Tutorial

CSCI361 – Computer Security

Sionggo Japit
sjapit@uow.edu.au

TUTORIAL - MISCELLANEOUS

What is the difference between "computational security" and "provable security"?

Computational security is measured through the amount of effort required to successfully attack a system.

Provable security, potentially a misleading term, means that the security of a system can be reduced to the difficulty of a problem considered to be hard. For example, factoring large numbers into prime. It is really "relatively provably secure", in the sense of being as hard as the related problem. Someone may find a way to easily solve that problem though and the cryptosystem is then no longer computationally secure.

TUTORIAL - MISCELLANEOUS

What does it mean for a system to be compromised?

For the security to be by-passed or breached, in particular for the secret information which the security of the system relies on to be obtained by some other party.

It could refer specifically to a user who's password has been stolen. The user could be referred to as being compromised.

TUTORIAL - MISCELLANEOUS

What does it mean for a cryptosystem to be broken?

A cryptosystem is said to be broken if there is an attack which is better (in terms of computational complexity) than brute force.

TUTORIAL - MISCELLANEOUS

Can an unbroken scheme be insecure?

For this and the next question you need to look at what it means to be secure. It is secure if the best attack against the system is computationally infeasible to mount.

It is unbroken if the best attack is brute force. If the key space is small a system may be insecure, even if unbroken, since there are not many keys to check. For example an unbroken complexity theoretic scheme with 1000 keys will not be secure.

TUTORIAL - MISCELLANEOUS

Can a broken scheme be secure?

With reference to the previous question & answer, it is possible to have a system with a theoretical attack which reduces the complexity but not to a level which is **practical** for attacking the system. For example, if the "brute force" complexity for a system is 2^{80} and this is considered secure, and there is a theoretical attack with complexity 2^{60}, the scheme is broken but is probably still secure.

TUTORIAL - MISCELLANEOUS

	Broken	Unbroken
Secure	Better than brute force known but still computationally hard.	Brute force is the best known and computationally hard.
Insecure	Better than brute force known and computationally not hard.	Brute force is the best known and computationally not hard.

TUTORIAL - MISCELLANEOUS

One important security principle is known as the principle of effectiveness. What does it mean? Give an example to support your argument.

- Control must be used properly
  - Using the right solution, the right level of security, protecting the right assets
  - Control measures should be easy to use and efficient

TUTORIAL

One important security principle is known as the principle of timeliness. What does it mean? Give an example to support your argument.

- Items should only be protected while they are valuable, and that the level of protection should be consistent with their value.

TUTORIAL - MISCELLANEOUS

What are differences between block and stream ciphers?

A block cipher acts on blocks of data, acting on each block in the same way, with the same key. Security is based on confusion and diffusion.

In a stream cipher we combine the plaintext with a keystream, The characters the stream cipher acts on can be of different sizes, for example 8-bits or 16-bits. Most of stream ciphers have no diffusion. They are faster than block ciphers.

TUTORIAL - MISCELLANEOUS

What is steganography? How is it related to encryption?

We encrypt messages to preserve confidentiality, that is, to make sure unauthorised parties cannot read the message. Another means of providing confidentiality is to hide the message itself, so people don't even know it is there. This is referred to as steganography.

Classic examples include invisible ink, "first letter messages" and character marking.

One advantage over encryption is that a communication is not necessary observed at all. In some circumstances communication between parties may be enough to compromise them.

TUTORIAL - MISCELLANEOUS

Describe Plaintext Cipher Block Chaining (PCBC) mode.

PCBC mode is very similar to CBC (Cipher Block Chaining). In CBC the input to the i^{th} round of encryption is

$$P_i \oplus C_{i-1}$$

where P_i and C_{i-1} are, respectively, the i^{th} plaintext block and the $(i-1)^{th}$ ciphertext block.

TUTORIAL - MISCELLANEOUS

Describe Plaintext Cipher Block Chaining (PCBC) mode.

