CS 6431 - Security and Privacy Technologies
Fall 2014

Homework #3

Due: 7:30pm EST, November 12, 2014

NO LATE SUBMISSIONS WILL BE ACCEPTED

YOUR NAME: _____

Collaboration policy

No collaboration is permitted on this assignment. Any cheating (*e.g.*, submitting another person's work as your own, or permitting your work to be copied) will automatically result in a failing grade.

Homework #3 (50 points)

Problem 1 (5 points)

Some spammers are known to send fake BGP route advertisements for unallocated or someone else's IP addresses. How does this attack work and why is it useful to spammers?

Problem 2 (5 points)

The Bank of Molvanîa's webpage is hosted at `https://BofM.mi`. Whenever a Web browser connects to this server, the server presents a certificate and the browser correctly checks that the certificate is issued to the domain the browser requested. The front page loads for a couple of seconds, then fetches and executes a script from `https://BofM.mi/scripts`.

Molvanîan browsers have a couple of odd features. First, they do not cache IP addresses for resolved domain names (DNS bindings); instead, they perform a separate DNS lookup for each HTTP request. Second, while the browser has an open HTTPS session to a server, all new HTTPS connections to the same site are assumed to be part of the existing session and do not require a certificate check.

Explain how a remote, off-path attacker (*i.e.*, *not* a man-in-the-middle) can steal the cookie of `BofM.mi` when the user visits `BofM.mi` using a Molvanîan browser.

Problem 3

Problem 3a (5 points)

In DNSSEC, delegation records for child zones are not signed. Why?

Problem 3b (5 points)

Suppose the attacker forges a delegation record for a child zone that participates in DNSSEC. Does this enable the attacker to forge DNS records of that zone? If not, explain how and when is this attack prevented and/or detected?

Problem 4

Problem 4a (5 points)

Explain why enforcement of the same origin policy in modern browsers fundamentally relies on the integrity of the DNS (Domain Name System).

Problem 4b (5 points)

One solution for enforcing the same origin policy even when DNS may be compromised is to associate the server's public key with each Web object retrieved over HTTPS. When one Web object attempts to access another object, the browser checks whether the keys match.

Does this solution provide complete enforcement of the same origin policy, or can it still be subverted for certain Web objects by an attacker who controls DNS? Explain.

Problem 5

Sotirov et al. used MD5 chosen-prefix hash collisions to forge a rogue SSL certificate for the name "MD5 Collisions Inc."

Problem 5a (5 points)

What are chosen-prefix collisions (as opposed to random MD5 collisions) and why are they essential for this attack?

Problem 5b (5 points)

Why was it necessary, as part of the attack, to purchase multiple sequential certificates from RapidSSL?

Problem 5c (5 points)

The forged "MD5 Collisions Inc." certificate is not one of the root certificates stored by Web browsers. Would a browser accept a `gmail.com` certificate issued using the forged certificate? Why or why not?

Problem 6 (5 points)

Which broad category of distributed denial-of-service attacks discussed in class would be difficult to study using a network telescope? Why?