An Opt-in Strategy for a Safer Computing Platform

Ernie Brickell

Intel

9/17/03

Agenda

- Motivation for an opt-in strategy
- Opt-in and functionality choices
- User experience for opt-in
- System functionality required

Motivation for Opt-in Strategy

- A safer computing platform has hardware security features to enable new security functionality
- Concern: A user may not desire all of the security functionality
- Goal: Give the customer control to select which security features to enable

Security functionality by choice rather than by mandate.

Functionality of TPM

TPM – Trusted Platform Module
– Security processor added to motherboard

- Create, use, and protect cryptographic keys
- Random number generator
- Record software and BIOS environment in Platform Configuration Registers (PCRs)
- Sealed storage
  - Encrypt data and specify PCRs
  - Decrypt only when the PCRs match specified values
- Attestation

Attestation

Attestation

- –Signs software (and BIOS) environment recorded in the TPM
- –Signature by Attestation Identity Key (AIK)
- –Provides description of hardware from platform certificate

- Useful in many usage models
  - Corporate remote access
  - Protection of medical records
  - Assists users in establishing trust in platform

Optional Attestation

- Some users may not require attestation
- These users may prefer that attestation is not enabled on their platform
- With attestation turned off, other security advantages of the TPM can still be available
  - Better protection of cryptographic keys
  - Secrets sealed to a specific software environment

Attestation can be optional and selected by the user.

Agenda

- Motivation for an opt-in strategy
- Opt-in and functionality choices
- User experience for opt-in
- System functionality required

Opt-in Choices

- User can Opt-in to enable TPM
  - Activate TPM
  - Establish owner of TPM
    - Set owner authorization value
- Owner control of TPM features
  - Enable TPM to perform attestation
  - Enable specific software environments to use TPM
  - Fine-grain control of TPM
    - Specify which software environment (PCR values) can use which TPM capabilities
      - Ex. 1. Allow sealed storage and attestation
      - Ex. 2. Allow sealed storage without attestation

Agenda

- Motivation for an opt-in strategy
- Opt-in and functionality choices
- User experience for opt-in
- System functionality required

Security Feature Opt-in Requirements

- Owner must make initial opt-in choice after possession or at point of purchase
- Owner must have obvious means to control choice.
- Security feature changes require positive confirmation from owner
- Security feature selection must be sticky across reset
- Software must not control security feature selection

Additional Desires

- Desirable not to require user activated entrance into BIOS Setup
  - Some users are unfamiliar
- Desirable to use existing hardware infrastructure
  - I.e. no new hardware button

Physical Presence

Physical Presence – a user action that can't be performed by software

- **Required to change some opt-in settings**
  - Enable TPM
  - Establish owner
- **Implementation examples of physical presence**
  - Physical button on PC
  - Selections made during BIOS setup

Getting to BIOS Setup for Opt-in

- User indicates in OS that he wants to change his option states
- Flag is set that is readable from BIOS
- System reboots
- If FLAG is set, BIOS puts up a UI to let user select which security features to enable.
  - If flag is not set, then the BIOS does not put up a UI
- User selects security features, and then asked to confirm
- If user confirms, then security feature settings are permanent until user changes them
- FLAG is turned off
- System reboots and this time the UI is not displayed

Benefits of Method

- Does not require user to know how to enter the BIOS setup
- Changes in the security features settings are protected by the BIOS
- Software cannot modify the security feature settings
- BIOS could include software for fine-grain control of security features
  - Administrator Module

