

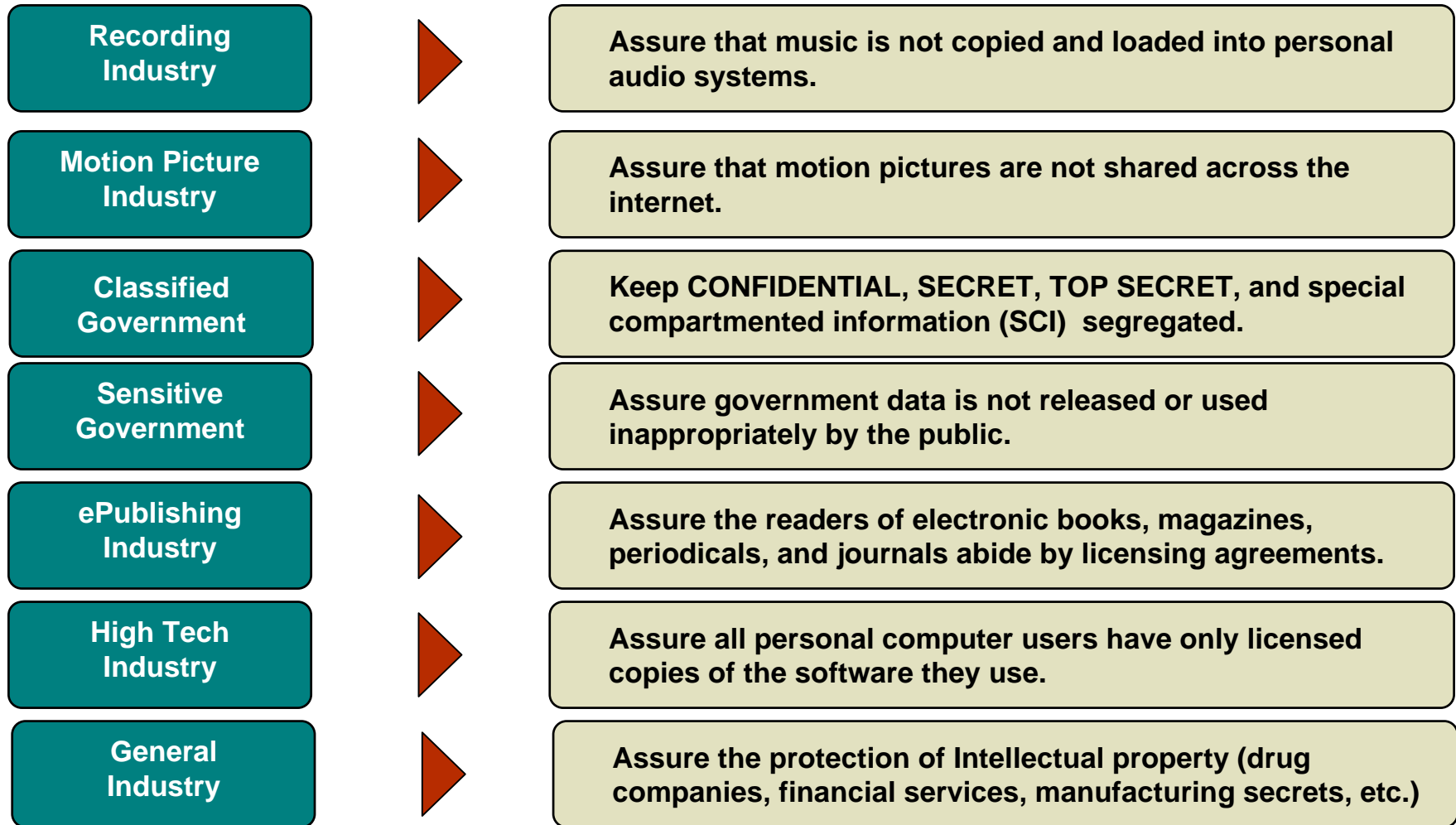
ACSAC Presentation

Digital Rights Management:

Stakeholder analysis and use by DOD for MLS/MSL/CDS

Tucson, AZ
8 December 2004

Can you think of a business/political issue that unites the entertainment industry, the high tech industry, other big business, and government? If you can, then perhaps we should worry!



