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

Thursday, May 26, 2005
8:30 am – 11:30 am
Booth #1743
# Agenda

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
<th>speaker(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 am</td>
<td>Introduction</td>
<td>Brian Berger, <em>Wave Systems</em></td>
</tr>
<tr>
<td>8:35 am</td>
<td>Keynote Speaker</td>
<td>Roger Kay, <em>IDC</em></td>
</tr>
<tr>
<td>9:05 am</td>
<td>TCG Architecture</td>
<td>Monty Wiseman, <em>Intel</em></td>
</tr>
<tr>
<td>9:25 am</td>
<td>Open Source Solutions</td>
<td>Dr. David Safford, <em>IBM</em></td>
</tr>
<tr>
<td>9:45 am</td>
<td>Writing and Using Trusted Applications</td>
<td>Alexander Koehler, <em>Utimaco Safeware AG</em>; Steven Sprague, <em>Wave Systems</em></td>
</tr>
<tr>
<td>10:30 am</td>
<td>Trusted Storage and Applications</td>
<td>Michael Willett, <em>Seagate Technology, Inc.</em></td>
</tr>
<tr>
<td>10:50 am</td>
<td>Trusted Network Connect Overview</td>
<td>Jon Brody, <em>Sygate Technologies</em></td>
</tr>
<tr>
<td>11:15 am</td>
<td>Q&amp;A</td>
<td></td>
</tr>
</tbody>
</table>
TCG Mission

Develop & promote open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms.
Trusted Computing: The “BIG” Picture

TCG Standards

Applications

Credentials

Operating Systems

Web Services

Mobile Phones

PDAs

Authentication Devices

Input Devices

Security Hardware

Desktops

Notebooks

Servers

Storage

Security Infrastructure
TCG Membership Momentum

- 103 Member company’s as of May, 2005
- BOD – AMD, HP, IBM, Intel, Microsoft, Seagate, Sony, Sun, Verisign
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.
The Future of Trusted Computing

Roger L. Kay
Vice President
Client Computing
Agenda

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

(In millions of units shipped)

Source: IDC
TPM Attach: Desktops

(In millions of units shipped)

Source: IDC
Network Security: A Perimeter Problem

- Maginot Line
- Security is only as strong as the weakest link
- The client has been neglected in the past
- Mobility is a special case
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
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.
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
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
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
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?
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?
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
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
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
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
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
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.*
Open Source Solutions

Dave Safford, IBM Research
Outline

• Threat Trends
• Trusted Computing
• Open Source Projects
• What's Missing
• The Future
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
**July 2004 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)
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
## Programming view of the TPM

<table>
<thead>
<tr>
<th>Functional Units</th>
<th>Non-volatile memory</th>
<th>Volatile memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>RNG</td>
<td>Endorsement Key (2048b)</td>
<td>RSA Key Slot-0</td>
</tr>
<tr>
<td>Hash</td>
<td>Storage Root Key (2048b)</td>
<td>. . .</td>
</tr>
<tr>
<td>HMAC</td>
<td>Owner Auth Secret (160b)</td>
<td>RSA Key Slot-9</td>
</tr>
<tr>
<td>RSA Key Generation</td>
<td></td>
<td>. . .</td>
</tr>
<tr>
<td>RSA Encrypt/Decrypt</td>
<td></td>
<td>PCR-0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>. . .</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PCR-15</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Key Handles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Auth Session Handles</td>
</tr>
</tbody>
</table>
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/
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
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 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:

- Measured kernel, initrd, sealed K, TPM Authentication
- TPM
- EVM
- SLIM
- Normal checks
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
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
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
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.
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
Risks in IT - Types of Attacks and Misuse

- Laptop theft
- Sabotage
- Financial fraud
- Theft of proprietary info
- Unauthorized Access
- Net abuse
- Denial of Service
- Virus

The Base Protection Issue on Notebooks

- In Windows® XP the SAM database stores passwords
- Microsoft® recommends to encrypt the SAM database with \textquotedblleft syskey\textquotedblright\ (*).
  - 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
  - All remaining data on the disk is still stored in plain.

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
Authentication

- Pre-Boot Authentication in combination with a TPM offers authentication in a compact and protected environment.

- **Security**
  - Vulnerabilities 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®
- Authentication
  – Boot
  – Authorization

• 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
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)
Operational

- **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
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
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.

