Trusted Computing Platform Alliance: The Mother(board) of all Big Brothers

Lucky Green

c y p h e r p u n k s . t o

TCPA's Business Objectives

- Prevent use of unlicensed software.
- Digital Rights Management (DRM).
  - Prevent CD ripping and DivX creation.
  - Plug "analog hole."
  - Enable information flow control.
- Make PC the core of the home entertainment center, growing overall market.
- Meet operational needs of law enforcement and intelligence services (FBI, Homeland, NSA, non-U.S. law enforcement).

TCPA's Technical Objectives

- Prevent the owner of a computer from obtaining root access.
- Enforce three levels of access privileges:
  - Privileged access [TCPA members only].
  - Underprivileged access [platform owner].
  - Unprivileged access [non-TCPA applications].

TCPA Heritage

- To succeed where previous efforts have failed:
  - Processor ID (Intel, 1995-1998).
  - Encrypted CPU instruction sets (Intel, 1995-TCPA Phase II).
  - International Cryptography Framework (HP, 1996).
  - Smartcards on motherboard (IBM, ongoing).

TCPA History

- Founded in 1999 by:
  - Intel
  - Microsoft
  - HP
  - Compaq
  - IBM

TCPA Membership Profile

- The TCPA is a forum of platform product vendors.
  - CPU:
    - Intel, Advanced Micro Devices (AMD), Motorola.
  - BIOS/Chips:
    - Phoenix/Award, American Megatrends (AMI), National Semiconductor.
  - Security:
    - VeriSign, Wave Systems, RSA Security, Check Point, Certicom, Trend Micro, Symantec, Tripwire, Crypto AG [NSA].
  - Applications:
    - Microsoft, Adobe.
  - Systems:
    - HP, IBM, Dell, Gateway, Fujitsu, Samsung, Toshiba.

TCPA's 170+ Member Companies

360 Degree Web
3Com Corp.
Access360
Acer, Inc.
ActivCard Inc.
Adhaero Technologies
Adobe Systems, Inc.
Advanced Micro Devices, Inc.
Aesec Corporation
Aladdin Knowledge Systems
Algorithmic Research Ltd.
American Express Company
American Megatrends Inc.
Argus Security Corporation
Atmel Corporation
ATMEL Rousset
Authentium, Inc.
Autotrol Uruguaya S.A.
Baltimore Technologies Ltd
BERGDATA AG
BindView Development
BitStream Technology Corporation
Blueice Research
Broadcom Corporation
Carraig Ltd
Caveo Technology LLC
Cavium Networks
CE-Infosys Pte Ltd
Cerberus Information Security Limited
Certicom Corp.
Check Point Software Technologies Ltd
CHECKFLOW
Chrysalis-ITS
Cimarron Systems Incorporated
CipherKey Exchange Corporation
Cloakware Corporation
Communication Intelligence Corporation
Compagnie Européenne de Développement SA
Compal Electronics, Inc.
Compaq Computer Corporation
Computer Elektronik Infosys GmbH
Crypto AG.
Cygate ESM Oy
CYLINK Corporation
Dell Computer Corporation
DICA Technologies Inc.
DigiGAN, Inc
Digital Innotech Co.
Digital Persona Inc.
Discretix Technologies Ltd.
e-PCguard.com, Inc.
eCryp, Inc.
Eltan Comm B.V.
Enova Technology Corporation
Ensure Technologies
Entrust Technologies Ltd.
ERACOM Pty Ltd

