Imperial College London

Network and Web Security

DNS

Dr Sergio Maffeis
Department of Computing
Course web page: http://331.cybersec.fun

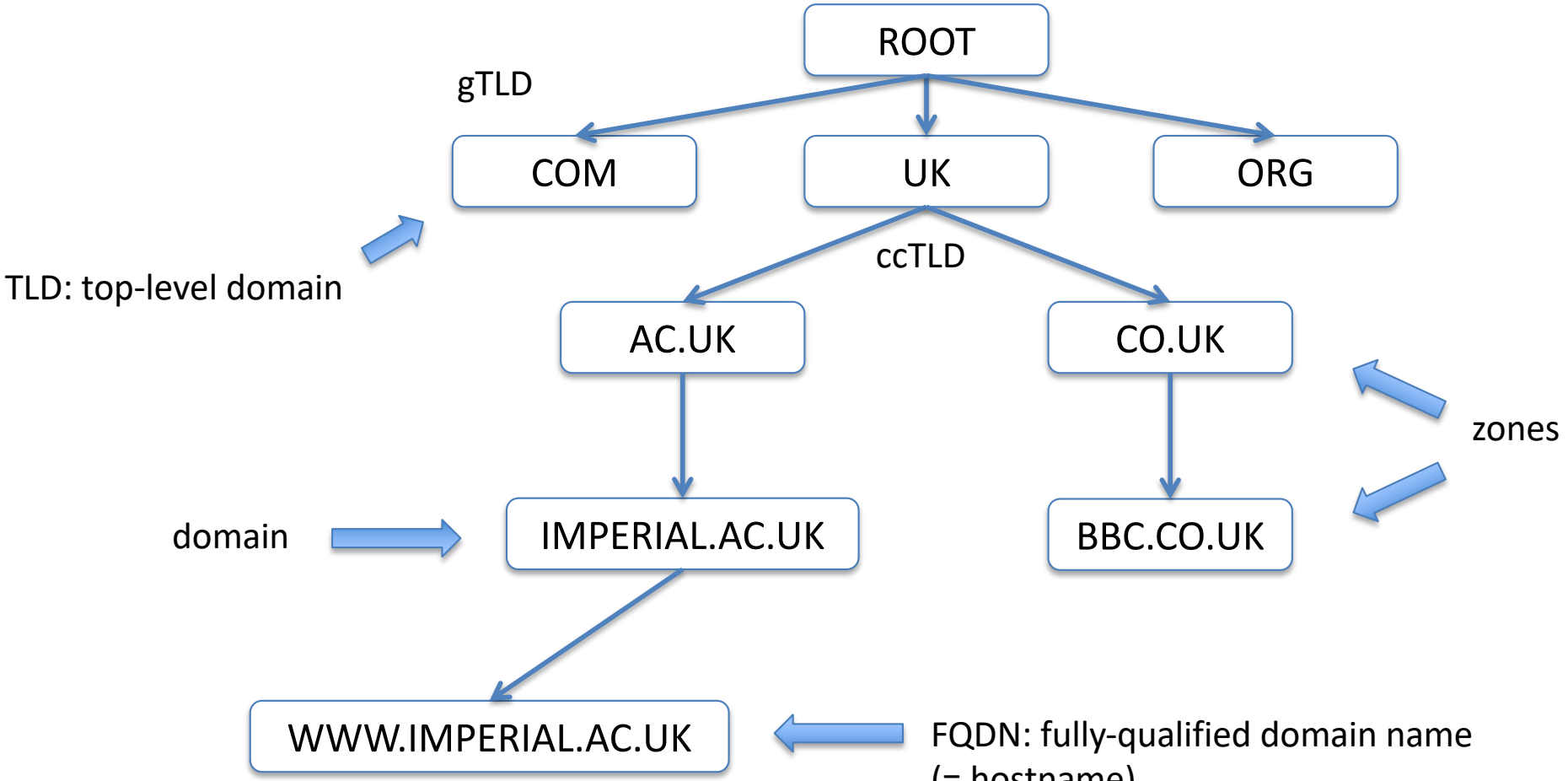
Domain Name System

Imperial College London

- The Domain Name System (DNS) lets us identify hosts via *hostname* instead of IP address
  - `www.imperial.ac.uk` instead of `155.198.140.14`
  - Hostnames are easy to remember, descriptive of service or brand
  - The DNS separates the logical address of a service from the physical address of the host running that service
    - Hostname does not need to change as we switch network provider
- *DNS Resolution*
  - Before creating an IP packet, a local *DNS client* (or *resolver*) looks up the IP address of the target hostname
    - Hostname-IP responses are valid for a limited amount of time (TTL)
    - Often responses are in the local cache
    - Otherwise, the resolver queries an external *primary* (or *recursive*) *DNS server*
  - Normal DNS traffic is sent over UDP
    - Typical queries and responses are small and fit in 1 UDP packet (512 bytes)
    - When more data needs to be exchanged, DNS falls back to TCP
- Domain names are organized hierarchically
  - DNS is managed by ICANN/IANA, which runs the root DNS servers

