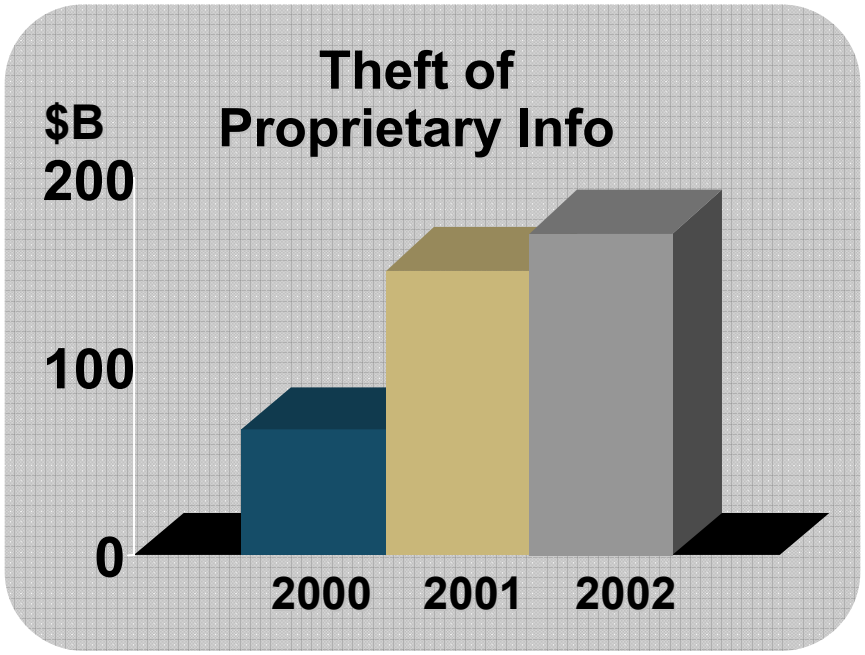
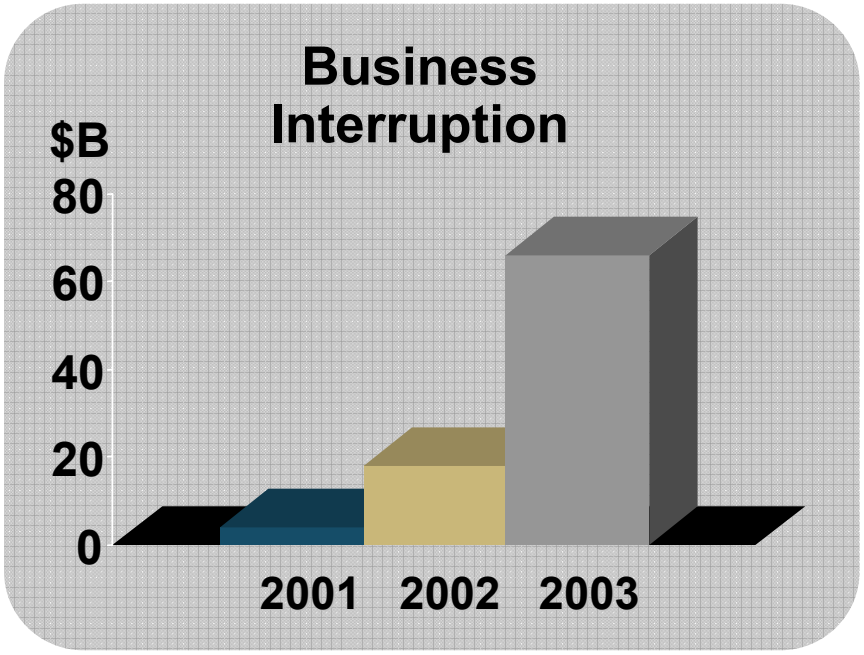
Trusted Computing Group

Making Computing Safer and More Secure Through Industry Standards

Environment: Security Costs Growing Exponentially





Source: 2003 CSI/FBI Survey

- $7B Estimate for Overt Digital Attacks Worldwide for 2002

  - Mi2g intelligence 10/22/02

TRUSTED COMPUTING GROUP™

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."

