confidence for security products.

Evaluation Methodology

An evaluation standard provides the following:

- A set of requirements defining security functionality.
- A set of assurance requirements needed for establishing the functional requirements.
- A methodology for determining that the functional requirements are met.
- A measure of the evaluation result indicating the trustworthiness of the evaluated system.

Cryptographic Functions

For *cryptographic functions*, federal agencies are required to use products that either have been approved by the NSA, or have been validated to FIPS 140-1 or 140-2, *Security Requirements for Cryptographic Modules*.

- Approximately 150 vendors of cryptographic modules have had independent labs perform compliance/conformance testing of their modules.
- FIPS 140-2 defines four levels for certification for crypto devices designed for protection of sensitive but unclassified information,

FIPS 140-2 Levels

These are levels of certification for cryptographic devices:

- Level 1: basic security; at least one approved algorithm or function.
- Level 2: improved physical security, tamper-evident packaging.
- Level 3: strong tamper-resistance and countermeasures.
- Level 4: complete envelope of protection including immediate zeroing of keys upon tampering.

Lessons

- Certification standards for security products would help the consumer understand what they need and what they're buying.
- For cryptographic products, the government provides guidance in the form of standards FIPS 140-1 and 140-2.

Next lecture: The Common Criteria