Network Security and Cryptography

M.V.V Anil Kumar
B.E. Student
Computer Science & Engineering Department
Saveetha University

Abstract—This paper aims to provide a broad review of network security and cryptography, with particular regard to digital signatures. Network security and cryptography is a subject too wide ranging to coverage about how to protect information in digital form and to provide security services. However, a general overview of network security and cryptography is provided and various algorithms are discussed. A detailed review of the subject of network security and cryptography in digital signatures is then presented. The purpose of a digital signature is to provide a means for an entity to bind its identity to a piece of information. The common attacks on digital signature was reviewed. The first method was the RSA signature scheme, which remains today one of the most practical and versatile techniques available. Fiat-Shamir signature schemes, DSA and related signature schemes are two other methods reviewed. Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation was reviewed. The objective of this paper is to provide the reader with an insight into recent developments in the field of network security and cryptography, with particular regard to digital signatures .cryptography was used as a tool to protect national secrets and strategies. The proliferation of computers and communications systems in the 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services. DES, the Data Encryption Standard, is the most well-known cryptographic mechanism. It remains the standard means for securing electronic commerce for many financial institutions around the world. The most striking development in the history of cryptography came in 1976 when Diffie and Hellman published New Directions in Cryptography.

I. Introduction

A digital signature of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed. Signatures must be verifiable; if a dispute arises as to whether a party signed a document (caused by either a lying signer trying to *repudiate* a signature it did create, or a fraudulent claimant), an unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's secret information (private key). The first method discovered was the RSA signature scheme,Which remains today one of the most practical and versatile techniques available. Sub-sequent research has resulted in many alternative digital signature techniques. The Feige-Fiat-Shamir signature scheme requires a one-way hash function.

A. Information Security and Cryptography

Cryptography, an understanding of issues related to information security in general is necessary. Information security manifests itself in many ways according to the situation and requirement. Over the centuries, an elaborate set of protocols and mechanisms has been created to deal with information security issues when the information is conveyed by physical documents. Often the objectives of information security cannot solely be achieved through mathematical algorithms and protocols alone, but require procedural techniques and abidance of laws to achieve.The concept of information will be taken to be an understood quantity. For example, privacy of letters is provided by sealed envelopes delivered by an accepted mail service.

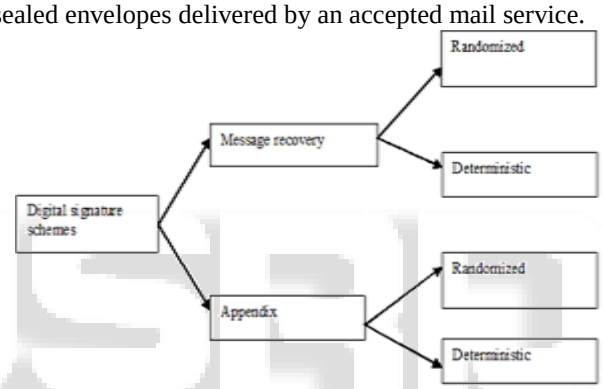

Fig. 1: Taxonomy of Signature Schemes

II. Attacks On Digital Signatures

- Key-Only Attacks: In these attacks, an adversary knows only the signer's public key.
- Message Attacks: Here an adversary is able to examine signatures corresponding either to known or chosen messages. Message attacks can be further subdivided into three classes:

1. Known-Message Attack: An adversary has signatures for a set of messages which are known to the adversary but not chosen by him.
2. Chosen-Message Attack: An adversary obtains valid signatures from a chosen list of messages before attempting to break the signature scheme. This attack is non-adaptive in the sense that messages are chosen before any signatures are seen. Chosen-message attacks against signature schemes are analogous to chosen cipher text attacks against public-key encryption schemes .
3. Adaptive Chosen-Message Attack: An adversary is allowed to use the signer as an oracle; the adversary may request signatures of messages which depend on the signer's public key and he may request signatures of messages which depend on previously obtained signatures or messages.

Signing procedure
Entity A (the *signe*r) creates a signature for a message m € M by doing the following:

1. Compute $s = S_A(m)$.
2. Transmit the pair (m, s). s is called the *signature* for message m.

Verification procedure
To verify that a signature s on a message m was created by A, an entity B performs the following steps:

1. Obtain the verification function V_A of A.
2. Compute $u = V_A(m, s)$.
3. Accept the signature as having been created by A if u = *tru*e, and reject the signature if u = *fals*e.

A. The RSA Signature Scheme

The message space and cipher text space for the RSA public-key encryption scheme are both $Z_n = \{0, 1, 2\ldots n-1\}$ where n = pq is the product of two randomly chosen distinct prime numbers. Since the encryption transformation is a bijection, digital signatures can be created by reversing the roles of encryption and decryption. The RSA signature scheme is a deterministic digital signature scheme which provides message recovery. The signing space M_S and signature space S are both Z_n. A redundancy function R: $M \rightarrow Z_n$ is chosen and is public Knowledge.

Algorithm: Key generation for the RSA signature scheme
Summary: each entity creates an RSA public key and a corresponding private key.
Each entity A should do the following:

1. Generate two large distinct random primes p and q, each roughly the same size.
2. Compute n = pq and $\Phi = (p-1)(q-1)$.
3. Select a random integer e, $1 < e < \Phi$, such that gcd $(e, \Phi) = 1$.
4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer d, $1 < d < \Phi$, such that $ed \equiv 1 \pmod{\Phi}$.
5. A's public key is (n, e); A's private key is d.

Algorithm: RSA signature generation and verification
SUMMARY: entity A signs a message m € M. Any entity B can verify A's signature and recover the message m from the signature.

