TRUSTED COMPUTING GROUP™

Securing Data & Systems with Trusted Computing Now and in the Future

Brian Berger, bberger@wavesys.com
TCG Director
EVP Marketing & Sales, Wave Systems Corp.

December 2, 2010

Cybercrime Explodes

- From 2005-present, Privacy Rights Clearinghouse reports that for the govn't. sector alone, 130,035,135 records have been breached
  - In ALL sectors, the org reports that 510,528,937 records have been breached in same period.
- Fr. Deloitte 2010 Cyber Crime report, "perimeter-intrusion detection, signature-based malware, and anti-virus solutions are providing little defense and are rapidly becoming obsolete—for instance, cyber criminals now use encryption technology to avoid detection."
- Meanwhile, the leak of data managed by network security provider Omniquad has caused the Cloud Industry Forum to warn that this was "yet another example as to why customers have a natural fear of the risks associated with online business activity."
- Gartner's Neil MacDonald writes that cloud providers should be held to a standard that's even higher than those required to maintain internal standards and integrity because in the cloud "the impact of the lapse [in security] is magnified."

Let’s walk away with Vision!!

Imagine a world where:

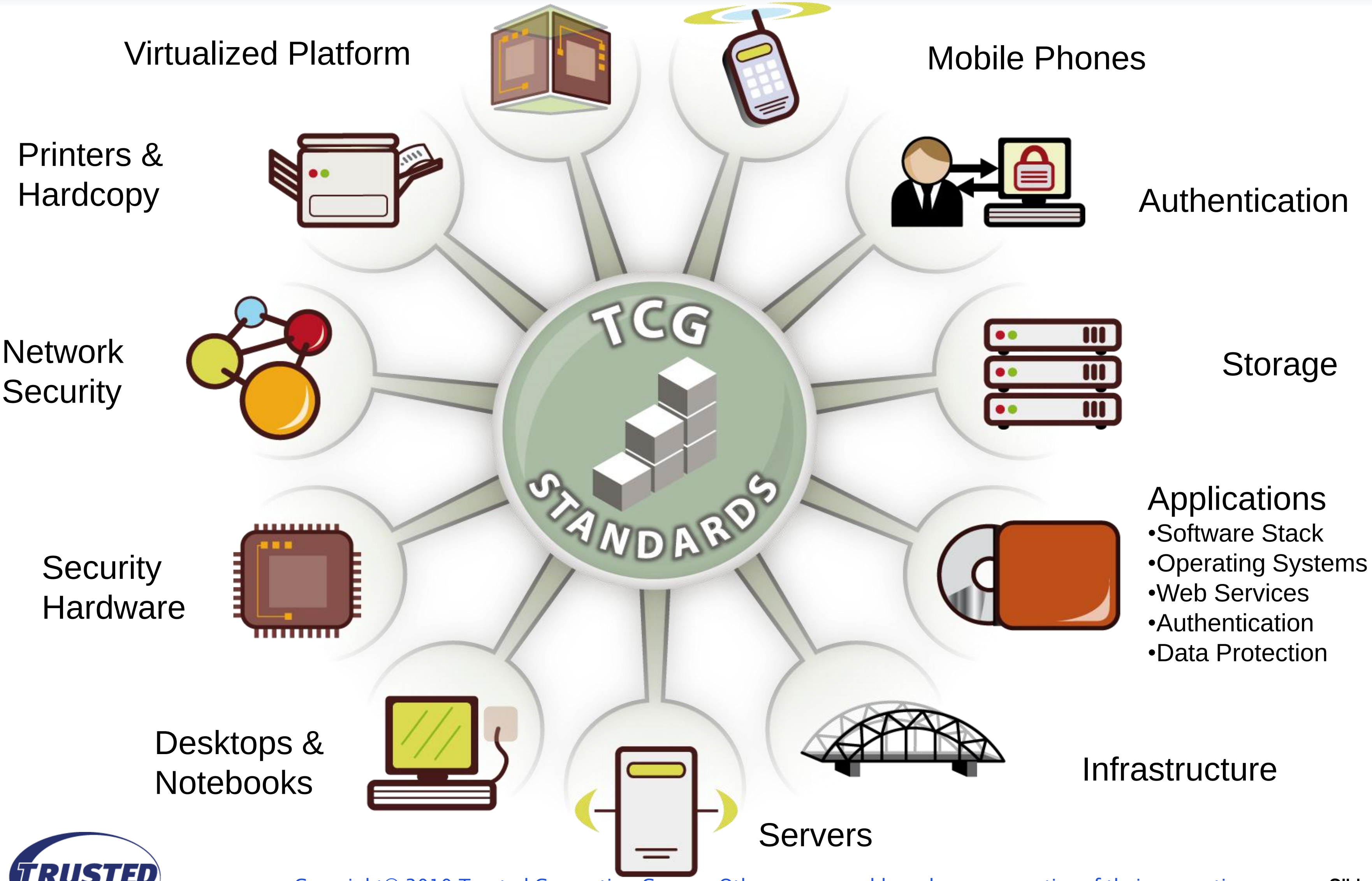
1. Only known machines are accessing networks where they are recognized as “members”
2. When a laptop is lost, the data is persistently protected with hardware security.
3. A machine runs only validated code and the user and owners of the machine don’t worry about unauthorized code.
4. Only services and authorized users/machines can have a relationship.
5. Authentication and data protection are the priority for a successful cloud service.

