Raluca Ada Popa
Spring 2018

CS 161
Computer Security

Discussion 8

Week of March 12, 2018

Question 1 ***DNS Walkthrough*** **(15 min)**

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

(a) Assume the DNS resolver receive 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 poinson the DNS cache, what values do the adversary need to guess?

(c) Why can't we use TLS to secure DNS?

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

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

(a) Suppose the case of a negative result (the name requested doesn't exist). Why can't the nameserver just return a signature on a statement such as "`aaa.google.com` does not exist"? What should the nameserver return instead?

(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 3 ***Detection Strategies*** **(20 min)**

Suppose you are responsible for detecting attacks on the UC Berkeley network, and can employ host-based monitoring (a HIDS) that can inspect the keystrokes that users enter during their shell sessions. One particular attack you are concerned with is malicious modification or deletion of files in the directory `/usr/oski/config/`.

(a) One method of detection is called signature matching. This involves looking for particular well-defined patterns in traffic that are known to represent malicious activity. Give a couple of examples of signatures you can use to detect these attacks. What are some limitations of this approach?

(b) Another approach is to search for behaviors. Instead of looking for known attacks, the detector might use knowledge of the system to look for suspicious sets of actions. Give two examples of host-based behavioral detection. Be specific as to how your examples differ from signature matching that looks for known attacks. What are some problems with this approach?

(c) Suppose now we aim to detect modifications to any files in `/usr/oski/config/` using the following procedure. Each night, we run a cron job that checksums all of the files in the directory using a cryptographically strong hash like SHA256. We then compare the hashes against the previously stored ones and alert on any differences. (This scheme is known as Tripwire.) Discuss issues with false positives and false negatives.