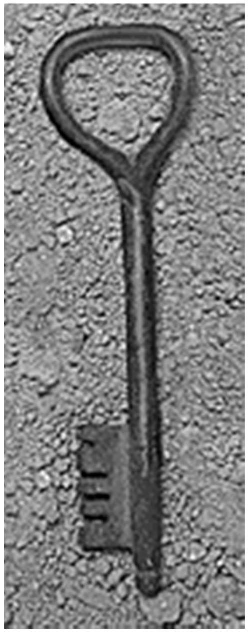
Trusted Computing



The TCG Guidelines

What is TCG?

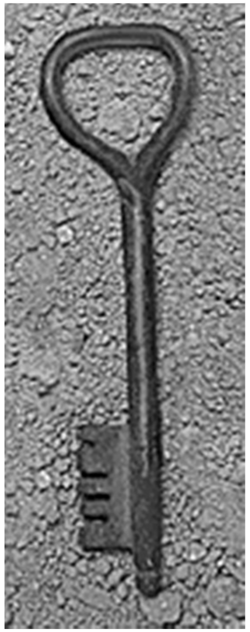
The Core Component - TPM

TPM provides:

- ♦ Secure Input & Output
- ♦ Memory curtaining / Protected execution
- ♦ Sealed storage
- ♦ Remote attestation

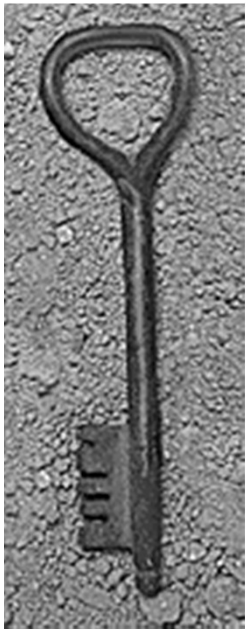
System Layout based on TCG

Controversy



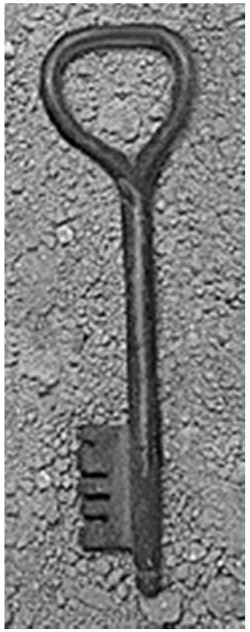
Why Are Systems Insecure?

- Commodity OS are too complex to build secure applications upon
- Commodity OS poorly isolate applications
- Only weak mechanisms for authentication, making secure distributed applications difficult
- No trusted path between users and programs



Idea: Trusted Computing

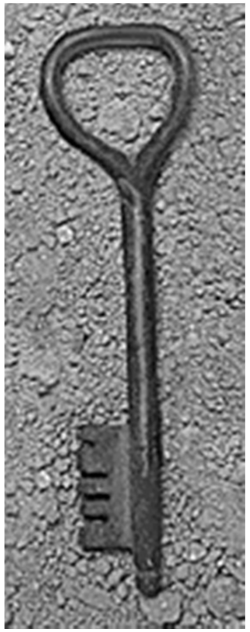
- Minimal trusted computing base
  - Implemented in a tamper-resistant hardware chip
- Provides basic security capabilities
  - Sealed storage
  - Remote attestation of machine′s state
  - Curtained memory
  - Secure input and output
- ‟Bootstrap″ security from kernel to applications
  - Prevent malicious code from running in the kernel
  - Remotely ‟attest″ that you running a particular software stack (from OS to applications)



Business Objectives

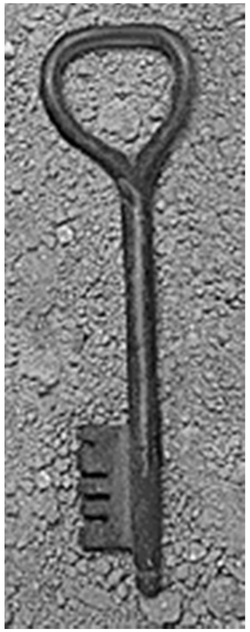
- ♦ Prevent use of unlicensed software
- ♦ Digital rights management (DRM)
  - – Prevent execution of unlicensed applications
  - – Idea: before a streaming service releases music for your computer, you must prove that there is no ripping software running in your execution environment
- ♦ Law enforcement and intelligence
- ♦ "The mother(board) of all Big Brothers"

- Lucky Green



Trusted Computing Group (TCG)

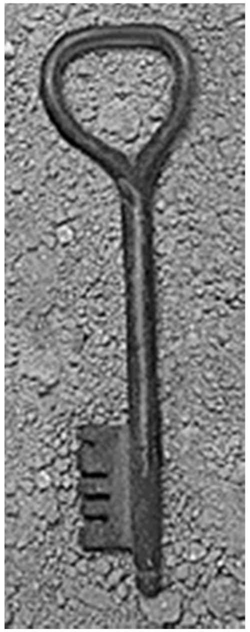
- Formed in Spring 2003, adopted the specifications of TCPA (Trusted Computing Platform Alliance), which was founded 1999
- Core members
  - AMD, Infineon, HP, IBM, Intel, Microsoft, Sun
- Mission
  - To develop ,define,and promote open standards for hardware-enabled trusted computing and security technologies
- http://www.trustedcomputinggroup.org



About the TCG(continued)

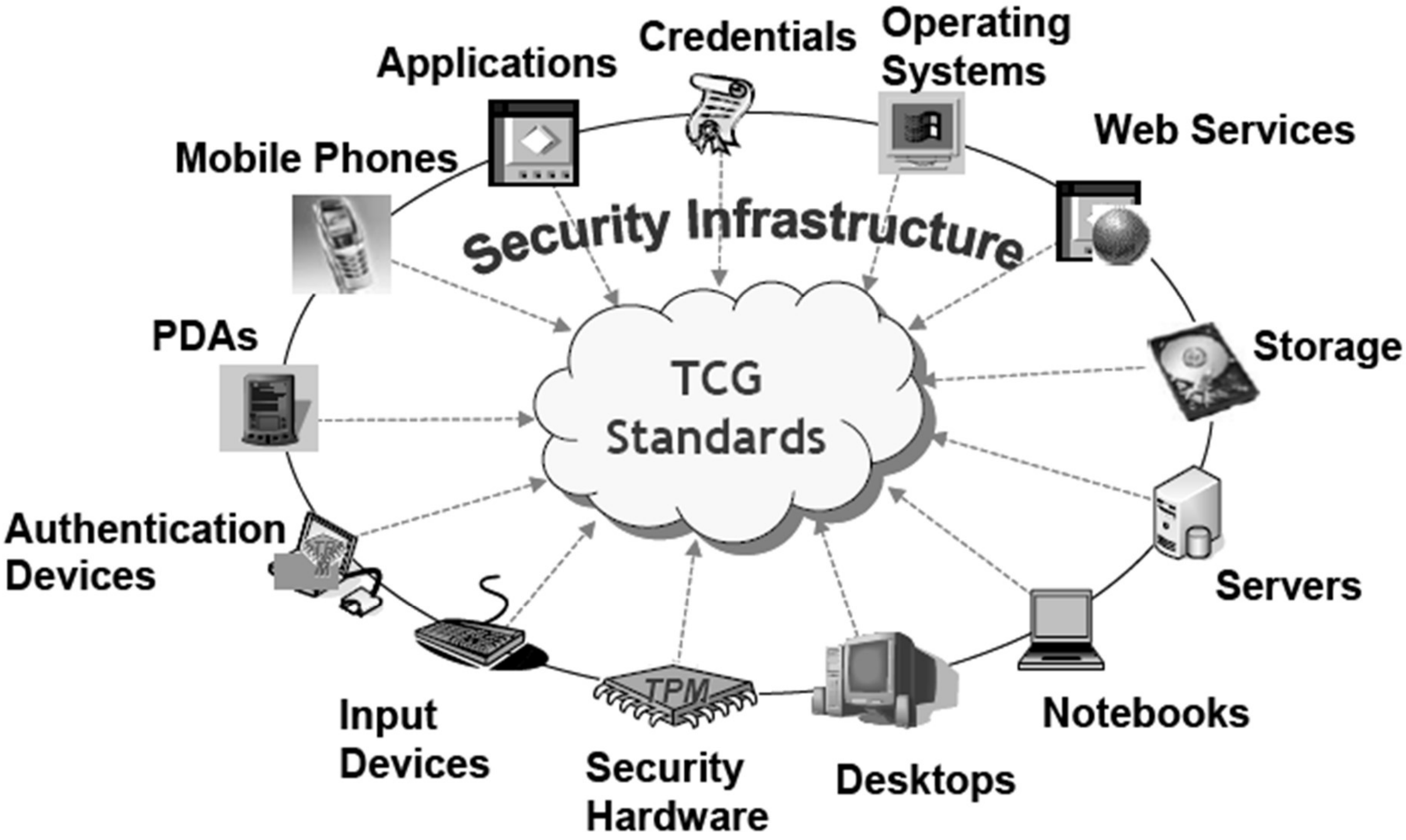
Groups of TCG

- Infrastructure
- Mobile
- PC Client
- Server
- Software Stack
- Storage
- Trusted Network Connect
- Trusted Platform Module(TPM)

