Internet Security

50.520 Systems Security

Paweł Szałachowski

Internet Security

- End-to-end communication through the Internet
- Applications are usually service-oriented
  - Services are associated with names
- How to define a service (with the OSI model)?

Internet Security

- What protocols are involved?
  - How to translate names to addresses?
  - How to reach addresses?
  - How to talk securely to the service/endpoint?
- Desired properties
  - Make sure what is an authentic address
  - Make sure that traffic is sent via an authentic path
  - Make sure that the service/endpoint is authentic and data is protected

Border Gateway Protocol (BGP)

- Dominant Inter-domain routing protocol
  - Need of a dynamic Internet routing protocol
  - Determines how packets traverse the Internet
  - Autonomous Systems (ASes) are the protocol parties
  - Allows to express routing policies

Border Gateway Protocol (BGP)

- AS-level entities
  - Each AS has a unique number associated (ASN)
- IP address blocks are assigned/delegated to ASes
  - Scalability reasons
  - ICANN is the root

Border Gateway Protocol (BGP)

- Route origination
  - Border routers announce prefixes
  - Longest prefix match
    - More specific prefix is preferable
    - Storage overhead
- Business relationships
  - Valley-free routing

BGP Security

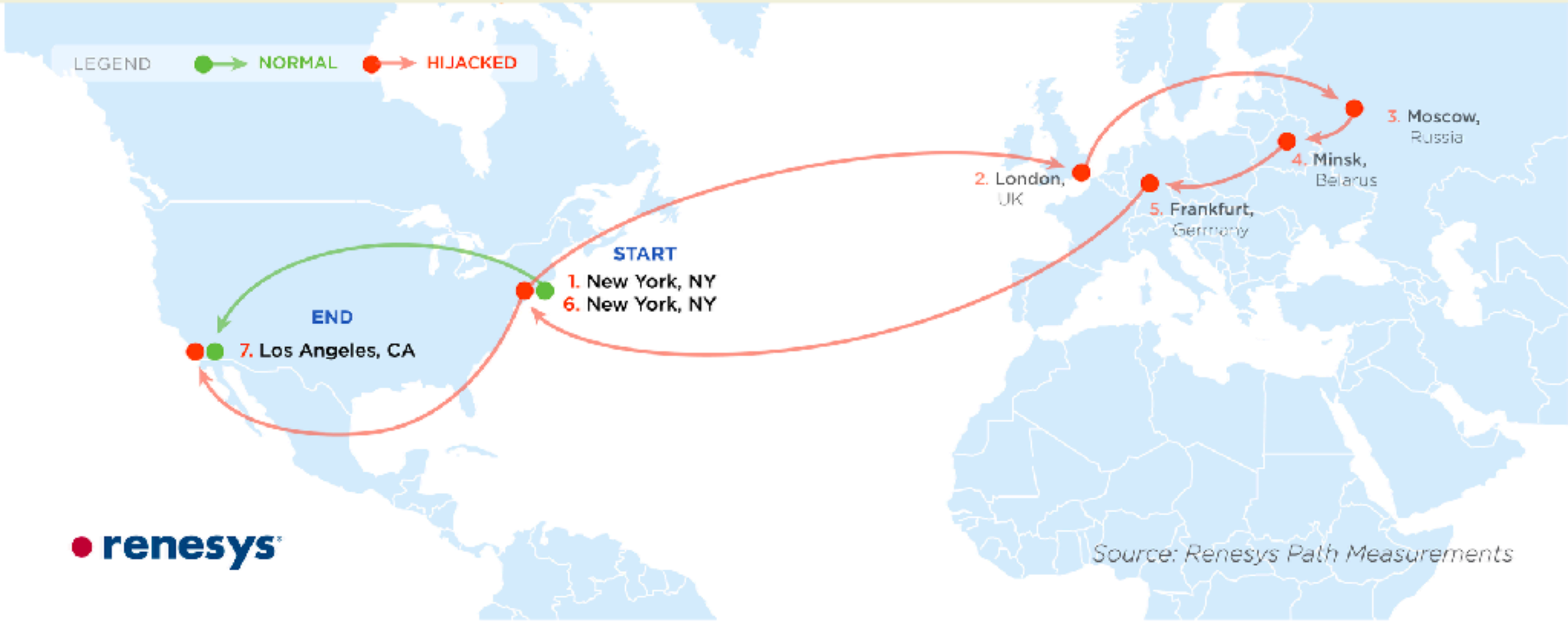
- Attacks on TCP
- Path manipulation
- Misconfigurations
- Malicious Route Origination
  - Route hijacking
    - Targeted attacks
  - Blackholing

