Security Considerations for an Idealised DRM Framework

WORK IN PROGRESS

Alapan Arnab and Andrew Hutchison
Computer Science Department
University of Cape Town
Rondebosch, 7700
{aarnab, hutch}@cs.uct.ac.za

***Abstract*— There are currently no complete solutions for digital rights management. In [1], we describe a possible solution, which makes use of various web services to fulfil its functions. In this paper, we discuss some of the security considerations that are required in our proposed system; many of these considerations apply to web services in general.**

I. INTRODUCTION

Digital Rights Management (DRM) aims to provide persistent access control over digital data. In the past few years, DRM has been seen as a solution to media piracy and has been widely implemented for distributing music online. While the concepts used in DRM can be extended to protect any type of digital data, there have been very few products that offer such services. While, Microsoft's Rights Management Services (RMS) does have many of the features desired in a general rights management system, the current system has too many flaws for use as a full blown security system.

In [1], we proposed an idealised framework for rights management that aims to overcome many of the flaws in RMS and other current DRM systems. Our framework is componentized, with each component serving one or more roles proposed by Bartolini et al. [2] and Arnab et al. [3] Our proposed architecture is shown in Figure 1 and as discussed in [1], each component can serve as a web service thus allowing for scalability and cross platform portability.

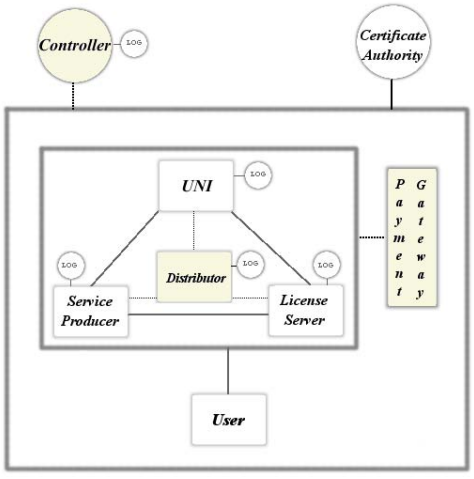

Fig. 1. Architecture of our proposed DRM framework [3]

ITU-T's X.800 recommendations define a set of security services that should be provided by a system to ensure its security [4]. In this paper we discuss how some of these services will affect the design of our DRM framework. The services we discuss are listed below, and while the last service, *availability*, is not explicitly stated in X.800, many consider it as an essential security service [4].

- **Authentication**
- **Access Control**[1]
- **Data Confidentiality**
- **Data Integrity**
- **Non-Repudiation**
- **Availability**

II. SECURITY SERVICES

In this section, we shall detail some of the design considerations for each of the security services mentioned in the previous section.

A. Authentication

Authentication is defined in RFC 2828 as *the process of verifying an identity claimed by or for a system entity* [5]. RFC 2828 separates the process of authentication into two steps – Identification, where an entity presents an identifier to the security system and Verification, where the service can corroborate the entity and the identifier. In our system, there are two distinct areas where authentication is crucial.

Firstly, when an end user wants to use a DRM protected work, the user must be authenticated and the user's right to access the work must be established. The DRM Controller or Virtual Machine (described in more detail in [1]) is the system entity and resides in the user's machine. The DRM work has an associated use license that the DRM controller will use for corroboration. In our framework, we prescribe the use of X.509 certificates as the user's identifier. The DRM controller will match the user's certificate and the users listed in the use license for authentication.

The other area where authentication is crucial is between the services themselves. Although the services can be deployed as totally anonymous, free and open services that do not require any form of authentication to use them, they should also cater for more restricted deployments, like online stores. As mentioned previously, all entities in our framework make use of digital

[1]The purpose of a rights management system is to create and enforce persistent access control of data regardless of the location of the data. The access control service (and other services) in the list refers to the access controls for the services in the framework itself.

certificates and we intend extending the use of certificates for all authentication purposes. The Certificate Authority can be used in the process of verification.

B. Access Control

RFC 2828 defines access control as *protection of system resources against unauthorized access* [5]. As discussed earlier, access control mechanisms for the services are not mandatory for implementation, but would still be required for some scenarios. We propose the use of access control lists together with certificates for authenticating and determining access control rights for the services.

C. Data Confidentiality

RFC 2828 defines the data confidentiality service as a *service that protects data against unauthorized disclosure* [5]. This service is different to privacy which is discussed in section III. Confidentiality of data must be ensured at all times in the DRM framework, as any unauthorised access to data will render the system a failure. There are two distinct areas where data confidentiality must be ensured - during communication between services and the storage of data by the services.