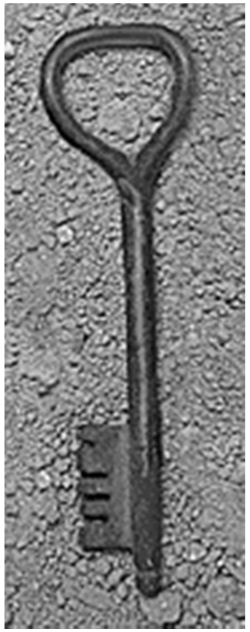


TCG Architecture Overview (continued)

Trusted Computing Security Ecosystem

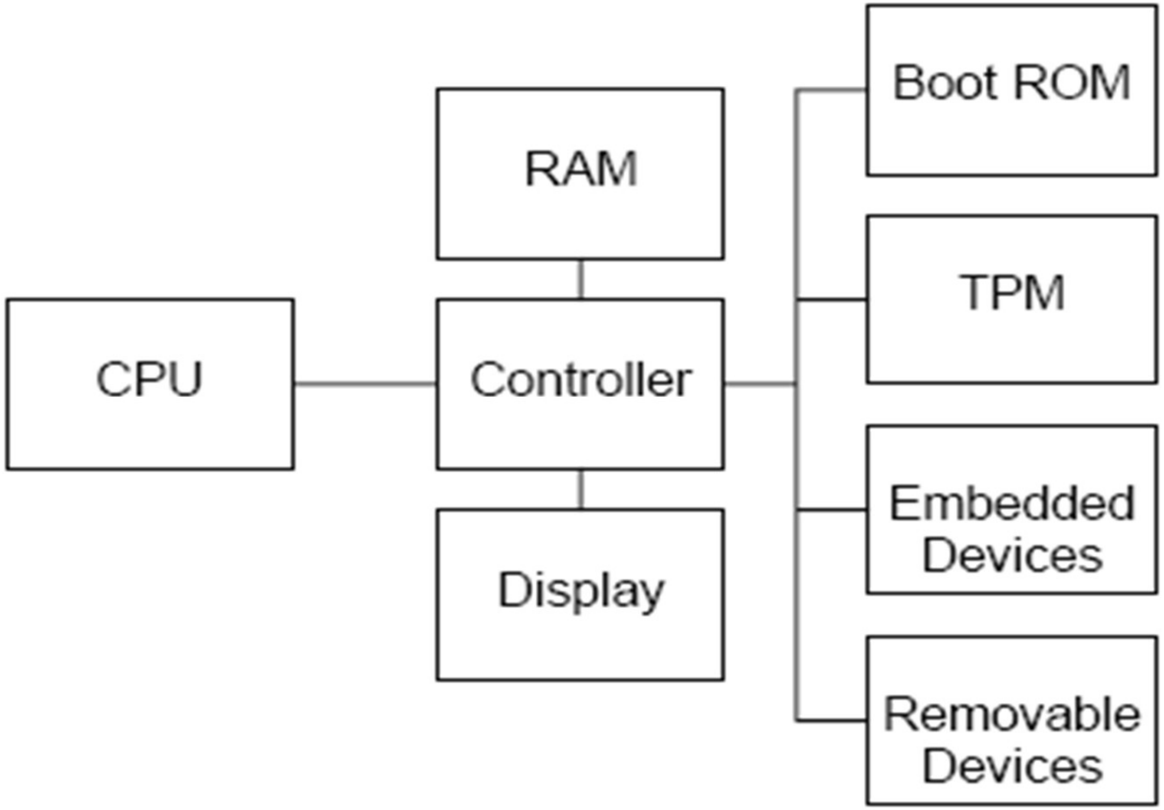


Source: TCG, 2006



TCG Architecture Overview (continued)

Reference PC Platform Containing a TCG Trusted Platform Modules



CPU

RAM

Controller

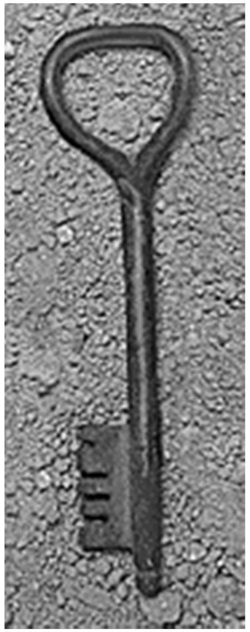
Display

Boot ROM

TPM

Embedded Devices

Removable Devices



The TCG Guidelines

What is TCG?

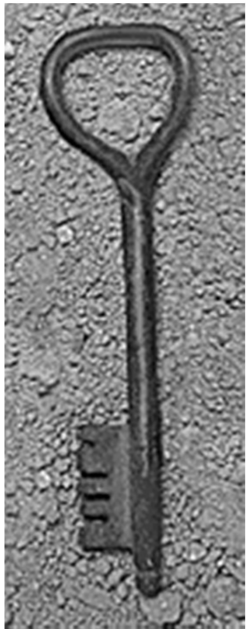
The Core Component - TPM

TPM provides:

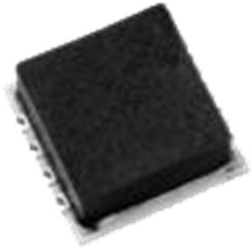
- ♦ Secure Input & Output
- ♦ Memory curtaining / Protected execution
- ♦ Sealed storage
- ♦ Remote attestation

System Layout based on TCG

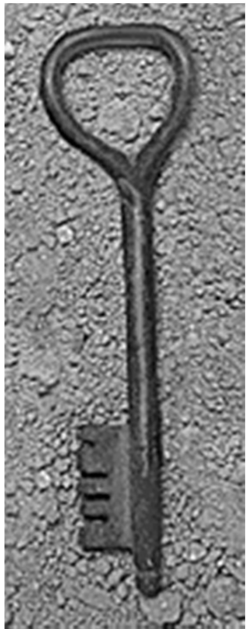
Controversy



Idea: Use Hardware

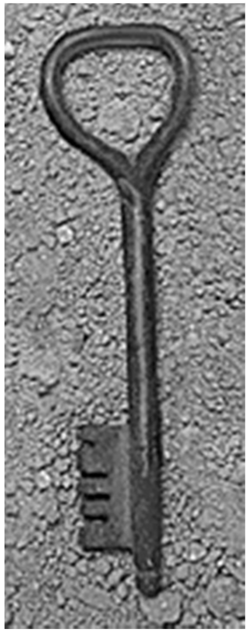


- ♦ Trusted Platform Module (TPM)
  - "Smartcard soldered to motherboard"
  - Cheap, fixed-function, tamper-proof hardware device
    - Contains at least an AES key and an RSA key pair
    - "Platform configuration registers" to store the hash of the currently running OS and maybe applications
- ♦ Must be close to the chipset
  - Involved in OS initialization; can't be a real smartcard
- ♦ Contains other security capabilities
- ♦ Requires changes to BIOS, OS, applications



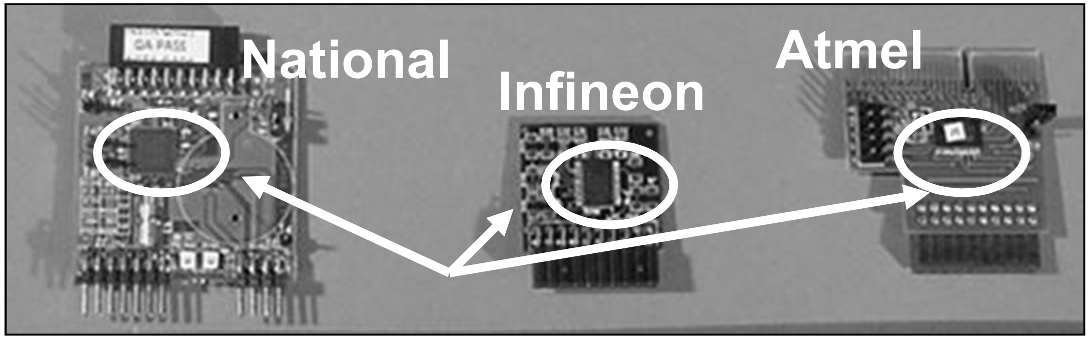
TPM in the Real World

- $7 chip
  - Many manufacturers: Atmel, Infineon, National, STMicro
- Installed in many desktops and notebooks
  - IBM/Lenovo, HP, Fujitsu
- Used in some secure systems software
  - File encryption: Vista, IBM, HP, Softex
  - Attestation for enterprise login: Cognizance, Wave
  - Single sign-on: IBM, Utimaco, Wave

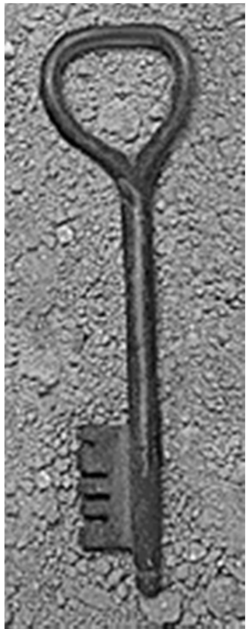


The TPM : a reality

Infineon, National Semiconductor, Atmel and ST Microelectronics already propose compatible TCG components

