Computer and Internet Forensics
Alternative Assessment
Countering the use of non-repudiation methods to compromise privacy

Dylan Leigh
Student # s3017239

Semester 2 2010

Abstract

This report examines ways in which non-repudiation mechanisms can be exploited to compromise the anonymity or privacy of their users. Some of the possible consequences of privacy breaches are discussed, and an overview of Australian privacy legislation is provided. Two non-repudiation techniques which allow customers to remain anonymous and keep their communications private are explored.

Contents

1 Introduction

Non-repudiation protocols are used to prevent a party in a transaction from denying (repudiating) that the transaction took place. They are often utilized in electronic commerce to prevent a customer from denying that they have received a service, or the vendor from denying that they have received payment [1]. Because non-repudiation is strongly linked to identity, many applications of non-repudiation protocols can also be used to trace the identity of the parties to the transaction. [2]

In many cases it is not the intent of the non-repudiation system to allow easy tracking of users. However many non-repudiation systems - unless specifically designed for privacy protection - can impair the privacy of their users and allow them to be easily tracked. Conversely, attempts to improve privacy of a protocol can impair the capacity for non-repudiation [1].

In some applications is is desirable or necessary to keep the identity of one party of the transaction concealed from other parties. For example:

- Vehicular networks - User identity and location can be revealed unnecessarily and an individual's journey may be traceable, a significant invasion of privacy.
- Pay-TV systems and Digital Rights Management pay-per-view systems - non-repudiation is required to ensure payment but it can be also used to track customers viewing preferences against their wishes.
- Voting and election protocols - guaranteeing that each citizen votes, and only votes once, but the content of their vote is secret.
- E-cash - e-cash should be able to be used anonymously, but this restriction makes it difficult to ensure that it is only "spent" once.

There are a number of ways of dealing with these privacy issues, including via legislation and via technological methods which limit identity exposure. Legal issues from an Australian perspective are discussed in section 2.2. Two non-repudiation technologies which operate without exposing the identity of the participants are presented in section 3.

2 Legal, Ethical and Social Issues

2.1 Government Tracking via Non-repudiable signatures

In his article "Beware, your computer may betray you" [2], Colin Barras identifies some of the privacy and security issues associated with non-repudiation. The case of Sayed Pervez Kambaksh, an Afghan student sentenced to death for downloading and distributing a "blasphemous" document, is used to illustrate the dangers of allowing easy tracking of online activities and identity.

The article focuses on research by Sassaman and Patterson [3] on the Bitfrost security model used in the "XO" laptops produced by the "One Laptop Per Child" project[1]. The Bitfrost anti-theft system, "P_THEFT", connects to an anti-theft server each day, transmitting the laptop's serial number to the server. The server sends an activation lease back to the laptop. If a laptop has been reported as stolen it will be denied the activation lease and cannot be used.

Bitfrost uses non-repudiable digital signatures, which identify a specific laptop. As the laptops are registered to a specific user the signatures can also be used to track the laptop's user - or deliberately deactivate the laptop of a specific user by preventing it from receiving the activation lease. It is noted that although this was not the intention of the Bitfrost model, it is still possible to use the signatures to track laptops, and that the model does not seem to consider the user's government as a possible security or privacy risk. Sassaman and Patterson are working on a modified version of Bitfrost, with improved privacy protection.

[1] The OLPC project website is located at http://laptop.org/en/.

There is some debate over whether or not governments will be interested in monitoring or disabling children's laptops. clinical psychologist Ricky Greenwald argues that the 5-10 year old children using the laptops will be using their laptops for games and schoolwork and governments will not be interested in monitoring their internet activity. Sassaman disagrees, arguing that in some countries where the XO laptops are used there are child soldiers as young as 11, and it would be beneficial to enable them to "whistleblow" without being tracked by government agencies. Sassaman also points out that the XO laptops and network may be used by adults and older children.

