Security of Networks, Services, and Systems

DNS vulnerabilities

Ricardo Morla

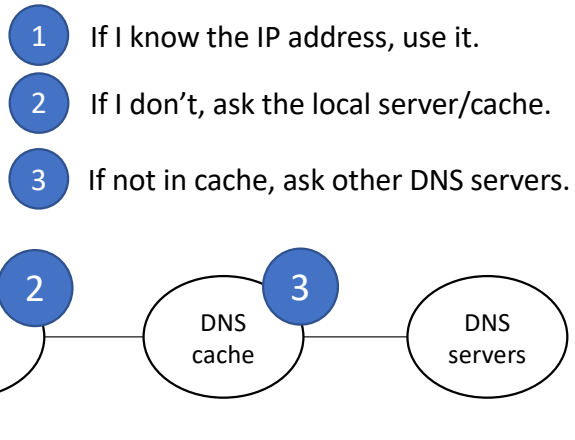
FEUP – SSR/M.EEC, SR/M.EIC

Importance of DNS

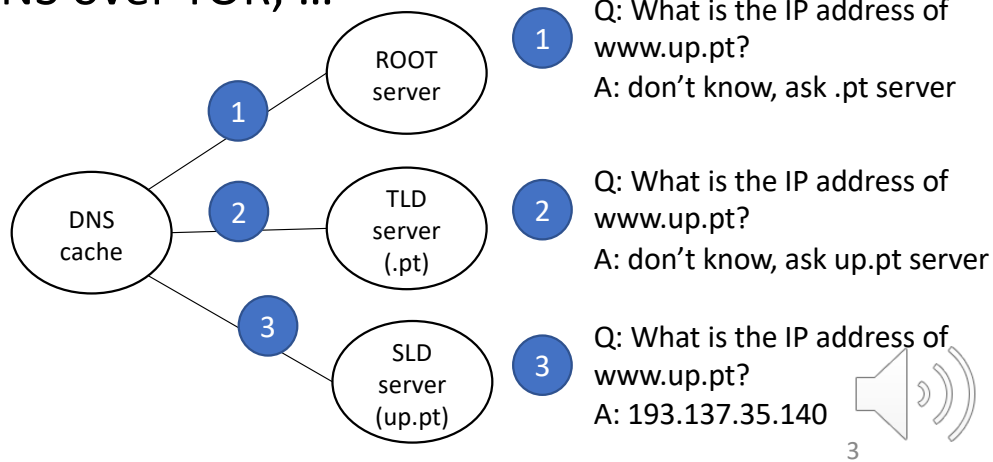
- Domain names are what people use to access web sites
  - Applications also use them to access other applications
- IP adddresses is how information gets routed on the Internet
- DNS does mapping between domain names and IP addresses

- Disrupting DNS means disrupting the Internet

Architecture and Protocol



- Local
  - /etc/hosts, resolv.conf, DHCP
  - Non-recursive, recursive, iterative
- DNS Request and reply messages
  - QR, AA, NAME, TYPE
  - Over TCP or UDP ports 53; DoT, DoH, DNS over TOR, …
- Servers
  - Local DNS server / DNS cache
  - Root name server, TLD, SLD
  - Caching
  - Split server