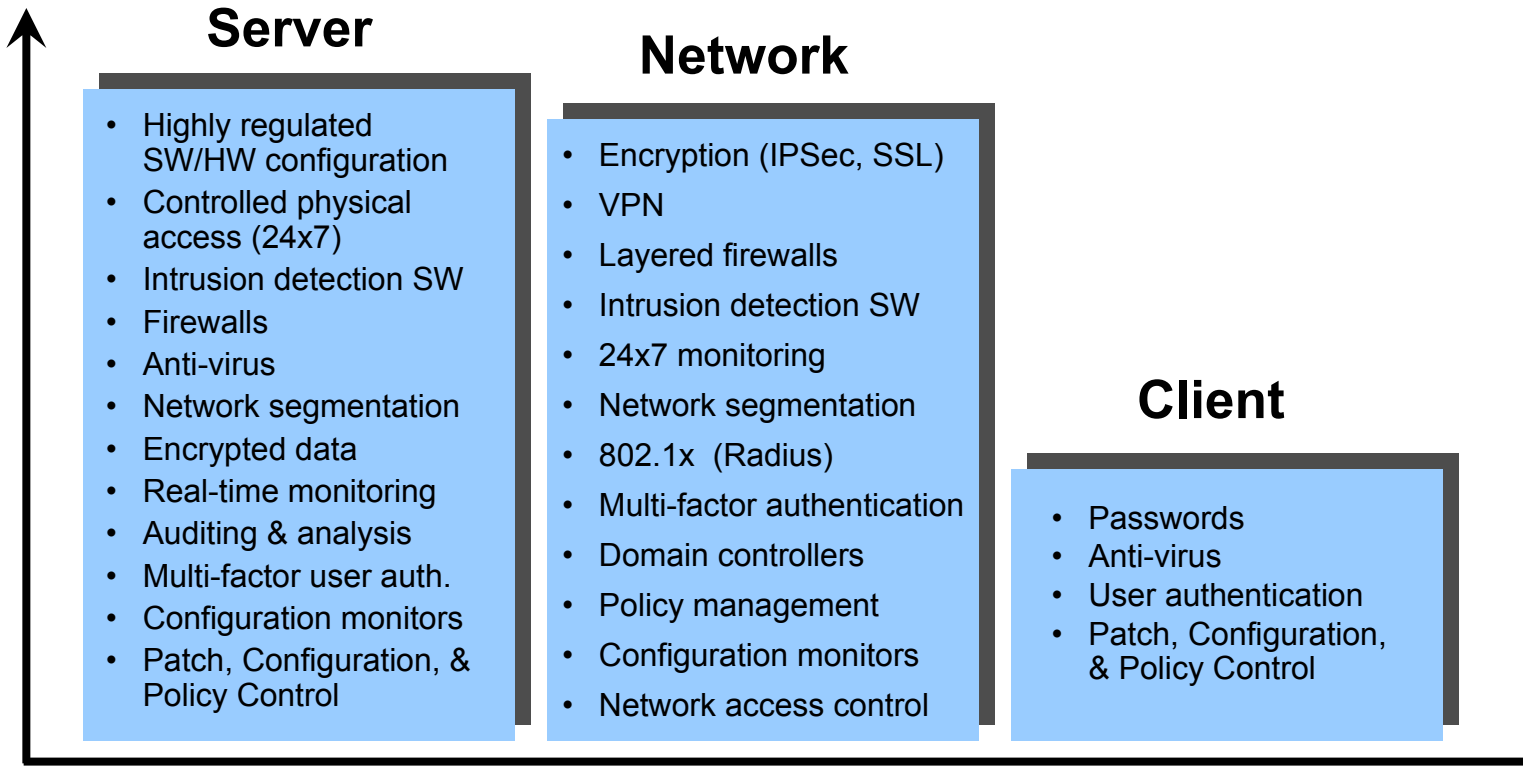
"Identity theft cost consumers and their banks and credit-card companies about $11.7 billion in losses for the 12 months through April 2004, estimates Gartner "

"…(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…"

TRUSTED COMPUTING GROUP™

Challenge: Enterprise Unprotected
Software Alone Not Working



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

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™

Define Trusted Computing

- Summary of benefits
- Protect against viruses, spam, phishing
- Protect data and identities
- Protect against physical theft
- Etc.

TRUSTED COMPUTING GROUP™

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.

