Tufts University

Department of Computer Science

SECURITY OF DIGITAL SIGNATURES AGAINST ADAPTIVE CHOSEN-MESSAGE ATTACKS

Sam Heilbron

Mentor: Ben Hescott

Abstract. *Digital signature schemes are methods of ensuring the authenticity of a digital message. This paper will provide a brief background on cryptography and proceed to introduce the three major components to a digital signature scheme – a key generation algorithm, a signing algorithm and a signature-verifying algorithm. It's important to analyze previous schemes in order to appreciate the complexities involved in generating even the simplest of signature schemes. However, with the improving nature of attacks that can be performed against schemes and the potential development of quantum computing, there is only one scheme that is known to be secure. Lamport's one-time signature, though simple and only effective on one message at a time, can be implemented using a tree structure, making it an extremely secure way of ensuring the authenticity of a digital message.*

Tuesday December 15 2015

For the Community

Have you ever heard the expression, "Just put your John Hancock on the dotted line"? This expression alludes to John Hancock's prominent signature on the Declaration of Independence, signed in 1776 in Philadelphia, Pa. For the past 300 years we've accepted that a signature is a stylized, *handwritten* depiction of someone's name. While a fingerprint is the most personal marker of a human identity, a signature is the clearest identifier that an individual decided to complete an action. This could be as simple as signing a check or as profound as signing a marriage license. As a result, the need for signatures has been around for as long as the need for distinguishing our identities and conveying consent.

Introduction

The method of identifying ownership and conveying agreement has adapted over the years to fit the latest prevailing technology [1]. Cave dwellers scratched marks in the dirt to signal agreement. The Sumerians, who lived in Mesopotamia, a place abundant with clay, created clay tablets for the temple scribes. Around 3000BC the Egyptians mixed symbols and art to form hieroglyphics and created papyrus scrolls, which became the prevailing written documents for the next 3500 years. Papyrus was followed by parchment, which was followed by paper, and by the 15th century, paper was used for all written documents in Europe. With the development of the Greek, (and soon after) Latin alphabet, words and handwritten signatures were formed. The key theme is that throughout history signatures were written on the materials that most used to communicate. As we move into an age that is increasingly reliant on digital

communication, the need for a secure way of authenticating a digital document has evolved.

Digital Signature Background

A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital message. For a signature to be valid, it must follow three specific criteria: It must be publicly verifiable, transferable and non-refutable. When something is publicly verifiable it means that if someone verifies a signature on a given message as being legitimate, then we can assume that all other parties who receive the same, signed, message will also verify its' authenticity. This concept implies that signatures are transferable. That is, a signature by an individual on a message can be shown to a third party who can verify that the signature is authentic. That third party should be able to repeat this process (on the same message) with another third party. Finally, for a signature to be non-refutable it cannot later be denied.

Application

The application of digital signatures is already widespread in the world today. Take for example, a software company that wants to send out updates of their software in a secure manner. The company needs to have their clients, who own previous versions of the software, to be able to recognize that the software patch, m, is authentic. The clients also need to identify when a malicious third party, masking as the company, attempts to release a software patch, m'.

Since an individual signature is only secure when used by one individual (or company) there is a need to be able to generate multiple signatures easily. This is what prompted the development of a signature scheme. A scheme is comprised of a tuple of algorithms responsible for generating keys, signing messages, and verifying signatures on messages. The algorithms are randomized so that a single scheme can generate a set of signatures.

The company generates a public key and a secret key using the key generation algorithm, which we will refer to as Gen(k), where k refers to the key length in bits. This algorithm produces a public key, a value private to the company and its clients, and a secret key, a value known only to the company. The public key is distributed securely to clients when they first purchase the product[1]. Then, when the company would like to distribute a patch, m, they use the signing algorithm, Sign(sk, m), where sk refers to the company's secret key and m refers to the message. This produces s, the signed message. The pair of (m,s) are sent out to every client. The clients then verify the authenticity of m by using the verification algorithm, Vrfy(pk, m, s), where pk is the public key the client was distributed initially, m is the message and s is the signed message. Vrfy returns a valid bit, 1, if the signature s, on message m, is authentic, or 0 if it did not come from a trusted source. As a result, a client would verify that all messages signed by the company are valid and all signed by a third party, posing as the company, are unauthentic. The simplicity of this method is that no matter how many clients receive this technology, only one public key and secret key are needed.

[1] This is done through a Certification process, which, for the sake of this paper, will be assumed to be entirely secure.

History of Digital Signatures

Over the years, a variety of signature schemes have been developed, each with varying levels of success. Just as a handwritten signature can be forged to varying amounts, so too can signature schemes be broken.

