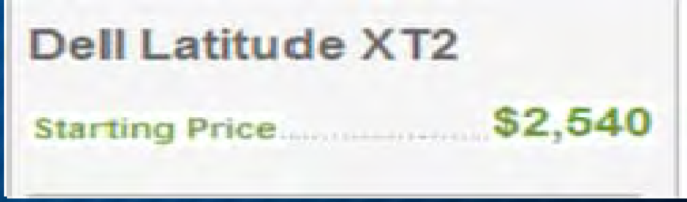
Simplifying Encryption and Authentication

Trusted Computing Group Opal Self-Encrypting Drives

Robert Thibadeau, Ph.D.
Office of CEO, Wave Systems Corp.

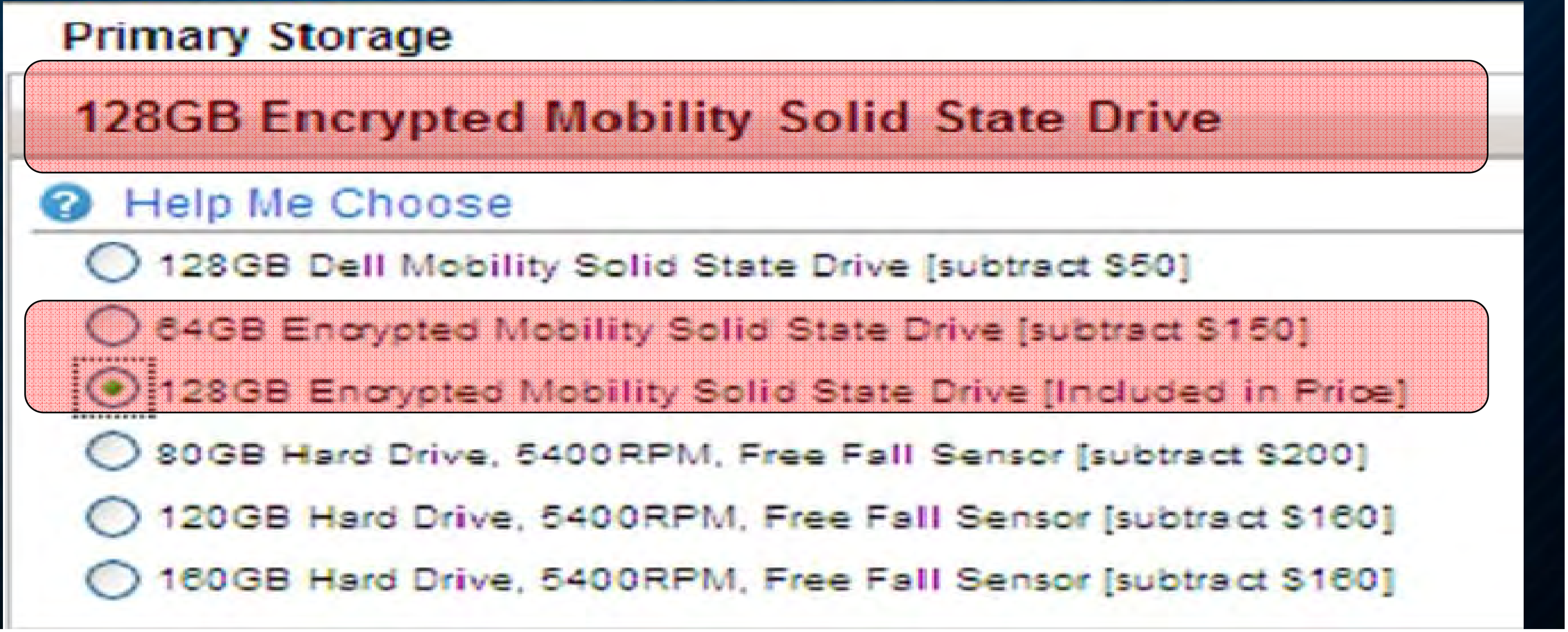
wave®

Simplifying Encryption and Authentication



Dell Latitude XT2

Starting Price $2,540



Primary Storage

128GB Encrypted Mobility Solid State Drive

○ 128GB Dell Mobility Solid State Drive [subtract $50]