TRUSTED COMPUTING GROUP™

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…

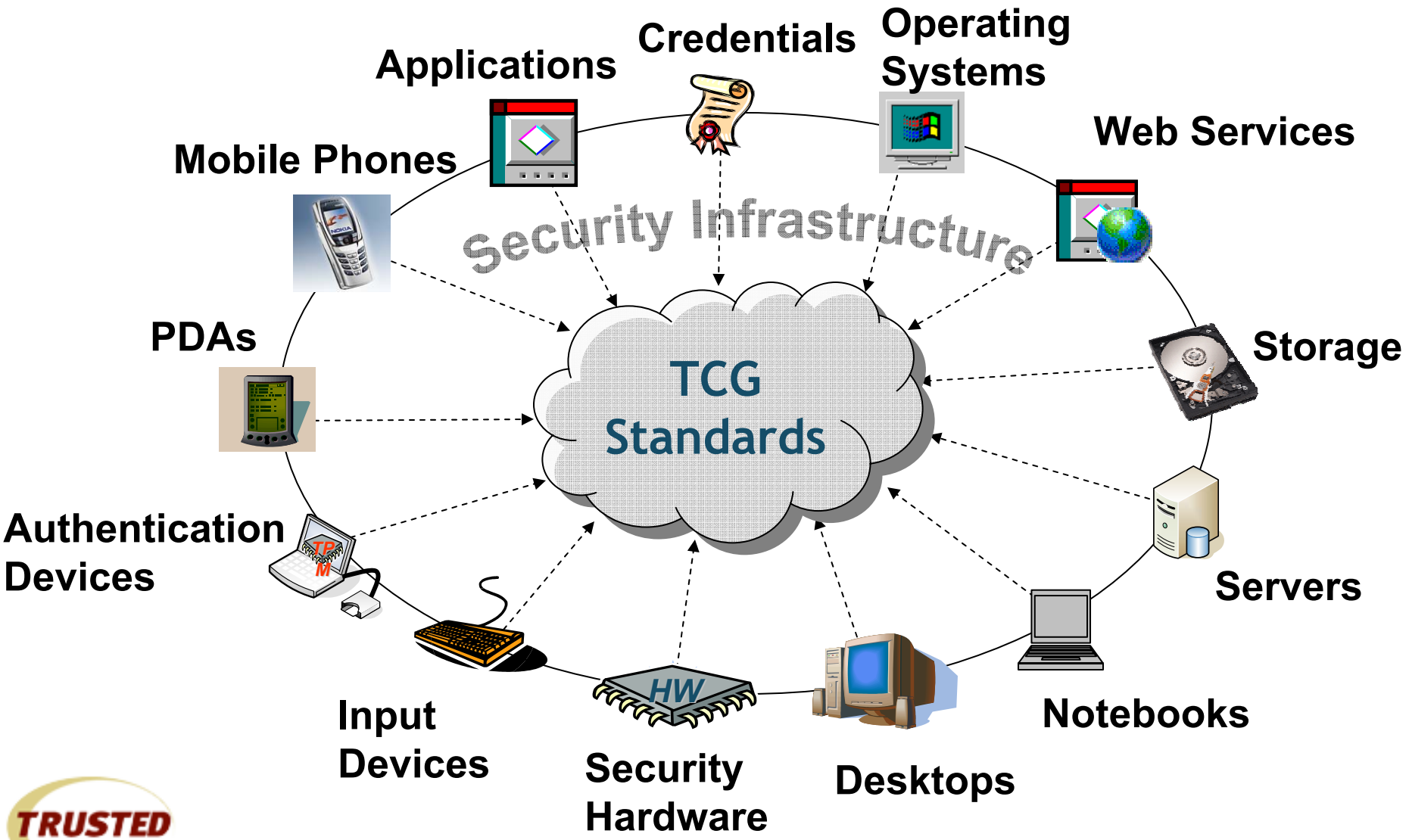
TRUSTED COMPUTING GROUP™

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

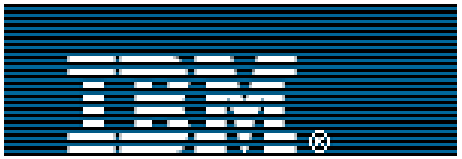
TRUSTED COMPUTING GROUP™

Trusted Computing: The "BIG" Picture



TRUSTED COMPUTING GROUP™

TCG Board of Directors



