





Trusted Computing in Drives and Other Peripherals

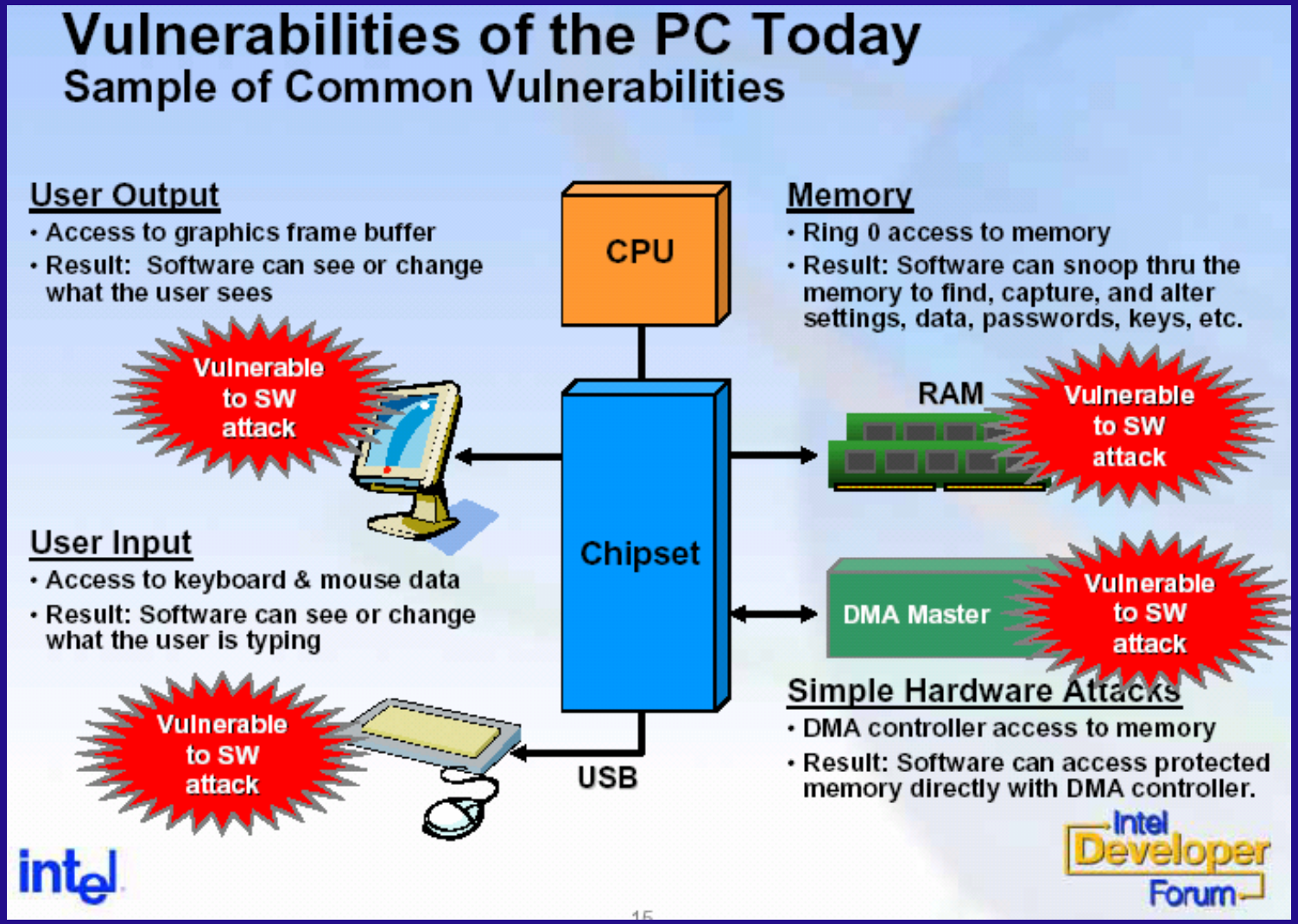
Michael Willett

TCG and Seagate

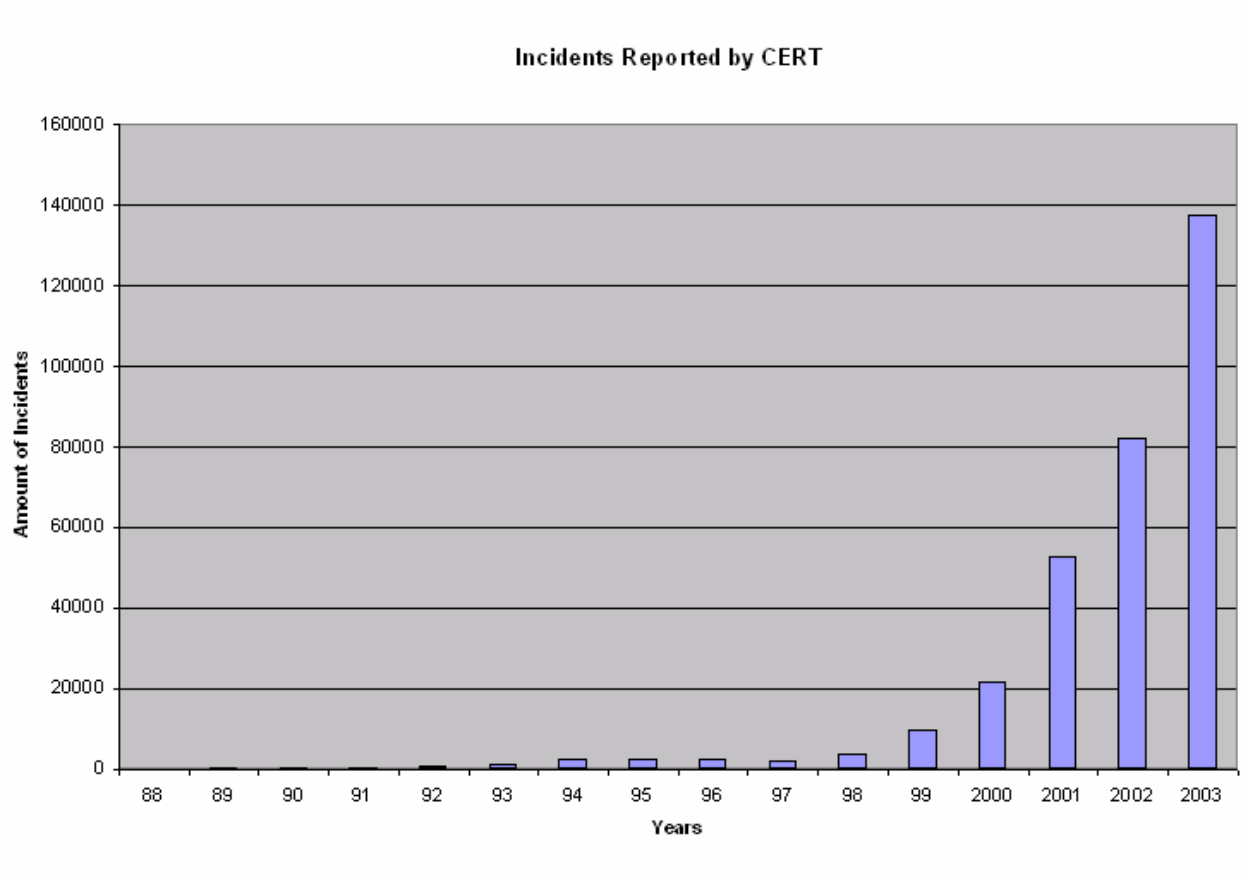
12 Sept 2005

TCG Track: SEC 502

The Need for Trusted Computing



The Real World



- **Innovation is needed:**
  - **Client software and hardware**
  - **Networks**
  - **Infrastructures**

- Trust - doing what was intended

- Cryptographic SIGNING
  - PlaintextMessage + Signed(Hash(PlaintextMessage))
    - Hash = Reduces message to 20 Bytes (2^160th number)
    - Sign = Encrypts with a private key that only the corresponding public key can decrypt and verify
  - Microsoft signs the Microsoft software proving it is the software from Microsoft…
  - X signs Y and Y signs Z -- **Chain of Trust**
- An X.509 Certificate is a cryptographically SIGNED attestation of a fact or claim
  - Basis for Trust in ALL BANKING WORLDWIDE
  - Basis for Trust in Windows and Linux and Web