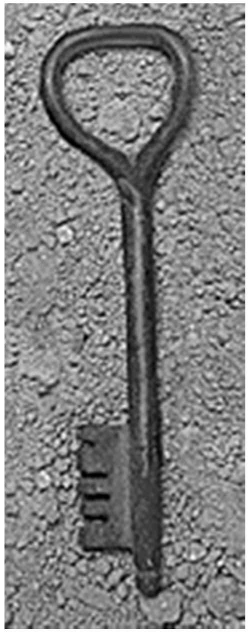


Infineon SLD9630TT TPM
Atmel AT97SC3201
National SafeKeeper PC21100
And others manufacturers soon like
ST Microelectronics ST19WP18-TPM

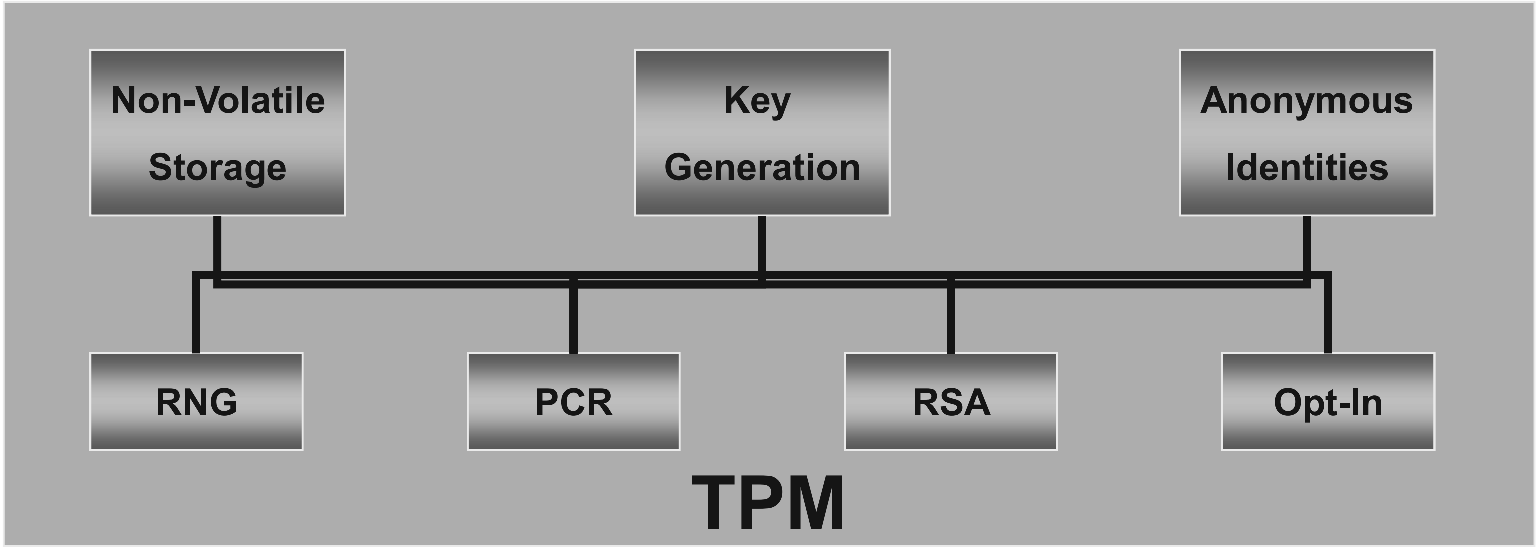


Core Features

- Separate protected execution environment for applications that need higher security
  - Strong process isolation
- Privileged cryptographic services for these apps
- Secure path to and from the user
- Big idea: "project trust" into the main OS



TPM Components



Non-Volatile Storage

Key Generation

Anonymous Identities

RNG

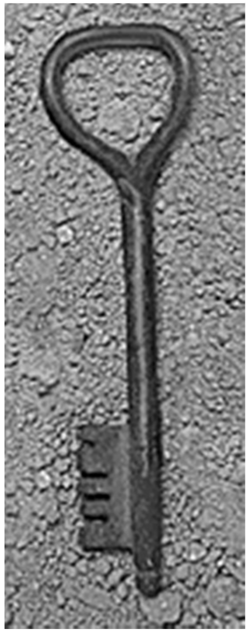
PCR

RSA

Opt-In

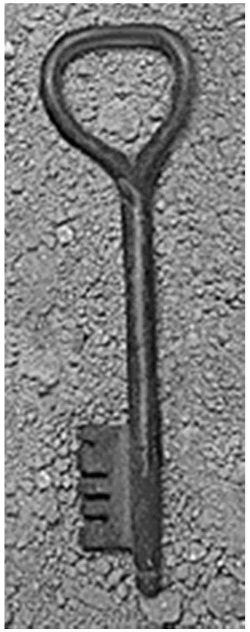
TPM

- ♦ Generate and use RSA keys
- ♦ Provide long-term protected storage of RSA root key
- ♦ Store measurements in PCR
- ♦ Use anonymous identities to report PCR status



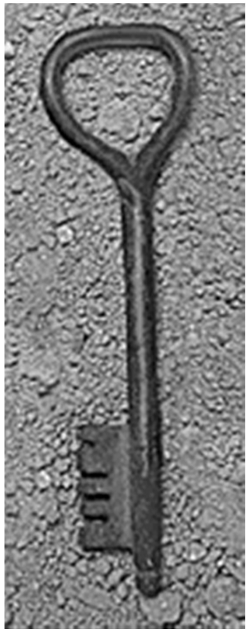
Non-Volatile TPM Memory

- ♦ Endorsement key (EK)
  - – Unique RSA key, created once for the life of the TPM at the time of manufacture
    - • Proves that the TPM is genuine
  - – Certified by TPM manufacturer
  - – Root of the attestation chain
- ♦ Storage root key (SRK) and owner password
  - – Generated when user takes ownership
- ♦ Persistent flags
  - – For example, has ownership been taken?



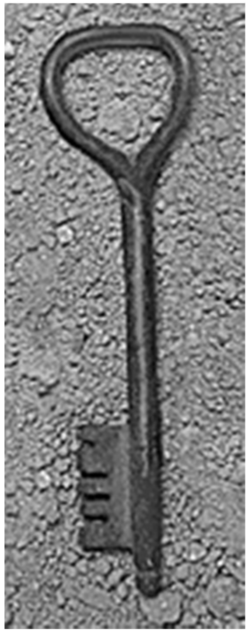
Code "Identity"

- In the trusted computing model, the host always knows what code is running on it
  - Can assign access rights to code identities
- Booting kernel causes its hash to be computed and stored in a read-only, tamper-proof register
  - "Platform configuration register" (PCR)
- Kernel recursively provides similar features for applications executing on the system
  - Can think of the hash of the code as code's identity



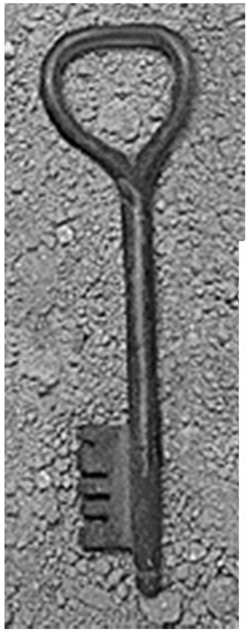
Platform Configuration Registers

- At least 16 PCRs on chip, each stores SHA-1 hash
- Initialized to default value (e.g., 0) at boot time
- PCR values can be read and updated at runtime
  - TPM_Extend(n,D) stores SHA-1(PCR[n],D) in PCR[n]
  - TPM_PcrRead(n) reads value of PCR[n]
- TPM can save PCR values on shutdown and restore them on restart
  - TPM_SaveState and TPM_Startup(ST_STATE)