TRUSTED COMPUTING GROUP™

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

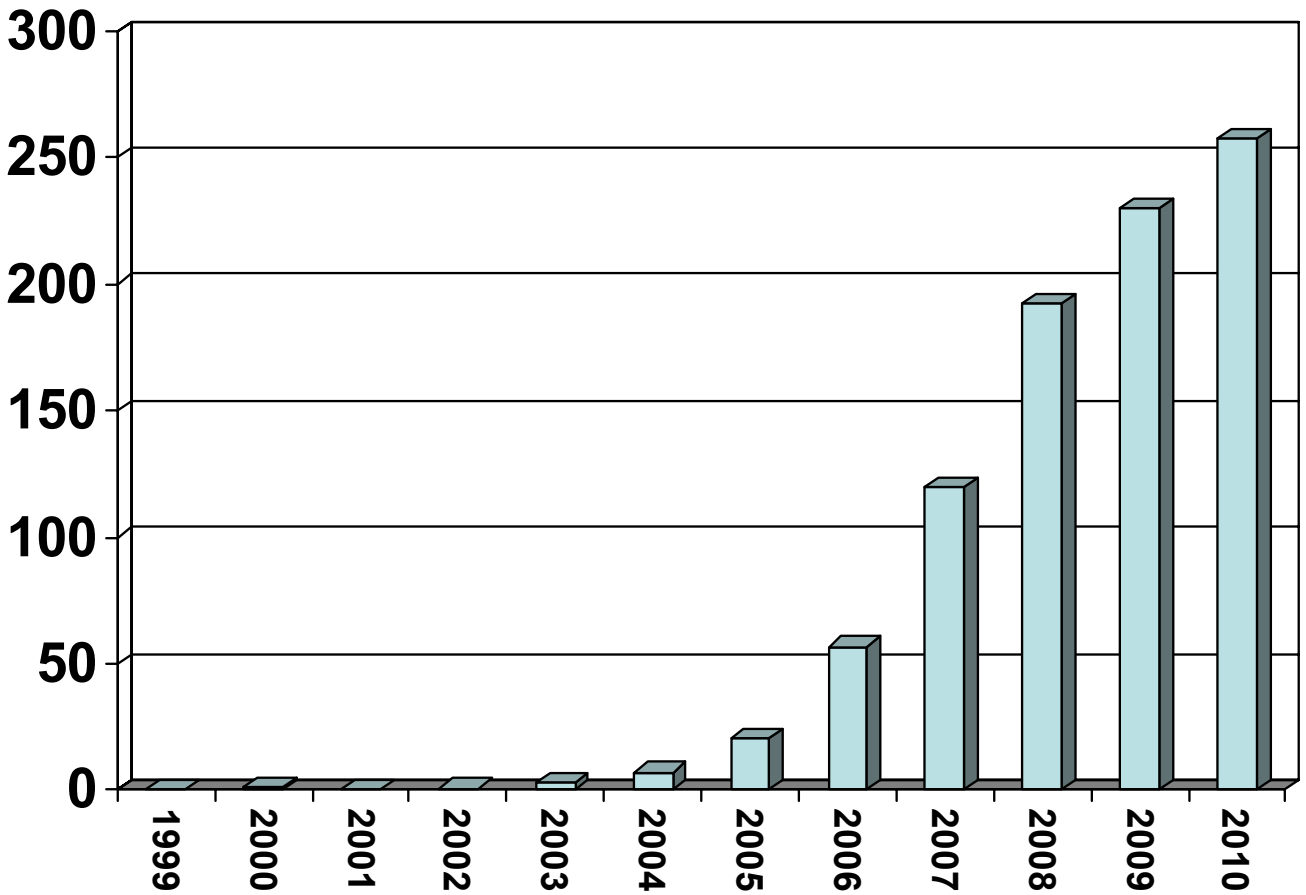
Applications – Utimaco, Wave, NTRU, others, ex.:

- Bulk encryption
- Password management
- Single sign-on
- Open source SW stack available

TRUSTED COMPUTING GROUP™

TPM Module Forecast

(In millions of units shipped)