Root of Trust

- Hardware that
  - **you cannot change**
  - **can sign**

  and therefore start off a chain of trust.
- A TPM (trusted platform module) is a tiny processor on the motherboard that can sign and can't have the firmware modified.
- Disk Drives can be roots of trust since you can't upload firmware to change them.
  - Additional "hardening" needed

Introduction to the Trusted Computing Group

The Trusted Computing Group (TCG) is an industry standards body, comprised of computer and device manufacturers, software vendors and others with a stake in enhancing the security of the computing environment across multiple platforms and devices.

Conceptual Motivation

- Internet-connected devices will always have un-trusted activities going on inside, so …
- Create internal trustable sub-units and secure paths … the building blocks, so …
- Other processes use the building blocks for sensitive computations, so…
- In the future, you (IT) can know the trusted subsystem won't be compromised even if exposed to Internet (and other) attacks (or accidents).

TCG Organization

Board of Directors
Jim Ward, *IBM*, President and Chairman

Marketing Workgroup
Brian Berger, Wave

Technical Committee
Graeme Proudler, *HP*

Best Practices
Jeff Austin, *Intel*

Advisory Council
Invited Participants

Administration
VTM, Inc.

Public Relations
Anne Price, *PR Works*

Events Marketing Support
VTM, Inc.

TPM Work Group
David Grawrock, *Intel*

TSS Work Group
David Challener, Lenovo

Mobile Phone WG
Panu Markkanen, *Nokia*

Peripherals WG
Colin Walter, Comodo

Server Specific WG
Larry McMahan, *HP*

Conformance WG
Manny Novoa, *HP*

PC Client WG
Monty Wiseman, *Intel*

Infrastructure WG
Thomas Hardjono, Verisign

PDA WG
Jonathan Tourzan, *Sony*

User Auth WG
Laszlo Elteto, *Rainbow*

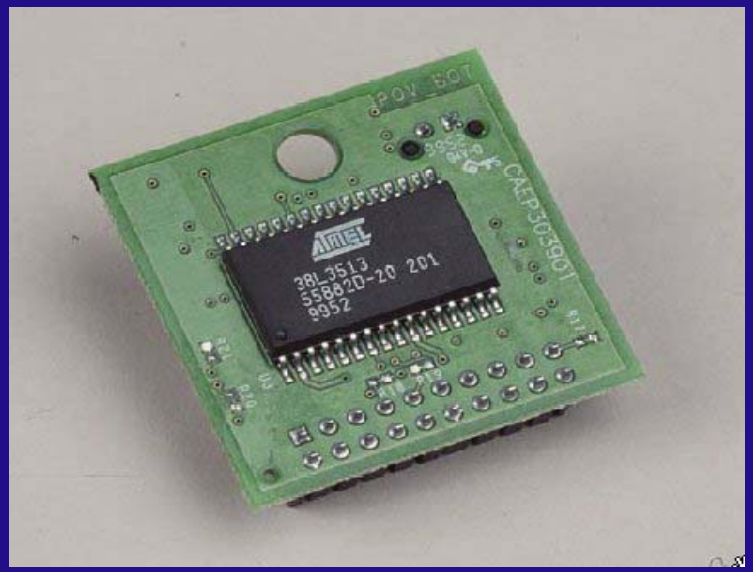
Storage Systems
Robert Thibadeau, *Seagate*

TRUSTED COMPUTING GROUP™

Trusted Platform Module

TPM v1.2 functions include:

- Store platform status information
- Generates and stores a private key (+ derivative keys)
- Hashes files using SHA-1
- Creates digital signatures
- Anchors chain of trust for keys, digital certificates and other credentials