* 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
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
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)
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
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.
Writing and Using Trusted Applications: Security Solutions Using TCG Technology

Steven Sprague
Wave Systems Corp.
May 26, 2005
Solution Opportunities

Current Problems

- Insecure Distribution of Data
- Identity Theft
- Worms, Viruses
- Hackers, Attacks
- Phishing
- Exposed Data
- Regulatory Compliance
- Fraud
- Privacy Issues
- Insecure & Forgotten Passwords

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
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
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

Copyright© 2005 Trusted Computing Group - Other names and brands are properties of their respective owners.
How’s it Work

The 2 minute guide
TPM Security Programming Model

- **Software Application Layer**
  - Application 1
  - Application 2
  - Application 3

- **Software Infrastructure Layer**
  - MSCAPI
  - HDW CSP
  - TCG Enabled CSP
  - TCG Enabled Middleware

- **Hardware Layer**
  - HDW - Driver
  - Smartcard or token
  - TPM

---

Copyright © 2005 Trusted Computing Group - Other names and brands are properties of their respective owners.
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
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.
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
- Prompted or Auto Login
- Web and PC Application Credential Storage
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
Data Signing

- Random document authentication
- PDF signing tools
- Paperless contracts
Server Tools

- Backup and recovery
- Access Control
- Web Authentication
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)
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.
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
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…
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
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 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
Extending Trust to Platform Peripherals

Authentication/Attestation

Capability Level

Ability to interact with the Platform

LOW

HIGH
General Risk Model of a Peripheral

Peripheral Controller Electronics

- Primary Host Interface
- Loadable Firmware
- Data Sink / Source
- Power
- Firmware Functions
- Special Hardware Functions
- Diagnostic Ports
- Probe Points

Trust = systems operate as intended

Objective: Exercise control over operations that might violate trust

Needed: Trusted peripheral commands
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
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)
## DEVICE CREDENTIAL

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

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
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

Wave EMBASSY Software

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
www.trustedcomputinggroup.org

THANK YOU!

QUESTIONS?
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 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.
## One business problem at a time.

<table>
<thead>
<tr>
<th>Problem 1</th>
<th>Problem 2</th>
<th>Problem 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Put your business on the web</td>
<td>Put your employees on the web</td>
<td>Permit any device on the web on your network</td>
</tr>
<tr>
<td>Advantage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get global market access</td>
<td>Enable telework on corporate laptops</td>
<td>Enable outsourcing, consultants</td>
</tr>
<tr>
<td>Security Technology</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set up a perimeter</td>
<td>VPN</td>
<td></td>
</tr>
<tr>
<td>Isolate your business systems</td>
<td>Goodbye perimeter, hello endpoints</td>
<td></td>
</tr>
<tr>
<td>with firewalls</td>
<td>Add host protection – IDS, IPS, Antivirus</td>
<td></td>
</tr>
<tr>
<td>Intruders beget IDS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security process</td>
<td>periodic compliance</td>
<td></td>
</tr>
<tr>
<td>Assessment and vulnerability</td>
<td>Create 10,000 CISOs</td>
<td></td>
</tr>
<tr>
<td>scans.</td>
<td>Chase untrustworthy devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Centralized Policy Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Location Awareness</td>
<td></td>
</tr>
</tbody>
</table>

Besides swapping out closed networks nearly overnight for TCP/IP equipment, we’ve been playing catch up to business issues one at a time.
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**
Effort and Value misaligned

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
TNC Solution Creates a “Virtual Airlock” for Network Access & Protection
New Framework to Marshal Assets

Endpoint Integrity
- AV
- Spyware
- PFW
- Buffer Overflow
- OS Behavior
- hIPS
- Remediation
- DRM
- Encryption

Policy Enforcement Points
- Address Services - DHCP
- Remote Access SSL & IPsec
- Identity Services - RADIUS
- LAN Switching & Wireless
- Endpoint - PFW
- Inline Gateway Gig-E

Access Devices
- Unmanaged
- Managed Desktops
- Managed Mobile User
- Unmanageable
- PPC 2003
TNC Architecture

Access Requestor
- Integrity Measurement Collectors
- TNC Client
- Network Access Requestor
- Supplicant/VPN Client, etc.

Policy Enforcement Point
- Peer Relationship
- Policy Enforcement Point
- Switch/Firewall/VPN Gateway

Policy Decision Point
- Integrity Measurement Verifiers
- TNC Server
- Network Access Authority
- AAA Server, Radius, Diameter, IIS, etc.

Integrity Measurement Layer

Platform Trust Service (PTS)
- TSS
- TPM
- Int Log.

Network Access Layer
NAP alignment

Access Requestor
- Integrity Measurement Collectors
- TNC Client
- Network Access Requestor
- Platform Trust Service (PTS)
- TSS
- TPM
- Int Log.