TCG VISION

Mission Statement

The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, industry standards for trusted computing building blocks and software interfaces across multiple platforms.

Complete Trusted Enterprise Solutions



Virtualized Platform

Mobile Phones

Printers & Hardcopy

Authentication

Network Security

Storage

Security Hardware

Applications
- •Software Stack
- •Operating Systems
- •Web Services
- •Authentication
- •Data Protection

Desktops & Notebooks

Servers

Infrastructure

What we need are standards

- Trusted services need to run on any device then we have a trusted enterprise.
  - Requirements:
    - Common internationally recognized hardware specification and building blocks
    - Geographical and Geopolitically neutral
    - Common programming interfaces
    - Interoperability
    - Vendor neutrality
- Enable the broadest flexibility in application and solution support

Participate in standards!!

Benefits of TCG and its technology

- **Reduce cost**
  - TPM is half the cost of a smart card and a third the cost of a token – See case study
  - It is already on every machine
- **Reduce time to market**
  - Already deployed on millions of products
  - Turn it on, no IT restart required
- **Multivendor interoperability**
  - Example: Multiple vendors developed a plug fest for SED, TPM and TNC solutions
- **International standardization and broad distribution drives adoption and membership in TCG**
  - Example: ISO/IEC has approved the TPM specification

TCG TODAY

Where do we see TCG Technology today?