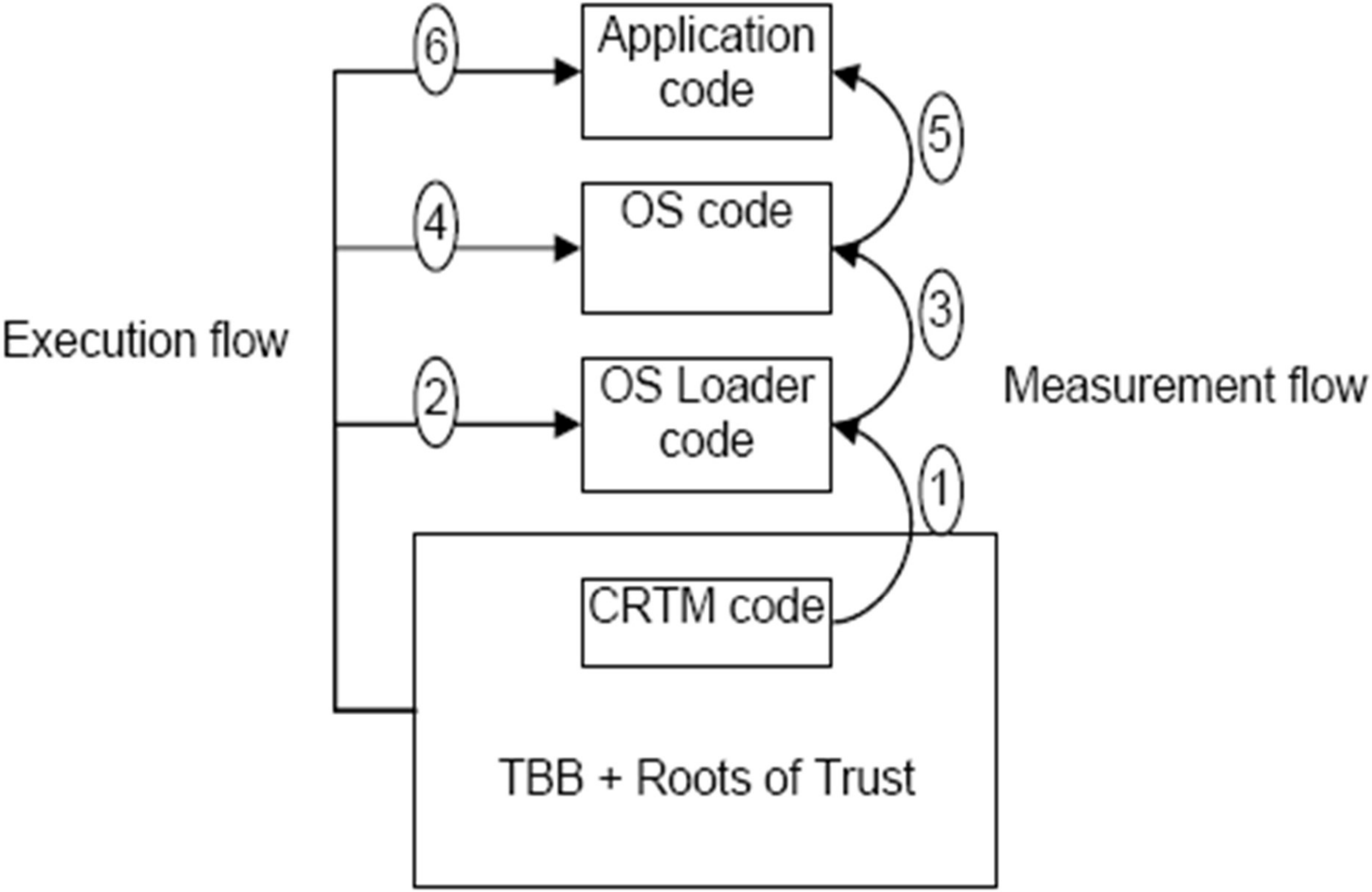


Bootstrapping the Trust Chain

- Secret key is embedded in hardware, signed (certified) by hardware vendor
- Hardware certifies firmware
- Firmware certifies boot loader
- Boot loader certifies OS
- OS certifies applications, virtual machines, etc.

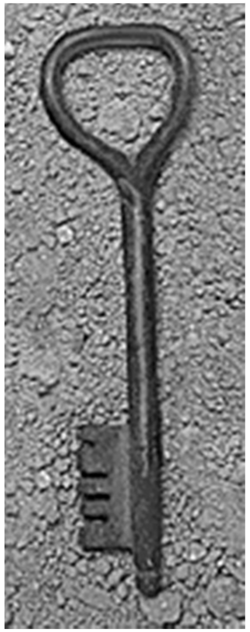


Transitive Trust



Execution flow

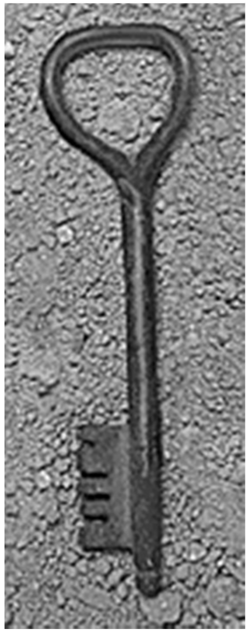
Measurement flow



Using PCRs

- ♦ PCR[n] initialized to 0 at startup
- ♦ BIOS boot block:
  - – Calls TPM_Extend(n, <BIOS code>)
  - – Loads and runs BIOS post-boot code
- ♦ BIOS:
  - – Calls TPM_Extend(n, <MBR code>)
  - – Loads and runs MBR
- ♦ Master boot record (MBR):
  - – Calls TPM_Extend(n, <OS loader code, config>)
  - – Loads and runs OS loader and so on…

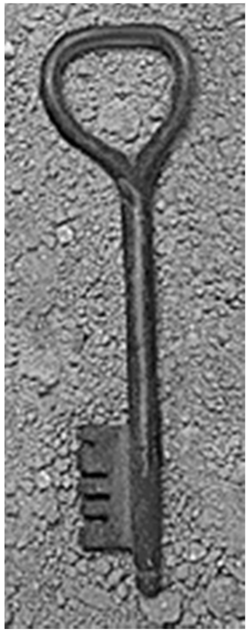
What does this operation do?



Component Certification

A component wanting to be certified...

- ♦ Generates public/private key
- ♦ Makes ENDORSE call to lower-level component
- ♦ Lower-level component generates and signs a certificate containing:
  - – SHA-1 hash of attestable parts of higher component
  - – Higher component′s public key and application data



The TCG Guidelines

What is TCG?

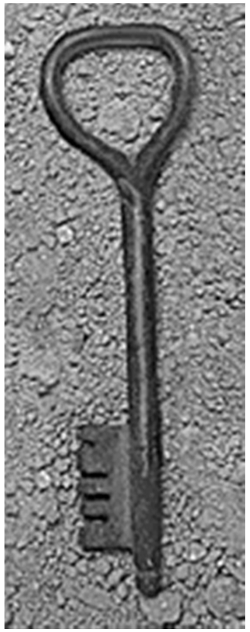
The Core Component - TPM

TPM provides:

- ♦ Secure Input & Output
- ♦ Memory curtaining / Protected execution
- ♦ Sealed storage
- ♦ Remote attestation

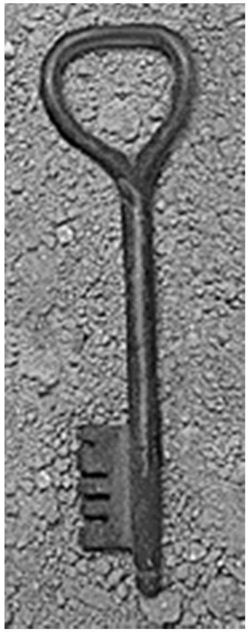
System Layout based on TCG

Controversy



Secure Input and Output

- Isolation, sealed storage and attestation aren′t enough to keep secrets safe
- Users can be fooled into thinking they′re talking to a trusted system when they′re not
- I/O channels must be protected from sniffing
  - Keyboard, frame buffer, etc.
- Protected path between user and application



The TCG Guidelines

What is TCG?

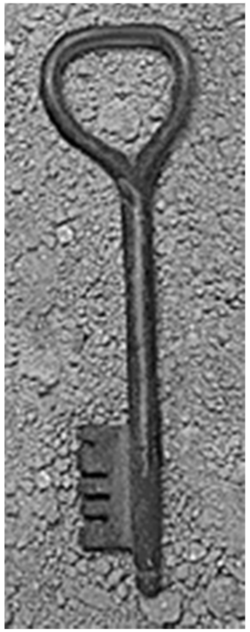
The Core Component - TPM

TPM provides:

- ♦ Secure Input & Output
- ♦ Memory curtaining / Protected execution
- ♦ Sealed storage
- ♦ Remote attestation

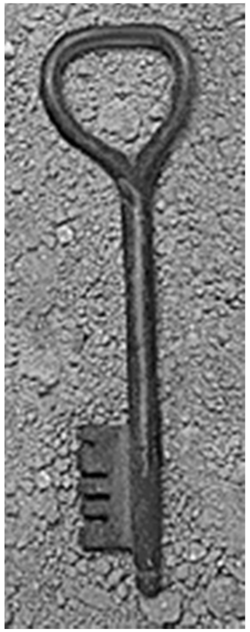
System Layout based on TCG

Controversy



Memory Curtaining

- Memory curtaining has the hardware keep programs from reading or writing each other′s memory
- Even OS access is denied
- Information is secure from an intruder with control over OS



The TCG Guidelines

What is TCG?

