Trusted Computing: How to Make Your Systems and Data Truly Secure

Thursday, May 26, 2005

8:30 am – 11:30 am

Booth #1743

Agenda

8:30 am	Introduction Brian Berger, *Wave Systems*
8:35 am	Keynote Speaker Roger Kay, *IDC*
9:05 am	TCG Architecture Monty Wiseman, *Intel*
9:25 am	Open Source Solutions Dr. David Safford, *IBM*
9:45 am	Writing and Using Trusted Applications Alexander Koehler, *Utimaco Safeware AG*; Steven Sprague, *Wave Systems*
10:30 am	Trusted Storage and Applications Michael Willett, *Seagate Technology, Inc.*
10:50 am	Trusted Network Connect Overview Jon Brody, *Sygate Technologies*
11:15 am	Q&A

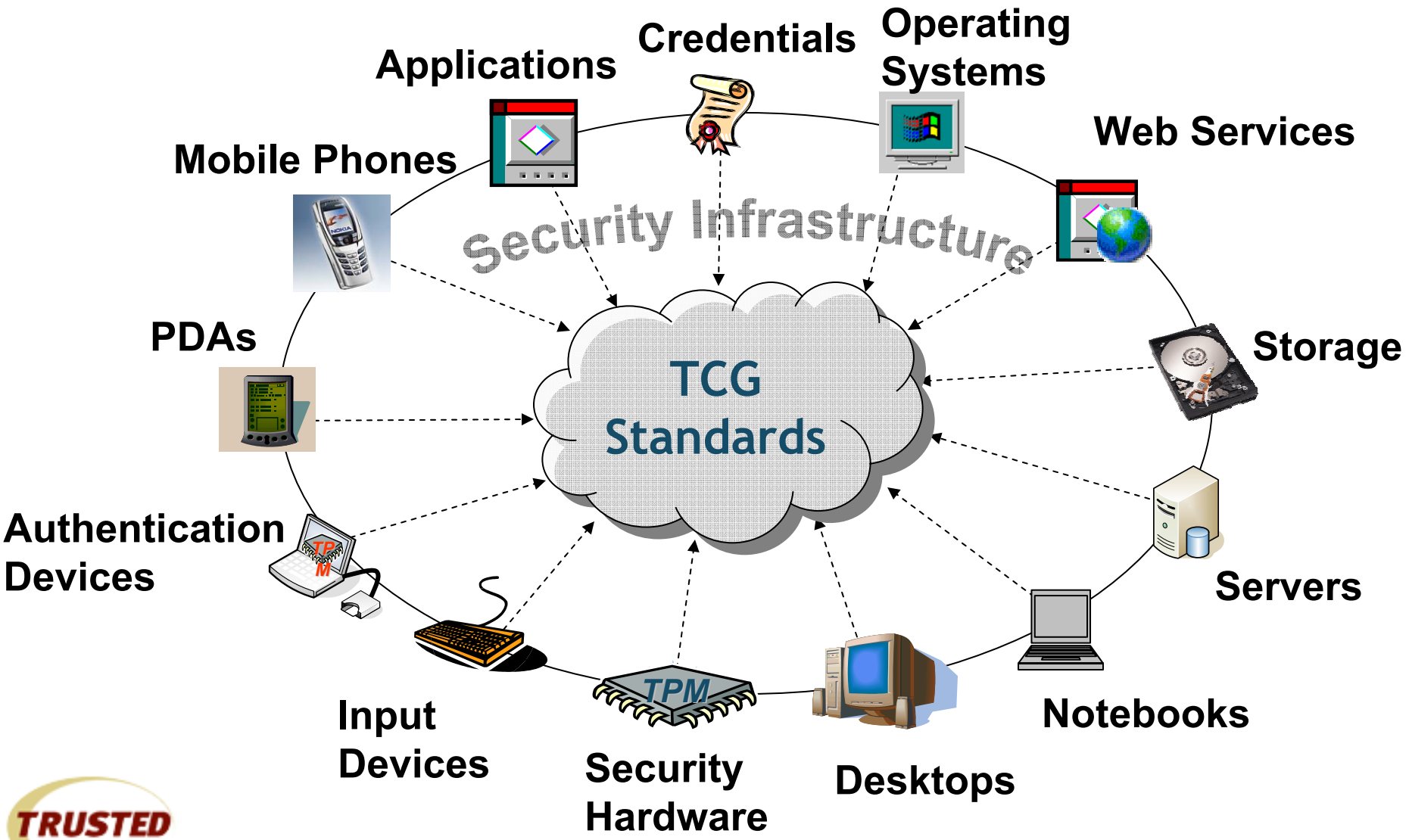
TRUSTED COMPUTING GROUP™

TCG Mission

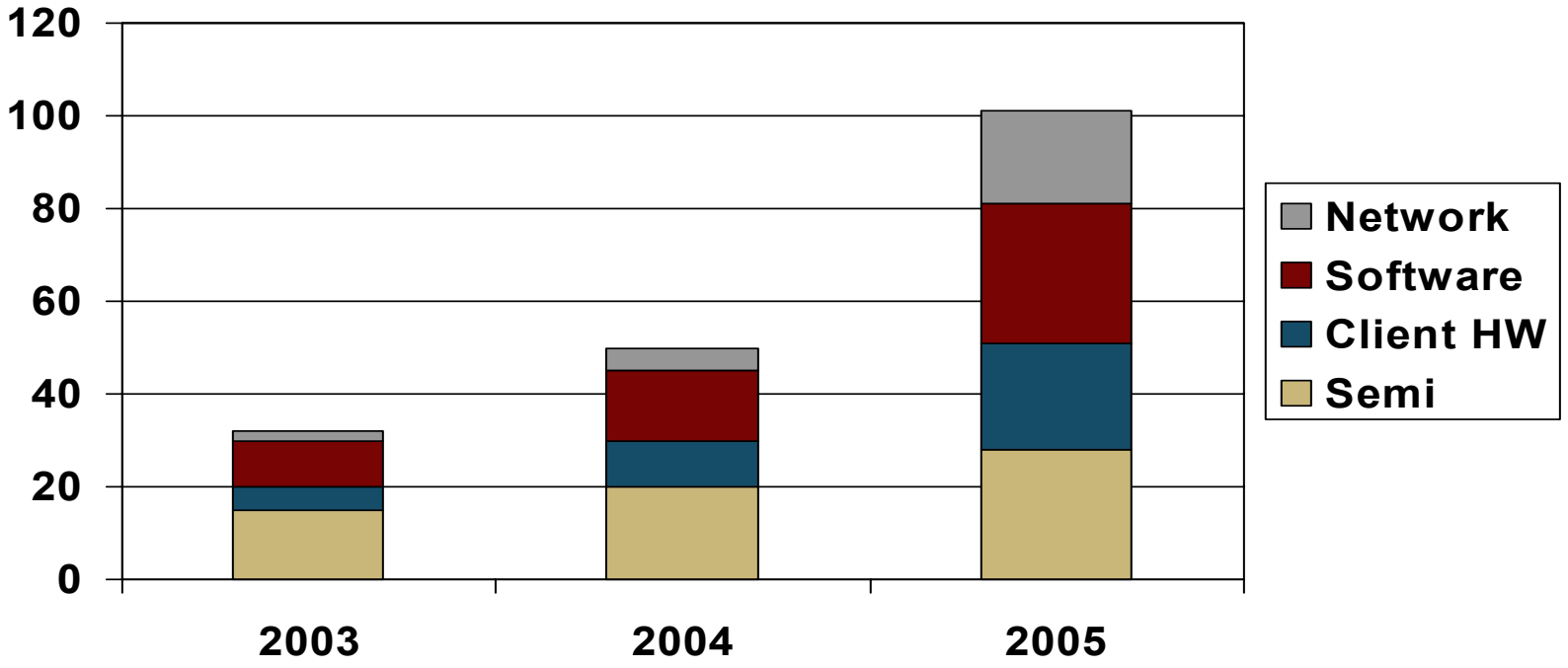
Develop & promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms.

TRUSTED COMPUTING GROUP™

Trusted Computing: The "BIG" Picture



TCG Membership Momentum



- 103 Member company's as of May, 2005
- BOD – AMD, HP, IBM, Intel, Microsoft, Seagate, Sony, Sun, Verisign

TRUSTED COMPUTING GROUP™

Agenda

8:35 am

Keynote Speaker
Roger Kay, *IDC*

Roger L. Kay *is IDC's Vice President of Client Computing. He has responsibility for covering technological, market, and competitive developments related to desktop and portable personal computers. In his capacity as leader of the PC client team, Mr. Kay authors research on competition, technology, and markets in the PC business; produces forecasts; speaks at IDC and other industry forums; contributes to consulting projects; and advises PC industry participants on desktop and notebook matters.*

TRUSTED COMPUTING GROUP™

IDC
Analyze the Future

The Future of Trusted Computing

Roger L. Kay
Vice President
Client Computing

40
CELEBRATING 40 YEARS
INTEGRITY • ACCURACY • INSIGHT

Agenda

- Philosophy, history, and issues
- TPM forecast
- A bit about trusted network access
- Final notes

A Sea Change in Public Thinking

IDC
Analyze the Future

- Before 9/11, people wanted all the privacy they could get
  - Only criminals had fingerprints on record
- Post 9/11, people want to be known as who they are
  - Identity theft and other heretofore unknown dangers
  - Increased value of stored data
- This change creates a base for mass acceptance of security features in the computing environment

Recap of Efforts Thus Far

- IBM pioneered technology in 1999
- Gave to Trusted Computing Platform Alliance October 1999
- TPM 1.1b spec released 1Q02
- Grand plans for broad usage: PKI
- Formation of Trusted Computing Group April 2003
- TPM 1.2 final spec released February 2005
- Focus on client authentication seen as more realistic near-term goal
- Broad adoption by industry in 2005
- Discrete
  - e.g., Atmel TPM
- Integrated
  - e.g., Super I/O of Winbond, Network chip of Broadcom, Processor of Transmeta
  - More to come

Hardware Security: The Right Answer

IDC Analyze the Future

- In 2000, nCipher of Cambridge, England proved that software-based security had fatal flaws
  - Came up with algorithm that searched main memory, looking for a high degree of entropy
  - Good random numbers have a high degree of entropy
  - In software security, the key, algorithm, and data to be encrypted must be in main memory at the same time
  - With a Trojan horse like Back Orifice and the nCipher algorithm, an Internet intruder could take command of a PC with only software security and gather its private keys
- In hardware security, cryptographic operations are routed through the TPM chip, giving a greater degree of protection

Segment Behavior

- Enterprise
  - Policies can be set by fiat
  - Perimeter defined
  - Corporate is trusted 3rd party
- Consumer
  - Nobody sets policies for everybody
  - Credentials could be passed around
  - There is no trusted 3rd party

Segment Adoption

- Enterprise picks and chooses
  - Justification is easier, but conservatism leads to slow adoption
  - However, many will “buy up” in hardware to prepare for arrival of Longhorn

- Consumers take what’s on the shelf
  - Uptake could be rapid once integration and trust issues are solved

Client Side Access Control

- Biometrics, particularly fingerprint, will dominate
- What you are as opposed to what you know or what you have
- Multifactor
- Fingerprint reader paring with TPM lags

Integrated vs. Discrete

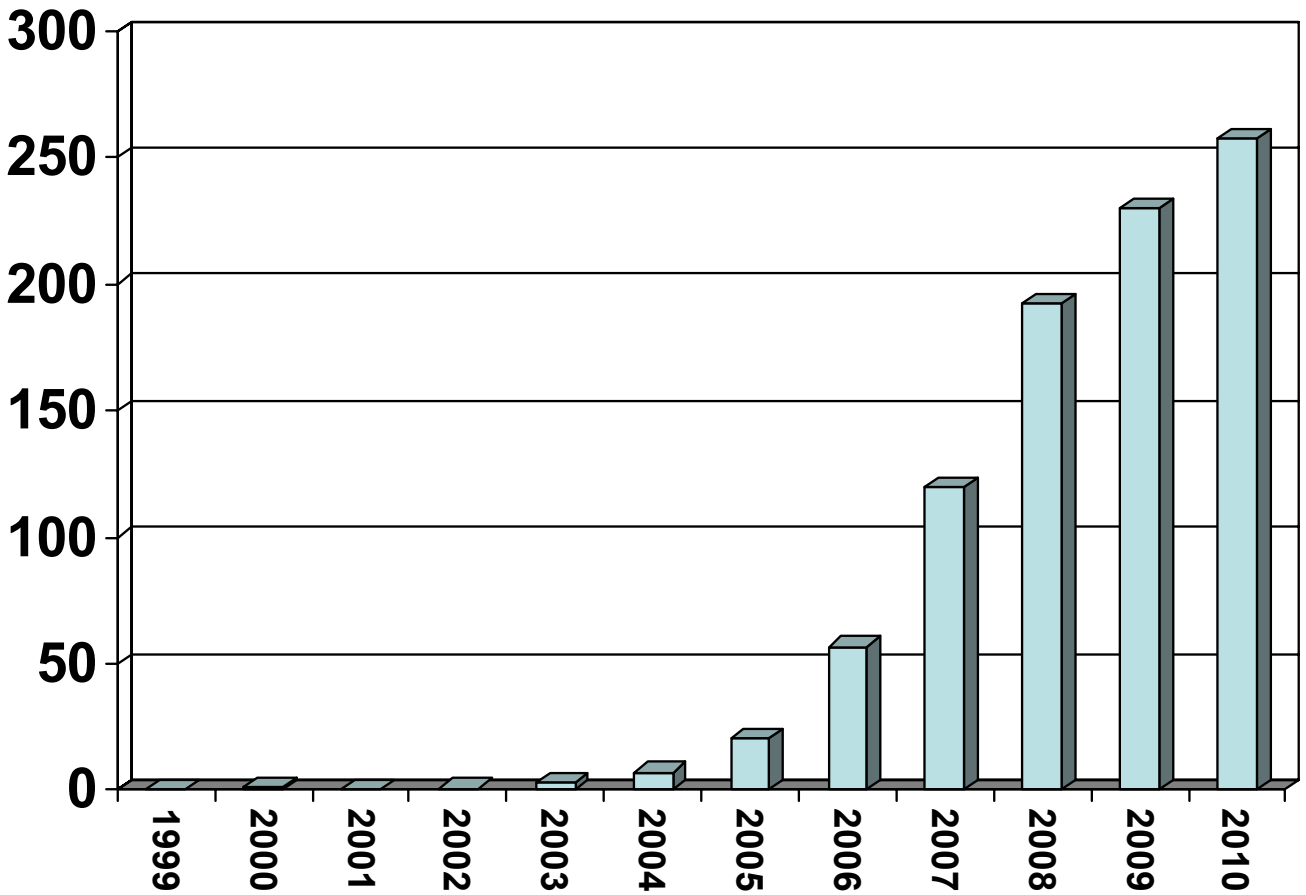
- Integration beats discrete on cost
- Discrete could have 10-20% of the market over time, sold as being more resistant to hacking
  - Having a FIPS-4 part will be required in some cases, desirable in others
- Must solve flash in South Bridge issue for complete integration in core logic
  - Intel was burned badly by the CPU serial number fiasco in 1999, but it's a new world
- Some countries worry about where they're made:
  - Today: Taiwan, China, Germany, United States, others

TPM Forecast Assumptions

- Big boosts to hardware security solution:
  - Dell entry in 2005
  - Most OEMs commit strongly in 2005 with 1.2 spec
  - Longhorn (N.G.S.C.B.) incorporation in 2006
  - Intel integration in South Bridge by 2008
  - Saturation of client space by 2010

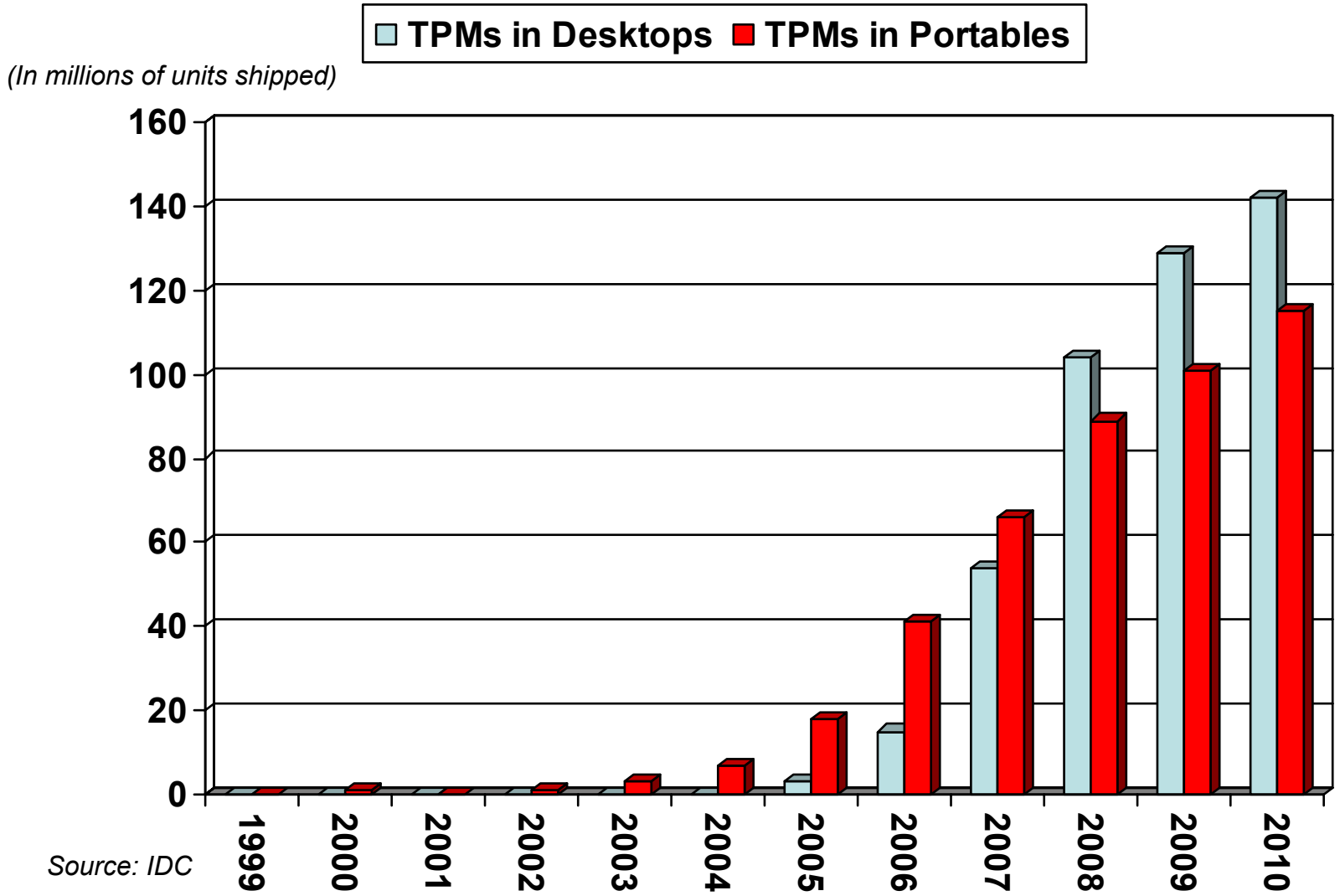
TPM Module Forecast

(In millions of units shipped)



