Digital Rights Management using a Master Control Device

Imad Abbadi
Information Security Group
Royal Holloway, University of London
i.abbadi@rhul.ac.uk

Main Idea

- Protect content from being illegally used by unauthorised users.

- Allow consumers to use content on all devices they own.

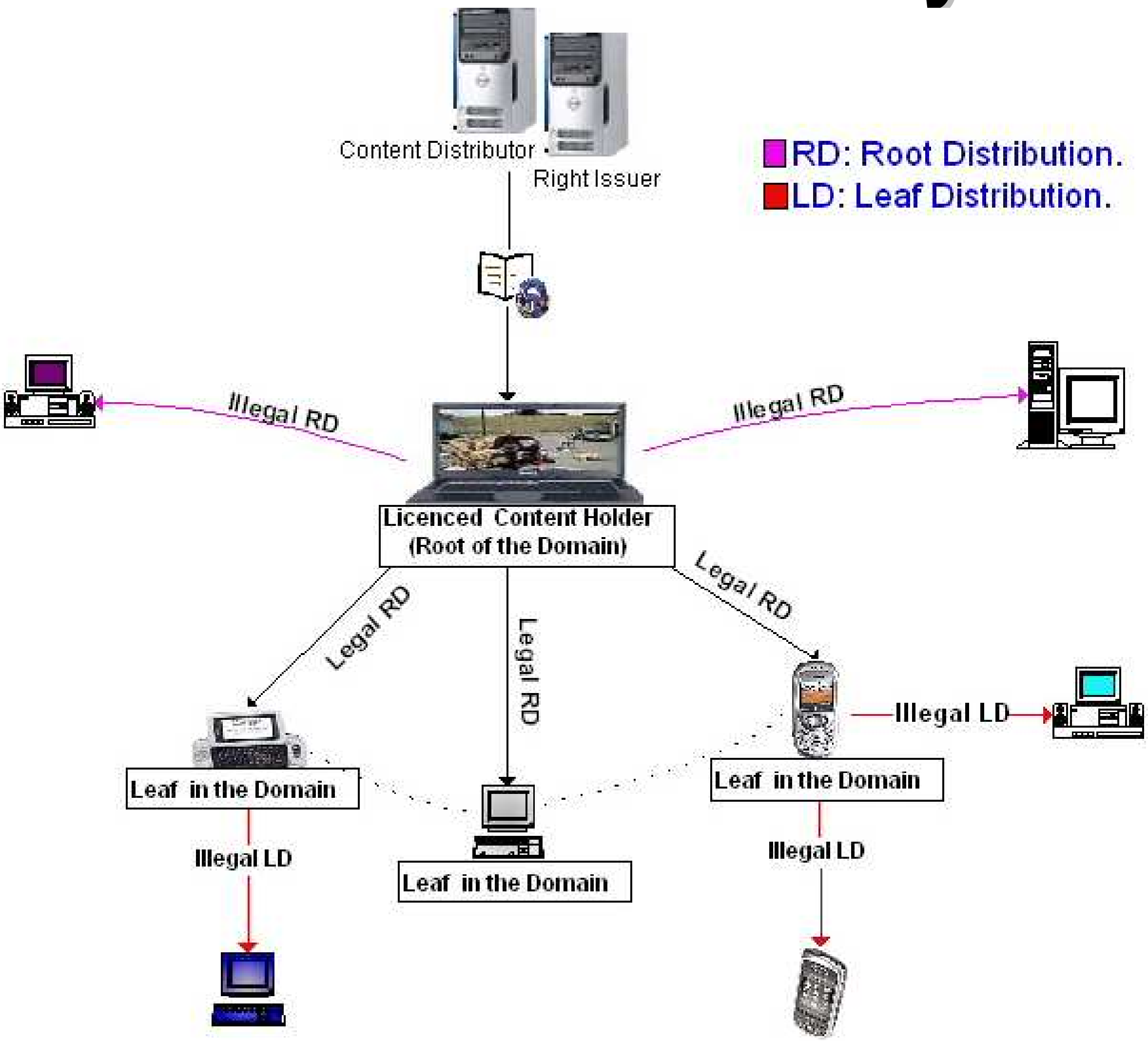
- Allow controlled content sharing.

What is the problem?

- How things should be?

- What is happening in practical life?

Content Piracy



Content Distributor

Right Issuer

🟪RD: Root Distribution.

🟥LD: Leaf Distribution.

