4/25/17

4/25/17 3:18 PM

DNS

How to spoof DNS

- When you send a DNS request you send it with a query ID, so you know which request to match it
- Possibility – figure out query id, then causing a race to get your own response faster than the correct response
    - Come back with the answer faster than their request
- DNS records live for a pretty long time – ~7 days
- How does the evil adversary figure out the query id?
    - Query id == qid
    - Qid has to match
    - How can an off path attacker figure out the qid?
        - Nothing is signed at the moment
        - Only 16 bits – about 65 seconds to brute force
        - What if we can get the victim to look at a nice website operated by the evil person
            - Can induce this query to happen
            - Request image from bu.edu
            - I will induce the request
            - Still don't know the query id
            - Query id generated -> sequential
                - Have a fairly good range of qids to flood the victim with
- Easy case for the attacker:
    - Fixed port
    - Sequential ID
        - Learn these 2 values when attackers innocent website is visited because DNS query will go to attackers servers
- Attackers web page
    - I'm gonna imbed many images
        - Non existent weird names
        - Victim will send more dns bad requests NXDOMAIN
            - And they will be longer requests (bigger attack window)

- The attack wouldn't work with a popular site because it is in your cache
    - Many requests guaranteed

DNS

- If I answer your request
    - I don't know the answer, but here's a name server that might – NS record, actual IP address of the name server
    - Glue record
        - We are gonna give a fake glue record
        - Now hes poisoned the cache for an of the .bu.edu
            - Poison the name server

Responses will redirect to another name server operated by the attacker

Aaaxxq.bu.edu --→

←NS ns1.bu.edu, A, attackers IP address – will have incorrect ip addresses

Kaminski Attack

Solutions:

- Query id randomizations
    - 2^16 security – not very high – can still try to win the race
    - Kaminsky attack is still doable in 10s
    - port randomization
        - another 11 bits of security for 2^27 total

DNS sec

- Maps
    - Key – domain
    - Value – public key
- Secure a mapping – by signing it
- Adds a new record type called
    - "RRSIG"
        - resource record signature

What does that do to the DDoS Amplifying?

- Adding length to dns is not a good thing

New Record Type – DNS is essentially a database look up

- DNSKey-contains the public key

Simple version:

- New record type – DS – delegation signer
- Comes together with NS
- Get a NS record
- DS record – here's the hash of their PK
    - Come with an RSA
- Now I only need to know the root public key