"Putting Trust Into Computing: Where Does it Fit?"

Monday, February 14, 2005
9:00 a.m. – 12:00 p.m.

Agenda

09:00am	Introduction Jim Ward, *IBM, TCG Board President / Chair*
09:05am	Trusted Network Connect Overview Thomas Hardjono, *VeriSign*
9:45am	Open Source Solutions Dr. Dave Safford, *IBM*
10:25am	Writing and Using Trusted Applications Ralph Engers, *Utimaco Safeware AG*; George Kastrinakis, *Wave Systems*; William Whyte, *NTRU Cryptosystems, Inc.*
11:15am	Customer Case Studies Stacy Cannady, *IBM*; Manny Novoa, *HP*
11:50am	Q&A Mark Schiller, *HP*; Jim Ward, *IBM*; Brian Berger, *Wave Systems*

TRUSTED COMPUTING GROUP™

Agenda

09:00am

Introduction
Jim Ward, *IBM, TCG Board President / Chair*

Jim Ward is a Senior Technical Staff Member and security architect within the IBM software group division.

Ward has been a core contributor in the security standards space and currently serves as the President and Board Chair of the Trusted Computing Group.

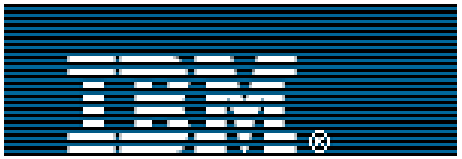
TRUSTED COMPUTING GROUP™

TCG Mission

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

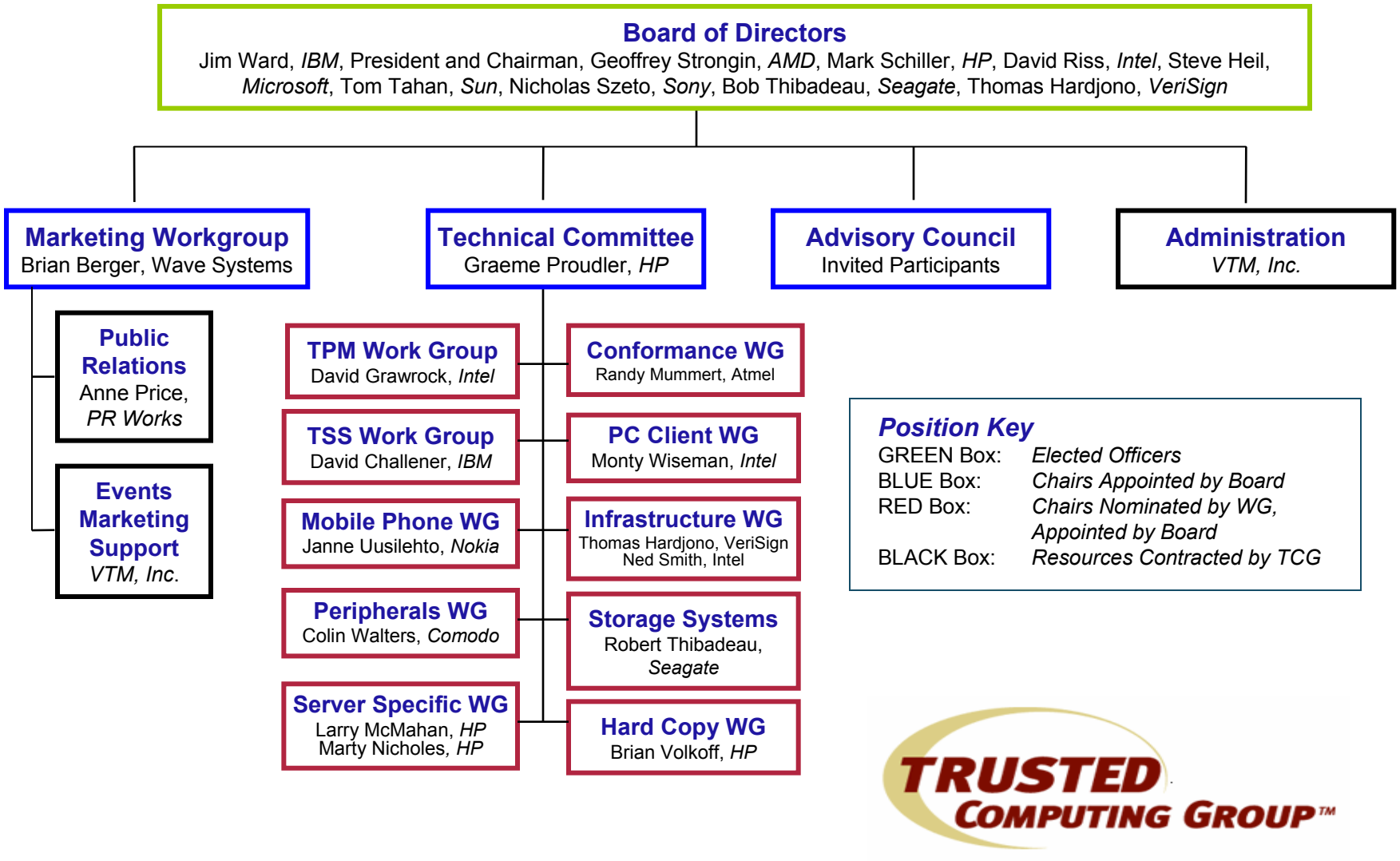
TRUSTED COMPUTING GROUP™

TCG Board of Directors



TRUSTED COMPUTING GROUP™

TCG Organization



TCG Membership

92 Total Members as of January 13, 2005
7 Promoter, 64 Contributor, 21 Adopter

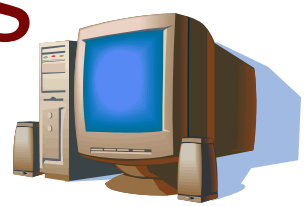
Promoters
AMD
Hewlett-Packard
IBM
Intel Corporation
Microsoft
Sony Corporation
Sun Microsystems, Inc.

Adopters
BigFix, Inc.
Citrix Systems, Inc
Enterasys Networks
Foundry Networks Inc.
Foundstone, Inc.
Gateway
Industrial Technology Research Institute
Interdigital Communications
Latis Networks, Inc.
MCI
Nevis Networks, USA
PC Guardian Technologies
Sana Security
Senforce Technologies, Inc
Silicon Integrated Systems Corp.
Silicon Storage Technology, Inc.
Softex, Inc.
Telemidic Co. Ltd.
Toshiba Corporation
TriCipher, Inc.
ULi Electronics Inc.

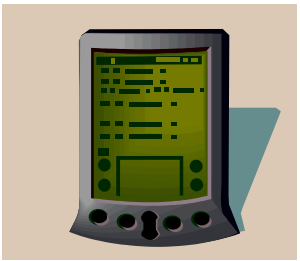
Contributors
Agere Systems
ARM
ATI Technologies Inc.
Atmel
AuthenTec, Inc.
AVAYA
Broadcom Corporation
Certicom Corp.
Comodo
Dell, Inc.
Endforce, Inc.
Ericsson Mobile Platforms AB
Extreme Networks
France Telecom Group
Freescale Semiconductor
Fujitsu Limited
Fujitsu Siemens Computers
Funk Software, Inc.
Gemplus
Giesecke & Devrient
Hitachi, Ltd.
Infineon
InfoExpress, Inc.
iPass
Juniper Networks
Lenovo Holdings Limited
Lexmark International
M-Systems Flash Disk Pioneers

Contributors
Meetinghouse Data Communications
Motorola Inc.
National Semiconductor
nCipher
Network Associates
Nokia
NTRU Cryptosystems, Inc.
NVIDIA
OSA Technologies, Inc
Philips
Phoenix
Pointsec Mobile Technologies
Renesas Technology Corp.
RSA Security, Inc.
SafeNet, Inc.
Samsung Electronics Co.
SCM Microsystems, Inc.
Seagate Technology
SignaCert, Inc.
Sinosun Technology Co., Ltd.
Standard Microsystems Corporation
STMicroelectronics
Sygate Technologies, Inc.
Symantec
Symbian Ltd
Synaptics Inc.
Texas Instruments
Transmeta Corporation
Trend Micro
Utimaco Safeware AG
VeriSign, Inc.
Vernier Networks
VIA Technologies, Inc.
Vodafone Group Services LTD
Wave Systems
Zone Labs, Inc.

Technical Work Groups



- Technical Committee
- Work Groups
  - Trusted Platform Module (TPM)
  - TPM Software Stack (TSS)
  - PC Specific Implementation
  - Peripheral Implementation
  - Server Specific Implementation
  - Storage Systems Implementation
  - Mobile Phone Specific Implementation
  - Conformance (Common Criteria)
  - Infrastructure
  - Hard Copy
  - Trusted Network Connect
- Marketing Work Group



TRUSTED COMPUTING GROUP™

Agenda

09:05am

Trusted Network Connect Overview
Thomas Hardjono, *VeriSign*

Thomas Hardjono is principal scientist and director within VeriSign. His work includes cryptography, network security, multicast/group security, PKI systems, wireless and 3G networks, digital rights management and trusted computing.

He is currently co-chair of the Infrastructure Work Group within the Trusted Computing Group. He also represents VeriSign Inc. on the TCG Board of Directors..

TRUSTED COMPUTING GROUP™

The TCG Trusted Network Connect (TNC) Architecture: An Overview

Trusted Computing Seminar
RSA 2005 Conference
February 14, 2005

Contents

- The Challenge of Trusted Computing
- Features & Benefits of Trusted Platforms
- Trusted Network Connect (TNC)
- Summary

TRUSTED COMPUTING GROUP™

Introduction

The Challenge of Trusted Computing

The Challenge of Trusted Computing

- Trusted Computing
  - How to create a safer computing environment that is faced with increasing frequency and sophistication of attacks
  - Protect end-user data
  - Enable trusted eCommerce transactions
  - Hardware-rooted trust
- Increase the level of trust in the PC platform
  - Increase consumer confidence in Internet use
  - Reduce business risks, specially for security-conscious sectors
    - Financial Services, Insurance, Government, Healthcare
  - Increase in transaction volume and value with hardware enforced protections
- Increase trust in other platforms
  - Laptops, Desktops, PDA, Servers, Mobile Phones, Network gear, etc.

TRUSTED COMPUTING GROUP™

Technical Challenge & the TP Solution

- Challenge:
  - Allow communicating platforms to dynamically accept and execute code supplied by the network.
  - Allow a platform connect and interact with remote platforms.
  - Protection of data from misuse.
- Solution:
  - Turn the entire platform into a trusted environment.
  - Enable a platform to prove that a given software environment is a protected environment.
  - Secrets are protected until the correct software environment exists
    - Only then are secrets released into that environment.

TRUSTED COMPUTING GROUP™

Features of Trusted Platforms

What distinguishes TPs

Features of a Trusted Platform

1. Protected Capabilities

- The set of commands with exclusive permission to access Shielded Locations (SL).
- SL are places (memory, register, etc.) where it is safe to operate on sensitive data.
- The TPM implements protected capabilities and shielded-locations.

2. Integrity Measurement and Storage

- The Process of obtaining metrics of platform characteristics that affect the integrity (trustworthiness) of a platform.
- The storing those metrics and the placement digests of those metrics in Platform Configuration Registers (PCR).

TRUSTED COMPUTING GROUP™

Features of a Trusted Platform (cont)

3. Integrity Reporting

- The process of attesting to the contents of integrity storage (i.e. PCRs).
- Philosophy: a platform may be permitted to enter any state possible (including insecure states), but it may not be permitted to lie about states that is was or was not in.
- Multiple *Roots of Trust* in TPM (i.e. keys)

4. Attestations

- The process of vouching for the accuracy of information (e.g. in the PCRs).
- Attestations by the TPM and Platform
- Attestation digitally signed using various TPM-bound and Platform-bound certificates.

