CS2107 Tutorial 1 (Introduction & Encryption)

School of Computing, NUS

August 2019

1. Alice was the Web administrator of the company *WhatSecurity**. A malicious attacker sent an email to Alice. The email instructed Alice to click on a link so as to login to the company's HR system to view a report. In the email, information of the "sender" had been modified to be the HR manager of *WhatSecurity*. Alice wrongly believed that the email was indeed sent by the manager, and followed the instructions. In doing so, she revealed her password to the attacker. Using Alice's password, the attacker then logged-in to the Web server, and invoked many processes. As a result, the server got overloaded.

   With respect to the security requirements mentioned in the lecture (confidentiality, integrity, availability, authenticity, etc.), discuss what aspects of security were compromised.

2. Suppose it takes 512 clock cycles to test whether a 64-bit cryptographic key is correct, when given a 64-bit plaintext and its corresponding ciphertext.

   (a) How long does it take to exhaustively check all the keys using a 4GHz (single-core) processor?

   (b) How long does it take on a cluster of 1024 servers, each with a quad-core 4Ghz processor.

   (*Hint*: For simplicity, you can take 1 year $\approx 2^{25}$ seconds. Also note that: 1K = 2^{10}, 1M = 2^{20}, 1G = 2^{30}.)

3. Suppose it takes 512 clock cycles to test whether a 32-bit cryptographic key is correct, when given a 32-bit plaintext and its corresponding ciphertext.

   How long does it take to exhaustively check all the keys using a 4GHz (single-core) processor? Using exhaustive search, is it then possible to crack a ciphertext and obtain its plaintext in realtime?

   Now consider a walkie-talkie system called *Secure Walkie Talkie* (SWT)*, which encrypts its communication using a 32-bit symmetric keys k. In each communication session of SWT, the first 64 bits of the plaintext are always the string of zeros, and the last 64 bits the string of ones. Given a plaintext m and the key k, the encryption is done in the following way:

   (a) Randomly choose a 32-bit IV;

   (b) Compute $\widetilde{k} = IV \oplus k$;

(c) Use a stream cipher to encrypt the plaintext m with $\widetilde{k}$ as the secret key, and output the ciphertext c;

(d) Transmit the IV, followed by the ciphertext c, over the air.

We assume that attackers can eavesdrop and capture all ciphertexts (including the IVs) transmitted over the air. We know that a 32-bit key is too short, and can be broken. However, as calculated above, it would take a relatively long time. In their marketing efforts, SWT thus claims that its 32-bit key is sufficient for many applications. This is what appeared in their advertisement: "The 32-bit key is sufficient. By the time your message is maliciously decrypted, it already becomes useless".

Now, you want to design a hand-held device that is able to crack SWT system and obtain its plaintexts in *realtime*. The hand-held device can have computing resources comparable to a mobile phone. Note that in order to achieve its objective, the device should be able to determine the employed 32-bit secret key readily (say within 0.1 second) when given a ciphertext. Suggest a way to derive the secret key very fast.

(*Hint*: Assume that the hand-held device can hold a large, say 32GB, of pre-computed table whereby the key can be looked up.)

4. Lecture 1 mentioned that Winzip can encrypt a compressed file. Why it is meaningless to carry out the two operations in the other way, that is, first encrypts the file, and then compresses the encrypted file?

   (*Hint*: Consider the effectiveness of compression on "random" sequences, and also a requirement of a good encryption scheme.)

5. Bob encrypted a video file using Winzip, which employs the 256-bit key AES. He chose a 6-digit number as password. Winzip generated the 256-bit AES key from the 6-digit password using a hash function, say SHA1.

   Alice obtained the ciphertext. Alice also knew that Bob used a 6-digit password. Given a guess of the 256-bit key, Alice could determine whether the key successfully decrypted the file.

   How many guesses did Alice really need in order to get the video from the ciphertext encrypted with a 256-bit key in this case?

6. Find out more about these terminologies:

   - *Cryptology, Cryptanalysis, Cryptography,*
   - *NSA, NIST, Cryptography backdoor, Key Escrow, Decryption order.*

   Find out more about the following well-known persons in cryptography:

   - *Whitfield Diffie, Ron Rivest, Alice, Bob, Eve, Mallory*, and *Trent.*

(*Optional*) Consider the following questions:

- Can NSA break AES?
- Can NSA by-pass cryptography?

*: Companies are purely fictional.

Hands-on Exercise: Linux Set-Up

A Linux system will be necessary for your assignments later. Hence, you will need to set up a **Linux host**. An **Ubuntu desktop** is recommended since it is user friendly enough even for new users. Please use a recent Ubuntu version, such as Ubuntu 16.04.5 LTS (Xenial Xerus), which is available from: `http://releases.ubuntu.com/16.04/`. A 32-bit PC (i386) desktop image is sufficient.

If you use a Windows notebook/PC, you can use **VirtualBox** or **VMWare** to create an **Ubuntu VM**. You can follow the steps described in: `https://www.lifewire.com/run-ubuntu-within-windows-virtualbox-2202098`. Simply use the "NAT" or "bridge adapter" connection/networking mode for your VM, so that it can access the Internet.

It is also expected that you have rudimentary proficiency in using a Linux system. You can read the tutorial given at: `https://www.digitalocean.com/community/tutorials/an-introduction-to-the-linux-terminal`. However, more knowledge might be needed, and it is expected that you do some self-exploration. You may want to refer to this freely-downloadable good book on Linux: "**The Linux Command Line**", which is available from `http://linuxcommand.org/tlcl.php`.

If you have any issues and need help with your Linux set-up, your TAs will open an open consultation session after releasing Assignment 1 later. Please do your own self exploration first in setting up your Linux system.

— End of Tutorial —