Policy Enforcement Point
- Peer Relationship
- Policy Enforcement Point
- Supplicant/VPN Client, etc.
- Switch/Firewall/VPN Gateway
- MS DHCP, Routing
- MS DHCP, Routing

Policy Decision Point
- Peer Relationship
- Integrity Measurement Verifiers
- TNC Server
- Network Access Authority
- AAA Server, Radius, Diameter, IIS, etc.

NAP System Health Agents
- Quarantine Agent MS XP SP2/2003

Quarantine Server (Longhorn)

Health Agents
- Quarantine Agent
- MS XP SP2/2003
NAC Alignment

Access Requestor
- Integrity Measurement Collectors
- TNC Client
- Platform Trust Service (PTS)
  - TSS
  - TPM
  - Int Log.

Policy Enforcement Point
- Peer Relationship
- Policy Enforcement Point
  - Network Access Requestor
    - Supplicant/VPN Client, etc.
  - Switch/Firewall/VPN Gateway
  - Cisco Routers (now), Cisco Switches & VPN Concentrators (later)

Policy Decision Point
- Peer Relationship
- TNC Server
- Network Access Authority
- AAA Server, Radius, Diameter, IIS, etc.

Cisco Trust Agent
- NAC AV Clients
- NAC AV Servers
- Cisco ACS
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

Copyright © 2005 Trusted Computing Group - Other names and brands are properties of their respective owners.
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
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

<table>
<thead>
<tr>
<th>Requirements:</th>
<th>Solution:</th>
<th>Benefits:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Eliminate or control access by non corporate</td>
<td>• Leverage existing standards (802.1x)</td>
<td>• Stop malicious code from entering the network via laptops and desktops</td>
</tr>
<tr>
<td>devices</td>
<td>• Leverage existing infrastructure</td>
<td>• Broad policy coverage within existing</td>
</tr>
<tr>
<td>• Ensure government devices on LAN and VPN</td>
<td></td>
<td>operational process</td>
</tr>
<tr>
<td>are compliant with policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Juniper SSL, Cisco Switches, any AV</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• No forklift upgrades</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Integrate with existing incident response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>systems.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright© 2005 Trusted Computing Group - Other names and brands are properties of their respective owners.
Global Oil Services Company, enforce employee data privacy policy

<table>
<thead>
<tr>
<th>Requirements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Protect sensitive HR, business data on SAP system from being compromised at endpoint</td>
</tr>
<tr>
<td>• Stop malicious code from entering the network via mobile users &amp; contractors</td>
</tr>
<tr>
<td>• Juniper SSL, Cisco Switches, any AV</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Secure web-based remote access</td>
</tr>
<tr>
<td>• Integrate with SAP R/3 via IIS Web Server</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Benefits:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• No additional user IDs required for distribution to endpoints – leverage existing SAP portal</td>
</tr>
<tr>
<td>• No additional inline devices required to provide secure access to SAP data</td>
</tr>
</tbody>
</table>
International Financial Services
policy to protect “anydevice” access

<table>
<thead>
<tr>
<th>Requirements:</th>
<th>Solution:</th>
<th>Benefits:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Secure “anytime, anydevice, anyplace” computing</td>
<td>• Implemented location-dependent policies for home, traveling, and office connections</td>
<td>• 87% decrease in incident response time</td>
</tr>
<tr>
<td>• React to internal events in near real-time</td>
<td>• Integrated with Tripwire host-based and network-based intrusion detection systems</td>
<td>• Reduced desktop change management costs due to policy enforcement</td>
</tr>
<tr>
<td>• Flag unauthorized applications (e.g. Kazaa) when installed</td>
<td></td>
<td>• Improved patching policy compliance</td>
</tr>
<tr>
<td>• Juniper, Nortel, Cisco Infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• any AV, Alteris Config management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright© 2005 Trusted Computing Group - Other names and brands are properties of their respective owners.
## ATM Manufacturer

enforces remote access policy

<table>
<thead>
<tr>
<th>Requirements:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Protect 5,000 mobile &amp; remote users</td>
<td></td>
</tr>
<tr>
<td>• Enforce security policy &amp; patching</td>
<td></td>
</tr>
<tr>
<td>• Control consultant &amp; employee external access to internal resources</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensure compliance before permitting network access</td>
<td></td>
</tr>
<tr>
<td>• Nortel VPN integration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Benefits:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Saving $25,000+ per month in remote connection costs</td>
<td></td>
</tr>
<tr>
<td>• Immune to Blaster and other worms with strict patch enforcement</td>
<td></td>
</tr>
<tr>
<td>• Eliminated copyright violations with active policy enforcement</td>
<td></td>
</tr>
</tbody>
</table>
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
Questions & Answers
Thank You