Trusted Computing Group

Making Computing Safer and More Secure Through Industry Standards
Environment: Security Costs Growing Exponentially

- $7B Estimate for Overt Digital Attacks Worldwide for 2002
  - Mi2g intelligence 10/22/02

Source: 2003 CSI/FBI Survey
Theft, Malware Raging

“…Carnegie Mellon University notified 19,000 students, staff and alumni that their personal information may have been compromised by a computer security breach.”

“Identity theft cost consumers and their banks and credit-card companies about $11.7 billion in losses for the 12 months through April 2004, estimates Gartner.”

“(A) thief recently walked into a University of California, Berkeley office and swiped a computer laptop containing personal information about nearly 100,000 alumni, graduate students and past applicants, highlighting a continued lack of security…”

“…58% of the breaches recorded by California officials have occurred after a computer or other device containing personal information is lost or stolen…”
Challenge: Enterprise Unprotected
Software Alone Not Working

Server
- Highly regulated SW/HW configuration
- Controlled physical access (24x7)
- Intrusion detection SW
- Firewalls
- Anti-virus
- Network segmentation
- Encrypted data
- Real-time monitoring
- Auditing & analysis
- Multi-factor user auth.
- Configuration monitors
- Patch, Configuration, & Policy Control

Network
- Encryption (IPSec, SSL)
- VPN
- Layered firewalls
- Intrusion detection SW
- 24x7 monitoring
- Network segmentation
- 802.1x (Radius)
- Multi-factor authentication
- Domain controllers
- Policy management
- Configuration monitors
- Network access control

Client
- Passwords
- Anti-virus
- User authentication
- Patch, Configuration, & Policy Control

Mismatch between security measures and the financial value of data created & stored on clients
TCG Mission

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

Standards = Adoption
Define Trusted Computing

• Summary of benefits
• Protect against viruses, spam, phishing
• Protect data and identities
• Protect against physical theft
• Etc.
The Opportunity of Trusted Computing

• Standards-based with industry support to:
  – Enable a safer computing environment
  – Protect end-user data
  – Enable trusted e-commerce transactions
  – *Hardware-rooted trust*

• Benefits of more trust
  – Increase user and administrator confidence in Internet use
  – Reduce business risk, specially for security-conscious verticals
    • Financial Services, insurance, government, healthcare
  – Increase in transaction volume and value with *hardware protection*

• Extend trust to other platforms – everything is connected
  – Laptops, desktops, PDA, servers, mobile phones, network gear, etc.
The Trusted Computing Solution

• Turn the entire platform into a trusted environment
  – Dynamic platform communication with the network
  – Protection of data
  – Remote communication
• 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
• The TPM is: A building block for enabling “Trust” in a product.
  – TPM’s are semiconductors known as “modules”
  – Integrated capabilities in other semiconductors:
    • Current examples: Broadcom Gigabit Controller and Winbond Super IO
    • Future TPM capabilities in network products, cellular phones, graphics controllers, processors…
Trusted Computing Enables

• Solutions
  – Examples:
    • PC’s with TPM Modules
    • Software from third parties that use the TPM modules
      – Data Protection
      – Network Access
      – Identity Management
      – Authentication
    • Network Products
      – Radius Server, Virus Protection, Policy Management
    • Disk Drive
      – Full-disk Encryption
    • Servers
  – Future Products
    • Mobile Phones
    • Input Devices
    • Displays
    • OS Implementations

• Why do I need this?
  • Software only solutions are not enough
  • Hardware security is proven to be secure
  • Hardware security is authentic and available
Trusted Computing: The “BIG” Picture

TCG Standards

Applications

Credentials

Operating Systems

Web Services

Security Infrastructure

Mobile Phones

PDAs

Authentication Devices

Input Devices

Security Hardware

Desktops

Notebooks

Servers

Storage

Copyright© 2005 Trusted Computing Group - Other names and brands are properties of their respective owners.
Protecting the Enterprise: Trusted Systems Reach Critical Mass