https://en.wikipedia.org/wiki/Domain_Name_System

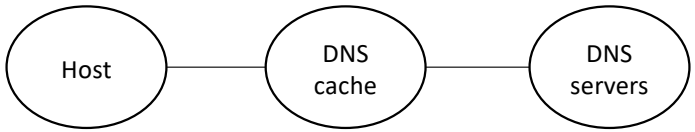
DNS tool: dig

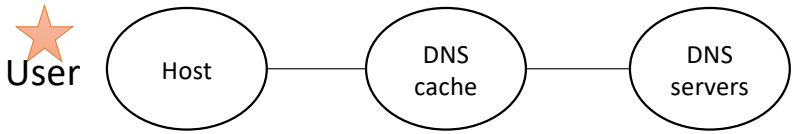
```
$ dig sigarra.up.pt

;; QUESTION SECTION:
;sigarra.up.pt.                 IN      A

;; ANSWER SECTION:
sigarra.up.pt.          49      IN      A       193.137.35.140

;; AUTHORITY SECTION:
up.pt.                  4904    IN      NS      ns4.up.pt.
up.pt.                  4904    IN      NS      ns2.up.pt.
up.pt.                  4904    IN      NS      ns3.up.pt.
up.pt.                  4904    IN      NS      ns1.up.pt.

;; ADDITIONAL SECTION:
ns1.up.pt.              10275   IN      A       193.137.55.30
ns2.up.pt.              2204    IN      A       193.137.55.31
ns3.up.pt.              74589   IN      A       193.137.55.32
ns4.up.pt.              26925   IN      A       193.137.55.33
ns1.up.pt.              11393   IN      AAAA    2001:690:2200:a10::30
ns2.up.pt.              2204    IN      AAAA    2001:690:2200:a10::31
ns3.up.pt.              74589   IN      AAAA    2001:690:2200:a10::32
ns4.up.pt.              26925   IN      AAAA    2001:690:2200:a10::33
```

```
$ dig cloudflare.com
(...)
;; QUESTION SECTION:
;cloudflare.com.                IN      A

;; ANSWER SECTION:
cloudflare.com.         300     IN      A       104.16.132.229
cloudflare.com.         300     IN      A       104.16.133.229

;; AUTHORITY SECTION:
cloudflare.com.         6256    IN      NS      ns4.cloudflare.com.
cloudflare.com.         6256    IN      NS      ns7.cloudflare.com.
cloudflare.com.         6256    IN      NS      ns5.cloudflare.com.
cloudflare.com.         6256    IN      NS      ns6.cloudflare.com.
cloudflare.com.         6256    IN      NS      ns3.cloudflare.com.

;; ADDITIONAL SECTION:
ns3.cloudflare.com.     64      IN      A       162.159.0.33
ns3.cloudflare.com.     64      IN      A       162.159.7.226
ns4.cloudflare.com.     64      IN      A       162.159.1.33
ns4.cloudflare.com.     64      IN      A       162.159.8.55
ns5.cloudflare.com.     64      IN      A       162.159.2.9
ns5.cloudflare.com.     64      IN      A       162.159.9.55
ns6.cloudflare.com.     64      IN      A       162.159.3.11
ns6.cloudflare.com.     64      IN      A       162.159.5.6
ns7.cloudflare.com.     64      IN      A       162.159.4.8
ns7.cloudflare.com.     64      IN      A       162.159.6.6
ns3.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:21
ns3.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:7e2
ns4.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:121
ns4.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:837
ns5.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:209
ns5.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:937
ns6.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:30b
ns6.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:506
ns7.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:408
ns7.cloudflare.com.     64      IN      AAAA    2400:cb00:2049:1::a29f:606
```

What's on the menu for DNS vulnerabilities

- Misleading domain names
- Compromise the victim's host
- Spoofing the local DNS client
- Poison a DNS cache (local)
- Poison a DNS cache (remote)
- Reply forgery from malicious server
- DNS rebinding
- DNS server vulnerabilities
- DoS
- Tunneling, exfiltration





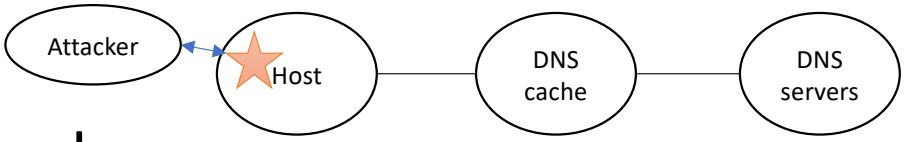
Misleading domain names

- Human vulnerability
- Simple typos
  - gooogle.com g0ogle.com
- Use of visually similar characters in other alphabets

