Personal Digital Rights Management for Mobile Cellular Devices

Siddharth Bhatt[1], Bogdan Carbunar[2], Radu Sion[1], and Venu Vasudevan[2]

[1] Network Security and Applied Cryptography Lab
Computer Science, Stony Brook University
{sbhatt,sion}@cs.stonybrook.edu
[2] Pervasive Platforms and Architectures
Motorola Labs
{carbunar,vvenu}@motorola.com

Abstract. Driven by an unparalleled advance in network infrastructure support as well as a boom in the number of interconnected personal communication, computation and storage devices, the modern mobile customer experience has become increasingly compelling. Traditional barriers between the roles of information consumer and producer have disappeared. Users increasingly produce and distribute valuable and often personal content such as pictures and free or purchased copyrighted media. It becomes essential to enable user-level DRM controls for content access, data integrity and rights management.

In this presentation we will overview the design and implementation of a a personal digital rights management system for mobile devices. The Personal DRM Manager enables user-defined ORCON-type controls for personal content originating in a cell phone or other mobile device. Users can transparently define, generate, package and migrate content licenses between mobile devices on-demand. Networked cellular devices cooperate in the enforcement mechanisms.

Design. Main user-land components include: license generation, content packaging, secure networking over both blue-tooth and 802.11, and compliant content rendering. A device can naturally act as both sender and recipient. Additionally, we developed a public key infrastructure to allow devices to be both uniquely identified and to allow for session key exchanges with forward security.

We demonstrate the main features of our system, involving a set of live E680i GSM devices. A subset of the devices will generate content and transparently associate both state-full and state-less use licenses with the newly generated content. We will illustrate scenarios ranging from simple use-counters (this content cannot be played more than N times) to more complex conditional licenses such as (this content can be accessed only between October 7th and October 9th at full resolution and down-sampled to 56KBps otherwise). Additionally, we will discuss a few of the design choices for both the enforcement and the secure network hand-shake protocols.

E680i Platform. The Motorola E680i is a multi-feature palm-size embedded-linux based cell phone with direct MPEG4 video capture and playback, a real-time 3D sound engine and 3D stereo speakers, an integrated MP3 player, a large capacity internal memory of up to 2GBytes, a removable SD memory card slot, a 240 x 320 color screen, and an integrated VGA camera with 8x zoom.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-3-540-77366-5_37

S. Dietrich and R. Dhamija (Eds.): FC 2007 and USEC 2007, LNCS 4886, p. 246, 2007.