Innocence of Traced Traitors

Jesse Wu

Friday, 21 October 2005

Abstract

As digital piracy becomes more common everyday, there needs to be a way to stop it. Chor et al [1] introduces the idea of a Traitor Tracing Scheme, a way to trace keys that have been redistributed to non-authorized users.
Although traitor tracing is advantageous, some of the keys found in the possession of non-authorized users by the Traitor Tracing Algorithm, do not always indicate that the owner of the keys, have been redistributing the keys for malicious intentions.
This paper discusses the problems that may occur including False Positives and the extremely difficult task of mapping keys to people.

1 Introduction

Waves of piracy constantly consume our internet bandwidth, while companies lose millions. There should be a way to stop it. The paper by Chor et al [1] on Traitor Tracing offers a notion on how to counter piracy, i.e. by tracing keys.

Chor et al. [1] define a **traitor** as *"the (set of) authorized user(s) who allow other, nonauthorized parties, to obtain the data."*. If an authorized user's set of keys had been intercepted and stolen before they were even touched, and these keys are found to be used in pirate decoders, then these 'authorized' users would most likely be labeled traitors by this definition until proven innocent. How can one be certain that the authorized users allowed the nonauthorized users access intentionally? The keys could have been accidentally shared[3]. The **owner** of a key is one who is authorized to use the keys.

Boldyreva and Hakobsson [3] defines **accidental sharing** as the "sharing caused by theft of the proprietary secret key". Relating this term to Traitor Tracing, accidental sharing would be the sharing caused by the theft of an authorized users' set of keys. According to this definition of Traitor Tracing, accidental sharing can be seen as the result of theft of an authorized user's set of keys.

A Traitor Tracing Scheme [1] consists of three components, a user initialization scheme, an encryption/decryption scheme and a Traitor Tracing algorithm. The user initialization scheme is where a set of keys is allocated to the authorized users. An encryption/decryption scheme describes how the content is converted to a secure from plaintext, and recovered from the secure form. The Traitor Tracing algorithm is a method for tracing keys back to their owner.

2 Traitor Tracing Schemes

Traitor Tracing schemes could be used in many different ways. For a such a scheme to be successful, specific goals and properties [7] must be satisfied.

The goals and properties of this scheme include deterring authorized users from distributing keys, being able to trace unauthorized use of keys, but must not allow for false positives. When unauthorized use has been detected, the traced keys should be disabled, and then the scheme should be able to supply some legally acceptable evidence of the activity.

The idea of being able to trace keys is such a good idea. It reduces piracy in many ways. Authorized users would be discouraged from releasing keys to nonauthorized users, just by knowing that it could be traced back to them. The Traitor Tracing algorithm is used to determine which keys have been used in a found pirate decoder.

The next two subsections give a brief description of the advantages and disadvantages of each type of Traitor Tracing Schemes. The way that efficiency is measured in Traitor Tracing Schemes is also explained.

2.1 Types of Traitor Tracing Schemes

Traitor Tracing Schemes based on the paper from Chor at el [1] are either

Symmetric or **Asymmetric**. A Symmetric Scheme is one where both the data supplier and the authorized users encrypt and decrypt with the same keys. An asymmetric Scheme is a scheme where the data supplier and the authorized users have different encrypting and decrypting keys. The trade off is with respect to computational time (fast for symmetric schemes, slow for asymmetric schemes), and data redundancy (high for symmetric, low for asymmetric).

Static or **Dynamic**. Dynamic schemes are good for those situations where the keys need to be changed every now and then. A good example of this would be a subscription to pay-television service. Static schemes, on the other hand, are good where the keys probably will not need to be changed, perhaps a single-player game, for example.

There are alternative types of Traitor Tracing Schemes, summarized briefly by Trevathan and Ghodosi [7], include inserting personal information from the authorized users into the keys (this notion is similar to Proprietary Certificates [2]), *"using a stream cipher to generate a unique traceability sequence"*, and many others constructed from watermarks and combinatorics.

2.2 Efficiency of Traitor Tracing Schemes

The efficiency of Traitor Tracing Schemes is measured by three factors [1]

"The memory and computation requirements for an authorized user". These requirements must be very small since we might assume that the authorized user has a computer new enough and fast enough to perform the calculations online, it is generally not a good assumption to make in business situations.

"The memory and computation requirements for the data supplier". These requirements do not matter as much as the previous one since the data supplier can perform their computations offline.

"The data redundancy overhead". This requirement must be reasonable. To allow for traceability, there must be enough storage space to keep the extra information that the scheme demands. For Example, on a CD-ROM a few extra Megabytes is not such a big deal. But in a situation where the authorized users has a modem internet connection speed (56kbps), that increased load might be too annoying for the authorized user.

3 Innocence and Guilt

This introduces a new area of consideration: the innocence or guilt of the parties involved. We must consider the consequences of both these possible verdicts.

