April 11, 2016

Instructions. We will break into groups to discuss the following questions. Please think of as many solutions as you can. Be original! Maybe you will come up with something no one has thought of yet. Be prepared to talk about your solutions with the rest of the section.

Question 1  DNSSEC  (10 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) How could an attacker use this feature to enumerate all the record names in a particular zone. Could this be a security concern?

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

HINT: One of the crypto primitives you learned about will be helpful.
(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 Cert. Auth. (CA)
8. All of the CA’s that come configured into Oski’s browser
9. All of the CA’s 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 CA’s, 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 CA’s, 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 (eg. 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  Port Scanning and Defenses  (5 min)

Having taken CS161, you’ve become an expert in computer security. You’re hired by Famous Inc. to test their software for vulnerabilities. Their primary product is server software. For administrative purposes, this software allows authenticated admin access on a special port $p$.

You discover that the proprietary third-party library they use for authentication has a bug. As a result, anyone who knows $p$ can gain admin access to the software. Famous Inc. can’t update the third-party library immediately, but they still want to protect the users of their software. So, they thus introduce a configuration option into their software (which they control) that sets $p$ to be a random 16-bit number.

Is this strategy an effective defense? If not, how could an attacker gain admin access?

Question 4  Detecting attacks  (7 min)

Suppose that $S$ is a network-based intrusion detector that works by passively analyzing individual UDP and TCP packets. Suppose that $A$ is a host-based intrusion detector that is a component of the browser that processes and analyzes individual URLs before they are loaded by the browser.

Your company decides to build a hybrid scheme for detecting malicious URLs. The hybrid scheme works by combining scheme $S$ and scheme $A$, running both in parallel on the same traffic. The combination could be done in one of two ways. Scheme $H_E$ would generate an alert if for a given network connection either scheme $S$ or scheme $A$ generates an alert. Scheme $H_B$ would generate an alert only if both scheme $S$ and scheme $A$ generate an alert for the same connection. (Assume that there is only one URL in each network connection.)

(a) Assuming that decisions made by $S$ and $A$ are well-modeled as independent processes, and ignoring any concerns regarding evasion, what can you say about the false positives and false negatives of $H_B$ and $H_E$?

(b) If deploying the hybrid scheme in a new environment, is one of $H_E$ and $H_B$ clearly better?