ECE 544 - Trustworthy Computing

Final Project Phase 2

Digital Rights Management: “Distributed DRM With Lending”

Derek Wang

Kaitlin Menzie

Zachary Windoloski

Don Liang

1. Abstract

When dealing with Digital Rights Management (DRM), there has always been a compromise between freedom and security. Too much restriction, and legitimate users of software end up forfeiting some of their rights as content holders. When systems lack proper security, users can break copyright and license laws by being able to easily share content over the internet without repercussions. This takes away revenue from content creators. With the current security measures, it makes sharing content difficult. While you can easily lend a friend a book, it is not easily as possible to lend a friend your ebook. Especially not without needing a main server being involved, which is not ideal. What we are proposing is a system that will allow users to share peer to peer, but without the constant use of a main server. We will have a main server for registering users, but the files exchanged will be tagged with a timestamp that tells decrypting softwares whether it is in the time allowed to decrypt for a certain user. Borrowers will be able to only use it in a certain time, while lenders will only *not* be able to use it in that time. This system works better than today's system because it tries to solve the issue of sharing, which has not been done much, while removing the need for a server to be part of it at all times.

2. Specific Aims

There are varying solutions to the problem of Digital Rights Management. All of these solutions need to balance between the level of security and the inconvenience to the user that is brought about by the security solution. For example, one non disruptive DRM technique is encrypted with a CD-Key such that only someone possessing a key is able to access and download a file. Another highly disruptive DRM solution is checking in constantly with an

online server. With a consistent internet connection, this theoretically should cause no problems. If there is ever a disruption, however, whether it be due to power, server maintenance, or internet availability issues however, the service will be unavailable. This can be extremely frustrating, especially when hacked or "cracked" copies of the game are more convenient to use than a legitimate copy.

One of the big problems with almost any DRM solution is the lack of an ability to loan your digital media or license. As there is nothing more annoying than having an inconvenient DRM technique with breaks in service, we want to solve this issue in a low impact way. This means that we want to check in with a server as little as possible and never have any breaks in availability of our service. An additional concern we must deal with is the integrity of the license that is being loaned, in that only one person should be able to access one instance of a licence at a time to ensure that no laws are broken.

3. Background and significance

With the popularity of the personal computer, the ability of any given user to exchange content with other users has increased exponentially. As a result, the possibility of users distributing, editing, and modifying copyrighted works also increases exponentially. In order to counter this possibility of "digital piracy", companies that distribute and license copyrighted content turn to DRM(Digital Rights Management) in hopes of deterring and/or preventing "digital piracy". DRM refers to technologies that restrict the usage, modification, and distribution of copyrighted work.

By using DRM, the aim of these companies is to regulate the distribution of their copyrighted materials as is regulated in physical mediums. That is, for the amount of copies of a copyrighted material in circulation to be no greater than the amount permitted to be in circulation. For example, it is not cost feasible given a paper copy of a book to replicate that book exactly as was printed by the manufacturer. However, in a digital medium this would be very easy. DRM is an attempt to provide an analogous regulation in digital mediums.

There are several popular DRM techniques,

- Limited Install Activation
- Persistent Online Authentication
- Software Tampering
- CD Keys

The current popular DRM techniques do not allow for users to lend content to each other in the same way that one would be able to lend a physical copy of content to another user. If there was a method where users could lend content to each other in a way that doesn't violate the purpose of DRM(inc, it would bring the distribution and sharing of digital content closer to the distribution and sharing of physical content.

4. Preliminary studies

In their 2011 paper, "A Decentralized Authorization Scheme for DRM in P2P File-sharing Systems," Qiu, Tang et al present a method for securely integrating DRM into traditional P2P file-sharing systems. They argue that a decentralized system is favorable a) because existing P2P frameworks will need rights management implementations as more users

create their own content to distribute, and b) the scalability of such an environment (one balanced between providers and consumers) would suffer if the system were centralized. They review those centralized implementations nonetheless, as well as previous decentralized implementations. However, they argue that the existing decentralized ideas either don't provide rights management beyond the scope of the P2P environment, or inhibit normal usage. Therefore, they propose a new approach. The central mechanism in their proposal is a proxy re-encryption scheme.

