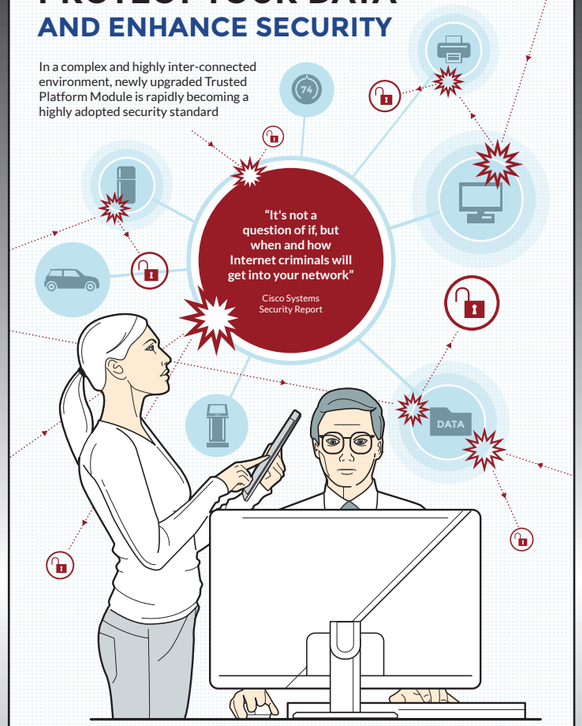
PROTECT YOUR DATA
AND ENHANCE SECURITY

In a complex and highly inter-connected environment, newly upgraded Trusted Platform Module is rapidly becoming a highly adopted security standard



Living on the Edge

Malicious actors are using trusted applications to exploit gaps in perimeter security:

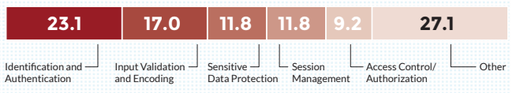
The risks

Key areas of authentication, authorization, input validation, and encryption are the most common (and critical) risks. Potential threats typically exploit these areas with an increasing number of attacks and are difficult for existing tools to understand and diagnose. At the same time, attacks against infrastructure are targeting specific resources - 85% of the malicious sites were found on legitimate web hosts that had been compromised.

98%
of applications presented at least one application security risk

22.4
risks registered by the average application

Distribution of Risks by Security Area (%)

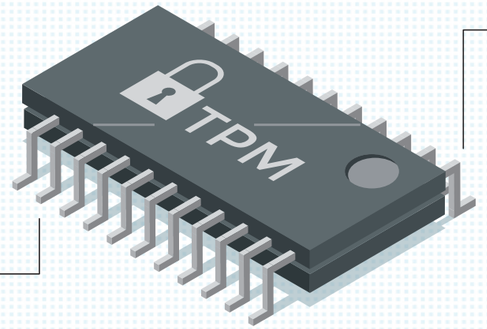


Locking Your Valuables

The combination of a properly designed password storage method and a properly designed methodology/policy for a user password choice is absolutely critical. Enter TPM, the Trusted Platform Module, created by Trusted Computing Group. TPM is kind of a digital fingerprint, a microcontroller that stores keys, passwords and digital certificates, enabling:

Integrity checks of systems with the TPM

Authentication



Secure repository for certificates, keys, passwords that's safer than storing these in software

Cryptographic capabilities to create a unique digital fingerprint for systems

Over two billion TPMs are embedded into PCs, servers, networking gear and other devices, protecting users against unauthorized changes: TPM stores personal data, making it more secure from software attack and physical theft.

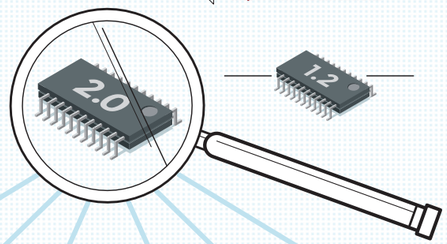
Access to data and secrets in a platform can be denied by policy settings, making critical applications and capabilities such as secure email, secure web access and local protection of data much more secure.

Protect your entire digital environment

Fast forward to TPM 2.0 library specification, looking beyond SHA1 and RSA cryptography, to make the features less ambiguous, more manageable and applicable across various devices used in an Internet of Things environment, designed to function in many kinds of embedded systems. Furthermore, TPM 2.0 is expected to be widely used and meet government requirements in many countries.

Comparison

Compared to TPM 1.2, new specifications include six important modifications



1 Flexible support for algorithms
Variety of algorithms with the potential to add support for more algorithms in the future with minimal revisions

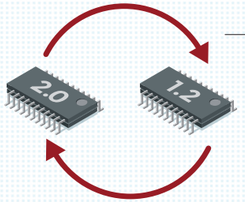
2 Support for more than one "bank" of Platform Configuration Registers
TPM to keep track of platform state using more than one distinct hash algorithm

3 Inclusion of three administration hierarchies
"Platform hierarchy" for platform protection, an "endorsement hierarchy" for privacy control and a "storage hierarchy" for general cryptographic usage

4 Support for enhanced authorization
Very flexible and fine-grained control over how and when TPM-protected data and keys can be accessed

5 Support for additional key usage
Ability to provide more general cryptographic operations with public and symmetric keys, including signature verification and symmetric encryption

6 Support for multiple "trusted keys"
More than one "endorsement key" and more than one "storage root key", each potentially using different algorithms



Will TPMs based on the 1.2 specification be replaced by ones based on the TPM 2.0 specification?

TPM 1.2 currently is an ISO/IEC 11889 standard and we anticipate seeking it for TPM 2.0 in the coming months. TCG will provide a certification program as well, similar to the one provided now for TPM 1.2 implementations. In the near term, it is expected that both TPM 1.2 and TPM 2.0 will be available and that vendors will provide implementations that support both TPM 1.2 and TPM 2.0.

Technologies already supporting TPM 2.0

Intel® TXT
Including Intel TXT Toolkit, TPM 2.0 Provisioning Tools and Intel TXT Policy Generator (in development)

Boot Guard
Prevents booting of machines that fail boot measurements (expected to be available 2015)

Microsoft® Windows 8
New spec enables usage of key TPM features without user intervention for various purposes

TPM2.0 Emulator
Plugs into PLC header (or TPM module socket) and provides both hardware and software protection