○ 64GB Encrypted Mobility Solid State Drive [subtract $150]

● 128GB Encrypted Mobility Solid State Drive [Included in Price]

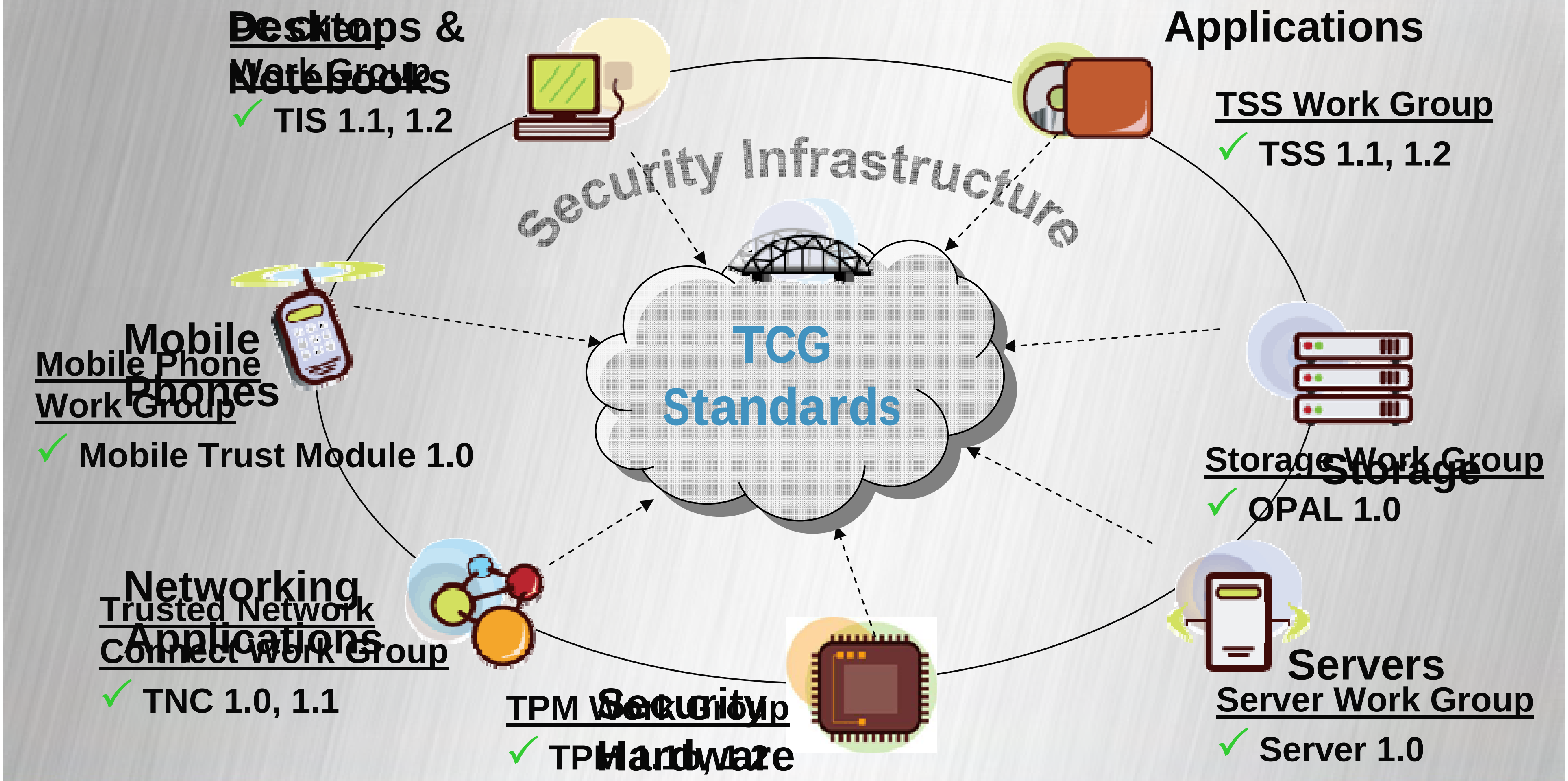
○ 80GB Hard Drive, 5400RPM, Free Fall Sensor [subtract $200]