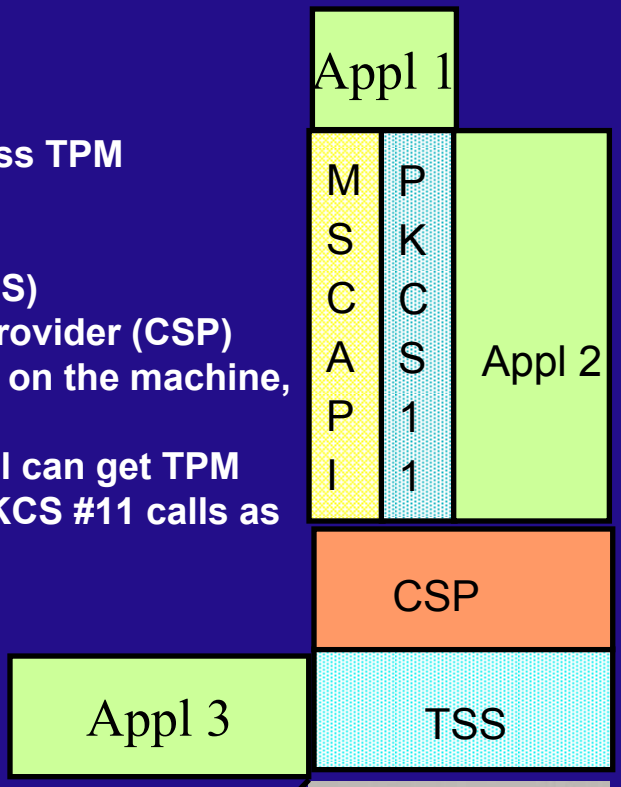


Simplified Software Stack for TCG-enabled devices

Applications (Appl) can access TPM Services thru:

- **The TCG Software Stack (TSS)**
- **If a Cryptographic Service Provider (CSP) package that uses the TSS is on the machine, it can use the CSP**
- **If a CSP is available, the appl can get TPM services thru MSCAPI and PKCS #11 calls as well**

How and where to connect to TPM services depends on mission, skills and what assumptions you make about what tools are available on the platform





MSCAPI and PKCS #11 are well-known APIs for requesting cryptographic services

The CSP provides a menu of cryptographic services

The TSS provides a standard interface to the TPM

The TPM:

- **performs all TPM v1.2 functions**
- **stores private keys**
- **hashes files using SHA-1**
- **creates digital signatures**
- **anchors chain of trust of keys, digital certificates and other credentials**

TCG System Benefits

- Benefits for today's applications
  - **Measurable security for data (files) and communications (email, network traffic)**
  - **Hardware protection for Personally Identifiable Information (Digital IDs)**
  - **Strong protection for passwords : theft of data on disk provides no useful information**
  - **Lowest cost hardware security solution : no token to distribute or lose, no peripheral to buy or plug in, no limit to number of keys, files or IDs**
- Benefits for new applications
  - **Safe remote access through a combination of machine and user authentication**
  - **Enhanced data confidentiality through confirmation of platform integrity prior to decryption**

TPM Provides Enhanced Protection for Business

Usage	Protection	Examples
Hardened Data Protection	Helps protect the integrity and confidentiality of data assets through hardware-based protection of encryption keys	**Email, file encryption**
Hardened Electronic Digital Signatures	Increases confidence in digital signature operations by providing hardware-based protection of Digital IDs. Prevents cloning by performing signature operation in tamper resistant hardware.	**Online purchases, contracts**
Hardened User Authentication	Helps protect integrity and confidentiality of user login credentials. Can also act as the “something you have” in multi-factor authentication scenario	**Can replace smart cards, secure tokens**
Hardened Platform Authentication	Helps to ensure that only authorized platforms and users gain access to corporate network and that security policy settings / security software haven't been attacked.	**Virtual Private Networks (VPN)**

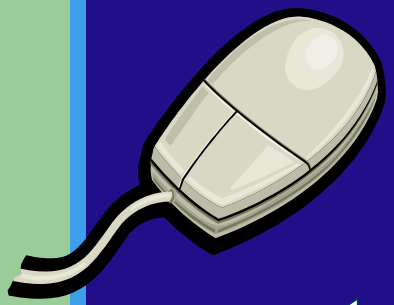
Value proposition speaks to urgent needs of security-minded businesses