Ethentica
Excalibur Solutions, Inc
FARGOS Development, LLC
FINGLOQ AB
First Access, Inc.
Fortress Technologies Inc
Fujitsu Limited
Fujitsu-Siemens-Computers
Gateway, Inc.
Gemplus Corporation
GLOBEtrotter Software
Hewlett-Packard Company
Hitachi, Ltd. PC Div.
HyperSecur Corporation
I/O Software, Inc.
ICSA.net
ID Tech
IdentAlink Limited
Infineer Inc.
Infineon Technologies Corporation
Infineon Technologies Asia Pacific Pte Ltd
InfoCore, Inc.
Insyde Software Corp.
Integrity Sciences, Inc.
Intel Corporation
Interlok Technologies L.L.C.
International Business Machines Corporation
International Service Consultants Ltd.
Internet Dynamics, Inc.
Internet Security Systems
InterTrust Technologies
Iomega Corporation
Kasten Chase Applied Research
Keycorp Ltd.
Keyware Technologies, Inc.
Lanworks Technologies Co.
Legend (SHENZHEN) R&D Center, Legend Group Ltd
Lexign
Liquid Audio, Inc.
Litronic Inc.
LOGISIL Consulting
M-Systems Flash Disk Pioneers
M3S Enterprises
Macrovision Corporation
Massive Media Group
Media DNA Incorporated
Medialogic Co., Ltd
Miaxis Biometrics Co.
Micron Electronics, Inc

Microsoft Corporation
Mitac International Corporation
Mobile-Mind, Inc.
Motorola
National Semiconductor
nCipher Inc.
NDS Limited
NEC Corporation
Net Nanny Software International
NetActive Inc.
NetAtmosphere Inc.
NetOctave, Inc.
NetSecure Software Canada
Network Associates, Inc.
New Trend Technology Inc.
Novell, Inc.
nVidia
O2Micro
Open Source Asia
PC Guardian
Philips Semiconductors
Phoenix Technologies, Ltd.
Pijnenburg Custom Chips B.V.
Precision Digital Hardware
Pricewaterhouse Coopers
Prism Resources, Inc.
Pro-Team Computer Corp.
Protect Data Security Inc.
Rainbow Technologies, Inc.
Raytheon Company
Raz-Net Inc.
Redstrike B.V.
RSA Security, Inc.
SafeNet, Incorporated
SAFLINK Corporation
SAGEM MORPHO, Inc.
SAGRELTO Enterprises, Inc.
SAMSUNG ELECTRONICS CO. LTD
SAS Institute
Schlumberger, Smart Cards
Science Applications International Co.
Scienton Technologies Inc.
SCM Microsystems
Sectra Communications AB
Securant Technologies
Secure Computing Corporation
Secure Systems Solutions
Siemens AG
Softex, Inc.

SPYRUS, Inc.
SSH Communications Security, Inc.
Standard Microsystems Corporation
STMicroelectronics
Symantec Corporation
Symbol Technologies, Inc
Texar Software Corp.
Thales e-Security, Inc.
TimeCertain, LLC
Titan Systems Corporation
Toshiba Corporation
Trend Micro, Inc.
Tripwire, Inc.
Trispen Technologies
TrueTime Inc.
TruSec Solutions
Trustpoint Corporation
TVN Entertainment Corporation
Ubizen
Utimaco Safeware AG
ValiCert Inc.
VeraSafe, Inc.
Veridicom, Inc.
Verisign, Inc.
Viewpoint Engineering
Voltaire Advanced Data Security Ltd
Wave Systems Corp.
Wincor Nixdorf
WinMagic, Inc.
WinVista Corporation

TCPA's Technology (Phase I)

- Trusted Platform Module (TPM), aka the "Fritz Chip."
  - Tamper resistant chip to be included on all future motherboards.
  - Surface mount; either a separate part or integrated into the chipset.
  - Common Criteria EAL3 [augmented] certified.