TRUSTED COMPUTING GROUP™

Benefits of using TP Features

- Integrity self-protection of a platform
  - Building blocks to turn the platform into a trusted environment.
  - Allow to prove that a given software environment is a protected environment.
  - Secrets encrypted to a given platform configuration
    - Decipherable only by the platform in that configuration
- Platform Authentication (Remote Attestations)
  - *Platform Authentication*: a platform proves to another that it is in a given configuration
  - In a network authentication scenario, becomes the basis for proving *Network End-Point Integrity*
    - The Trusted Network Connect (TNC) approach

TRUSTED COMPUTING GROUP™

Trusted Network Connect

Platform Authentication & Network End-Point Integrity

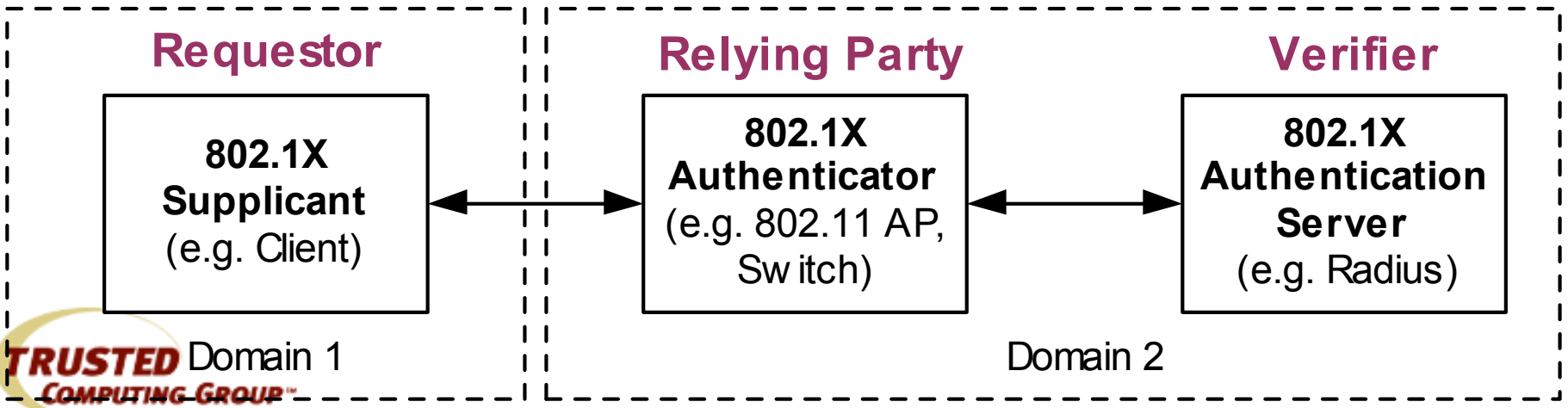
Trusted Network Connect (TNC)

- TNC: Network end-point integrity using Trusted Platform features
  - A Client seeking connectivity to a network is integrity-evaluated against a given set of policies and (expected) platform configurations.
  - Clients failing integrity-evaluation have the option of being Remediated.
- Technological components:
  - Common standardized architecture/framework
  - Platform authentication model using TP features
  - Platform authentication protocol(s)
  - Standardized APIs

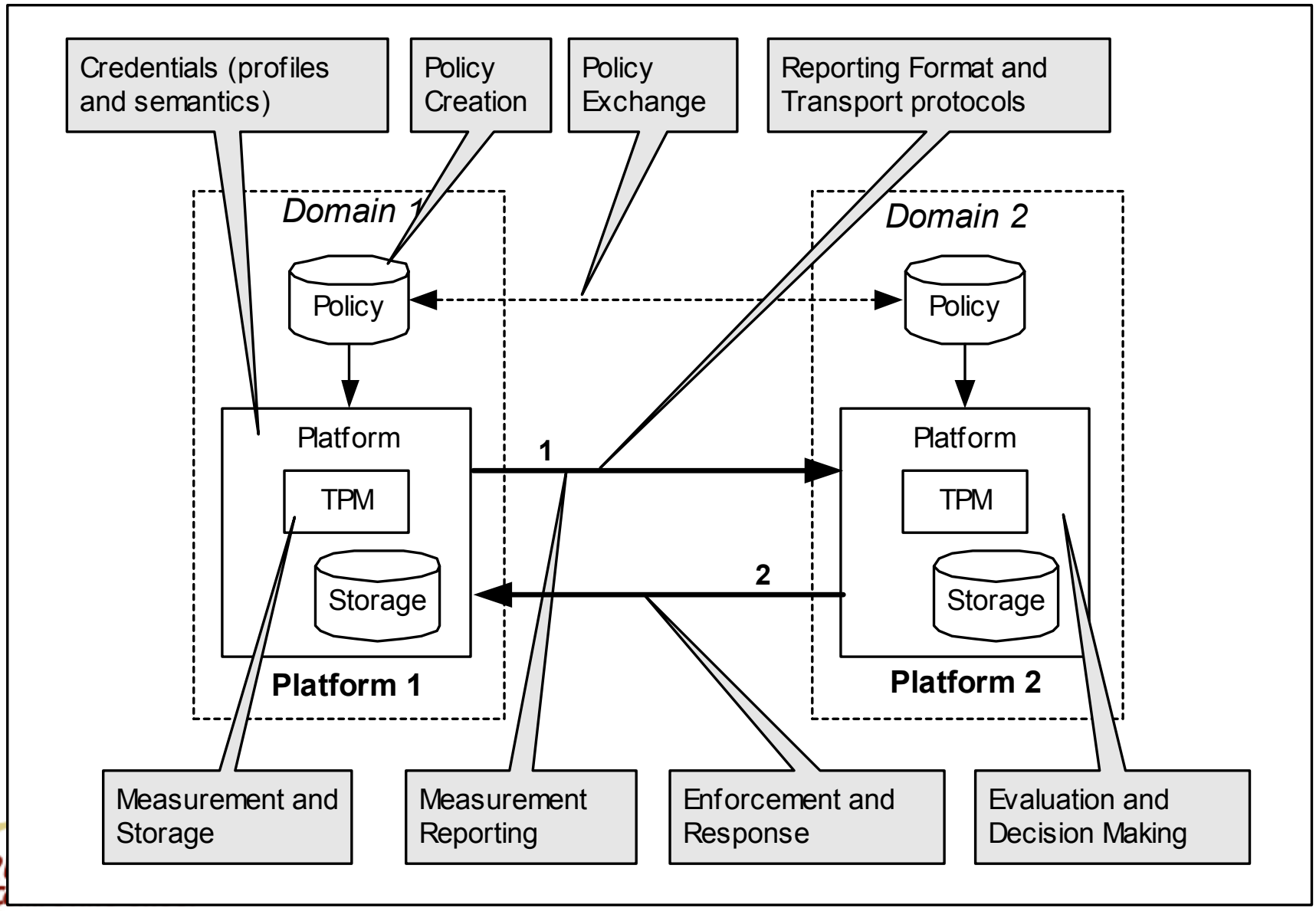
TRUSTED COMPUTING GROUP™

Basic Authentication Model

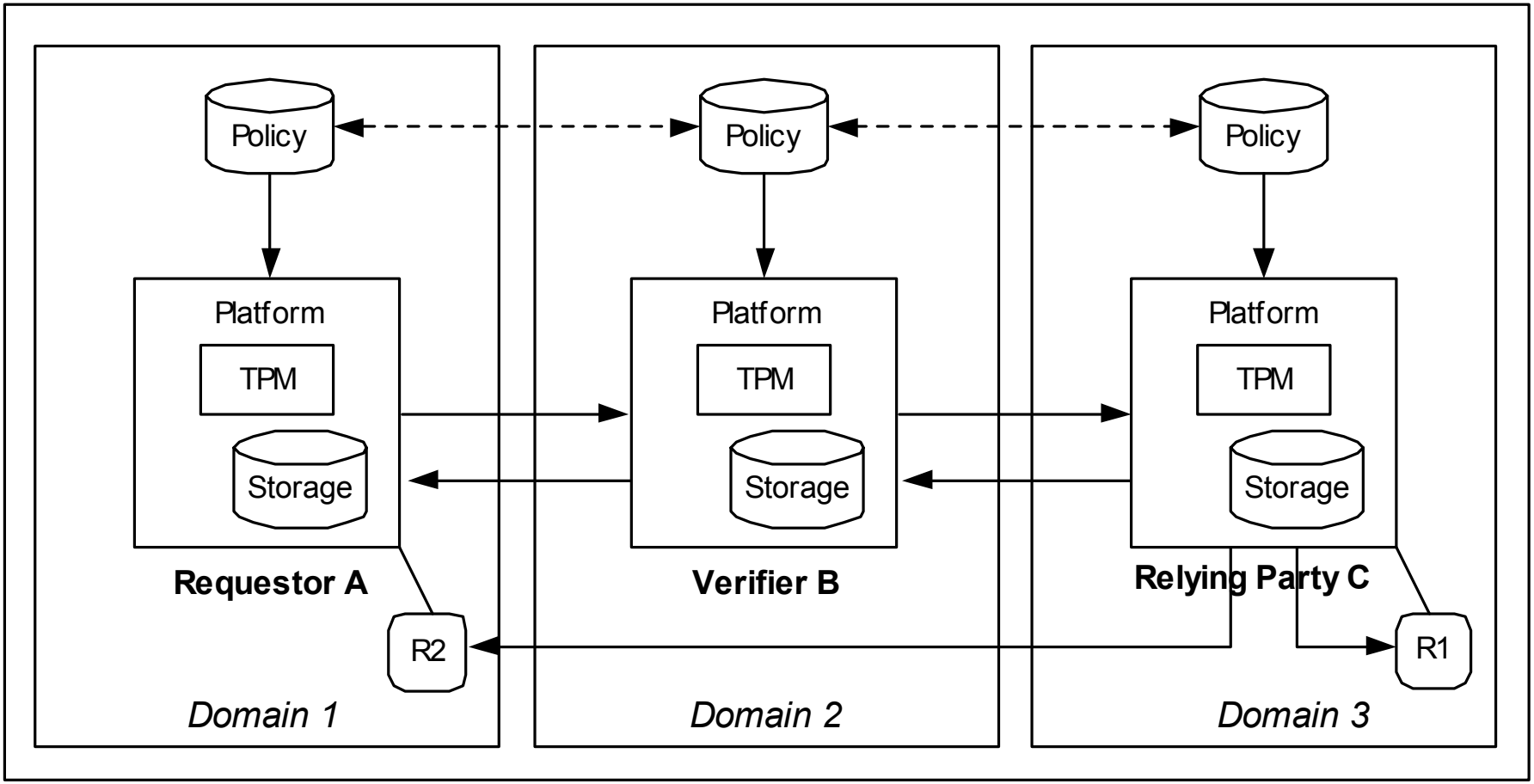
- The 3-party model
  - *Requestor* seeks services or access to resource from the *Relying-Party*
  - *Verifier* performs the evaluation of the Requestor's assertions
- Outcome of the Verifier's evaluation can be binary (accept/reject) or a trust score



Platform Authentication Features



Platform Authentication (3-Party)

