Security Against Off-Path Attackers

- **Before Kaminsky's attack (2008)**
- **Challenge-Response Defenses**
  - **Same question section as in request**
  - **Same (random 16-bit) ID field**
  - **Response received within reasonable delay**
    - **Ignore if already received valid response for this query**
- **High TTL**

Idea: High TTL

- Response is cached for TTL time interval
  - Further requests responded from cache
  - Can not repeat the attack until record expires from cache
- Idea: make cache-poisoning impractical by increasing TTL
- ***Is this secure?...***

Kaminsky's Observation:

- The bad guy does not have to wait to repeat the attack
  - ask for: 1.bank.com, 2.bank.com, …
  - Each query is different , so each triggers a request
    - TTL ***prevents*** repeated requests for same query
  - Since each query is different, each triggers a request
- Eventually the attacker hits the TXID for i.bank.com and poisoning succeeds
- But, what is poisoned?

Using Kaminsky's Observation

- Option 1: 123.bank.com is at 6.6.6.6
  - Not very useful…
  - Although, may foil some SOP mechanisms (e.g., cookies)!
- Option 2: go ask ns.bank.com, it is at 6.6.6.6
  - ns.bank.com is the name server of bank.com…
  - If resolver caches ns.bank.com at 6.6.6.6 attacker hijacks entire domain of bank.com
  - Main idea of Kaminsky's attack (2008)

BlackHat 2008: Kaminsky's Attack

1st idea: cause request - to random, non-existent domain

How? Open resolver / link in page / mail / …

2nd idea: poison by NS or glue records

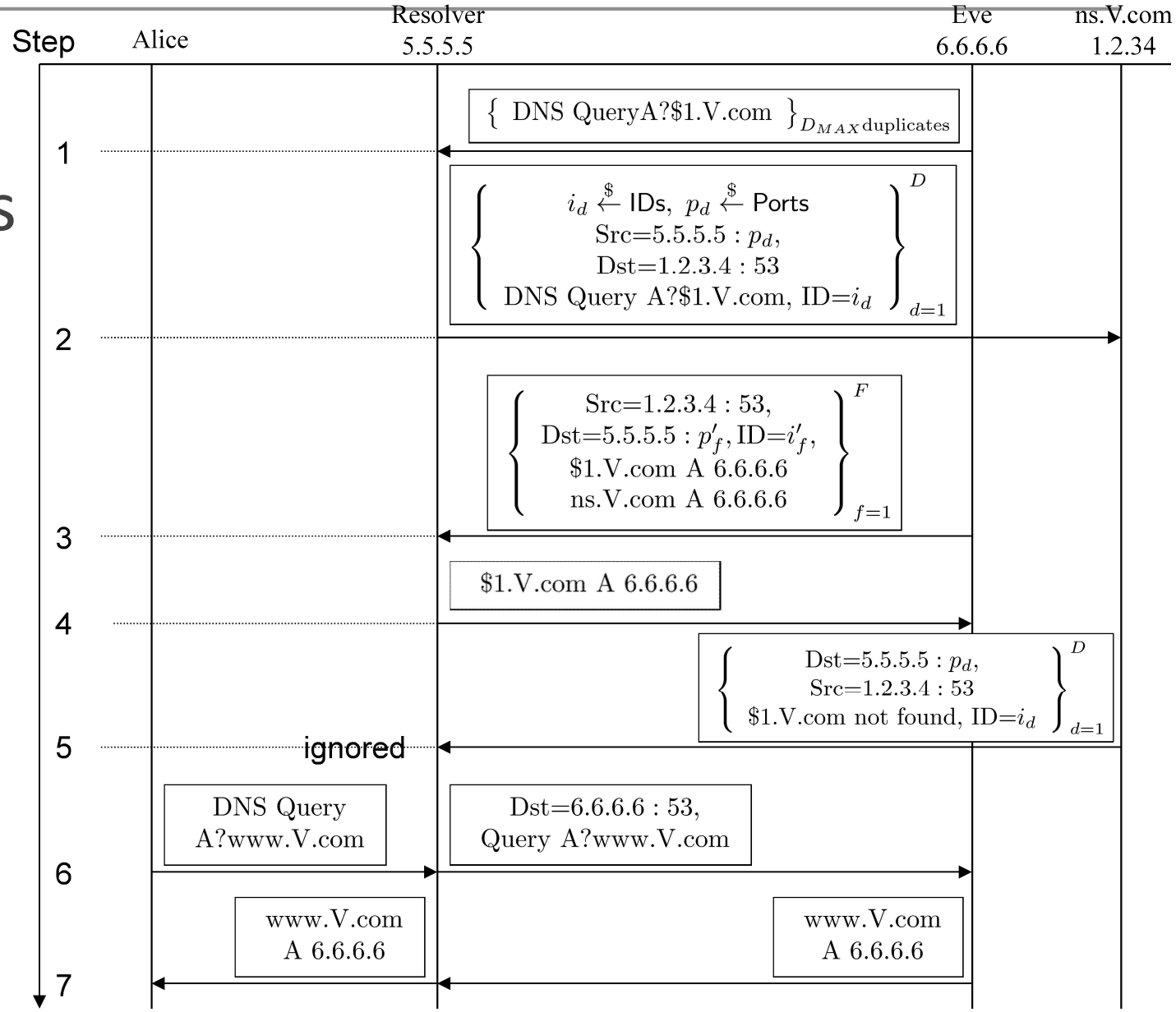
Resolver sends `regular' query, to <rnd>.victim.com

Attacker sends spoofed responses, **redirecting:**

victim.com NS eve.com **OR** ns.victim.org A 6.6.6.6

3rd idea: *D* duplicate requests ➔ Birthday paradox

Kaminsky's Attack [Black--Hat08]



Post-Kaminsky Challenge-Response Defenses

- **Previous: question, (16-bit) TX-ID field**
- **Plus, RFC 5452:**
  - **Prevent dup-queries (birthday)**
  - **Dest IP address and port from request**
    - **Chosen randomly; preferably: pool of IPs**
  - **Same IP address of responding DNS server**
    - **Most domains have 2-3 likely-to-be-used servers**
  - **Response received within reasonable delay**
    - **Ignore if already received valid response for this query**
- **0x20: DNS query randomization** (cApitaLIZatIoN)

Post-Kaminsky Challenge-Response **Attacks**

- **Port prediction**
  - **Resolver-behind-NAT [HS12]**
  - **Proxy and Forwarding Resolvers setup [HS13a]**
  - **Port-overloading [HS13b]**
- **Response modification with fragmentation [HS13c]**