TPM Functionality Categories

- Measurement
- Reporting

TPM Measurement

- Cryptographic operations
- Key store
- Key management
- Boot process hashing

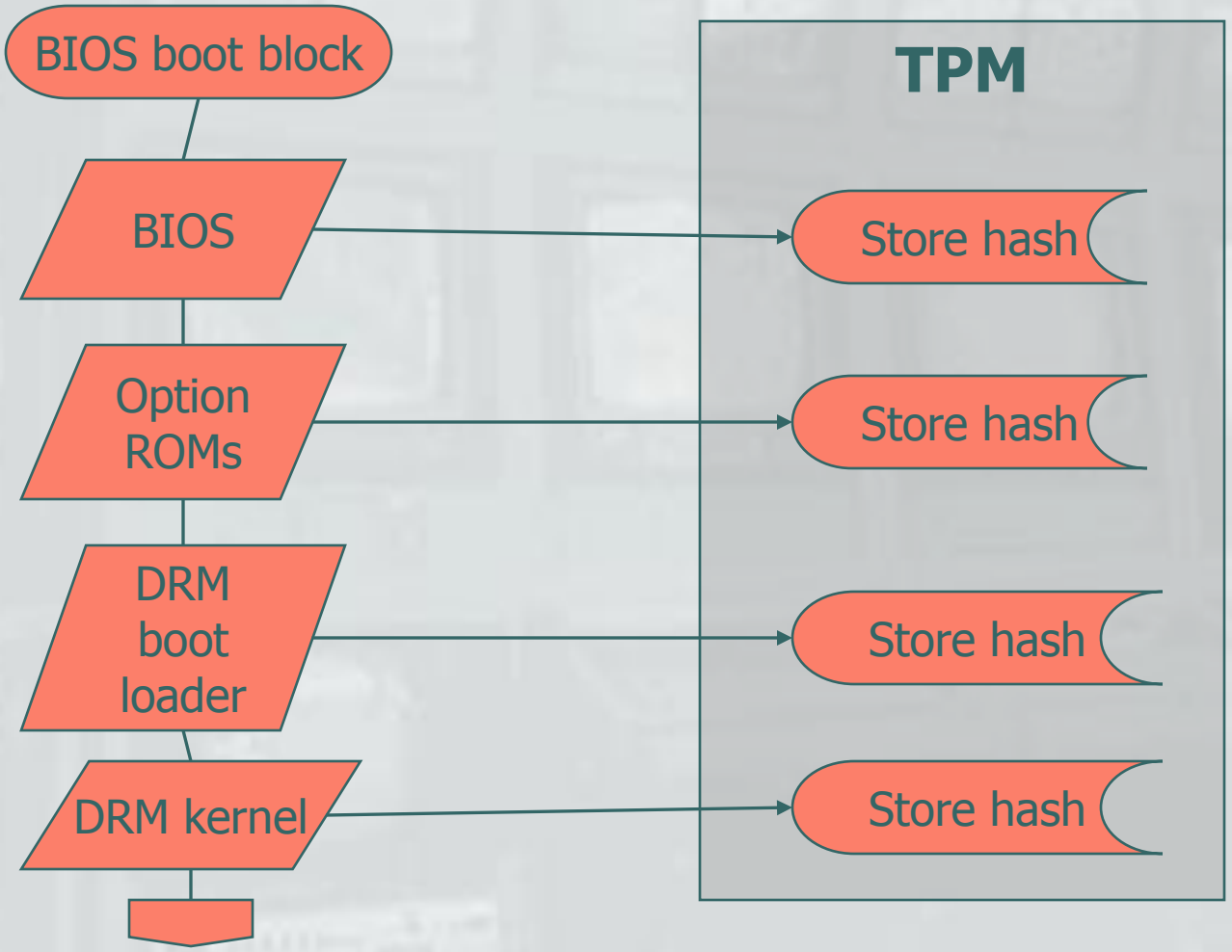
TPM Internals

- Cryptographic operations:
  - Hashing (SHA-1, HMAC).
  - Random number generation (RNG), post-whitening output only.
  - Asymmetric key generation (2048-bit RSA).
  - Asymmetric key encrypt/decrypt (2048-bit RSA).
  - Symmetric encrypt/decrypt (3DES, AES).
    - Symmetric key operations may be performed off-chip.
- Tamper-resistant hash and key store.