If someone has committed a crime, say a murder, how does the legal system determine their guilt? Evidence is gathered from the crime scenes, interview witnesses and interrogate suspects. This information is processed (for example, blood is analyzed for spatter, DNA, rate of coagulation, the testimony of witnesses are compared and analyzed.) and the courts weigh this evidence. A judgement of guilt is positively determined only when the evidence is believed beyond reasonable doubt.

In our culture, we hold that it is better for the guilty to walk free of a crime, than for the innocent to be convicted wrongly. We consider that state of affairs to be unjust, and an outrage against humanity.

3.1 False Positives

In the murder case example, there are many problems with those kinds of protocols. If these convicted suspects are in reality innocent (they did not have anything to do with the murder) then these people has been falsely convicted and are false positives. Many things that may have happened to induce the false conviction include circumstances like: The evidence at the crime scene could have been falsely planted, some evidence might have been destroyed or modified by insiders, or witnesses could be giving false evidence etc ... this is just a small subset out of all the possible circumstances.

Just as we demand that our justice system extend every effort to protect the innocent, then we must be very careful to make sure that we do not incorrectly accuse someone.

3.1.1 Effects of False Positives in real life

False positives could have a devastating effect on people's everyday lives. For example, if a person is told by a qualified professional that they have AIDS, where they really do not, they may be driven to some extreme, possibly even to ending their life.

3.2 False Positives in Traitor Tracing Schemes

The protocols used in criminal investigation are similar to traitor tracing. The Traitor Tracing algorithm finds the specified keys that are being used properly (like in pirate decoders). The keys that are found to have been used improperly by the traitor tracing algorithm, do not automatically mean that the guilty party are the owner of the keys.

3.2.1 Effects of False Positives in Traitor Tracing Schemes

A false accusation in the Traitor Tracing Schemes is *"far worse than an undetected redistribution"* [4]. False accusation could be damaging to both the data supplier and the convicted traitors involved. It could cost both the data supplier and the authorized users a lot of time and money even if, eventually, the authorized users were found innocent, and the charges dropped. Whilst an undetected redistribution might only cost the data supplier a few dollars.

3.2.2 Situations where False Positives could arise in Traitor Tracing Schemes

Similar problems to the criminal investigation example arise with Traitor Tracing schemes. Many things could have occurred to cause a false conviction. Below is a subset of these problems. [fig 1.]

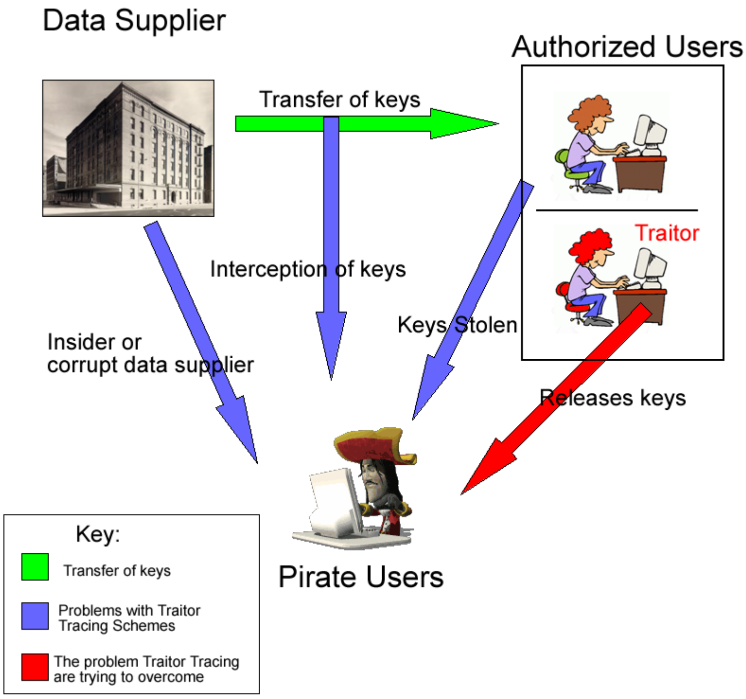

Figure 1: Problems that may occur around a Traitor Tracing Scheme

Interception of keys by pirate users. The most frequent example of this is the Man-in-the-Middle attack. This is where an unauthorized user pretends to be the authorized users that was expecting the keys. This attack can still happen whether the keys are sent by air mail, surface mail or on a securely encrypted port.

Keys stolen from authorized users. An authorized users keys might have become compromised if, for example, their computer was stolen. Perhaps they kept it on an external device (CD-ROM, USB key) which they lost later.

An insider from the data supplier. This is the most likely possibility. According to Byers et al [5] , 77 out of 285 samples of pirated popular movies turned out to have been leaked from industrial insiders.

A corrupt data supplier. This situation is highly unlikely, but not unheard of.