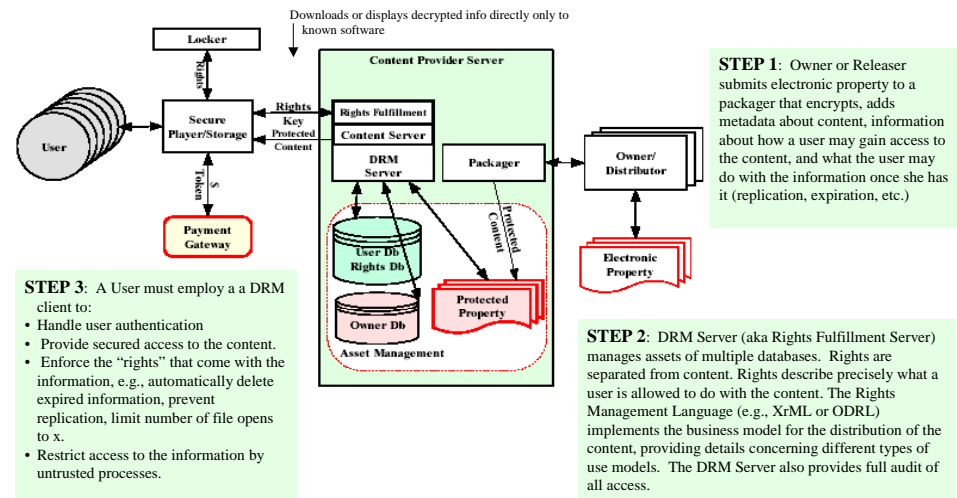
Digital Rights Management (DRM) systems restrict the use of digital files in order to protect the interests of copyright holders.

Digital Rights Management (DRM)

- ▶ DRM **legislation** requiring the inclusion of copy control systems are rapidly evolving and a number of intended and unintended consequences are cause for concern.
- ▶ DRM **technologies** can control file access (number of views, length of views), altering, sharing, copying, printing, and saving. These technologies may be contained within the operating system, program software, or in the actual hardware of a device.
- ▶ Private sector and governmental DRM **policies** will evolve to depend on this technology.
- ▶ DRM **Implementations** are being developed under the Trusted Computer Platform Alliance.
- ▶ **Privacy** advocates have legitimate concerns

Examples of Persistent Digital Rights

Read Once
Redacted Read
Copy Once, No Replication
Copy with Replication Rights
Copy with No Edit Rights on Copy
Copy with Edit Rights on Copy
Copy with Auto Expiration on Copy
Copy with Rights to Add Comments to Original



Key events are shaping the legal, policy, and technology landscape

DRM Key Events

- ▶ In October 1999 the Trusted Computer Platform Alliance (TCPA) was formed by Compaq, HP, IBM, Intel and Microsoft. The TCPA is an industry working group focused on improving trust and security on computing platforms. The alliance has since grown to 170+ companies.
- ▶ In September 2001, Senator Fritz Hollings (D-SC) announced plans to introduce the Security Systems Standards and Certification Act (SSSCA). The SSSCA would require equipment manufacturers to embed government-approved copy protection systems into all computer equipment.
- ▶ In March 2002, Hollings introduces Consumer Broadband and Digital Television Promotion Act (CBDTPA) to regulate interstate commerce in certain devices by providing for private sector development of technological protection measures to be implemented and enforced by Federal regulations to protect digital content and promote broadband as well as the transition to digital television, and for other purposes.
- ▶ In June 2002, Microsoft announced its Palladium project, a project that would embed DRM into software and hardware.
- ▶ Representative Howard Berman (D-CA) introduced H.R. 5211 in July 2002. The bill would actually permit copyright owners or their agents to engage in behavior currently illegal under a computer fraud act in order to interdict filetrading.
- ▶ In August 2002, the FCC issued a notice of proposed rulemaking (NPRM) to consider whether digital television signals should incorporate a digital broadcast flag. Such a flag would mark digital content as "protected" and direct devices to limit individuals' use of the content.