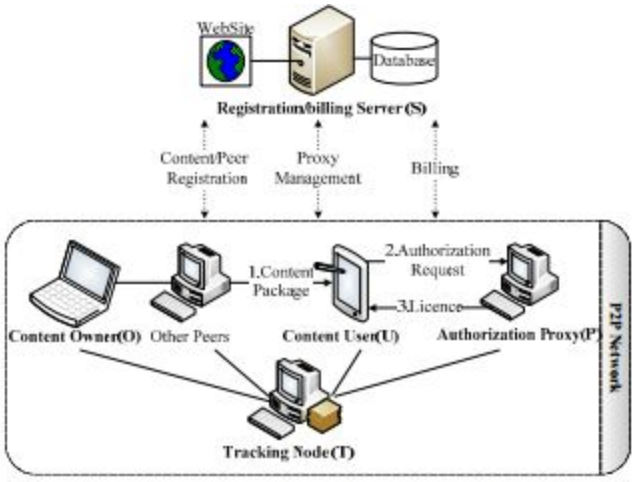


Figure 1. The proposed system model.

They also include a 'trusted server' for payment and key distribution (see figure). Other than that, the structure follows that of a regular P2P setup.

Their procedure has five phases. First, the users authenticate their identities with a server and receive a key. Second, when a peer wants to begin a transfer, they grant a third party (in this case, another peer) a 'qualifying certificate', which gives that party the ability to decrypt/re-encrypt data with their key (but doesn't give them access to the key itself) and their ciphertext. Third, the neutral party packages the content with the first peer's identifiers. In the fourth step, the second peer (the content consumer), authenticates itself to the trusted server (and

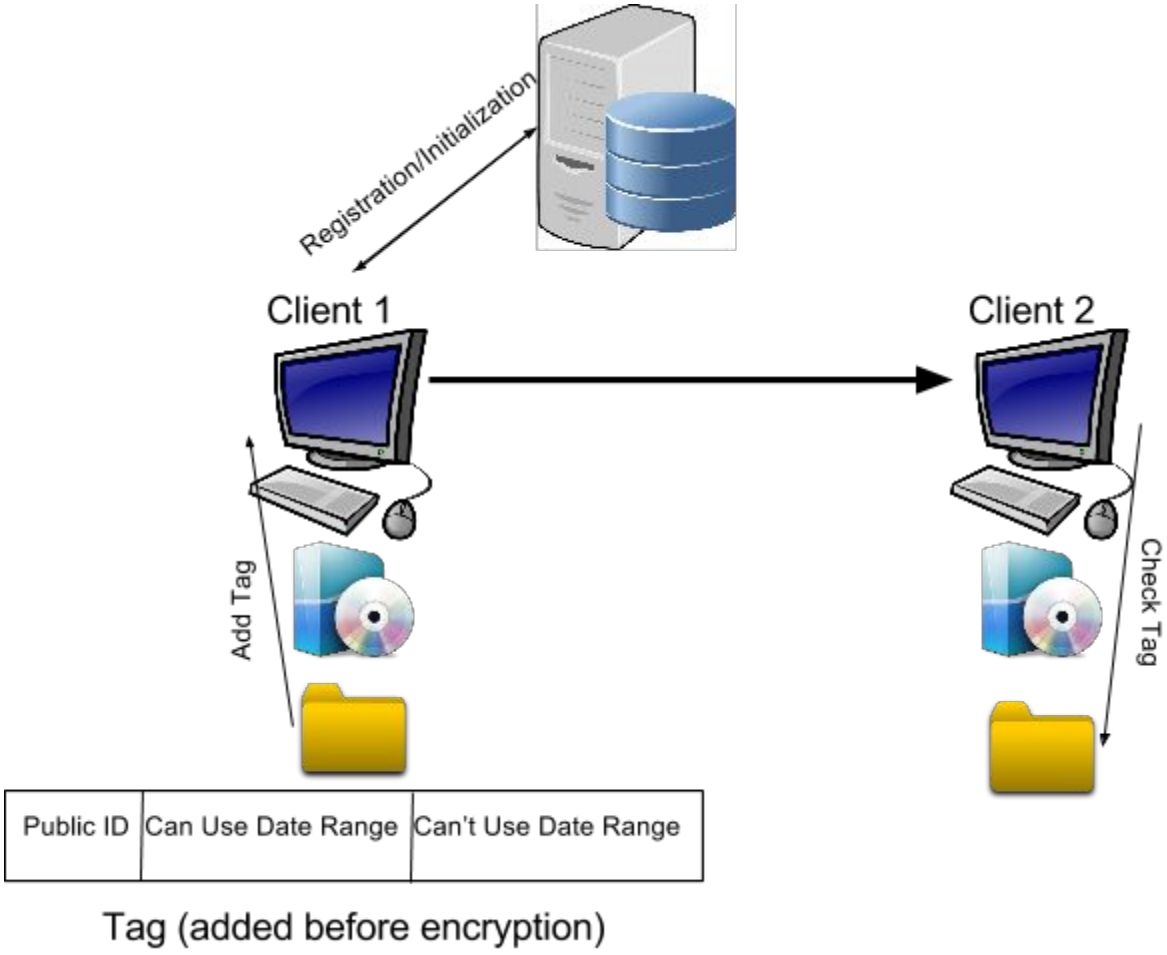
follows the necessary steps, ie payment, to get access to the DRMed content), then has the neutral party generate a license for the content it wants that gives them the unique ability to decrypt a re-encrypted copy of the ciphertext for their new content. Finally, when the second peer (content receiver) wants to access their content, they use the license granted by the third party to do so.