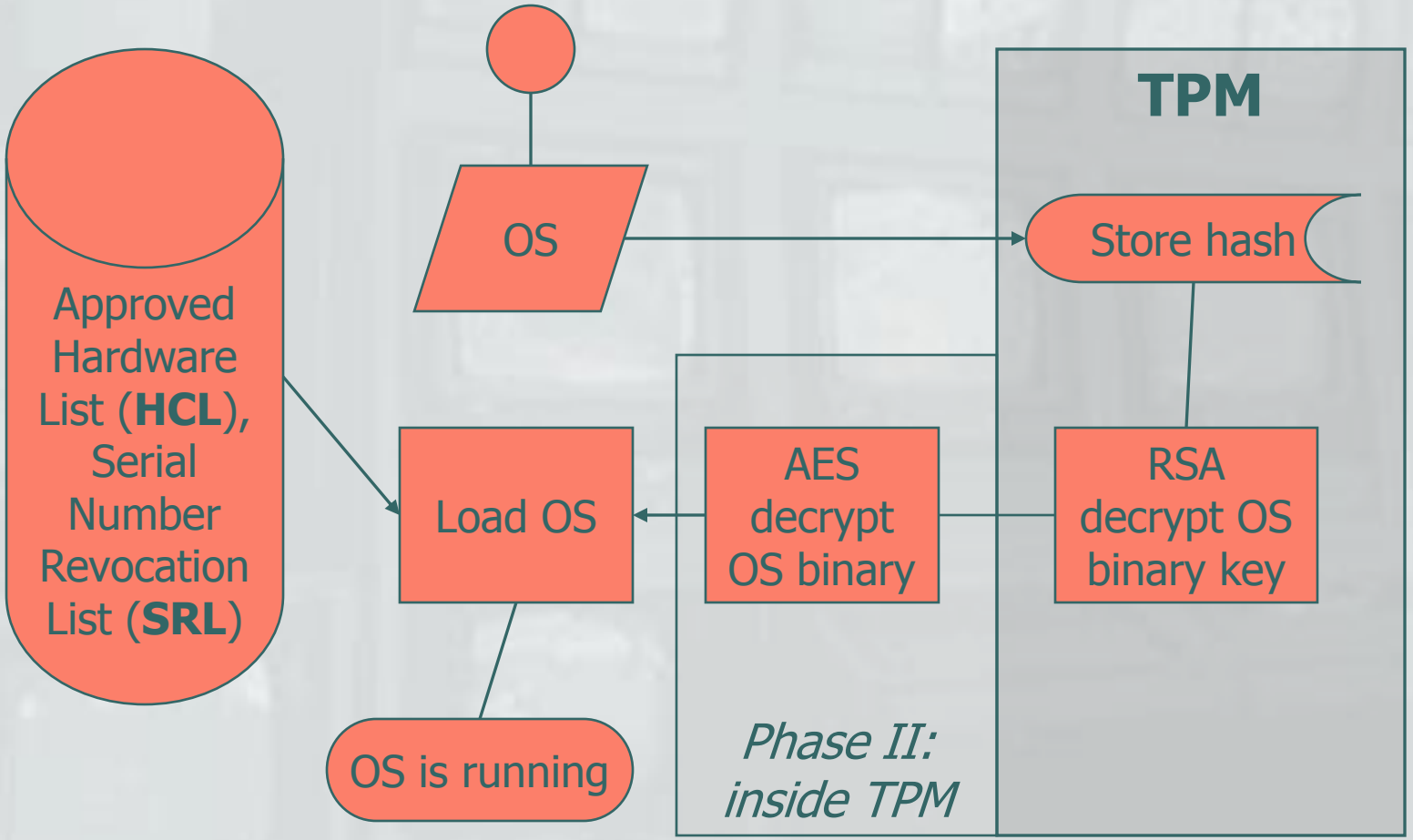
TPM Key Management

- Endorsement Key
  - Unique RSA key generated at time of manufacture. Signed by manufacturer's key, which is signed by the TCPA master key. Used to prove that the TPM is genuine.
- User Keys
  - One or more user RSA keys certified by a "Privacy CA" at time of TPM activation. Used to identify user.

TCP pre-OS Boot Process



TCP OS Boot Process



TCP OS Known Initial State

- BIOS is TCPA-approved.
- PCI cards are TCPA-approved.
- DMA devices do not enable unapproved access to operating RAM.
- No kernel-level debugger is loaded.
- Initial list of undesirable applications is available for processing.
- Examples of TCPA operating systems:
  - Microsoft: Palladium (DRM OS patent).
  - HP: Linux.