Denver to Denver

Traceroute Path 2: from **Denver**, CO to **Denver**, CO via ***Iceland***

NYC to LA

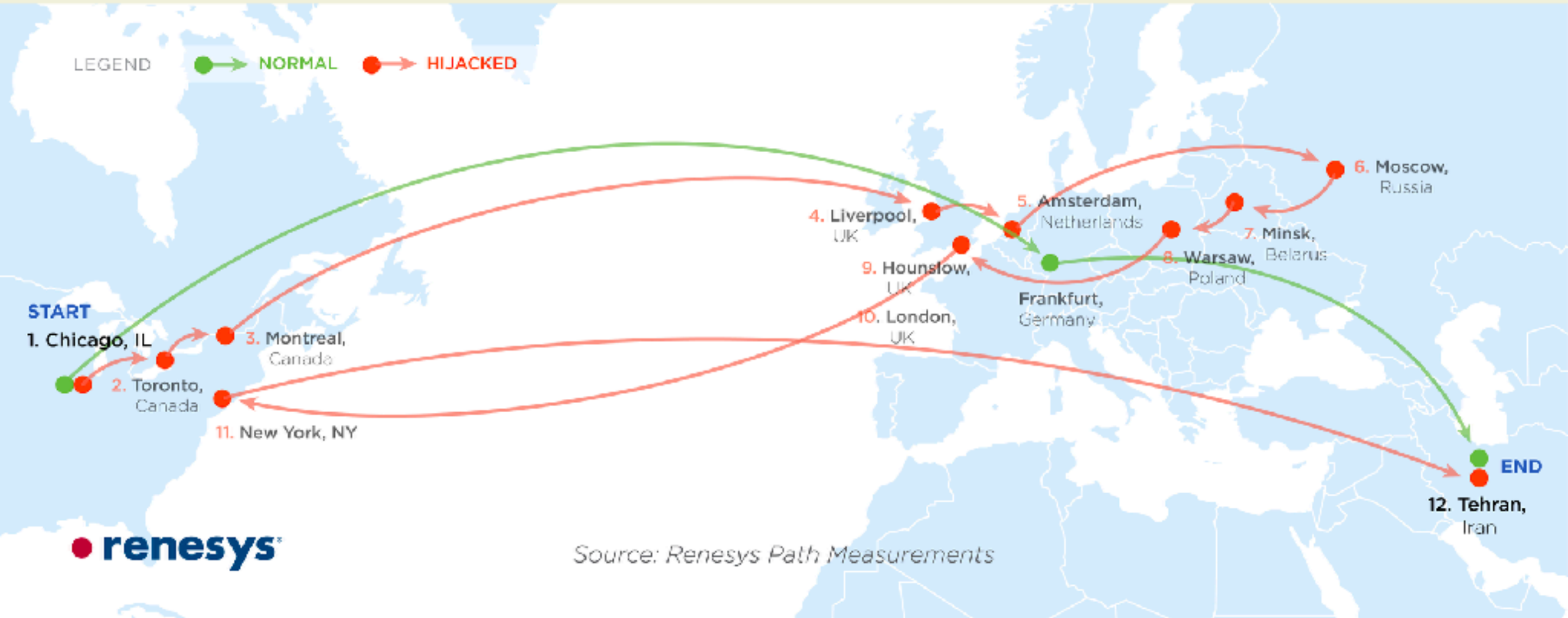
Traceroute Path 3: from **New York**, NY to **Los Angeles**, CA via ***Belarus***



Guadalajara to Washington DC

Chicago to Tehran

Traceroute Path 4: from **Chicago**, IL to **Tehran**, Iran



Frankfurt to Fremont

Traceroute Path 5: from **Frankfurt**, Germany to **Fremont**, CA via ***Iceland***

Proposals

- Secure BGP (S-BGP)
- Secure Origin BGP (soBGP)
- Interdomain Route Validation (IRV)
- …

S-BGP

- Introduces public-key infrastructure (PKI)
- Address allocation hierarchy is authenticated
- Certificates are used to authenticate AS
  - Address attestation proves that AS can originate an address
  - Route attestation proves what ASes are on the path