TPM and OS Status

- Each TPM includes 16 Platform Configuration Registers (PCRs)
- Each register can be used to store status information about the condition of a component of the operating system (hash value)
- PCRs are set by a formal integrity process
- PCRs are used by comparing stored hash to current hash for the relevant component
  - If not equal, the component has been changed since the formal integrity process was executed

The purpose of the PCRs is to make it possible to determine if BIOS, drivers, loaders or other important elements of the OS have been changed since they were installed

Extending Trust to Platform Peripherals





Ability to interact with the Platform

Authentication/Attestation

LOW

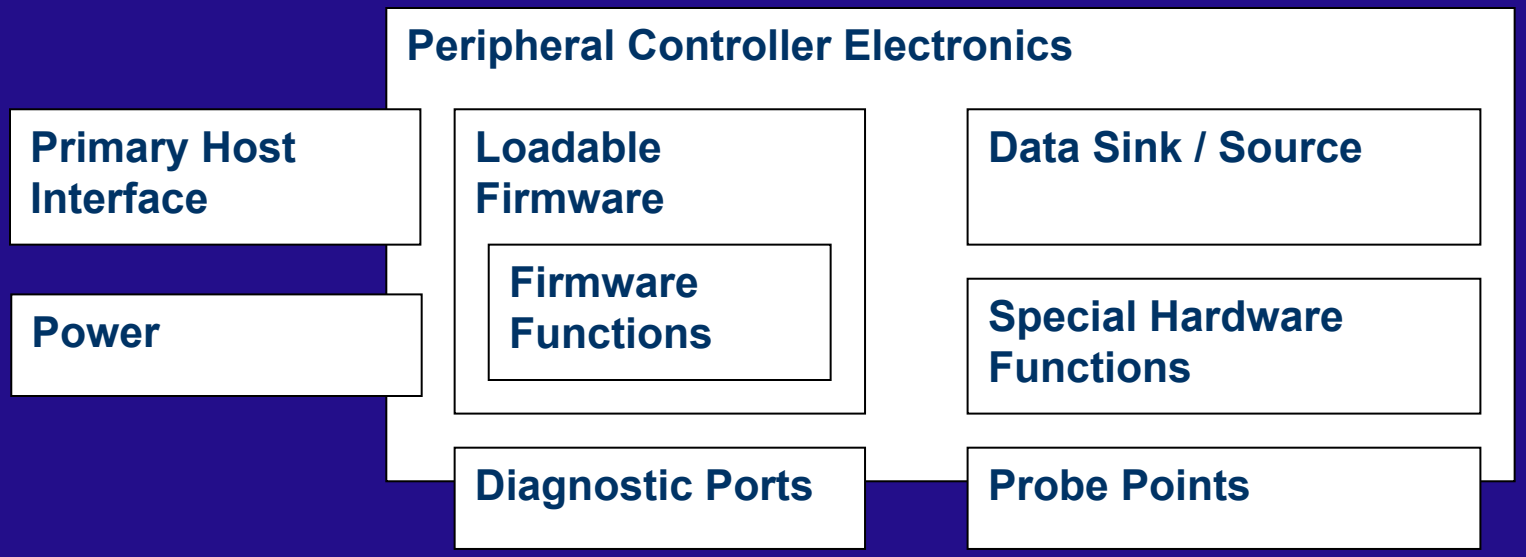
HIGH

Capability Level





General Risk Model of a Peripheral



Trust = systems operate as intended

Objective: Exercise control over operations that might violate trust

Needed: Trusted peripheral commands

Multi-Component Trusted Platform (MCTP)

Trusted Peripheral



Secure
Communications

Trusted Platform

TPM

Life Cycle: Manufacture, Own, Enroll, PowerUp, Connect, Use, …

Joint Work with ISO T10 (SCSI) and T13 (ATA)

TRUSTED SEND

(Protocol ID = xxxx .....)



TRUSTED RECEIVE

T10/T13 defining the "**container commands**"

TCG/Storage defining the "**TCG payload**"

Protocol IDs assigned to TCG, T10/T13, or reserved

Protocol ID = 0 and Credential

TRUSTED SEND

(Protocol ID = 0 …..)



TRUSTED RECEIVE

(Device Credential, ….)





