Peyrin & Ryan
Summer 2020

CS 161
Computer Security

Discussion 7

Network Security II

Question 1 ***TLS threats*** ()

An attacker is trying to attack the company Boogle and its users. Assume that users always visit Boogle's website with an HTTPS connection, using ephemeral Diffie-Hellman. You should also assume that Boogle does not use certificate pinning. The attacker may have one of three possible goals:

1. Impersonate the Boogle web server to a user
2. Discover some of the plaintext of data sent during a past connection between a user and Boogle's website
3. Replay data that a user previously sent to the Boogle server over a prior HTTPS connection

For each of the following scenarios, describe if and how the attacker can achieve each goal.

(a) The attacker obtains a copy of Boogle's certificate.

(b) The attacker obtains the private key of a certificate authority trusted by users of Boogle.

(c) The attacker obtains the private key corresponding to an old certificate used by Boogle's server during a past connection between a victim and Boogle's server. Assume that this old certificate has been revoked and is no longer valid. Note that the attacker does not have the private key corresponding to current certificate.

Question 2 ***DNS Walkthrough*** ()

Your computer sends a DNS request for "www.google.com"

(a) Assume the DNS resolver receives back the following reply:

```
com. NS a.gtld-servers.net
a.gtld-servers.net A 192.5.6.30
```

Describe what this reply means and where the DNS resolver would look next.

(b) If an off-path adversary wants to poison the DNS cache, what values does the adversary need to guess?

(c) Why not use cryptography to make the DNS connection secure?

Question 3 *DNS* (14 min)

(a) Alice wants to access Berkeley's diversity advancement project Dare, `dare.berkeley.edu`. Her laptop connects to a wireless access point (AP).

Alice worries that a hacker attacks the DNS protocol when her laptop is looking for the IP address of `dare.berkeley.edu`. Assume that DNSSEC is not in use.

◇ **Question:** Which of the following can attack the DNS protocol and have Alice's browser obtain an incorrect IP address for DARE? (Select 0 to 8 options.)

□ The laptop's operating system.

□ The laptop's network interface controller.

□ The wireless access point.

□ An on-path attacker on the local network.

□ The local DNS resolver of the network.

□ The root DNS servers.

□ `berkeley.edu`'s DNS nameservers.

□ An on-path attacker between the local DNS resolver and the rest of the Internet.

(b) Now assume that `berkeley.edu` implements DNSSEC and Alice's recursive resolver (but not her client) validates DNSSEC.

◇ **Question:** Which of the following can attack the DNS protocol and have Alice's browser obtain an incorrect IP address for DARE? (Select 0 to 8 options.)

□ The laptop's operating system.

□ The laptop's network interface controller.

□ The wireless access point.

□ An on-path attacker on the local network.

□ The local DNS resolver of the network.

□ The root DNS servers.

□ `berkeley.edu`'s DNS nameservers.

□ An on-path attacker between the local DNS resolver and the rest of the Internet.

(c) An attacker wants to poison the local DNS resolver's cache using the Kaminsky attack. We assume that the resolver does not use source port randomization, so the attacker will likely succeed.

In the Kaminsky attack, the attacker asks the resolver for a *non-existing* subdomain of UC Berkeley, *e.g.*, `stanford.berkeley.edu`, instead of asking for an *existing* domain like `dare.berkeley.edu`.

⋄ **Question:** What is the advantage of asking for a non-existent domain compared to asking for an existing domain? (answer within 10 words)

____

____