S-BGP

- Infrastructure
  - Network Operation Center (NOC)
  - Regional Registry (e.g., APNIC)
  - Repositories of certificates, revocations, and AAs
  - Routers

S-BGP

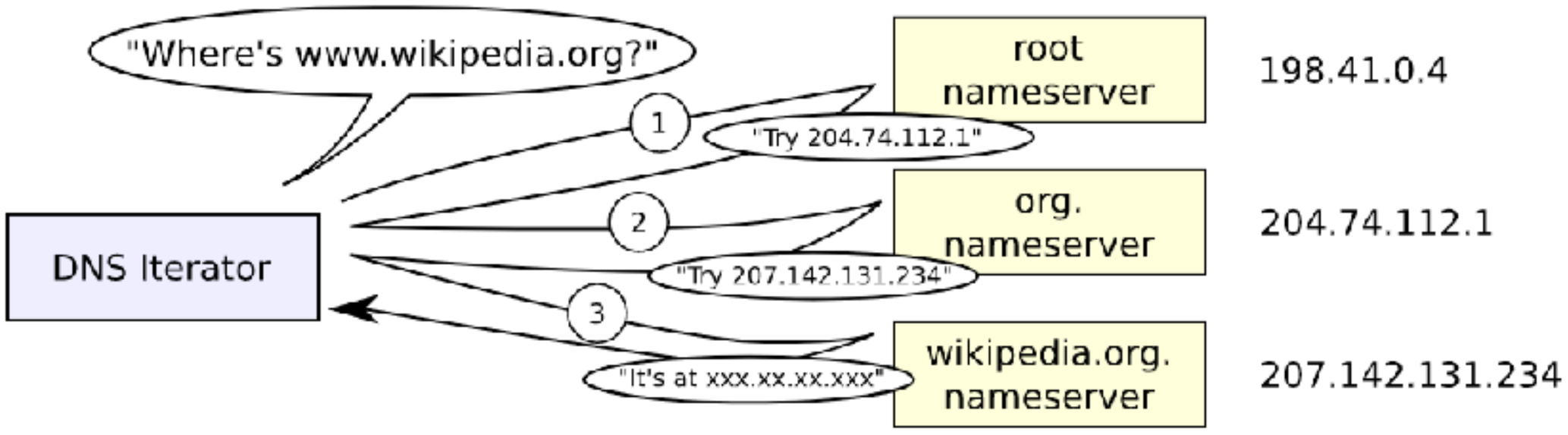
- Not widely deployed
  - Plain BGP still dominates
- Too complex for Ases
- CPU/mem/storage and SW/HW upgrades are necessary

Domain Name System (DNS)

- Hierarchical and decentralized naming systems
  - Name hierarchy with IANA as the root
- Public database with different resource records (RRs)
  - A, AAAA, TXT, PTR, …
- UDP used by default