2.2 Privacy Principles

Graham Greenleaf's article "Privacy Principles - irrelevant to cyberspace?"[4] discusses the extension of the Australian privacy laws - in particular the eleven "Privacy Principles" (PPs) - to the private sector. The Privacy Principles apply only to personal information, defined as 'about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion' [5]. Greenleaf points out that much routinely collected information, such as email addresses and sometimes IP addresses, identifies a person and is thus personal information. The definition is considered "problematic" and Greenleaf recommends that it should be clarified by new legislation. This definition also does not properly account for aggregated data not personally identifiable but which may still constitute a privacy invasion.

To comply with the PPs the user must be informed why information is collected, and any other organizations with whom the data is "usually" disclosed. In situations where possible personal information might be routinely collected (e.g. a IP address logged when visiting a web page) determining when the user has been informed may be problematic. A user may visit a site starting at any page via a link from elsewhere on the web, and may not always pass through a "front page" where they can be given notice of the collection of personal information more easily.

Many issues with "finality" are identified. "Finality" refers to the way in which the use and disclosure of personal information is restricted to the purposes for which it is originally collected. This restriction is easily evaded as organizations are not required to narrowly define or limit the purpose of collecting information. This is particularly notable in the case of large, multi-domain organizations, which can broadly define the purpose of collecting information and use the information in many areas. The Act also allows use for a "directly related purpose". As there are no limits on how narrowly the purpose of collecting information is defined, the information may be collected for "marketing" purposes, which will have many "directly related" uses which allow using the data in many ways and sharing the data with other organizations.

Organizations may also disclose personal information to others if the subject of the information is "reasonably likely to be aware" of the disclosure. This enables the organization to justify disclosing the information to third parties more easily if the user is reasonably aware. Conversely, organizations which receive data from other organizations may be liable to the subject of any personal information, if they use or disclose the information for any purpose not related to the purpose it was collected for.

The access and correction principles require that a person has the right to access their personal information held by an organization and the organization must make corrections (including adding or deleting data) to ensure that it is accurate and relevant (given the purposes it is collected for). The organization must also provide "reasonable" security to protect the personal information against misuse. Organizations may need to provide a secure means of accessing and updating personal information to the subjects of that information. It is noted that this service may be costly and the usefulness of collecting the data may not justify this cost.

Any person has the right to inquire if an organization records any personal information (in general, not necessarily about the person making the inquiry), and to obtain details about how the organization stores and uses this information. Organizations are required to maintain a register of these details, which can be inspected by others upon request. This register must be provided annually to the Privacy Commissioner who publishes an annual compilation (the "Personal Information Digest"). It is noted by Greenleaf that this digest "receives little use".

Some deficiencies in the current principles, mentioned by the Australian Privacy Charter [6], are covered; the "Achilles heel" of "finality" has already been mentioned. It is also noted that although consent is required by the PPs, it may not be adequately informed. Persons giving their consent may have no option but to give it in order to obtain a benefit or service, which may pressure people into giving consent unwillingly. Public registers such as search engines also raise privacy issues not adequately handled by the privacy principles, as the information they collect and provide to others is not for a well defined use.

Provision for anonymity is also mentioned - the PPs do not provide an explicit right to anonymity, and Greenleaf argues transaction structures should be in place which permit anonymous or pseudo-anonymous transactions. The privacy charter also mentions other factors not covered by the PPs: a right to not be disadvantaged by exercising one's right to privacy (e.g. forced consent to access a service, as mentioned above) and that any costs incurred by allowing users to exercise their rights to privacy should be explicitly considered part of normal organizational running costs.