Data confidentiality during transmission can be ensured through the use of secure communication sessions between the web services. Established protocols such as TLS can be used for this purpose. Alternatively, the data can be encrypted using the public key of the recipient and then embedded in SOAP messages. Because we aim to create each service as a stand alone web-service, it is desirable to make use of the second approach.

The storage of data during and after processing must also be considered. For example, a creator would submit their work to be DRM enabled to the service producer. It would defeat the purpose of DRM protection, if the work is stored unsecured by the service producer during and after processing. The use and enforcement of access control to the service becomes crucial at this point. Deletion of the original work after production would help with data security but the securing of data during processing is a difficult challenge.

D. Data Integrity

The data integrity service *protects against unauthorized changes to data, including both intentional change or destruction and accidental change or loss, by ensuring that changes to data are detectable* [5]. Currently, the data integrity service makes use digital signatures and we intend to do the same.

E. Non-Repudiation

The non-repudiation service aims to *provide protection against false denial of involvement in a communication* [5]. The use of logs could be used to keep a record of activity, but that would not necessarily be enough for the purpose of non-repudiation, as it could be argued that the logs were falsely generated. In our framework and in the roles described by Bartolini et al., the controller is a trusted third party that monitors the DRM transaction. The controller can be used for the purpose of non-repudiation but it does bring up questions of privacy. An alternative is for the use of *trusted entities* as used in Microsoft's RMS [6], but that would limit the use of the framework.

F. Availability

RFC 2828 defines availability as *a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system* [5]. With the possibility of global deployment, the availability of some of the services like the license server and distributor becomes important. However, there are no easy solutions against a denial of service attack. The framework must also ensure that the services are scalable as that could also impact on availability. We hope our componentized approach will overcome most of these problems.

III. Privacy

Privacy is one of the biggest concerns for current DRM systems [7] because DRM systems potentially have the ability to monitor the activities of the end user. For this reason, privacy concerns must be addressed by our framework. Privacy concerns are further amplified in our framework because of the componentized structure. Potentially different systems and companies may implement the various components and the users would not like their private information shared between the various services. For example, the user would be willing to share his/her bank details with the payment gateway and not with the license server.

To get round this problem, we are looking at a solution similar to the dual signatures used in the Secure Electronic Transaction (SET) protocol [4]. This would allow different services to communicate without sharing confidential data. The use of an external control set as discussed in [1] gets round many of the privacy concerns highlighted by Mulligan et al. like tracking usage of DRM works [7].

IV. Future Work

The current focus is to create a complete specification of the system. This includes the message formats, the communication protocols and the specifications must take into account the security considerations discussed in this paper.

V. Conclusion

In this paper we presented the security considerations that must be taken into account for the design of a complete DRM framework. However, many of the solutions to these problems need to be further investigated and detailed before integration into the proposed framework. Most of the security considerations detailed in this paper can be applied to web services in general.

References

[1] A. Arnab and A. Hutchison, "Idealised framework for rights management," submitted to the 4th ACM workshop on Digital Rights Management
URL: http://people.cs.uct.ac.za/∼aarnab/masters/proposal.pdf.

[2] F. Bartolini, Cappellini, A. Piva, A. Fringuelli, and B. M, "Electronic copyright management systems: Requirements, players and technologies," in *Proceedings of the Tenth International Workshop on Database and Expert Systems Applications*. IEEE, 1999, pp. 896–899.

[3] A. Arnab and A. Hutchison, "Digital rights management - an overview of current challenges and solutions," in *Presented at Information Security South Africa (ISSA) Conference 2004*, 2004.

[4] W. Stallings, *Network Security Essentials – Applications and Standards*, international second ed. Prentice Hall, 2003.

[5] R. Shirey, "Rfc 2828 – internet security glossary," 2000,
URL: http://www.faqs.org/rfcs/rfc2828.html.

[6] "Technical overview of windows rights management services for windows server 2003," Microsoft," White Paper, 2003.

[7] D. Mulligan, J. Han, and A. Burstein, "How DRM based content delivery systems disrupt expectations of "personal use"," in *Proceedings of the 2003 ACM workshop on Digital Rights Management*. ACM, 2003, pp. 77–89,
URL: http://doi.acm.org/10.1145/947380.947391.

Authors' Biography

Alapan Arnab graduated with a BSc (Hons) in Computer Science (First Class) from UCT in 2003. He is currently a MSc candidate in the field of digital rights management. Andrew Hutchison is an Adjunct Professor of Computer Science at UCT. Both are members of the Data Network Architectures research group.