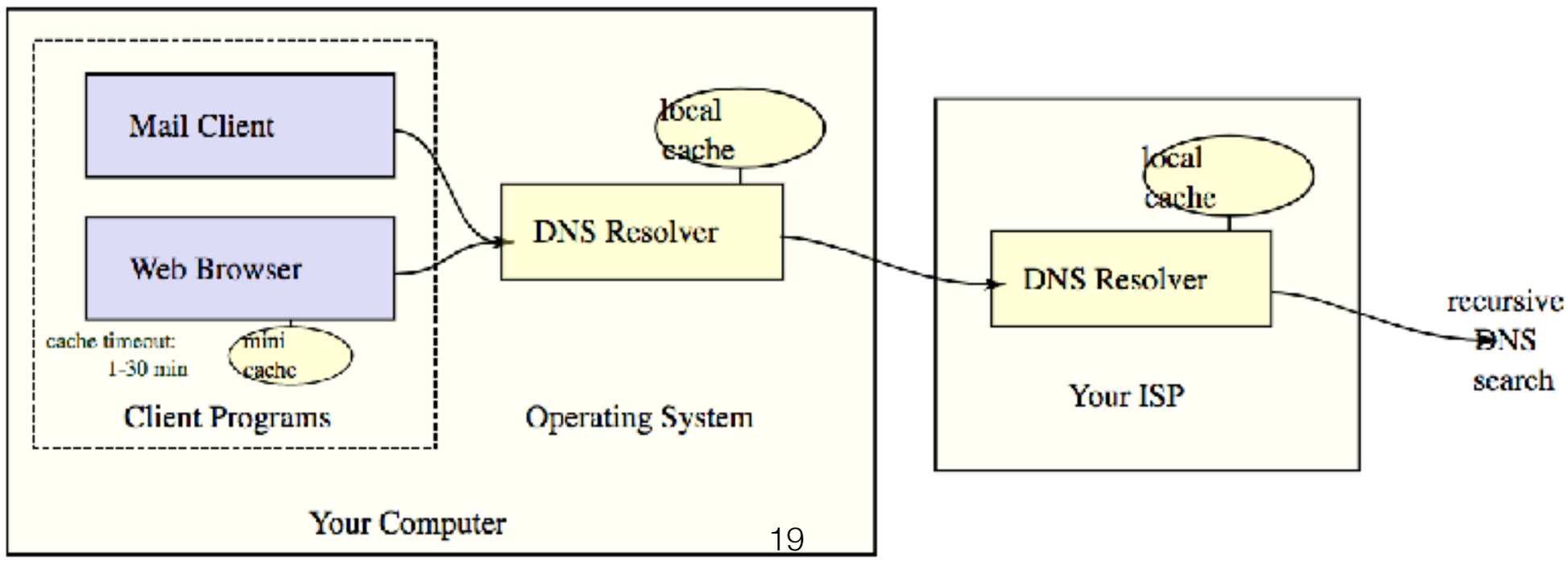
DNS resolution

- Domain zone
  - All DNS resources associated with the domain name
  - NXDOMAIN
- DNS resolvers, servers, clients, …
- Responses contain sections (e.g., Authority and Additional Section)



DNS Caching

- Results are cached
  - Efficiency reasons
- Cache is kept at many places



DNS Security

- DNS does not provide security properties
- On-path adversary
  - Can freely manipulate DNS responses
- Off-path adversary
  - Kaminsky DNS Vulnerability (2008)

Kaminsky's Attack

- Scenario
  - Adversary can query a remote (open) resolver
- Query format
  - IPs, ports, …
  - Query ID
    - Has to be unique to associate queries&responses
    - Implemented sequentially (as counter)

Kaminsky's Attack

- Idea
  - With predicted Query ID and source port the adversary *could inject* a malicious DNS response
- Ports are usually random (need brute-force) but Query IDs are sequential. How to predict them?
  - The adversary can use the resolver to resolve own domain name

Kaminsky's Attack

- With the Query ID predicted the adversary can flood the resolver with responses (try to brute-force the port)
- Many variants of the attack
  - Target given response (knowing that a given domain will be queried)
  - Ask for a non-cached result and inject NS response

Prevention

- Randomization of the Query ID field

- More comprehensive protection against DNS attack

DNS Security Extension (DNSSEC)

- Introduces PKI
  - Basing on namespace hierarchy
- Provides authentication for resource records

DNSSEC

- New RRs
  - RRSING: contains a signature for another RR
  - DNSKEY: stores a public key
  - DS: hash of a domain owner name and DNSKEY record

DNSSEC

- Not widely deployed
  - Complex management, operation, overhead, …
  - Can cause “problems”
- Increases amplification factor (when used via UDP)
- Difficult to modify/extend/patch
- Authenticating negative info (NXDOMAIN)

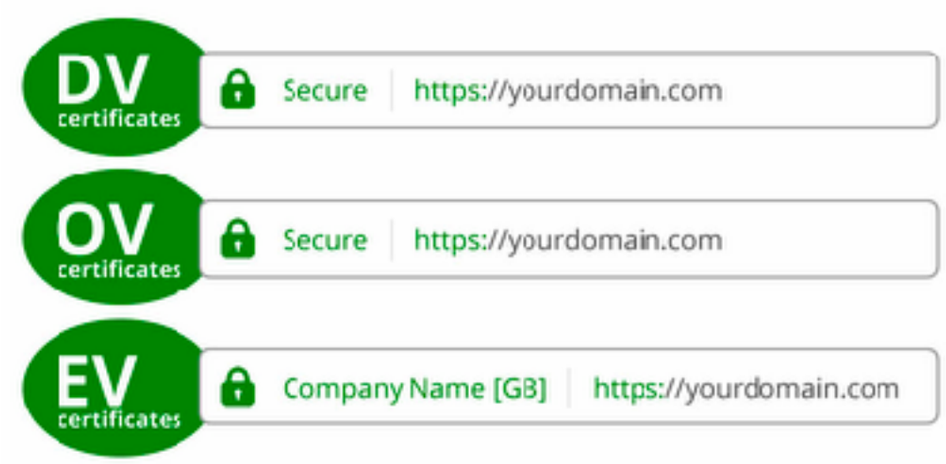
Why no one is concerned about that?