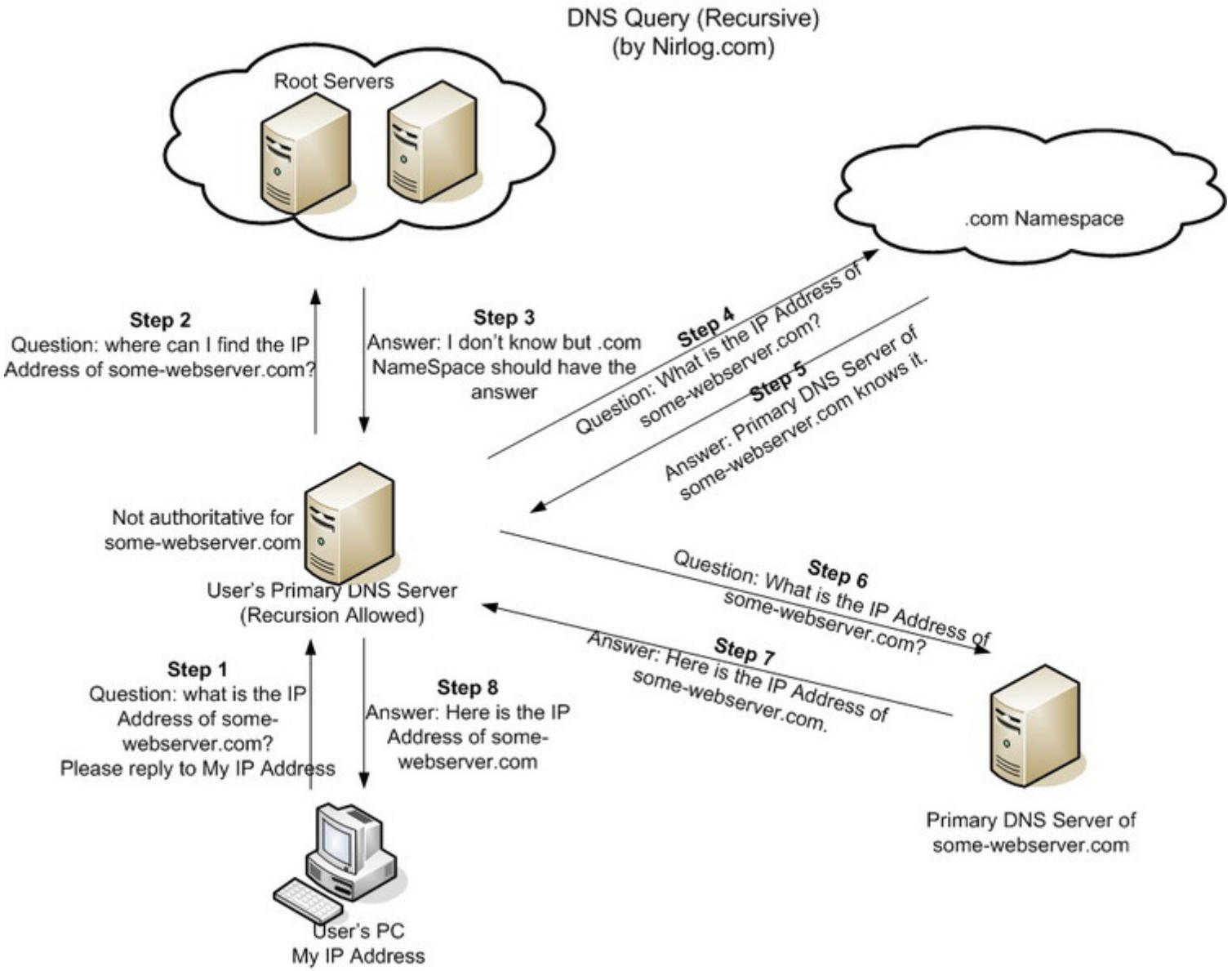
Domain Name System

Imperial College London



DNS resolution

Imperial College London



Common DNS records

Imperial College London

Resource Record	Description
SOA (Start of Authority)	Indicates that the server is the best authoritative source for data concerning the zone. Each zone must have an SOA record, and only one SOA record can be in a zone.
NS (Name Server)	Identifies a DNS server functioning as an authority for the zone. Each DNS server in the zone (whether primary master or secondary) must be represented by an NS record.
A (Address)	Provides a name-to-address mapping that supplies an IPv4 address for a specific DNS name. This record type performs the primary function of the DNS: converting names to addresses
AAAA (Address)	Provides a name-to-address mapping that supplies an IPv6 address for a specific DNS name. This record type performs the primary function of the DNS: converting names to addresses.
