available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

A personal mobile DRM manager for smartphones

Siddharth Bhatt[a], *Radu Sion*[a,*,1], *Bogdan Carbunar*[b]

[a]*Stony Brook Network Security and Applied Cryptography Lab, Computer Science, Stony Brook University, Stony Brook, NY 11794, USA*
[b]*Applied Research and Technology Center, Motorola Labs, 1295 E. Algonquin Rd. IL05, Schaumburg, IL 60195, USA*

ARTICLE INFO

Article history:
Received 11 February 2009
Received in revised form
5 March 2009
Accepted 6 March 2009

Keywords:
Digital Rights Management
Mobile devices
Cellular
Smartphones
ORCON policies

ABSTRACT

In this paper we report on our experience in building the experimental Personal Digital Rights Manager for Motorola smartphones, an industry first.

Digital Rights Management allows producers or owners of digital content to control the manner in which the content is consumed. This may range from simply preventing duplication to finer access policies such as restricting who can use the content, on what devices, and for how long. In most commercial DRM systems, the average end user plays the role of content consumer, using DRM protected content made available by a service. Here we present a personal digital rights system for mobile devices where the end user has the ability to place DRM protection and controls on his or her own personal content.

We designed the personal DRM system to allow users of a mobile device to transparently define controls and generate licenses on custom content and securely transfer them to other mobile devices. A user is able to define and restrict the intended audience and ensure expiration of the content as desired. Compatible devices automatically detect each other and exchange credentials. The personal DRM system on each device safely enforces the content usage rules and also handles moving licenses between devices while preventing leakage of content. We implemented a prototype of our system on Motorola E680i smartphones.

1. Introduction

Digital Rights Management (DRM) refers to a collection of technologies used to control access to digital data. It is generally used by copyright owners or publishers of digital content to specify who can access the data and in what manner. This is accomplished by specifying the rights that the user of the content has, and the restrictions on the consumption of the content.

For instance, an online movie rental service that lets users download video files to a personal computer for a certain period uses DRM protection to enforce the terms of the rental license. Thus, even though the downloaded file is on the user's computer and may be seen as being under the "user's control", DRM is used to lock the file and essentially make it difficult to play after the expiration of the rental period.

DRM is also used in mobile devices where, driven by huge advances in network infrastructure support as well as a boom in the number of interconnected personal devices, the modern mobile customer experience has become increasingly compelling. A large set of novel communication and content streaming services have become accessible, ranging from simple SMS messaging to live TV broadcasts. This trend is likely to accelerate with the eventual introduction of fully packet switched 4G networks featuring increased bandwidth and global mobility.

* *Corresponding author*. Tel.: +1 631 731 1695; fax: +1 631 632 1690.
E-mail addresses: sid@sidbb.com (S. Bhatt), sion@cs.stonybrook.edu (R. Sion), carbunar@motorola.com (B. Carbunar).
[1] Supported by Motorola, NSF (IIS-0803197, CNS-0627554,0716608,0708025), IBM, Xerox, CEWIT.

doi:10.1016/j.cose.2009.03.001

Mobile devices are increasingly being used as personal media centers. Traditional boundaries between the roles of information "producer" and "consumer" are blurring as device users produce and distribute content such as personal pictures and videos on their mobile devices. In such a scenario, it makes sense to have technology that lets the individual user retain control over the dissemination of such personal content. It is essential to enable user-level DRM controls for content access, data integrity and rights management.

Currently, most DRM technologies are geared toward the end user being the content consumer, and the DRM protected content coming from a commercial service. The model can be viewed as analogous to a client–server system, with the end user being the client that consumes the content provided by the server, e.g. an online music store. In contrast, we see the need for a personal DRM system that can be viewed as analogous to a peer-to-peer model, with every end user being able to act as content producer, and assert rights and retain control of his or her own content. Any given device can act as both sender (content producer) and recipient (content consumer).

