Homework 4: DNS, BGP & TLS
Due at 11:59PM on Monday April 22 as a PDF via websubmit (as HW6).

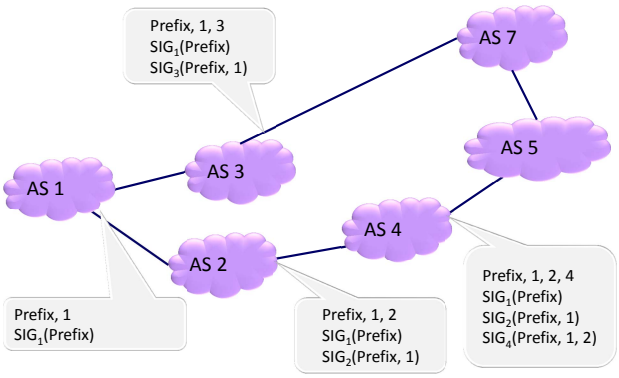
April 18, 2013

Exercise 1. 'Secure BGP' is generally considered to be "more secure" than 'secure origin BGP (soBGP)'. Read the following paper for a description of these two protocols:

`http://static.cs.brown.edu/courses/csci1800/sources/2010_ProcIEEE_SurveyBGPSecurity.pdf`

and give an example of an attack on BGP that succeeds against secure BGP but fails against soBGP.

Exercise 2. Consider the following variant of the BGP routing protocol, where the notation $SIG_1(m)$ again is the (public-key) digital signature on message m signed by the secret key of 1.



Suppose that AS 5 is adversarial, and wants to convince AS 7 that is has a path directly to AS 1. Is this possible? If yes, write down the message AS 5 sends to AS 7 to convince AS 7 that AS 5 has the path "Prefix, 1, 5". If not, explain why not.

Exercise 3. TCP.

- What are TCP SYN cookies, and what attack do they protect against?
- Why do TCP-based censorship boxes resort to sending RST packets to both sides of a TCP connection? Why not send a FIN packet, or drop acknowledgement packets, or do something else?

Exercise 4. Consider a Kaminsky attack on a recursive resolver that randomizes the DNS Query Id but not the UDP Source Port in the packets it sends. Suppose that for every random name query the attacker issues (*e.g.,* `junkjunk12313.bankofamerica.com`) the attacker can generate 60 forged DNS responses where the IP addresses from the `bankofamerica.com` nameservers in the glue records point to the attacker's own server. How many random name queries and forged DNS queries should the attacker send before he has a 70% probability of poisoning the cache?

Exercise 5. Write down the strongest attack you can think of on/using DNS recursive resolvers that:

1. Do not use source port randomization or query ID randomization.
2. Only use transaction ID randomization.
3. Do not use DNSSEC, but randomize the source port and query ID.
4. Do not perform bailiwick checking
5. Prefer caching records with a very long TTL over records with a shorter TTL.
6. Allow multiple queries for the same question to be outstanding (*i.e.,* To send multiple queries for the same question "What is the A record for `google.com`" before receiving an answer)
7. Are willing to resolve domains for a user with an source IP address.

Exercise 6. The designers of DNSSEC often claim that it is NOT a PKI. Explain why.

Exercise 7. Read the article on the China iroot incident here:
`http://www.renesys.com/blog/2010/03/fouling-the-global-nest.shtml`
`http://www.renesys.com/blog/2010/06/two-strikes-i-root.shtml`
and explain the incident in your own worlds. Based on the details of the incident, where do you think the censorship middle was located? (*i.e.,* between the recursive resolver and the nameservers? (also, which nameserver?), between the stub resolver and the recursive resolver? Or perhaps the recursive resolver itself was performing censorship?)

Submission policy.

Every submitted assignment MUST include the following information:

1. List of collaborators
2. List of references used (online material, course nodes, textbooks, wikipedia, etc.)
3. Number of late days used on this assignment
4. Total number of late days used thus far in the entire semester

If any of this information is missing, at least 20% of the points for the assignment will automatically be deducted from your assignment. See also discussion on plagiarism on the course syllabus.