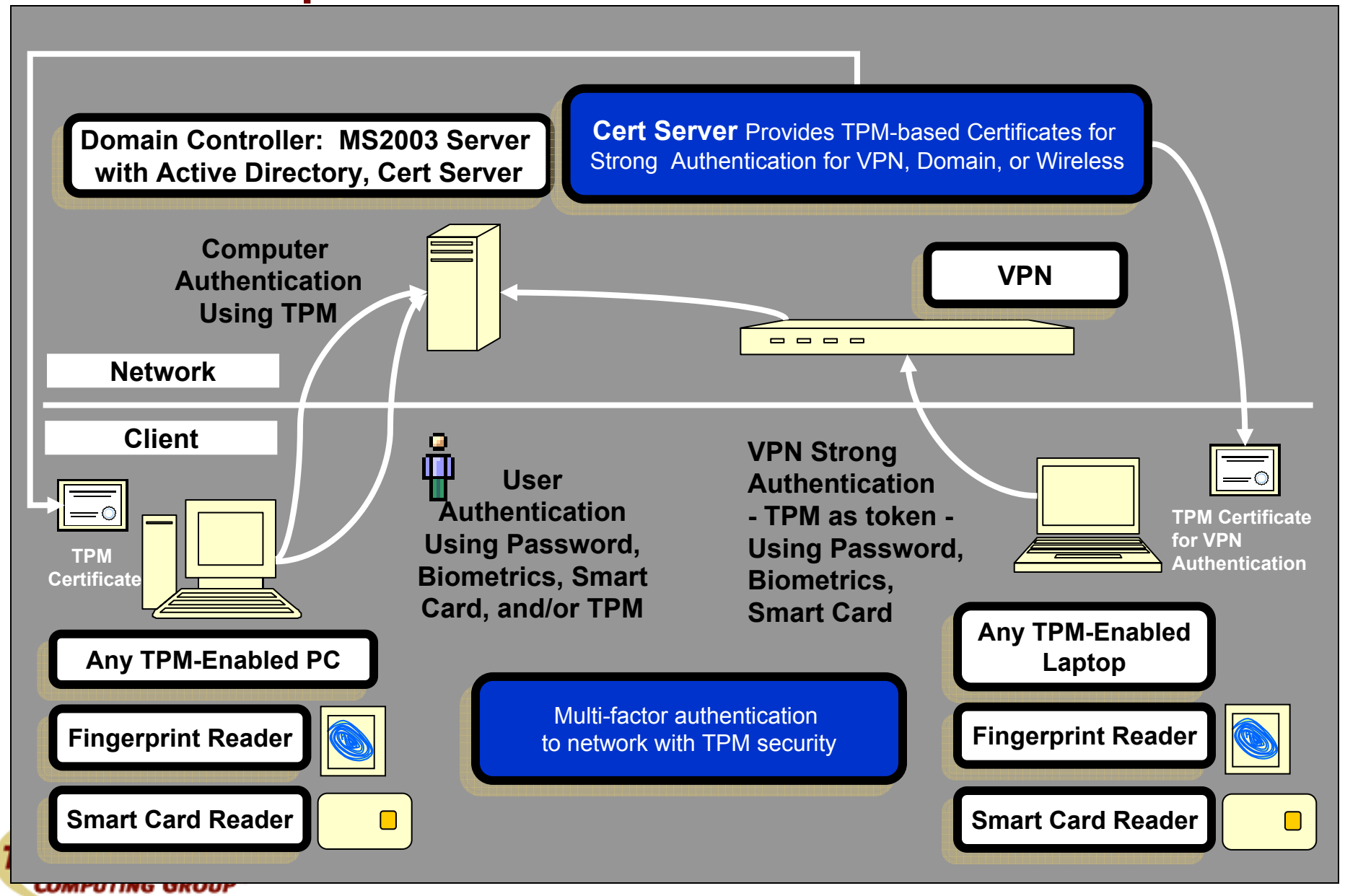
Source: IDC

5 Major Solutions Being Addressed

- Machine Authentication
- User Authentication
- User Authorization
- User Administration
- Auditing and Reporting