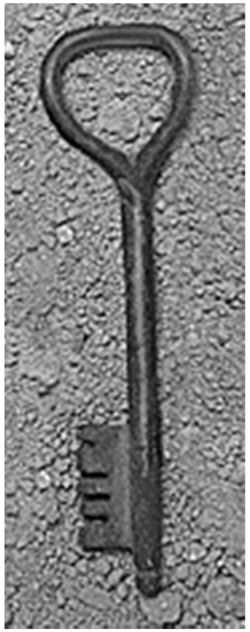
The Core Component - TPM

TPM provides:

- ♦ Secure Input & Output
- ♦ Memory curtaining / Protected execution
- ♦ Sealed storage
- ♦ Remote attestation

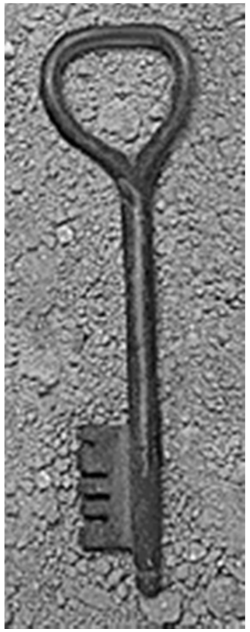
System Layout based on TCG

Controversy



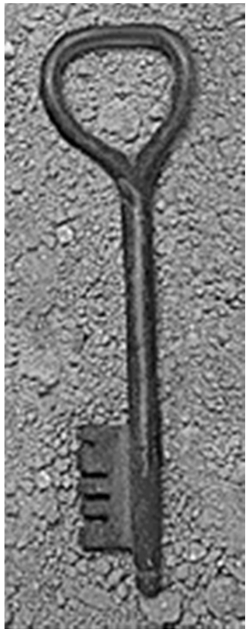
Sealed Storage

- ♦ Protects private information with encryption from a key derived from corresponding hardware and software
- ♦ Data can only be read by the same combination of software and hardware
  - – Example: Web server′s SSL private key that can only be read by an unmodified copy of the server′s code
- ♦ Prevent reverse-engineering of software
  - – If MBR or OS changed, software won′t load
- ♦ Not a perfect solution
  - – Updating OS, application, config requires re-sealing



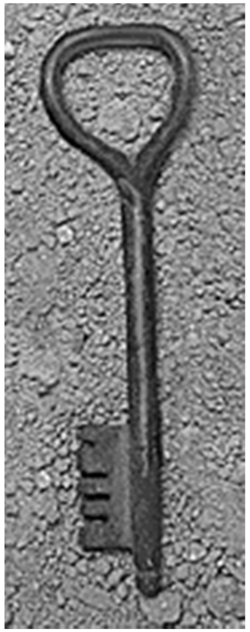
Sealing Process

- TPM_TakeOwnership(OwnerPassword, …)
  - Creates 2048-bit RSA storage root key (SRK)
  - Can only be done once (by IT dept or computer owner)
- Optional: TPM_CreateWrapKey
  - Create more RSA keys certified by SRK
  - Each key identified by a 32-bit keyhandle
- TPM_Seal – encrypt data using RSA key
  - Arguments: keyhandle (which TPM key to use), password for using that keyhandle, PCR values to embed, symmetric key
  - Returns encrypted "blob" (under symmetric key)



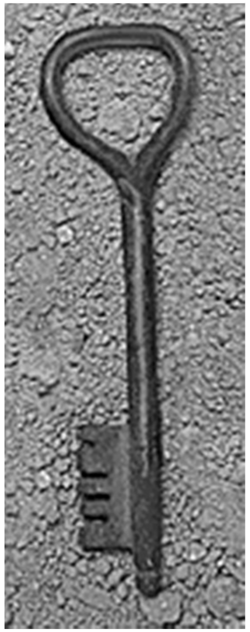
Key Features of Sealed Storage

- TPM_Unseal decrypts the "blob" <u>only</u> if current PCR values match those in the blob
  - Only certain applications can decrypt the data
  - Changing MBR or OS kernel changes PCR values
- Why can't attacker disable TPM until after boot, then extend PCRs with whatever he wants?
  - Root of trust: BIOS boot block
- Rollback attacks are possible
  - For example, "undo" security patches by opening blob with an old version of application



TPM Counters

- ♦ TPM must support at least four hardware counters
  - – Increment rate: every 5 seconds for 7 years
- ♦ Provide time stamps on encrypted blobs
- ♦ Support DRM applications
  - – Example: "music will play for 30 days only"



The TCG Guidelines

What is TCG?

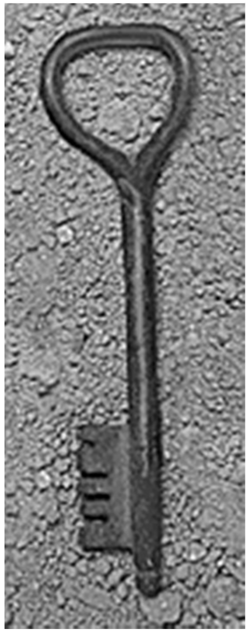
The Core Component - TPM

TPM provides:

- ♦ Secure Input & Output
- ♦ Memory curtaining / Protected execution
- ♦ Sealed storage
- ♦ Remote attestation

System Layout based on TCG

Controversy

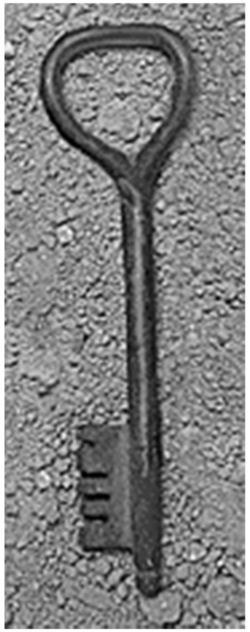


Remote Attestation

Are You A Dog?

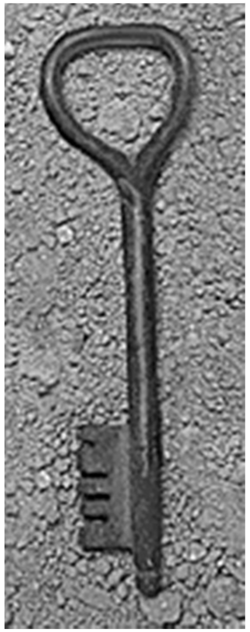
- On the Internet no one knows you are a dog

- On the Internet no one knows if you have a proper configuration



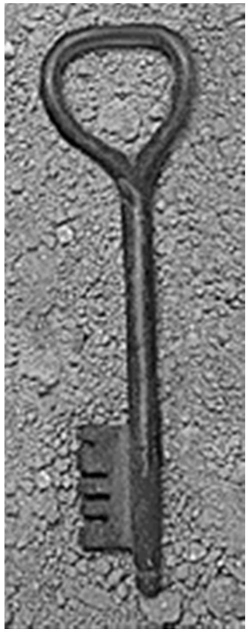
Attestation Definition

- ♦ Remote attestation allows changes to user′s computer to be detected
- ♦ Hardware generates a certificate stating what software is currently running
- ♦ Combined with public-key encryption to present certificate to remote party
- ♦ Information that could be attested to includes:
  - – HW on platform
  - – BIOS
  - – Configuration options
  - – And much more



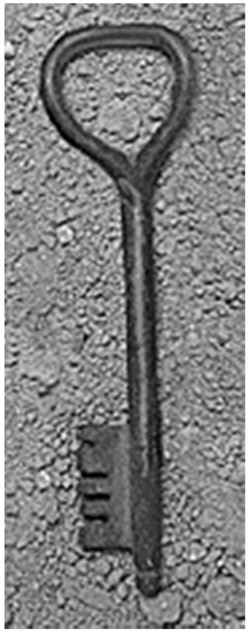
Attestation Promise

- TCG never lies about the state of measured information
- This requires
  - Accurate measurement
  - Protected storage
  - Provable reporting of measurement



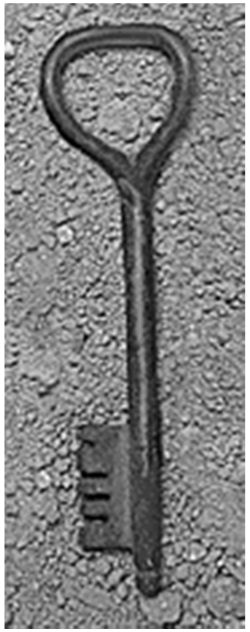
Remote Attestation

- ♦ Goal: prove to remote entities what software (OS, applications) you are running
- ♦ Remote entity (e.g., digital content provider) can request attestation of state via the Internet
- ♦ What can be proved?
  - – Platform is in an approved configuration
    - • Owner of machine doesn′t have privileged access to CPU
  - – OS and applications have not been modified
    - • Or even that they are licensed with maintenance fees paid
  - – Only approved applications are loaded



Attestation Examples

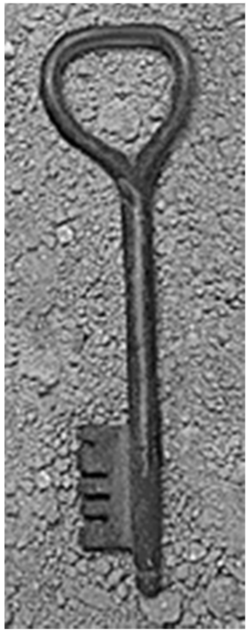
- Financial institution allows data download only if computer′s OS has all current security patches
- Laptop can connect to corporate network only if it runs authorized software
- Multi-role game players can join the game only if their game clients have not been modified
- Music store allows music download only if there are no unauthorized players installed