(continue…)

For PCBC the input to the i^{th} round of encryption is

$$P_{i-1} \oplus P \oplus_i C_{i-1}$$

Thus encryption depends on the previous block of ciphertext, the current block of plaintext, and also directly on the previous block of plaintext.

PCBC is used in Kerberos V.4, an authentication/key establishment protocol.

TUTORIAL - MISCELLANEOUS

You may have noticed that some of the modes only use the encryption function, not the inverse (decryption) function. Which modes have this property and why?

These modes are k-bit CFB, k-bit OFB and CTR modes.

In each of these modes the cipher effectively acts as a stream cipher in which a keystream is generated for combination with the plaintext. The same keystream is generated for decryption so we don't need the inverse cipher, that is we don't need the decryption function.

TUTORIAL - MISCELLANEOUS

What is authenticated encryption?

An authenticated encryption scheme is one where protection against attacks on confidentiality and integrity/authentication are provided. Thus the scheme provides encryption, protecting against confidentiality breaches, and authentication, protecting against integrity breaches.

Generally, but not always, confidentiality **and** integrity/authenticity are desired. Sometimes authentication is enough, a public post that is verifiable for example, but usually encryption by itself is not enough. Note that including special knowledge in a message which allows the sender to be identified after decryption is really adding a form of authentication, where the special

TUTORIAL - MISCELLANEOUS

Does a one-time pad provide confusion and diffusion?

From the definition, confusion is about having a complex relationship between plaintext, ciphertext and key. Diffusion is about changing the statistical property of the of the input (plaintext) such that a single bit change in the plaintext causes an unpredictable changes in the ciphertext. One-time pad provides a perfect confusion, but not diffusion.

Look at the definitions of confusion and diffusion. Diffusion is to do with each input bit having an effect on each output bit (within a block say). Confusion is about having a complex relationship between plaintext, ciphertext and key. A one-time pad doesn't diffuse at all, but it provides perfect confusion so it doesn't need to.

TUTORIAL - MISCELLANEOUS

Calculate the minimum number of persons needed so that the probability of two having the same birth month is at least 0.5.

We are talking about the birthday attack for finding collisions in hash functions. From the lecture we have a formula for the probability of at least one collision, given *k* randomly chosen messages and a digest space of size *m*:

$$P(m,k) > 1 - e^{\frac{-k(k-1)}{2m}} = \varepsilon$$

TUTORIAL - MISCELLANEOUS

- For our case we have m=12 (months), and the probability being ½.

$$P(m,k) > 1 - e^{\frac{-k(k-1)}{24}} = \frac{1}{2}$$

$$\frac{1}{2} > e^{\frac{-k(k-1)}{24}}$$

- We find we need k=5.

TUTORIAL - MISCELLANEOUS

What is an output feedback mode?

TUTORIAL - MISCELLANEOUS

What are the advantages and disadvantages of output feedback mode over the other block cipher modes?

TUTORIAL - MISCELLANEOUS

What are the various type of attacks against encryption schemes?

- Ciphertext-only attack
- Known-plaintext attack
- Chosen-plaintext attack
- Chosen-ciphertext

TUTORIAL - MISCELLANEOUS

Ciphertext-only attack

- The opponent gets to see only ciphertext, and try to decrypt a message.
- The most difficult type of attack, because the opponent has the least amount of information.
- Involve guessing some plaintext that might or will be associated.

TUTORIAL - MISCELLANEOUS

Known-plaintext attack

- Opponent knows the plaintext and ciphertext, and try to determine or find the decryption key.
- If successful, the opponent can then use the knowledge on the decryption key to decrypt other ciphertexts.
- Known-plaintext attach is more powerful than a ciphertext-only attack because the opponent get more information (in this case, the plaintext.)

TUTORIAL - MISCELLANEOUS

Chosen-plaintext attack

- Opponent has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts.
- Not realistic in practice, but it is possible.
- For example, in the context of public key cryptography, the encryption key is public and the opponent can encrypt any plaintext the opponent choose.

