Paxson
Spring 2017

CS 161
Computer Security

Discussion 11

Week of April 17, 2017

Question 1 ***DNSSEC*** **(20 min)**

In class, you learned about DNSSEC, which uses certificate-style authentication for DNS results.

(a) In the case of a negative result (the name requested doesn't exist), what is the result returned by the nameserver to avoid dynamically signing a statement such as "`aaa.google.com` does not exist"? (This should be a review from lecture.)

(b) One drawback with this approach is that an attacker can now enumerate all the record names in a zone. Why is this a security concern?

(c) How could you change the response sent by the nameserver to avoid this issue?

HINT: One of the crypto primitives you learned about will be helpful.

Question 2 ***DNSSEC / TLS*** **(15 min)**

(a) Oski wants to securely communicate with CalBears.com using TLS. Which of the following entities must Oski trust in order to communicate with confidentiality, integrity, and authenticity?

1. The operators of CalBears.com
2. Oski's computer
3. Cryptographic algorithms
4. Computers on Oski's local network
5. The operators of CalBears.com's authoritative DNS servers
6. The entire network between Oski and CalBears.com
7. CalBears.com's CA
8. All of the CAs that come configured into Oski's browser
9. All of the CAs that come configured into CalBears.com's software
10. The operators of `.com`'s Authoritative DNS servers
11. The operators of the Authoritative DNS root servers

(b) Suppose we didn't want to trust any of the existing CAs, but DNSSEC was widely deployed and we were willing to trust DNSSEC and the operators of the root zone and of `.com`. How could TLS be modified, to avoid the need to trust any of the existing CAs, under these conditions?

(c) Assume end-to-end DNSSEC deployment as well as full deployment of your change. Oski wants to securely communicate with CalBears.com using TLS. What changes are there to the list in part A (i.e., what must Oski trust in order to communicate with confidentiality, integrity, and authenticity)?

(d) Is this change good or bad? List at least one positive and one negative effect that would result from this change.

Question 3 ***TLS downgrade attacks*** **(15 min)**

(a) Rather than prescribing specific cryptographic functions, the TLS protocol allows the browser and server to agree on a cipher suite. What are the different components of a cipher suite that the parties need to negotiate?

(b) How do the parties find out which cipher suites the other supports? Who ultimately gets to choose which cipher suite is chosen? How do they choose?

(c) Suppose Mallory knows how to break certain cryptographic primitives. Alice and Bob.com, communicating over TLS, both support the cipher suite with the vulnerable crypto, as well as others that are not broken. How can Mallory carry out a man-in-the-middle attack? Which of the crypto primitives must she be able to break for the attack to succeed?

(d) Is there anything Alice and Bob.com can do to prevent attacks like this?