Some international legal issues are considered - European Union countries will prohibit exporting personal information to countries which do not have "adequate" privacy legislation. Hong Kong, Taiwan and Quebec have similar export restrictions in their privacy laws. It is argued that Australia should include similar export provisions, and that this will increase the chance of Australian laws being considered "adequate" under the EU laws, and attract more European-based business. It is also argued that foreigners should be given the same privacy protection rights against Australian organizations as Australian residents, and that in reciprocal arrangements Australia should try to ensure that our residents are given protection under other countries laws. This means that organizations will need to carefully consider international privacy laws as well as those of their own country.

The current difficulty of enforcing Australian laws against organizations based in other countries is noted (the USA is particularly significant here as many organizations and server operations are US based, but the USA has "negligible" privacy laws). It is noted by Greenleaf that "A high percentage of internet privacy breaches against Australians are likely to be untouchable by our laws". It is argued that this is not a reason against enacting strong privacy protection legislation, but that effective international privacy protection will be provided by "a patchwork quilt of national laws" which will become more uniform and enforceable through international agreements and cooperation.

The article concludes by noting that although often the best privacy defense is to prevent access to information by technical means, once personal information *has* been obtained, legal measures are the best defence against the misuse of the data.

3 Technological Solutions

3.1 Pay-TV System with Strong Privacy Protection

Pay-TV systems provide a variety of television programs or channels to their customers for a subscription fee. They typically use a Conditional Access System (CAS) to ensure only the subscribers to particular channels can view those channels. Pay-TV systems currently allow the vendor to easily track the customer's viewing preferences through the CAS, which customers may find disconcerting.

Song and Korba [7] note that although many privacy protection schemes have been proposed for Pay-TV systems, these deal primarily with protection against outside eavesdroppers, whereas real customers are usually more concerned with misuse of their personal information by the vendors themselves. They propose a new "e-ticket" based CAS which uses Abe and Fujisaki's blind signature scheme [8]. Privacy and anonymity is supported through the use of the blind signature scheme and anonymous, temporary public keys.

Customers create a temporary, anonymous public key (keeping the matching private key secret) and transmit this public key in a blind message to the vendor when buying an e-ticket. The e-ticket is signed by the provider and contains the temporary, anonymous public key. The

customer can then use (i.e. "spend") the e-ticket later, and the temporary key is used to encrypt (on the vendor side) and decrypt (on the customer side) the authorization keys which allow the customer to access a channel or program.

The vendor can confirm that the e-ticket is genuine because it signed the e-ticket; however, it cannot trace the e-ticket back to the customer because it can not read the temporary, anonymous key during the purchasing phase, when the customer's identity is known. The system also allows for "adaptation" and "suspension" i.e. changing and removing which channels the customer is subscribed to.

Privacy in terms of viewing preferences is assured as the vendor only knows how much the customer spends on e-tickets, not what channels they are subscribed to. If the protocol is modified such that a bank issues e-cash instead of having the providers issue e-tickets, neither the bank nor the vendor can determine anything about the customer's viewing or spending.

As all messages are signed, an independent arbiter can verify the authenticity of the messages in the case of any conflicts. The signatures do not reveal any of the customer's private information. This system also protects against the "theft" of an e-ticket - if copied by an attacker it cannot be used (or "spent") without the matching private key only known by the customer.

3.2 VANETS enhancement

Armknecht, Festag, Westhoff and Zeng [9] propose a security architecture for Vehicular Ad-Hoc Networks (VANETs) which provides both improved non-repudiation and privacy. Using a modified Public Key Infrastructure (PKI) system [10], users create certified pseudonyms which can be used to confirm that they are an authorized vehicle, but make it difficult to trace the vehicle.[2]

VANETs can be used for many purposes including collision warning, toll collection, parking payments, rental car management and communicating road traffic conditions. Some of these are private communications and require non-repudiation for the purposes of private payment processing, others are public but still require non-repudiation so that a vehicle which misuses the public system to send false safety or traffic congestion information can be blocked from the system and held accountable for any damages. A malicious vehicle may do this for the purpose of simple vandalism or to alter road traffic flow to its own advantage. It is necessary to ensure that vehicles can trust the safety messages and there are consequences for sending false safety messages.