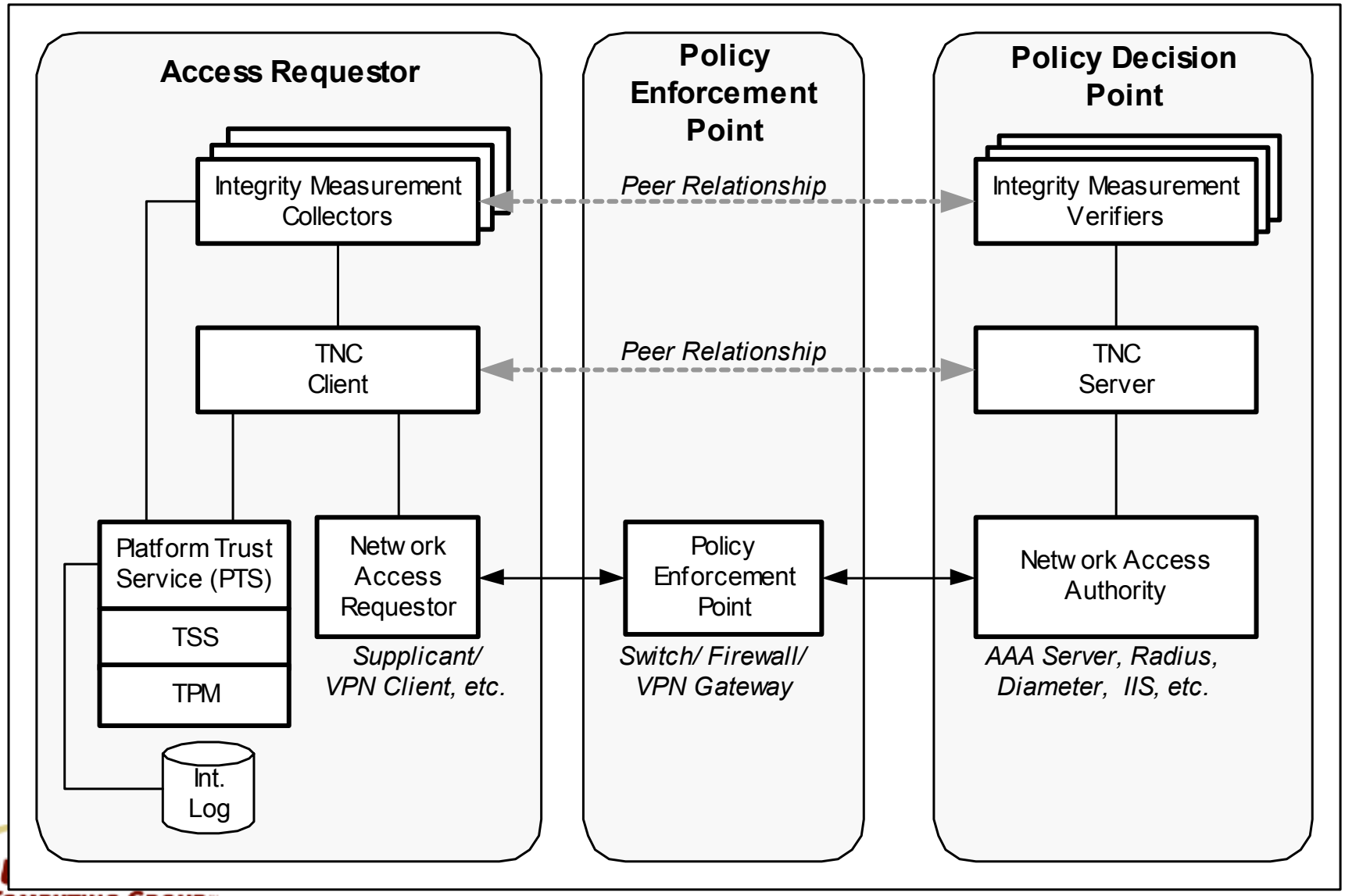


The TNC Architecture

- Trusted Network Connect (TNC)
  - Specifications for End-Point Integrity developed by networking vendors within the TCG.
  - TNC-Subgroup is a working group under the TCG's Infrastructure Working Group developing the specs.
- Purpose of the TNC Architecture:
  - Common reference framework for end-point integrity
  - Component specification & functional standardization
    - APIs, data formats, messages
  - Applicable to as wide use-cases as possible
    - e.g. 802.1X, VPN, dial-up & other network-access

TRUSTED COMPUTING GROUP™

The TNC Architecture



Architecture Entities

- Access Requestor (AR):
  - *Integrity Measurement Collector:*
    - Measures aspects of the AR's integrity (e.g. AV, etc).
    - May use *Platform Trust Services* (PTS) to obtain integrity information regarding every component on the platform.
  - *TNC Client:*
    - Aggregates integrity measurements (from IMCs)
    - Assists the management of the integrity check handshakes
    - Assists in the measurement & reporting of platform and IMC integrity.
  - *Network Access Requestor:*
    - Network-layer negotiation & access onto a given network.
    - Network layer transport protocol.
    - End-to-end secure channel creation & management.

TRUSTED COMPUTING GROUP™

Architecture Entities (cont)

- Policy Decision Point (PDP)
  - *Integrity Measurement Verifier:*
    - Verifies AR's integrity based on measurements received from IMCs, against network security policy.
  - *TNC Server:*
    - Manages IMV-to-IMC (peer) message flows.
    - Gathers recommendations from IMVs.
    - Provides action-recommendation to the NAA.
  - *Network Access Authority:*
    - Decides whether a Access Requestor should be granted network access.
    - Network layer transport protocol.
    - End-to-end secure channel creation & management.

TRUSTED COMPUTING GROUP™

Architecture Entities (cont)

- Platform Trust Services (PTS)
  - System service that exposes trusted platform capabilities to TNC components that reside on a Trusted Platform containing a TPM.
  - PTS Services include: protected key storage, asymmetric cryptography, random numbers, platform identity, platform configuration reporting and integrity state tracking.
- Protocols for integrity reporting:
  - *TLS-Attestations*: uses Extensions capabilities in TLS to exchange integrity data.
  - *TLS/IAP*: allows IMCs and IMVs to communicate as peers, regardless of underlying transport.

TRUSTED COMPUTING GROUP™

Summary

- Features of Trusted Platforms as the basis for establishing strong End-Point Integrity.
  - Protected Capabilities, Integrity Measurement & Reporting, and Attestations
- Mutual Platform Authentication achieved using building blocks in the TCG
  - 3-Party authentication model, making use of TP features
  - Requestor, Relying Party and Verifier
- TNC designed to provide End-Point Integrity based on features of Trusted Platforms
  - Mutual Platform Authentication
  - Trust rooted in Hardware (the TPM)
  - TNC Architecture defines entities, functions and services for network end-point integrity

TRUSTED COMPUTING GROUP™

Agenda

9:45am

Open Source Solutions
Dr. Dave 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 Support for Trusted Computing

Dave Safford, IBM Research

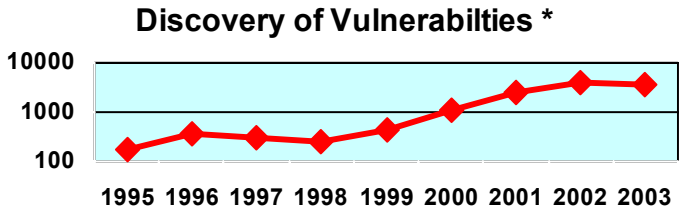
Outline

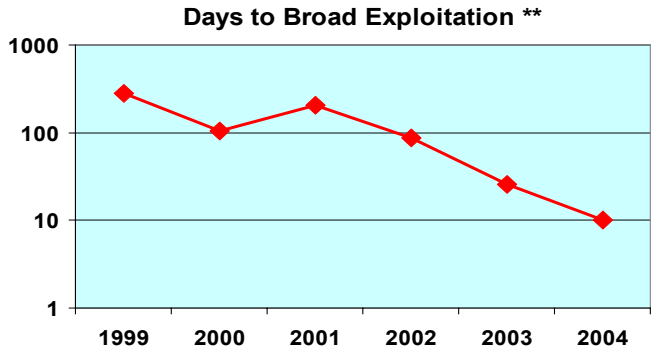
- Threat Trends
- Trusted Computing
- Open Source Projects
- What's Missing
- The Future

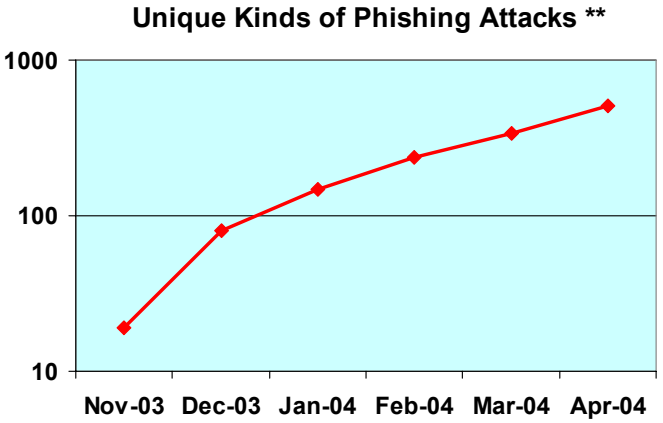
TRUSTED COMPUTING GROUP™

The Problem: Client Risk is Dramatically 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
  - The myDoom.O virus overloaded networks around the world in August 2004
  - Blaster worm attack cause First Energy's Davis Besse Nuclear Reactor to loose digital control for over four hours in January 2003
  - Viruses are already deploying attacks against AV software
  - 80% of clients have spyware infestations
  - 30% of clients already have back doors (FSTC)
- Increase in vulnerability rate is slowing, but 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







TRUSTED COMPUTING GROUP™

How can the Trusted Platform Module (TPM) 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)

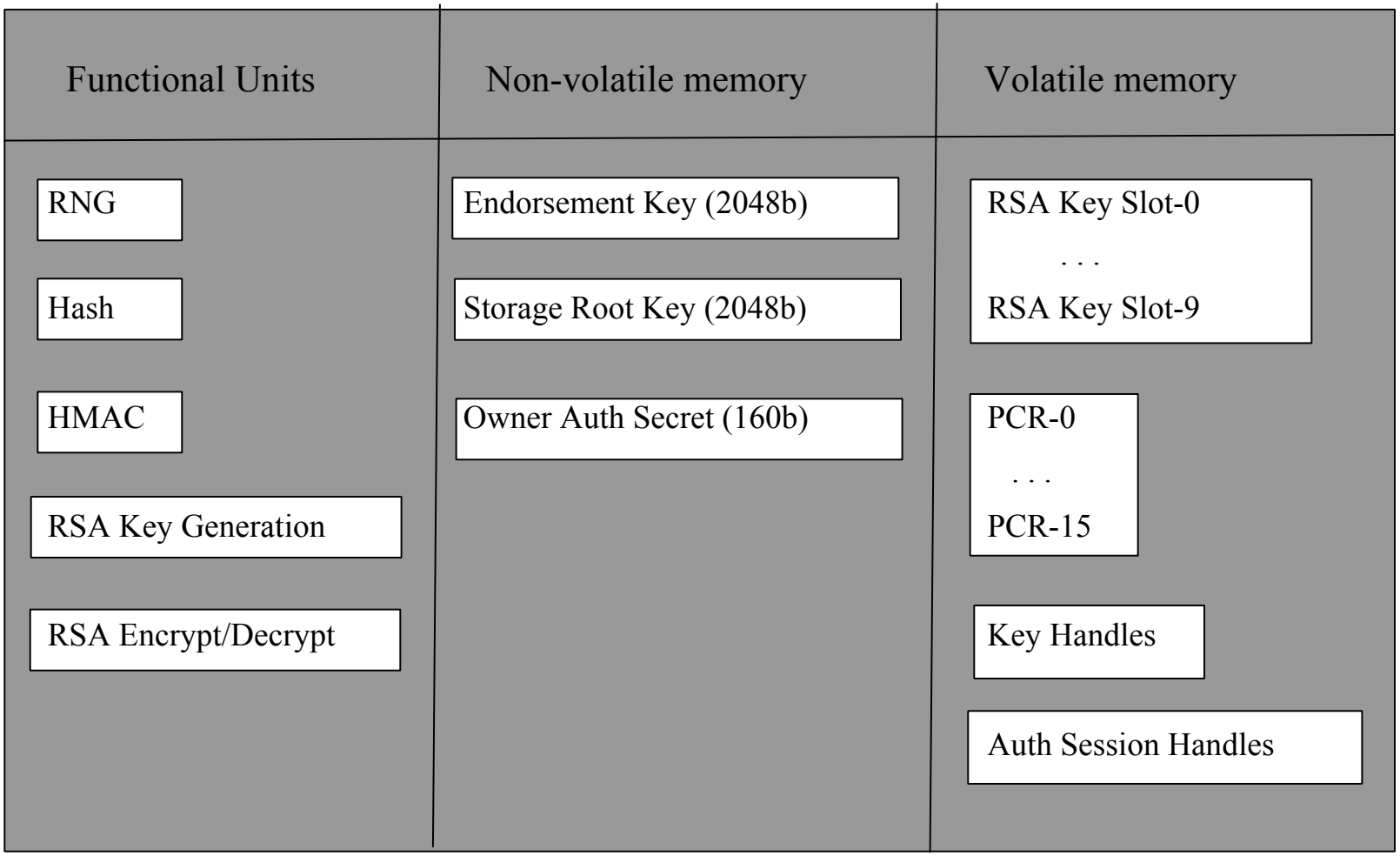
TRUSTED COMPUTING GROUP™

Understanding TPM:

- Main Specification:
  - Trusted Computing Group (TCG) home page:
    - http://www.trustedcomputinggroup.org
- Problem:
  - Spec is over 320 pages (version 1.1b)
  - very hard to understand
- 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
  - TPM Key Migration server
  - 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™

Open Source TPM Projects

- IBM Research
  - Linux Device Driver/library/applications
    http://www.research.ibm.com/gsal/tcpa

  - Linux device driver
  - simple access library
  - basic applications
    - tpm_demo
    - takeown
    - createkey, loadkey, listkeys, evictkey
    - signfile, verifyfile
    - bindfile, unbindfile
    - sealfile, unsealfile

TRUSTED COMPUTING GROUP™

Open Source TPM Projects

- TPM Key Migration server
  - If keys are locked within a TPM, what happens if TPM breaks?
    - for authentication keys, may be acceptable to create new, and reregister
    - for storage keys, broken TPM could mean loss of data
  - Current product solution saves copy of root on removable media
  - Need a solution which preserves hardware boundary guarantees

  - Key migration server uses a trusted third party with TPM to
    - backup/restore TPM keys to server's TPM
    - broker key migration from one TPM to another TPM
    - broker migration from one PCR state to another on same TPM

    - hides complexity of key migration from user

TRUSTED COMPUTING GROUP™

Open Source TPM Projects

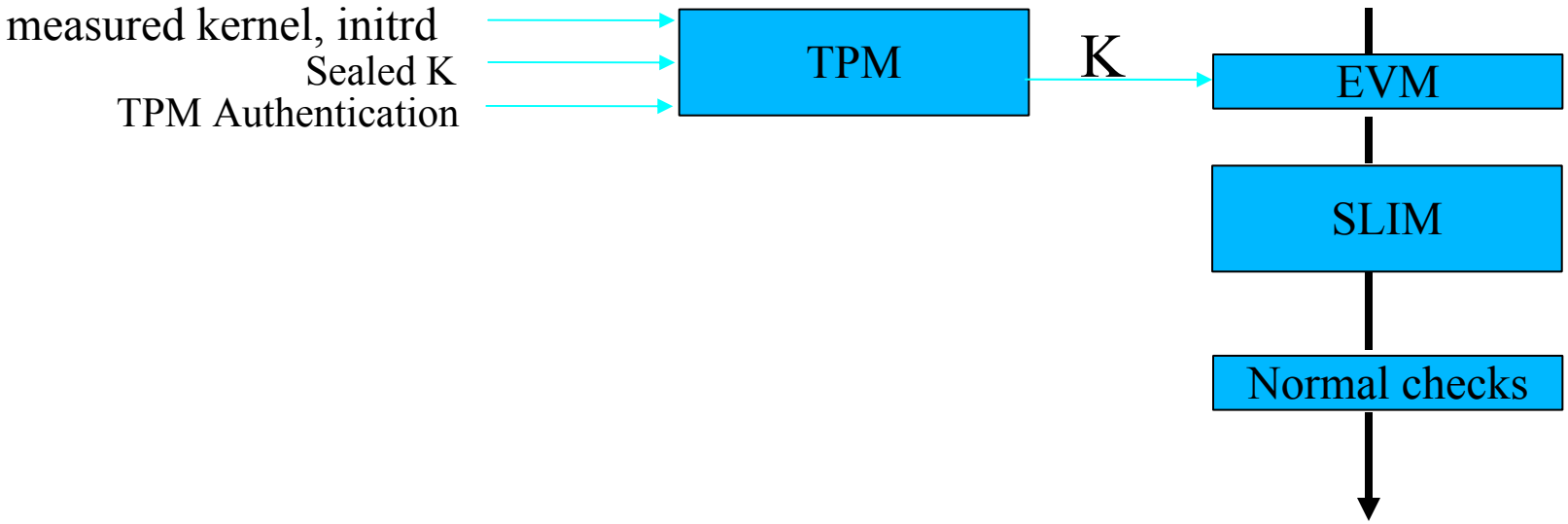
- Trusted Linux Client
  - Goals:
    - protect integrity of system from current attacks
    - be transparent to user
      - let user get job done
      - block only malicious activity
  - Foundations:
    - TPM
    - LSM
  - Functionality
    - TPM measured and authenticated boot
    - Authenticated file metadata for storing hashes, labels
    - Enhanced Lomac style Mandatory Access Control

TRUSTED COMPUTING GROUP™

Trusted Linux Client LSM 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:



TPM Module

- TPM measures integrity of boot process through kernel and initrd
- In initrd boot, user supplies sealed kernel key and authorization PW
- If TPM measurements match, and password matches, TPM releases K.
- Master key K is used to generate derived keys for
  - encrypted home directory partition loopback
  - authenticated file attribute checking (EVM)

TRUSTED COMPUTING GROUP™

Extended Verification Module: EVM

- Use extended file attributes to store authenticated file metadata
  - file hash
  - mandatory access control labels
  - version
  - antivirus status
- Use tpm based symmetric kernel key to HMAC these attributes
- Verify file once at open/execute, and cache verification
- “heavy lifting” done at install time, runtime is just file hash and HMAC
- Extensible, policy based definition of attributes and actions

TRUSTED COMPUTING GROUP™

SLIM Sandbox:

- Simple Linux Integrity Module (SLIM)
  - Use of LSM framework hooks
  - EVM context information to enable sandbox decision
  - Includes Lomac's low-water mark integrity model for ease of administration
  - With Caernarvon's separation of read and write/execute permissions
  - With Caernarvon's signed guard processes – verified trusted programs

- Basic Integrity Operation:
  - Low Integrity processes can read and execute up, but not write up
  - High Integrity processes can write down, but are demoted on read/execute down
  - Trusted “guard” processes, verified by EVM, can read down without demotion
    - rpm
    - sshd

SLIM Access Classes

All Files are labeled with an Integrity and Secrecy MAC label

```
Integrity Access Classes (IAC)
   SYSTEM
   USER
   UNTRUSTED
   EXEMPT

Secrecy Access Classes (SAC)
   SENSITIVE
   USER
   PUBLIC
   EXEMPT
```

All Processes have upper and lower Integrity and Secrecy lables:

```
Integrity Write/Execute Access Class (IWXAC)
Integrity Read Access Class (IRAC)
Secrecy Write Access Class (SWAC)
Secrecy Read/Execute Access Class (SRXAC)
```

(Upper and Lower are the same, except for guard processes.)

