

Integrating User Authentication with Platform Authentication and Key Management

Ned Smith

CardTech/SecureTech 2007

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

TRUSTED COMPUTING GROUP™

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Authentication



Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Why Better Authentication is Necessary

- Notebooks have sensitive information
  - Social Security, FTC, AICPA, Ernst & Young, Hotels.com, Equifax, District of Columbia, Medicaid, Boeing, U.S. Dept. of Veterans Affairs, American International Group, YMCA … and many others (src: wikipedia)
  - Losses totaled over $6.7 Million in 2005 (src: FBI)

TRUSTED COMPUTING GROUP™

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Why Better Authentication is Necessary

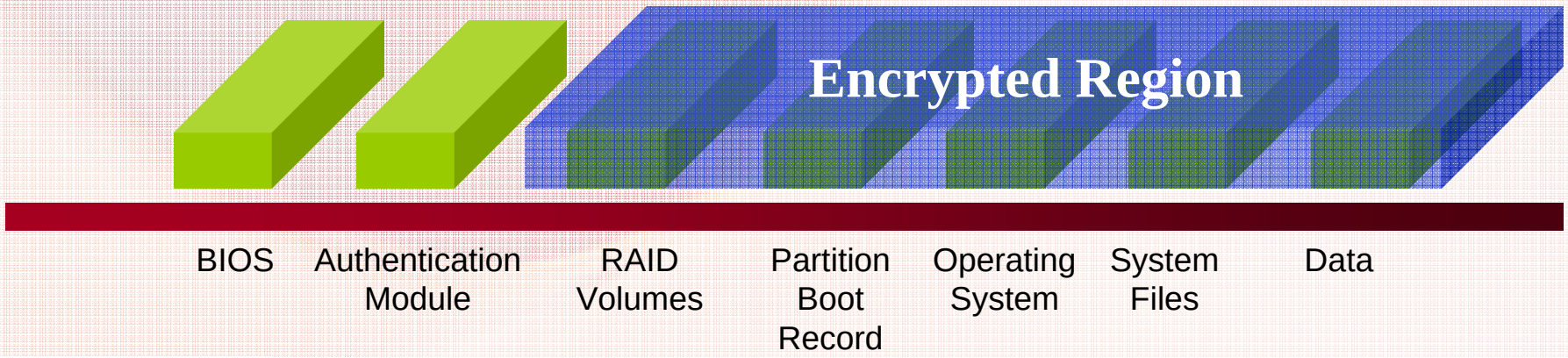
- Website fraud
  - **Middle District of Florida**. A defendant has been indicted on bank fraud charges for obtaining names, addresses, and Social Security numbers from a Web site and using those data to apply for a series of car loans over the Internet. (src:US Dept. of Justice)
  - On-line retailers loose over $3 billion in 2006; a 7% increase over previous year (src: Network World 11/4/06).
  - Forrester Research of Cambridge estimated breaches have cost companies between $90 and $305 per lost record, including notifying customers, hiring contractors to fix computer systems, fines, and lost business.
- Enterprise IT Security Costs
  - The National Institute of Standards and Technology, a U.S. government agency, estimates computer security problems cost between US$22.2 billion to $59.5 billion per year (src: CSO Online May, 2006)

TRUSTED COMPUTING GROUP™

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Full-Disk Encryption Protects Data at Rest

- FDE means authentication is done early
  - Before OS is loaded
  - Before RAID subsystem is initialized
- …during pre-boot!



Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

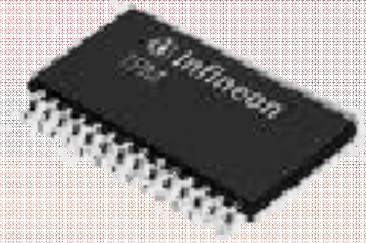
Quiz

- As value of assets controlled by your PC increases, how can authentication be improved to match the value?
  - A) Choose longer passwords
  - B) Use different passwords for different accounts
  - C) Let your lawyer handle it
  - D) Employ multiple factors

TRUSTED COMPUTING GROUP™

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

TPM Provides another Factor of Authentication

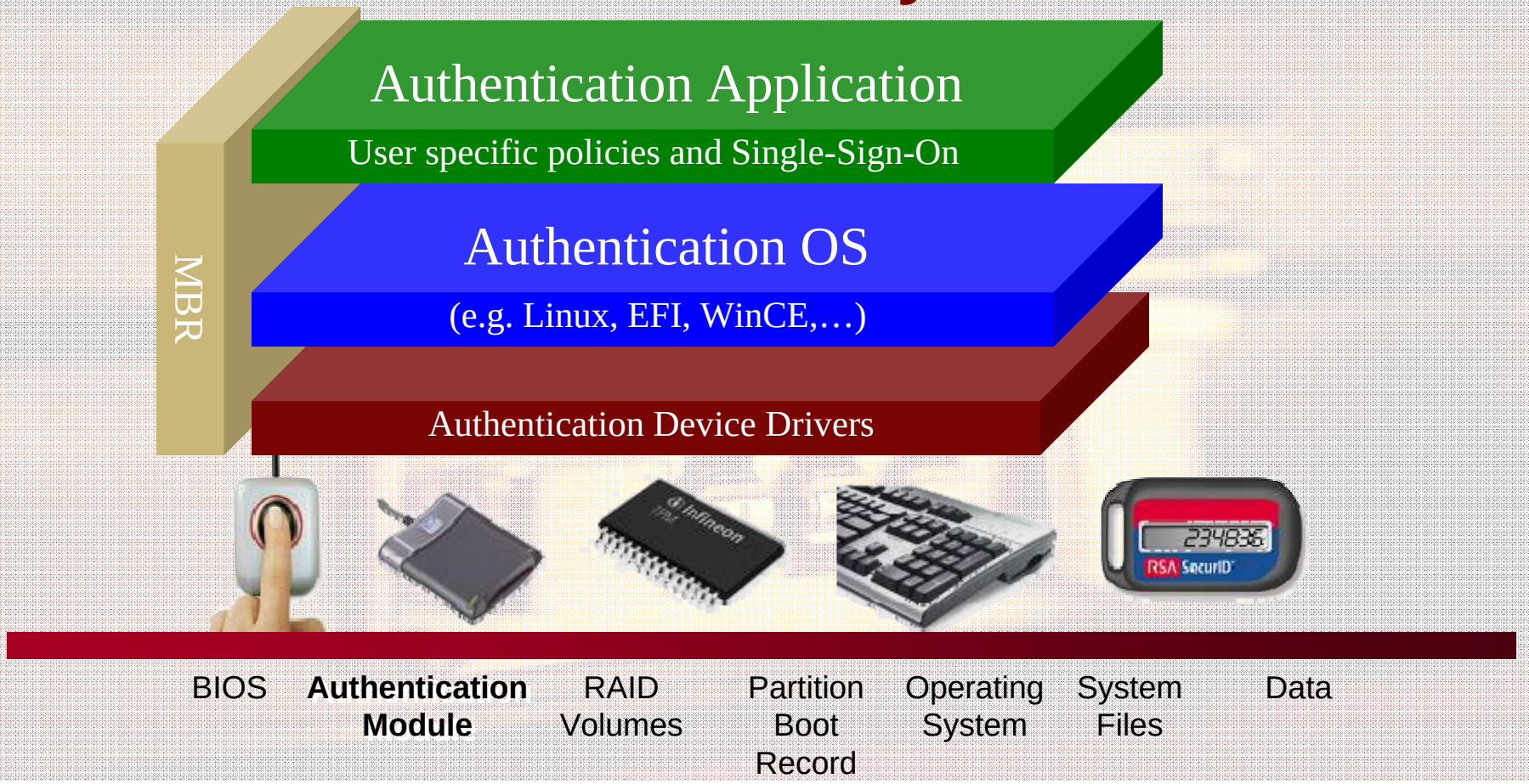


- TPM is something you have
  - It has a unique non-spoofable platform identifier
  - An authentication challenge with TPM means an attacker who knows your password, but doesn't have your PC can't impersonate you.
- It also means the attacker may want to steal your PC, BUT…
  - Only if they can circumvent its authentication subsystem

TRUSTED COMPUTING GROUP™

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

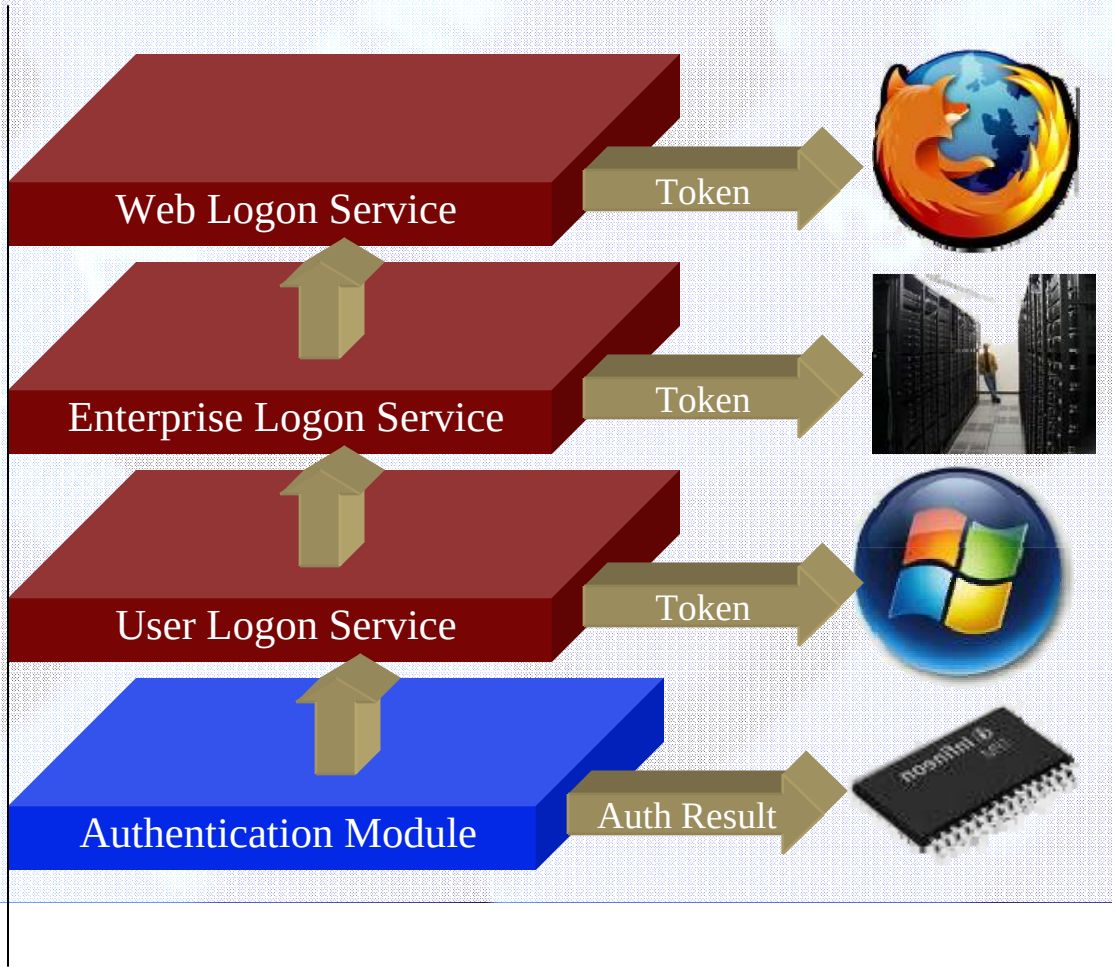
Pre-boot Authentication Module Software Layers



Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Single Sign On Means User Authenticates Once

- Pre-boot Passwords
  - Disk Drive(s)
  - BIOS Console
- Operating System Login
  - User and Administrator
- Enterprise Access
  - VPN
  - Email
- Web Server Login
  - Shopping
  - Banking
  - Broker
  - Entertainment



Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Summary

- Pre-boot “authentication module” is like a locker that contains a universal remote control…
- Robust multi-factor authentication on the *locker* ensures all buttons on the remote are only accessed by the right person
- Platform Authentication provides another factor of authentication that links the *locker* to the *universal remote*

TRUSTED COMPUTING GROUP™

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

More Information on TCG

- New Working Groups
  - Authentication
  - Storage
- Infrastructure Working Group
  - Management of trusted drives, devices and platforms
- www.trustedcomputinggroup.org



Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.

Backup

Copyright© 2007 Trusted Computing Group - Other names and brands are properties of their respective owners.