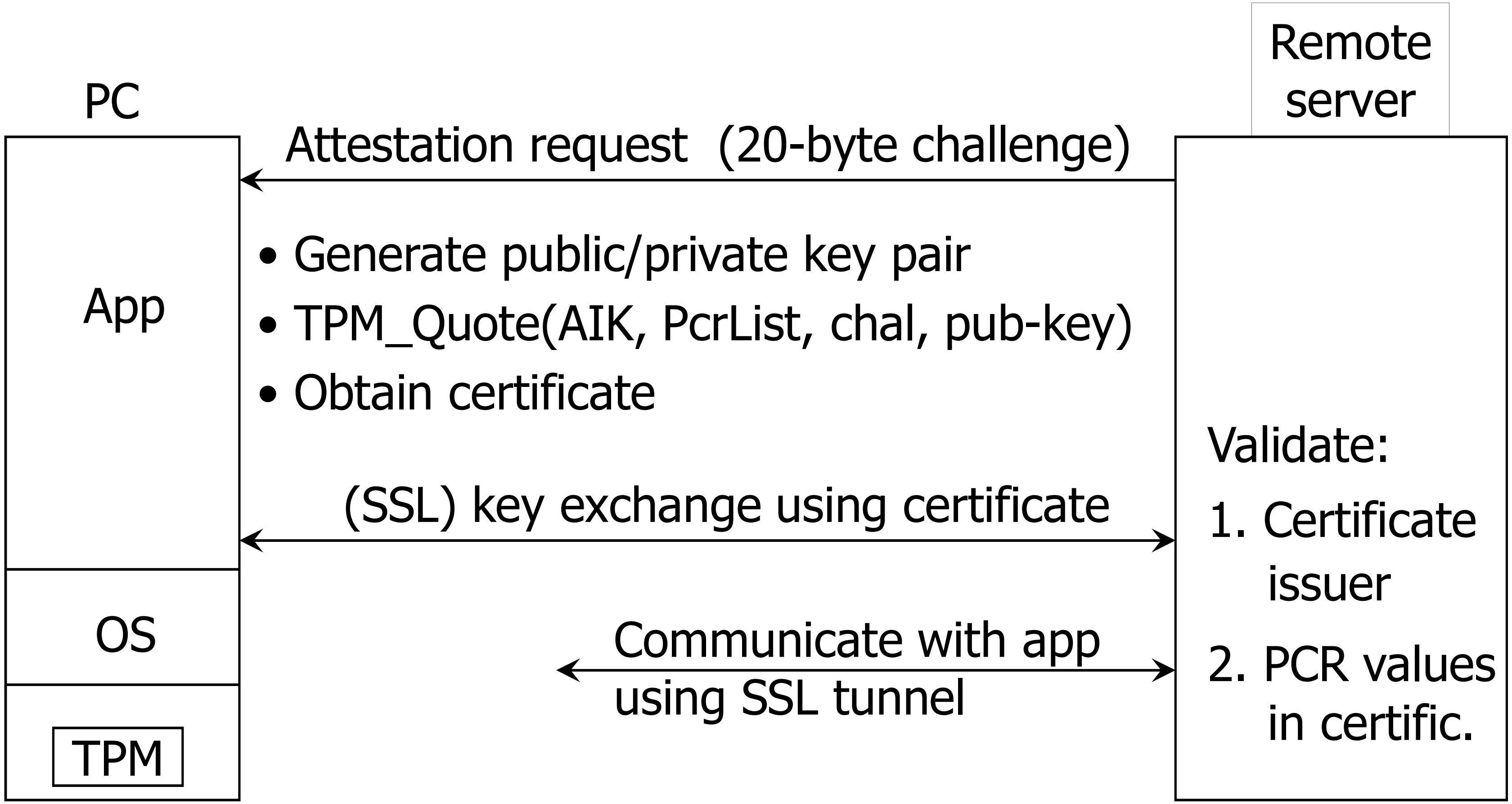


Attestation Process

- ♦ Create attestation identity key (AIK)
  - – Known only to TPM, public key certificate issued only if certificate for EK (endorsement key) is valid
    - Recall that EK is unique for TPM, stored in hardware
- ♦ Sign PCR values using TPM_Quote
  - – Arguments: keyhandle (which AIK to use), password for this keyhandle, list of PCRs to sign, 20-byte challenge from remote server, additional user data
    - What is the challenge needed?
- ♦ Return PCR values + signature

How Attestation Should Work





PC

App

OS

TPM

Remote server

Attestation request (20-byte challenge)

- Generate public/private key pair
- TPM_Quote(AIK, PcrList, chal, pub-key)
- Obtain certificate

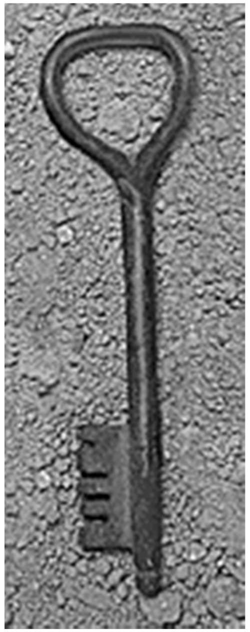
(SSL) key exchange using certificate

Communicate with app using SSL tunnel

Validate:

1. Certificate issuer
2. PCR values in certific.

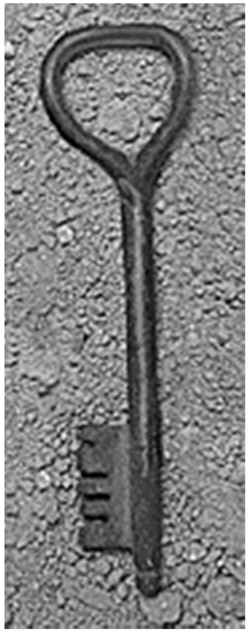
- Attestation should include key exchange
- Application must be isolated from rest of system



Nexus OS

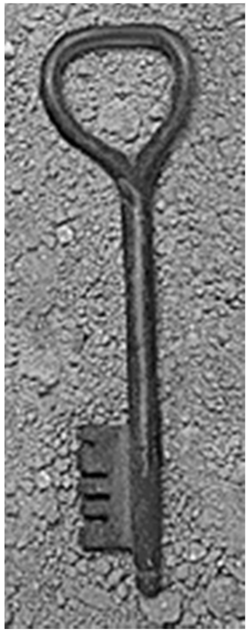
[Shieh et al. at Cornell]

- Attesting to hashed kernel and application code is not always feasible
  - Too many possible software configurations
- Better approach: attesting to <u>code properties</u>
  - For example, "application never writes to disk"
- Nexus OS supports general attestation statements
  - "TPM says that it booted Nexus;
    Nexus says that it ran checker with hash X;
    checker says that application A has property P"



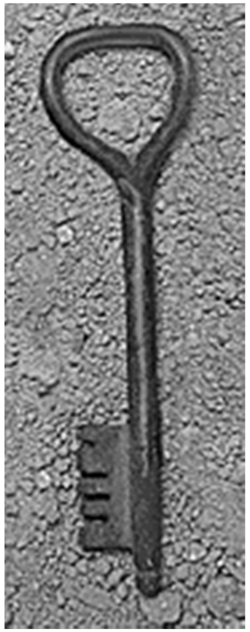
Attestation Issues

- ♦ Attestation only certifies what code was loaded
  - – Does <u>not</u> attest the current state of a running system
  - – Code could have been compromised after loading, e.g., by exploiting a vulnerability
- ♦ May interfere with security software
  - – Malicious music file exploits bug in a music player
  - – TCG prevents anyone from getting music file in the clear – how does anti-virus company develop defense?
- ♦ Exposure of a single endorsement key is deadly
  - – Using exposed key in TPM emulator, can attest to anything without actually running it



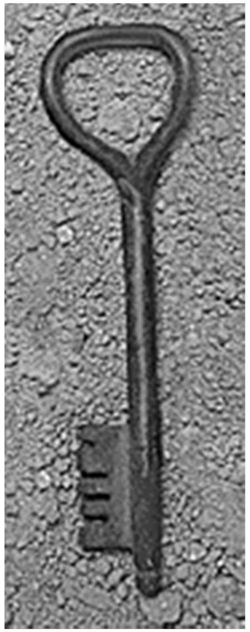
Privacy Issues in Attestation

- Each trusted machine has sets of unique AES and RSA hardware keys
  - Unique identifiers, may be used to track user behavior
  - Intel CPUID fiasco
- Basic approach: opt-in
  - User designates what software can access the sealed storage and authentication functions that use the keys
- Authentication key disclosure strictly controlled
  - Access to the RSA public key components is restricted
  - Only one export of the RSA public key per power cycle



