Trusted Computing Group
TCG Update for ISPAB

June 16, 2004

Monty Wiseman
Security Architect
Intel Corporation

TCG Organization

TCG Mission

Develop and promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms

TRUSTED COMPUTING GROUP™

Specifications moved from TCPA to TCG

- Reasons
  - TCPA was not a formal organization
  - Lacked transparency
  - Lacked IP policies

- Results
  - Better industry participation
  - Transparent specification development process
  - Documented IP policies

TRUSTED COMPUTING GROUP™

TCG Structure

- TCG is incorporated as a not-for-profit corporation, with international membership
  - Open membership model
    - Offers multiple membership levels: Promoters, Contributors, and Adopters
  - Board of Directors
    - Promoters and member elected Contributors
  - Typical not-for-profit bylaws
  - Industry typical patent policy (Reasonable and Non Discriminatory) for all published specifications
  - Working Groups

TRUSTED COMPUTING GROUP™

TCG Organization

Board of Directors
Jim Ward, *IBM*, President and Chairman, Geoffrey Strongin, AMD, Mark Schiller, HP, David Riss, Intel, Steve Heil, Microsoft, Tom Tahan, Sun, Nicholas Szeto, Sony, Bob Thibadeau, Seagate, Thomas Hardjono, Verisigin

Marketing Workgroup
Nancy Sumrall, *Intel*

Technical Committee
Graeme Proudler, *HP*

Best Practices
Jeff Austin, *Intel*

Advisory Council
Invited Participants

Administration
VTM, Inc.

Public Relations
Anne Price, *PR Works*

Events Marketing Support
VTM, Inc.

TPM Work Group
David Grawrock, *Intel*

TSS Work Group
David Challener, *IBM*

Mobile Phone WG
Panu Markkanen, *Nokia*

Peripherals WG
Jim Wendorf, *Philips*

Server Specific WG
Larry McMahan, *HP*

Conformance WG
Manny Novoa, *HP*

PC Client WG
Monty Wiseman, *Intel*

Infrastructure WG
T. Hardjono, VeriSign / Smith, Intel

PDA WG
Jonathan Tourzan, *Sony*

User Auth WG
Laszlo Elteto, *Rainbow*

Storage Systems
Robert Thibadeau, *Seagate*

Position Key

GREEN Box:	*Elected Officers*
BLUE Box:	*Chairs Appointed by Board*
RED Box:	*Chairs Nominated by WG, Appointed by Board*
BLACK Box:	*Resources Contracted by TCG*

TRUSTED COMPUTING GROUP™

TCG Membership

- 69 Total Members as of June 8, 2004
  - 7 Promoter, 50 Contributor, 12 Adopter

Promoters
AMD
Hewlett-Packard
IBM
Intel Corporation
Microsoft
Sony Corporation
Sun Microsystems, Inc.

Adopters
Ali Corporation
American Megatrends, Inc.
Foundry Networks
Foundstone, Inc
Gateway
Industrial Technology Research Inst.
iPass
OSA Technologies
Silicon Integrated Systems Corp.
Softex, Inc.
Toshiba Corporation
Winbond Electronics Corporation

Contributors
Agere Systems
ARM
ATI Technologies Inc.
Atmel
AuthenTec, Inc.
Broadcom Corporation
Comodo
Dell
Extreme Networks
Fujitsu Limited
Fujitsu Siemens Computers
Funk Software
Gemplus
Infineon
InfoExpress, Inc.
Juniper Networks
Legend Limited Group
Meetinghouse Data Communications
Motorola Inc.
M-Systems Flash Disk Pioneers
National Semiconductor
nCipher
Network Associates
Nokia
NTRU Cryptosystems, Inc.