Illegal RD

Illegal RD

Licenced Content Holder
(Root of the Domain)

Legal RD

Legal RD

Legal RD

Leaf in the Domain

Leaf in the Domain

Leaf in the Domain

Illegal LD

Illegal LD

Illegal LD

Existing Schemes

- **How they addressed the problem?**
- Domain
- Controlled using a counter

- **Have major security flaws and usability limitations**
- Abused by leaving and rejoining
- Expandability
- Backup/recovery
- No binding between content protection key with domain owner

Our Solution

- Domain consists of devices owned by a single owner
- Each domain has two domain limits.
- Each domain has a domain-specific key used for content protection
- Protecting the domain key
  - Securely stored inside domain devices
  - Not available in the clear even to the domain owner.
  - Bind domain key to the domain owner

Binding domain devices to a single owner

- Authenticating the domain owner using two-factor authentication, which involves:

- “something the domain owner has”, i.e. a Master Control device

- “something the domain owner is or knows”, i.e. a biometric or password/PIN authentication mechanism that is implemented by the Master Control device.

The Master Control Device

- Controls and manages consumers domains.
- Binds devices joining a domain to itself, as follows:
  - using a key that can be conditionally transferred from the master control device to other devices joining the domain.
  - devices joining a domain must be in physical proximity to the master control device.
- Binds itself to a single owner, as follows:
  - authenticating the domain owner using biometric or password/PIN authentication mechanism (before adding a device into the domain).

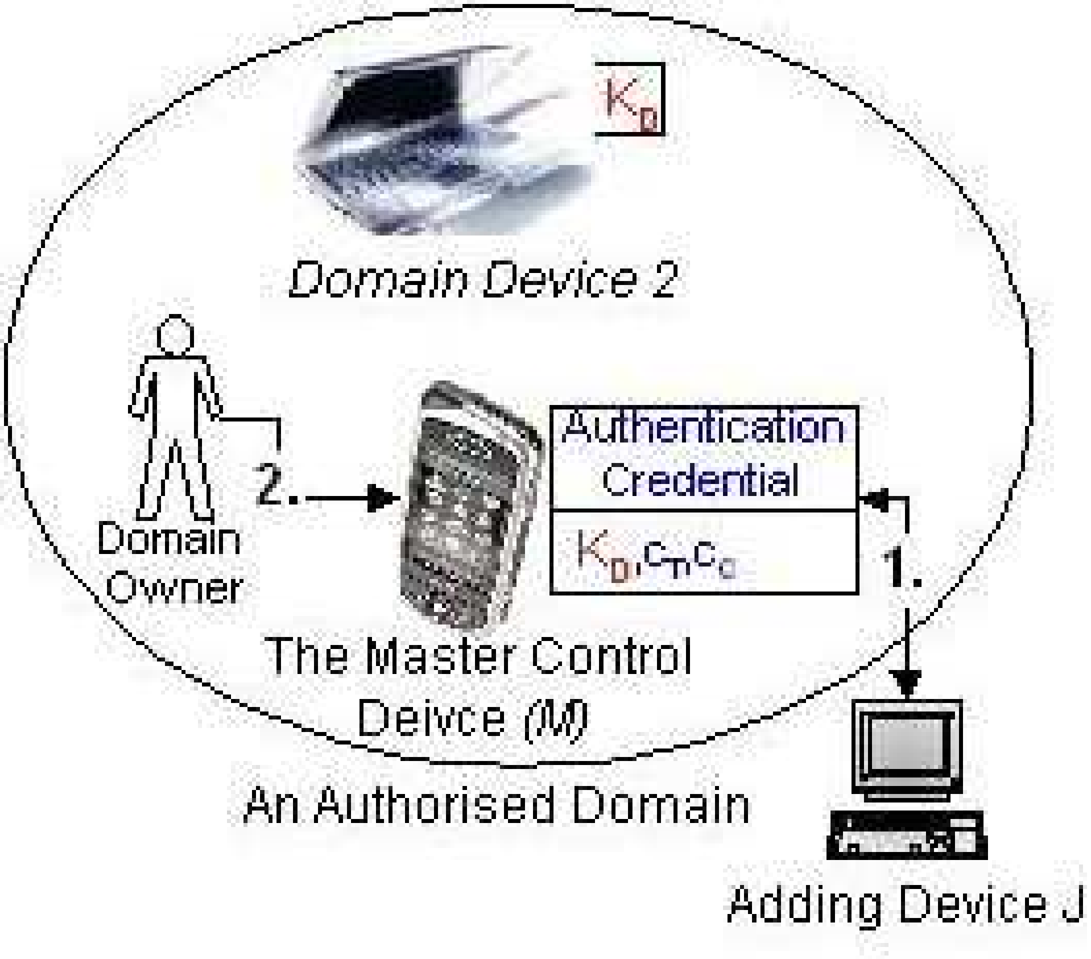
Domain Establishment Workflow

- The DRM agent in the master control device instructs the domain owner to provide his authentication credential.