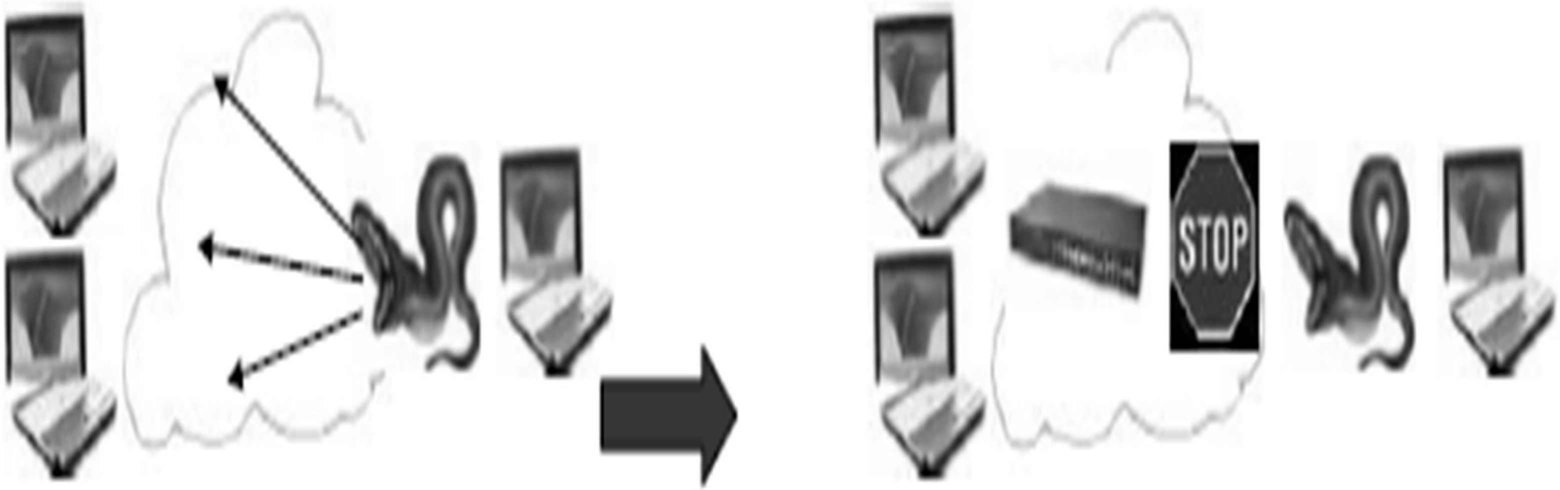
Pseudo-Identities

- If every party I communicate with needs my hardware RSA public key to encrypt some info for me, the key becomes a platform ID
- Solution: pseudo-identity
  - Generate a temporary RSA key pair
  - Use hardware key once to certify the pseudo-identity key, then just use the pseudo-identity keys
- Need a third-party certification authority ("Privacy CA") for certifying temporary keys



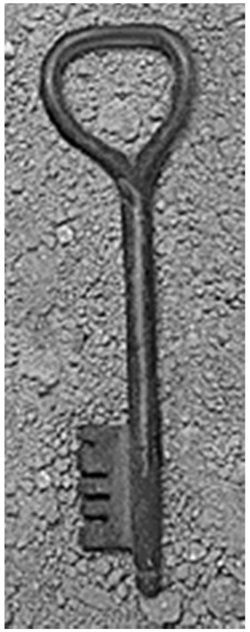
Illustration

A TCG-based Security Can Eliminate Security Attacks



A worm spreads from a single PC across the network

TCG standards deny network access to an infected PC preventing worm propagation

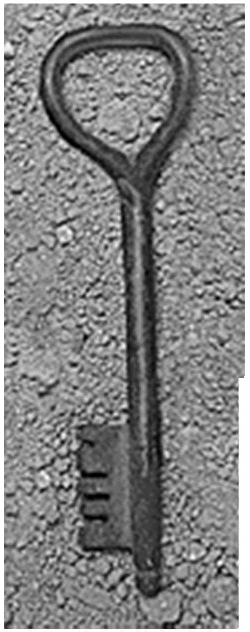


Illustration(continued)

A TCG-based Security Can Eliminate Security Attacks

A rogue access point provides an avenue for a war driver to sniff the network

A rogue access point is immediately recognized as an untrusted device and denied access to the network

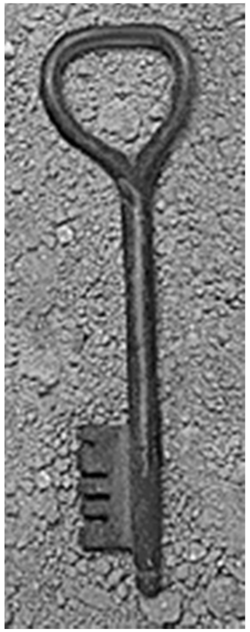


Illustration(continued)

A TCG-based Security Can Eliminate Security Attacks

A thief steals a PC with cleartext confidential data

A thief steals a PC with encrypted confidential data



The TCG Guidelines

What is TCG?

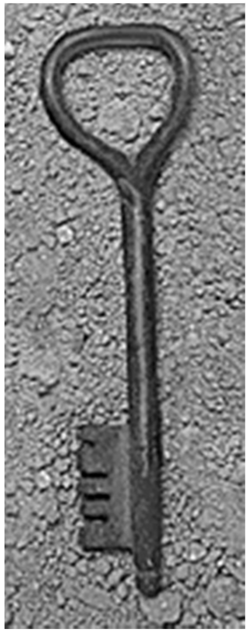
The Core Component - TPM

TPM provides:

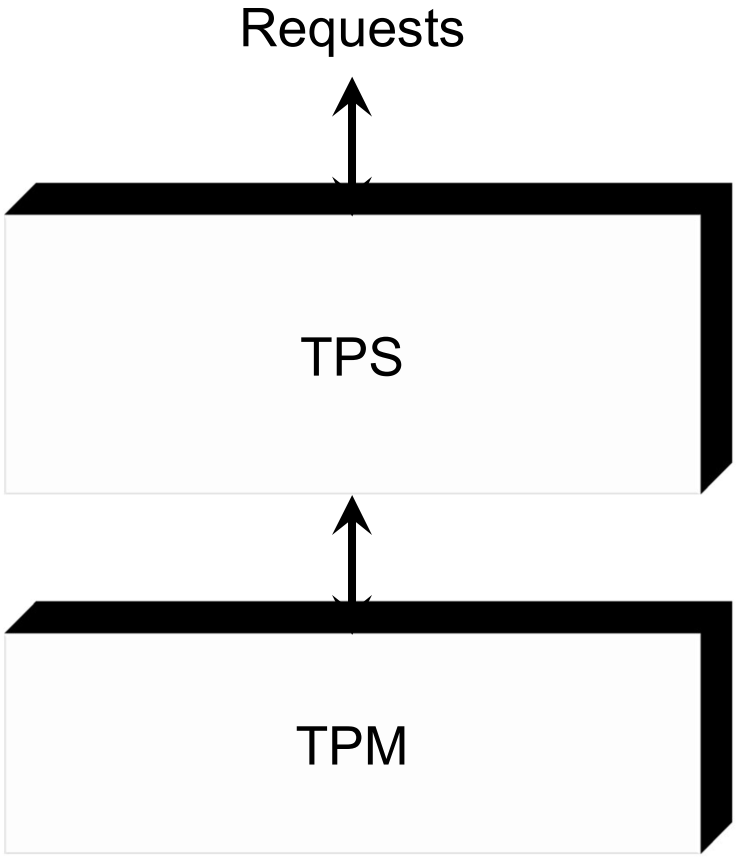
- ♦ Secure Input & Output
- ♦ Memory curtaining / Protected execution
- ♦ Sealed storage
- ♦ Remote attestation