○ 120GB Hard Drive, 5400RPM, Free Fall Sensor [subtract $160]

○ 160GB Hard Drive, 5400RPM, Free Fall Sensor [subtract $160]

Trusted Computing Group (TCG)

Developing Open Industry Standards



Desktops & Notebooks

Desktop Work Group

✓ TIS 1.1, 1.2

Applications

TSS Work Group

✓ TSS 1.1, 1.2

Security Infrastructure

TCG Standards

Mobile Phones

Mobile Phone Work Group

✓ Mobile Trust Module 1.0

Storage

Storage Work Group

✓ OPAL 1.0

Networking Applications

Trusted Network Connect Work Group

✓ TNC 1.0, 1.1

Security Hardware

TPM Work Group

✓ TPM 1.1b, 1.2

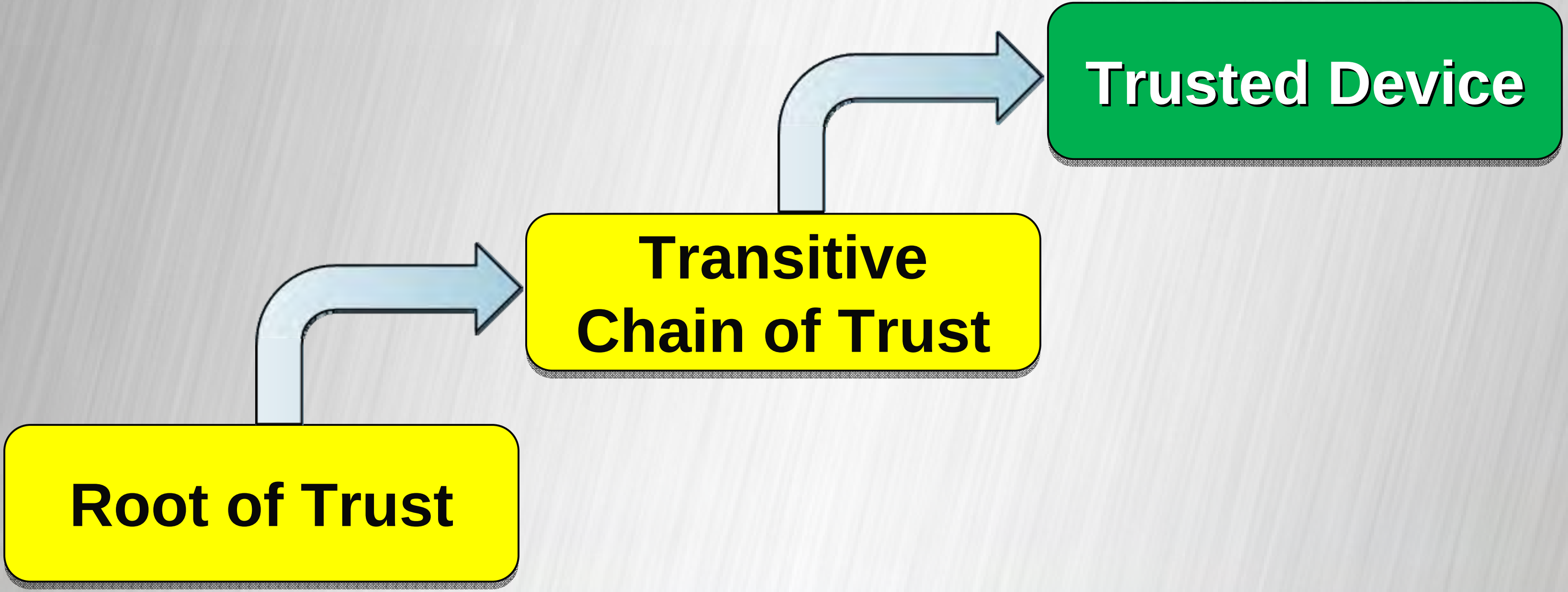
Servers

Server Work Group

✓ Server 1.0

Prerequisite - Hardware Root of Trust

- A platform root of trust, *based in hardware*, is essential for all security in the device
- Software **CANNOT** provide a secure root of trust