Source: IDC

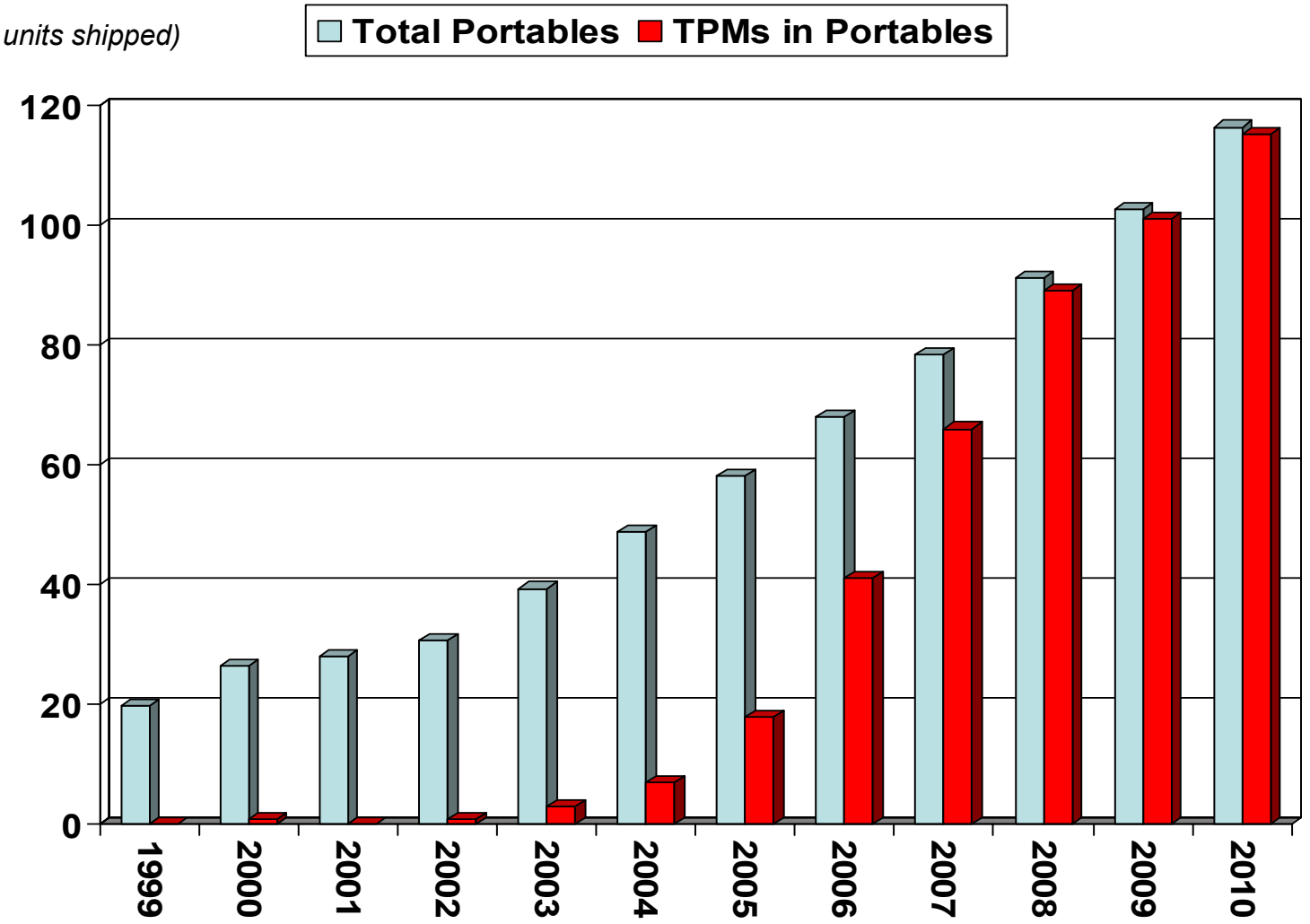
Notebook vs. Desktop



Source: IDC

TPM Attach: Portables

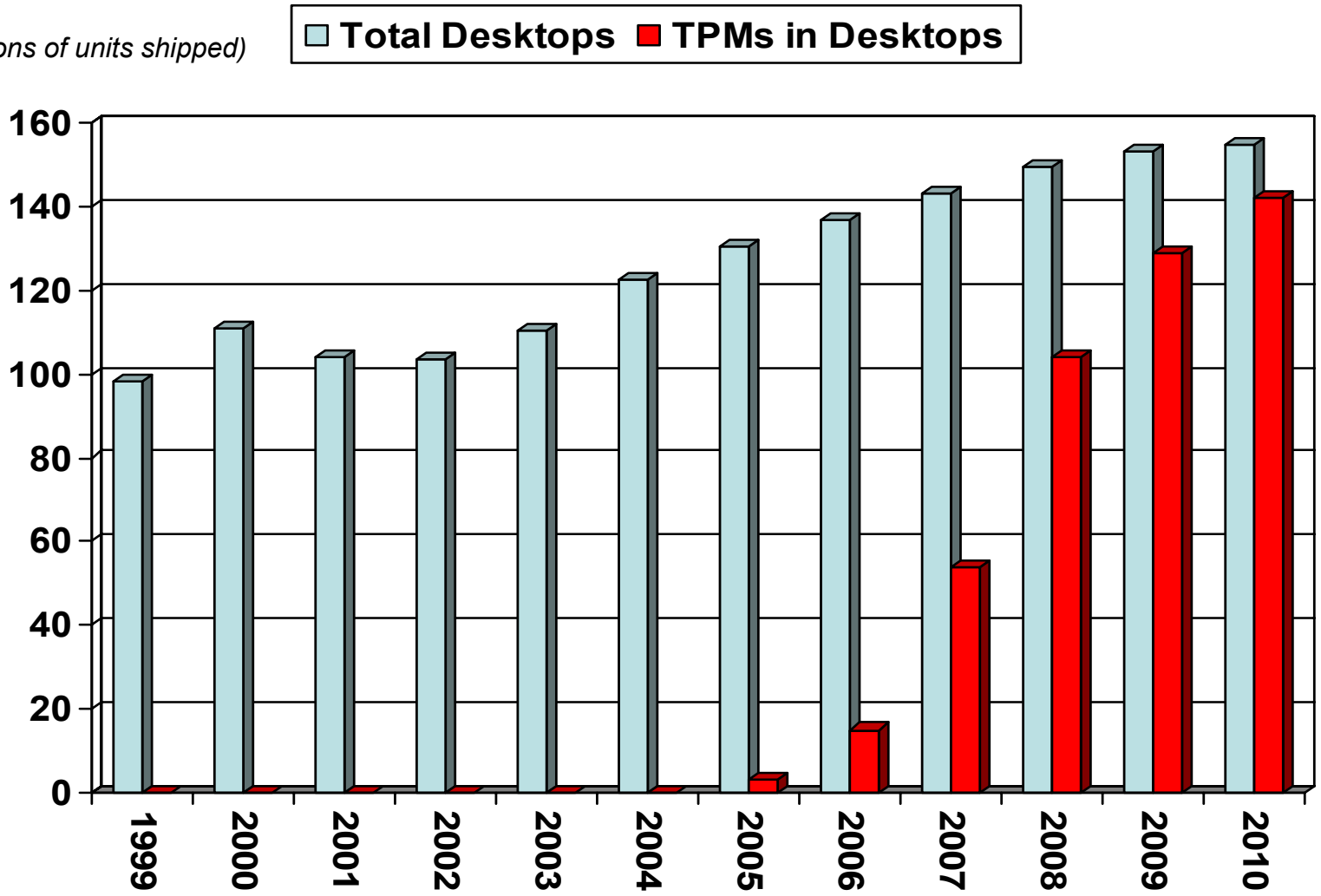
(In millions of units shipped)



Source: IDC

TPM Attach: Desktops

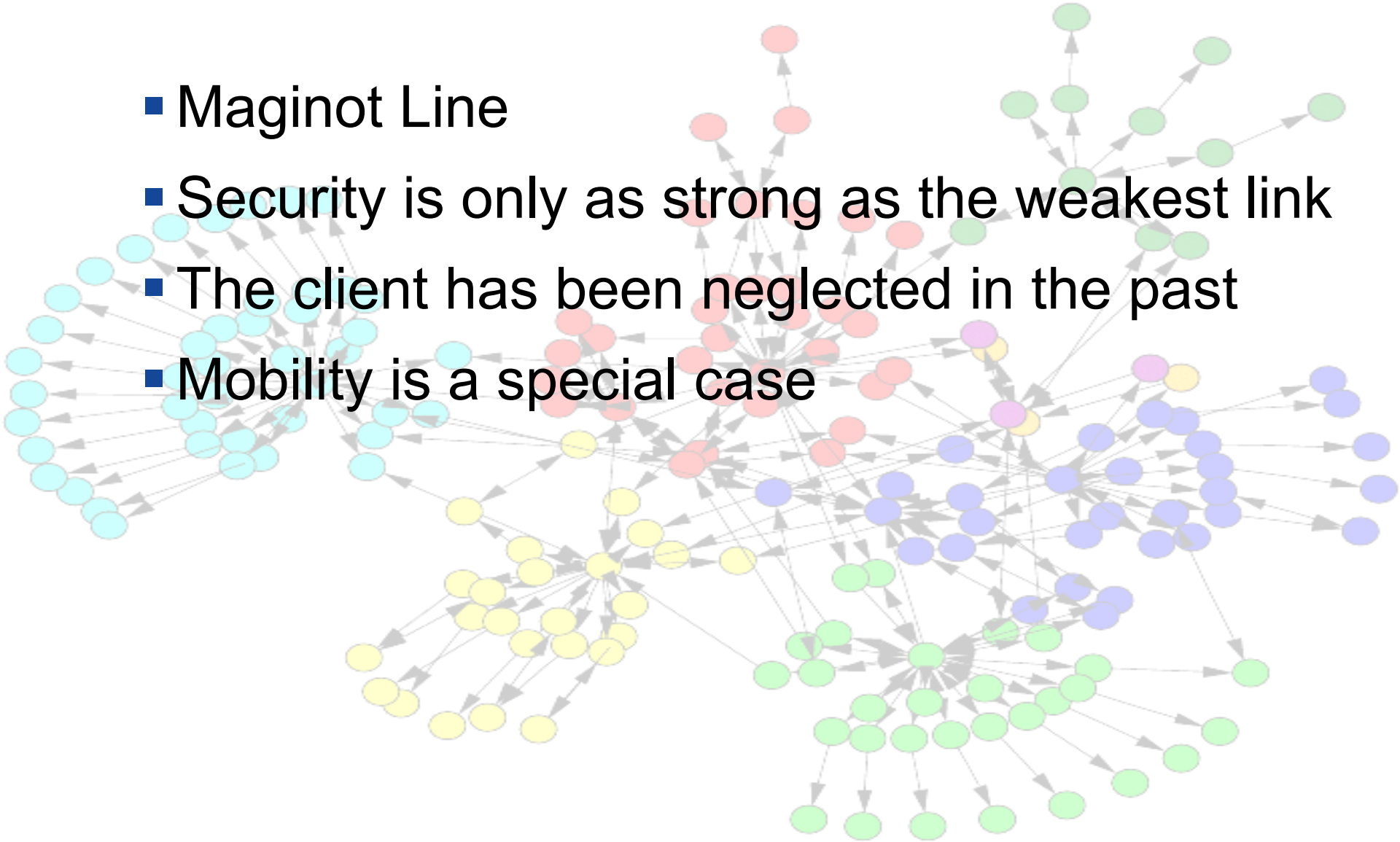
(In millions of units shipped)



Source: IDC

Network Security: A Perimeter Problem

IDC Analyze the Future



- Maginot Line
- Security is only as strong as the weakest link
- The client has been neglected in the past
- Mobility is a special case

Trusted Network Connect

IDC Analyze the Future

- What is TNC?
  - Represents a significant, high profile development directly applicable to today's network operations
  - Introduced in April 2005, an open standard that allows network operators to establish policies for client access
  - Presents a roadmap for technology development and deployment
  - As a standard, allows components from many vendors
- Establishes endpoint profile and integrity before allowing entry to a trusted network
  - TNC Client — collector of integrity information, including TPM data, bundles as part of network access request
  - TNC Server — determines quality of client compliance, hands off to quarantine and remediation or to the network or bounces, depending on policy

Final Notes

- Other specs are in the works:
  - Server
  - Mobile phone
  - Peripherals
    - Storage
    - Keyboard and mouse
  - Infrastructure
  - PC
  - Software
- The exciting news: TCG is applying the trust specification developed for PCs to a broader — potentially universal — set of devices

Contact Info

Please email me at
Rkay@idc.com

Agenda

9:05 am

TCG Architecture
Monty Wiseman, *Intel*

Monty Wiseman *is currently a Security Architect for Intel's Desktop Architecture Lab. His areas of specialty include high performance mass storage systems, filesystems, directory services, and authentication mechanisms. His current projects include architecture for TCG and Intel's LaGrande Technologies. He has 20 years experience in Desktop, Network and Mainframe environments holding security related and other engineering positions at Novell, Fujitsu, and Control Data.*

TRUSTED COMPUTING GROUP™

TCG Architecture: The Trusted Platform Module

Monty Wiseman
monty.wiseman@intel.com
Security Architect
Intel, Corp.

TPM Abstract Architecture

- Core component is a Trusted Platform Module (TPM)
  - Protected storage
  - Protected operations
  - Platform authentication under user control
    - User control to handle the uniqueness appropriately
- Platform Specific Specifications
  - Defines how a TPM is implemented on specific platforms
    - Does not define mechanisms
- Infrastructure
  - How TPMs and TCG-enabled platforms exist and interact within the enterprise

TRUSTED COMPUTING GROUP™

TPM Key Features for Platforms

- Indicates platform as “valid”
  - Platform is the one issued by IT
- Indicates platform is in a “valid” or authorized state
  - Platform configuration
    - Are Pre-OS, OS & Apps what IT has authorized
- Protected storage
  - Uses isolated environment to protect keys

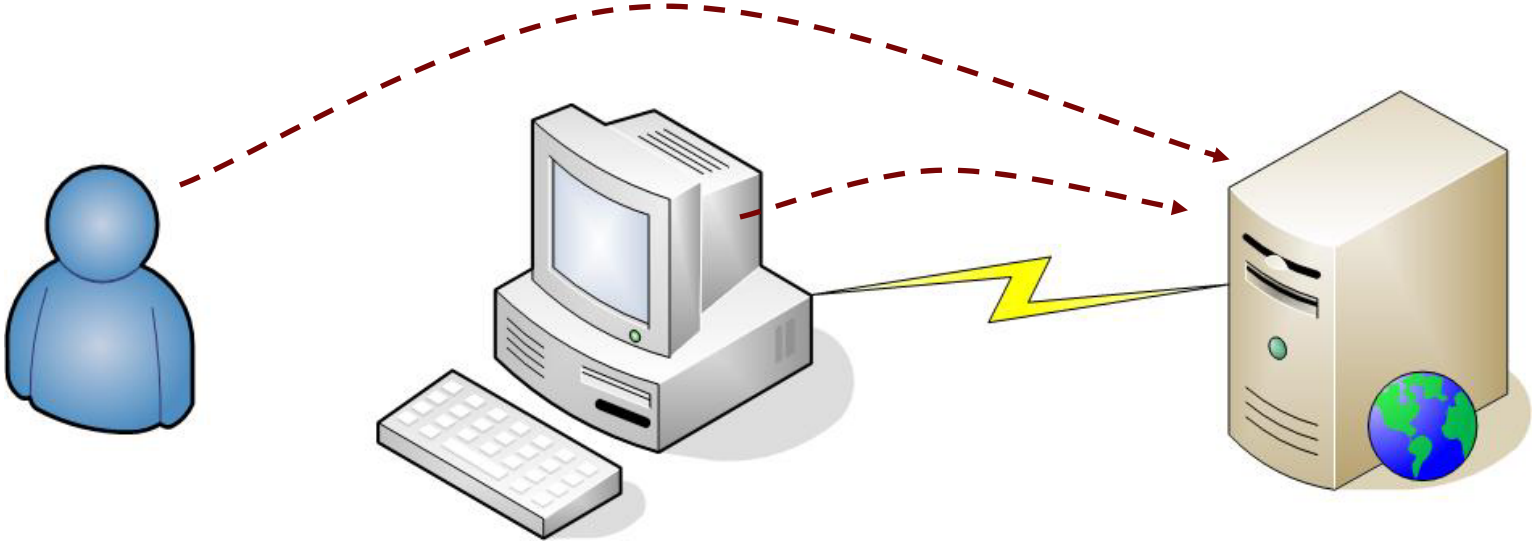
TRUSTED COMPUTING GROUP™

TPM Overview

- Module on the motherboard
  - Can't be moved or swapped
  - Secrets in TPM can't be read by HW or SW attackers
- Uses asymmetric cryptography
  - Private key operations occur inside TPM
  - Default keys are 2048-bit RSA
- Holds Platform Measurements
  - PC measures software, TPM is repository of measurements
  - Multiple repositories, or Platform Configuration Registers (PCR)
  - Can only extend PCR, hash with new value, not write directly
- Using signature key can report on PCR contents
- High Quality Random Number Generator
- SHA-1 Hash Computation Engine
- Nonvolatile memory

TRUSTED COMPUTING GROUP™

Platform Authentication



- Applications tend to focus on “user authentication”
- But how does the IT infrastructure know which platform is being used?
  - Is it authorized to be attached to the network?