BANK OF AMERICA

www.xn--bakofamerica-qfc.com.	-->	www.baŋkofamerica.com.
mail.xn--bnkofmeric-q5aef.com.	-->	mail.bänkofämericä.com.
secure.xn--bakofamerica-qfc.com.	-->	secure.baŋkofamerica.com.
www.xn--ankofamerica-70c.com.	-->	www.bankofamerica.com.
www.xn--bakofamerica-qfc.com.	-->	www.baŋkofamerica.com.
www.xn--banofamerica-p7b.com.	-->	www.bankofamerica.com.
www.xn--bnkofamerica-pob.com.	-->	www.bąnkofamerica.com.
www.xn--bnkofmeric-ggeef.com.	-->	www.bɑnkofɑmericɑ.com.
www.xn--bnkofmeric-q5aef.com.	-->	www.bänkofämericä.com.
xn--ankofamerica-70c.com.	-->	bankofamerica.com.
xn--bakofamerica-qfc.com.	-->	baŋkofamerica.com.
xn--banofamerica-p7b.com.	-->	bankofamerica.com.
xn--bnkofamerica-pob.com.	-->	bąnkofamerica.com.
xn--bnkofmeric-ggeef.com.	-->	bɑnkofɑmericɑ.com.
xn--bnkofmeric-q5aef.com.	-->	bänkofämericä.com.

https://www.pbs.org/newshour/nation/hackers-are-flooding-the-internet-with-more-fake-domain-names-heres-how-you-can-protect-yourself



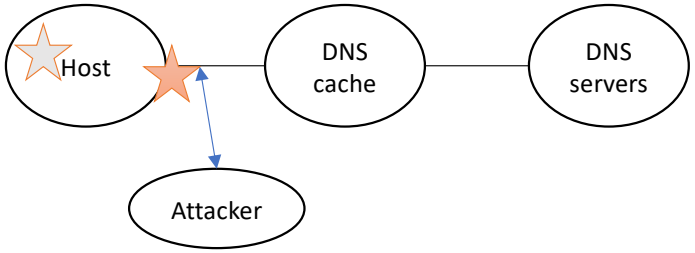
Compromise the victim's host

- The victim's host bootstraps the name resolution process via:
  - /etc/hosts – file with IP-domain mapping local to the host
  - resolv.conf – list of servers to be used by the local DNS resolver

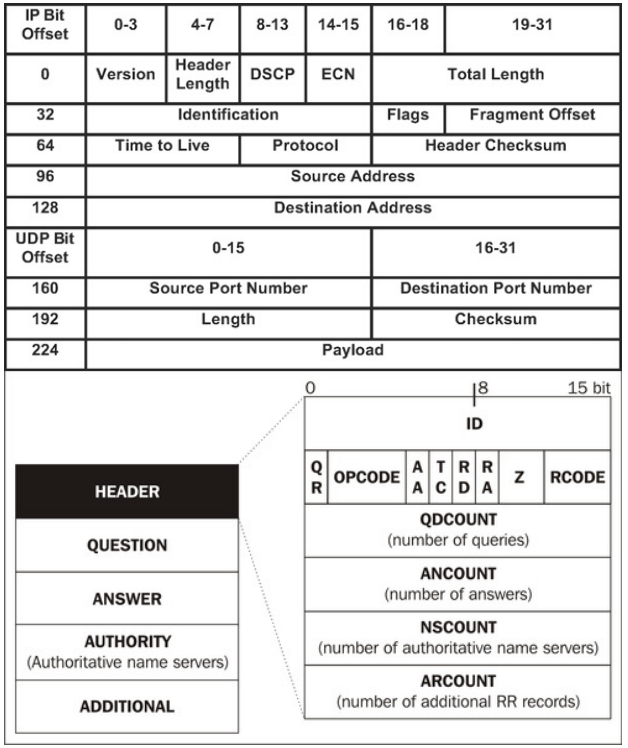
- If the attacker can modify the content of these files, then it can:
  - Directly redirect domain names in host applications to attacker IP (/etc/hosts)
  - Force the victim's DNS resolver to use a DNS server of the attacker

- Restrict write access to these files
  - -rw-r--r--

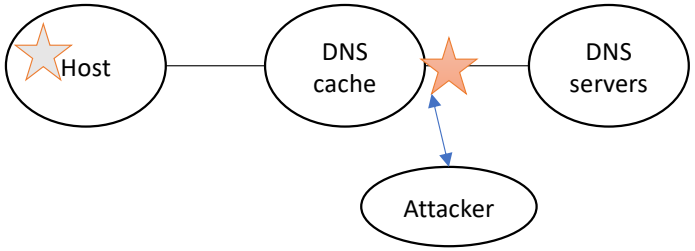
Spoofing a local DNS cache



- Sniff a DNS request from the client
- Spoof a DNS reply back to the client faster than the DNS cache can reply
  - Spoofed reply maps the requested domain name to whatever IP address the attacker wants
- Then the client uses that IP address instead of the real one