In 1976, Whitfield Diffie and Martin Hellman first conjectured that signatures schemes existed. Soon after, the RSA signature scheme was developed. This scheme was based off the notion of generating a public key that was the product of two large, n-bit prime numbers p and q. As a result, RSA signatures are multiplicative, which means that the signature of a product is the product of the signatures. Therefore, if an attacker obtained the signatures for messages m1 and m2 such that m2 = m / m1, they could forge a valid signature on m [Go].

From here Michael Rabin extended the security of signature schemes by creating a scheme in which finding the private key and forging a signature are provably as hard as integer factorization. Similar to the RSA scheme, the public key is comprised of the product of two large prime numbers p and q. However, for the message to be signed it must have a square root mod n. If it doesn't have these elements at the outset, then it is modified slightly to fit these criteria. These random bits of padding that are applied to it make it very challenging to create a forgery.

As signature schemes have become more advanced, so too have the attacks against them. However, there remains one signature scheme that is known to be secure. This is referred to as Lamport's one-time signature. Unfortunately, this is only secure for signing a single message. This would defeat the purpose of a signature scheme if a new

key needed to be generated for each message. Luckily, chaining these signatures together in a tree structure allows for a single key to be used on multiple messages.

Signature Scheme Secureness

It's important to understand the various classes into which signature schemes are separated based off their security. Below are classes of signature scheme ordered by increasing secureness [GoMiRi]:

Totally Breakable: The true algorithm for signing messages can be determined and replicated.

Universally Forgeable: An algorithm to sign messages can be created that is functionally equivalent to the true signing algorithm. However, it is not an exact replica of the true signing procedure.

Selectively Forgeable: A signature for a particular (specific) message may be forged.

Existentially Forgeable: A signature of at least one message may be forged, but the enemy has no control over which message it is.

Attacks On Signature Schemes

In order to determine the secureness of a scheme, attacks are performed on it. The most common type of attack is a message attack, where the enemy has access to pairs of messages and corresponding signatures. The goal of an attack is to learn information about the signing procedure so as to forge the signature on future messages. Below are descriptions of specific attacks, ordered by increasing severity [GoMiRi]:

Known message attack: The enemy is granted access to a list of messages and corresponding signatures, but the attacker did not choose the messages.

Generic (non-adaptive) chosen message attack: The attacker can choose a list of messages for which he will obtain signatures, but the message list is created before seeing the public key or any of the signatures. This attack is non-adaptive because the messages are selected before any signatures are visible.

Directed (non-adaptive) chosen message attack: This is similar to the generic chosen message attack, but the public key is known before the enemy generates a list of messages to be signed.

Adaptive chosen message attack: The attacker can request signatures on messages having seen previously signed messages that the enemy selected. This is the most dangerous type of attack because it is adaptive; the enemy bases their decisions off of previously gathered information.

Conclusion

We have come a long way from Hancock's distinctive signature on the Declaration of Independence; in the 21st century many documents, including software updates and rental/lease agreements are signed digitally. Corresponding to this new technology we've developed systems to secure digital signatures. But just as there are forgers who seek to compromise written signatures, there are individuals who seek to disrupt digital signatures. Given the difficulty of securing a digital signature scheme against an adaptive chosen message attack, the outlook may seem grim. However,

although the potential development of quantum computers threatens the secureness of more digital signatures, Lamport's one-time signature is believed to remain secure [BeBuDa]. Ultimately, it is an ongoing challenge to continue to develop new signature schemes to protect the integrity of digital messages.

References

[Ba] Gascoigne, Bamber. "History of Writing Materials" HistoryWorld. From 2001, ongoing. http://www.historyworld.net/wrldhis/PlainTextHistories.asp?historyid=aa92

[BeBuDa] Bernstein, Daniel J., Johannes Buchmann, and Erik Dahmén. *Post-quantum Cryptography*. Berlin: Springer, 2009. Print.

[Go] Goldreich, Oded, *Foundations of Cryptography: Basic Tools*. Cambridge: Cambridge UP, 2001. Print. pp 421 – 456.

[GoMiRi] S. Goldwasser, S. Micali, and R. Rivest, A digital signature scheme secure against adaptive chosen-message attack, SIAM J. Comput., 17 (1993), pp. 281 – 308

[KaLi] Katz, Jonathan, and Yehuda Lindell, *Introduction to Modern Cryptography*. Boca Raton: Chapman & Hall/CRC, 2008. Print.

[Mer] Ralph C. Merkle. A certified digital signature. In G. Brassard, editor, *Advances in Cryptology* – CRYPTO '89, volume 435 of *Lecture Notes in Computer Science*, pages 218-238. Springer-Verlag, 1990, 20-24 August 1989.