EVM and SLIM 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
```

Open Source TPM Projects

- IBM Linux Technology Center
  - Official Device Driver to be included in base Linux 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™

Open Source TPM Projects

- Rick Wash (umich) BSD port of IBM driver/library/applications
  - http://www.citi.umich.edu/u/rwash/projects/trusted/netbsd.html

TRUSTED COMPUTING GROUP™

Open Source TPM Projects

- Dartmouth enforcer
  - http://sourceforge.net/projects/enforcer
  - Similar in goals to TLC
    - integrity measurement, enforcement
    - Lilo bootloader support
    - does not include MAC

TRUSTED COMPUTING GROUP™

Open Source TPM Projects

- Swiss Federal Institute of Technology – TPM emulator
  - http://www.infsec.ethz.ch/people/psevinc/
  - Linux Kernel module which emulates TPM
  - Compatible with IBM device driver and applications
  - Gives backwards compatibility software option

TRUSTED COMPUTING GROUP™

Open Source TPM projects – What's Missing?

- OpenSSL and PKCS-11 support
  - Example applications already use OpenSSL key formats
  - Need way to use TPM for client side SSL authentication

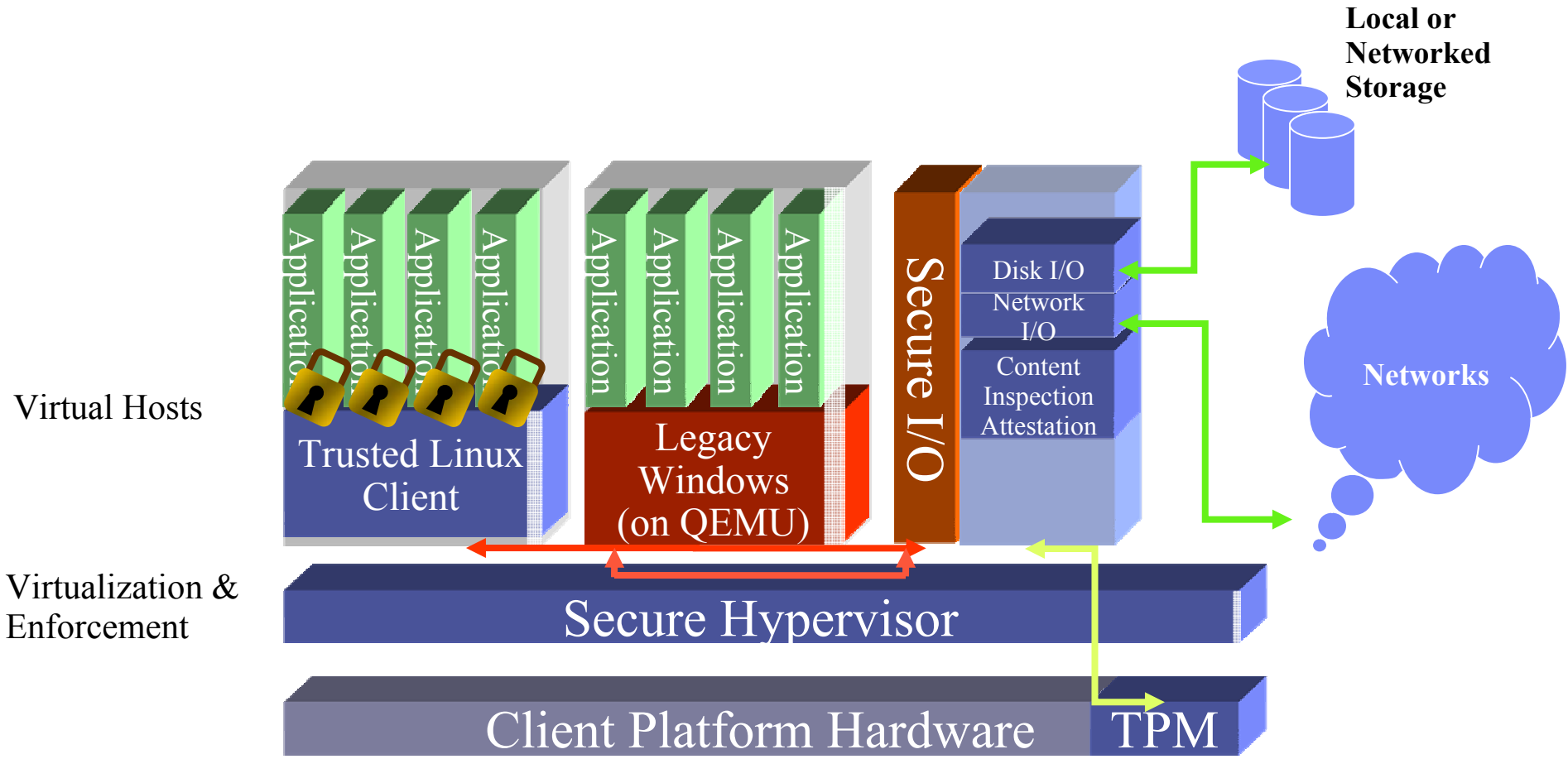
TRUSTED COMPUTING GROUP™

Open Source Trusted Computing – The Future

- The bigger picture:
  - linux and windows
  - cross platform, open architecture
  - strong defenses, and rapid recovery
  - leverage linux, TLC for part of the solution
  - use open hypervisor (Xen) for integration/isolation

TRUSTED COMPUTING GROUP™

Hypervisor technology provides strong isolation and controlled sharing among applications



Agenda

10:25am

Writing and Using Trusted Applications
Ralph Engers, *Utimaco Safeware AG*; George Kastrinakis, *Wave Systems*; William Whyte, *NTRU Cryptosystems, Inc.*

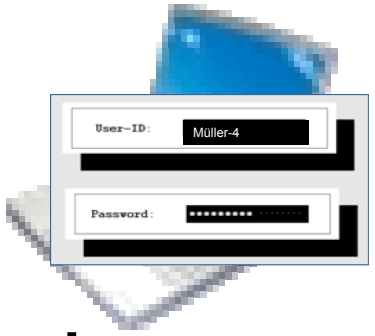
Ralf Engers is responsible for research and development in the personal device security line of business of Utimaco Safeware AG.

Quality assurance and certification is part of Engers' work. The products of the line of business provide a complete basic security for mobile clients, using bulk (hard disk) encryption, transparent file encryption, container encryption and policy enforcement.

Security Solutions in Operation

Ralf M. Engers
CTO Device Security
Utimaco Safeware AG

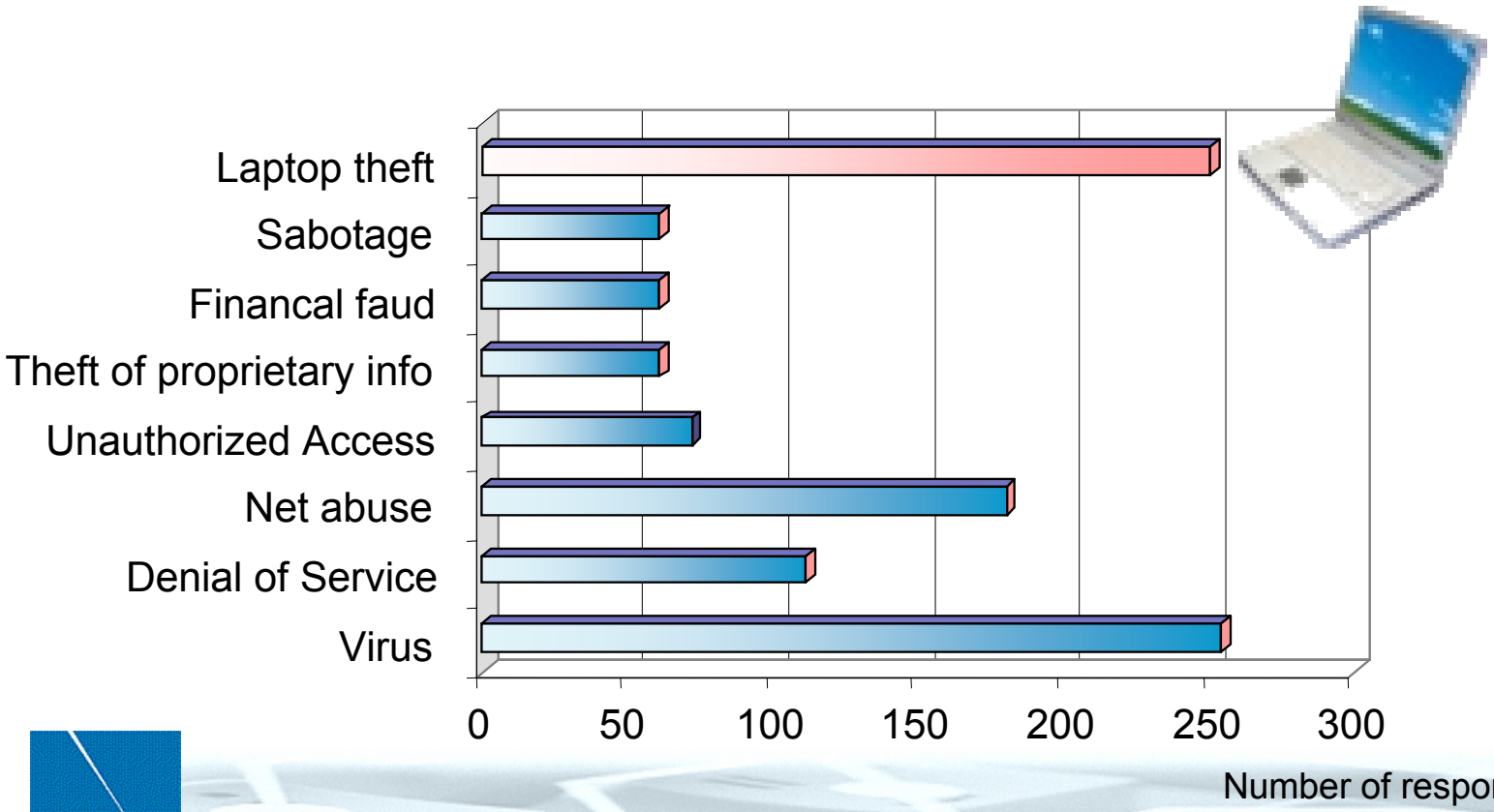
Writing Trusted Applications



- **Pre-Boot-Authentication**
  - One way to hack a Windows system is to bypass the GINA authentication. The solution:
    - Increased protection of credentials (encrypting the SAM)
    - Implementation of an authentication system, independent from the operating system: Pre-Boot-Authentication
- **CSP for the TPM**
  - Applications which use already CSPs can use those CSPs, which drive TPMs
  - Most security benefits of a smart card, but no additional hardware to be bought/installed
- **Encryption**

TRUSTED COMPUTING GROUP™

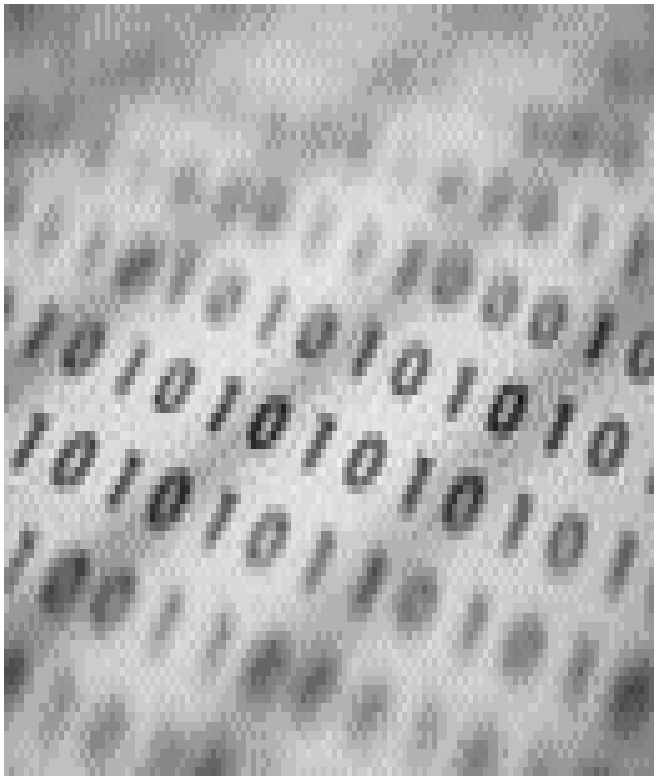
Risks in IT - Types of Attacks and Misuse



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

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 the need to carry around a floppy
  - It is not convenient for users



- **All remaining data on the disk is still stored in plain.**

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

Use Case Mobile Devices

- **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.
- The TPM increases protection
  - Keys are stored in protected hardware or protected through hardware
  - Dictionary attacks become almost impossible

TRUSTED COMPUTING GROUP™

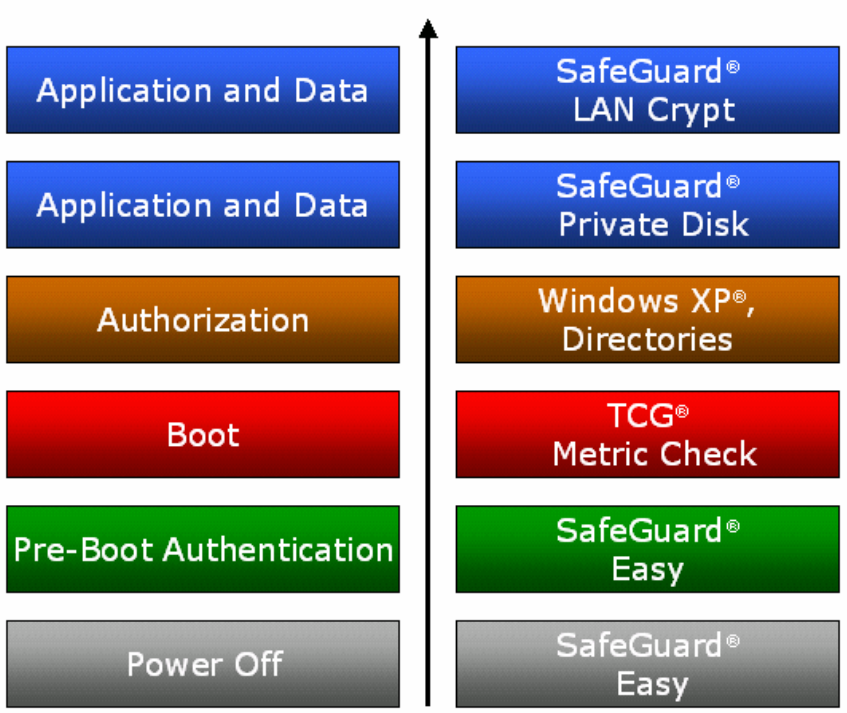
Use Case Mobile Devices and Desktops

- **Bulk Encryption with SafeGuard® Easy**
- **Power-On Protection**
  - Credentials stored in or protected by hardware
    - Certificates
      - Protection of encrypted Virtual Drives‘ content
      - Protection of encrypted Collaboration Work data
    - Passwords / Passphrases
    - SSO credentials
  - Data are tied to the platform (Machine Binding)
    - Extraction of the HDD from the desktop and mounting into another platform will not provide access to data.
  - True Random Number Generator (RSA keys)
  - Authentication Client - Server mutually

TRUSTED COMPUTING GROUP™

Layered Approach to Security

- As soon as the Base Protection Issue is solved, more fine granular security structures can be implemented
- The highly secure **pre-boot authentication** can be used to single-sign-on to further applications
  - High level of security,
  - Secrets stored in the TPM
  - SSO using certificates
    - Encrypted Containers
    - Encrypted Workgroup Data
  - SSO based on passwords
    - Legacy applications
  - WebSSO



TRUSTED COMPUTING GROUP™

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‘ company site
    - 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 all 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 data: High level of protection combined with a very user friendly security policy
- The synergy: Proactive increase of client security by key storage in hardware and machine binding
- Low cost disposal of notebooks at end of lifecycle

TRUSTED COMPUTING GROUP™

Bulk Encryption and TCG in Operation

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