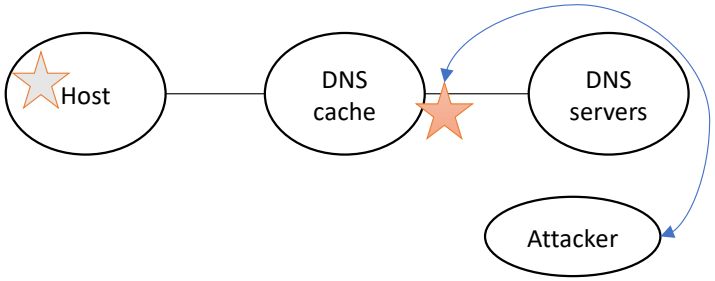


Poisoning a DNS cache (local)



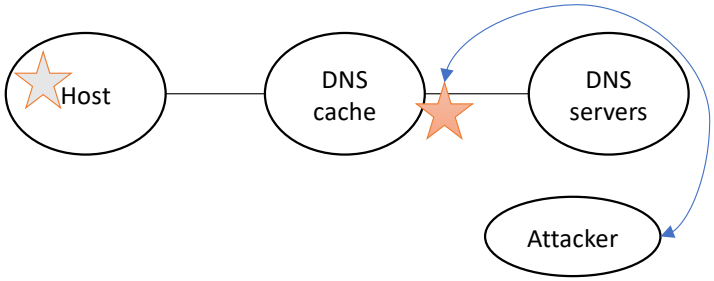
- Sniff a DNS request from the DNS cache to the Internet
  - Local: need to tap into the traffic otherwise will not be able to sniff
- Spoof a DNS reply back to the DNS cache faster than the Internet DNS server can reply
  - Spoofed reply maps the requested domain name to whatever IP address the attacker wants
- Then the DNS cache will be poisoned
  - Any subsequent request/replies from hosts to the cache will be compromised

Poisoning a DNS cache (remote)



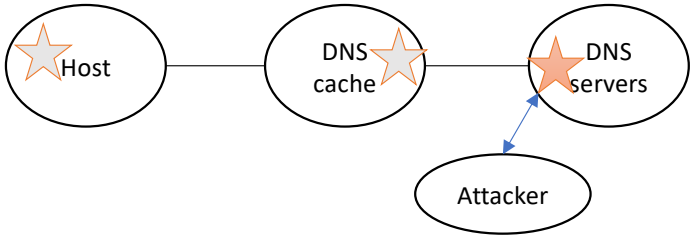
- Often not easy to sniff packet, especially if the attacker is in a remote network
- Approach: remotely trigger DNS request (easy), then spoof reply without sniffing request (hard)
- Difficulties:
  1. DNS queries have ‘random’ DNS transaction ID and client UDP port number, spoofed response must match them
  2. If the actual DNS server replies before the attacker, then attacker will have to wait for a while until cached answer expires
- Kaminsky, 2008

Poisoning a DNS cache (remote)



- Kaminsky, 2008
  - Brute force transaction ID and UDP port number
  - Negate cache effect by querying random domain name (eijdfke.up.pt) under target domain name (up.pt), and append authority section for target domain name (up.pt) with IP address of compromised DNS server
- If attack fails:
  - Choose another random domain name (lalioesjdv.up.pt) under victim SLD (up.pt), repeat brute force attack for transaction ID and UDP port number
  - Ok because new random name will not have been cached
- If attack succeeds:
  - Compromised DNS server for target domain name will have been cached in the victim DNS cache
  - Subsequent requests for domain names under up.pt will be sent to compromised DNS server

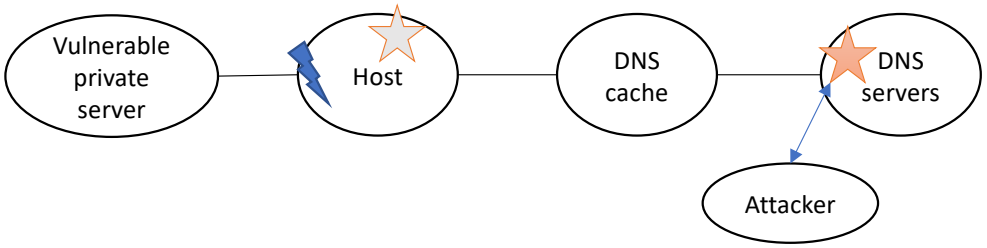
Reply forgery (& poisoning) from malicious DNS server



