DNS Security

Outline

- DNS Security
  - Concepts (Review)
  - DNS Security Threats
  - DNS Security Protocols
    - DNSSEC
    - DoT; DoH
    - other

DNS Concepts

- Review
  - Purpose of DNS and its role on the Internet
  - DNS architecture
    - distributed, hierarchical structure
    - root servers, TLDs
    - authoritative name servers
      - provide definitive answers for DNS queries (iteratively) about specific domains and resources they are responsible for
    - textual databases (resource records)
    - recursive resolvers (usually local resolvers)
  - Common queries
    - SOA, A, AAAA, MX, CNAME, NS, PTR,…

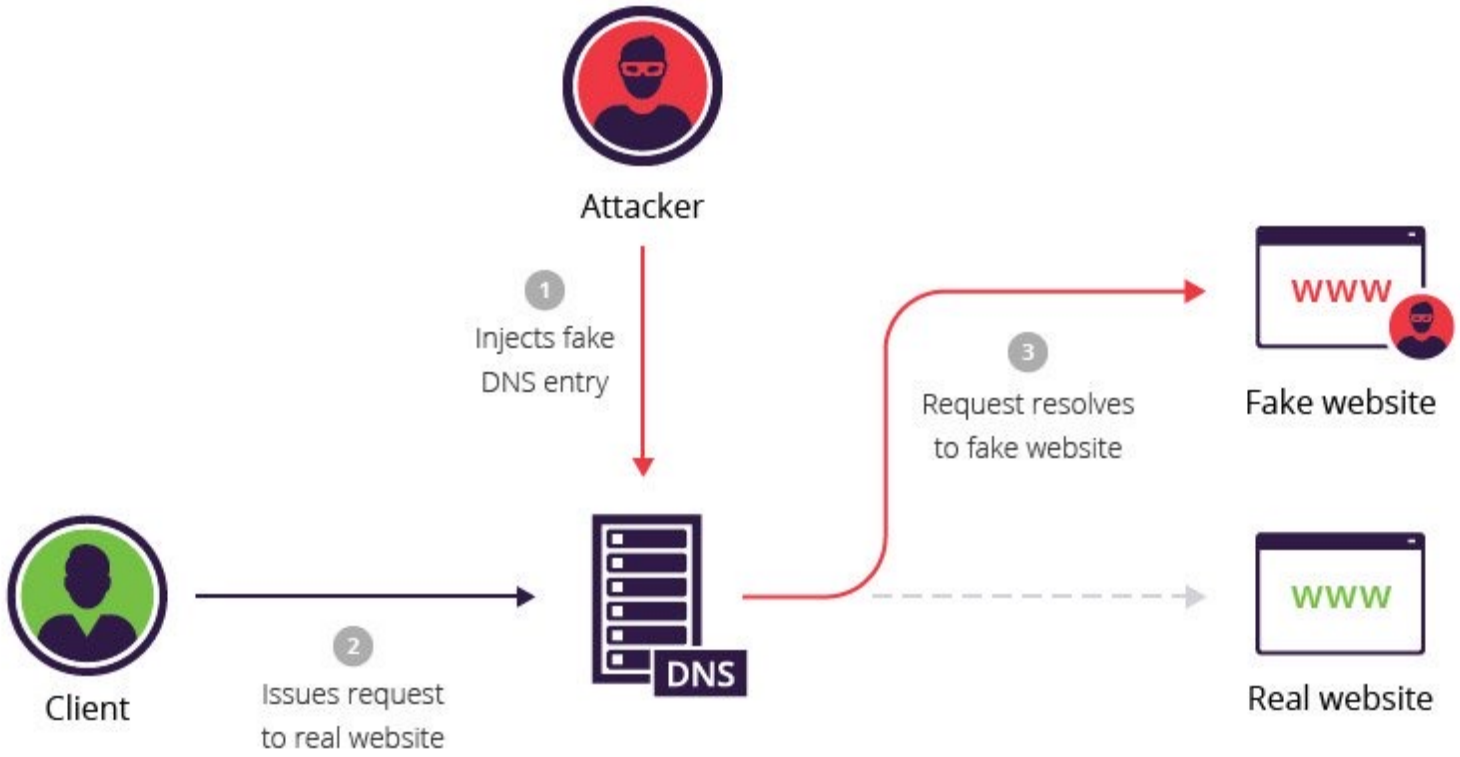
DNS Concepts

- Default application behavior
  - most applications use system's DNS resolver calls (via system libraries such as `gethostbyname()` or `getaddrinfo()`) for simplicity and portability
  - the system resolver typically communicates with a recursive DNS server (config in `/etc/resolv.conf` on Unix-like systems or via DHCP)
  - communication is usually unencrypted, using traditional DNS over UDP/TCP (port 53)
    - vulnerable to attacks, privacy concerns
  - few apps secure DNS name resolution
    - browsers (e.g., Mozilla Firefox, Google Chrome) offer built-in DoH
    - specialized apps that require privacy and/or security (e.g., VPN clients)

DNS Security - Threats

- DNS Spoofing (Cache Poisoning)
  - attacker manages to insert false DNS information into a resolver's cache, causing users to be directed to malicious websites
    - e.g., fake IP address is returned for a legitimate domain, redirecting users
  - subsequent requests from other users or applications will get malicious data from DNS caching system
  - attacker may also exploit TTL of cache entries to ensure malicious data persistence
  - may result in phishing attack or credential theft
  - Mitigation
    - use DNSSEC to verify the authenticity of DNS responses
    - use short RR TTLs to reduce risk of cache poisoning

DNS Security - Threats



DNS Spoofing (Cache Poisoning)