Transport Layer Security (TLS)

- End-entity PKI
  - Entities are usually identified by domain names
- Orthogonal to DNSSEC
- Certification Authorities (CAs) are trusted entities
  - (Too) many root and intermediate CAs

TLS Certificates

- Domain-Validated (DV) Certificates
  - Proving ownership over domain name
    - Email, HTTP, or DNS
- Organization-Validated (OV) Certificates
  - Domain ownership + checking organization
- Extended-Validated (EV) Certificates
  - Domain ownership + checking organization + F2F meeting

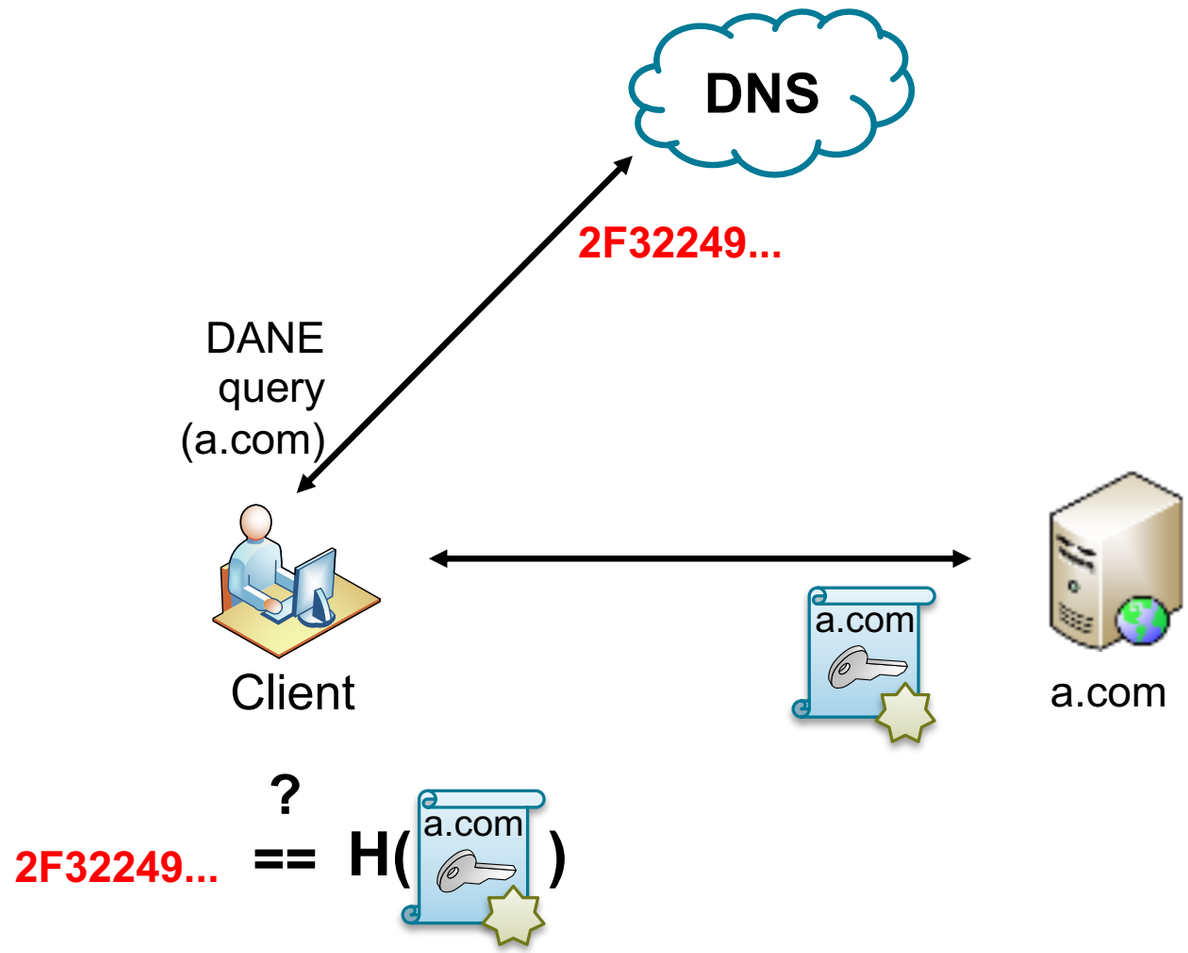