Contributors
NVIDIA
Philips
Phoenix
Renesas Technology Corp.
RSA Security, Inc.
SafeNet, Inc.
Samsung Electronics Co.
SCM Microsystems, Inc.
Seagate Technology
Shang Hai Wellhope Information
Silicon Storage Technology, Inc.
Standard Microsystems Corporation
STMicroelectronics
Sygate
Symantec
Synaptics, Inc.
Texas Instruments
Transmeta Corporation
Trend Micro
Utimaco Safeware AG
VeriSign, Inc.
VIA Technologies, Inc.
Vodafone Group Services LTD
Wave Systems
Zone Labs

TRUSTED COMPUTING GROUP™

Outreach programs

- Interaction with EU

  Interactive venue for EU concerns

- Best Practices

  Develop a set of documents for responsible implementations of this technology

TRUSTED COMPUTING GROUP™

TCG Introduction & Overview

Implementation Status

- Trusted Platform Modules (TPM) based on 1.1b specification available from multiple vendors
  - Atmel*, Infineon*, National Semiconductor*
- Compliant PC platforms shipping now
  - IBM* ThinkPad notebooks and NetVista desktops
  - HP* D530 Desktops and nc4010, nc6000, nc8000, and nw8000 Notebooks
  - Intel* D865GRH motherboard
  - Fujitsu* LifebookS notebook PC series
  - More expected soon
- Application support by multiple ISV's
  - Existing familiar applications are using TCG/TPM through standard cryptographic APIs like MC-CAPI and PKCS #11
- TPM 1.2 Specification announced late fall 2003
  - Atmel has announced chips based on new spec; anticipate other TPM vendors to make silicon available soon

TRUSTED COMPUTING GROUP™

* Other names and brands may be claimed as the property of others.

Goals of the TCG Architecture

TCG defines mechanisms that

- Protect user keys (digital identification) and files (data)
- Protect secrets (passwords)
- Enable a protected computing environment

While…

- Ensuring the user's control
- Protecting user's privacy

Design Goal: Delivering robust security with user control and privacy

TRUSTED COMPUTING GROUP™

TCG Policy Positions

Privacy Effect of TCG Specifications

TCG is committed to ensuring that TCG specifications provide for an increased data capability to secure personally identifiable information

Open Platform Development Model

TCG is committed to preserving the open development model that enables any party to develop hardware, software or systems based on TCG Specifications. Further, TCG is committed to preserving the freedom of choice that consumers enjoy with respect to hardware, software and platforms

TRUSTED COMPUTING GROUP™

TCG Policy Position

Platform Owner and User Control

TCG is committed to ensuring owners and users of computing platforms remain in full control of their computing platform, and to require platform owners to opt-in to enable TCG features

Backwards Compatibility

TCG commits to make reasonable efforts to ensure backward compatibility in future specifications for currently approved specifications

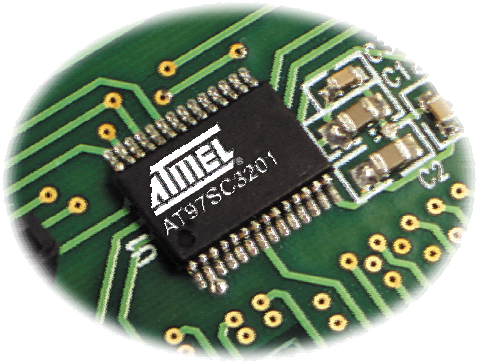
TRUSTED COMPUTING GROUP™

TCG System Benefits

- Benefits for today's applications
  - **Hardware protection for keys used by data (files) and communications (email, network traffic)**
  - **Hardware protection for Personally Identifiable Information (Digital IDs)**
  - **Hardware protection for passwords stored on disk**
  - **Lowest cost hardware security solution : no token to distribute or lose, no peripheral to buy or plug in, no limit to number of keys, files or IDs**

- Benefits for new applications
  - **Safer remote access through a combination of machine and user authentication**
  - **Enhanced data confidentiality through confirmation of platform integrity prior to decryption**

TRUSTED COMPUTING GROUP™



TPM and Malicious Behavior

- **Solutions to these problems depend on being able to build upon some kernel or root of trust**
  - This ‘root of trust’ has to be hardware – cannot ask a software system to ‘validate’ itself.
  - Cannot even rely on the PC OEM or TPM vendor – the TPM must be certified by trusted third parties.
- **The TPM can help enforce good policies and practices**
  - Constrain usage of keys or secret data to environments that are appropriate – a certain software state or only in conjunction with a hardware token like a smart card.
  - Private key data stored on a TPM cannot typically be obtained by a user under any circumstances. But it can be backed up using an authorized mechanism.
  - Access to network services can be predicated on having an approved platform and software.