Root of Trust

Transitive Chain of Trust

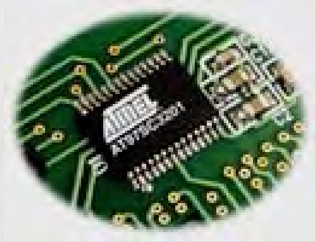
Trusted Device

Trusted Computing in Action

- Virtually all “business grade” laptops and desktops include TPMs as part of their standard configuration
  - Tier 1 – Dell, HP, Lenovo
  - Tier 2 – Acer, Fujitsu, Sony, Toshiba
- US Government agencies are mandating TPMs
  - Air Force “Mainstream Buying Standards” requires TPM 1.2
  - Army requires TPM 1.2 for all new Window’s PCs
  - OSD Mandates TPM on all new PCs
- Integration within Intel vPro chipset – iTPM
- Microsoft Vista® leverages TPM for enhanced security
  - BitLocker® - Integrated FDE that utilizes a TPM
    - Gartner strongly recommends using a TPM

⇨ TPM install base is headed towards ubiquity ~300 Million

⇨ TPM aware applications are entering the market



First Application: Device Identity

Information Assurance and Security is based on **Strong Identity**

Billions has been spent on providing identity to users but that is only **half the solution**

It is now time to invest in the **secure identity of all devices**

Secure identity requires a hardware root of trust

Device Identity is not a New solution

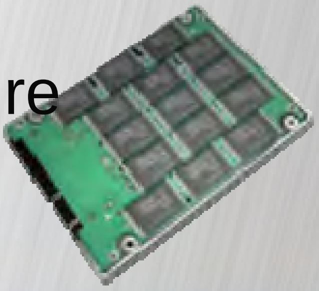
- The cellular network went to strong identity of devices in the transition to digital in mid 90's
- The cable industry transitioned in the mid 80's
- The satellite industry transitioned in the mid 80's
- The garage door opener got an identity in the 70's

It is now time to adopt a proven platform identity solution for Cyber security on the Internet

Self-Encrypting Drives

Changing the Landscape of Data Encryption

- Strong specifications for attached storage
- Should apply to all USB data storage
- Moves PC authentication to PRE OS stage
- Integrated support for multiple authentication factors
  - ❑ Card
  - ❑ Password
  - ❑ Network
  - ❑ TPM
- Data protection in hardware is the right architecture



Trusted Computing in Action

Factory-Installed Self-Encrypting Drives

- Optional on Dell Latitude, Optiplex and Precision Workstations
  - ❑ Latitude E4200, 4300, 5400, 5500, 6400 and 6500
  - ❑ Latitude D530, 531, 631 and 830
  - ❑ Precision M2400, 4400, 6400, T3500, 5400, 7400
  - ❑ Optiplex 760, 960
- Supported by Lenovo and HP – as custom features
- TCG’s Opal Self-Encrypting Drive Specification (2/09)
- Seagate Drives have NSA National Security System Approval
- All PCs should be procured with Self Encrypting Drives

⇨ ***Compliance Regulations are Driving Adoption***

Our Vision ....

- In the future –
  - ❑ You will log into your device and your device will log you into everything else.
  - ❑ Only authorized PCs will be on my network and I can definitively identify them all.
  - ❑ The PC will have the premier Root of Trust and Privacy Models for all devices. Scalable and Global
  - ❑ When My PC is un-attended or lost my data is safe.

Trusted Computing just getting started.

The components exist and are ubiquitous.

Simplifying Encryption and Authentication

Thank You

Robert Thibadeau, Ph.D.
Office of the CEO
Wave Systems Corp.
rthibadeau@wavesys.com