TUTORIAL - MISCELLANEOUS

Chosen-ciphertext attack

- The opponent has the ability to choose both the ciphertext and its associated plaintext.

TUTORIAL - MISCELLANEOUS

What are the 3 security goals? Provide a primitive for each goal.

- **Confidentiality**: inaccessible to unauthorized parties (Encryption/Decryption)
- **Integrity**: assets should be unmodified or un-forgeable, without detection, by unauthorized parties (MIC/MAC -> Hashing)
- **Availability/Authentication**: available to the authorized parities/providing who they claimed to be (Digital Signatures/Access Control/Puzzle Challenge)

TUTORIAL - MISCELLANEOUS

What are the four important functions in the AES block cipher?

1. Byte substitution (S-box, 8-bit to 8-bit).
2. Shift row (rotating order of bytes in each row).
3. Mix column (linear mixing of a word column).
4. Key mixing (addition).

TUTORIAL - MISCELLANEOUS

How does a threat to information security differ from an attack? How can the two overlap?

A threat to information secuirty differ from an attack in that a threat is the **potential to use or exploit vulnerability** within the information system. The threat is the weakness in the system that is used for the attack. An attack is **the realization of the threat** that cause damage to the information system.

The two overlap in that the **threat agent actually causes the attack on the system**.

TUTORIAL - MISCELLANEOUS

Describe the important properties of hash functions.

- It can be **applied to any size input**.
- The **output must be of fixed size**.
- **One-way**: Easy to calculate but hard to invert.
- **Pre-image resistant**: For any given **Y**, it is difficult to find an **X** such that **H(X)=Y**.
- **Second Pre-image resistant**: Given $\mathbf{X_1}$ it should be difficult to find another $\mathbf{X_2}$ such that $\mathbf{H(X_1)=H(X_2)}$.
- **Collision resistant**: It is computationally infeasible to find messages **X** and **Y** with **X≠Y** such that **H(X)=H(Y)**.

Tutorial - Miscellaneous

An important cryptographic primitive is known as the "threshold signature". Explain what it is and what the purpose of having that cryptographic primitive is.

- A **(t, w)** threshold scheme is a method of sharing a key **K** among a set of **w** participants in such a way that any **t** participants can compute the value of **K**, but no group of **t-1** participants can do so.

TUTORIAL - MISCELLANEOUS

An important cryptographic primitive is known as the "group signature". Explain what it is and what the purpose of having that cryptographic primitive is.

- It is a scheme that allows any member of a group to digitally sign a document on behalf of a group. It works in a manner such that any member of a group is able to digitally sign a document, and a verifier can confirm that it came from the group, but does not know which individual in the group signed the document. The protocol allows for the identity of the signer to be discovered, in case of disputes, by a designated group authority that has some auxiliary information.

TUTORIAL - MISCELLANEOUS

What is Discrete Logarithm problem? Show an example of a signature scheme that relies on the security of discrete logarithm problem.

- The discrete logarithm problem refers to rules and operations related to mathematical entities called groups. It is defined as follows: given an element g in a group G of order t, and another element y of G, the problem is to find x < p, such that $y = g^x \ mod \ p$.

TUTORIAL - MISCELLANEOUS

What is factorisation problem? Show an example of a signature scheme that relies on the security of factorisation problem.

- Factorization refers to splitting of an integer number into a set of factors (a smaller set of numbers) which when multiplied together will get back the original integer. All integer numbers may be prime-factorized; i.e., expressed as a product of many prime numbers. When one has an integer number and wants to find the factors of these prime numbers, that can produce back the integer number, is difficult. This problem is known as factorisation problem. Many public-key cryptosystems base on this factorization problem, including the RSA cryptosystem as well as RSA digital signature system.