TRUSTED COMPUTING GROUP™

TPM and Spam

Standard e-mail authentication schemes rely on software storage of a Digital ID, which is too easily revealed to convey much trust

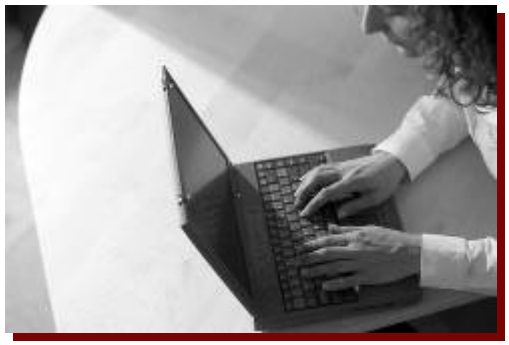
- **TPM stores Digital ID in hardware**
  - Prevents cloning by malicious software or other users
  - The recipient has an increased level of trust in that ID
- **Sender can prove to the recipient that his/her Digital ID is stored in a TPM**
  - Sender can prove that it is stored in such a way that no one (not even the PC owner) can see the private part
- **The TPM can be used to store the root(s) of trust for the certificate verification chain that is used to verify email signatures**

TRUSTED COMPUTING GROUP™

TPM and Viruses, Worms, etc.

- **TPM protects 'measurements' of software as the system is booted**
  - If BIOS or other early stage software has been corrupted, or is from a version that has a problem, it can be detected.
- **TPM can be used to provide verification that virus protection software, updates and virus description files are bona fide**
  - Modifications and/or use can depend on information sealed to a TPM/platform.
  - TPM can securely store a verifying public key (root of trust) that can be used to validate certificates attesting to the software
- **TPM can help to limit spread of email based viruses**
  - The TPM requires authentication to use the digital IDs stored in it. Assuming that the recipient requires an authenticated (signed) email, automatically generated and sent emails may lack that authentication.

TRUSTED COMPUTING GROUP™



TPM and False Identity

If a digital ID is not securely stored, or another party has no way to determine the authenticity of an ID, fraud can occur

- **Spoofing – email looks real and asks users to type in their password or other sensitive information (recent eBay scams)**
  - Retailer can store their digital ID on a TPM to prevent its misuse. Enabling signature checking on the recipient's mail reader would show this as a problem email.
- **Internet auction scams - steal an identity to sell non-existent merchandise, or create a fake account to get merchandise without paying**
  - The auction site can post information about the trust level of the ID of a party on the site – both sellers and buyers. Those with TPMs would have a higher trust level.
  - Participants can require proof of a TPM-stored ID.

TRUSTED COMPUTING GROUP™

TPM and Computer Theft

Using software tools to encrypt data on the hard disk doesn't protect against attacks on the data if the computer is stolen. The data can often be decrypted anyway.

- **TPM can protect the encryption keys to provide world class security**
  - Transforms an attack on the data to an attack on the TPM, which can provide multiple layers of defense against exhaustive attacks
- **TPM is permanently connected to the computer**
  - Some systems provide robust protection against a sophisticated attacker that might try to move the TPM to another computer
- **Use of keys can be tied to hardware state of system**
  - So the use of debuggers or other analytical tools can be detected
- **Track, Trace, Kill**
  - When the thief connects to the internet an automatic check in a data base of stolen computers occurs and the computer can be disabled at boot

TRUSTED COMPUTING GROUP™

Trusted Computing Market Drivers

- OEM Shipment and availability of the platforms
- ISV Enablement of applications that create the value of the hardware
- ROI for Trusted Platforms is easily understood
- Trusted Platforms begin to solve market requirements
  - HIPAA – Multi-Factor Authentication, Data Protection
  - Sarbanes Oxley – Strong Authentication, Data Protection
  - Safe Harbor – Data Protection
  - Gramm-Leach-Bliley - – Strong Authentication, Data Protection
  - Strong Authentication
  - Perimeter Security Problems
  - Client Component of Layered Network Security

TRUSTED COMPUTING GROUP™

Emerging Application Solutions

- **Secure Login**
  - Uses the TPM to add security and a second factor of authentication to the standard OS/Network login.
  - May be combined with other authentication technologies including fingerprint, smart card, or single sign-on.
- **Multifactor Authentication**
  - Adding a second factor of authentication to the standard userid/password for Windows login, application login, specific application feature, and authentication to the TPM.
- **Secure Email**
  - Enabling the TPM and ease-of-use in existing email programs.
- **Secure VPN and Web Services**
  - Adding strong authentication and attestation giving TPM-based machines special rights
  - Enablement and revocation of access from IT can be certificate based.
- **Data Protection**
  - Ability to secure documents with the TPM with the flexibility to store them anywhere and share them securely with others
  - Backup capabilities are critical