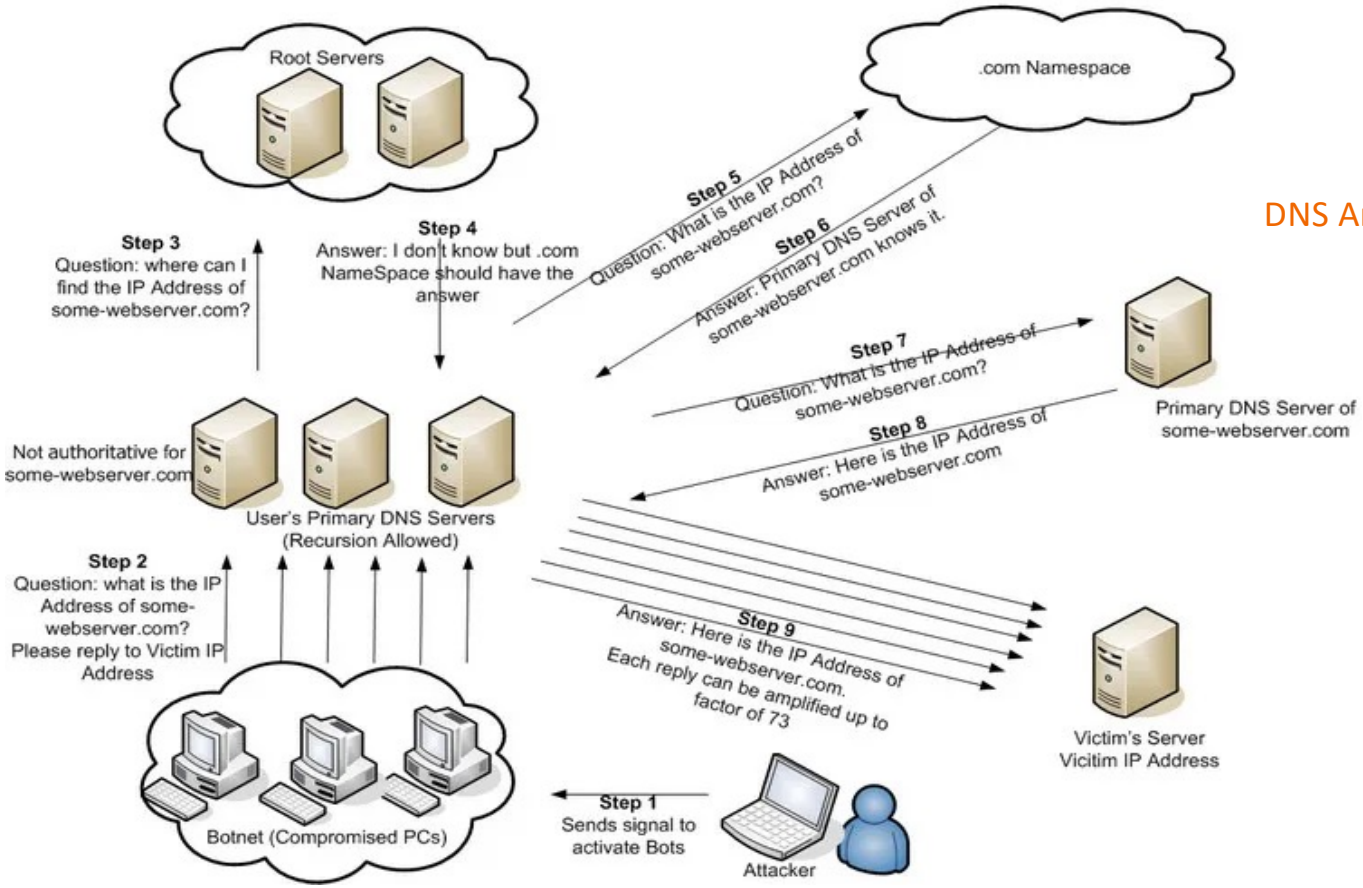
DNS Security - Threats

- DNS Reflection Attack
  - attacker sends DNS queries to a resolver with a spoofed source IP (victim's IP), causing the resolver to send responses to the victim
  - often used in conjunction with DNS amplification to overwhelm a target
  - may cause DoS at target
  - Mitigation
    - disable recursion for non-authorized clients
    - implement response rate limiting (RRL) on DNS servers

DNS Security - Threats

- DNS Amplification Attack (DDoS attack)
  - attacker sends small DNS queries with spoofed source IPs (victim's IP), causing large DNS responses to flood the victim
    - e.g., single 60-byte query may generate a 4,000-byte response, overwhelming the target (using IP blacklists is ineffective!)
  - may result in service outages and degradation of targeted systems
  - Mitigation
    - configure DNS servers to prevent open resolvers (respond to queries from anyone on the Internet regardless of whether it's responsible for them)
    - implement response rate and response size limits
    - use ingress/egress filtering to prevent IP spoofing, i.e., only IP addresses belonging to the network can query and send responses, blocking IP spoofing blocks the attack

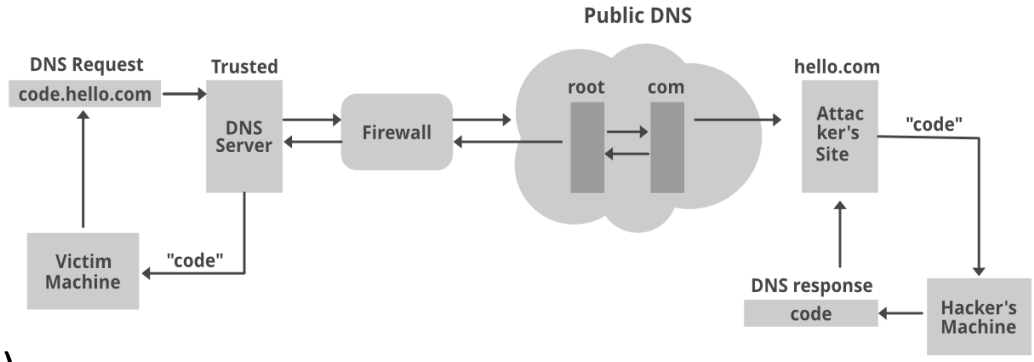
DNS Security - Threats



DNS Amplification (DDoS)

DNS Security - Threats

- DNS Tunneling Attack
  - requires a compromised host (e.g., infected with malware)
  - attacker encodes data in DNS queries/responses effectively bypassing network security controls to exfiltrate data or create a backchannel
    - e.g., for sending pwd, malware encodes and queries for `c2VjcmV0.hello.com`
  - results in data breaches, furtive command and control (c2) comm.
  - Mitigation
    - monitor for unusually high volume of DNS queries or suspicious domains
    - use DNS traffic analysis tools to detect tunneling activity (long names, TXT, CNAME RRs)



DNS Security - Threats

- DNS Man-in-the-Middle (MitM) Attack
  - attacker intercepts DNS communication between a client and legitimate server, monitoring or altering the data in transit
    - e.g., injecting spoofed responses (DNS spoofing) or blocking legitimate DNS responses
  - attacker positioning can be achieved via network-based techniques like ARP spoofing, DNS server compromise, or rogue APs
  - may result in data theft, phishing, or injection of malicious payloads
  - Mitigation
    - use DNS over HTTPS (DoH) or DNS over TLS (DoT) to encrypt DNS traffic
    - secure communication channels and use authentication mechanisms (*more soon…*)
    - however, most apps still delegate DNS resolution to OS via system libraries