System Layout based on TCG

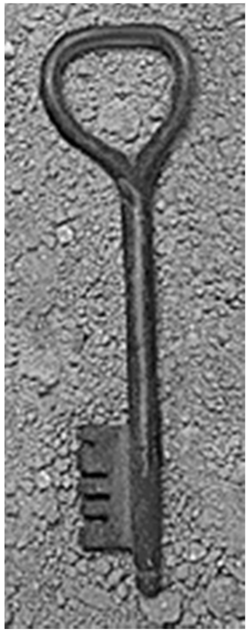
Controversy



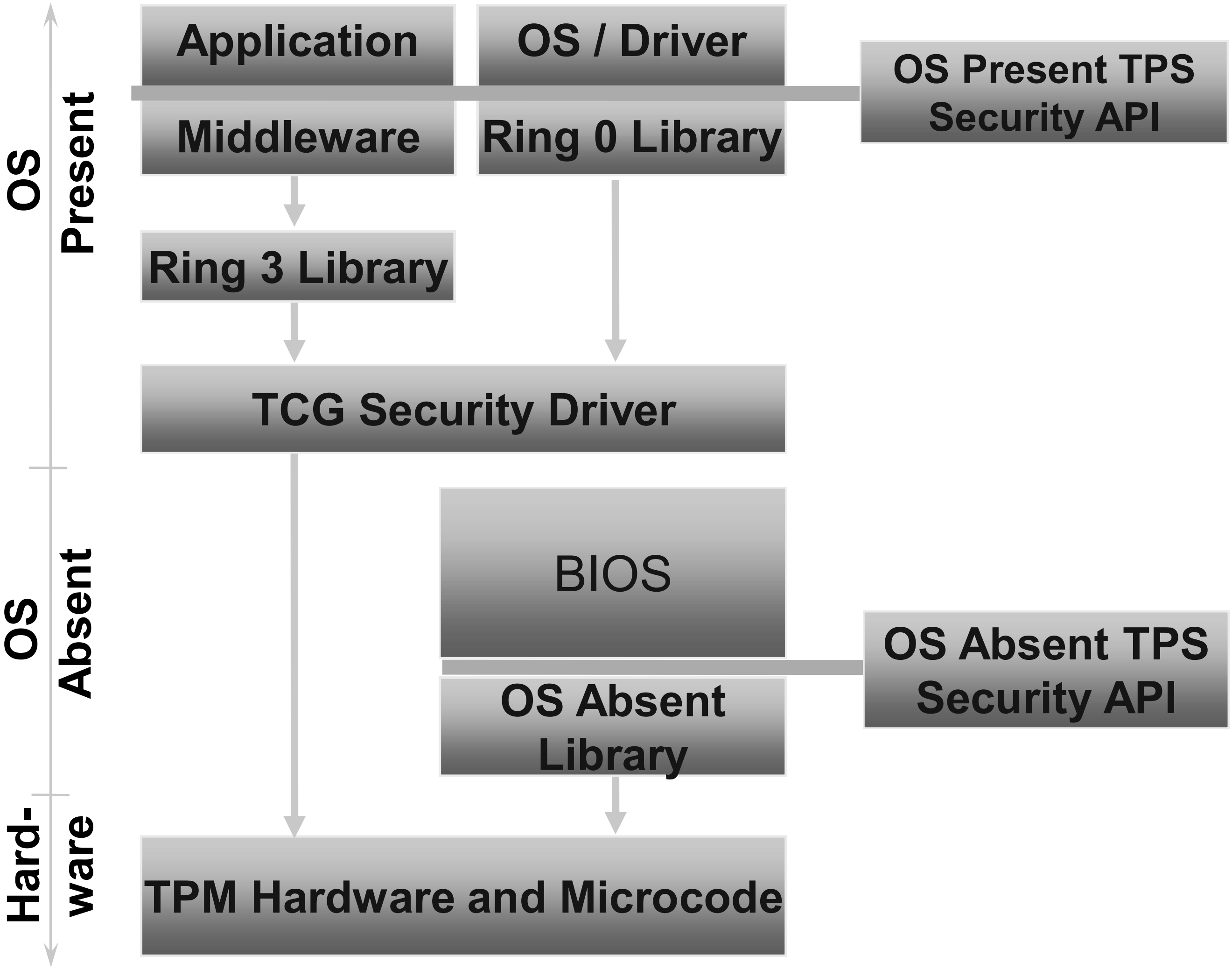
Functional Layout



- **TPS – Trusted Platform Subsystem**
  - **BIOS**
  - **Drivers**
  - **ALL operations come through TPS**
- **TPM – Trusted Platform Module**
  - **Hardware**
  - **Microcode**
  - **Protected functionality**
  - **Shielded locations**



System Architecture



OS Present

Application

OS / Driver

OS Present TPS Security API

Middleware

Ring 0 Library

Ring 3 Library

TCG Security Driver

OS Absent

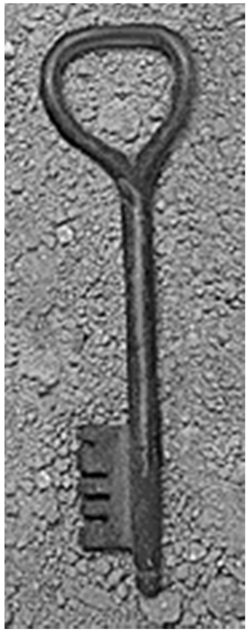
BIOS

OS Absent TPS Security API

OS Absent Library

Hard-ware

TPM Hardware and Microcode



The TCG Guidelines

What is TCG?

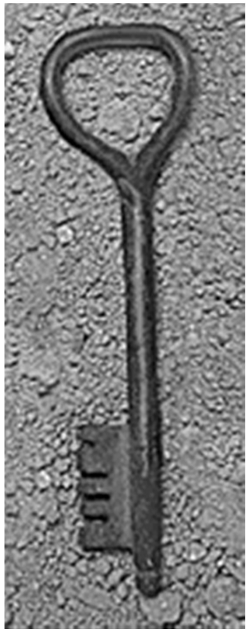
The Core Component - TPM

TPM provides:

- Secure Input & Output
- Memory curtaining / Protected execution
- Sealed storage
- Remote attestation

System Layout based on TCG

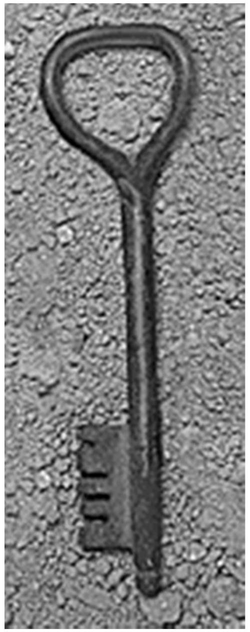
Controversy



Controversy

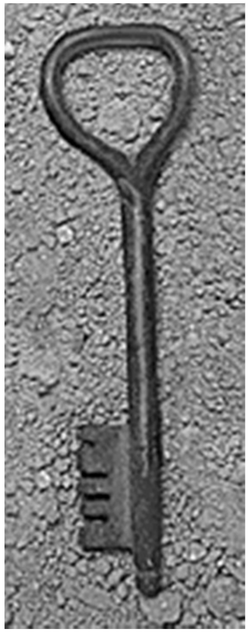
“TC allows computer manufacturers and software authors to monitor and control what users may do with their computers”

- Users can’t change software
- Users do not control information they receive
- Users do not control their data
- Loss of Internet Anonymity
- Proposed owner override for TC



Controversy Continued…

- There is no way to determine if the hardware has been properly implemented or if any backdoors have been added.
- Cryptographic designs and algorithms may become obsolete which will mean that users will be forced into unwanted upgrades with high switching costs.
- In the event of a hardware failure, there is no way to reclaim encrypted data which means vital information may be lost forever.



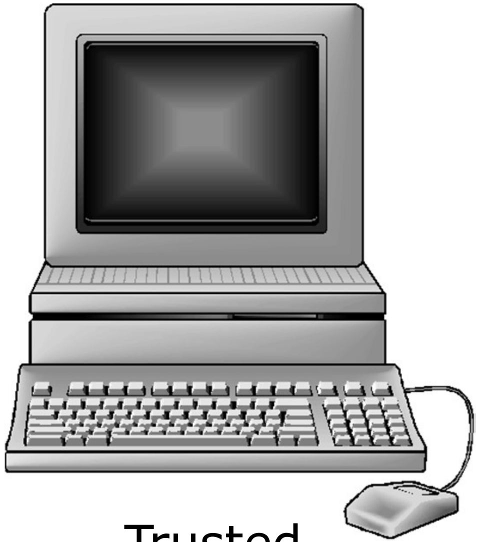
Threat Models – Scenario 1
Traditional PC Threat Model

- ♦ The owner is trusted, has full control over the PC, and is recognized by a password or biometrics.
- ♦ Adversary is an unauthorized user.

PC Owner

Trusted

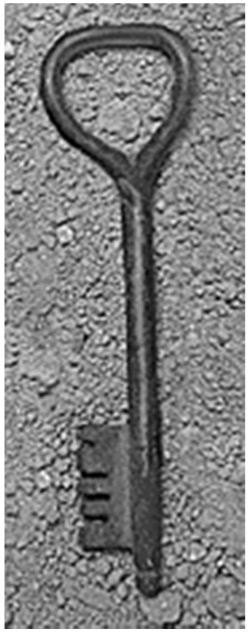
PC



Trusted

Hacker

Not Trusted



Threat Models – Scenario 2
TC Threat Model

- Similar to Personal Computers Mode, except that in this case the trust between the PC and its owner is broken. Only the PC is trusted.

PC Owner

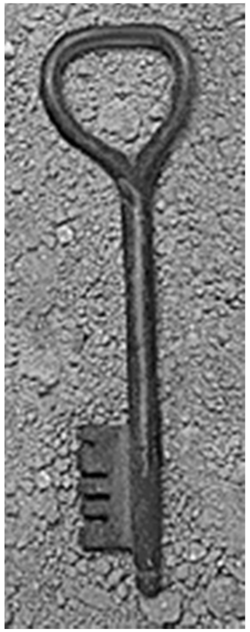
Not Trusted

PC

Trusted

Hacker

Not Trusted

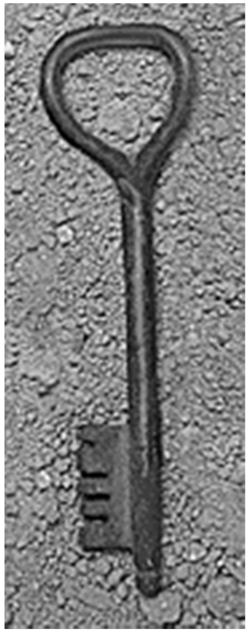


Drawbacks

Against-TCPA

Don't let them take YOUR RIGHTS!

- CD's
  - Could only be played with one media player
  - Could only be playable a certain number of day's
- Vigilantism
  - Large companies enforcing laws that they're not responsible for enforcing.
  - Taking huge liberties on interpretation the laws
- Legalized logic bombs
- Helps big companies, discourages competition
- Gives large corporations / government ability to do whatever they want with your computer. Most likely will include a backdoor for the FBI
- "in 2010 President may have two red buttons on his desk - one that sends the missiles, and another that turns off all the PCs"

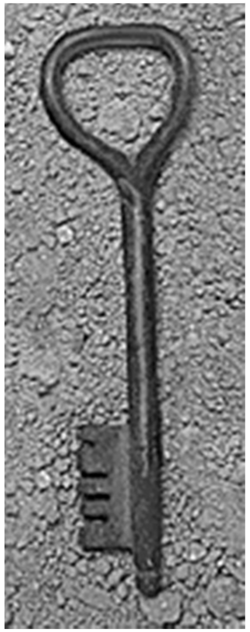


Summary

- TCG is a TRAP
- Do you want a company notorious for its security flaws to be in charge of your computer's security?
- Anti-competitive practices are bad for the consumer.

Against-TCPA

Don't let them take YOUR RIGHTS!



Questions?