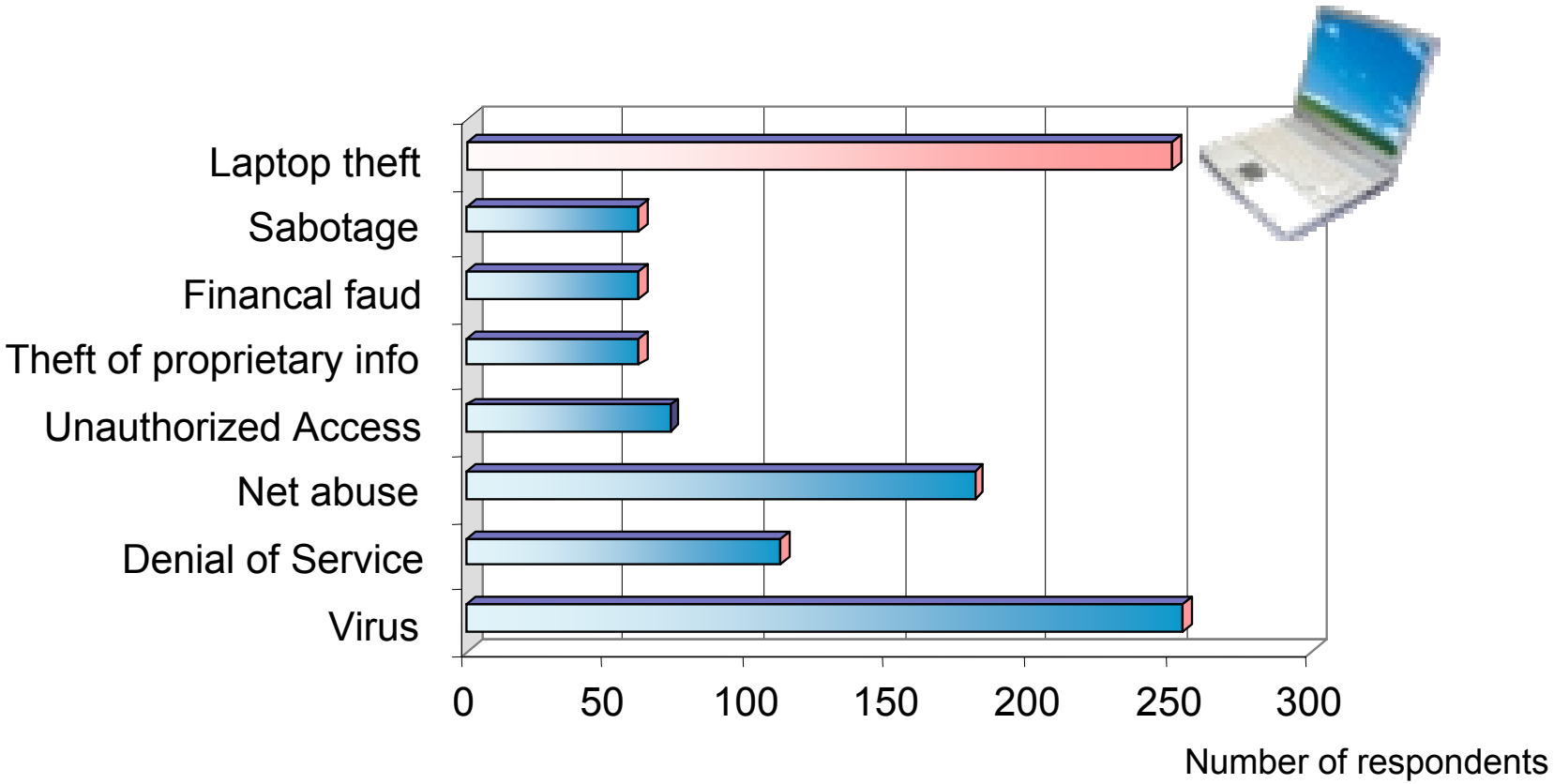
TRUSTED COMPUTING GROUP™

Emerging Application Solutions (cont'd)