TUTORIAL - MISCELLANEOUS

- Suppose Alice wants to send a message m to Bob in such a way that Bob is assured the message is both authentic, has not been tampered with, and from Alice. Alice creates a digital signature s by exponentiating: $s=m^d \bmod n$, here d and n are Alice's private key. She sends m and s to Bob. To verify the signature, Bob exponentiates and checks that the message m is recovered: $m = s^e \bmod n$, where e and n are Alice's public key.

TUTORIAL - MISCELLANEOUS

What is a perfect security in one-time pad?

- It refers to the security provided by one-time pad. Because one-time-pad produces random output that bears no statistical relationship to the plaintext, and since the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code, and thus it is said to be perfectly secured.

TUTORIAL - MISCELLANEOUS

What is message authentication code (MAC), and how is it differ from a digital signature scheme?

A message authentication code (MAC) is an authentication tag known as a checksum that is generated by applying an authentication scheme, together with a secret key, to a message. This tag is then appended to the original message. Unlike digital signatures, MACs are computed and verified with the same key, so that they can only be verified by the intended recipient.

A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified with the public key of the party that signed the message.

TUTORIAL - MISCELLANEOUS

What is the difference between one-way function and trapdoor one-way function?

A one-way function is a function that is easy to solve in one direction (forward direction), but hard in the opposite direction (inverse direction); that is for all x, finding f(x) is easy, but knowing f(x), it it hard to find x.

A trapdoor one-way function is a function which looks like a one-way function, but it is equipped with a secret trapdoor. If this secret trapdoor is known, the inverse can be easily calculated.

TUTORIAL - MISCELLANEOUS

Describe the Diffie-Hellman key agreement protocol.

The Diffie-Hellman key agreement protocol is explain using example as follow:

- Adam and Barbie choose a large random prime p and a generator $g \in Zp$.
- The prime p and g are publicly known.
- Privately, Adam chooses integer x, a secret known to Adam, and Barbie chooses y, a secret known to Barbie.
- Next Adam sends $g^x \ mod \ p$ to Barbie, and Barbie sends $g^y \ mod \ p$ to Adam.
- Adam and Barbie can now compute the joint key $(g^x)^y = (g^y)^x \ mod \ p$.

TUTORIAL - MISCELLANEOUS

If an attacker has a polynomial algorithm to factor n, which is a large arbitrary integer. Why this makes RSA based public key cryptography insecure?

The reason is that the attacker can compute the victim's private key from the victim's public key.

It is noted that $ed=1 \bmod \phi n$, and $\phi n=(p-1)(q-1)$. If the attacker has a polynomial algorithm, then the attacker can compute $n=p \times q$. Knowing the value of n, the attacker can then compute d from the victim's public key e using $d=e-1 \bmod \phi(n)$. Thus the message can is revealed.

TUTORIAL - MISCELLANEOUS

One-time-pad is known to provide the *perfect security*. What does the term *perfect security* mean?

It refers to the security provided by one-time pad. Since one-time-pad produces random output that bears no statistical relationship to the plaintext, and since the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code, and therfore it is said to be perfectly secured.

TUTORIAL - MISCELLANEOUS

One important security principle in cryptology is known as Kirchoff's principle. State what is this principle.

Kerckhoff's principle says that one should always assume that the attacker knows the algorithm being used; in other words, a cryptographer must assume that all possible ways of breaching security must be examined, because the attacker knows the algorithm being used.

TUTORIAL - MISCELLANEOUS

What is the main drawback of the one time pad cryptosystem?

The main drawback of the one time pad cryptosystem is that the size of the key must be the same as the size of the plaintext, and this key must be secretly communicated in advance between communication parties. This is a severe practical difficulty. Another critical problem with one time pad is the difficulty in finding or creating a random keys for the plaintext, especially if the plaintext is large.

TUTORIAL - MISCELLANEOUS

What is the difference between diffusion and confusion?

Confusion is about **having a complex relationship** between plaintext, ciphertext and key. Diffusion is about **changing the statistical property** of the input (plaintext) such that a single bit change in the plaintext causes an unpredictable changes in the ciphertext.