- DNS cache triggered into making request for domain name in compromised DNS server
- Compromised DNS server appends fake data about legitimate domain names in responses
- IP address for legitimate domain name compromised in DNS cache
- Responses in authority and other sections

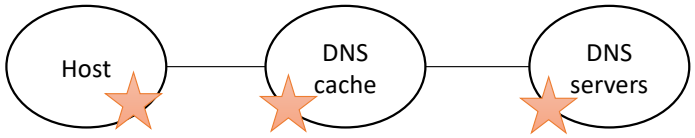
```
$ dig mmm.attacker.uieh

;; QUESTION SECTION:
; mmm.attacker.uieh.                    IN      A

;; ANSWER SECTION:
mmm.attacker.uieh.              16      IN      A       192.0.2.21

;; AUTHORITY SECTION:
attacker.uieh.                  1811    IN      NS      attacker.uieh.
google.com.                     1811    IN      NS      attacker.uieh.
```

DNS rebinding



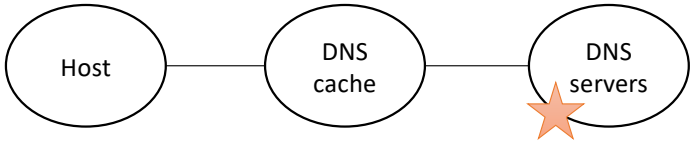
- Threat model
  - Remote attackers want to exploit vulnerable server
  - Server is not directly accessible, inside protected network (NAT, firewall)
  - Run malicious code on victim's browser, inside protected network
  - Browser sandboxing prevents this
- Attack: bypass sandboxing Same Origin Policy (SOP)
  - Provide fake IP for attacker's domain name
  - The fake IP is the IP of the target, vulnerable server inside the private network
  - SOP is not violated because it looks at domain names – not IP addresses
  - Attacker code on victim's browser can now exploit private server

DNS server vulnerabilities



- CVE-2002-1219
  - Buffer overflow in named in BIND 4 versions 4.9.10 and earlier, and 8 versions 8.3.3 and earlier, allows remote attackers to execute arbitrary code via a certain DNS server response containing SIG resource records (RR).
- CVE-2020-8625
  - BIND servers are vulnerable [...] Although the default configuration is not vulnerable, GSS-TSIG is frequently used in networks where BIND is integrated with Samba, as well as in mixed-server environments that combine BIND servers with Active Directory domain controllers. The most likely outcome of a successful exploitation of the vulnerability is a crash of the named process. However, remote code execution, while unproven, is theoretically possible.

DoS



- Issue more requests than those that a server can handle
  - Spoof source address in DNS request, reflection attack
  - Amplification attack, reply to victim with more data than request

- Issue time-consuming requests
  - NXDOMAIN attack, water torture
  - NXNSAttack, request/reply storm between resolvers (DNS caches) and authoritative NS

https://www.akamai.com/content/dam/site/en/documents/research-paper/dns-reflection-vs-dns-mirai-technical-publication.pdf
Water torture https://dl.acm.org/doi/pdf/10.1145/3297156.3297272
NXNSAttack https://www.usenix.org/conference/usenixsecurity20/presentation/afek

Tunneling, exfiltration, covert channels

- Firewalls typically don’t filter DNS traffic
- This makes it desirable for attackers
- Tunneling
  - Use modified DNS servers and clients
  - Send and receive data over DNS requests and replies
  - Use different fields in the DNS packets
- Exfiltration only
  - Encode information as characters (83jh8wdlkjdf)
  - Create domain name with those characters, 83jh8wdlkjdf.exfiltration.uieh
  - exfiltration.uieh DNS server receives information in DNS request

https://www.akamai.com/blog/news/introduction-to-dns-data-exfiltration
https://en.wikipedia.org/wiki/Covert_channel

Security of Networks, Services, and Systems

DNS and routing vulnerabilities

Ricardo Morla

FEUP – SSR/M.EEC, SR/M.EIC