- **Private and Secure Depository for Passwords & Personal Data**
  - Web and PC application password manager
  - Automated log-in process
  - Protected location for passwords and critical information
  - Web form fill with secured data
- **TPM Key Back-up, Restore and Migration**
  - Ability to recover application keys for hard drive, motherboard, or TPM failure
  - Automation, extraction from user
  - IT management capabilities
- **Digital Signature Capabilities**
  - Secure and hardware-protected certificates
  - Lifecycle management of signed documents
- **Enterprise IT Management**
  - Infrastructure for key management and platform management and certificate management
- **Secured Corporate Content for Delivery to the Desktop**
  - Ability to use the TPM to securely deliver content for corporate information
- **Secure Automatic Update**
  - Need the ability to securely update applications in real-time

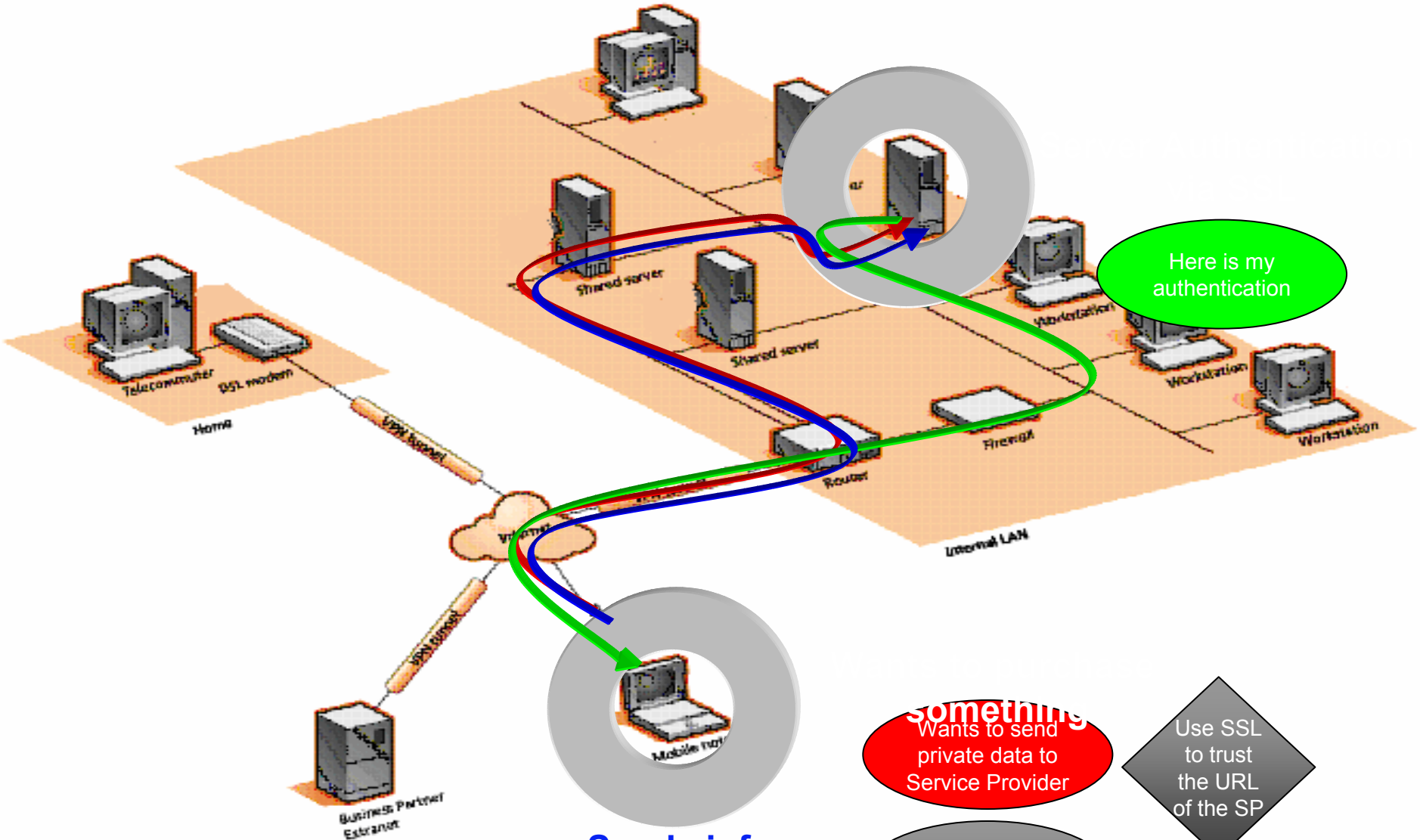
TRUSTED COMPUTING GROUP™

Risks in IT - Types of Attacks and Misuse

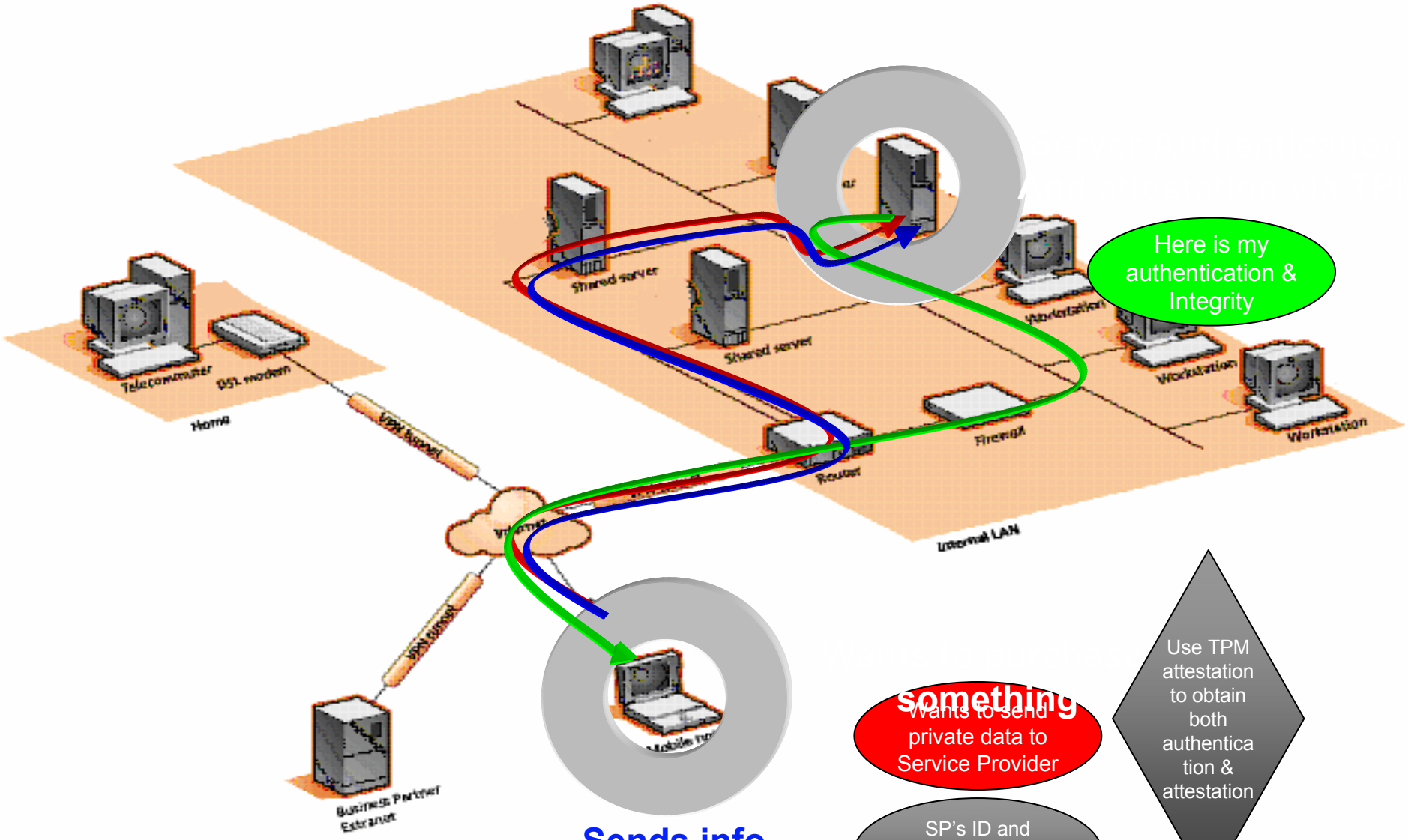


Source: CSI/FBI: Computer Crime and Security Survey 2003
http://www.gocsi.com/db_area/pdfs/fbi/FBI2003.pdf