- The domain owner provides the authentication credential, which gets securely stored by the master control device.

- The master control device generates: the domain key and the two domain counters, and then associates them with the provided authentication credential.

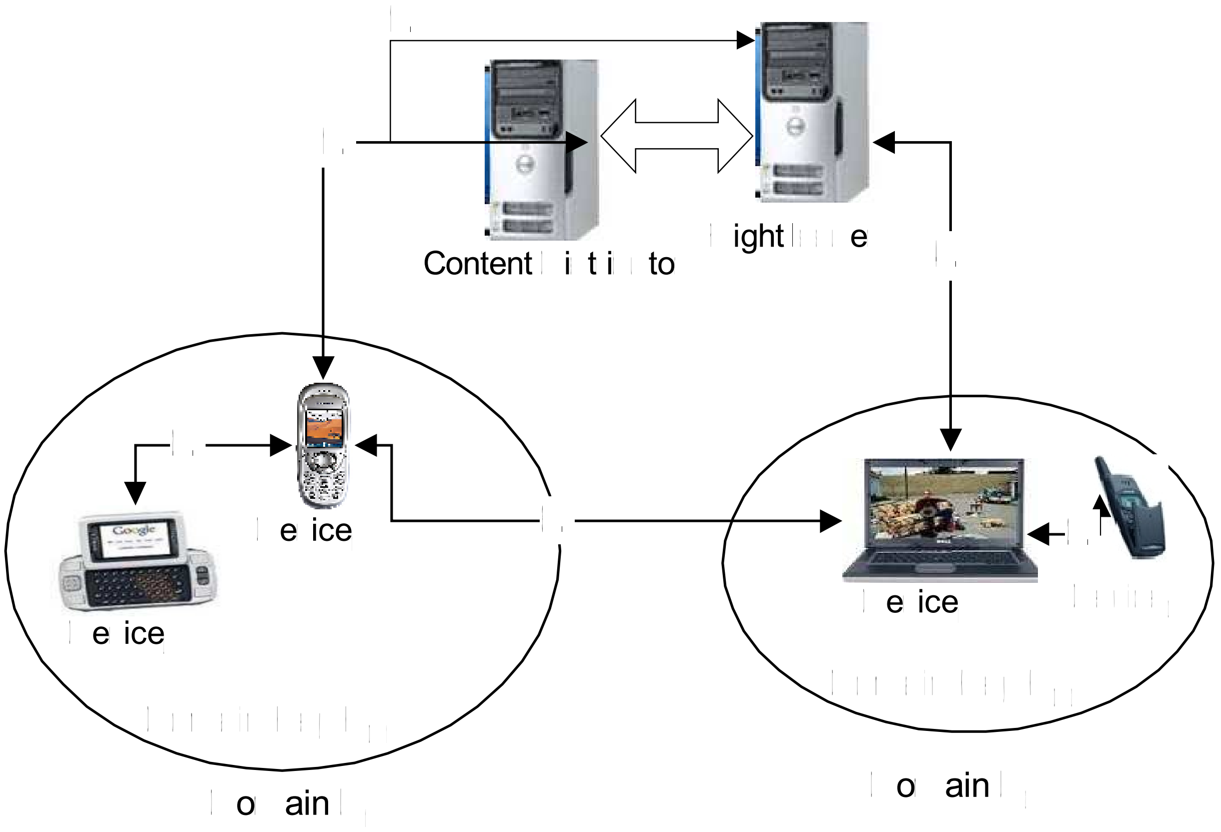
Adding a device to a Domain



The Master Control Device:

- Authenticate the domain owner using biometric or password/PIN
- Verifies device *J* is Trusted?
- Checks domain Counters?
- Checks physical proximity?

Exchanging Content



Conclusion

The proposed scheme addresses:

- **Root Distribution and Leaf Distribution.**
- **Other DRM requirements, such as:**
- Flexibility
- Backup and recovery
- Ease of Use
- Performance

Thank You…*

Questions?

* This work is partially funded by Associated Newspapers Ltd – UK.