Status: Container Commands (IN/OUT) and Device Credential Submitted to T10/SCSI (under review)

DEVICE CREDENTIAL

Field name	*Description*
Credential Serial Number	The unique serial number of the credential
Credential Validity Period	The time for which the credential is valid as determined by the issuer of the credential
Credential Issuer	The issuer of the credential
Credentialed Entity	Identifies the device to which the credential applies
Device public key	Holds the public key information for devices capable of asymmetric key operations
Revocation Information	Location of revocation information relevant to the credential.
Supported Protocols	Indicates which security protocols are supported by the device
Signature Algorithm	Algorithm identifier for the signing algorithm used to sign the credential
Signature Value	Contains a digital signature computed over all other fields of the credential.

Scope of Payload Commands w/ Protocol ID = "TCG"

- Establishing/managing communications:

  Secure Messaging, RPC

- Parameter management: "table" entries w/ Access Control

- Security management: Secure Partitions, Authority, ACLs

- Cryptography:

  digital signature, random numbers, key generation,

  encrypt/decrypt, hash

- Admin: clock, backup

Send/Receive w/Access Control

TRUSTED SEND

(Protocol ID = TCG .....)

TRUSTED RECEIVE

-Authentication and Access Control

-Protecting Hidden Storage and Trusted Drive security features

-Join TCG and help!!

Versatile Access Control per Command



Password

Biometrics

RSA Authentication

MAC Challenge/Response

TCG Storage/Peripherals Use Cases

- Enroll a Device with a Platform (establish trust)
  - Platform trusts peripheral, peripheral trusts Platform
- Set Security Policies on Device
- You can connect and disconnect device at will
  - TCG TPM on Motherboard and the Device recognize AND TRUST each other; user has to do nothing
- Building Blocks
  - “Hidden Space” Plus Versatile Access Control

TCG Storage Systems Use Cases (examples)

Full Disc Encryption

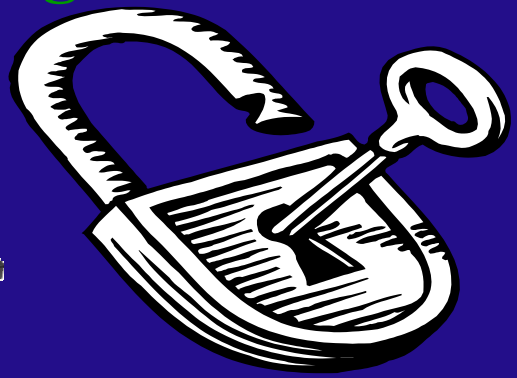
- -Laptop Loss or Theft
- -Re-Purposing
- -End of Life
- -Disk Erase Enhancement

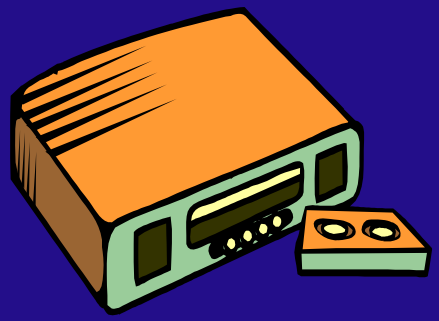


Crypto Key Management

DriveLocking







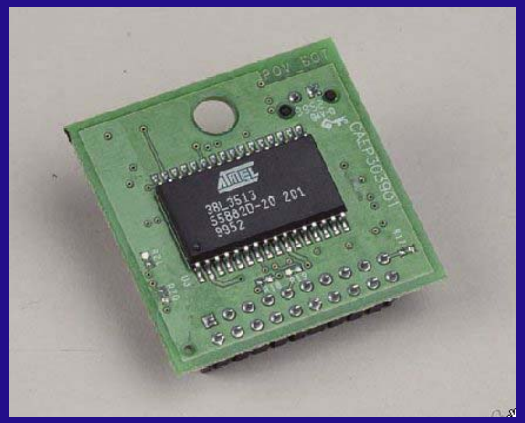
Personal Video Recorders

Forensic Logging

DRM Building Blocks

www.trustedcomputinggroup.org

THANK YOU!





QUESTIONS?