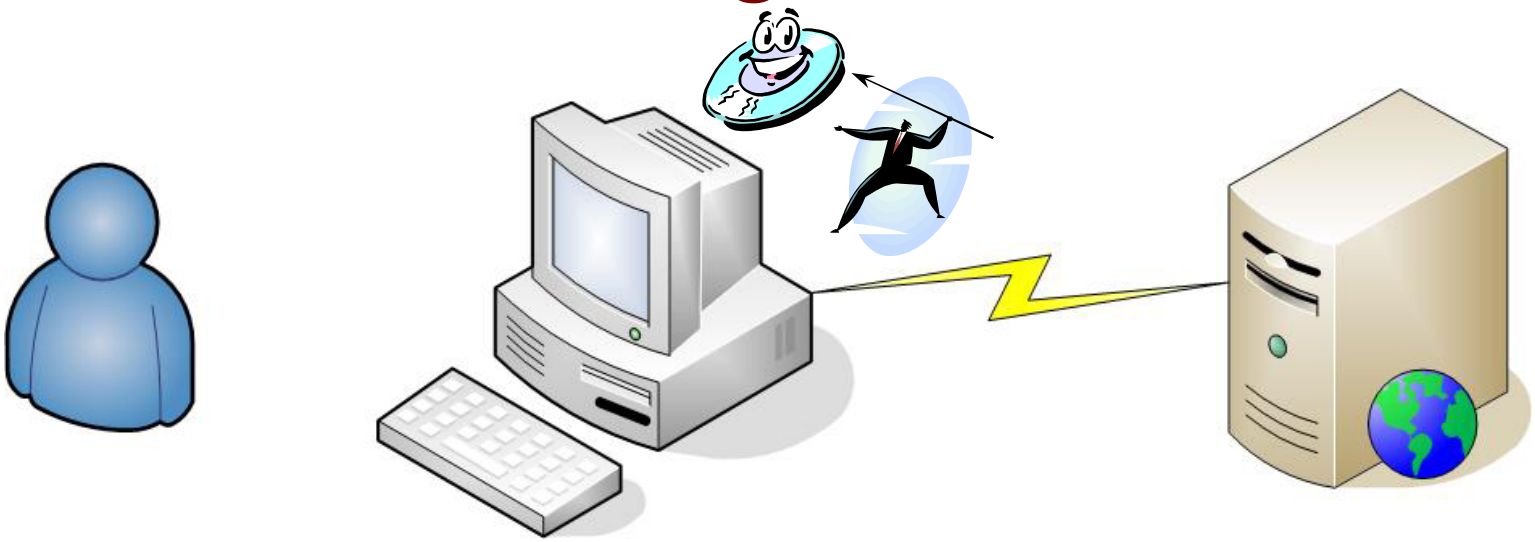
TRUSTED COMPUTING GROUP™

Platform Attestation

- Applications tend to assume they have not been attacked
  - Especially true of “monitoring” or “defensive” apps
- But how does the IT infrastructure know if the platform is executing the application as authorized?

TRUSTED COMPUTING GROUP™

Protecting Secrets

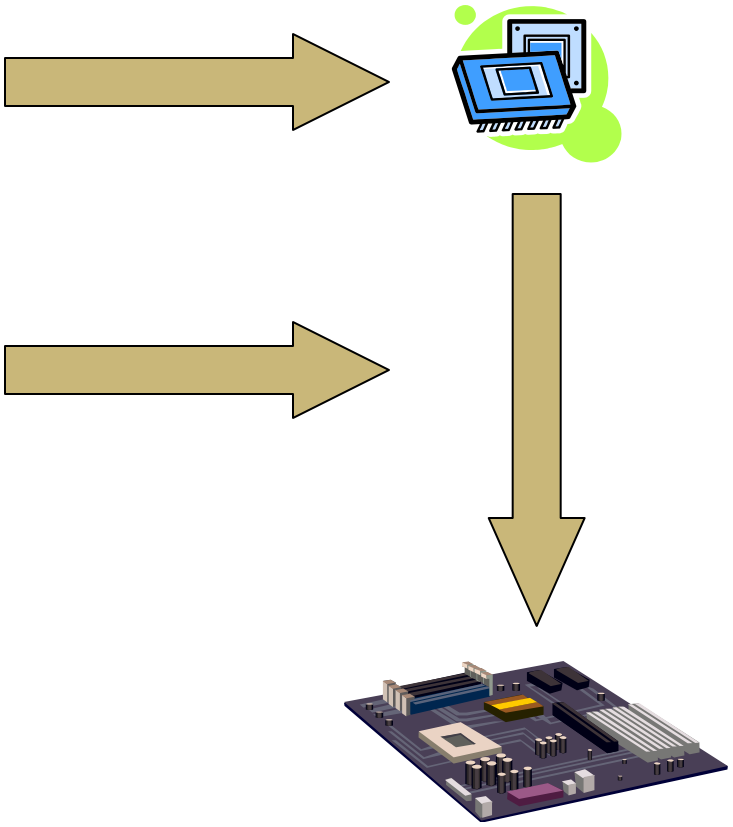


- OS and Applications use software to protect keys and secrets
  - They lack a standardized and isolated place to create, store and use them
- All software can be attacked
  - Offline attacks are not difficult

TRUSTED COMPUTING GROUP™

Purview of Specifications

- TPM Specification defines only the protected capabilities of the TPM
  - Functionality not specific to any type of platform
  - Bus protocol and type not defined
- Platform Specific Specifications define attachment of TPM to platform
  - Bus
  - H/W protocol
  - Specific integrity metrics



TRUSTED COMPUTING GROUP™

Ongoing Work In The TCG

- Platforms
  - PC Client
  - Server
  - Mobile
  - Peripherals and Storage
- Infrastructure
  - TNC
  - Credential formats
- Work is progressing
  - If you or your company are interested please join TCG and participate

TRUSTED COMPUTING GROUP™

Implementation Status

- PCs with TPMs available; millions deployed
  - Dell
  - IBM* ThinkPad notebooks and NetVista desktops
  - HP* D530 Desktops and nc4010, nc6000, nc8000, and nw8000 Notebooks
  - Intel* D945GNTLKR, D945GTPLKR, D945GCZLKR motherboards
  - Fujitsu* LifebookS notebook PC series
  - Toshiba, Acer, Gateway and others
- Application support by multiple ISV's
  - Familiar applications use TPM through standard cryptographic APIs like MS-CAPI and PKCS #11
  - Single sign-on, password management, hard drive encryption and others now available

TRUSTED COMPUTING GROUP™

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

Dispelling 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**
- TPMs can work with any operating systems or application software
  - **The spec is open and the API is defined; specs available publicly**
  - **All types of software can (and will, we hope) make use of the TPM**

TRUSTED COMPUTING GROUP™

Thank You

Agenda

9:25 am

Open Source Solutions
Dr. David Safford, *IBM*

Dr. Dave Safford *manages the Global Security Analysis Lab in IBM's T.J Watson Research Center in Hawthorne, New York, where he directs research in security analysis tools, data forensics, security hardware, secure Linux, security engineering, and ethical hacking.*

His current research includes work on the Distributed Wireless Security Auditor for 802.11 networks and Linux support for the Trusted Computing Trusted Platform Module component.

TRUSTED COMPUTING GROUP™

Open Source Solutions

Dave Safford, IBM Research

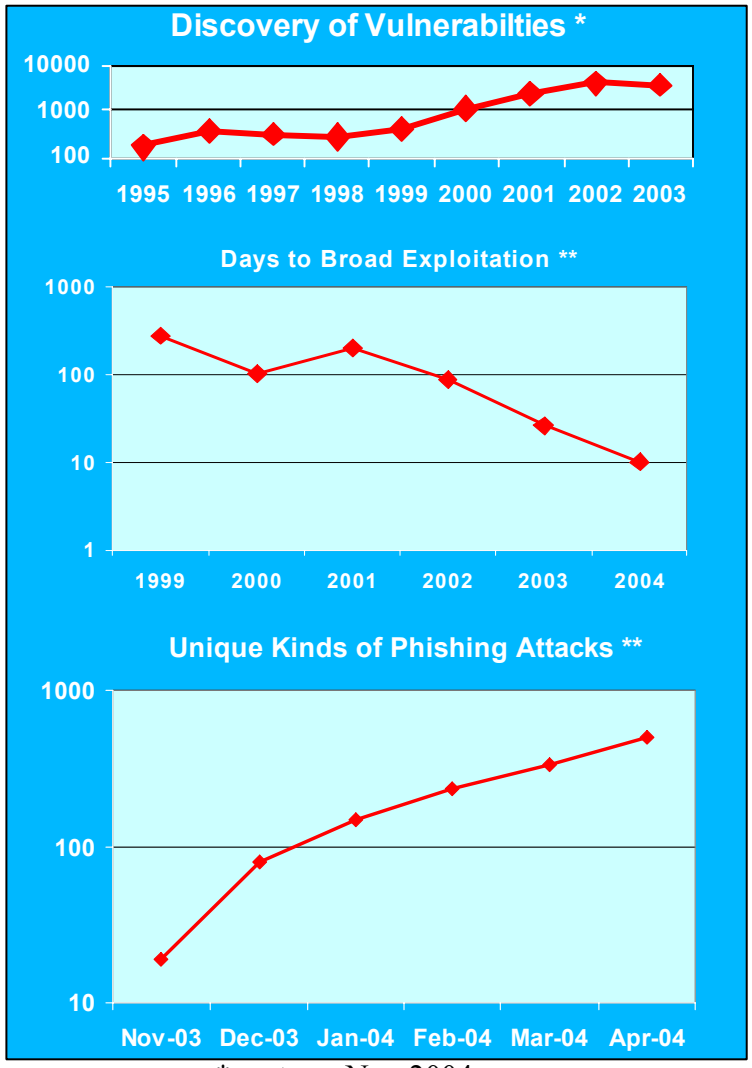
Outline

- Threat Trends
- Trusted Computing
- Open Source Projects
- What's Missing
- The Future

TRUSTED COMPUTING GROUP™

Client Risk is Rising

- The number of attacks in the wild, and their lifetimes and impact are growing fast
  - 450% increase in Windows viruses over last year
  - 1500% growth in BotNets Jan to Jun 2004
  - Viruses are already deploying attacks against AV software
  - 80% of clients have spyware infestations
  - 30% of clients already have back doors (FSTC)
- The time between the publication of a security vulnerability and the broad exploitation of it is markedly decreasing
- Financial losses rapidly increasing:
  - Phishing attacks: $500M direct losses in first half of 2004
  - Identity theft is the fastest growing crime in US



* cert.org Nov 2004
**July2004 Information Security

A Trusted Platform Module (TPM) Can Help

- RSA crypto
  - key generation, signature, encrypt, decrypt
- Secure storage
  - private keys
  - master keys (eg loopback)
- Integrity measurement
  - Platform Configuration Registers (PCR)
  - compromise detection
  - Tie key use to uncompromised environment
- Attestation
  - host based integrity/membership reporting
  - (RSA 2004 Demo)

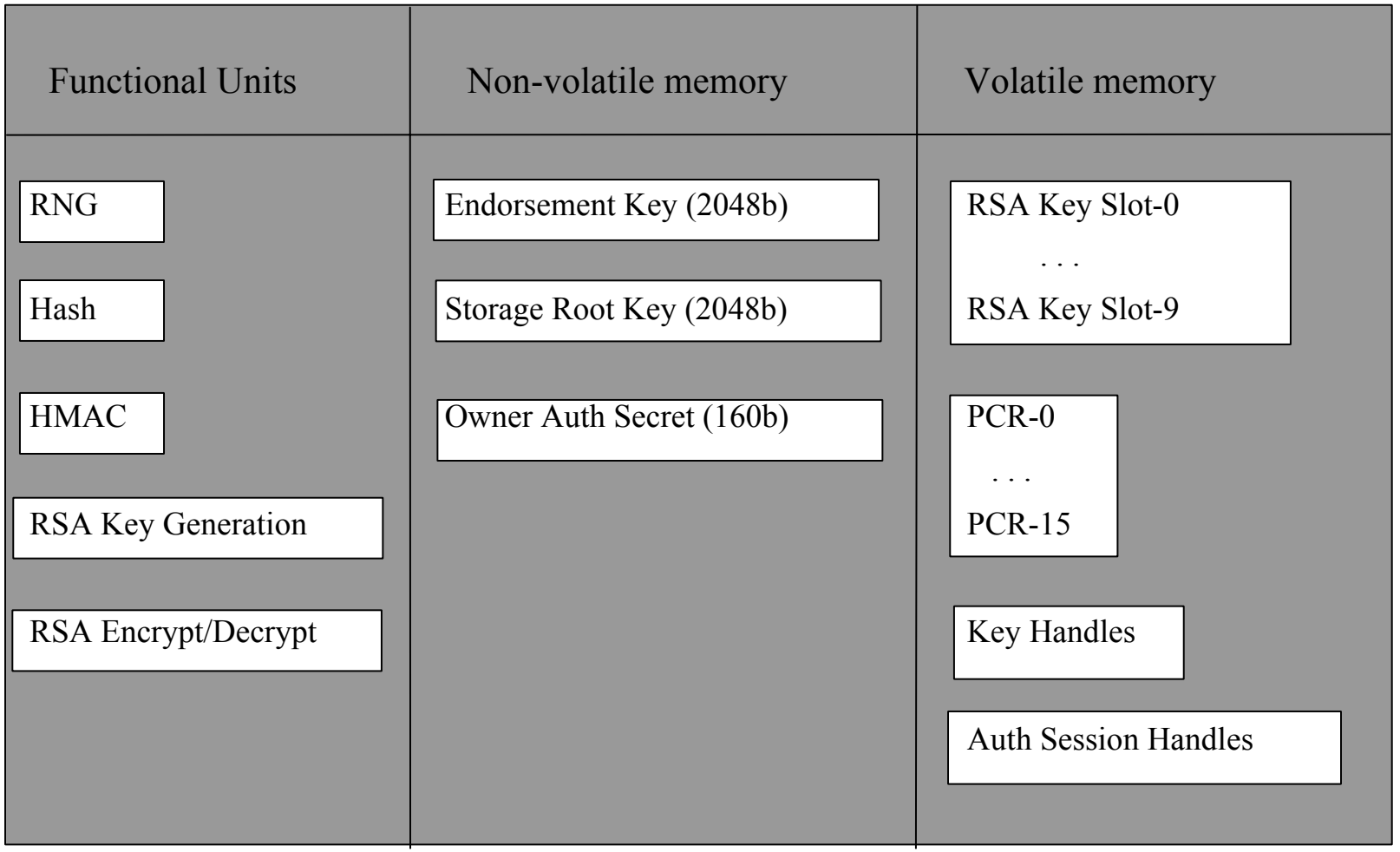
TRUSTED COMPUTING GROUP™

Understanding The TPM:

- Main Specification:
  Trusted Computing Group (TCG) home page:
  http://www.trustedcomputinggroup.org
- Tutorial/Introduction paper: (4 pages)
  Linux Journal, August 2003
- White papers, open source code
  http://www.research.ibm.com/gsal/tcpa
  device driver/access library/example applications

TRUSTED COMPUTING GROUP™

Programming view of the TPM



Open Source TPM projects

- IBM Research
  - Linux Device Driver/library/applications
    http://www.research.ibm.com/gsal/tcpa
  - Trusted Linux Client
- IBM Linux Technology Center
  - http://sourceforge.net/projects/tpmdd
  - http://sourceforge.net/projects/trousers
- Rick Wash (umich) BSD port of IBM driver/library/applications
  - http://www.citi.umich.edu/u/rwash/projects/trusted/netbsd.html
- Dartmouth enforcer
  - http://sourceforge.net/projects/enforcer
- Swiss Federal Institute of Technology – TPM emulator
  - http://www.infsec.ethz.ch/people/psevinc/

TRUSTED COMPUTING GROUP™

IBM Linux Technology Center

- Official Device Driver included in 2.6.12 kernel
  http://sourceforge.net/projects/tpmdd

- Open source TCG Software Stack (TSS)
  http://sourceforge.net/projects/trousers
  Full software stack, including
    synchronization
    resource control (loaded keys)
    example applications
    testing programs

TRUSTED COMPUTING GROUP™

IBM Research: Trusted Linux Client

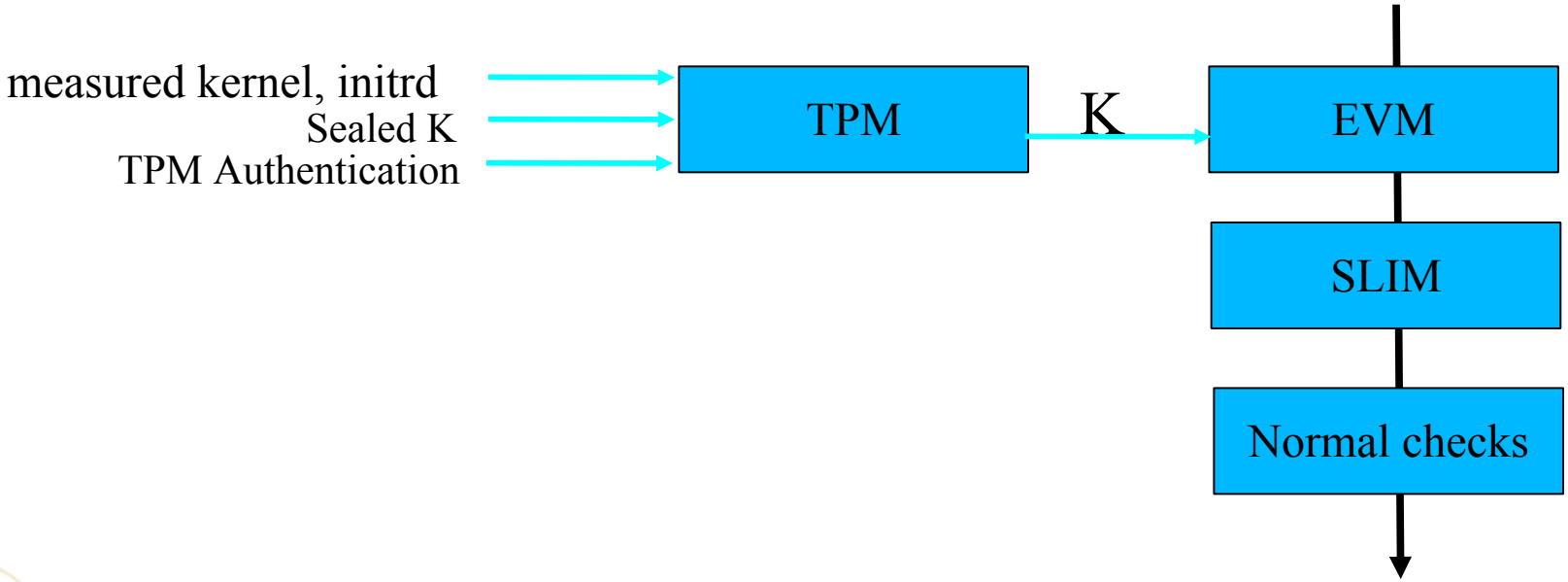
- Goals:
  - protect integrity of system from current attacks
  - be transparent to user
    - let user get job done
    - block only malicious activity
- Foundations:
  - TPM
  - LSM (Linux Security Modules)
- Functionality
  - TPM based “Trusted Boot”
  - Authenticated file metadata for storing hashes, labels
  - Enhanced Lomac style Mandatory Access Control

TRUSTED COMPUTING GROUP™

Trusted Linux Client Modules:

- TPM: driver measures integrity of kernel and initrd, and releases kernel key
- EVM: Extended Verification Module – authenticates extended attributes, data
- SLIM: Simple Linux Integrity Module – Mandatory Access Control Sandbox

- Implemented as stacked LSM module:



TLC Extended Attributes

EVM Extended Attributes:

```
  security.evm.hash  - hash of file data (from signed rpm)
  security.evm.hmac  - hmac-sha1 of security.* attributes
  security.evm.packager – signer of package
  security.evm.version  - version of package
```

SLIM Extended Attributes

```
  security.slim.level – six class values (values are space delimited)

     IAC    - File's Integrity Access Class
     SAC    - File's Secrecy Access Class

     IRAC   - guard process Integrity Read Access Class
     IWXAC  - guard process Integrity Write/Execute Class
     SWAC   - guard process Write Access Class
     SRXAC  - guard process Read/Execute Class
```

TRUSTED COMPUTING GROUP™

Open Source TPM projects – What's Missing?