Platforms – top 5 vendors with TPMs
- Dell
- IBM
- HP
- Toshiba
- Fujitsu
- Toshiba
- Sony

Recent announcements from Gateway, NEC, Acer and others

Applications –
- Utimaco, Wave, NTRU, others, ex.:
- Bulk encryption
- Password management
- Single sign-on
- Open source SW stack available
TPM Module Forecast

(In millions of units shipped)

Source: IDC
5 Major Solutions Being Addressed

• Machine Authentication
• User Authentication
• User Authorization
• User Administration
• Auditing and Reporting
Example: Network Authentication

Cert Server: Provides TPM-based certificates for strong authentication for VPN, Domain, or Wireless.


Computer Authentication Using TPM.

Network

Client

Any TPM-Enabled PC

TPM Certificate

Smart Card Reader

Fingerprint Reader

VPN

User Authentication Using Password, Biometrics, Smart Card, and/or TPM.

VPN Strong Authentication - TPM as token - Using Password, Biometrics, Smart Card.

Multi-factor authentication to network with TPM security.

Any TPM-Enabled Laptop

TPM Certificate for VPN Authentication

Fingerprint Reader

Smart Card Reader

Client

Network
can we format slides 27 and 28 so consistent with 29 and other examples/
, 8/30/2005
Example: Data Protection and Key Management

- **Network File Server**
- **Server: MS2003 Server with Active Directory, SQL Server**
- **Network**
- **Client**
- **Shared Secure Virtual Drives**
- **TPM Key and Certificate Archive (Ensures recovery of encrypted data)**
- **Any TPM-Enabled PC**
- **Encryption Products**
  - Provides TPM-secured Virtual Drives
- **Multi-factor authentication to Secure Virtual Drives**
- **Client application to archive and restore keys**
- **Fingerprint Reader**
- **Smart Card Reader**
- **Authentication To Secure Drives**
- **Local Secure Virtual Drive**
- **Ensures management, archive, recovery of TPM-enabled platforms**
Trusted Network Connect: Protecting the Network Through Access Control and Endpoint Integrity
Trusted Network Connect Working Group

• Goal: To develop & promote an open solution architecture that enables network operators to establish, extend, and enforce policies regarding client/endpoint integrity when granting the systems access to a trusted network infrastructure.

• Active working group within TCG with participation open to all TCG Contributor members. More than 60 current TNC members include:
  – Security Vendors (especially Client Security and Endpoint Integrity)
  – Network Infrastructure Vendors (Switches, Routers, VPNs, etc.)
  – Endpoint, Configuration/System Mgmt, Hardware and OS Vendors
Infrastructure Building Blocks

- Network Authentication
- Users, Platforms
- Network Access Control
- Remote Management
- Setup
- Issues Management
- Data Migration and Synchronization
- Between Trusted Devices
- Key Management
- Backup, Disaster Recovery
- Device Replacement
- Integrity Measurement
- Devices, Apps, People
- State of Platforms
- Security Policies
- IT Management and Control
- Asset Management and Tracking
- Deployment, Operation
- Retirement, Lost/Stolen Devices
- Issues Management
Key Computing Trends Drive the Need for TNC

**Trend**
- Increasing network span to mobile workers, customers, partners, suppliers
- Network clients moving to wireless access
- Malware increasingly targeting network via valid client infection
- New malware threats emerging at an increasing beat rate

**Implication**
- Less reliance on physical access identity verification (i.e., guards & badges)
- Remote access sequences easily monitored, cloned
- Clients ‘innocently’ infect entire networks
- Client scanning demands move from once/week to once/login

---

**Identity/Trust Challenges**

**Client Integrity Challenges**
TNC Solution Creates a “Virtual Airlock” for Network Access & Protection
Securing Mobile Devices
Why TCG works on mobile security

• Mobile phones are increasingly more sophisticated and capable of basic computing tasks.
• Mobile data services are increasingly popular and varied.
• Internet and mobile domains converge.

➤ This requires ...

