CMPT 479 Assignment2

Junchen Li

301385486

2022/7/24

1. (a) When Alice and Bob exchange their public keys over an insecure channel like SMTP, a third party like the Man in the Middle may intercept them, but may no decode them. It is known problem on ECDH, so Alice uses the public encryption key to encrypt the e-mail, the encryption does not provide authenticity/integrity. Anyone can send such a cipher text. They can try ECDSA, Alice is able to sign a message with her private key and Bob can validate the signature using Alice's public key since Alice should be able to produce valid signatures. In other words, Alice should send e-mail along with a digital signature on email using Alice's private key

   (b) Bob stores a hash of the encrypted version of the password using SHA-512, it is a mistake. Because SHA is not encryption and it is a one-way hash function to take a large document. Therefore, Bob still can use AES instead of SHA to store a hash of the encrypted version of the password.

   (c) Encryption does not provide authenticity/integrity. it is vulnerable to message modification: modifying the last 128 bits of the packet disrupts only the last 128 bits of the message that Bob receives, and Bob won't detect that the message was tampered with. This violates the message integrity goal. They can establish a shared 128- bit secret key instead of 256-bit.

   (d) With RSA, the public modulus size as found in the public key is what's quoted as size, or key size. Its relationship to security level is more complex than in ECC. They should use 2048-bit RSA key instead of 512-bit RSA key.

2. (a) Nowadays, RSA is not "perfect security" since the security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". When a quick polynomial algorithm for integer factorization has been found, then some public-key cryptosystem (algorithm) like RSA is not security any more. All files and data that use encryption system will become insecure. Unless our key size is billions of orders of magnitude larger than what we currently use. However, it is no practical use at all. All relevant parties such as cryptosuite developers should find a more secure and efficient encryption method

to improve the security of cryptocurrency. HTTPS will not work. So most of our online life will be lost, people can't enjoy online shopping. Unless some new agreement emerges.

(b) When the private signing key is leaked, the unknown group may first apply digital signatures to malicious programs that trick browser filters and some antivirus programs. Instead of some scripts or executables from unknown source, the browser now thinks it could come from trusted source and allows it to download. All user personal information are in danger at that time. The Facebook must regenerate a new private signing key and revoke the old one. The Facebook should stop its losses in time and count the number of users' accounts affected. Facebook is also important to fix the bug as early as possible and provide the public with true reports of the impact.

(c) Firstly, all the program, system or files which are related to SHA-2 hash will not insecure any more. The CIA principle will be broken since it is easy to get the corresponding input. All relevant parties such as cryptosuite developers should be decided to change another hash function or method. At the same time, we should either improve SHA-2 encryption capabilities or choose to deprecate it.

(d) The Shor algorithm is an algorithm that can be run in polynomial time to find integer prime factors. If Large, practical quantum computers have been constructed, then the Shor algorithm can be used to break public key cryptography schemes. For example, RSA, The Finite Field Diffie-Hellman Key Exchange. All products of the electronic information age need to be replaced, and all networks and cryptography mechanisms are no longer secure. For all relevant parties such as Cryptosuite developers, they need to make timely announcements to the public and find a better encryption method. Based on resources from the network, Shor algorithms and the emergence of quantum computers also facilitated research on new cryptosystems that are secure from quantum computers, collectively called post-quantum cryptography.
(Source from Wikipedia https://en.wikipedia.org/wiki/Shor%27s_algorithm).