# Rights Management in a Security Framework

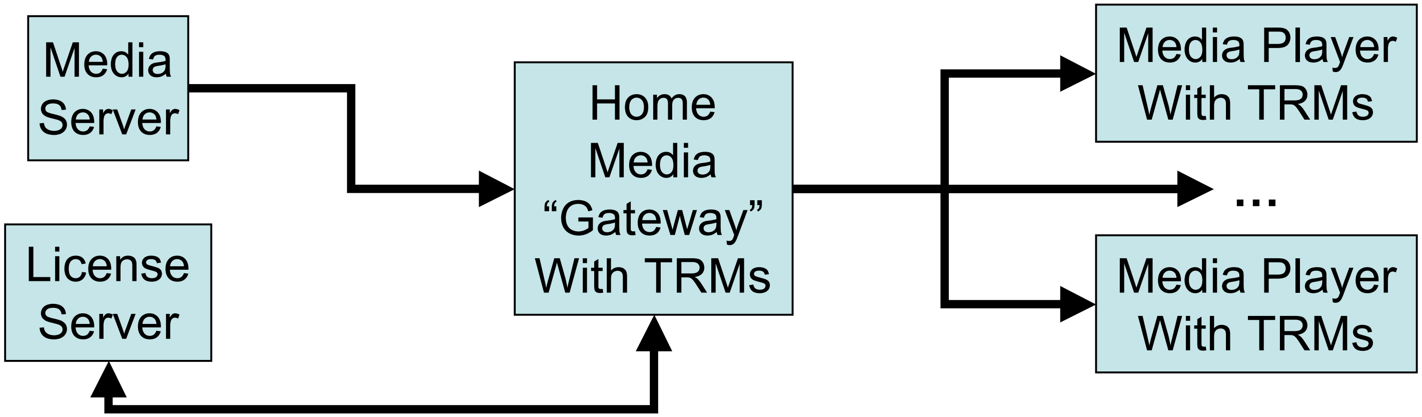
Mark Baugher

Cisco Systems

# Rationale

- Prevailing DRM approach is insecure to the extent it doesn’t trust end-user
- Secure rights-management is possible within a security relationship between provider & customer
- PERM can be used in this way – and in conventional DRM systems as well

# DRM & Tamper-resistant Mechanisms (TRM)



- Media gateway gets key & license
- Media gateway forwards/caches content work
- Media player gets keys, rights spec & content
- Tamper-resistant mechanisms *considered to be needed* to protect keys, rights spec and content

# Why TR-DRM is Insecure

- No one has invented the tamper-resistant mechanism that can’t be defeated when the device is controlled by attacker
- License enforcement, however, treats the device user as an attacker with respect to data stored in the tamper-resistant mechanism
- Therefore, we can’t trust the user or the tamper-resistant mechanism

# Why TR-DRM Isn’t Always Needed

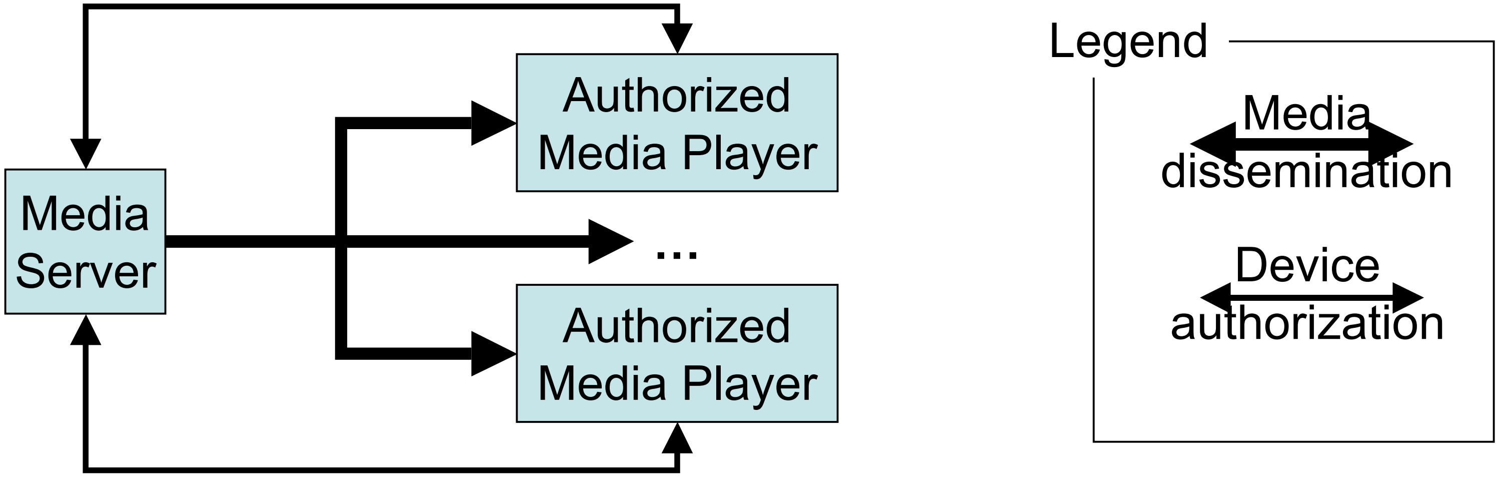
- Some of the most commercially-viable technologies have broken tamper-resistant mechanisms (such as DVD CSS, iTunes)
  - Anybody can copy a tune or DVD movie
  - But iTunes approaching 3M legal downloads/month
  - And DVD rivals VC**R**s as a commercial success
  - In fact, the threat is not from customers but professional copy operations, much outside US
- Some compelling business models (e.g. iPoD) don’t use tamper-resistant DRM