In this paper we discuss a new personal digital rights management system for mobile devices in which a user is able to transparently define, generate, package and migrate content licenses between mobile devices on demand. Our system lets a user select a certain piece of content on a mobile device and associate various controls with it and specify who can consume the content. The controls may include restrictions such as how many times the content can be played etc, as well as whether the content may be exported to other devices.

We designed the personal DRM system and developed a prototype on the Motorola E680i smartphone. Each device automatically detects other personal DRM enabled devices in its proximity and exchanges credentials with them. It presents the user with an efficient graphical user interface that can be used to specify restrictions on any digital content on the phone, and lets the user select a target device to send the content to. Files are transferred between devices using a secure transfer protocol. Each device can play any content it is authorized to, and safely enforces the controls associated with the protected content.

2. Background

The core entities in a Digital Rights Management system are the users, the content and the rights. A DRM system design models these entities and the relationships between them, as shown in Fig. 1. A DRM system can also be modeled by more complex relationships between finer-grained entities, as described in Iannella (2001). For instance, the "rights" entity can be broken down into usage rules which include the obligations of the rights holder, such as paying for use, and permissions and constraints. Permissions specify *what* the user can do with the content, and constraints specify *how*. For instance, permissions may specify that the user can play or print the content. The constraints on the play permission may specify that the content can be played between certain dates.

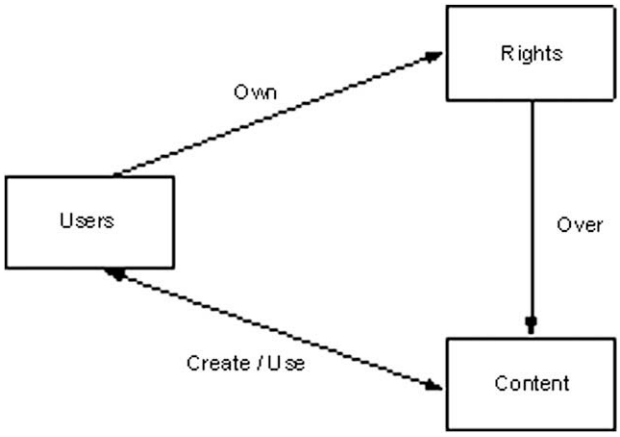

Fig. 1 – Core entities in a DRM system.

The constraint on the print permission may specify how many times the content can be printed.

In terms of actual implementations, Park et al. (2000) describe and compare various security architectures for use in dissemination, control and tracking of digital content, such as encapsulated or independently distributed access rights, online or offline access, virtual machine based architectures etc.

In most such traditional DRM models, all devices are equally trustworthy and have discretionary control over all protected content. Popescu et al. (2004) suggest a deviation from this paradigm and propose a multilevel security policy based model that differentiates between devices based on their types and tamper-resistance properties. For instance, a device that has high tamper resistance would be restricted from sending protected content to a device with low tamper resistance, or a device would not be allowed to send protected video content to an audio device.

Trusted computing (Weiss, 2006) is increasingly being touted as an ideal platform for the implementation of digital rights management. In spirit, trusted computing suggests there should be mechanisms in place to enforce what a device can or cannot do. This is enforced by a hardware chip called the trusted platform module which provides tamper-resistant security functions. Several models of DRM on trusted platforms have been suggested (Cooper and Martin, 2006; Erickson, 2003; Reid and Caelli, 2005). Using tamper resistant trusted computing hardware would prevent attacks based on dismantling hardware and reading sensitive information from chips. The trusted computing base would be outside the operating system, and so it would be possible to use unmodified software and yet have strongly enforced DRM. Trusted hardware would also provide a component for providing a tamper resistant clock source which is crucial for DRM systems.

In this paper we propose a software based DRM for personal content generated on mobile devices, in particular a Motorola E680i phone. Our goals, of protecting and enforcing access control rules on content generated on mobile devices would certainly benefit from the existence of a trusted platform module. However, we believe the cost of such devices and the incentives attackers have to circumvent protection