TLS

- Widely deployed
  - The Let’s Encrypt project issues free certificates
- Downgrading attacks
  - SSL/TLS stripping
- Impersonation attacks
  - Attacked CAs: DigiNotar, Comodo, …
- DNS-based PKI enhancements
  - DNS-based Authentication of Named Entities (DANE)
  - Certification Authority Authorization (CAA)

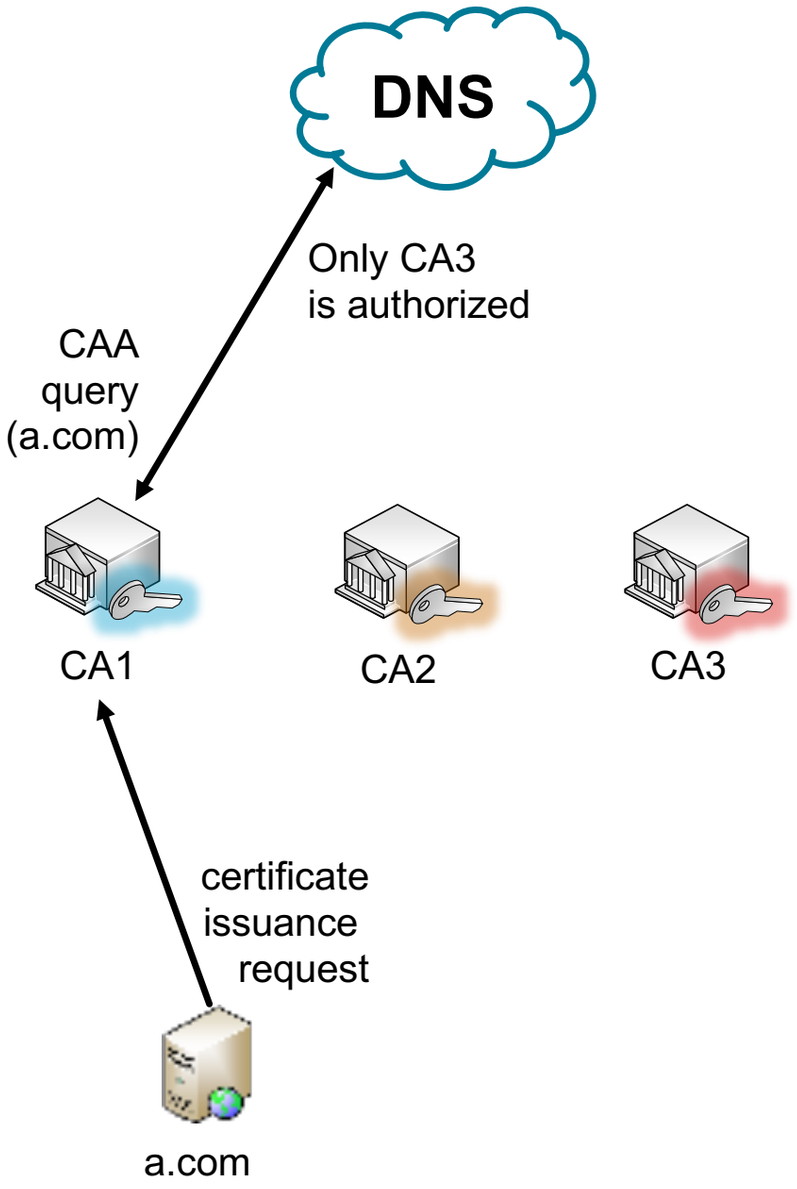
DANE

- Domains can specify keys they trust
  - Their keys
  - CAs' keys
- Requires DNSSEC



CAA

- Trust agility
  - Allows to list trusted CAs
- DNSSEC recommended
- Mandatory from Sep 2017



Questions?