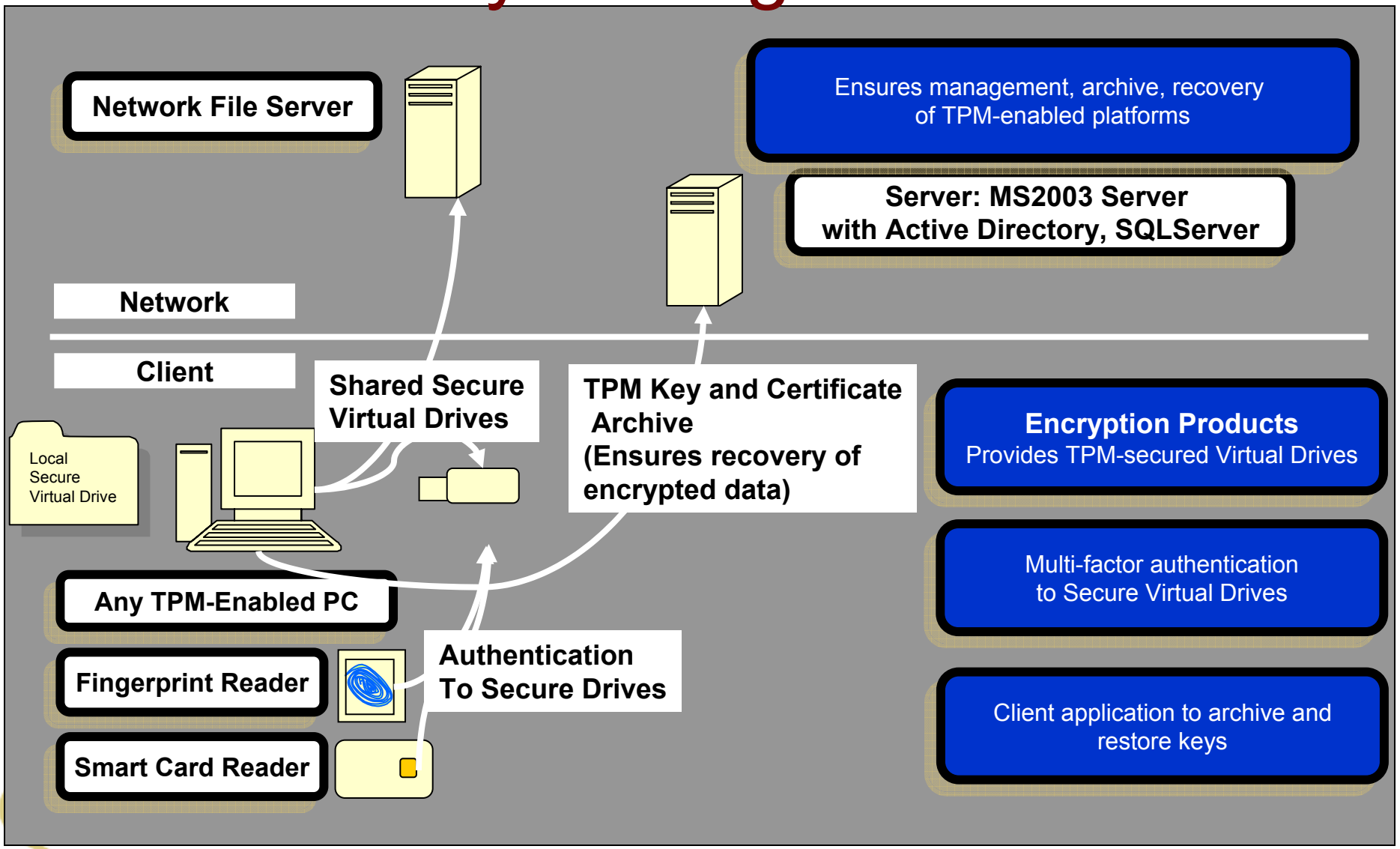
TRUSTED COMPUTING GROUP™

Example: Network Authentication



12 can we format slides 27 and 28 so consistent with 29 and other examples/
, 8/30/2005