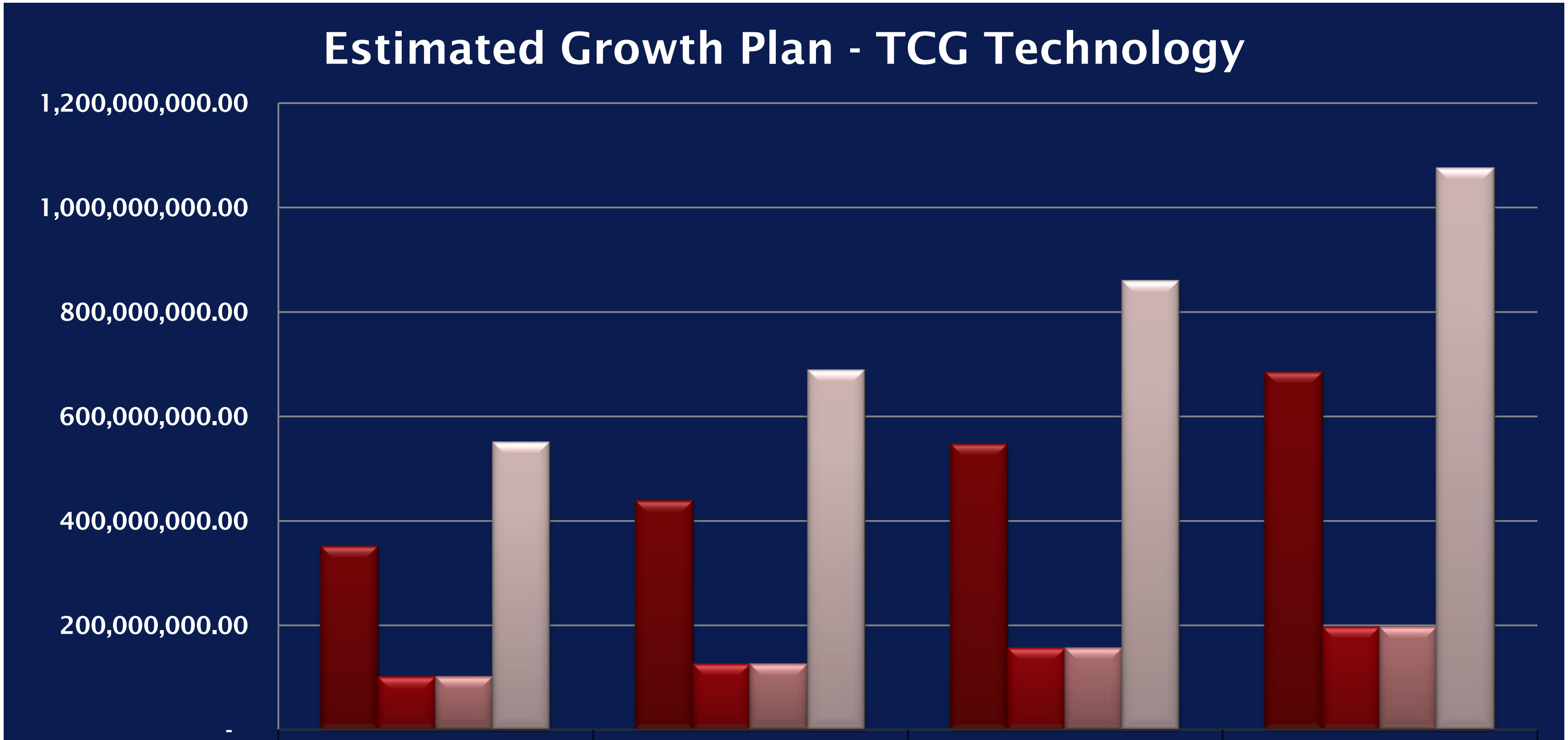
Commercialized and available

1. High Assurance Platforms (HAP)
2. Self Encrypting Drives (SEDs)
3. Network Security (TNC)
4. Trusted Platform Modules (TPMs)

Applications/solutions that use TCG Technology

1. Machine Identity
2. VPN/Wireless Access
3. Data at Rest
4. SCADA
5. Clientless endpoint meta data management
6. Hardware-based cloud subscriber management
7. Trusted execution

