



Trusted Computing As a Solution!

Brian Berger

EVP Marketing & Sales & TCG Director

Wave Systems Corp. www.wave.com

Trusted Computing Group www.trustedcomputinggroup.org

Agenda

- ◆ **State of Hardware Security**
- ◆ **Best Practices**
- ◆ **Case Examples**
- ◆ **Summary**

The Case for Hardware-Based Endpoint Security

- ◆ The rise of data protection regulations and the associated heightened awareness are driving the need for stronger security
 - A data breach can cost in the millions of dollars and destroy a brand
 - Software is vulnerable, e.g., cold boot attacks
- ◆ Data security is more than just data encryption
 - Data protection, authentication and access and network security
- ◆ Enterprises want to expand their security coverage without dramatically increasing their security budgets
 - “Built in” hardware is more cost effective to acquire, deploy and manage
 - Standards based solutions ensure interoperability across diverse systems
 - Provides a reputable compliance solution
- ◆ Industry’s positive reaction to the market
 - Standards for hardware-based endpoint security technologies
 - Leading data storage and security chip OEMs have solutions available today
 - Tier one PC OEMs are making these technologies available
 - The number one PC chipset manufacturer is bringing solutions to market

Security Best Practices

- ◆ **Hardware security is a MUST for protecting information, access to information and controlling where information goes**
 - Purchase all new laptops with FDE drives
 - Retrofit high-risk legacy machines with FDE drives
 - Restrict access to sensitive data to machines with FDE drives
 - Move software digital certificates TPM protection
 - Store/Protect pre-boot and Windows authentication credentials in hardware
 - Leverage the TPM for VPN, remote and wireless access
 - Manage your data and potential rogue removable storage devices with TPMs
 - NAC solutions rely upon known state of machines (hardware and software) to make proper decisions.

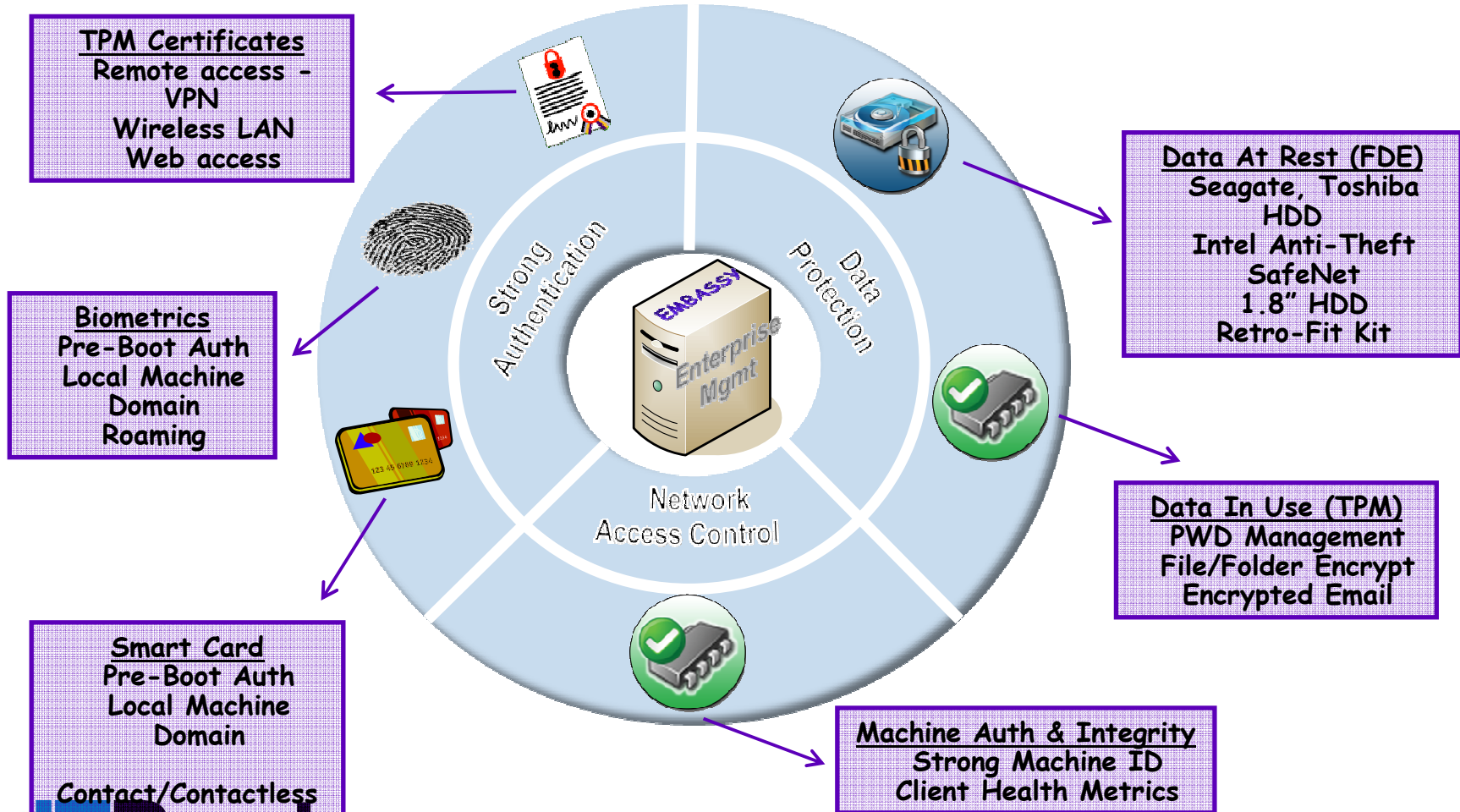
Security Best Practices

◆ An enterprise security solution should be a comprehensive product, not a disparate “point solution”

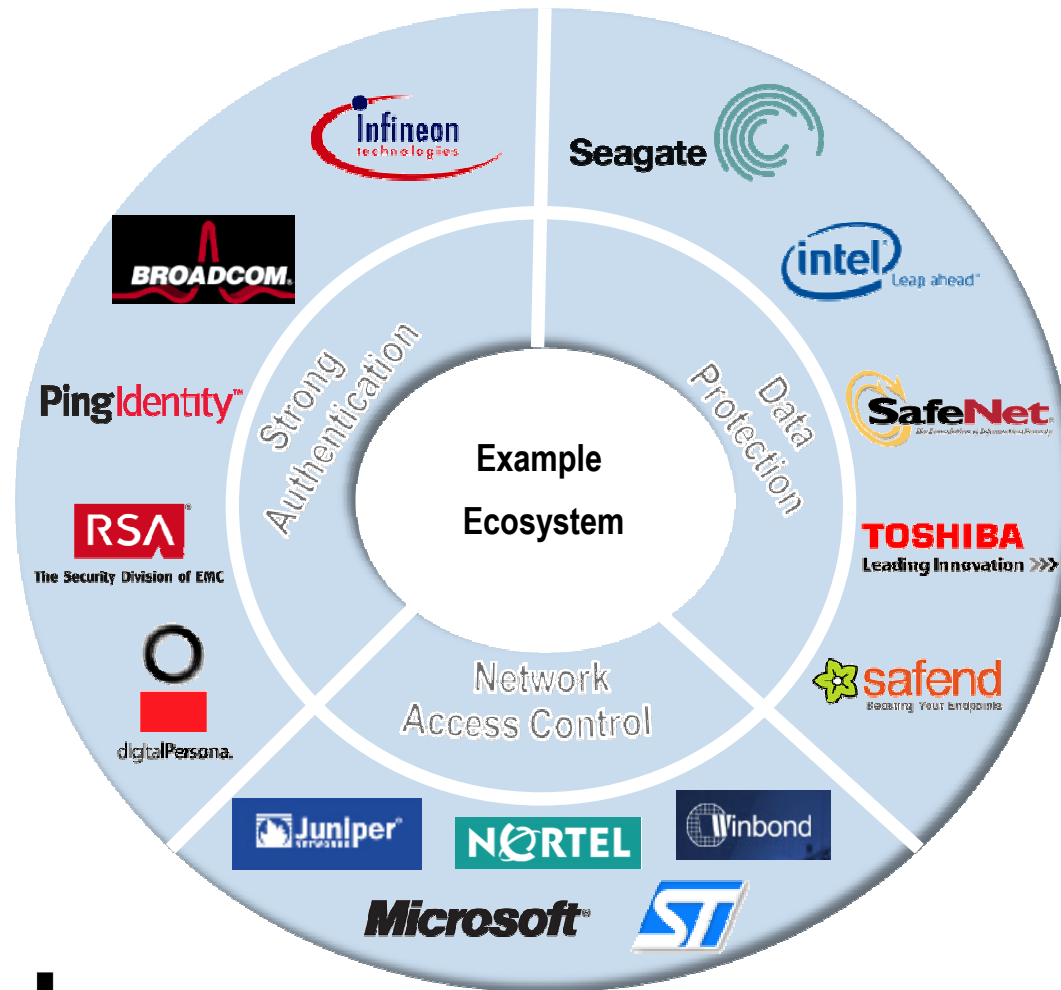
- Questions to ask:

1. Does the solution manage both hardware and software based Full Disk Encryption? And, what technologies does the solution support? Fully Encrypting FDE, SW FDE, Intel's Anti-Theft ® Technology?
2. Does the solution support the industry standard for authentication and network access (TPM)? Does it support all TPM's?
3. Does the solution support in-band and out-of-band management?
4. What about help desk?
5. Does the user manage the security, policies and choice to enable or is it enterprise managed as done with other technologies in business?
6. What about on/off line use, does it work?
7. What about key management? Who manages the keys?
8. Is there a single product that can meet this requirement?
9. Are there standards that support this model?
10. When deploying NAC, what is your authentication and data security solution?

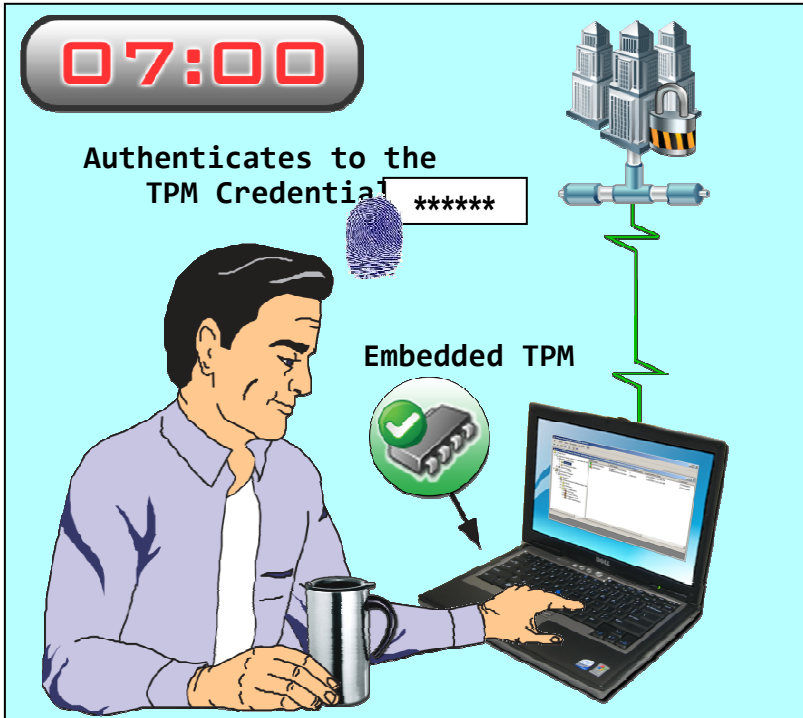
Best Practices in Action



Who's who? in technology!



A Day in the Life – At Home




07:00

Authenticates to the TPM Credential *****

Embedded TPM

Dan logs onto his office VPN using a TPM security chip as a token.

The illustration shows a man sitting at a laptop. A digital clock displays 07:00. A text box says 'Authenticates to the TPM Credential *****' with a fingerprint icon. A server rack icon is connected to the laptop by a green line. A circular icon with a green checkmark and a TPM chip is labeled 'Embedded TPM'.



07:05

Rich's PC

Dan emails his boss, Rich, his latest sales figures and they are automatically encrypted using TPM hardware security.

The illustration shows the same man at his laptop. A digital clock displays 07:05. A laptop icon labeled 'Rich's PC' is connected to the man's laptop by a green line. A cloud icon with a padlock is also connected to the man's laptop by a green line.

A Day in the Life – At the Office

09:00

Authenticates to the FDE Drive (Options)



Dan powers on his laptop and enters his password for preboot authentication. Usually he has single sign-on, but his password expired and he is prompted to change it.


11:00



Dan finishes his sales presentation and backs it up to a USB token protected by the TPM. Only Dan can access the encrypted data from his laptop unless he sets sharing parameters.


A Day in the Life – On the Road

14:30 Home Office Help Desk



Dan powers on his laptop at HQ, but forgets his new password and is stuck at preboot. He calls the help desk for a recovery password and logs on.

14:35



Dan connects to the wireless LAN at HQ. He has been set up for 802.1x authentication using the TPM so it identifies him as well as his machine.

Benefits of a Complete Solution



User Scenario – *At Home with TPM technology*

IT Benefits –

- Eliminate distribution/replacement/help desk costs of hardware tokens
- Enhance security to comply with regulations and internal security policies



User Scenario – *In the Office with FDE drives and TPM technology*

IT Benefits –

- Wave pre-boot authentication is not vulnerable to published BIOS attacks
- Ensure compliance with secure configuration logs



User Scenario – *On the Road with FDE drives and TPM technology*

IT Benefits –

- Secure, remote password recovery
- Lock down wireless LANs to only known users and known machines
- Intuitive UI lets administrators set up users and policies in just minutes



Thank You

Brian Berger
EVP Marketing & Sales & TCG Director
Wave Systems Corp.
Trusted Computing Group