- Business Need: To cope with theft and corruption of notebooks in case of theft or left

- Statistics: It is expected that from 5000 laptops 500 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 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 to the benefit for the customer
  - Increased level of security
  - Decreased costs
  - Improved managability
  - Standardization

- Utimaco is committed to integrate TCG technology to continue in providing leading edge security technology to enterprise customers

TRUSTED COMPUTING GROUP™

Ralf M. Engers
CTO Device Security
Utimaco Safeware AG
Hohemarkstraße 22
61440 Oberursel

ralf.engers@utimaco.de

You are invited to visit us at
Utimaco booth # 1510 or TCG booth # 332

Agenda

10:25am

Writing and Using Trusted Applications
Ralph Engers, *Utimaco Safeware AG*; George Kastrinakis, *Wave Systems*; William Whyte, *NTRU Cryptosystems, Inc.*

George Kastrinakis is Director of Product Management within Wave Systems. He manages product strategy for Wave, including product requirements definition, collaboration with engineering, partnering with sales, marketing and partners, and maintaining customer relationships. He has worked with security products for the past five years and in the computer software industry for 17 years.

TRUSTED COMPUTING GROUP™

Security Solutions Using TCG Technology

George Kastrinakis
Wave Systems Corp.
February 14, 2005

Overview

- Solution Opportunities
- General Security Programming Model
- TCG Programming Model
- Data Security
- Password Management & Security
- TPM Management & Security
- TPM Key Archive & Restore

TRUSTED COMPUTING GROUP™

Solution Opportunities

Current Problems

Need Trusted Solutions

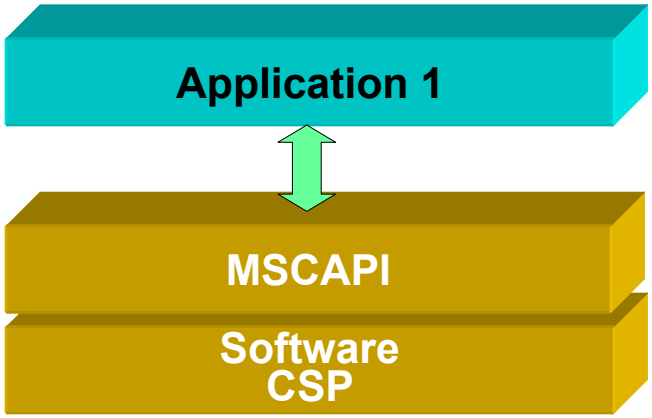
1. Stronger Network Authentication
2. Data Protection
3. Strong Authentication to VPNs
4. Password Protection
5. Secure Information Distribution
6. Secure E-mail

RESULT

Security and trusted computing represent major new services and integration opportunities

TRUSTED COMPUTING GROUP™

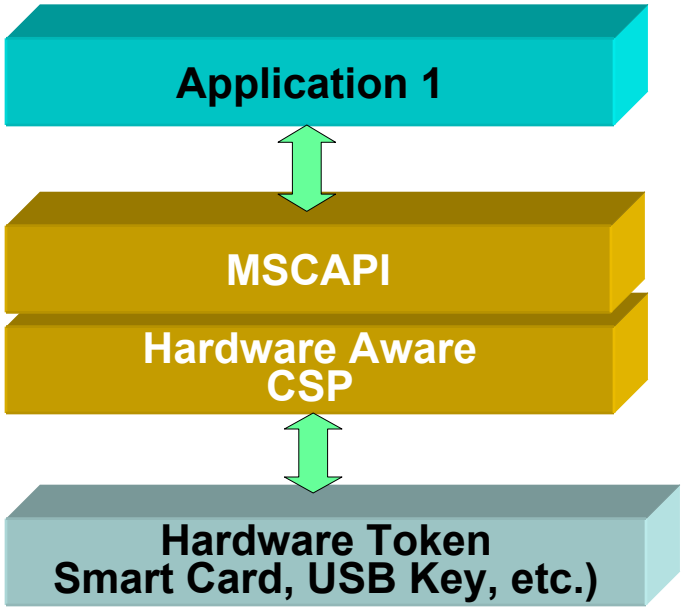
Security Programming Model
(Software Based)



- Cryptographic Service Provider (CSP)
  - Supplies crypto, key generation, key management, etc.
  - Supplied with Windows OS
    - Software based
  - Standard MSCAPI Access
- PKCS#11
  - Alternative to MSCAPI/CSP

TRUSTED COMPUTING GROUP™

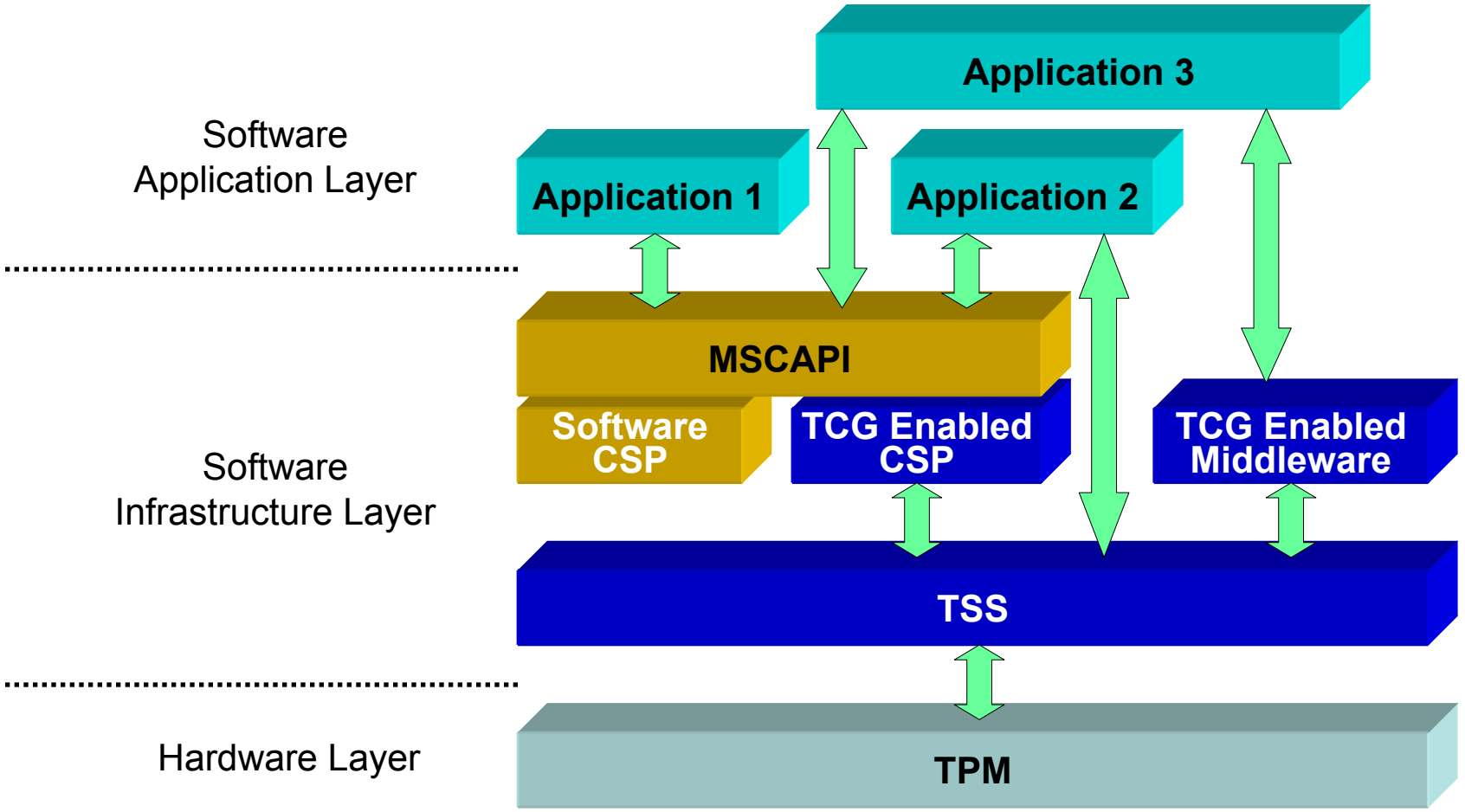
Security Programming Model
(Hardware Token)



- CSP + Hardware Token
  - Hardware token has fixed security function, CSP handles the rest
  - 3rd Party, typically supplied as a package
    - Software & Hardware based
  - Standard MSCAPI Access

TRUSTED COMPUTING GROUP™

TPM Security Programming Model



TRUSTED COMPUTING GROUP™

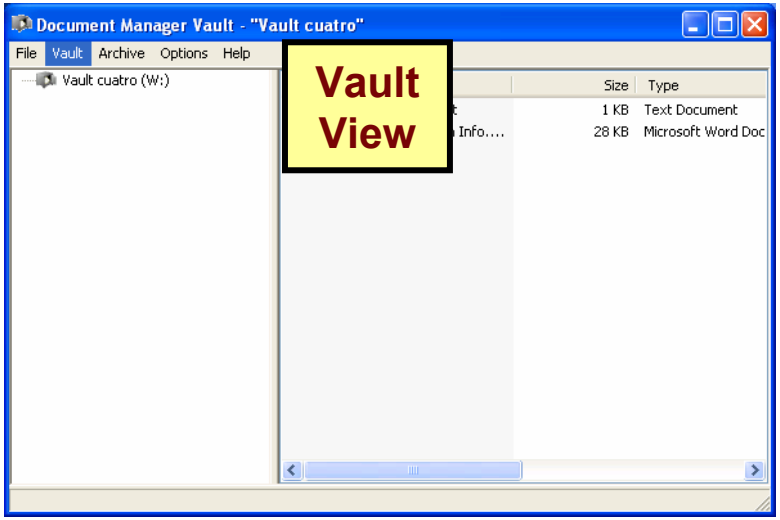
Wave's Solution Focus

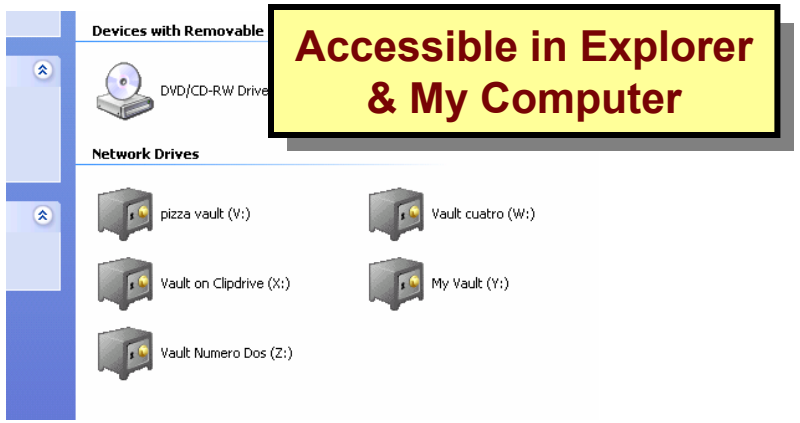
- Intuitive and **easy-to-use**
- **Interoperable** and validated across all available platforms, TPM vendors, and TSS software implementations
- Server solution upgrades enhance the **value for enterprises, resellers, & system integrators**

TRUSTED COMPUTING GROUP™

Data Security

- Wave's Document Manager
  - **Document and data encryption**
  - **TPM Hardware protected keys**
  - Data protected against unauthorized access, theft of PC.

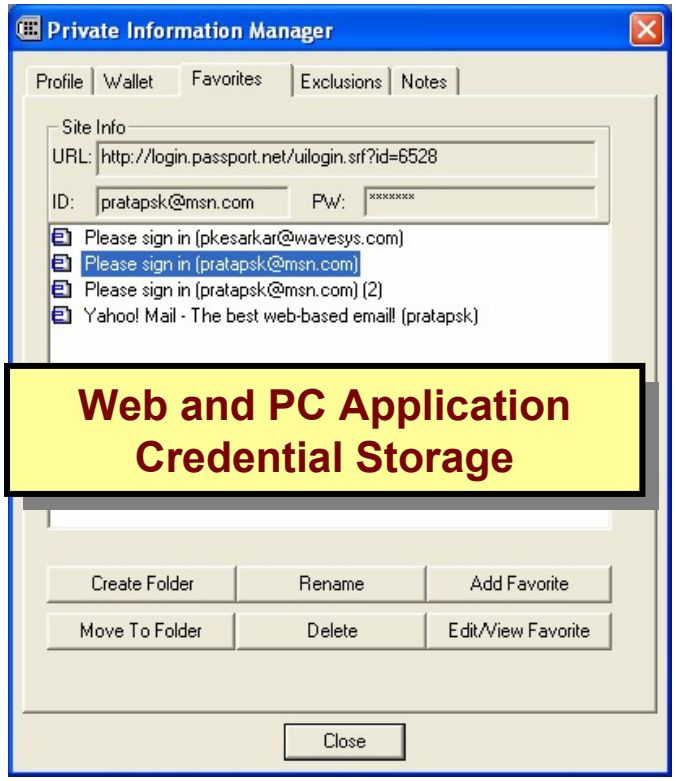




TRUSTED COMPUTING GROUP™

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

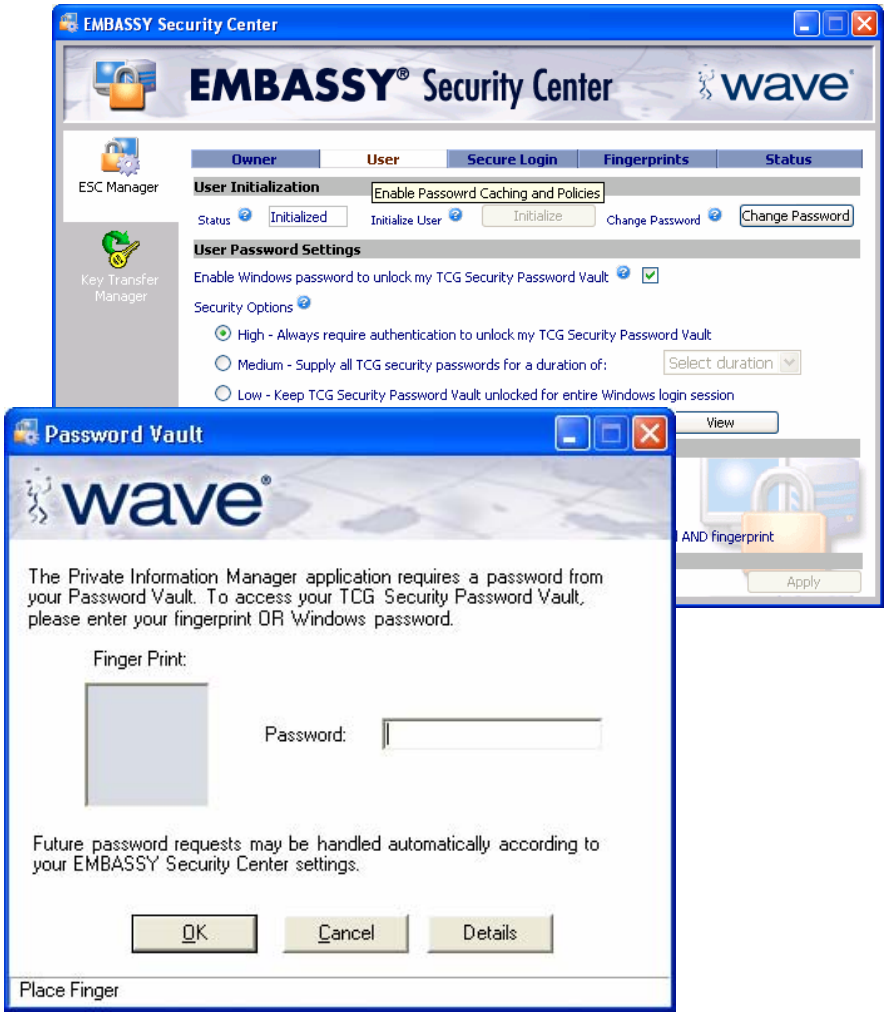


Web and PC Application Credential Storage

Prompted or Auto Login

TPM Management & Authentication

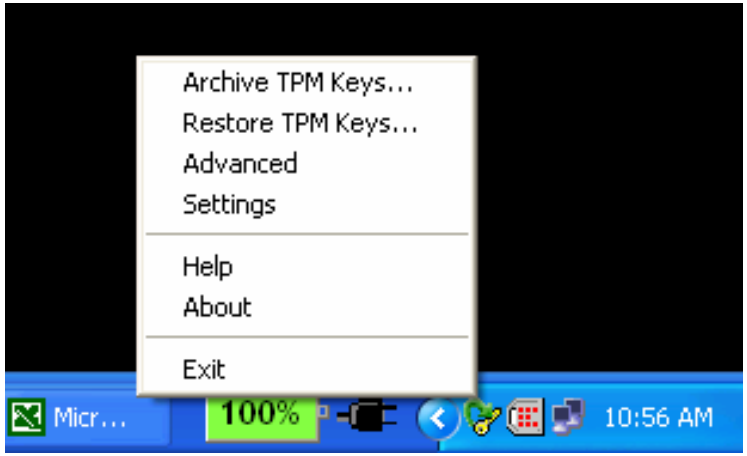
- Wave's EMBASSY Security Center
  - TPM Management
  - Multifactor Authentication with Biometric, Smart Card, TPM/PKI
    - Secure Windows Logon
    - TPM Key Authentication
  - TPM Key Password Management



TRUSTED COMPUTING GROUP™

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
  - Client and Server modes



Agenda

10:25am

Writing and Using Trusted Applications
Ralph Engers, *Utimaco Safeware AG*; George Kastrinakis, *Wave Systems*; William Whyte, *NTRU Cryptosystems, Inc.*

William Whyte is Director of Products and Services for NTRU. At NTRU, his responsibilities include oversight of all aspects of product management and technology development.

He has led the development of NTRU's highly successful Core TSS product, which has been licensed to STMicroelectronics and Atmel Corporation, and he has led consultancy projects with blue-chip customers, including Microsoft and Raytheon, to design and review secure trusted systems.

Uses of TCG Technology in Applications

William Whyte
NTRU Cryptosystems
February 14th 2005

Outline

- TSS Architecture
- Accessing TPM Functionality Through TSS
  - TPM 1.1
  - TPM 1.2
- NTRU's TSS

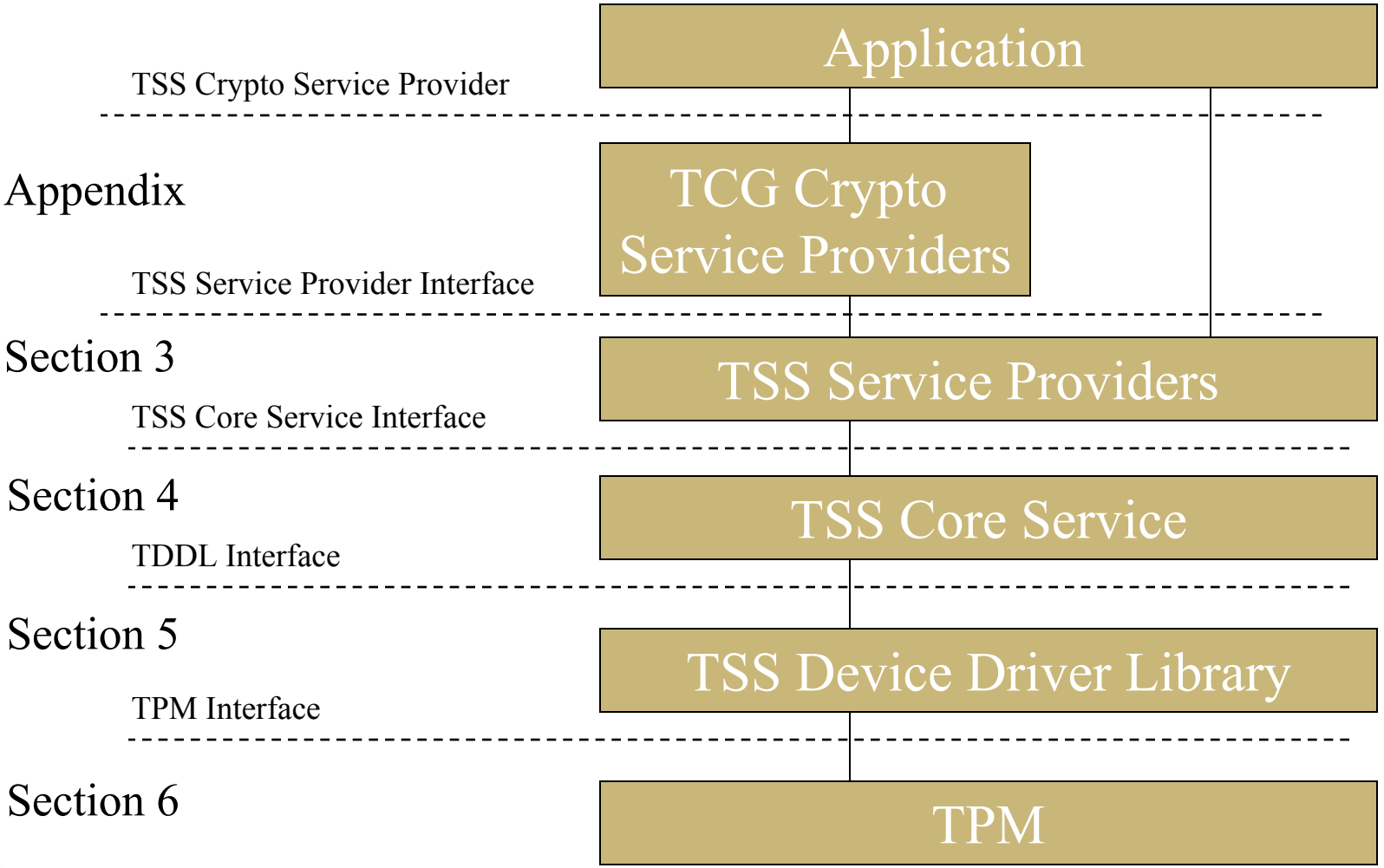
TRUSTED COMPUTING GROUP™

What is the TCG Software Stack (TSS)?

- The TSS is a software stack that exposes the functionality of the TPM and provides a common interface to access TPM functionality.
- The main goals of the TSS are:
  - Supply one entry point for applications to the TPM functionality
  - Provide synchronized access to the TPM
  - Hide building command streams with appropriate byte ordering and alignment from the applications
  - Manage TPM resources
  - Release TPM resources when appropriate