1) Signature Generation. Entity A Should Do The Following:

- Compute m = R (m), an integer in the range [0, n-1].
- Compute $s = m^d \bmod n$.
- A's signature for m is s.

2) Verification. To Verify A's Signature S And Recover The Message M, B Should:

- Obtain A's authentic public key (n; e).
- Compute $m = s^e \bmod n$.
- Verify that m € M_R; if not, reject the signature.
- Recover $m = R^{-1}(m)$.

B. Feige-Fiat-Shamir Signature Scheme

The Feige-Fiat-Shamir signature scheme and requires a one-way hash function $h:\{0, 1\}^* \rightarrow \{0,1\}^k$ for some fixed positive integer k. Here $\{0, 1\}^k$ denotes the set of bit strings of bit length k , and $\{0, 1\}^*$ denotes the set of all bit strings (of arbitrary bit lengths).
Algorithm: Key generation for the Feige-Fiat-Shamir signature scheme
SUMMARY: each entity creates a public key and corresponding private key.
Each entity A should do the following:

1. Generate random distinct secret primes p, q and form n = pq.
2. Select a positive integer k and distinct random integers s1, s2 , ... ,sk € Z^*_n
3. Compute $v_j = s^{-2}_j \bmod n$, $1 \le j \le k$.
4. A's public key is the k-tuple (v1, v2,… vk) and the modulus n; A's private key is the k-tuple (s1 , s2 ,… , sk).

Algorithm :Feige-Fiat-Shamir signature generation and verification
SUMMARY: entity assigns a binary message m of arbitrary length. Any entity B can verify this signature by using A's public key.

1) Signature Generation. Entity A Should Do The Following:

- Select a random integer r, $1 \le r \le n-1$.
- Compute $u = r^2 \bmod n$.
- Compute $e = (e1, e2, \ldots, ek) = h(m \| u)$; each e_i € {0, 1}.
- Compute $s = r.\Pi^k_{j=1} s_j^{e_j} \bmod n$.
- A's signature for m is (e, s).

2) Verification. To Verify A's Signature (E, S) On M, B Should Do The Following:

- Obtain A's authentic public key (v1, v2, …, vk) and n.
- Compute $w = s^2.\Pi^k_{j=1} v_j^{e_j} \bmod n$.
- Compute e' = h (m ‖ w).
- Accept the signature if and only if e = e' .

C. The Digital Signature Algorithm (DSA)

In August of 1991, the U.S. National Institute of Standards and Technology (NIST) proposed a digital signature algorithm (DSA). The DSA has become a U.S. Federal Information Processing Standard (FIPS 186) called the Digital Signature Standard (DSS), and is the first digital signature scheme recognized by any government The signature mechanism requires a hash function $h: \{0, 1\}^* \rightarrow Z_q$ for some integer q.
Algorithm: Key generation for the DSA
SUMMARY: each entity creates a public key and corresponding private key.
Each entity A should do the following:

1. Select a prime number q such that $2^{159} < q < 2^{160}$.
2. Choose t so that $0 \le t \le 8$, and select a prime number p where $2^{511+64t} < p < 2^{512+64t}$, with the property that q divides (p - 1).
3. (Select a generator α of the unique cyclic group of order q in $Z^*_{p.}$)
   - Select an element g €Z^*_p and compute $\alpha = g^{(p-1)/q} \bmod p$.
   - If α = 1then go to step 3.1.
4. Select a random integer a such that $1 \le a \le q-1$.
5. Compute $y = \alpha^a \bmod p$.
6. A's public key is (p, q, α, y); A's private key is a.

Algorithm: DSA signature generation and verification.

Summary: entity A signs a binary message m of arbitrary length. Any entity B can verify this signature by using A's public key.

1. Signature generation. Entity A should do the following:
- Select a random secret integer k; 0 < k<q.
- Compute r = (α^k mod p) mod q
- Compute k¯1 mod q.
- Compute s = k ¯1 {h (m) + ar} mod q.
- A's signature for m is the pair (r; s).
2. Verification. To verify A's signature (r, s) on m, B should do the following:
- Obtain A's authentic public key (p, q, α, y).
- Verify that 0 < r < q and 0 < s <q; if not, then reject the signature.
- Compute w = s¯1 mod q and h(m).
- Compute u1 = w .h(m) mod q and u2 = rw mod q.
- Compute v = ($\alpha^{u1}y^{u2}$ mod p) mod q.
- Accept the signature if and only if v = r.

III. Applications

Digital signatures have many applications in information security, including authentication, data integrity, and non-repudiation. One of the most significant applications of digital signatures is the certification of public keys in large networks. Certification is a means for a trusted third party (TTP) to bind the identity of a user to a public key, so that at some later time, other entities can authenticate a public key without assistance from a trusted third party.

IV. Conclusion

This paper has provided a broad review of network security and cryptography algorithms with particular regard to digital signatures The transformations SA (SIGNING) and VA (VERIFICATION) are typically characterized more compactly by a key that is, there is a class of signing and verification algorithms publicly known, and each algorithm is identified by a key. Thus the signing algorithm SA of A is determined by a key kA and A is only required to keep kA secret. Similarly, the verification algorithm VA of A is determined by a key lA which is made public. Handwritten signatures could be interpreted as a special class of digital signatures. To see this, take the set of signatures S to contain only one element which is the handwritten signature of A, denoted by sA. The verification function simply checks if the signature on a message purportedly signed by A is sA.

References

[1] Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996. http://Cacr.math.uwaterloo.com www.prenticehall.com
[2] Network Security and Cryptography by William Stallings.