Administrator Module

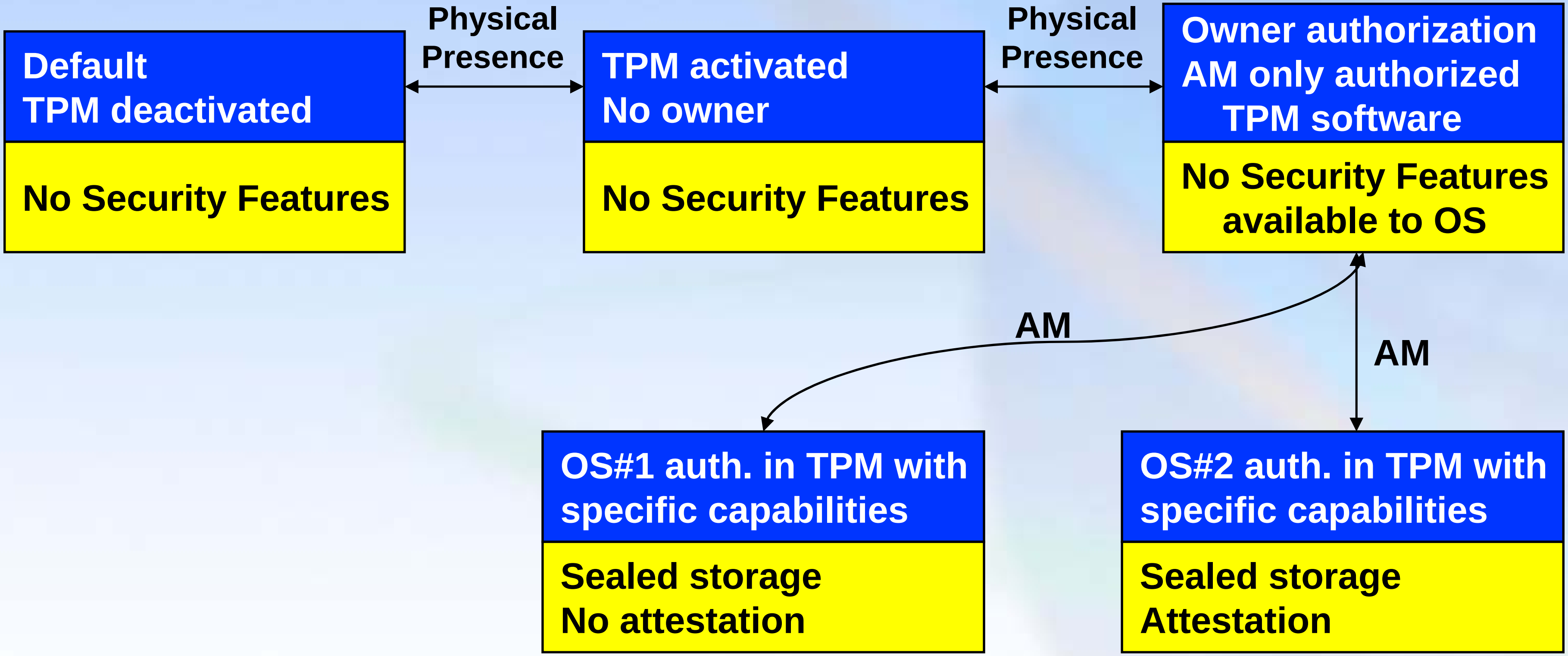
Administrator Module – Software which provides the user with controls to modify security feature states

- **Administrator Module is used after the user has chosen to use the TPM.**
- **Implementation choices for Administrator Module**
  - **BIOS code**
  - **Protected code**
- **Typical controls provided by Administrator Module**
  - **Allow attestation**
  - **Set which software environments can use TPM and which features they can use**

Use of Administrator Module

- OEM ships with a Administrator Module.
- Owner opts-in to use of TPM using physical presence
- Administrator Module is only software stack allowed to use TPM
- Owner uses Administrator Module to enable more software to use TPM and to specify security features permitted for each software environment

Security Feature Opt-in



Default
TPM deactivated

No Security Features

Physical
Presence

TPM activated
No owner

No Security Features

Physical
Presence

Owner authorization
AM only authorized
TPM software

No Security Features
available to OS

AM

AM

OS#1 auth. in TPM with
specific capabilities

Sealed storage
No attestation

OS#2 auth. in TPM with
specific capabilities

Sealed storage
Attestation

AM – Administrator Module

Agenda

- Motivation for an opt-in strategy
- Opt-in and functionality choices
- User experience for opt-in
- System functionality required

System Requirements for Opt-in Strategy

- Providing the implementation of opt-in through physical presence
- Implementation of an administrator module
- Security feature settings in BIOS that are sticky across reset

Summary

- Owner must take positive action to enable security functionality of TPM
- Owner can specify to use only the local security functionality, and not use attestation
- User choice can be implemented with a reasonable user experience

Thank you for attending.

Please fill out the Session Evaluation Form.