3.3 An Attempt to counter False Positives

To try to fix the problem, Pfitzmann proposed an extra trial protocol [4] inside an asymmetric Traitor Tracing Scheme. The data supplier tries to *"convince an arbitrary third party, called a judge, of the traced user being a traitor. For this, the information provider uses the string proof from tracing. Furthermore, the judge needs some input reliably linked to the accused user."* However, out of this arises another problem. The *"input reliably linked to the accused user"* may not be reliable at all. It also does not detect accidental sharing. Mapping **digital** input to a **physical** person is hard. This problem is discussed in the next section.

4 Mapping keys to people

It is immensely difficult to positively "map" keys to people. In real life, a particular, specific person might hold a key to a safe that contains secret information. If only that person has the key, and the secret had been revealed, then the person might reasonably be accused of revealing the information.

But, with keys, the authorized user might have accidentally shared [3] the key (e.g. the key got stolen) instead of sharing it intentionally.

The same problem occurs with the public/private key encryption systems [6]. How does one know that a public key definitely belongs to the person that it is supposed to belong to? When encrypting a secret message in, say, Alice's public key, all that is guaranteed is that any one with access to her private key is able to decrypt the secret message.

Efforts have been made to counter some of these problems. For example, in digital signatures, a trusted third party is included in the protocol. This party could encrypt Alice's public key with its own private key then store it in a database. Now, anyone can get Alice's public key from this database by decrypting the key stored there using the trusted third party's public key.

However, this protocol does not solve the problem of mapping keys to people. It just guarantees that the public key has been put there by someone that is or is pretending to be Alice.

Jakobsson, Jules and Nguyen introduces the notion of Proprietary and Collateral Certificates [2].

"We present a scheme whereby one certificate, known as a ***proprietary*** *certificate, may be linked to another, known as a* ***collateral*** *certificate. If the owner of the proprietary certificate shares the associated private key, then the private key of the collateral certificate is simultaneously divulged."*

To use the idea of Proprietary and Collateral Certificates in a Traitor Tracing Scheme, the Proprietary Certificate could contain the keys that can be traced. The Collateral Certificate might contain something very personal to the authorized user. However this idea would only deter users and not force the authorized user from deliberately sharing the Proprietary Certificate. There are problems, however. The user might lie about some personal information, like a false bank account number.

On the other hand, an authorized user might have concerns if they gave away personal information like account numbers. This information might be revealed to their disadvantage if the certificate fell into the hands of some villain. Boldyreva and Hakobsson [3] addresses this problem by introducing a CPU time delay and a real time delay so that accidental sharing may be detected and taken care of during the time delay.

Biometric measures like retina scans could be used, but the process is expensive and may endanger the users. Voice detection and fingerprints are also expensive, could be inaccurate, and are easily attacked.

Conclusion

Something has to be done to stop piracy spreading. If nothing is done, companies will lose money and may fail. If enough companies fail, then the economy, as a whole, is put at risk. This technique offers a way to identify those whose keys have been mis-used. But, the problem with Traitor Tracing Schemes lies in the area of generating false positives. False positives in Traitor Tracing strike at our culturally - derived sense of justice and fairness. So, it is not enough to implement a scheme like this, blind to the effects of an erroneous accusation. We must be aware of the possibility that keys are accidentally shared, and cannot assume that keys have been betrayed for nefarious purposes. This is constraint encourages us to take the kind of approach that is more commonly associated with a criminal investigation. Evidence must be gathered, preserved and analysed. But, there are difficulties with gathering evidence. It is very hard to map a key to a real person, for example. If problems like this do get resolved, we must still take into account the boundaries of what we, as a society, consider to be ethically correct. Our implementation must not only be just. It must be seen to be just.

References

[1] B. Chor, A. Fiat, M. Naor and B. Pinkas, *"Tracing Traitors"*, IEEE Trans. Inform. Theory, vol. 46, NO. 3,pp. 893-910, May 2000.

[2] M. Jakobsson, A. Juels and P. Nguyen, *"Proprietary Certificates"*, Proceedings of the The Cryptographers' Track at the RSA Conference 2002, LNCS Vol. 2271, Springer-Verlag, 2002

[3] A. Boldyreva and M. Hakobsson, *"Theft-protected proprietary certificates"*, in Proc. 2002 ACM Workshop on Digital Rights Management(DRM 2002).

[4] B. Pfitzmann, *"Trials of Traced Traitors"*, Workshop on Information Hiding, Cambridge, UK, LNCS 1174, Springer-verlag, pp. 49-64, 1996.

[5] S. Byers, L. Cranor, D. Korman, P.McDaniel, and E. Cronin, *"Analysis of security vulnerabilities in the movie prodiction and distribution process"*, in Proc. 2004 ACM Workshop on Digital Rights Management, ACM Press, 1-12, 2003

[6] R. L. Rivest, A. Shamir, L. A. Adleman, *"A method for obtaining digital signatures and public-key cryptosystems"* Communications of the ACM, Vol.21, Nr.2, pp. 120-126, 1978

[7] J. Trevathan and H. Ghodosi, *"Overview of Traitor Tracing Schemes"*, http://citeseer.ist.psu.edu/trevathan03overview.html