Example: Data Protection and Key Management



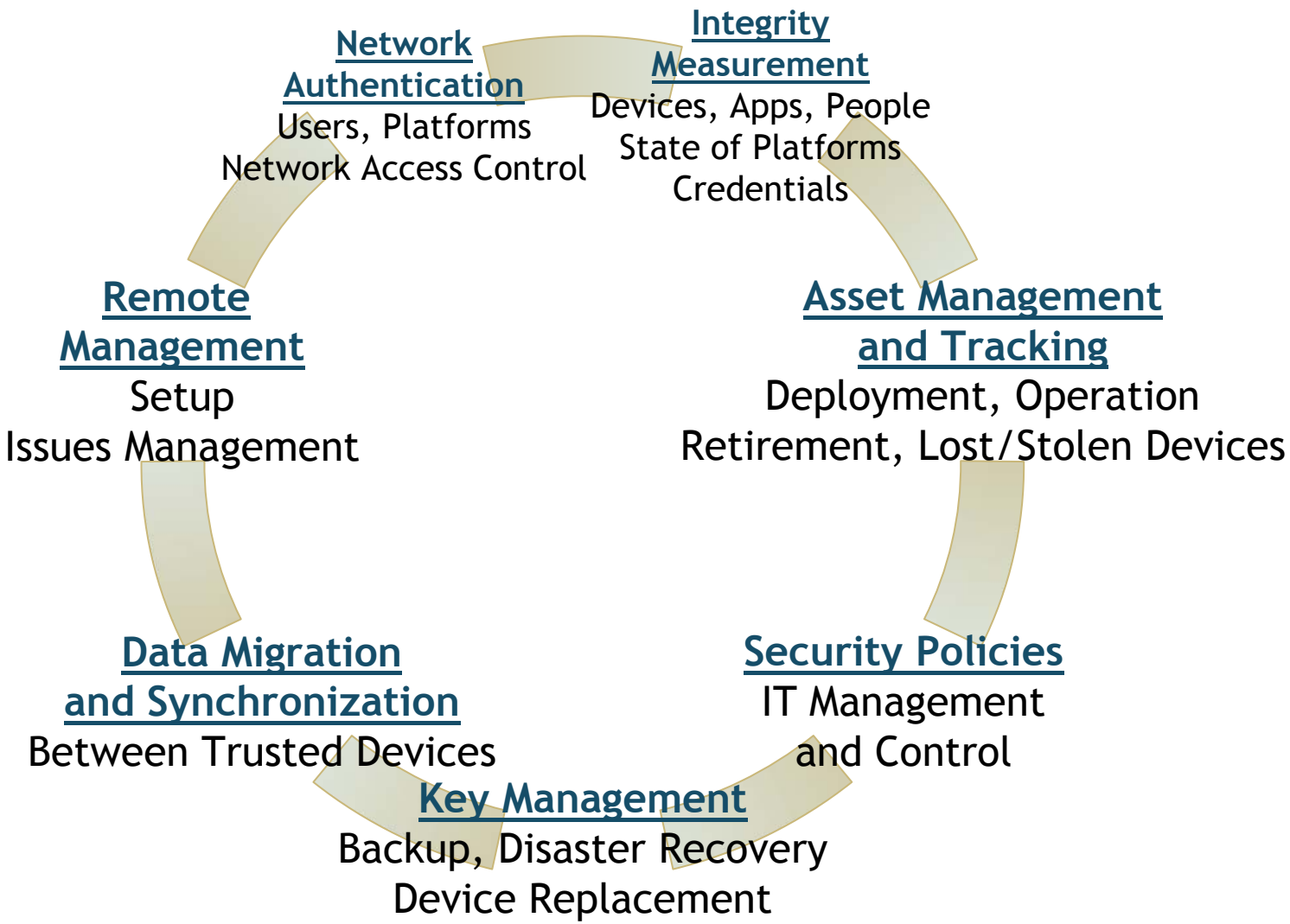
Trusted Network Connect: Protecting the Network Through Access Control and Endpoint Integrity