PTR (Pointer)	Provides an address-to-name mapping that supplies a DNS name for a specific address in the in-addr.arpa domain. This is the functional opposite of an A record, used for reverse lookups only.
CNAME (Canonical Name)	Creates an alias that points to the canonical name (that is, the "real" name) of a host identified by an A record. Administrators use CNAME records to provide alternative names by which systems can be identified.
MX (Mail Exchange)	Identifies a system that will direct email traffic sent to an address in the domain to the individual recipient, a mail gateway, or another mail server.
NXDOMAIN (Non-Existent Domain)	Name cannot be resolved: not registered or invalid.

DNS MITM attack

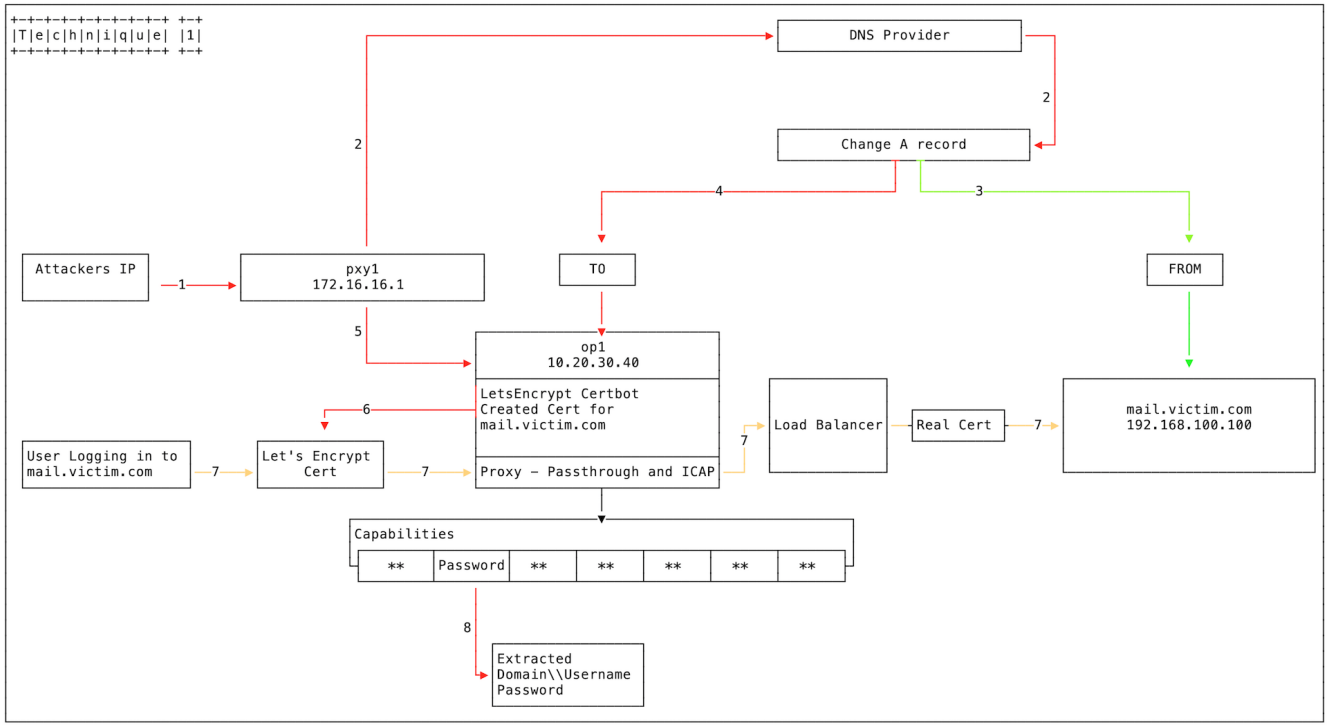
Imperial College London

- Turkish government wanted to block Twitter access in March 2014
- Forced ISPs to respond to DNS queries for twitter.com with the IP of a government website
  - Effectively the ISP DNS resolvers launched a MITM attack on link between user and public DNS servers
- Once it became obvious, users got around restriction using Google's Public DNS