- OpenSSL support
  - Example applications already use OpenSSL key formats
  - Need way to use TPM for client side SSL authentication
    - hooks for openSSL to call TPM library

TRUSTED COMPUTING GROUP™

Open Source Trusted Computing

- Future Work
  - Integration with virtualization (Xen)
  - Integration with Selinux
  - Integration with encrypted filesystems
- Summary
  - drivers, libraries, trusted boot available now
  - many more applications in work

TRUSTED COMPUTING GROUP™

Agenda

9:45 am

Writing and Using Trusted Applications
Alexander Koehler, *Utimaco Safeware AG*; Steven Sprague, *Wave Systems*

Alexander Koehler *completed his studies in mathematics and computer science at Karlsruhe University, Germany. After working as software development engineer on ground transportation simulation he joined Hewlett-Packard in 1981. Since 1997 his interests have been in IT security, which led him to Utimaco Safeware AG as head of business intelligence. He is the alliance manager for the Trusted Computing Group.*

TRUSTED COMPUTING GROUP™

Writing and Using Trusted Applications: Security Solutions in Operation

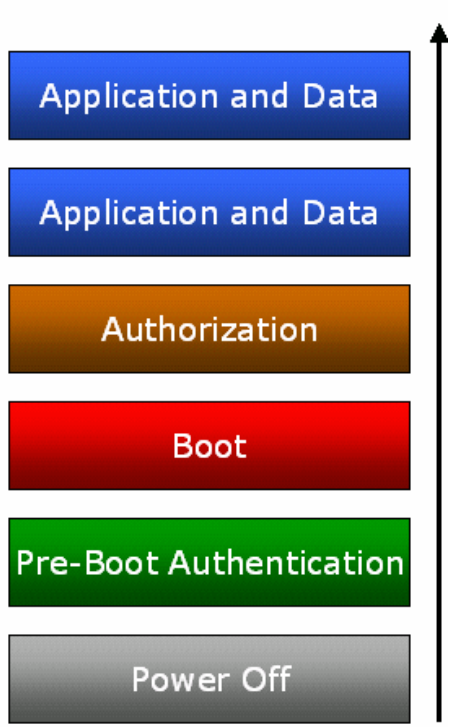
Alexander W. Koehler

Business Intelligence

Utimaco Safeware Inc.

Agenda

- Improvements of security at all three states of a mobile PC:
  - Power-Off
  - Boot
  - Operational

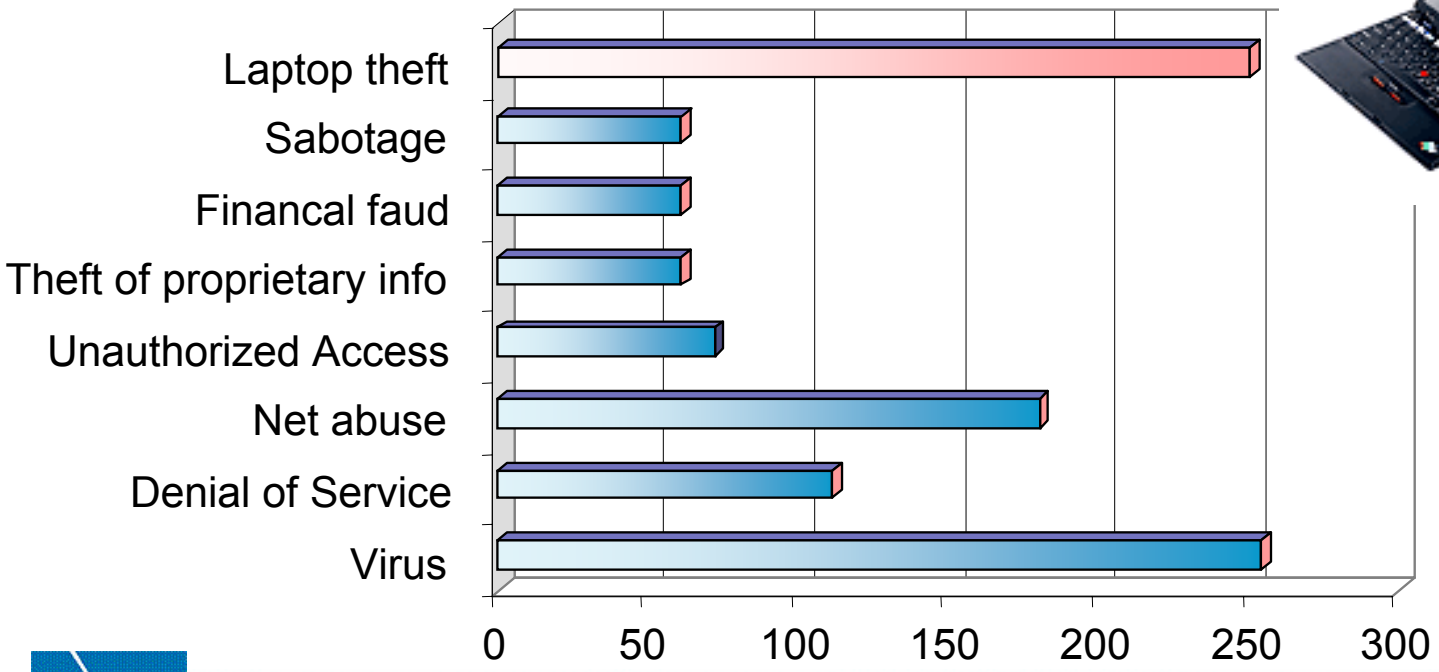


- From TCG to TCO (Total Cost of Ownership)
- Testimonials: It is not just theory, it works

TRUSTED COMPUTING GROUP™

Power Off

Risks in IT - Types of Attacks and Misuse

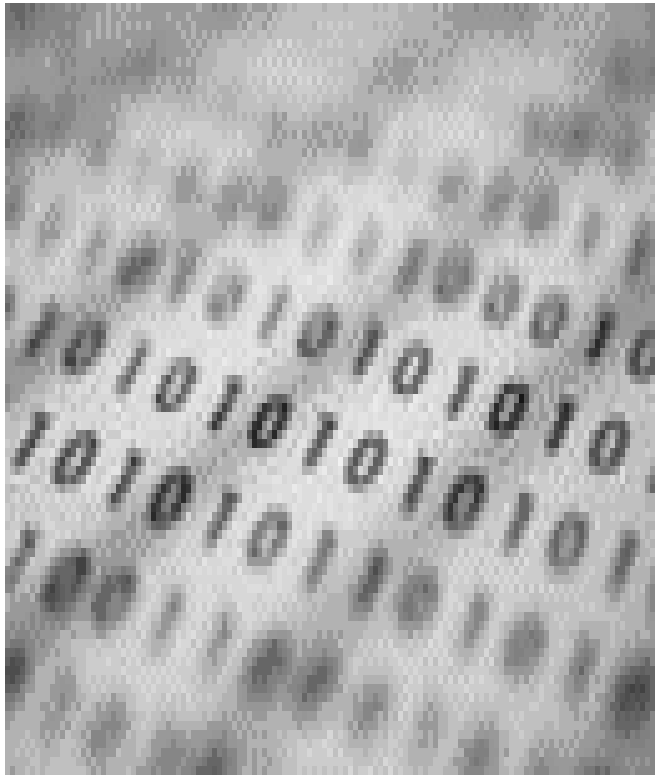


Source: CSI/FBI: Computer Crime and Security Survey 2003
http://www.gocsi.com/db_area/pdfs/fbi/FBI2003.pdf

Power Off

The Base Protection Issue on Notebooks

- In Windows® XP the SAM database stores passwords
- Microsoft® recommends to encrypt the SAM database with „syskey“ (*).
  - It requests either an additional password entry every time the notebook is booted or a floppy has to be carried around
  - It is not convenient for users



– **<u>All remaining data on the disk is still stored in plain.</u>**

– *: Source: Microsoft Windows Security Inside Out, Ed Scott, Carl Siechert, Microsoft Press

TRUSTED COMPUTING GROUP™

Power-Off Protection

- **Bulk Encryption with SafeGuard Easy®**
  - If an attacker steals the hard drive or the notebook, all data is protected.
    The SAM, system files, temporary files, page files, Microsoft Office® files, the hibernation file, a.s.o., everything is encrypted.
  - Encryption is compatible with most modern recovery mechanisms: IBM® 's Rescue & Recovery.

- The TPM increases protection
  - Keys are stored in protected hardware or are protected through hardware
  - Dictionary attacks become almost impossible
  - True RNG: Keys of highest crypto quality

TRUSTED COMPUTING GROUP™

Authentication

Pre-Boot Authentication

- Pre-Boot Authentication in combination with a TPM offers authentication in a compact and protected environment.
- Security
  - Vulnerabilites of a large system like an OS cannot be exploited
  - Credentials are protected through hardware
  - Mutual authentication „server-client“ through TPM generated keys
  - Central & remote administration secured by TPM generated keys
  - Secure identification of client device
- Convenience
  - Biometrics

- Image: UPEK® biometric fingerprint reader built-in IBM® ThinkPad®

TRUSTED COMPUTING GROUP™

- Authentication
– Boot
– Authorization

Authorization

Boot

Pre-Boot Authentication

- Security
  - Boot: Machine Binding

  - SSO: The TPM is the „Root of Trust“ for the SSO process
    - Credentials are protected through hardware
- Convenience
  - SSO
    - Highly complex passwords
    - Certificates (X.509)
      - Deployment
      - Revocation
      - PKI

TRUSTED COMPUTING GROUP™

Operational

- Protecting data through Virtual Disk
  - A Virtual Disk is a „vault“ for data
  - Virtual Disks can be mounted / dismounted as operating environments change (online, offline)
  - Neither content nor structure is visible
  - Protected through passwords or certificates
  - Virtual Disks on harddrives, floppies, USB sticks, flash memory cards, CD-ROM, DVD, Zip etc.
  - Drives on network locations: encryption / decryption locally
- The TPM provides
  - New true random key for each Virtual Disk
  - Passwords or certificates are protected through hardware
  - The link to management systems: IBM‘s ESS (Embedded Security Subsystem)

TRUSTED COMPUTING GROUP™

Operational

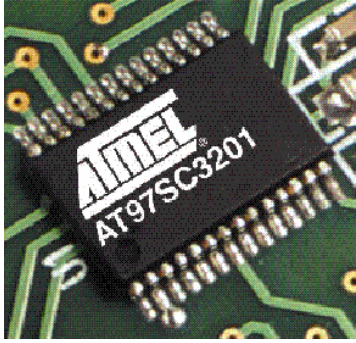
Application and Data

Authorization

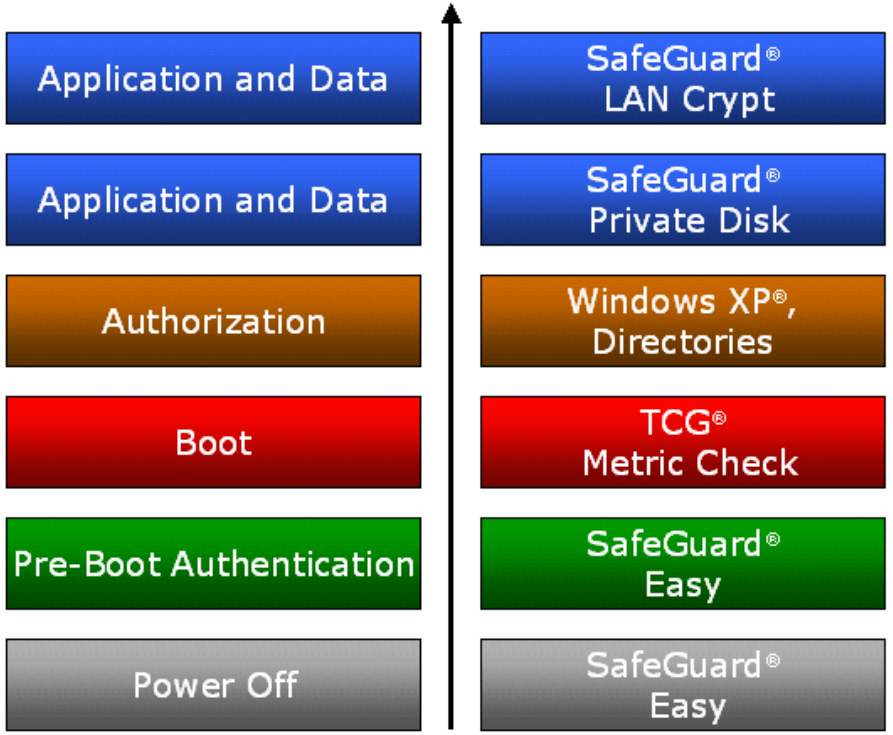
- Secure Media Exchange
  - Protection reaches beyond the PC platform
  - Virtual Disks can be exchanged between PC platforms and Converged Mobile Devices (phones, PDAs)
  - Content secured by secrets, which are protected through TPMs

TRUSTED COMPUTING GROUP™

The Trusted Platform Module Today



- The TPM provides a variety of solid improvements in security of system and application software
- Products are available already today for the benefit of the customer



TRUSTED COMPUTING GROUP™

From TCG to TCO

- TCO (Total Cost of Ownership)
  - **The TPM is a low-cost, built-in hardware unit**
  - No additional costs for purchase of e.g. tokens
  - No additional costs for lifecycle management
  - Gains in productivity
    - No extra deployment
    - No install
    - No downtime due to lefts
  - Gains in administration
    - It is standard
- What the analysts say

  „ … PC management has become more complicated over time, as IT managers are faced with an increasingly mobile workforce …
  ESS* can replace traditional hardware tokens and smart cards, providing users with a cost-effective solution that is not prone to loss or damage, “ said Technology Business Research.

TRUSTED COMPUTING GROUP™

*** ESS stands for Embedded Security Subsystem by IBM®, based on TPM.**

Bulk Encryption and TCG in Operation

- LBS Nord, Hannover, Germany
- Building society, 1 million customers
- The application:
  - Agents provide their consulting services inside the customers‘ premises
    - customers‘ workplace
    - customers‘ home
  - LBS proprietary consulting software and company data are stored on notebooks: corporate assets
  - Confidential customer data will be entered, processed and stored on notebooks: liability
  - Agents cannot take care about sophisticated security policies
- Costs have to be considered over the whole notebook lifecycle

Bulk Encryption and TCG in Operation

- **The solution:**
- IBM® T40 Thinkpads®, equipped with TPMs (Trusted Platform Module)
- IBM® ThinkVantage® Technology: Embedded Security Subsystem: Streamlined client management in conjunction with improved security
- Utimaco SafeGuard® Easy: Bulk Encryption of all HDD content: High level of protection combined with a user friendly security policy
- The synergy: Proactive increase of client security by key storage in hardware plus machine binding
- Low cost disposal of notebooks at end of lifecycle

TRUSTED COMPUTING GROUP™

Bulk Encryption and TCG in Operation

- SWIFT is the financial industry-owned mutual organization, supplying secure, standardized messaging services and interface software to 7,600 financial institutions in 200 countries.
  HQ: La Hulpe, Belgium

- Business Need: To cope with the consequences of theft of notebooks and prevent corruption of notebook data
- Statistics: It is expected that from 5000 laptops 500 units will get lost during lifecycle

TRUSTED COMPUTING GROUP™

Bulk Encryption and TCG in Operation

- **The Solution:**
  - IBM Thinkvantage ESS
  - Platform binding
    - data to the platform
    - platform to the network
  - High quality key generation by TPM
  - All data protection by all harddisk encryption
  - Notebook or HDD disposal at very low cost
  - TPM built-in at no extra cost
  - Hardware: 600 TPM equipped IBM Thinkpads (first roll-out)

TRUSTED COMPUTING GROUP™

Summary

- TCG technology leverages existing security technology for the benefit of the customer
  - Increased level of security
  - Decreased costs
  - Improved manageability
  - Standardization

- Utimaco is committed to continue integration of TCG technology to provide also in the future leading edge security technology for industry customers and government agencies

TRUSTED COMPUTING GROUP™

Alexander W. Koehler
Utimaco Safeware Inc.

10 Lincoln Road, Suite 102
Foxboro, MA 02035
Phone:(508) 543-1008
Fax:(508) 543-1009
Email: sales.us@utimaco.com
www.utimaco.us

Agenda

9:45 am

Writing and Using Trusted Applications
Alexander Koehler, *Utimaco Safeware AG*; Steven Sprague, *Wave Systems*

Steven Sprague *is president and CEO of Wave Systems Corp. Wave is a leader in delivering trusted computing applications and services with advanced products, infrastructure and solutions across multiple trusted platforms from a variety of vendors. In 1995 he founded Wave Interactive Network, a specialized consumer distribution channel. In 1996 Wave acquired Wave Interactive Network and Sprague was elected president and COO of Wave Systems. In 2000 he took over responsibilities as CEO.*

TRUSTED COMPUTING GROUP™

Writing and Using Trusted Applications: Security Solutions Using TCG Technology

Steven Sprague
Wave Systems Corp.
May 26, 2005

Solution Opportunities

Current Problems

Need Trusted Solutions

1. Stronger Network Authentication
2. Data Protection
3. Strong Authentication to VPNs
4. Password Protection
5. Secure Information Distribution
6. Secure E-mail

RESULT

Security and trusted computing represent major new services and integration opportunities

TRUSTED COMPUTING GROUP™

Getting started

1. Make sure all procured PCs contain TPM's
   - Dell, Fujitsu, HP, IBM/Lenovo, Intel, Toshiba…..
2. Solutions
   - Client applications
     - Data protection
     - Password Protection
   - Network applications
     - Asset management
     - Network access control
     - Digital Signing