One approach to handle nodes which send false safety messages and/or disrupt the system is to require all messages to be signed with a public key. A certificate authority (CA), possibly operated by a governmental road traffic/safety organization, would manage the authenticity of keys and revoke the key of disruptive users. If necessary, the CA can also trace the key back to a malicious user for legal proceedings. Unfortunately this approach allows an eavesdropper (including other users of the system who receive broadcast messages) to easily trace a vehicle by tracing the messages it has signed.

As a vehicle is generally operated by a single owner this is often equivalent to tracking the movements of the owner, a serious invasion of privacy. An adversary who knows other information about a vehicle (e.g. by receiving or intercepting a credit card toll or parking payment from the same vehicle) will be able to easily link the owner's name and personal details to the vehicle and the owner's movements.

The enhanced system provides anonymity by using pseudo-anonymous public/private key pairs (referred to here as "pseudonyms"). The customer proves their identity to the CA using the customer's secret public key, and receives a "master" key and certificate. The customer then creates any number of pseudonyms using the master key, master certificate, and the CA's public key. The customer can create these pseudonyms offline without the intervention of the CA, reducing load on the CA and increasing privacy protection - it is easier to create and use more pseudonyms.

[2] [9] also discusses some secure routing enhancements. VANETs have unusual routing requirements due to the highly mobile nature of the nodes and rapid changes within the network. As this report concentrates on non-repudiation issues the routing improvements will not be discussed in detail.

The CA does not have to track individual pseudonyms. If it becomes necessary to revoke a customer's pseudonyms, their master key and certificate are revoked which effectively revokes all pseudonyms created using them.

A vehicle can change its pseudonym constantly to prevent identity and location tracking, and can use different pseudonyms for different types of messages or different vendors. Only the CA can link the pseudonyms to a vehicle and owner, using the master key and certificate. Note that although the CA can trace users and revoke keys, nobody (including the CA) can falsely impersonate a customer, as this requires the customers secret private key (which is not shared with the CA). This provides the necessary non-repudiation.

4 Discussion

As discussed in section 2.1, non-repudiation techniques while often necessary can be used to track users with significant consequences for their safety and privacy. There are ways to protect user privacy, typically via legal protections (section 2.2) or technological protections (section 3).

There are many situations where legal protections are not sufficient - most obviously when the government itself is the attacker [2]. In this case, the use of technologies which cannot be used to track or monitor affected individuals is required. It is unusual that the Bitfrost security model discussed in section 2.1 does not consider governments and infrastructure operators as threats to privacy.

Legal protection may not be sufficient when dealing with internal use of data by corporations, especially with multi-domain and/or multi-national corporations which have ways to evade Australian privacy laws. Data stored and used in other countries is generally not protected by Australian privacy legislation, and multi-domain corporations can use their wide scope to use data collected for one purpose for other purposes. Conversely, Greenleaf points out that once an organization has access to (cleartext) data, only social pressure and legal protection can be used to prevent abuse of the data.

Compliance with the privacy laws also presents challenges for organizations collecting, storing and using personal information. It is necessary to ensure that users are informed about how their information is collected and why it is collected. It is necessary to keep it secure, and to avoid exposure and/or misuse of the data. Systems must be in place to allow persons who are the subject of information held by the organization to update it. In some cases the cost of implementing the necessary security and updating facilities may outweigh the benefit obtained from the collection and use of the data.

Strong privacy protection technology may be legally required; in some circumstances the use of certain techniques such as encryption or pseudo-anonymity may be mandated by legislation or codes of practice.

As mentioned earlier, non-repudiation systems (especially payment systems) can be used by a vendor to track customers against the customers wishes, although this tracking may not technically be necessary for provision of their service [7]. Although technical solutions which allow more privacy exist, the vendor may choose not to use them (preferring a system that lets them obtain more marketing data) unless legislation or pressure from their customers forces them to do so. Guaranteed privacy protection may increase patronage; customers may be more likely to use potentially embarrassing services if they cannot be identified doing so.