DNS Hijacking campaign

Imperial College London

- *DNSpionage (2019)*
  - Malicious actors compromised DNS resolution of global gov, telcos, web infrastructure websites to become MITM
  - Attributed to Iranian government by FireEye
- Techniques
  - Compromise DNS provider admin panel, change A record of target mail servers
  - Compromise registrar or TLD, change NS record, run rogue NS
  - Using either technique
    - Redirect queries for target mail servers coming from victim IPs to rogue mail server IP
    - Give honest answers to other queries
- See FireEye post in recommended reading for more details



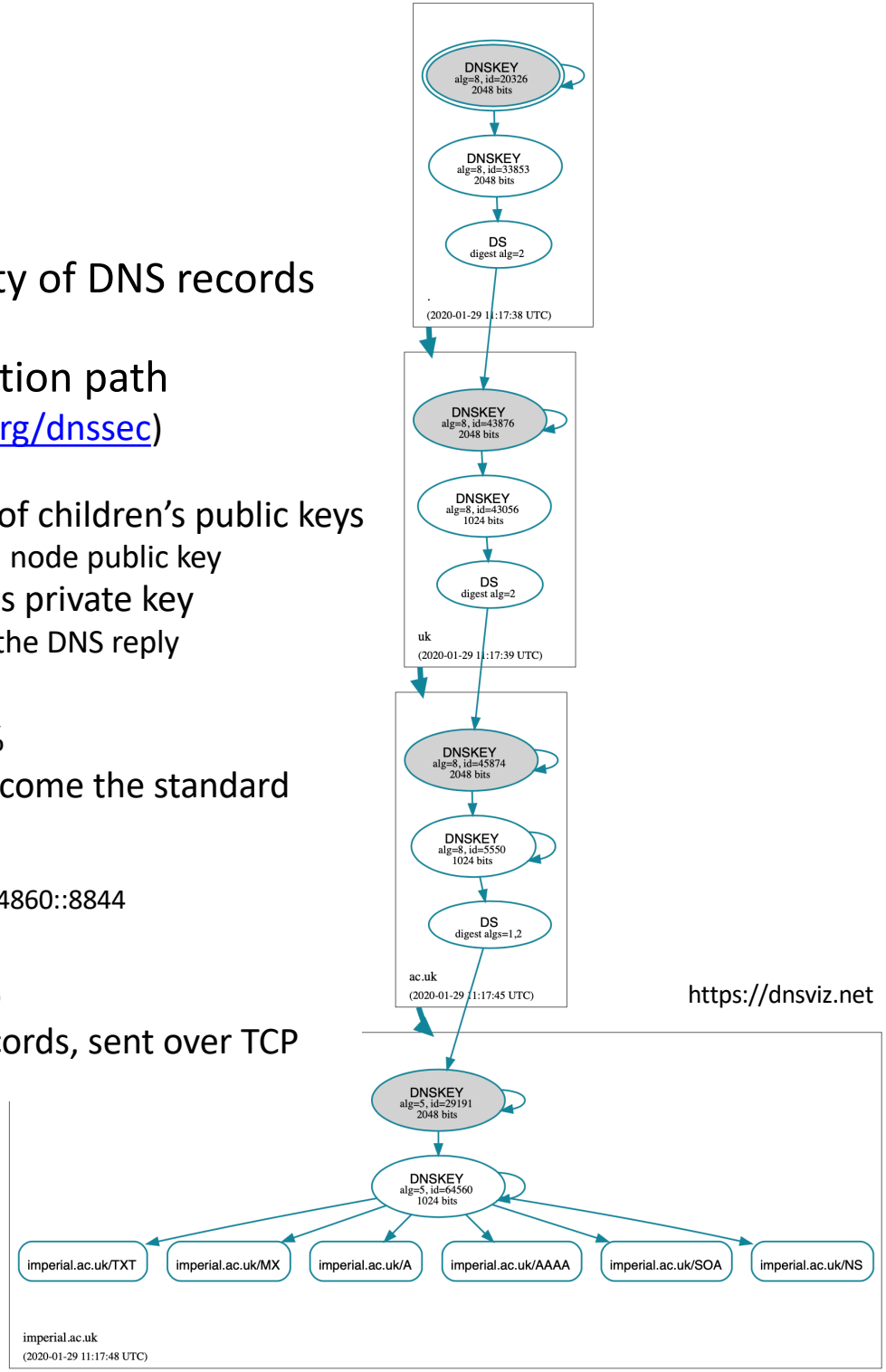
DNS security issues

Imperial College London

- DNS requests and responses are not authenticated
  - Attackers can map trusted domain names to malicious IPs
    - Trivial for MITM
      - Some legitimate ISPs intentionally replace NXDOMAIN responses with pages that display ads
    - Off-path attacker on LAN may be able to
      - Inject spoofed DHCP packets, advertising malicious DNS resolver
      - Inject spoofed replies to DNS queries, after seeing the query ID
        - » Try it in the lab this week!
    - LAN router compromise also used to advertise malicious resolvers
      - *DNSChanger* malware
      - We'll see CSRF-based *Drive-By Pharming* example later
  - *DNS cache poisoning*
    - Spoofed responses keep being served by intermediaries up to TTL
    - Off-path attacker can poison cache of honest DNS server
      - See recommended reading
    - DNSpooq vulnerabilities in *dnsmasq*, January 2021
  - *DNS rebinding*
    - We'll see example later in the course
- Name servers can be hacked
  - DNS hijacking
    - DNSpionage (previous slide)