Trusted systems widely available Estimates



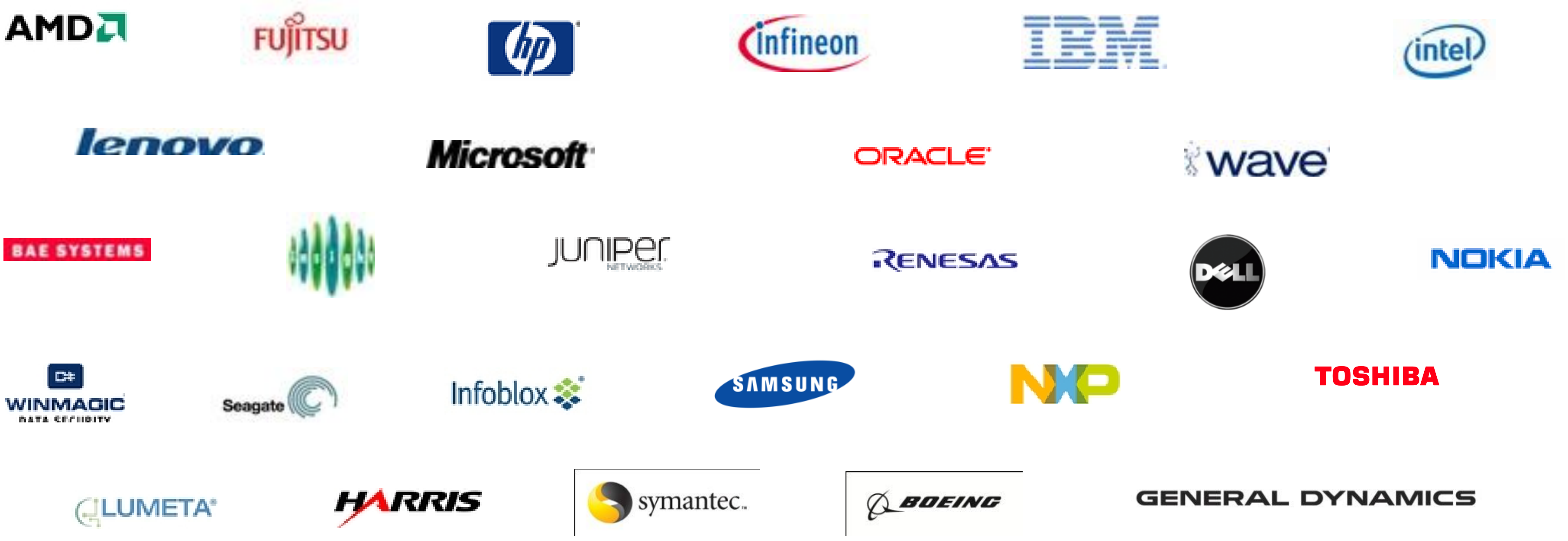
Estimated Growth Plan - TCG Technology

	2010	2011	2012	2013
■ PC's	350,000,000.00	437,500,000.00	546,875,000.00	683,593,750.00
■ Embeded	100,000,000.00	125,000,000.00	156,250,000.00	195,312,500.00
■ Networking	100,000,000.00	125,000,000.00	156,250,000.00	195,312,500.00
■ Totals	550,000,000.00	687,500,000.00	859,375,000.00	1,074,218,750.00

Who is involved in TCG?

Total Membership including Commercial, Liaison, Invited Experts and Government participants:

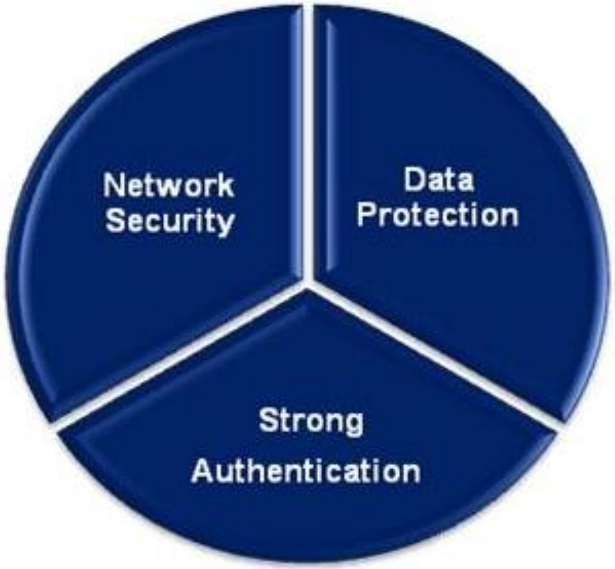
137 Member Organizations



Complete Membership List Available: http://www.trustedcomputinggroup.org/about_tcg/tcg_members

Solution focus – market demand

Trusted Computing solutions enable more secure computing environments through different applications for a range of industries without compromising functional integrity, privacy, or individual rights.



What we all need:

- In the broadest context
  1. Known devices on networks
  2. Known software running on devices
  3. Known users on networks and devices
  4. Known execution of known code on devices
  5. Interoperability across devices
  6. Adoption not limited by certification, import/export, and geographical issues.
     - All within the context of appropriateness, of course.
- Certification
  1. Definition for the supply chain for COTS security products that can be sold commercially to all vertical markets
  2. Definition of high assurance products that require special certification for government purchases

Membership

Trusted Computing Group Incorporation and Benefits

- The Trusted Computing Group (TCG) is incorporated as a not-for-profit industry standards organization focused on developing, defining, and promoting open standards for trusted computing that will benefit users. The organization's structure has been designed to enable broad participation, efficient management, and widespread adoption of the organization's specifications.
- Membership is open to a wide range of for-profit corporations, non-profit corporations, and other enterprises supportive of TCG's goals, with clearly defined benefits at different levels of membership
  - Reasonable and non-discriminatory (RAND) patent licensing policy between Members
  - Board, Committee, and Work Group structure with supermajority voting
  - Marketing Programs and Certification whitelist program
- More information on the benefits of membership available at:

  http://www.trustedcomputinggroup.org/join_now/membership_benefits

IDEAS TO WRITE DOWN!!!

TCG: A Foundation for your decisions

Start with the easy ones:

1. Protect your data with world-class protection in hardware – Request SEDs in your bids, proposals and procurement
2. Protect your network access, cloud services access and user access with TPM protected certificates – request software to manage your TPMs for network access in all your bids, proposals and procurement
3. Update your network security infrastructure with interoperable TNC solutions for access, authentication, meta data management and attestation in all bids, proposals and procurement. Link with TPM and SED.
4. Plan for mobile integration for data protection, network access and device recovery/device disablement as part of your overall network solutions.