TRUSTED COMPUTING GROUP™

What do I need

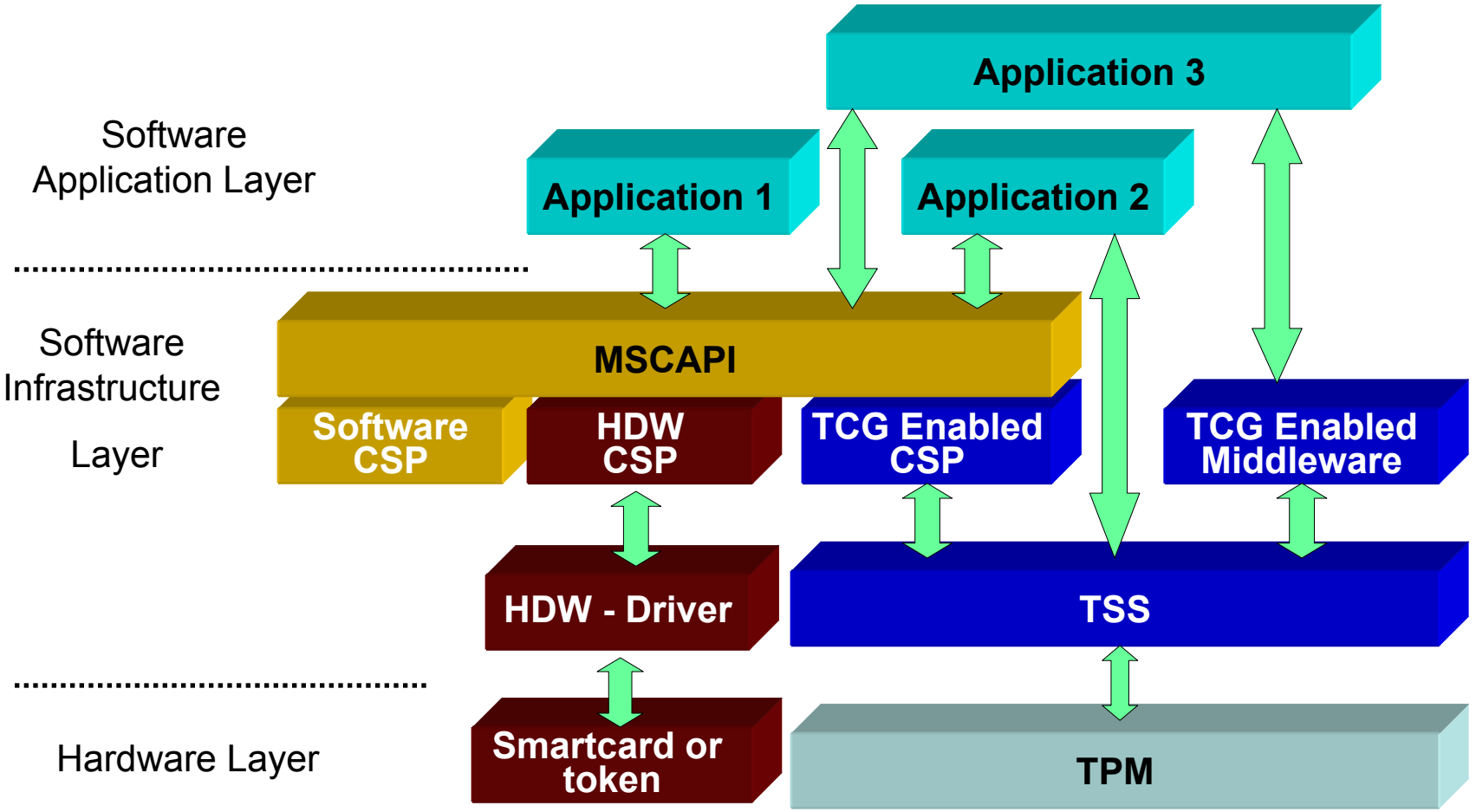
- Trusted computer with TPM and client Software
  - TPM 1.1b or TPM 1.2
  - Client software with CSP
  - Management utilities
  - Key Transfer Management tools Client

TRUSTED COMPUTING GROUP™

How's it Work

The 2 minute guide

TPM Security Programming Model



Client Applications

Data protection
Password Protection
Windows Logon
Data Signing

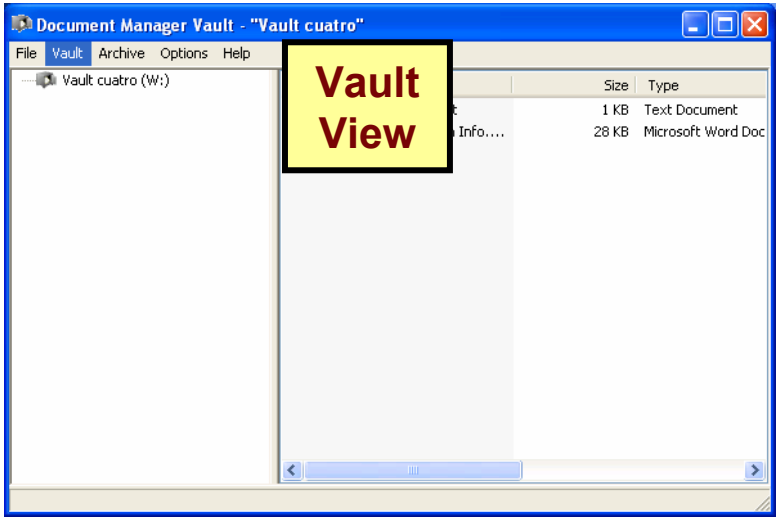
Data protection

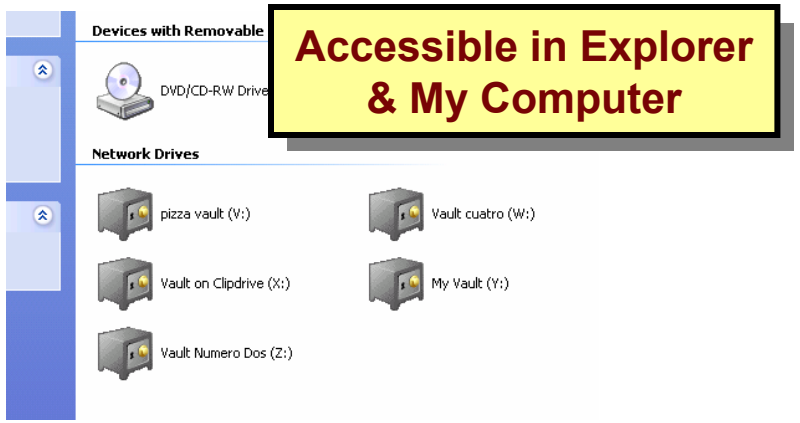
- Several Methodologies – not a 1 size fits all solution…
  - File and Folder Encryption
  - Work Group file and Folder encryption
    - Key Sharing
  - Drive Locking
  - Whole Disk encryption
  - Data signing

TRUSTED COMPUTING GROUP™

Wave's Document Manager

- Document and data encryption
- TPM Hardware protected keys
- Workgroup capability
- Integrated support for backup
- Data protected against unauthorized access, theft of PC.

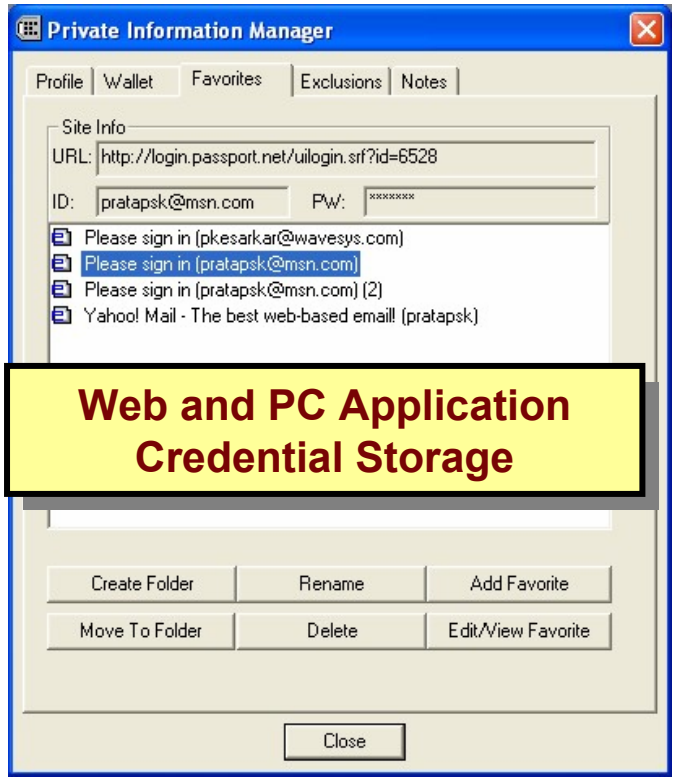




TRUSTED COMPUTING GROUP™

Password Management & Security

- Wave's Private Information Manager
  - TPM Secured storage of Web and Application usernames/passwords
    - Intelligent retrieval – automated
    - Auto capture of new login data
  - Multiple Profiles, Wallet, Favorite, Exclusions and Notes



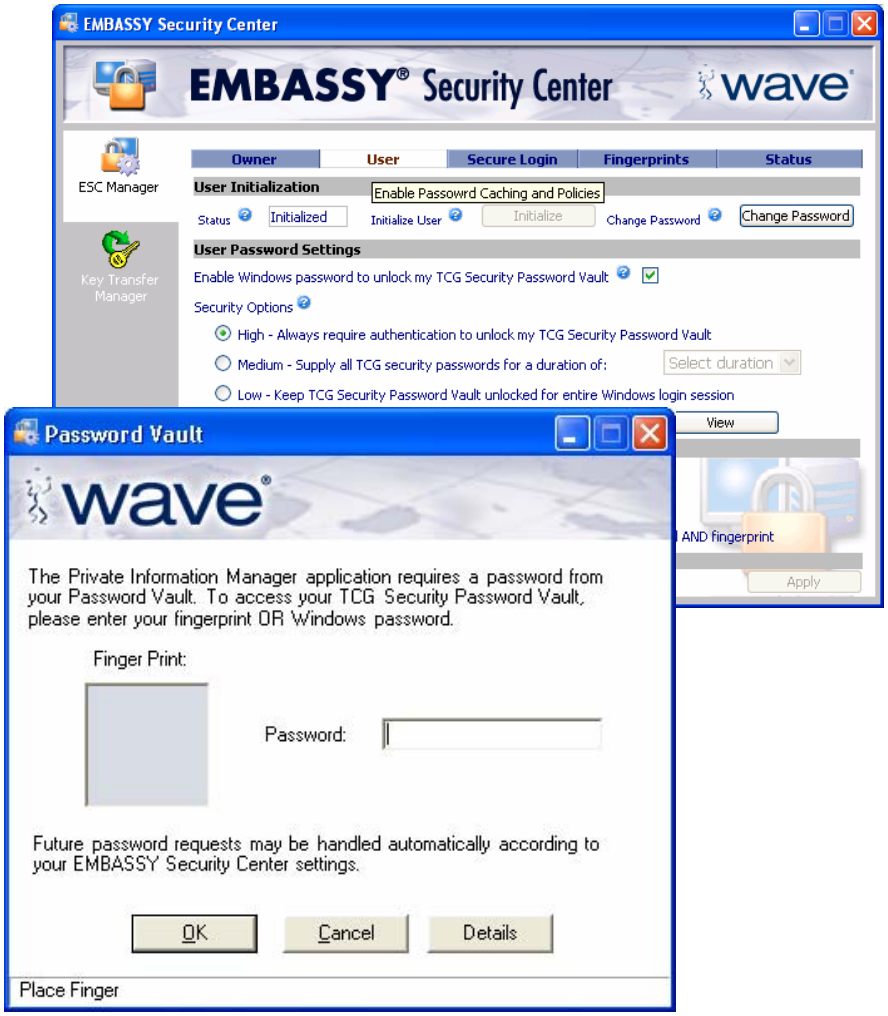
Web and PC Application Credential Storage

Prompted or Auto Login

TRUSTED COMPUTING GROUP™

TPM Management & Authentication

- Wave's EMBASSY Security Center
  - TPM Management
  - Multifactor Authentication with Biometric, Smart Card, TPM/PKI
    - Secure Windows Logon
    - TPM Key Authentication
  - TPM Key Password Management



TRUSTED COMPUTING GROUP™

Data Signing

- Random document authentication
- PDF signing tools
- Paperless contracts

TRUSTED COMPUTING GROUP™

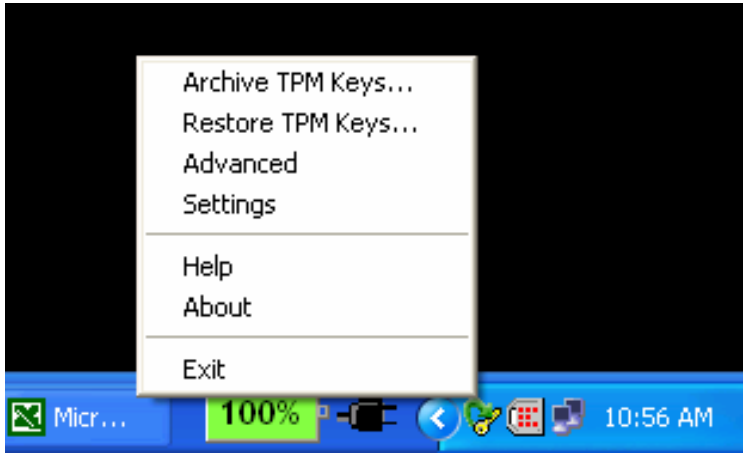
Server Tools

- Backup and recovery
- Access Control
- Web Authentication

TRUSTED COMPUTING GROUP™

TPM Key Archive/Restore

- Wave's Key Transfer Manager
  - Automatic or scheduled archive of client keys & certificates
  - Restore to same or different TPM PC
  - One button restore for platform failure
  - Active Directory Integration
  - Client and Server modes



Network Authentication

- Hardware Based Network Authentication
  - Integration with Microsoft VPN
  - Integration with VPN concentrators
  - Support any MS CSP compatible Networking equipment.
  - Both Simple PKI and full PKI support.
- Trusted Network Connect (TNC)

TRUSTED COMPUTING GROUP™

Web Authentication

- Business to Business capabilities
  - Supports active directory
  - Can be overlaid on existing user ID and Password systems
    - Many examples being explored by business's today for token authentication
  - Can eliminate passwords or increase security of access
  - All Web projects should support TPM compliant authentication as part of the task order
  - Can supplement Token or Smart Card Authentication to provide better security.

TRUSTED COMPUTING GROUP™

Government Need

Agencies like DHS can benefit today from this technology. Solutions such as strong authentication can ensure that the PCs on the DHS network actually belong to DHS. We can use hardware security to report client platform status and configuration to the network during initial authentication with the network. Additional capabilities such as key back up and restoration help ensure the manageability of agency networks

Joseph Broghamer, director, Authentication Technologies Department

The Office of the Chief Information Officer, Department of Homeland Security

TRUSTED COMPUTING GROUP™

Conclusion

- Trusted computing is available today.
  - Make sure all task orders ask for it.
- Trusted Computing Client only applications can make each computer more secure and automate compliance
- The server infrastructure can use Trusted Computing Platforms today and all future systems should request compliance.
- The technology is robust and secure and ready to join the battle and reduce the cyber threat.
- It just does as advertised…

TRUSTED COMPUTING GROUP™

Thank you

Questions

Contact Wave:

Steven Sprague, CEO 413-243-7011
Marty Wargon, VP Gov't Sales 561-752-4464

Providing the Software and experience to deploy trusted computing today

TRUSTED COMPUTING GROUP™

Agenda

10:30 am

Trusted Storage and Applications
Michael Willett, *Seagate Technology, Inc.*

Dr. Michael Willett *received his bachelor's degree from the US Air Force Academy and his Masters and Ph.D. degrees in mathematics from NC State University. After a career as a university professor of mathematics and computer science, Michael joined IBM as a design architect, later moving into IBM's Cryptography Competency Center. Currently, Michael is on the research staff of Seagate Technology, exploring future projects in security and privacy as well as serving on several external standards bodies, including the Trusted Computing Group (TCG).*

TRUSTED COMPUTING GROUP™

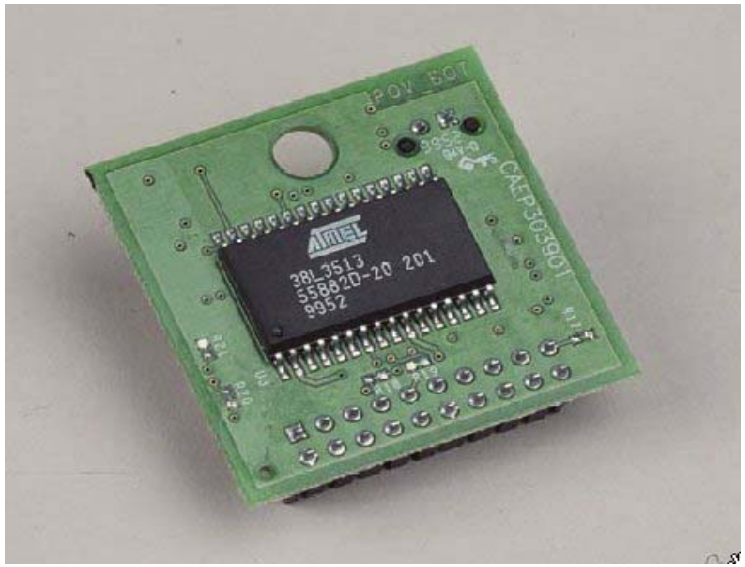
Trusted Storage and Applications: ™ Trusted Drive

Michael Willett, Seagate and TCG

TCG Trusted Platform Module

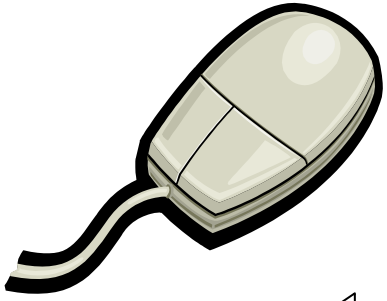
TPM v1.2 functions include:

- Store platform status information
- Generates and stores a private key (+ derivative keys)
- Hashes files using SHA-1
- Creates digital signatures
- Anchors chain of trust for keys, digital certificates and other credentials



TRUSTED COMPUTING GROUP™

Extending Trust to Platform Peripherals

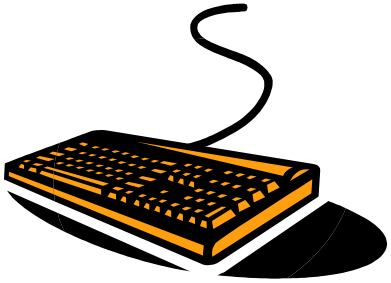


Ability to interact with the Platform

Authentication/Attestation

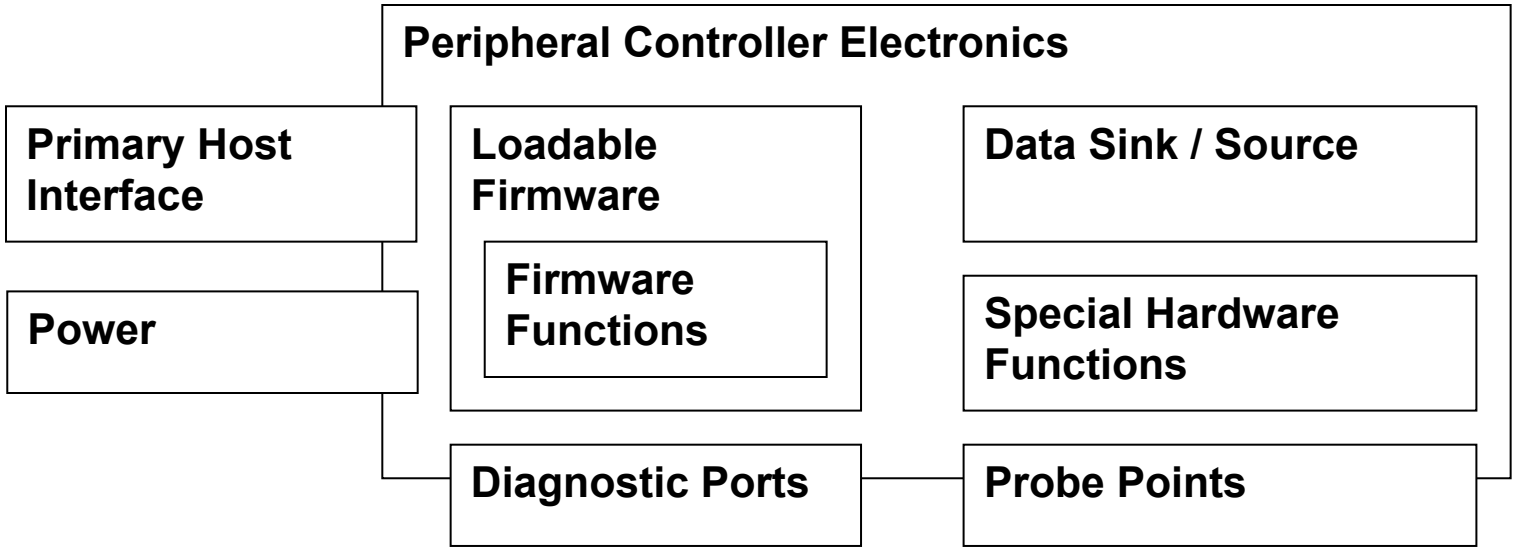
LOW **HIGH**

Capability Level



TRUSTED COMPUTING GROUP™

General Risk Model of a Peripheral



Trust = systems operate as intended

Objective: Exercise control over operations that might violate trust

Needed: Trusted peripheral commands

TRUSTED COMPUTING GROUP™

Joint Work with ISO T10 (SCSI) and T13 (ATA)

TRUSTED SEND

(Protocol ID = xxxx …..)