TRUSTED COMPUTING GROUP™

TSS Block Diagram



TSS Device Driver Library (TDDL)

- Creates an abstraction layer hiding OS-specific device driver interfaces from the TCS
- Single point of compatibility for TSS developers
- Allows the TPM vendor to get/set device driver capabilities

TRUSTED COMPUTING GROUP™

TSS Core Services (TCS)

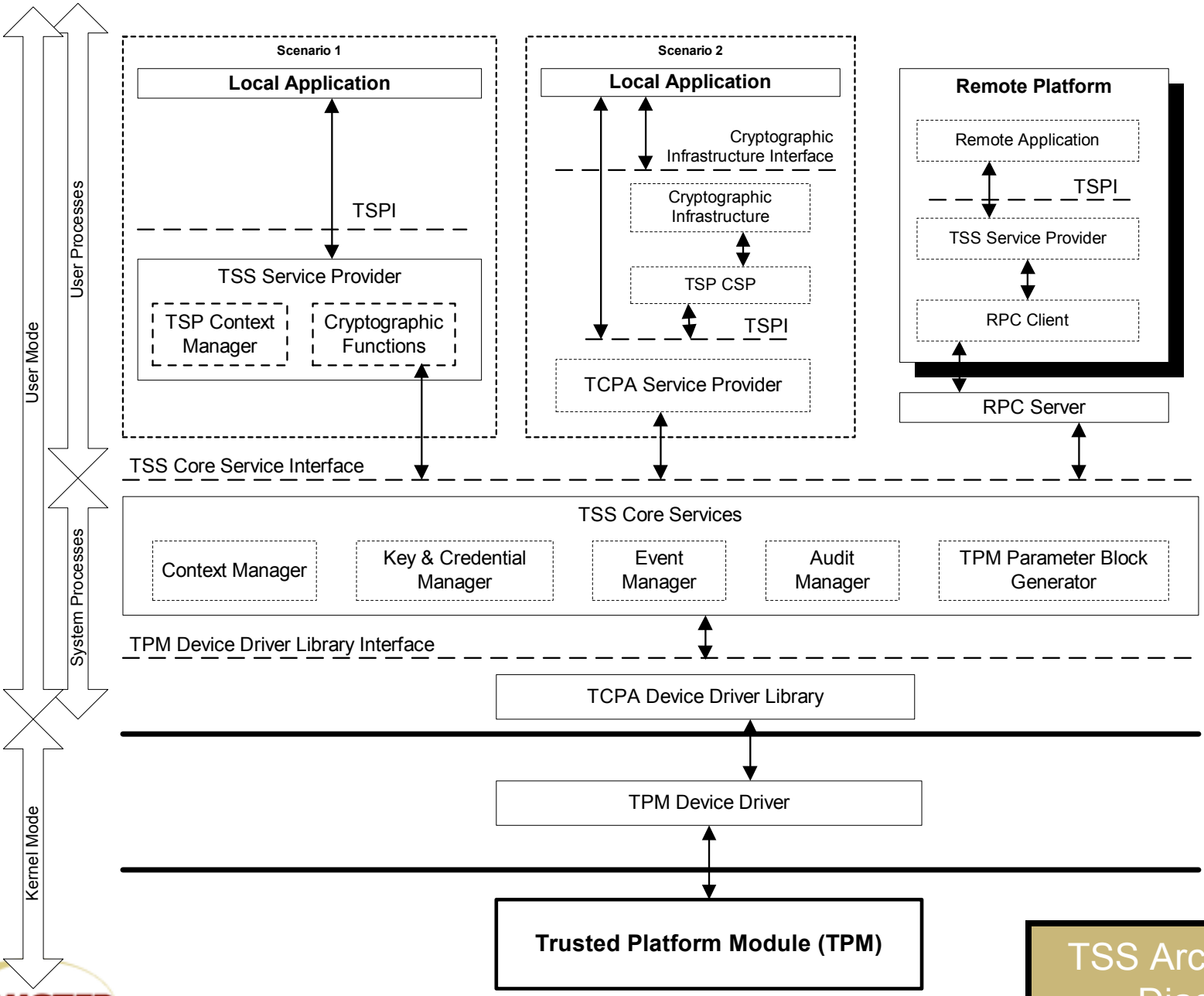
- Parameter Block Generator (PBG)
  - Converts ‘C’ style parameters into TPM format.
- Key and Credential Manager (KCM)
  - Allows the user to alias and persistently store a TPM key.
  - Dynamically swaps keys into and out of the TPM
- Context Manager
  - Allows multiple TSP modules to access TCS simultaneously
  - Performs memory management on a per context basis
- Event Manager
  - Generates, manages and exports “PCR Events”
- Audit Manager
  - This has been removed from the 1.1b specification

TRUSTED COMPUTING GROUP™

TSS Service Provider (TSP)

- Exposes TSPI
  - User Friendly API that incorporates object oriented principles
  - Abstracts the underlying protocols and data structures
- TSP Context Manager
  - Allows multiple instances of TSP layer
  - Performs memory management at the TSP Layer
- Public-key cryptography and hashing/HMAC
  - Not all cryptography requires the TPM
  - Performs public-key, hashing and HMAC algorithms to enhance cryptographic security and authorization for the TPM

TRUSTED COMPUTING GROUP™



TSS Architecture Diagram

TPM 1.1: Keys

- Endorsement key: the master key that the TPM uses to allow people to take ownership and to prove the security of identity keys.
- Key hierarchy
  - Each child key is encrypted under its parent.
    - Parents also known as “Storage keys”
    - SRK (Storage Root Key): Top of the tree
  - Keys are migratable or non-migratable
    - Non-migratable includes
      - SRK
      - The parent of any non-migratable key
  - Identity keys: non-migratable signing keys that can be certified by a CA as belonging to a TPM.
  - Other keys: bind keys for binding, signing keys for signing arbitrary data and legacy keys that can both sign and encrypt.

TRUSTED COMPUTING GROUP™

TSS and Key Management

- TSS virtualizes resource use inside the TPM
  - Multiple applications can run simultaneously, each using different keys
  - Applications do not have to manage key load/unload themselves
- To take ownership of the TPM, must write directly to the TSS
  - Currently not possible through higher-layer interfaces such as CSP

TRUSTED COMPUTING GROUP™

TSS/TPM 1.1: Functions (1)

- Sealing and unsealing (TPM_Seal)
  - Encrypting data (usually a symmetric key)
  - …using a non-migratable TPM storage key (an RSA key)
  - … so that ONLY that specific TPM can unseal the data.
  - Can be linked to sealing secret (password) and PCR state
- Binding and unbinding (TPM_Unbind)
  - Encryption for a bind key that a TPM can use (an RSA key that may or may not be migratable).
  - Not linked to a specific platform
  - Does not use a binding secret and it does not use PCRs.

TRUSTED COMPUTING GROUP™

TSS/TPM 1.1: Functions (2)

- Migration
  - The owner can select keys that the TPM will migrate keys to.
  - Migratable keys can be converted from one "parent" to another.
- Quote
  - A signature using an identity key that attests to the PCR state of the TPM.

TRUSTED COMPUTING GROUP™

TSS and TPM Functions

- Actions such as Seal are authorized using an authorization secret
  - TSS provides means to enter, cache, and expire the secret
- Architecture of TSS

TRUSTED COMPUTING GROUP™

TPM 1.2: Functions

- CMK - Certifiable migration key
  - TPM can attest they have only been inside the TPM or encrypted for a particular Migration Authority.
  - Enables key backup to other TPMs
- Transport Sessions
  - SSL-like functionality for interaction with the TPM
  - Enables remote administration without eavesdropping

TRUSTED COMPUTING GROUP™

TPM 1.2: Functions (2)

- Delegation
  - The ability to give authorization to an entity to do certain things that the owner can do or that a key can do.
  - Enables remote administration by authorized actors
  - Allows IT departments to restrict the damage end-users can do
- DAA – Direct Anonymous Attestation
  - Allow to prove that a command has come from a TPM, without specifying which TPM
    - Uses cryptographic technique known as “group signatures”
  - Partially inspired by European regulatory requirements for privacy

TRUSTED COMPUTING GROUP™

TPM 1.2: Functions (3)

- Tick Count
  - A time stamp mechanism.
- Monotonic Counter
  - A non-spoofable, non-resettable counter that can be signed.

TRUSTED COMPUTING GROUP™

TSS and TPM 1.2 Functions

- TSS virtualizes 1.2 resources
  - Tickstamps can be synchronized with system clocks

TRUSTED COMPUTING GROUP™

NTRU TSS

- Designed to interoperate with all existing TPMs
  - Testing currently on multiple TPMs
- Support for multiple operating systems
  - Windows XP/2000
  - Linux 2.4
  - Can be optimized for small size and constrained devices/OS
- Incorporates NTRU's crypto-engineering expertise and deep understanding of TPM and security practices
- Thread-safe design
- Designed for migration to TPM 1.2/NGSCB

TRUSTED COMPUTING GROUP™

Agenda

11:15am

Customer Case Studies
Stacy Cannady, *IBM*; Manny Novoa, *HP*