The TCG (formerly TCPA) is a powerful alliance which has undertaken this initiative in part as a defensive measure to prevent the entertainment industry from dictating which media players can “play” content, but other objectives are valid as well.

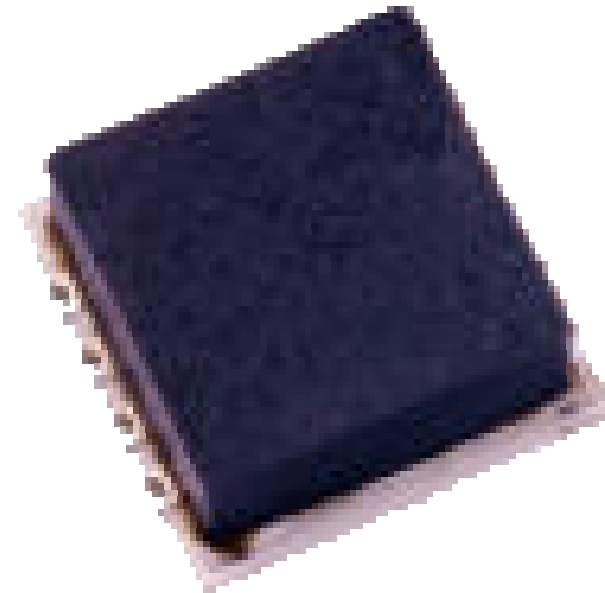
TCG Business Objectives

- ▶ Prevent use of unlicensed software.
- ▶ Digital Rights Management (DRM).
 - Prevent CD/DVD copying.
 - Plug “analog hole.”
 - Persistent enforcement of copy write restrictions throughout lifecycle
- ▶ 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).

The TCG would like to create the mother (board) of all big brothers. Phase I technology is based on the “Fritz” chip. Version v1.2 available in Nov 2003.

TCG Hardware

- ▶ **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.
- ▶ **Phase II** – Fully integrated into Pentium chip
 - Cryptographic keys and encryption embedded in processor
 - Highly Tamper Resistant
 - Common Criteria EAL3 [augmented] certified



The technical components of DRM form a full suite of security mechanisms for cryptographic operations, key store, key management, and secure booting.

Security Technologies Supporting DRM

- ▶ Cryptographic operations:
 - Hashing (SHA-1, HMAC).
 - Random number generation (RNG)
 - Asymmetric key generation (2048-bit RSA).
 - Asymmetric key encrypt/decrypt (2048-bit RSA).
 - Symmetric encrypt/decrypt (3DES, AES).
- ▶ Tamper-resistant hash and key store.
- ▶ Services supported by these mechanisms:
 - Authentication
 - Authorization
 - Auditing
 - Encryption
 - Integrity

There are least address five socioeconomic questions about DRM which need to be addressed.

QUESTION	PERSPECTIVE	COMMENTS
•What problem does DRM solve?	• Entertainment Industry	• Solves the copy protection problem
	• Software Industry	• Solves the software licensing problem
	• Government	• Solves the access problem to classified and sensitive information
•How well does DRM solve the problem?	• Entertainment Industry	• Not very well in the short term, needs agreements from media players and much better technology.
	• Software Industry	• Reasonably well
	• Government	• Not yet high enough assurance for classified information
•What new problems does DRM create?	• World Stability	• Promotes remote censorship by rogue states and fundamentalists
	• National Security	• Restricts foreign intelligence activities and counterterrorism
	• Law Enforcement	• Makes forensic examinations complex
	• New Companies	• Creates barriers to entry because incumbents control technologies
	• Open Software	• Embedded copy protection endangers open source software
•What are the economic and social costs?	• Vendors & Users	• Complex and expensive to implement and operate
	• Public	• Creates a big brother inside the computer
	• Public	• DRM cannot recognize fair use rights
•Is DRM worth the costs?	• Maybe	• Let's discuss