TCP OS Initial Tasks

- Start secure time counter (no turning back the system clock).
- Synchronize system time against authenticated online time servers.
- Obtain HCL and SRL updates over the Internet.

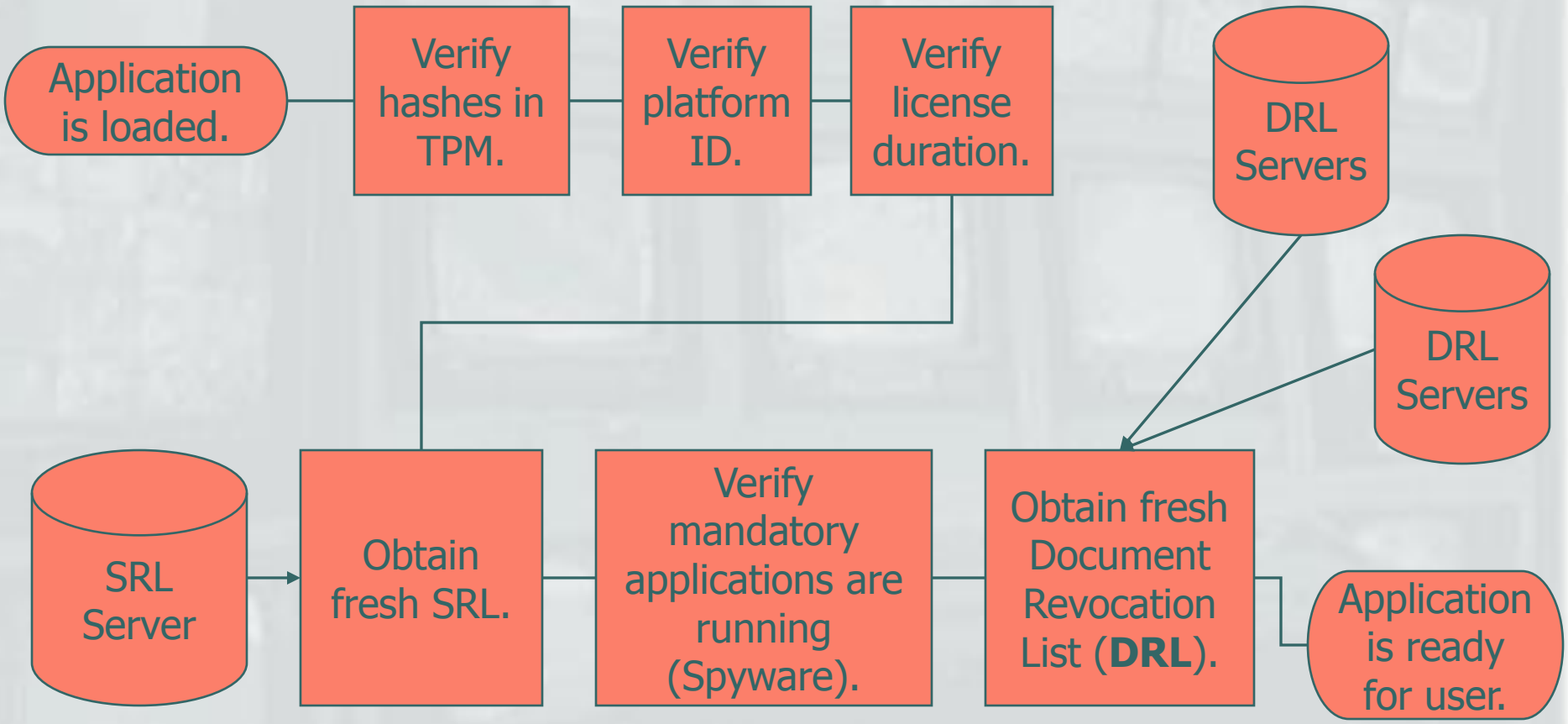
Pre-application Load

- Two primary application loader protection modes:
  - **Mandatory:** OS will refuse to load a non-TCPA approved application.
  - **“Voluntary”:** OS will load a non-approved application, sending SIGCOMP to all loaded applications.