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

TRUSTED COMPUTING GROUP™

Infrastructure Building Blocks



TRUSTED COMPUTING GROUP™

Key Computing Trends Drive the Need for TNC

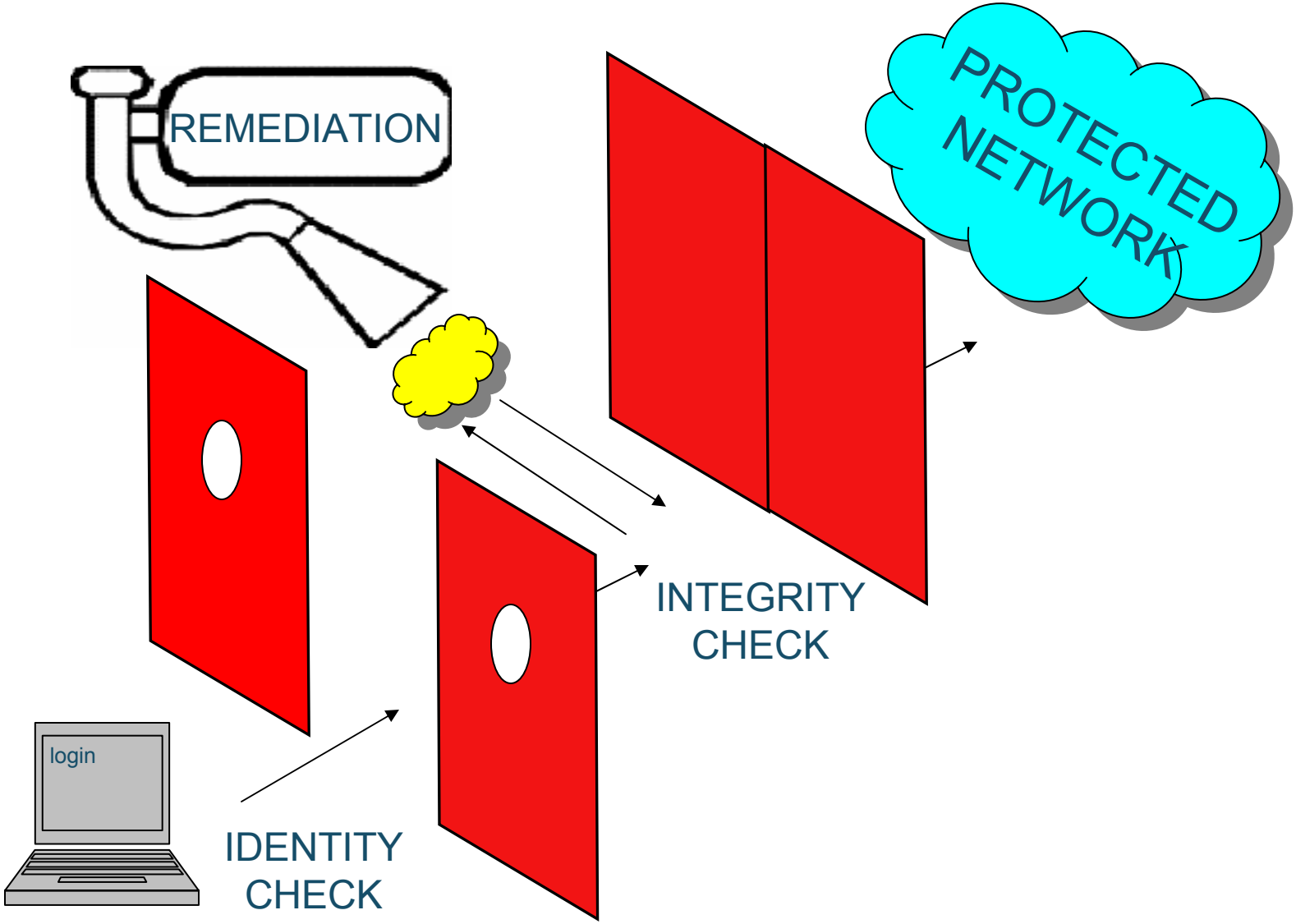
TREND	IMPLICATION
• Increasing network span to mobile workers, customers, partners, suppliers	• Less reliance on physical access identity verification (i.e. guards & badges)
• Network clients moving to wireless access	• Remote access sequences easily monitored, cloned
• Malware increasingly targeting network via valid client infection	• Clients 'innocently" infect entire networks
• New malware threats emerging at an increasing beat rate	• Client scanning demands move from once/week to once/login

IDENTITY/TRUST CHALLENGES

CLIENT INTEGRITY CHALLENGES

TRUSTED COMPUTING GROUP™

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



TRUSTED COMPUTING GROUP™

TRUSTED COMPUTING GROUP™

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

TRUSTED COMPUTING GROUP™

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

TRUSTED COMPUTING GROUP™

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.

TRUSTED COMPUTING GROUP™

Possible usage scenarios

Prove platform and/or application integrity to end user

Access Control

Purchase and redeem tickets

Identity cloning

Radio SW integrity

Platform Integrity

Platform Authentication – service provider

SIM/USIM

SW Use

Device locking

Content download

SW Updates

SW Download

TRUSTED COMPUTING GROUP™

TCG Organization

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

Marketing Workgroup
Brian Berger, Wave Systems

- **Public Relations**
  Anne Price, *PR Works*
- **Events Marketing Support**
  VTM, Inc.

Technical Committee
Graeme Proudler, *HP*

- **TPM Work Group**
  David Grawrock, *Intel*
- **TSS Work Group**
  David Challener, *Lenovo*
- **Mobile Phone WG**
  Janne Uusilehto, *Nokia*
- **Peripherals WG**
  Colin Walters, *Comodo*
- **Server Specific WG**
  Larry McMahan, *HP*
  Marty Nicholes, *HP*
- **Conformance WG**
  Randy Mummert, Atmel
- **PC Client WG**
  Monty Wiseman, *Intel*
- **Infrastructure WG**
  Thomas Hardjono, VeriSign
  Ned Smith, Intel
- **Storage Systems**
  Robert Thibadeau, *Seagate*
- **Hard Copy WG**
  Brian Volkoff, *HP*

Advisory Council
Invited Participants

Administration
VTM, Inc.

Position Key

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

TRUSTED COMPUTING GROUP™

TCG Membership

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

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
Cirond
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

TRUSTED COMPUTING GROUP™