About TCG

The Trusted Computing Group (TCG) is an international industry standards group. The TCG develops specifications amongst it members. Upon completion, the TCG publishes the specifications for use and implementation by the industry.

The TCG publicizes the specifications and uses membership implementations as examples of the use of TCG Technology. The TCG is organized into a work group model whereby experts from each technology category can work together to develop the specifications. This fosters a neutral environment where competitors and collaborators can develop industry best capabilities that are vendor neutral and interoperable.

Thank you

For more information, case studies, social media access, blog, membership and developer information

http://www.trustedcomputinggroup.org/

TRUSTED COMPUTING GROUP™

CASE STUDIES

Case Study – St. Mary’s County Public Schools

Who

- Public school district in MD
- 16,000 students, 2,100 staff
- 26 schools, Grades K-12
- New, intensive STEM academies

CHARTING A COURSE TO EXCELLENCE

St. Mary's County Public Schools

“Work Hard and Be Nice”

Problem

- Need strongest security
  - Only STEM laptops can connect
  - User-specific access controls
  - Strong health checks
  - All wireless traffic encrypted

Solution

- Juniper UAC with ...
  - Permanently resident agent
  - Continuous health checks
  - TNC Policy Decision Point, Client
- Any vendor’s wireless access points
  - 802.1X enforcement
  - Integrated via TNC's IF-PEP

Lessons Learned

- TNC = open, affordable security
  - Tightly controlled endpoints
  - Strong network security
  - Integrated with open standards

Case Study - Global Professional Services Firm

Who

- Global professional services firm
- 150,000 employees and partners
- 850 locations
- 142 countries

Problem

- User ID and Password authentication is no longer sufficient
- Social hacks are very pervasive for gaining access
- Other security breeches are becoming more prevalent

Requirements

- No additional sign-on/authentication process for the users.
- No external devices such as tokens or smart cards
- No biometrics
- Two factor authentication

Requirements

- Global in scope and scalable to 150K+ users
- Central Management
- Compatible with current PKI infrastructure
- Open Standards
- Broad applicability and acceptance

Solution / Results

- Use existing P's that include TPMs
- Use Wave Systems management software for interoperability and application integration
- TCO of using TPM plus Wave's Software reduced our implementation and management of other competing technologies by more than 50%
- The solution was scalable, improved manageability and increased user acceptance

Case Study - Mazda

Who

- Automotive Manufacturer (MNAO)
  - Mazda North American Operations
- Based in Irvine, CA
- Responsible for R & D, sales and marketing, parts and customer service in North America

Problem

- Protect customer personal identifiable information and confidential business information on Laptops
  - IT burden had to be low to none
  - Data protection is the highest priority
  - Protection against lost or stolen laptops

Solution

- Wave EMBASSY® Trusted Drive Manager & Remote Administration Server
  - Seagate SED's (Self Encrypting hard Drives)
  - Centralized administration of users, credentials and access privileges
  - Policy based controls
  - Proof of Compliance
  - Simplified machine re-provisioning, data destruction and EOL best practices
  - SSO, Windows® Password Synchronization
  - Password recovery "Help Desk" capabilities

Benefits

- Protects mobile data in minutes
- "Built in" encryption minimizes setup and support costs
- Centralized management of computer security policies
- Proof of compliance with data protection regulations

Case Study – Diebold

DIEBOLD

INNOVATION DELIVERED®

Who

- Premier safe and lock company
- ATM pioneer
- 170,000 employees in 90 countries
- Delivering self-service solutions and security systems for over 150 years

Problem

- ATM security is an ongoing concern
  - Aggressive, sophisticated criminals
  - $50bn in ATM cash withdrawn annually
- Physical brute force attacks
  - Prevented by locks, cameras, safes
- Cyber attacks
  - Thieves hack into ATM
  - Bypass onboard computer
  - Use unauthorized computer to issue commands
  - Result: fraudulent withdrawals

Copyright © 2009 Trusted Computing Group

Diebold - Solution

Solution

- ATM on-board computer contains a TPM
- Wave software integrated into ATM security framework
- Use TPM to generate hardware-based machine certificates within PKI infrastructure
- Unique, un-spoofable identifier for PC authentication
- Also supports user certificates for service technicians

Lessons Learned

- Hardware-level security provides stronger protection than software-only solution

– Standards-based security:
  - Ensures critical management functions
  - Provides assurance that applications run flawlessly with all TPM vendors – insulation from change