... more trust in the device, service, content and network
... a common trust approach for classical and mobile internet
Mobile Phone WG Scope

• The group will work on the adoption of TCG concept for mobile devices to enable different business models in market environment of open terminal platform.

• The group will enhance concepts of Trusted Computing as needed to address specific features of mobile devices like their connectivity and limited capability.
Deliverables

• **Usage scenarios:**
  • Consolidated collection of usage scenarios that are describing the usage of mobile devices in trusted environment, concentrated on exploring added value for mobile devices.

• **Requirements:**
  • List of high-level requirements (functional and non-functional) related to the adoption of trusted computing platform for mobile devices.

• **Mobile specific specifications:**
  • Proposal of extensions and modifications required for TCG main specification to be adopted for mobile devices.
Possible usage scenarios

- Prove platform and/or application integrity to end user
- Access Control
- Purchase and redeem tickets
- Identity cloning
- Platform Integrity
- Platform Authentication – service provider
- Radio SW integrity
- SIM/USIM
- SW Use
- Device locking
- Content download
- SW Updates
- SW Download
**TCG Membership**

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

**Contributors**
- Agere Systems
- American Megatrends, Inc.
- ARM
- ATI Technologies Inc.
- Atmel
- AuthenTec, Inc.
- AVAYA
- Broadcom Corporation
- Certicom Corp.
- Citrix Systems, Inc.
- Comodo
- Dell, Inc.
- Endforce, Inc.
- Ericsson Mobile Platforms AB
- Extreme Networks
- France Telecom Group
- Freescale Semiconductor
- Fujitsu Limited

**Contributors**
- Fujitsu Siemens Computers
- Funk Software, Inc.
- Gemplus
- General Dynamics C4 Systems
- Giesecke & Devrient
- Hitachi, Ltd.
- Infineon
- InfoExpress, Inc.
- InterDigital Communications
- iPass
- Lenovo Holdings Limited
- Lexmark International
- M-Systems Flash Disk Pioneers
- Meetinghouse Data
- Communications
- Mirage Networks
- Motorola Inc.
- National Semiconductor
- nCipher
- NEC
- Network Associates
- Nevis Networks, USA
- Nokia
- NTRU Cryptosystems, Inc.
- NVIDIA
- OSA Technologies, Inc.
- Philips
- Phoenix
- Pointsec Mobile Technologies

**Contributors**
- Renesas Technology Corp.
- Ricoh Company LTD
- RSA Security, Inc.
- SafeNet, Inc.
- Samsung Electronics Co.
- SCM Microsystems, Inc.
- Seagate Technology
- SignaCert, Inc.
- Sinosun Technology Co., Ltd.
- SMSC
- STMicroelectronics
- Sygate Technologies, Inc.
- Symantec
- Symbian Ltd
- Synaptics Inc.
- Texas Instruments
- Trend Micro
- TriCipher, Inc.
- UPEK, Inc.
- Utimaco Safeware AG
- VeriSign, Inc.
- Vernier Networks
- Vodafone Group Services LTD
- Wave Systems
- Winbond Electronics
- Corporation
- Zone Labs, Inc.

**Adopters**
- Advanced Network Technology Labs
- Apani Networks
- Apere, Inc.
- BigFix, Inc.
- Bradford Networks
- Caymas Systems
- Ciron
- CPR Tools, Inc.
- Credant Technologies
- Fiberlink Communications
- Foundry Networks Inc.
- Foundstone, Inc.
- Industrial Technology Research Institute
- Infosec Corporation
- Lockdown Networks
- Marvell Semiconductor, Inc.
- MCI
- PC Guardian Technologies
- Safend
- Sana Security
- Senforce Technologies, Inc.
- Silicon Integrated Systems Corp.
- Silicon Storage Technology, Inc.
- Softex, Inc.
- StillSecure
- Swan Island Networks, Inc.
- Telemidic Co. Ltd.
- Toshiba Corporation
- ULI Electronics Inc.
- Unisys
- Websense

110 Total Members as of August 18, 2005
7 Promoter, 71 Contributor, 32 Adopter