Application Loader Protection Modes Comparison

Mode	Mandatory	“Voluntary”
OS hashes application, stores hash in TPM.	YES.	YES.
OS loads TCPA-approved applications not listed on an SRL.	YES.	YES.
OS loads application on SRL.	NO.	NO.
OS loads non-approved application.	NO.	YES. TCP applications receive SIGCOMP, zeroize their operating RAM, and shut down.

TCP Application Initial Tasks



TCPA Stifling Competition

- “We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains.”

  -- *Bill Gates, Microsoft*

- “You could create Word documents that could be read only in the next week.”

  -- *Steven Levy, MSNBC/Newsweek*

Quiz: How will the Law Help TCPA Stifle Competition?

- Application vendors intend to wrap their file formats with DRM.
- Question: What does a federal prosecutor call an application that is compatible with a proprietary DRM-wrapped file format?
- **Answer: An illegal infringement device.**

Consequences of Ubiquitous Digital Rights Management

- Makes it illegal to create interoperable software in the U.S.
- Subjects authors of interoperable software to penalties of up to $500,000 and 5 years in prison (and double that for subsequent offenses).
- The law is already on the books: Digital Millennium Copyright Act (DMCA).

Software Authors' Choices

1. Do not create interoperable software.
2. Spend 5 years in prison.

TPM Reporting

- Proving State to Challengers
  - Local: operating system, applications.
  - Remote: challengers requesting state via the Internet (digital content servers, secure time servers, information authorization servers).

Reporting to Remote Entities

- Remote challengers can determine that:
  - Platform is in an approved state.
  - Owner of the machine does not have privileged access to the CPU.
  - OS and application software are fully licensed with maintenance fees paid.
  - OS and applications are unmodified.
  - Only approved applications are loaded.

TCPA Feature Enablement

- Secure ongoing revenue stream.
- Stifle competition (DMCA).
  - Defeat the GPL.
  - Enable information invalidation.
  - Facilitate intelligence collection.
  - Meet law enforcement needs.
  - ...and many more.

Defeat the GPL

- HP is developing a TCPA-compliant version of Linux.
- GPL requires the result to be Open Source.
- Source code will compile and can be verified.
- But: the source alone is useless without a TPM-specific certificate.

Suggested Fixes to the GPL

- Require software authors to provide whichever services are necessary to enable an application to operate as the user desires.
  - Violates Stallman's "Free Speech" vs. "Free Beer" principle.
  - TPM prevents application authors from providing the activation key even if they so desire. (Violation of the DMCA).
- Require third parties to provide the service.
  - Alice and Bob agree that Carol shall provide free beer to all comers in perpetuity. (Unenforceable Contract).

Information Invalidation

- Application queries Document Revocation List servers for the latest DRLs.
- Reasons for placing a document on a DRL:
  - Created by a compromised (unpaid) copy of the application.
  - Mandated by court order: Official Secrets Act, copyrighted material, danger to Homeland Security.
  - Locally illegal content: pictures of women without veils in Muslim countries, copy control ciphers in the US.
  - Any number of reasons.

Intelligence Collection

- Documents signed by user keys allow activity correlations.
- Globally unique document IDs facilitate traffic analysis.
- Preemptive information invalidation enables information flow control.

Law Enforcement Needs

- Undeniable proof of authorship.
- Document monitoring/tracking.
- Information invalidation by court order.
- Continued Law Enforcement access after public information invalidation for evidentiary purposes.

Will TCPA Meet Governmental Requirements?

- “We are talking to the government [...] There *are* governments in the world, and not just the U.S. Government.”
  -- *Mario Juarez, Microsoft, Palladium (TCPA) Product Manager*

Fritz Hollings Bill: S. 2048

- CBDPTA (formerly SSSCA)
- Plug “analog hole” with 2048-bit RSA.
  - Monitor out
  - Video out
  - Audio out
- Microsoft:
  - Additionally encrypt keyboard input to PC.
- S. 2048 makes it illegal to sell non-TCPA-compliant computers.

