UC Berkeley, MICS, W202-Cryptography

Week 09 Breakout 1

Key Exchange

Questions from the Asynchronous (for discussion)

10.4 Key Exchange Exercise, Part 1

Examine the following protocol and find as many problems with it as you can:

Alice ➔ Bob {password 1} encrypted in Bob's public key K_b
Bob ➔ Alice {password 2} encrypted in Alice's public key K_a
Alice ➔➔ Bob {message} a concatenation of password 1 | password 2
For example:
password 1 = 123
password 2 = 789
password 1 | password 2 = 123789

10.6 Key Exchange Exercise, Part 2

Suggest a set of modifications to fix the problems you found in the previous exercise.

Additional Discussion Questions

1. Assume a key exchange protocol is subject to a "replay attack". What is the biggest advantage that an attacker to carry out more significant attacks? (suggested answer below)

2. Give a real world example of a "replay attack". (suggested answer below)

3. Timestamps as nonces are one solution to a "replay attack". What is the danger of attack with timestamps? (suggested answer below)

Suggested Answers:

1. If a replay attacker can replay messages much later in the future, they have time to possibly also decrypt which would give them a much more significant future attack in addition to pure replay attacks.

2. An employee who gets fired. They had access to legitimate messages while they were working that they could replay in the future.

3. Time is not exactly a big secret. If an attacker can get a timestamp and note the time it was produced, they can probably make good guesses at future timestamps. In a lot of cases, people simply synchronize with the public atomic clocks, such as GPS clocks, which anyone can do.

Open Ended Discussions

Discuss key establishment and attacks in the following scenarios:

1. The US Navy has vessels that will be at sea for weeks or months. We need to constantly send and receive secure communications. We want to rotate keys daily in case a key is compromised.

2. The US government needs to send spies into foreign countries to gather intelligence and report it back on a daily basis. Spies may have very limited communication and may have to use very public places such as coffee shop WIFI. We want to rotate keys daily in case a key is compromised. Spies may be captured, so we also want to ensure past and future keys are not compromised if a spy is captured.

3. In a large metroplex area of the US, there are several TV stations, several cell phone providers, and numerous radios stations. The area covered may be several counties, each with a sheriff's department, and several cities, each with their own police department, and state police as well. We want to secure an "Amber Alert" system whenever a child is missing or in danger. Sadly, these types of systems when first implemented were subject to hoax calls. We need a system to establish identity to guard against hoax attacks, while balancing this with a lot of different law enforcement agencies, with varying levels of technical sophistication.

4. We just received a proposal from a venture capital company that has billions to spend on a new company to provide secure authentication for anything and everything. Their goal is to own the secure authentication market. Make a list of things for which we would want to provide secure authentication and an appropriate technology for each.