Our proposed procedure is very similar, except that we a) use plugins on both users' computers to act as a simulated third party, and b) extrapolate this idea so that peers can 'lend' each other content.

5. Research design and methods

A research methodology, collection of data, and data analysis are necessary for research ideas such as new encryption algorithms and network protocols. For such research projects data such as encryption speeds, time to break encryption, file size, and network impact might be useful. Our research proposal leans more toward a new methodology proposal such that digital media can be shared as a physical book or movie might be. Our proposal can be combined with existing DRM methods and contains no new encryption, authentication, or network transfer ideas. As a result, collection of data is absent from our research proposal. This idea that can be combined with existing DRM methods such that digital media can be shared in the way that a physical book or movie might be shared.

6. Implementation details or Test Bed



Our proposal is a system in which media can be shared securely without two clients using the same license at the same time, even offline. The only new aspect of our proposal is the use of "tags" on individual media files. These tags contain information pertaining to who is allowed to access the media as well as when they are allowed to access it. All other aspects of our system already exist and are based upon existing cryptographic methods.

In order for our system to work, our media files must be able to only be accessed by the correct user. In order to achieve this, we would need our media files and media library to be in a

customized format that only our software can read. Each individual file would have a header containing only enough data to recognize the file in plaintext, as well the encrypted data and usable time tag. The usable time would be changed as a file is lent to another user such that the original owner cannot use the file for the the amount of time that the file is lent to the other user. The recipient would receive a file encrypted with his public key, and the tag on the file would include the amount of time that the user would be allowed to use the file.

Each user would be able to read files meant for them and only them, and so each user would need both a public and private key. These public and private keys are managed by a server which contains tables of public and private keys as well as which user each key pair belongs to. Logging into the server would be dealt with using username and passwords. The original registration or logging in where an instance of our software obtains their public and private keys would be the only time our software would need to access a server.

7. Literature cited

Qiu, Qin, Zhi Tang, and Yinyan Yu. "A Decentralized Authorization Scheme for DRM in P2P File-sharing Systems." 2011 IEEE Consumer Communications and Networking Conference (CCNC). Web. 17 Nov. 2015.