TRUSTED RECEIVE

T10/T13 defining the "**container commands**"

TCG/Storage/Peripherals defining the "**TCG payload**"

Protocol IDs assigned to TCG, T10/T13, or reserved

TRUSTED COMPUTING GROUP™

Protocol ID = 0 and Credential

TRUSTED SEND

(Protocol ID = 0 …..)

TRUSTED RECEIVE

(Device Credential, ….)

Status: Container Commands (IN/OUT) and Device Credential Submitted to T10/SCSI (under review)

TRUSTED COMPUTING GROUP™

DEVICE CREDENTIAL

Field name	*Description*
Credential Serial Number	The unique serial number of the credential
Credential Validity Period	The time for which the credential is valid as determined by the issuer of the credential
Credential Issuer	The issuer of the credential
Credentialed Entity	Identifies the device to which the credential applies
Device public key	Holds the public key information for devices capable of asymmetric key operations
Revocation Information	Location of revocation information relevant to the credential.
Supported Protocols	Indicates which security protocols are supported by the device
Signature Algorithm	Algorithm identifier for the signing algorithm used to sign the credential
Signature Value	Contains a digital signature computed over all other fields of the credential.

Scope: Payload Commands w/ Protocol ID = “TCG”

- Establishing/managing communications:

  Secure Messaging, RPC

- Parameter management: table entries with Access Control

- Security management: Secure Partitions, Authority, ACLs

- Cryptography:

  random numbers, key generation, encrypt/decrypt, hash

- Admin: clock, backup

- Log: add, flush, clear

TRUSTED COMPUTING GROUP™

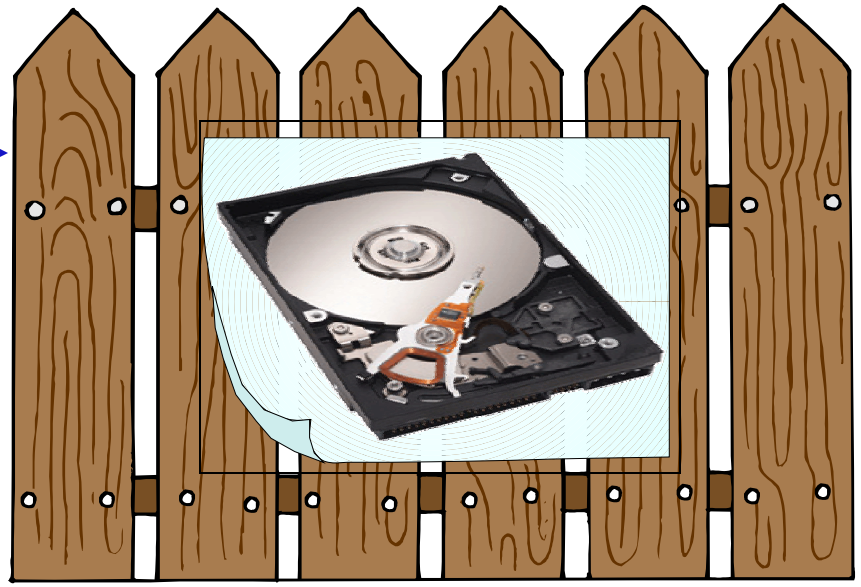
Trusted Send/Receive w/Access Control

TRUSTED SEND

(Protocol ID = TCG …..)

TRUSTED RECEIVE

Versatile Access Control per Command



-Authentication and Access Control

-Protecting Hidden Storage and Trusted Drive security features

-Join TCG and see!!

Password

Biometrics

RSA Authentication

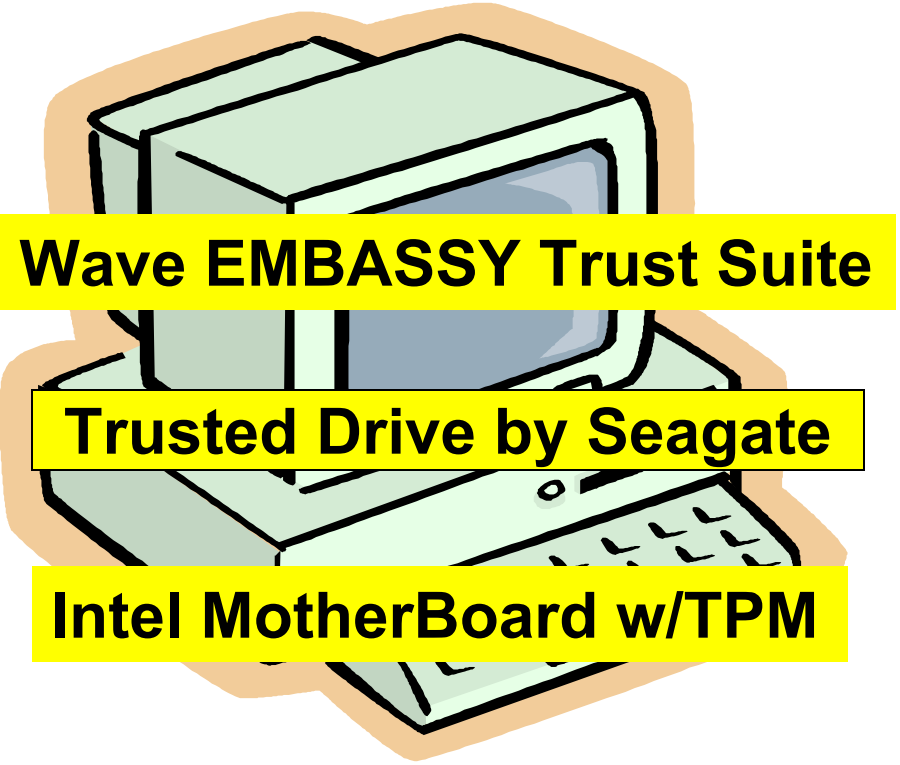
MAC Challenge/Response

TRUSTED COMPUTING GROUP™

Trusted Drive and TPM: TCG Use Case

Wave Systems Booth

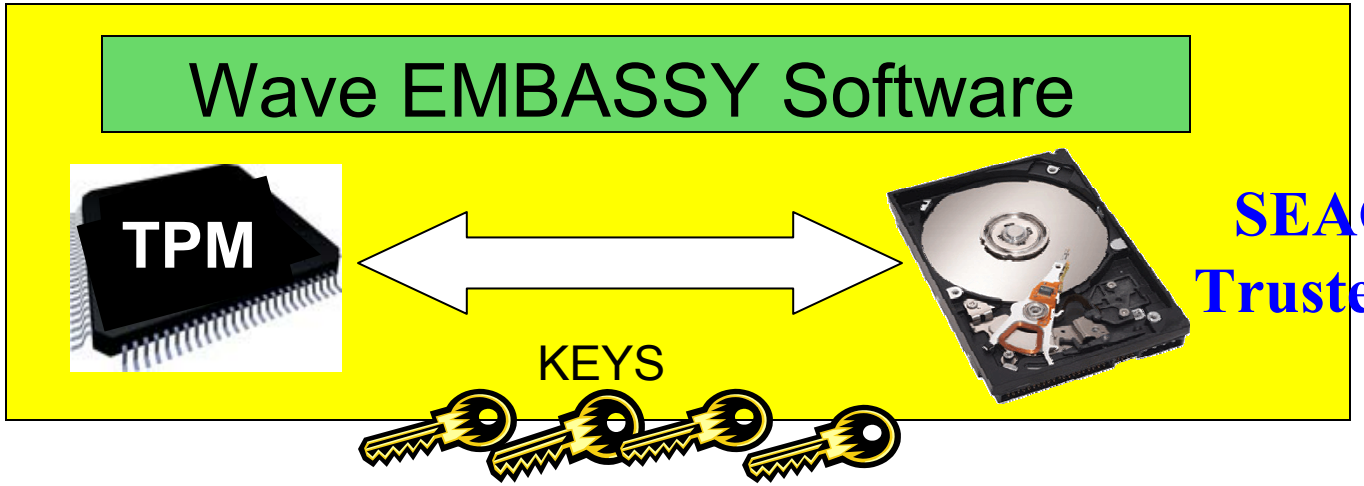
Trusted Platform Configuration



- **Enroll Drive with Platform Host**
- **Drive will not Read/Write unless attached to the Platform Host**

- **Prevents re-purposing (theft) of drives or attachment of drives on hosts not intended**
  - –Corporate/Government where “USB attached storage gets legs”
  - –Consumer electronics
  - –Desktop or laptop storage (theft)

Demonstration: Technical Details



Created During Enrollment

Both TPM and Trusted Drive Provide Strong Key Protection

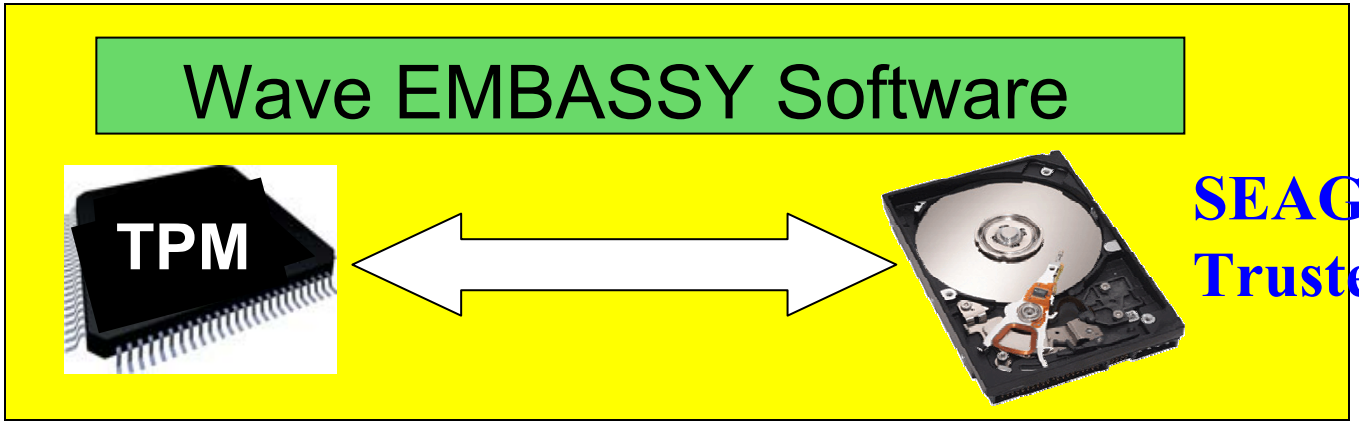
- Uses MAC Authentication and Secure Messaging
- 3DES symmetric keys
  - –secure messaging between drive and host (3DES encrypt the command payloads)
  - –drive to challenge the host (3DES encrypt a nonce)
  - –host to challenge the drive (3DES encrypt a nonce)
  - –key to provide admin control over other keys
- Wave's Key Transfer Manager
  - –Key escrow and key distribution service; more than one platform can be mated

TRUSTED COMPUTING GROUP

Contrast: Password-Only Drive Locking

Corporate user knows the password (user has to type it in!) so **user** can re-purpose the drive

compared to



User plugs the drive into the USB port:

–First time only, give the TPM password (not the drive password)

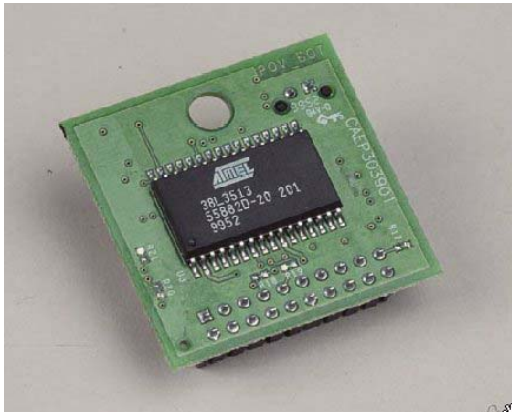
–After that, normal activity while the drive is mated to the platform

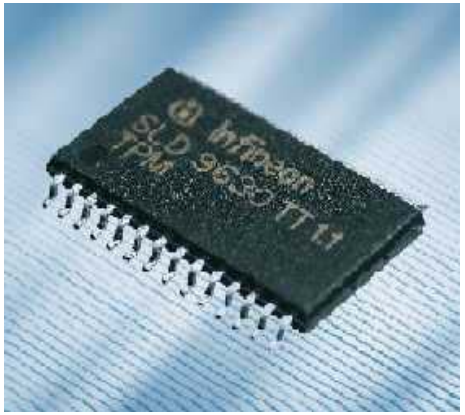
– TPM hides keys, even from user, but does not prevent migrating keys to other TPMs with proper password authorization

TRUSTED COMPUTING GROUP™

www.trustedcomputinggroup.org

THANK YOU!





QUESTIONS?

TRUSTED COMPUTING GROUP™

Agenda

10:50 am

Trusted Network Connect Overview
Jon Brody, *Sygate Technologies*

***Jon Brody**, Vice President of Marketing Communications, brings to Sygate nearly twenty years of expertise in building and marketing software solutions to global enterprises for secure collaboration and business integration. Brody's prior positions included Vice President of Marketing at PeerLogic as well as President of Veri-Q, Inc. Before heading Veri-Q, Brody lead development of the North American marketing, services and support operations of Verimation AB, vendor of the leading office automation and collaboration solution to multinational enterprises. Brody holds a BA in Biology from Case Western Reserve University.*

TRUSTED COMPUTING GROUP™

Trusted Network Connect Overview: Why, What, When

Jon Brody

VP Marketing, Sygate Technologies

TCG/TNC Member

Open networks: boon and bane

- Security approaches have always failed
  - but open networks have amplified the consequences of failure.
- Open networks are **better**
  - Open networks enabling new business models.
    - NYT 2/24/05 – even biotech jobs are moving overseas.
    - The Washington Times, 3/21/05 **"Teleworking significantly improves the survivability of the public…"**
  - **More at stake.**
- Open networks are **faster**
  - Enable real time revenue
  - Instant business pain from interruption
  - **Growing gap between incidents and response.**
- Open networks are **cheaper**
  - LAN port costs declined dramatically, Remote access costs trivial
  - Users can reconfigure networks (bridge your network to a hostile one for less than $100).
  - **Rapid adoption of new open network technology.**

TRUSTED COMPUTING GROUP™

One business problem at a time.

	Problem 1 Put your business on the web	Problem 2 Put your employees on the web	Problem 3 Permit any device on the web on your network
Advantage	Get global market access	Enable telework on corporate laptops	Enable outsourcing, consultants
Security Technology	Set up a perimeter Isolate your business systems with firewalls Intruders beget IDS	VPN Goodbye perimeter, hello endpoints Add host protection – IDS, IPS, Antivirus	Clientless web access Services available over wireless protocols
Security process	periodic compliance Assessment and vulnerability scans.	Create 10,000 CISOs Chase untrustworthy devices Centralized Policy Management Location Awareness	Secure any system that may need to access your services at any time from anywhere on the globe

Besides swapping out closed networks nearly overnight for TCP/IP equipment, we've been playing catch up to business issues one at a time.

TRUSTED COMPUTING GROUP™

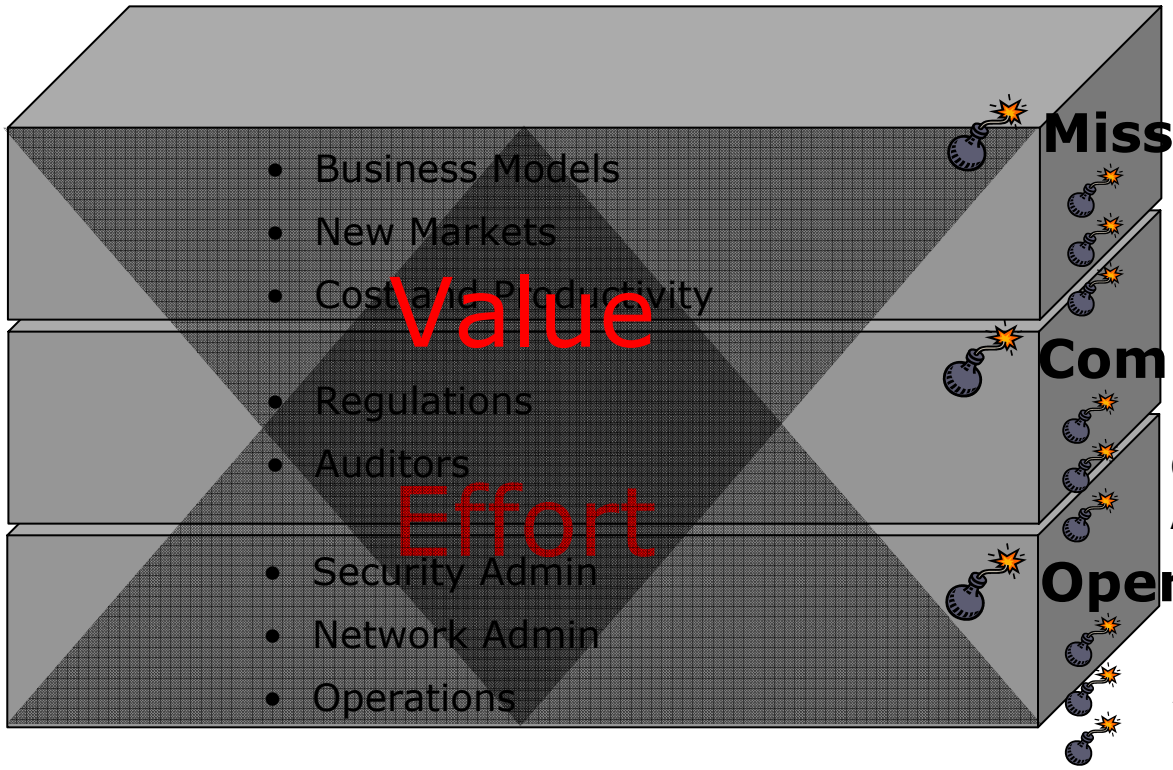
Root Cause - Open Networks Promiscuous and Permissive