Trust and Attestation: Today
Privacy Mechanisms and User Controls



Trust and Attestation:
TPM Privacy Mechanisms and User Controls



TRUSTED COMPUTING GROUP™

Common Misconceptions

- The TPM does not measure, monitor or control anything
  - **Software measurements are made by the PC and sent to the TPM**
  - **The TPM has no way of knowing what was measured**
  - **The TPM is unable to reset the PC or prevent access to memory**
- The platform owner controls the TPM
  - **The owner must opt-in using initialization and management functions**
  - **The owner can turn the TPM on and off**
  - **The owner and users control use of all keys**
- DRM is not a goal of TCG specifications
  - **All technical aspects of DRM are not inherent in the TPM**
- TPMs can work with any operating systems or application software
  - **The spec is open and the API is defined, no TCG secrets.**
  - **All types of software can (and will, we hope) make use of the TPM**

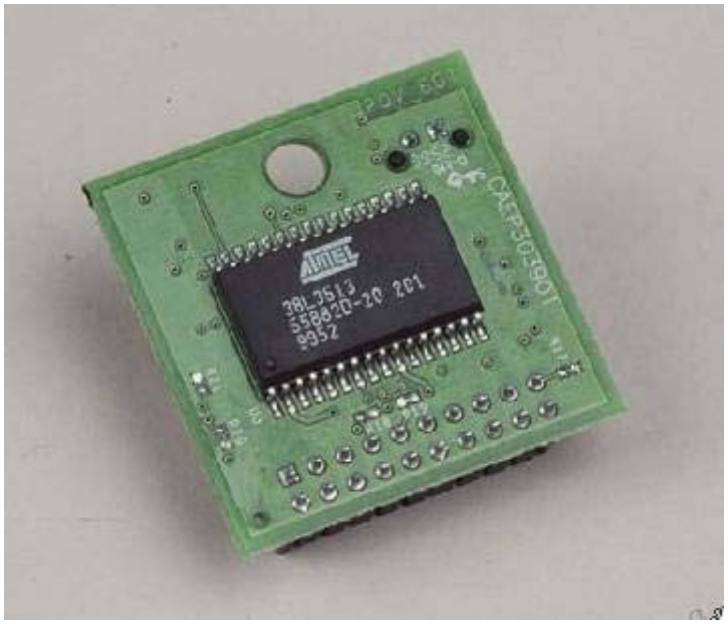
TRUSTED COMPUTING GROUP™

TCG Technology

The Trusted Platform Module

A silicon chip that performs all TPM v1.1 functions, including:

- Can store OS status information
- Generate and store a private key
- Hashes files using SHA-1
- Creates digital signatures
- Anchors chain of trust for keys, digital certificates and other credentials



TRUSTED COMPUTING GROUP™

TPM Abstract Architecture

- Module on the motherboard
  - Can't be removed or swapped
  - Secrets in module can't be read by HW or SW attackers
- Stores Private Keys
  - Perform the private key operation on board so that private key data never leaves TPM
- Hold Platform Measurements
  - PC measures software, TPM is repository of measurements

TRUSTED COMPUTING GROUP™

TPM Architecture

- Turnkey Secure Module
  - **Internal CPU to implement all TPM commands**
  - **Internal math engine to accelerate computation of asymmetric algorithm operations**
  - **Tamper resistance to prevent physical attacks that might reveal TPM or user secrets.**
  - **Communications channel to main processor (LPC typical)**
- Asymmetric Details
  - **RSA support mandatory, other algorithms optional. 512 through 2048 bit key length. On board key generation.**
  - **On board key cache stores frequently used keys, arbitrary number stored on disk. Off chip keys are protected using key that never leaves TPM.**
  - **Keys can be migrated from one TPM to another – if both the TPM owner and the key owner authorize the operation and if the key has been appropriately tagged at creation**

TRUSTED COMPUTING GROUP™

TPM Architecture (cont'd)