    - SeaTurtle (different techniques)

DNSSEC

- *DNSSEC* protects authenticity and integrity of DNS records
  - Each DNS zone has public/private key-pairs
- DNSSEC chain of trust follows DNS resolution path
  - Trust starts at DNS root (https://www.iana.org/dnssec)
    - Resolvers know public keys of root nodes
  - Parent node uses private key to sign hashes of children's public keys
    - This lets resolvers check the authenticity of a node public key
  - DNS resolution node signs zone data using its private key
    - This lets resolvers check the authenticity of the DNS reply
- Adoption
  - Low validation rate: USA 24%, UK 9%, CN 1%
  - As more services support DNSSEC, it may become the standard
    - Google's Public DNS uses DNSSEC by default
      - IPv4: 8.8.8.8 and 8.8.8.4
      - IPv6: 2001:4860:4860::8888 and 2001:4860:4860::8844
- Weaknesses
  - Increased load on DNS servers due to crypto
  - Decreased network performance: longer records, sent over TCP



https://dnsviz.net

DNSSEC zone enumeration

Imperial College London

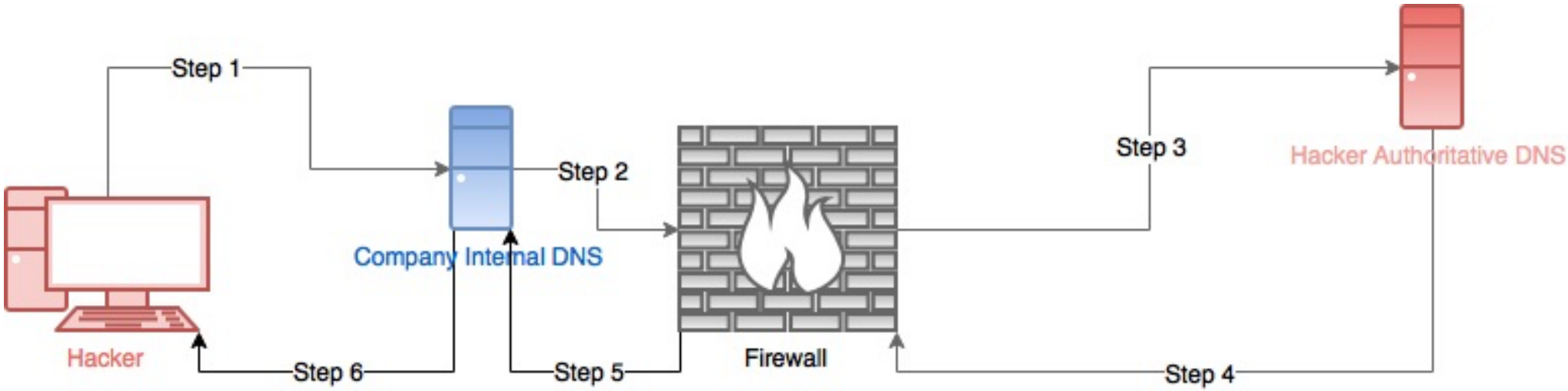
- If a domain does not exist, an NSEC record reveals alphabetically-closest neighbors
  - Failed query: “resolve bob.example.com”
  - Response: “no records exist between alice.example.com and charlie.example.com”
- NSEC is useful to *prove* that the domain does not exist
  - No further DNS queries are necessary
    - DNSSEC queries are relatively expensive
- Problem: this helps hacker’s intelligence gathering activities
  - Find out which domains don’t exist (bob) and discover “closest” ones (alice, charlie)
  - Target scanning activities reducing chance of detection
- NSEC3 extension mitigates problem by using (salted) hashes of domain names