Stacy Cannady has been in the IT industry for 23 years. For the last six years, he has worked as product manager for electronic commerce and security products and services. His tenure at IBM has been entirely focused on information systems security. Cannady is currently a senior security consultant and product manager for client security at IBM.

TRUSTED COMPUTING GROUP™

IBM customer use cases for TPM-enabled PCs

Stacy Cannady, CISSP
Product Manager, Client Security
IBM

Basic Principle of use: Solve the “Who Are You?” Question

Answering the question “Who are you?” is one of two basic values of a TPM.

There are two derivative values from this basic value:

- Protection of digital certificates used to uniquely identify people, programs or devices
- Root of trust for protection of confidential data stored on the device

These derivative values are the basis of this discussion.

TRUSTED COMPUTING GROUP™

Using a TPM to protect credentials

The credentials are

- Digital certificates
- Password/userid pairs

The basis of protection is use of the TPM to protect keys

TRUSTED COMPUTING GROUP™

Example:
Improve Network Security with TPM-equipped PCs

Customer: Asian pharmaceutical company

Problem: Who is connecting to the customer network?

Objective: Only customer employees have the ability to connect to the company network.

Strategy:

- Bind a digital certificate to the TPM in an employee PC
- That digital certificate is required for VPN client authentication
- Use IBM Client Security Software to force multi-factor authentication of the user

Result:

- Every PC in the network is a company PC
- Every person at the keyboard of those PCs is a company employee
- No other PCs or people are able to connect

Similar story from European Insurance company, USA legal and manufacturing co.s

TRUSTED COMPUTING GROUP™

Example:
How to use a security appliance to reduce administrative costs

Customer: Small business in USA

Problem: We **HATE** passwords! We MUST have some other way!
Objective: Consolidate end user userid/password pairs into one password

Strategy:
- Use TPM private key to encrypt a database of userid/password pairs
- ID database managed by Password Manager
- Password Manager requires a password or fingerprint before it accesses the database

Result:
- End users have one password to manage for windows logon and access to Web-based applications
- Improved user satisfaction
- Reduced password reset costs

Similar story from many firms in response to integrated fingerprint readers that work with TPMs

TRUSTED COMPUTING GROUP™

Using a TPM as a Root of Trust

The idea is that sensitive operations occur outside of the view of the OS

- The TPM private key encrypts other keys used in the system
- Once a key is encrypted, it can be stored anywhere

TRUSTED COMPUTING GROUP™

HIPPA Compliance

Customer: USA Hospital

Problem: Patient health information is kept on PCs, including laptops.
Objective: All patient information must be encrypted. Only authorized persons can access it.

Strategy:
- Encrypt My Documents. All data that goes into it is encrypted automatically. All data the comes out is unencrypted automatically
- Any request to unencrypt data must be authenticated first

Mechanism:
- Use TPM-enabled PCs for any PC that will contain patient information
- Use the TPM to encrypt all data-encryption keys
- Use TPM-aware authentication software to force authentication before data is unencrytped

Banks have copied this model for Graham-Leech-Bliley compliance

TRUSTED COMPUTING GROUP™

Confidential data on laptops

Customer: European Pharmaceutical firm

Problem: Must encrypt confidential data on laptop. Data is very sensitive – file encryption not good enough.

Strategy:

- Use TPM-aware full hard drive encryption software to encrypt all data all the time
- Use TPM enabled systems and bind the drive to the system using the encryption software
  - Benefit: drive won't unencrypt unless it is in the system it is bound to and the user authenticates
  - Benefit: at end of life, just separate drive from system, save cost of cleaning
  - Problem: PC must go to hibernate or be shut off when in transit

TRUSTED COMPUTING GROUP™

Questions?

Agenda

11:15am Customer Case Studies
Stacy Cannady, *IBM*; Manny Novoa, *HP*

Manny Novoa is a principal member of technical staff at Hewlett-Packard. Novoa is currently working on client security technologies within HP's Personal Systems Group Advanced Technology team. He is the lead architect for HP's Fingerprint Identification Technology (FIT) product and client-focused Trusted Computing efforts.

TRUSTED COMPUTING GROUP™

Manny Novoa
Hewlett-Packard

TCG Luncheon

- **The TCG hosted lunch will be held in Esplanade Room #301 from 12:00 p.m. – 1:00 p.m.**
- **Guest Speaker Rob Enderle, the Enderle Group, will address the attendees during the lunch session**

TRUSTED COMPUTING GROUP™

TCG Booth & Passport Program

- **The TCG will be showcasing a number of available member platforms running trusted applications in booth #332.**

- **Visit any five (5) of the Trusted Computing Group member companies participating in the TCG Passport Program and receive a free gift in the TCG Booth #332.**

TRUSTED COMPUTING GROUP™

Questions and Answers