Trusted Computing Group: Where Trust Begins
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Speaker</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:30 – 2:00</td>
<td>Welcome and Introduction to Trusted Computing Group</td>
<td>Steve Hanna</td>
<td>Infineon Technologies</td>
</tr>
<tr>
<td>2:00 – 2:25</td>
<td>Trust in the Cloud</td>
<td>Michael Donovan</td>
<td>Hewlett-Packard</td>
</tr>
<tr>
<td>2:25 – 2:55</td>
<td>Break: Demonstration Showcase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:55 – 3:20</td>
<td>Trusted Network Connect (TNC) and Security Automation</td>
<td>Lisa Lorenzin</td>
<td>Juniper Networks</td>
</tr>
<tr>
<td>3:45 – 4:10</td>
<td>Trusted Platform Modules (TPMs) as Virtual Smart Cards</td>
<td>John Fitzgerald</td>
<td>Wave Systems</td>
</tr>
<tr>
<td>4:10 – 4:30</td>
<td>Closing Remarks: Demonstration Showcase</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Today’s Cybersecurity Train Wreck

Data Breaches

System Compromise

Monitoring

Physical Impacts

Source: Historical photograph, Lagerlunda Railway Accident, 1875.
Untrusted Systems

Source: S E C Railway Narrow Gauge Museum of Nagpur
Benefits of Trusted Systems

Trust is...

the belief that a person or system will behave predictably, even under stress
based on experience and/or evidence
based on fundamental properties (identity, integrity)
easy to lose and hard to regain
What is a Trusted System?

A trusted system is…

- predictable, even under stress
- trusted based on experience and/or evidence
- based on fundamental properties (identity, integrity)
1. Build a Hardware Root of Trust into each device
What is a Hardware Root of Trust?

- **Hardware Security**
  - Trusted Platform Module (TPM)

- **Provides**
  - Foundation for Secure Software

- **Features**
  - Authentication
  - Encryption
  - Attestation

  - Identity
  - Integrity
Why Hardware?

Software Security is Not Enough

Defects per FP

Defect Removal Efficiency

SEI CMM 1

SEI CMM 3

SEI CMM 5

Graph used with permission of Capers Jones.
1. Build a Hardware Root of Trust into each device

2. Employ Hardware Storage Encryption
Hardware Storage Encryption

- **Hardware Security**
  - Self-Encrypting Drive (SED)

- **Provides**
  - Protection against Physical Attacks
  - Protection against Loss and Theft
  - Cryptographic Wipe

- **Features**
  - Encryption
1. Build a Hardware Root of Trust into each device

2. Employ Hardware Storage Encryption

3. Add Security Automation
Security Automation

- **Security Coordination Standards**
  - Connect Existing Systems
  - Enable New Capabilities

- **Provide**
  - Automation for All Phases of Cyber
    - Preparation
    - Detection
    - Analysis
    - Response
1. Build a Hardware Root of Trust into each device

2. Employ Hardware Storage Encryption

3. Add Security Automation

4. Protect Legacy Systems
Protect Legacy Systems

- **Legacy Systems**
  - ICS/SCADA or Old Systems
  - Vulnerable to Disruption or Infection
  - Need Protection

- **Protection**
  - Place into Enclaves
  - Overlay Secure Communications
  - Restrict to Authorized Parties
1. Build a Hardware Root of Trust into each device

2. Employ Hardware Storage Encryption

3. Add Security Automation

4. Protect Legacy Systems
Why Open Standards?

<table>
<thead>
<tr>
<th>Interoperability</th>
<th>Vendor Neutrality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Certification</td>
</tr>
<tr>
<td>Lower Costs</td>
<td>Ubiquity</td>
</tr>
</tbody>
</table>
TCG = Open Standards for Trusted Computing

- TCG is the only group focused on trusted computing standards
- TPM specification implemented in more than a billion devices
  - Chips, PCs, servers, printers, kiosks, industrial systems, and many embedded systems
- Trusted Computing is more than TPM
  - Secure Storage
  - Security Automation
  - Secure Cloud
  - Secure Mobile Devices
  - Secure Legacy Devices
What Can I Do Now?

1. **See What You Already Have**
   - Enterprise PCs and servers with TPMS
   - Microsoft Windows with built-in TPM support
   - Red Hat Enterprise Linux with built-in TPM support
   - Self-Encrypting Drives widely available for little to no cost differential
   - Network equipment supports TNC standards
   - ICS/SCADA gateways support TCG’s ICS standards
1. See What You Already Have

2. Deploy It
   - TPM as virtual smart card or for disk encryption
     - Huge cost savings, easier management, and better security
   - SEDs
     - Strong data protection, quick and secure drive re-use
     - Strict but easy compliance, “safe harbor” from data breach regulations
   - TNC
     - Secure wireless and wired networks
     - Ensure only healthy and approved devices are connecting
     - Also include security automation features
What Can I Do Now?

1. See What You Already Have
2. Deploy It
3. Demand More
   - Ask vendors for Trusted Computing support
   - Mention TCG standards in acquisition documents (RFPs, etc.)
   - Look for TCG certification
Questions?
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Presenter(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:30 – 2:00</td>
<td>Welcome and Introduction to Trusted Computing Group</td>
<td>Steve Hanna, Infineon Technologies</td>
</tr>
<tr>
<td>2:00 – 2:25</td>
<td>Trust in the Cloud</td>
<td>Michael Donovan, Hewlett-Packard</td>
</tr>
<tr>
<td>2:25 – 2:55</td>
<td>Break: Demonstration Showcase</td>
<td></td>
</tr>
<tr>
<td>2:55 – 3:20</td>
<td>Trusted Network Connect (TNC) and Security Automation</td>
<td>Lisa Lorenzin, Juniper Networks</td>
</tr>
<tr>
<td>3:45 – 4:10</td>
<td>Trusted Platform Modules (TPMs) as Virtual Smart Cards</td>
<td>John Fitzgerald, Wave Systems</td>
</tr>
<tr>
<td>4:10 – 4:30</td>
<td>Closing Remarks: Demonstration Showcase</td>
<td></td>
</tr>
</tbody>
</table>