# PERM & Tamper-resistance

- PERM is independent of license or rights enforcement mechanisms and thus tamper resistance is out of scope
- Instead, PERM can properly implement a secure exchange – in the true sense of the word “secure”

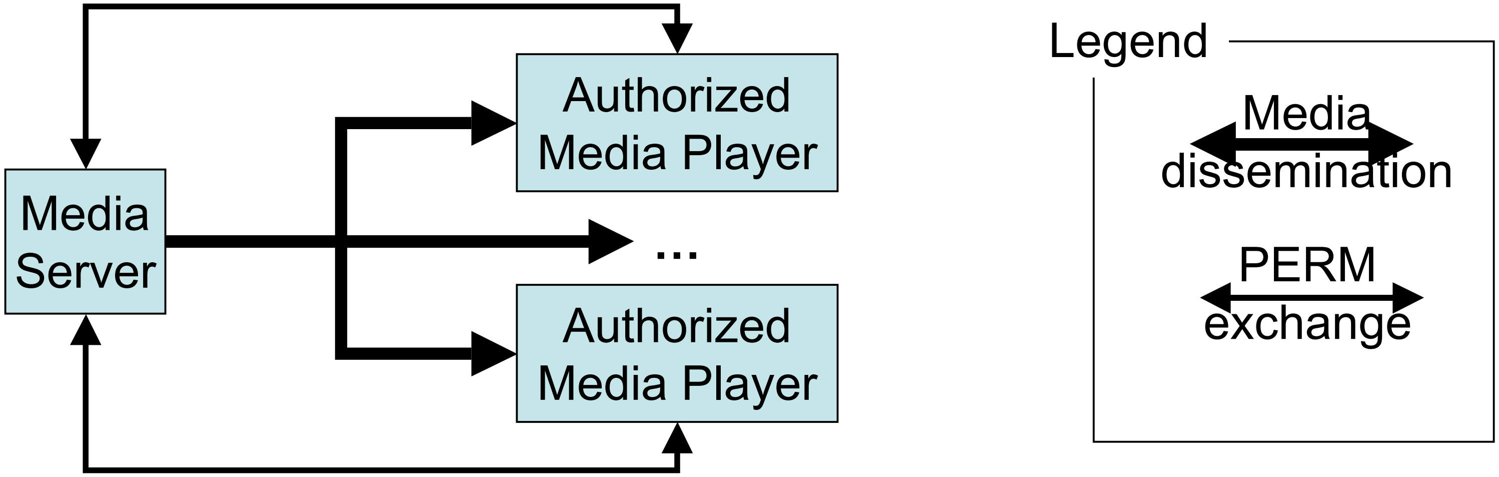
PERM can secure rights transactions between consenting persons who are motivated to protect secrets and adhere to a security policy. Creative Commons is one such application.

# The *Security Model* Alternative



- Leverages the provider/consumer security relationship
  - They are bound by a service-level agreement
  - They may be bound by a privacy & licensing agreements as well
- Content-work provider trusts customer to obey license
- Customer trusts the provider to adhere to an SLA
  - Provider protects customer’s personal, service, and billing info
  - The customer must want to preserve the security relationship

# PERM’s as a Security Protocol



- PERM can serve as secure key establishment protocol
  - Key establishment procedure that has a rights payload
  - Suitable for secure systems *or* TR-DRM system
- And an open-standard rights-management protocol
  - A baseline service for e.g. home entertainment networks
  - A core protocol that supports many business models

# Summary

- PERM does not address policy enforcement on consumer electronic devices
- PERM fulfills a need for secure rights-management between provider & consumer
- PERM is a *bona fide* security protocol when there is a security relationship between provider and consumer