1. Any device
   - Corporate, Employee, Guest, Consultant, Outsourcer
2. Anywhere
   - Home, Hotel, Kiosks
   - DSL, Wireless, Dial-up
3. Anything goes
   - Any application – p2p
   - Any configuration – missing patches
   - Any protection – turned off, old, out of date

Big responsibility – limited visibility, control & resources

TRUSTED COMPUTING GROUP™

Effort and Value misaligned



Mission disruption
Outsourcing
Internet Point of Presence
Telework, B2E Automation

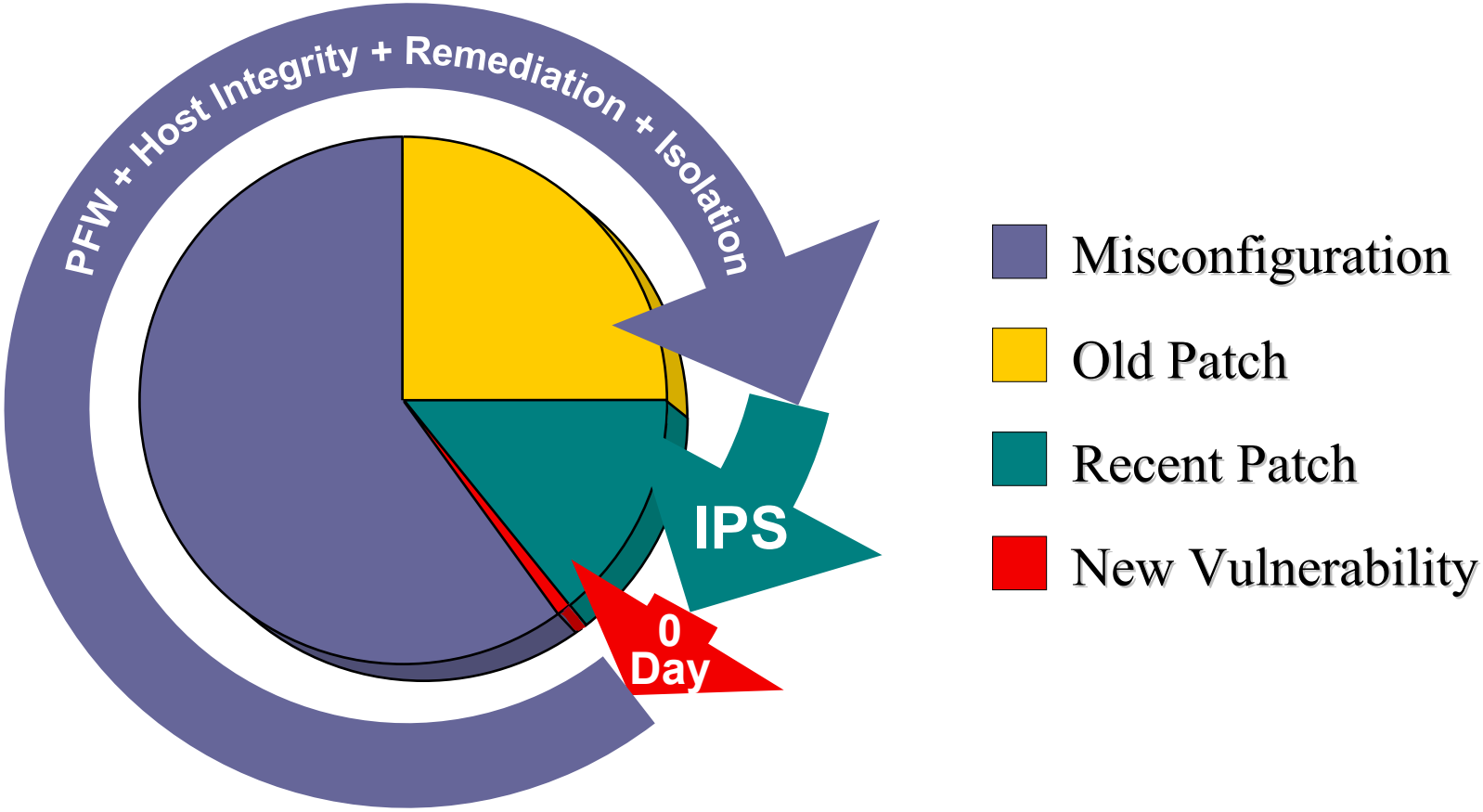
Compliance violation
Regulatory fines
Civil penalties
Audit findings

Operations impact
Incident Response
Availability
Helpdesk Overload

An OMB report on U.S. federal government security indicated there was little correlation between spending levels and actual security.

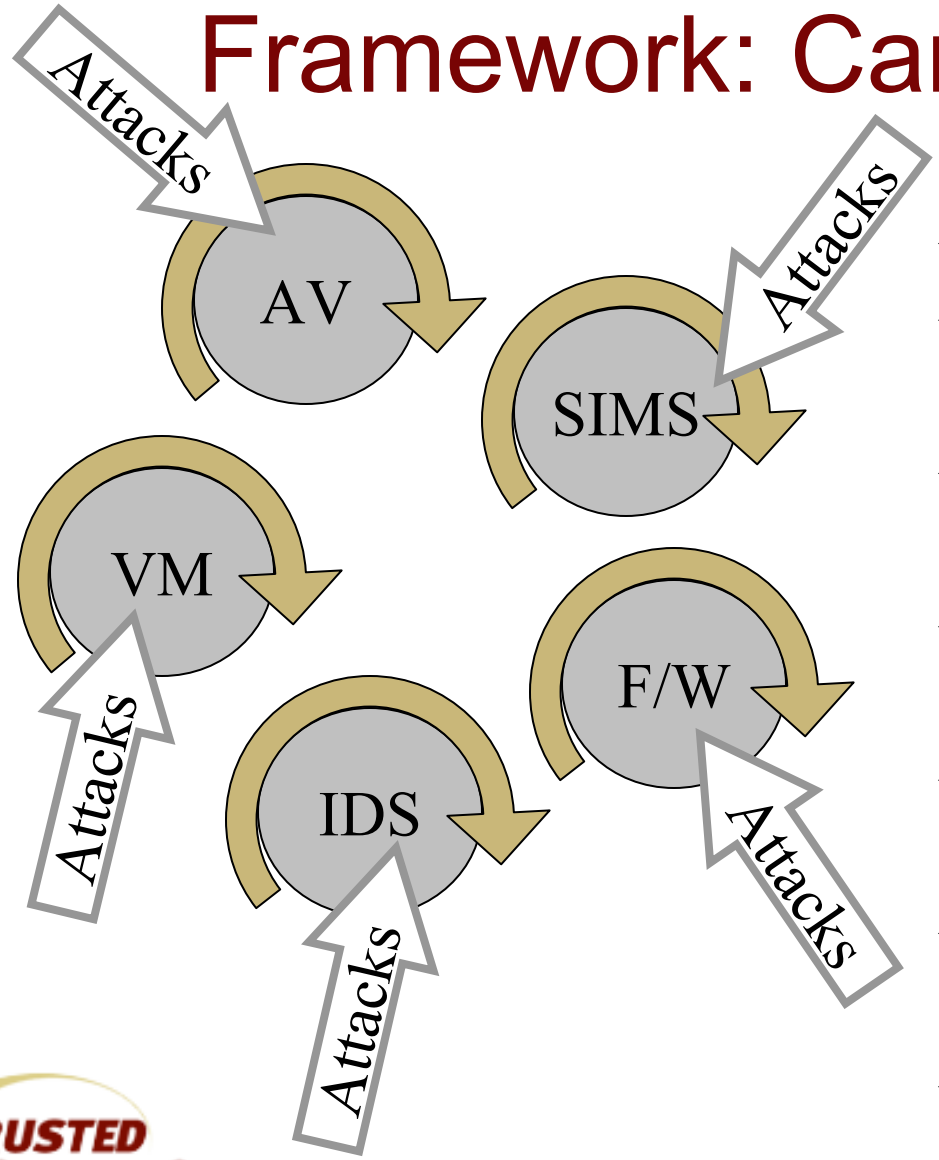
Pragmatic view

Misconfiguration, Misuse, and Malicious Access



Source: Gartner

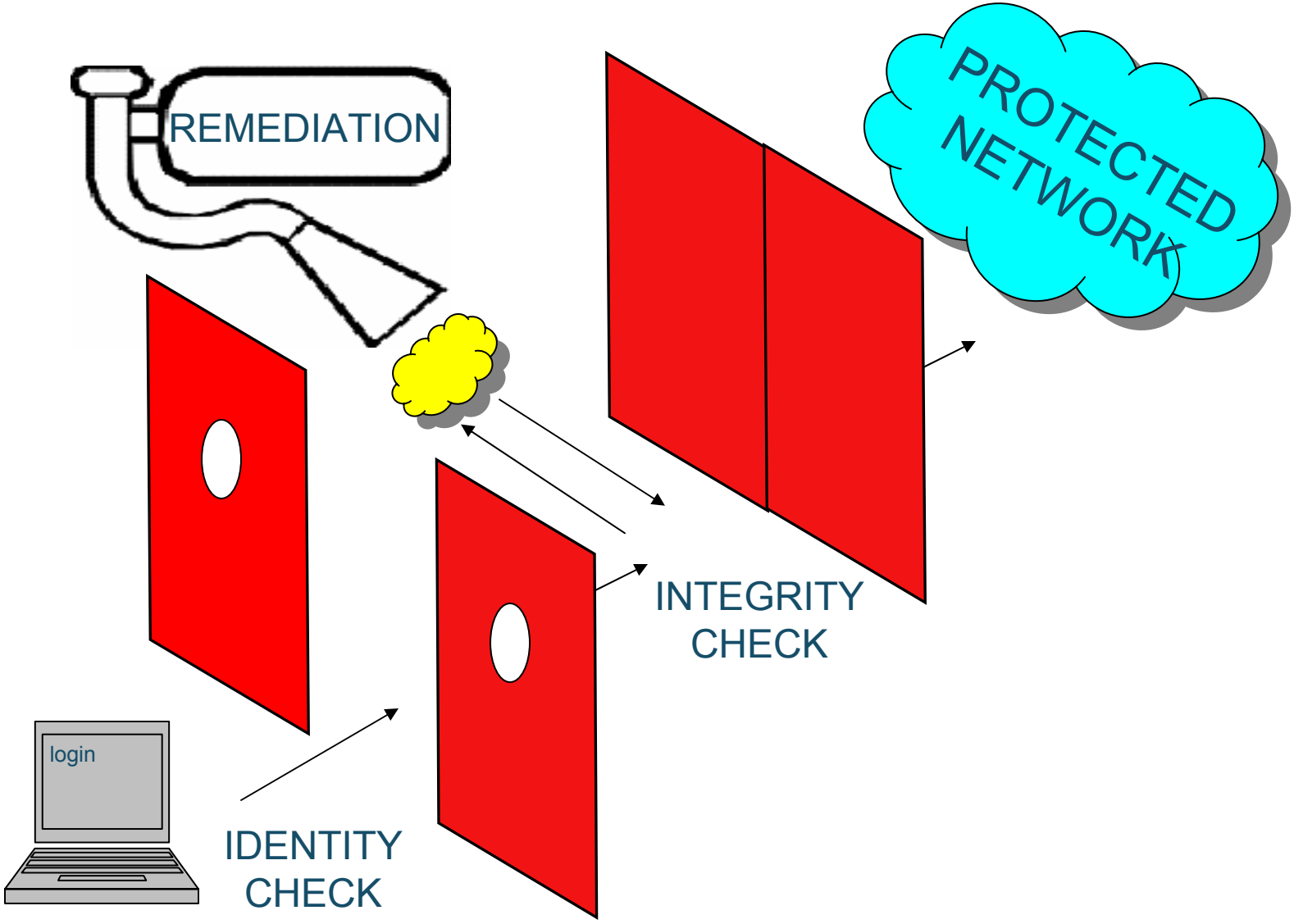
Without An Infrastructure & Framework: Can We Keep Up?



- ✓ Each an Individual Process
- ✓ Keep Turning on Same Cranks
- ✓ Continues to Produce Same Results
- ✓ Each One Has Unique Metric
- ✓ Neither Efficient or Effective
- ✓ No Integrated Solution Context
- ✓ Must Evolve or Die