- Integrity Metric Storage
  - **Multiple instances of Platform Configuration Registers (PCR)**
  - **Can be extended (hash with new value) but not cleared**
  - **Key usage can be connected to desired values**
  - **Platform can provide attestation of current values**
- High Quality Random Number Generator
  - **Used to prevent replay attacks, generate random keys**
- SHA-1 Hash Computation Engine
  - **Multiple uses: integrity, authorization, PCR extension, etc.**
- Nonvolatile memory
  - **Owner information (on/off, owner auth secret, configuration)**
  - **Platform attestation information**

TRUSTED COMPUTING GROUP™

Persistent Keys

- Endorsement Key (EK)
  - Provide controllable uniqueness
  - Permanent
  - Not part of the key hierarchy
- Storage Root Key (SRK)
  - All keys are protected by this key
    - Root of Key Hierarchy
  - Changed on new owner

TRUSTED COMPUTING GROUP™

Key Types and Classes

- Storage Keys
  - Protects keys or external data
- Signing Keys
  - Digital signatures
- Attestation Identity Keys (AIKs)
  - Special Signing keys
  - Provides attestation
- Non-Migratable Keys
  - Permanently bound specific TPM, i.e., platform
- Migratable Keys
  - Can be migrated to other platforms
- Certified Migratable Keys
  - Can be migrated to only “certified” authorities

TRUSTED COMPUTING GROUP™

Protected Storage

Seal / Unseal

- Purpose:
  - Seals data on the platform, to the platform
- Data Seals to the specific platform
- Data *may* be sealed to a platform's configuration
- All above restrictions apply even if valid authentication material present

Bind / Unbind

- Purpose:
  - Allows external app to send encrypted data to a specific one or set of platforms
- Bind is an external operation
  - Asymmetric encryption
- Unbind is a TPM operation
- Unbind key can be:
  - Sealed to a specific platform
  - A non-migratable key

TRUSTED COMPUTING GROUP™

Auxiliary 1.1 Functions

- Digital Signature functions
  - Signs a value using a TPM-protected signing key
- Random Number Generator
  - Use for internal nonce and get generation
  - Expose for external use

TRUSTED COMPUTING GROUP™

New 1.2 Functions

- Locality
  - Signals the TPM that a message is from a trusted process within the platform
- Delegation
  - Allows the owner of the TPM and objects to delegate their use
- Clear Endorsement Key
  - Optional command. Allows owner to clear out existing EK and establish a new one.
- NV Storage
  - Provides access controlled TPM-protected storage of any type of small data
- Monotonic Counter
  - Always incrementing counter. Usages include hardening audit capabilities
- Tick Counter
  - Allows a relative time to be associated with a command
- Transport Session
  - Protects data during transport to and from the TPM
- Context Management
  - Improves performance

TRUSTED COMPUTING GROUP™

Infrastructure WG Focus Areas

- Framework Architecture
  - Define usages, architecture and services necessary to support trusted computing
  - Platform deployment lifecycle provides context
- Trusted Network Connect (subgroup)
  - Defines protocol and schema supporting client authentication and integrity validation at network connect time
  - Includes 802.1x, wired, TLS and IPsec VPN connection methods
- Integrity Management and Services
  - Defines protocol and schema for collecting / querying integrity values and assertions for known good components
- Credentials
  - Defines data structures for EK believability and AIK issuance
- Key Backup and Migration Services
  - Defines protocol and schema for key backup and migration services

TRUSTED COMPUTING GROUP™

TPM Provides Enhanced Protection for Business

Usage	Protection	Examples
Hardened Data Protection	Helps protect the integrity and confidentiality of data assets through hardware-based protection of encryption keys	**Email, file encryption**
Hardened Electronic Digital Signatures	Increases confidence in digital signature operations by providing hardware-based protection of Digital IDs. Prevents cloning by performing signature operation in tamper resistant hardware.	**Online purchases, contracts**
Hardened User Authentication	Helps protect integrity and confidentiality of user login credentials. Can also act as the “something you have” in multi-factor authentication scenario	**Can replace smart cards, secure tokens**
Hardened Platform Authentication	Helps to ensure that only authorized platforms and users gain access to corporate network and that security policy settings / security software haven't been attacked.	**Virtual Private Networks (VPN)**

Value proposition speaks to urgent needs of security-minded businesses

TRUSTED COMPUTING GROUP™