The non-repudiation systems discussed here have different requirements and thus provide a different degree of privacy protection. Most significantly, the Pay-TV system is mainly concerned with privacy from the other party in the non-repudiable transaction, rather than eavesdroppers. The VANETs enhancement provides no extra protection from the central CA itself, but prevents eavesdroppers from identifying or tracking users of the network.

The VANETs system is an example of a system where central control over the system is maintained but the pseudo-anonymous users are unable to identify each other. It is still possible for the CA to track users, or expose a user (this is a necessary function of the system, to link

a pseudonym to malicious use of the network in legal proceedings). The users are therefore required to trust that the CA will not breach their privacy - as the system affects road safety, safety is given higher priority than privacy from the central authority. Note that although the CA has the ability to expose a user the CA may be under legal or contractual obligations to protect user privacy.

5 Conclusion

Non-repudiation techniques are an essential part of many transactions but can be used to track the activity of the parties involved. This can be the case even if the non-repudiation protocols are not intentionally designed for user tracking. Protocols exist which prevent user tracking and allow anonymous (or pseudo-anonymous) transactions to take place while maintaining non-repudiation.

Organizations must comply with the relevant privacy legislation, which may require implementing privacy-enhancing protocols and systems, and avoiding the unnecessary collection of personal information. Multi-domain and multi-national organizations are able to avoid many legislative restrictions due to their broad scope and international presence.

References

[1] R. Song, Ronggong Song, and M. Lyu. Analysis of privacy and non-repudiation on pay-tv systems, 2001. http://www.cse.cuhk.edu.hk/~lyu/paper_pdf/paper23.pdf.

[2] Colin Barras. Laptops could betray users in the developing world. *New Scientist*, 198(2659):26–27, July 2008. Also published under the title "Beware, your computer may betray you", http://www.newscientist.com/article/mg19826596.100-laptops-could-betray-users-in-the-developi

[3] Len Sassaman, Meredith L. Patterson, and David Chaum. Freezing more than bits: Chilling effects of the olpc xo security model, 2008. http://www.usenix.org/events/upsec08/tech/full_papers/patterson/patterson.pdf.

[4] Graham Greenleaf. Privacy principles - irrelevant to cyberspace? *Privacy Law and Policy Reporter*, 3, September 2006. http://www2.austlii.edu.au/itlaw/articles/IPPs.html.

[5] Privacy act 1988, 1998. http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/.

[6] The australian privacy charter. *Privacy Law and Policy Reporter*, 2(3), April 2005. http://www.austlii.edu.au/au/journals/PLPR/1995/31.html.

[7] Ronggong Song and Larry Korba. Pay-tv system with strong privacy and non-repudiation protection. *IEEE Transactions on Consumer Electronics*, 49(2):408–413, May 2003. http://ieeexplore.ieee.org/iel5/30/27208/01209533.pdf?arnumber=1209533.

[8] Masayuki Abe and Eiichiro Fujisaki. How to date blind signatures. In *Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology*, pages 244–251, London, UK, 1996. Springer-Verlag. http://portal.acm.org/citation.cfm?id=647093.760000.

[9] Frederik Armknecht, Andreas Festag, Dirk Westhoff, and Ke Zeng. Cross-layer privacy enhancement and non-repudiation in vehicular communication. In *4th Workshop on Mobile Ad-Hoc Networks (WMAN), Bern, Switzerland*, March 2007. http://www.network-on-wheels.de/downloads/Armknecht-etal_WMAN07_SIVC.pdf.

[10] Ke Zeng. Pseudonymous pki for ubiquitous computing. In *EuroPKI*, pages 207–222, 2006. http://www.springerlink.com/content/2h7j353538654x72/.