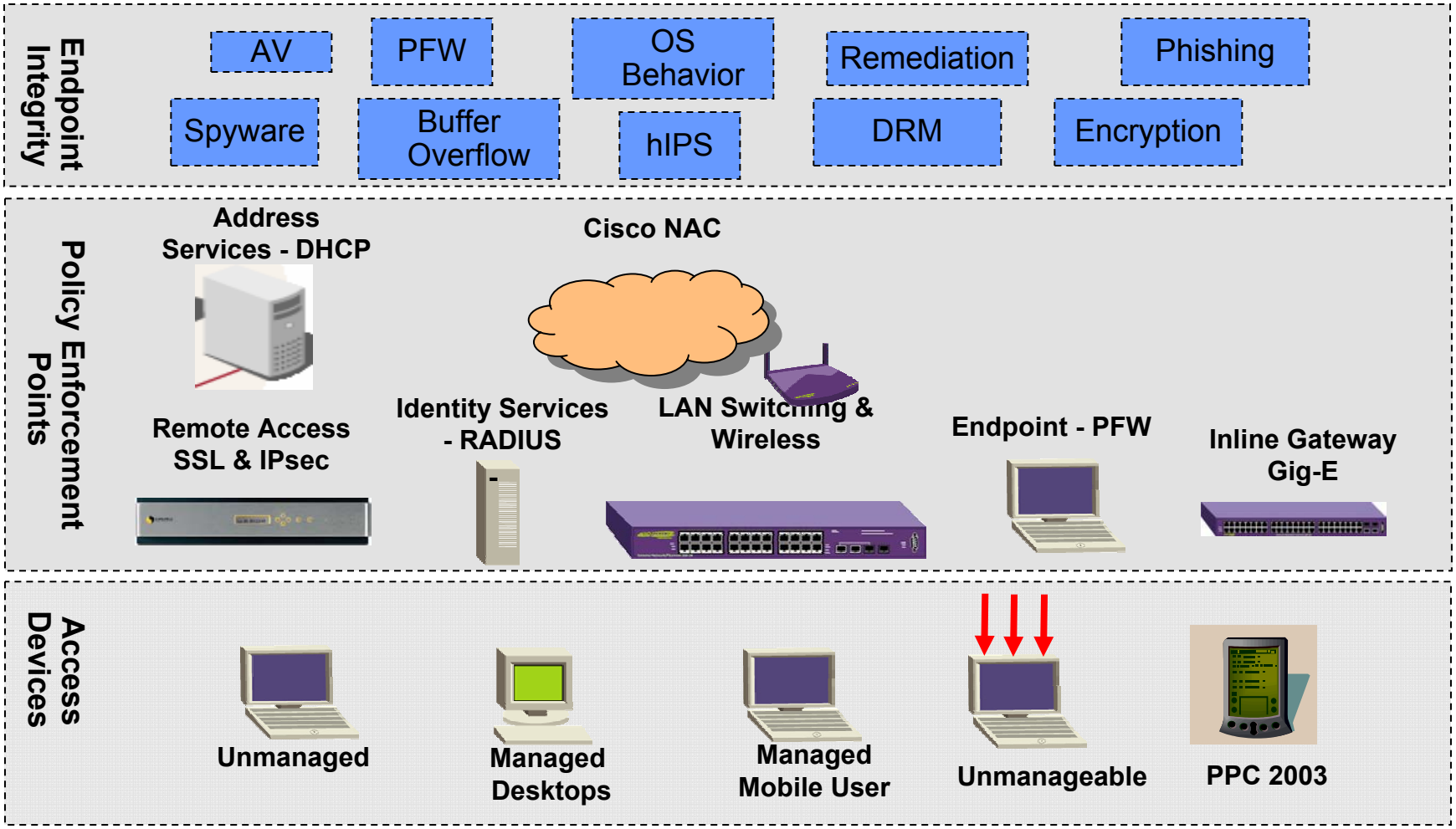
TRUSTED COMPUTING GROUP™

TNC Solution Creates a "Virtual Airlock" for Network Access & Protection

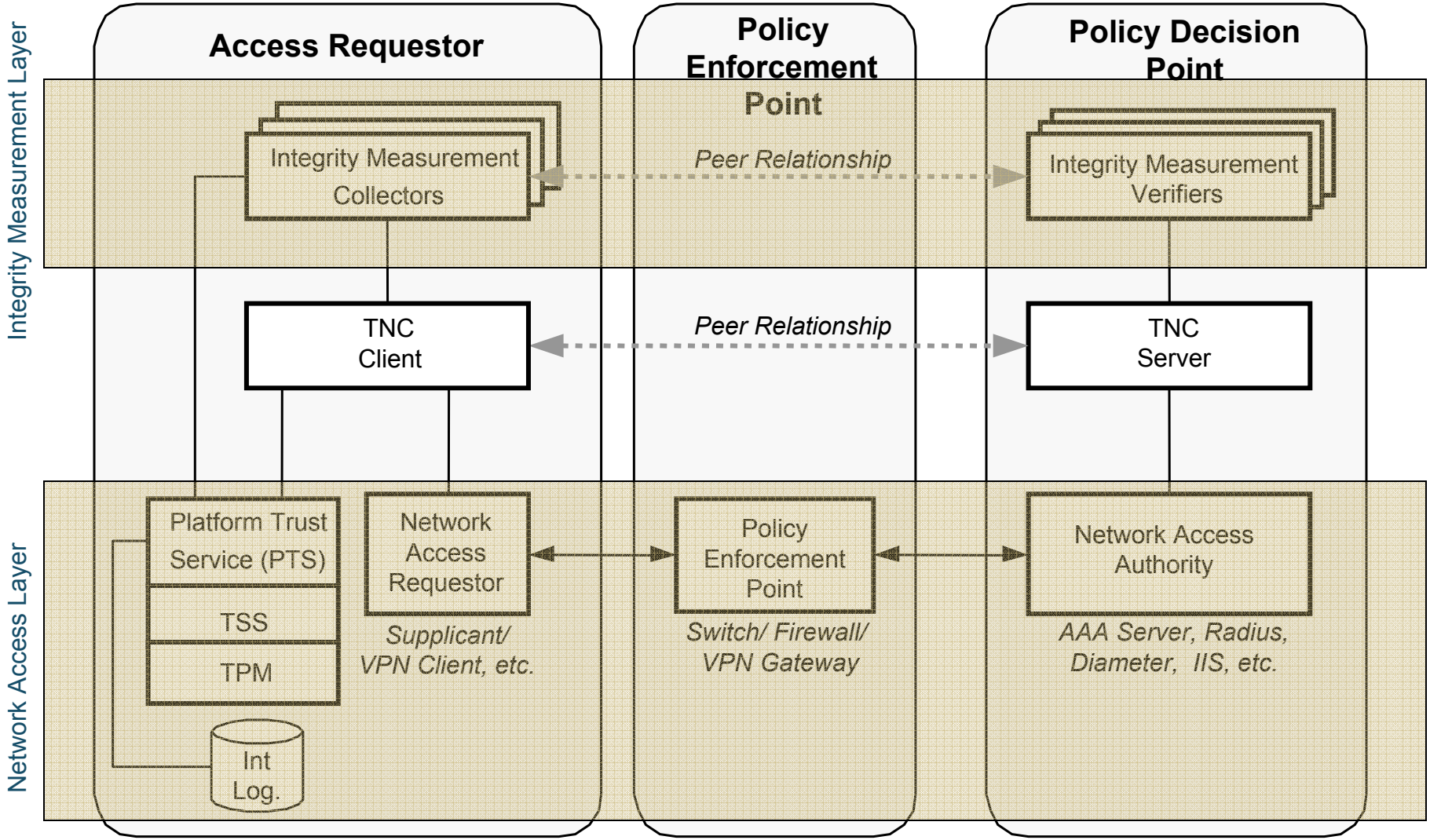


TRUSTED COMPUTING GROUP™

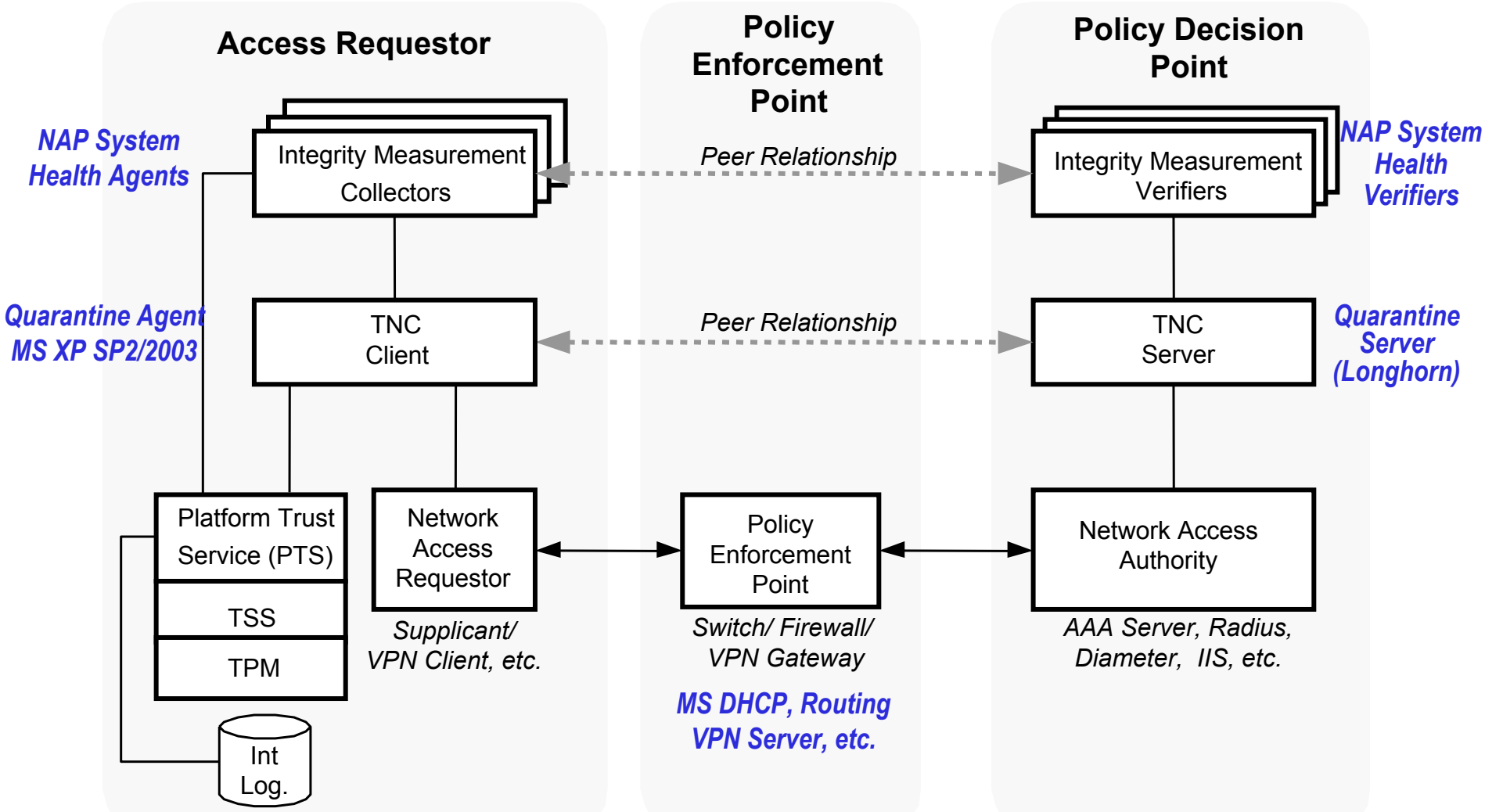
New Framework to Marshal Assets



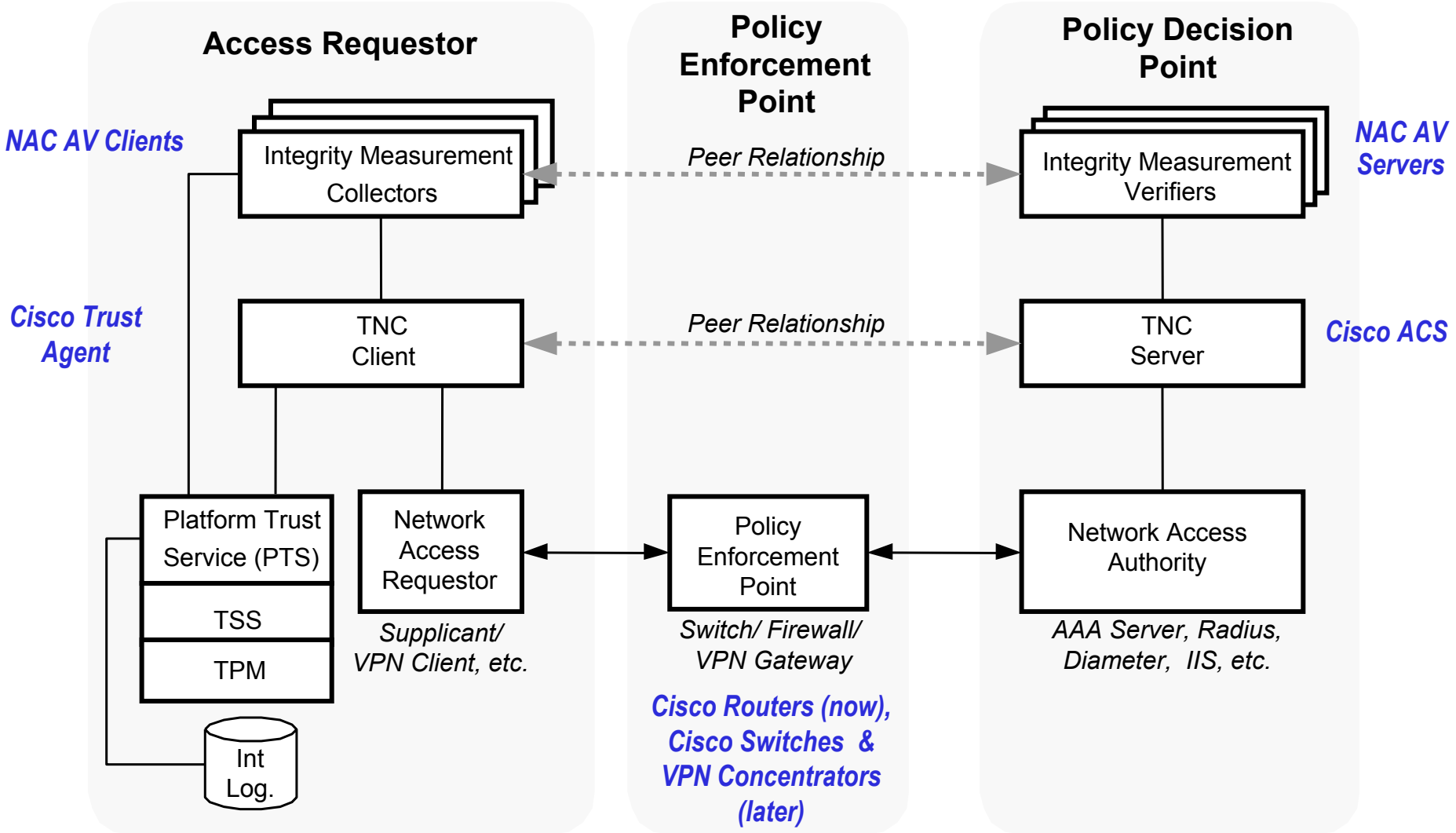
TNC Architecture



NAP alignment



NAC Alignment

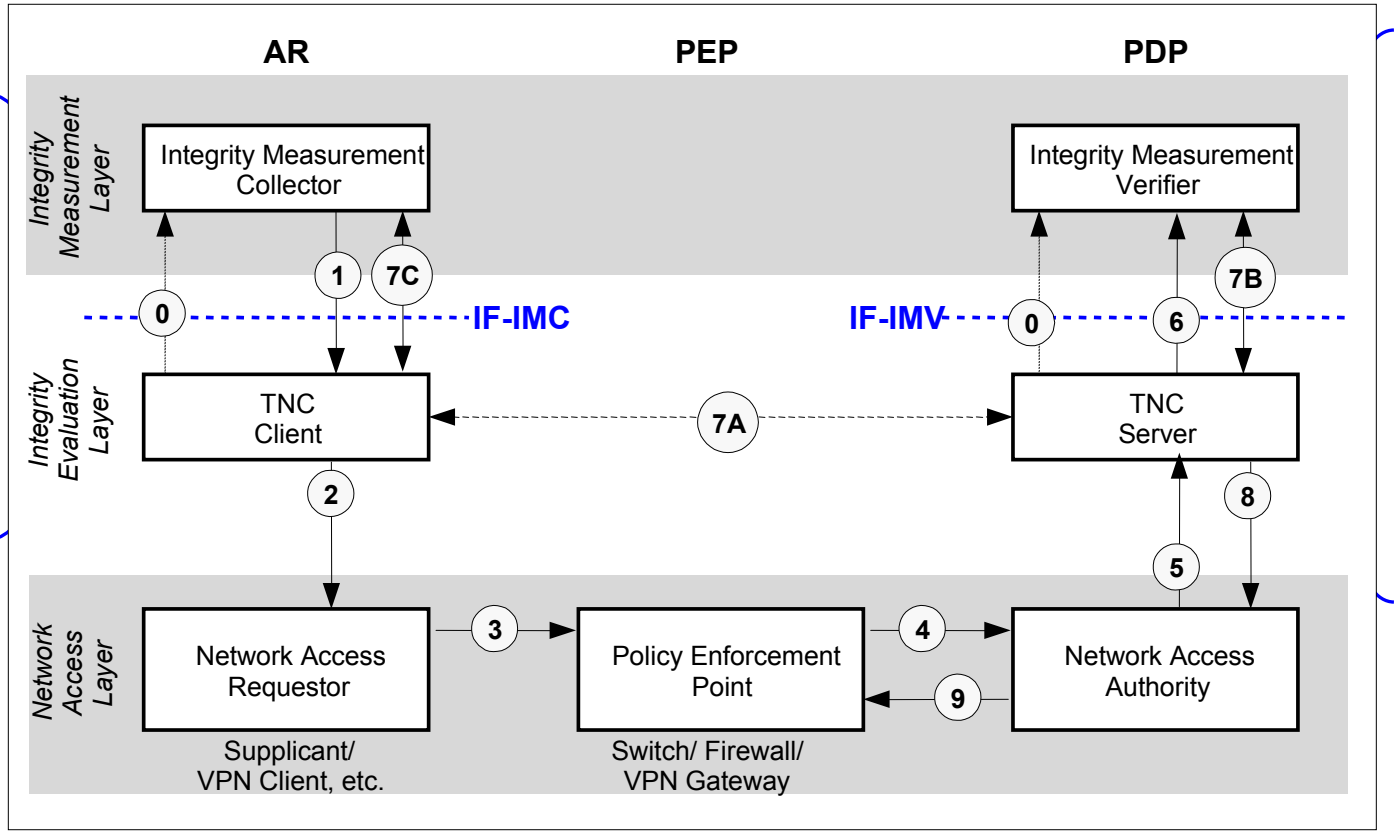


What's New Today

- **Client-Integrity Measurement Collector Spec (APIs)**
- **Server- Integrity Measurement Verifier Spec (APIs)**

IMC API Features

- Integrity Check Handshake
- Connection Management
- Remediation & Handshake Retry
- Message Delivery
- Batches



IMV API Features

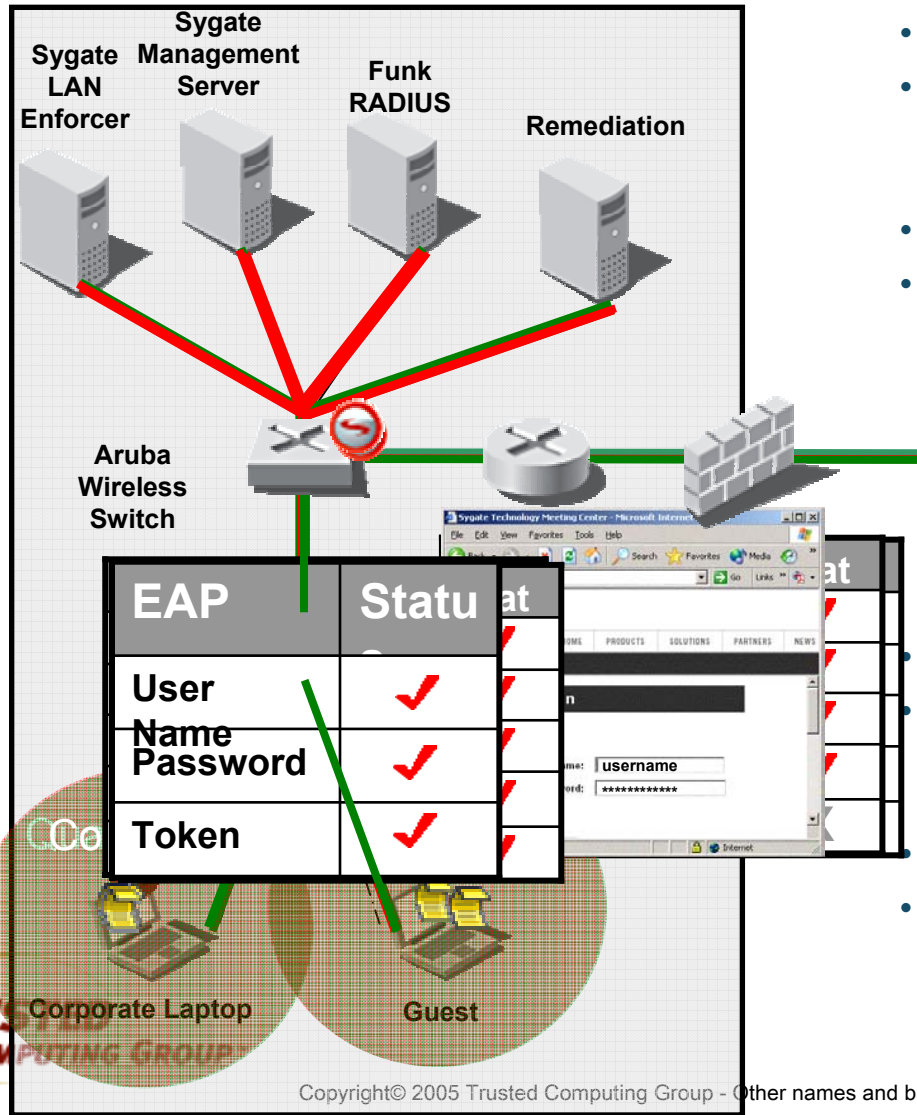
- Integrity Check Handshake
- Connection Management
- Remediation & Handshake Retry
- Stateless IMVs
- IMVs with Remote Servers
- Batches

What Can Vendors Do With Today's APIs?

- Develop interoperable products based on an open specification developed by the industry
- Spec designed so that vendors can upgrade existing products rather than re-engineer them, decreasing time to market for solutions
- Based on existing standards and protocols

TRUSTED COMPUTING GROUP™

Example: Integrated Corporate & Guest Compliance & Enforcement



Corporate Devices

- Authenticate using 802.1X/EAP (optional)
- Norton Anti-Virus, Sygate Security Agent, Patches Enforced using LAN Enforcer + 802.1x/EAP
- Dynamically assigned to corporate network
- Devices remediated if necessary

Guest/Rogue Devices

- Authenticate using Web Login
- Norton Anti-Virus, Sygate Security Agent, Patches Enforced Sygate On-Demand Agent (Java)
- Dynamically assigned to isolated network
- Devices remediated if necessary

Large Federal Agency enforce policy on guests

Requirements:

- Eliminate or control access by non corporate devices
- Ensure government devices on LAN and VPN are compliant with policy.
- Juniper SSL, Cisco Switches, any AV
- No forklift upgrades
- Integrate with existing incident response systems.

Solution:

- Leverage existing standards (802.1x)
- Leverage existing infrastructure

Benefits:

- Stop malicious code from entering the network via laptops and desktops
- Broad policy coverage within existing operational process

TRUSTED COMPUTING GROUP™

Global Oil Services Company, enforce employee data privacy policy

Requirements:

- Protect sensitive HR, business data on SAP system from being compromised at endpoint
- Stop malicious code from entering the network via mobile users & contractors
- Juniper SSL, Cisco Switches, any AV

Solution:

- Secure web-based remote access
- Integrate with SAP R/3 via IIS Web Server

Benefits:

- No additional user IDs required for distribution to endpoints – leverage existing SAP portal
- No additional inline devices required to provide secure access to SAP data

TRUSTED COMPUTING GROUP™

International Financial Services policy to protect "anydevice" access

Requirements:

- Secure "anytime, anydevice, anyplace" computing
- React to internal events in near real-time
- Flag unauthorized applications (e.g. Kazaa) when installed
- Juniper, Nortel, Cisco Infrastructure
- any AV, Alteris Config management

Solution:

- Implemented location-dependent policies for home, traveling, and office connections
- Integrated with Tripwire host-based and network-based intrusion detection systems

Benefits:

- 87% decrease in incident response time
- Reduced desktop change management costs due to policy enforcement
- Improved patching policy compliance

TRUSTED COMPUTING GROUP™

ATM Manufacturer enforces remote access policy

Requirements:

- Protect 5,000 mobile & remote users
- Enforce security policy & patching
- Control consultant & employee external access to internal resources

Solution:

- Ensure compliance before permitting network access
- Nortel VPN integration

Benefits:

- Saving $25,000+ per month in remote connection costs
- Immune to Blaster and other worms with strict patch enforcement
- Eliminated copyright violations with active policy enforcement

TRUSTED COMPUTING GROUP™

Trusted Computing Group Booth

- **The TCG will be showcasing a number of available member platforms running trusted applications at booth #1743**

- **Complete the Trusted Computing Group Seminar Survey**

TRUSTED COMPUTING GROUP™

Questions & Answers

Thank You