DNS Security - Threats

Aspect	DNS MitM Attack	DNS Spoofing (Subtype of MitM Attack)
Scope	Broad: Manipulating, observing, or blocking DNS communications	Narrow: Injecting falsified DNS responses
Position	Requires MitM positioning	May or may not involve MitM positioning (e.g., spoofed responses can arrive faster than legitimate ones)
Effect	Can modify, block, or observe traffic dynamically	Alters DNS records to mislead or redirect traffic
Persistence	Temporary or dynamic manipulation	May poison the cache for longer-lasting redirection
Examples	Redirecting queries dynamically, blocking DNS resolution	Redirecting victim to an attacker-controlled IP

- DNS MitM vs DNS Spoofing

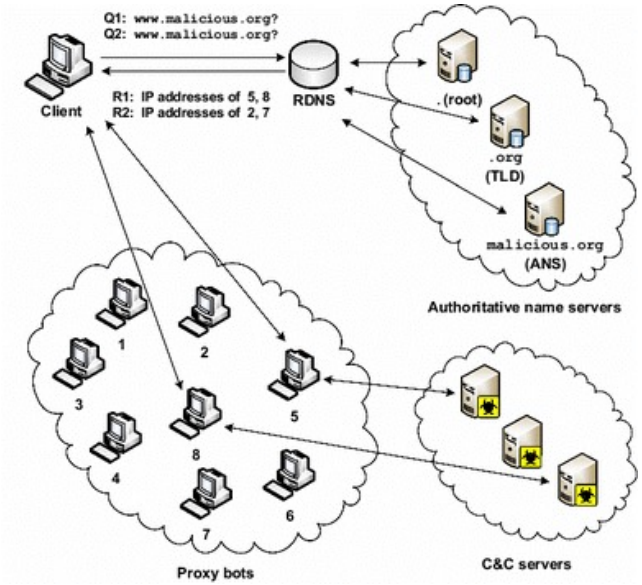
DNS Security - Threats

- Typosquatting (URL Hijacking) and Malicious Domains
  - attacker registers domains similar to legitimate domains (goolge.com)
  - redirect users to fake domains that mimic legitimate websites
  - may result in phishing attacks, malware downloads, financial fraud
  - Mitigation
    - monitor and blacklist suspicious domains
- Domain Hijacking
  - attacker gains unauthorized control over a domain by compromising its registrar account or exploiting vulnerabilities (critical)
  - Mitigation
    - use strong passwords and multi-factor authentication for registrar accounts
    - enable domain lock features to prevent unauthorized domain transfers

DNS Security - Threats

- Fast Flux Networks
  - attacker rapidly changes IP addresses* associated with its domain, making it difficult to detect and shutdown malicious servers
    - botnets use fast flux DNS to hide phishing or malware distribution servers
  - obfuscates malicious activities and prolongs attack lifespan
  - Mitigation
    - monitor for domains with unusually high DNS changes
    - collaborate with ISPs and domain registrars to block malicious nets
    - hard to tackle

* with very low TTLs!



DNS Security Protocols

- DNSSEC (DNS Security Extensions)
  - enhances security by ensuring the integrity and authenticity of DNS data, but does not encrypt DNS traffic
  - prevents attackers from tampering with DNS responses (e.g., cache poisoning), providing:
    - Data Integrity and Authenticity – based on signatures to validate responses
    - Public Key Infrastructure (PKI) – each DNS zone* has a key pair (public/private)
    - Chain of Trust – from the root zone down to individual domains
    - DNSSEC-Specific RR Types
      - RRSIG: contains the cryptographic signature of a DNS record
      - DNSKEY: publishes the public key used to verify signatures
      - DS (Delegation Signer): establishes trust between parent and child zones

* A zone is an administrative control area that holds DNS data for a domain, e.g. uminho.pt (parent zone), and can include its subdomains (child zones).