Quiz: Fritz Hollings S. 2048 Penalties

- Question: what is the penalty a person selling a non-TCPA approved computer will face under the Hollings bill?
  A. A “fix-it” ticket.
  B. Six months in jail.
  C. A $500,000 fine and 5 years in prison for the first offense; double that for each subsequent offense.
- **The correct answer is C:**

  A $500,000 fine and 5 years in prison for the first offense; double that for each subsequent offense.

But Palladium will be Released as Open Source!

- Microsoft announced that Palladium's source code will be published.
- "We are trying to be transparent in all this."

  -- *Jim Allchin, Group Vice President, Windows, Microsoft*
- Some take this as proof that Microsoft has changed its business practices.
- Others remain skeptical.

Quiz: Why is Microsoft Releasing the Palladium Source Code?

- Question: which of the following answers is correct?
  A. Microsoft intends to place MS Office under the GPL in 2003.
  B. Microsoft will release the Windows source code under the BSD license in 2004.
  C. Microsoft has little choice but to release Palladium as Open Source because S. 2048 requires it.
- **The correct answer is C:**

  S. 2048 requires that "the security system standards shall ensure [...] that any software portion of such standards is based on open source code."

Use of TPM's is Voluntary

- "One thing I can guarantee is that [Palladium] will be 'off' by default, an opt-in technology."

  -- *Stuart Okin, Security Officer, Microsoft, United Kingdom*

- Using gasoline in a car is an opt-in technology.

Would an OS Vendor Block "Undesirable" Applications?

- "Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer."

  Microsoft, Windows Media Player EULA

Phase I: Digital Holes

- Op codes are in plaintext on the bus.
  - Can be microprobed off the bus.
  - Solution: Encrypted CPU instruction sets in TCPA Phase II (TPM inside CPU).
- User can select non-TCPA-approved OS for minimum functionality.
  - Solution: Prevent non-approved OS from accessing CPU supervisor mode.
    - "There will be new modes and new instructions.... A whole new class of processors not differentiated by speed, but security." -- *Geoffrey Strongin, AMD*
    - "The new hardware architecture involves some changes to CPUs which are significant from a functional perspective." -- *Mario Juarez, Microsoft*

Why TCPA Might Succeed

- Processor ID:
  - Intel went alone. AMD publicly rejected Processor ID.
  - Online privacy advocates were not considered a serious threat.
- TCPA:
  - Intel, AMD, Motorola, BIOS vendors, system vendors, and application vendors are all on board.
  - Two-prong technical and legislative initiative.
  - Online privacy groups were briefed early.

TCPA-Enabled Platforms

Laptops

Servers

Mobile Phones

PDAs

The End Result

- “The end result is a system with security similar to a closed-architecture system but with the flexibility of the open Windows platform.”

  -- *John Manferdelli, General Manager, Microsoft "Palladium" Business Unit*

Questions

- Email Lucky Green
  shamrock@cypherpunks.to

  Replies will occur after DEF CON.

- Or, talk to me during the con.

References

- George Orwell, *1984*
- Trusted Computing Platform Alliance
  http://www.trustedcomputing.org
  - TCPA Main Specifications Version 1.1a
  - TCPA PC Specific Implementation Specifications Version 1.00
  - TCPA Trusted Platform Module Protection Profile Version 1.9.4
- Ross Anderson
  - TCPA / Palladium Frequently Asked Questions
    http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html
  - Security in Open versus Closed Systems - The Dance of Boltzmann, Coase and Moore
    http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf
- Steven Levy, MSNBC/Newsweek, “The Big Secret”
  http://cryptome.org/palladium-sl.htm
- Microsoft’s DRM OS (Palladium) US Patent 6,330,670 http://www.uspto.gov/patft/
- Microsoft PressPass Q&A Palladium
  http://www.microsoft.com/presspass/features/2002/jul02/07-01palladium.asp
- Consumer Broadband and Digital Television Promotion Act (S. 2048)
  http://thomas.loc.gov/cgi-bin/query/z?c107:S.2048: