Intel® Protected Access Architecture (IPAA)
http://developer.intel.com/design/security/paa/paa.htm

Luke Girard
Senior Architect - Intel Corporation
Introduction

Laptop theft is a growing concern

7% ($1B) of laptops stolen in 1996

Information on stolen laptops valued at $15B

Chubb 1998

…A Visa U.S.A, Inc. executive was hospitalized recently when thugs beat him up in a hotel parking lot and took his laptop...

Chubb 1998

Theft of Qualcomm chairman's laptop provides security lessons for users

Computer World 8/3/98

“Rising laptop theft tacks on $150 a box”

Computer World 9/19/2000

Safeware, The Insurance Agency '97


Cost of Laptop Theft ($M)

0 100 200 300 400 500 600 700 800 900 1000
“PC Security” Today

**Asset**
- Physical
  - Cables, Locks

**Prevention**
- “Screamers”
  - Motion Detectors
  - Radio “Leashes”

**Retrieval**
- “Phone Home” service

**Deterrence**
- Boot Block Modifiers
- BIOS Password

**Data**
- File & Directory Encryption (OS-present)
- ATA-3 Password

Usually Not Enabled

Current theft deterrence tools are not simple or ubiquitous
Improved Authentication

- Enforce pre-OS, manage OS-present
- Multiple authentication factors
- Common user authentication I/F
- Protected data store
- Ease-of-use
- TCO (Total Cost of Ownership)

Improved User Authentication = Greater confidence in user identity
Overview of Architecture (IPAA)

Entry → POST → Load OS

- BIOS UA Applet
  - UA API
  - STO-API
  - Finger Print SP
  - Smart Card SP
  - Other SP
  - Remote SP
  - Authentication HW
  - Storage
  - Token
  - Template Storage

- Control Layer
- Abstraction Layer
- Service Provider Layer
- Hardware Layer

Intel Labs
Benefits of Architecture (IPAA)

- Modular/Extensible
- Flexible authentication device support
- Flexible protected storage support
- Allow OEM, BIOS, and vendor differentiation
- Promotes strengthened pre-OS user authentication
- Supports remote management
- Supports pre-OS media protection
- Improves Ease-of-Use and TCO
- Solutions portable across platforms
- Supports finer authorization granularity
- Reduces testing, validation, and evaluation
- Combines with other security capabilities such as Intel’s PXE/BIS
Proposed IPAA Boot Flow

Pre-boot
- Initialize
- Authenticate User
- Unlock

OS-present
- Load OS
- Authenticate User
- Support Encrypted File System

Non-volatile Protected Storage

Hard Disk Drive

Rainbow Technologies*

GemPlus*
Summary

- Laptop theft is an issue

- IPAA designed specifically to deter laptop theft
  - Improved user authentication
  - Pre-OS enforcement
  - Flexible authentication device and protected storage support
  - Differentiated solutions

- IPAA specifies a common software interface

- IPAA Specification and SDK available now

- Additional PC Platform security and contact info
  - developer.intel.com/design/security
Questions?