DNS Security Protocols

- Extract of DNSSEC zone file

```
mydomain.com.   IN  A          192.0.2.1
mydomain.com.   IN  RRSIG      A 5 2 3600 ... (signature of the A record)
mydomain.com.   IN  DNSKEY     256 3 8 ... (public key)
mydomain.com.   IN  DS         ... (delegation signer record for parent zone)
```

- Open source tools:
  - DNSSEC-Enabled Servers: BIND 9 (ISC), Unbound (local resolver) and NSD (NLnet LABS)
  - DNSSEC Tools (Internet Society) – for DNS verification

DNS Security Protocols

- DNSSEC Advantages
  - prevents DNS cache poisoning (by verifying signatures)
  - ensures authenticity (only data signed with legitimate private key is accepted)
  - brings layer of trust to DNS
- DNSSEC Limitations
  - does not encrypt data
  - requires server/resolver updates
  - expired signatures may disrupt the service
  - increases response size
  - many servers and resolvers do not support DNSSEC

DNS Security Protocols

- DNS over TLS (DoT)
  - DoT encrypts DNS traffic using the TLS, ensuring privacy and integrity for DNS queries/responses
  - client sets a TLS session with resolver before sending any DNS queries
  - DoT resolver listens on port 853 for encrypted queries
- DNS over HTTPS (DoH)
  - DoH sends DNS queries/responses over HTTPS (also on port 443)
  - queries/responses are encapsulated within HTTPS requests/responses
  - apps (e.g., Firefox, Chrome) can directly resolve DNS queries using DoH, bypassing the OS resolver
  - not blocked by firewalls; obfuscate DNS traffic (also malicious domains)

DNS Security Protocols

Aspect	DoT	DoH
Encryption	Uses TLS to encrypt DNS traffic	Uses HTTPS to encrypt DNS traffic
Port	Dedicated port 853	Port 443 (shared with web traffic)
Integration	System-level resolver or application	Application-level (e.g., browsers)
Firewall Blocking	Easier to block (port-specific)	Harder to block (uses web port 443)
Centralization Risk	Exists but less prominent than DoH	Higher due to popular DoH providers
Monitoring	Traffic can be monitored more easily	Obscures DNS queries, harder to monitor

- DoT vs. DoH – both are expanding (DoH in web browsers, DoT in ISPs and enterprises)
- Despite their benefits, broader adoption faces challenges including performance overhead or lack of awareness

DNS Security Protocols

Other solutions

- Authenticated DNS (T-DNS)
  - uses TSIG (Transaction Signature[1]) or SIG(0)[2] to secure individual DNS server transactions (e.g., zone transfers) using cryptographic signatures
  - during a zone transfer, TSIG can authenticate the transfer session, while DNSSEC ensures that the zone data itself is authentic
  - primarily used for server-to server communications
- DNSCrypt
  - authenticates and encrypts DNS queries/responses between client and a supporting resolver, while DNSSEC ensures the resolver is retrieving genuine DNS data
  - does not rely on HTTP/TLS, own protocol over UDP
  - not natively integrated into OSs or browsers (as DoH and DoT), meaning users need to configure it manually or use third-party software

[1] uses PSK; [2] uses PKI.

DNS Security Protocols – Best Practices

- DNSSEC Integration with DoT/DoH
  - best current practice for securing DNS, but implementation may vary based on use case (enterprise, ISP, institutional, etc.)
  - DNSSEC ensures authenticity of DNS data, verifying that responses are from the correct source and haven't been tampered with (integrity)
  - DoT and DoH encrypt DNS traffic, protecting it from eavesdropping
  - combining these mechanisms ensures that:
    - DNS responses are verified (via DNSSEC)
    - queries/responses are protected from modification during transmission
  - limitations, if separated:
    - DNSSEC does not encrypt DNS traffic; DoT/DoH addresses this gap
    - DoT/DoH does not validate DNS records; DNSSEC provides this assurance

DNS Security Protocols – Best Practices

- Enterprises
  - often prioritize DoT due to easier integration with network-level controls (e.g., firewalls and monitoring)
  - DNSSEC may be deployed for securing internal and external domains but requires proper key management
- ISPs
  - increasingly offer DoT or DoH as default resolver options to protect customer privacy and prevent attacks like DNS spoofing
  - some also support DNSSEC validation, ensuring authenticity of DNS
- Institutions (gov, edu, org, etc.)
  - may deploy DNSSEC for authoritative servers to secure public records
  - typically use DoT for internal DNS traffic to balance confidentiality and performance

Summary

- DNS Security
  - Concepts (Review)
  - DNS Security Threats
  - DNS Security Protocols
    - DNSSEC
    - DoT; DoH
    - other