  - Failed query: “resolve bob.example.com”
  - Response: “no records exist between 4EE23198.example.com and D14DEA64.example.com, the salt is 65BF”
  - Still useful as a proof of non-existence
    - Given salt, check that 4EE23198 < Hash(bob|65BF) < D14DEA64
  - Salt hinders dictionary attacks: changes over time and across zones

DNS tunneling

Imperial College London

- Goal: bypass a firewall or proxy that prevents HTTP communication with the target



1. Attacker encodes data to be sent in a DNS query for a domain for which he controls the authoritative DNS
2. Domain is not found locally, eventually authoritative server is contacted
3. DNS queries (and in particular to non-blacklisted domains) are not filtered
4. Server replies encoding data in DNS response
5. Firewall forwards innocent-looking response
6. Attacker receives and decodes the reply

- Vanilla version: exfiltrate data encoded as subdomain-names
- Advanced version: DNS SOCKS proxy to browse arbitrary websites (very slowly)

Malicious domain registration

Imperial College London

- Cybersquatting
  - Register trademarked terms in order to re-sell to legitimate brand owner for higher price
  - Outlawed at lest in the US
  - Example: shanghaidreamworks.com (2011)
- Typosquatting
  - Register names that are 1 or a few typos away from existing legitimate domains
  - Visitors will come by mistake
  - Used to generate advertising revenue or deliver attacks
  - Nowadays *defensive* registrations are common
    - http://goolge.com redirects to https://www.google.com
- Bitsquatting
  - Same as above, but relying on accidental bitflip in memory or on the wire
  - https://amazon.co.uk versus https://a-azon.co.uk (ASCII for “m” is 1 bit-flip away from “-”)
  - Error rates are low (3 bit flips per month in 4GB DRAM)
    - But go up on old hardware, no ECC, on airplanes, etc
- Dropcatching
  - Register newly expired domains to resell to owners or exploit residual trust
  - Example: granny-daily.com re-registered to serve malware instead of granny-news

Other DNS abuse

Imperial College London

- Malicious actors use domain names
  - Avoid hard-wiring malicious IPs to evade detection and replace blocked hosts
  - Web-based attacks need to include malicious resources
  - Malware uses DNS to contact C&C and exfiltration servers
    - Domain Generation Algorithms (DGAS)
      - Create pseudorandom sequence of candidate names to be contacted in a sequential fashion until one responds
      - Attacker needs to register only some of these names, when needed
  - Random-looking names
    - Example: myypqmvzkgnrf.com
    - Easy to generate, compact, cheap
    - Easier to block by IDS
  - Dictionary-based
    - Example: milkdustbadliterally.com
    - Depending on dictionary, cannot be blocked as they may be legitimate
      - ww1-filecloud.com, cdn-imgcloud.com, font-assets.com, wix-cloud.com, js-cloudhost.com
  - Active research on detection of malicious traffic based on domain names
    - Rule-based approach risks too many false positives
    - Machine learning techniques are giving promising results: CNN, LSTM, …
- Administrators may loose track (control) of NS pointers
  - Expired registration, mistyped names, bitsquatting
    - Can happen at any point in the resolution path, with different impact
    - In 2017 a security researcher registered a dangling NS name for the .io zone
      - A 25% chance he could control any .io resolution
  - IP takeover via compromise
  - DNS information gathering tool: https://dnsdumpster.com