OFF-PATH ATTACKS AGAINST PUBLIC KEY INFRASTRUCTURES

Markus Brandt, Tianxiang Dai, Elias Heftrig, Amit Klein, Haya Shulman, Michael Waidner

AGENDA

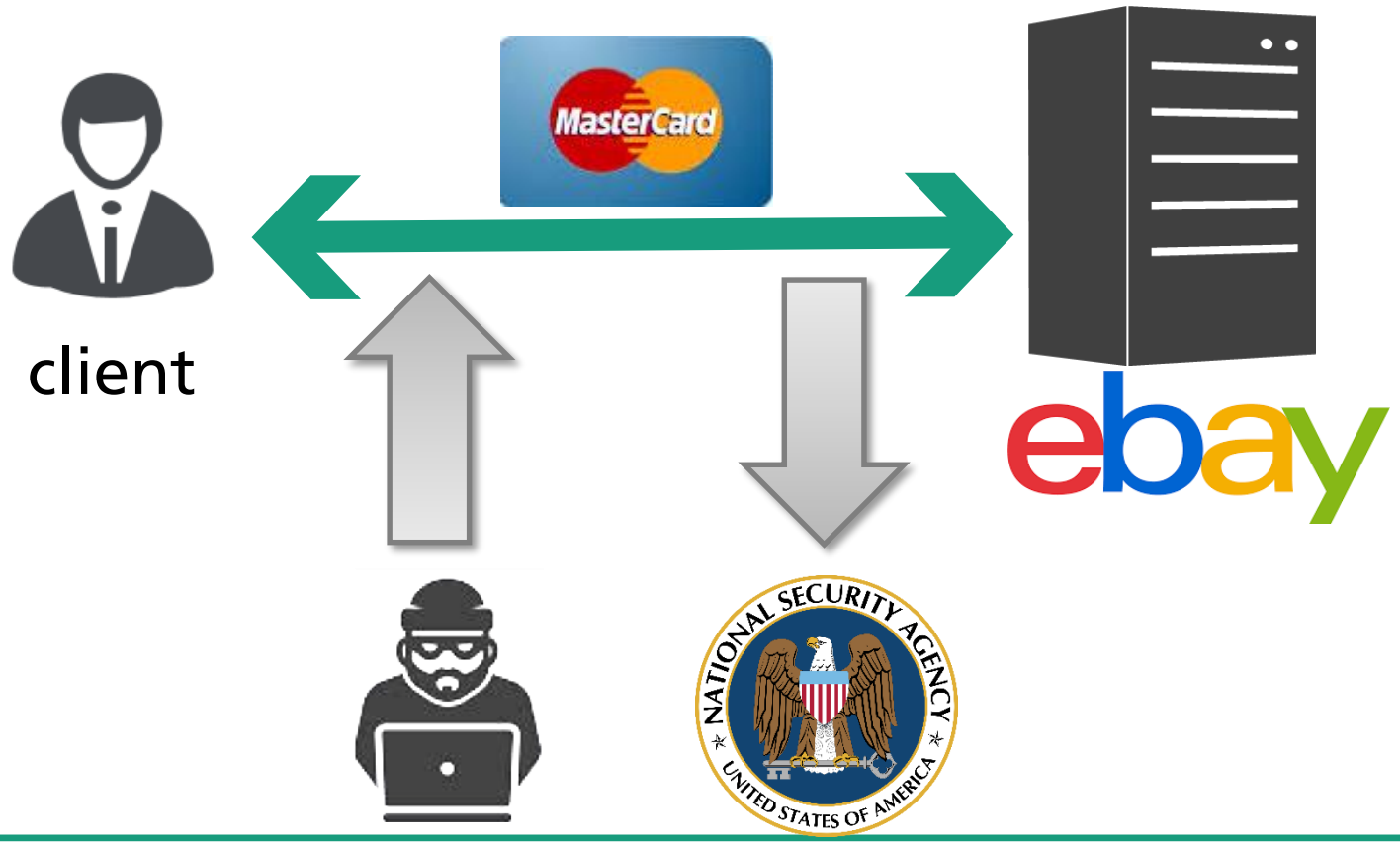
- Objectives
- Attacking
- Impact
- Mitigation
- Summary

AGENDA

- Objectives
- Attacking
- Impact
- Mitigation
- Summary

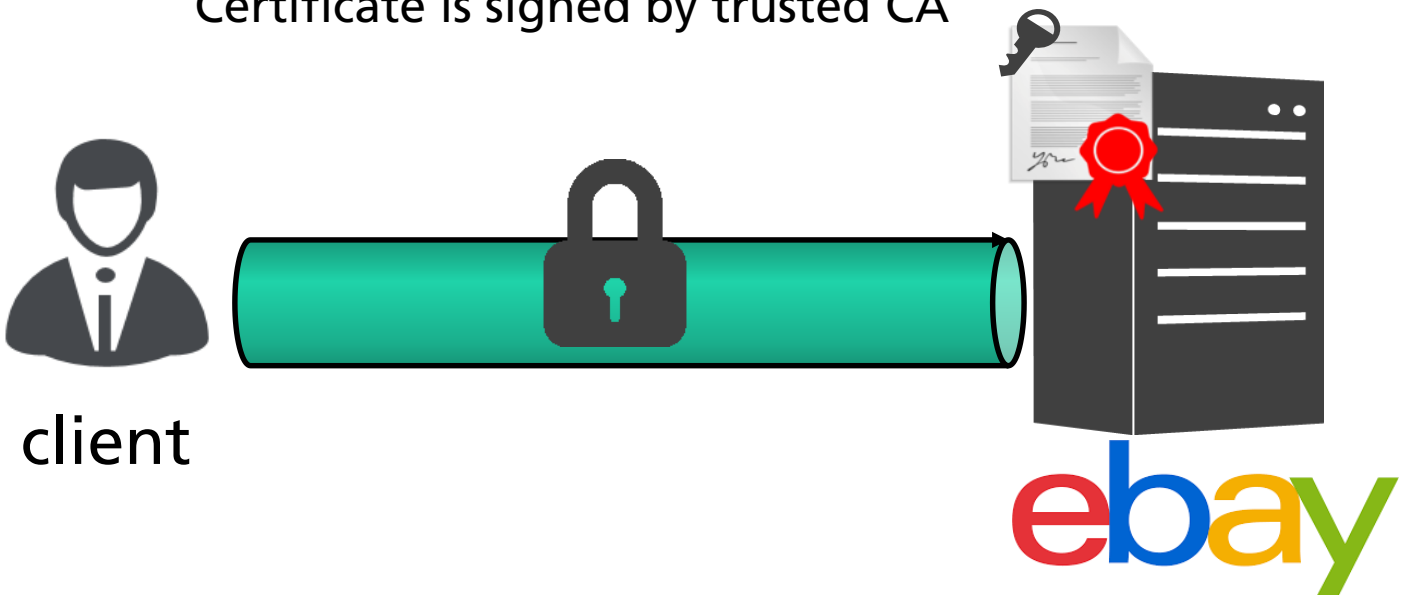
WEB PKI – WHAT IS IT GOOD FOR?

WEB PKI
UNSECURED COMMUNICATION

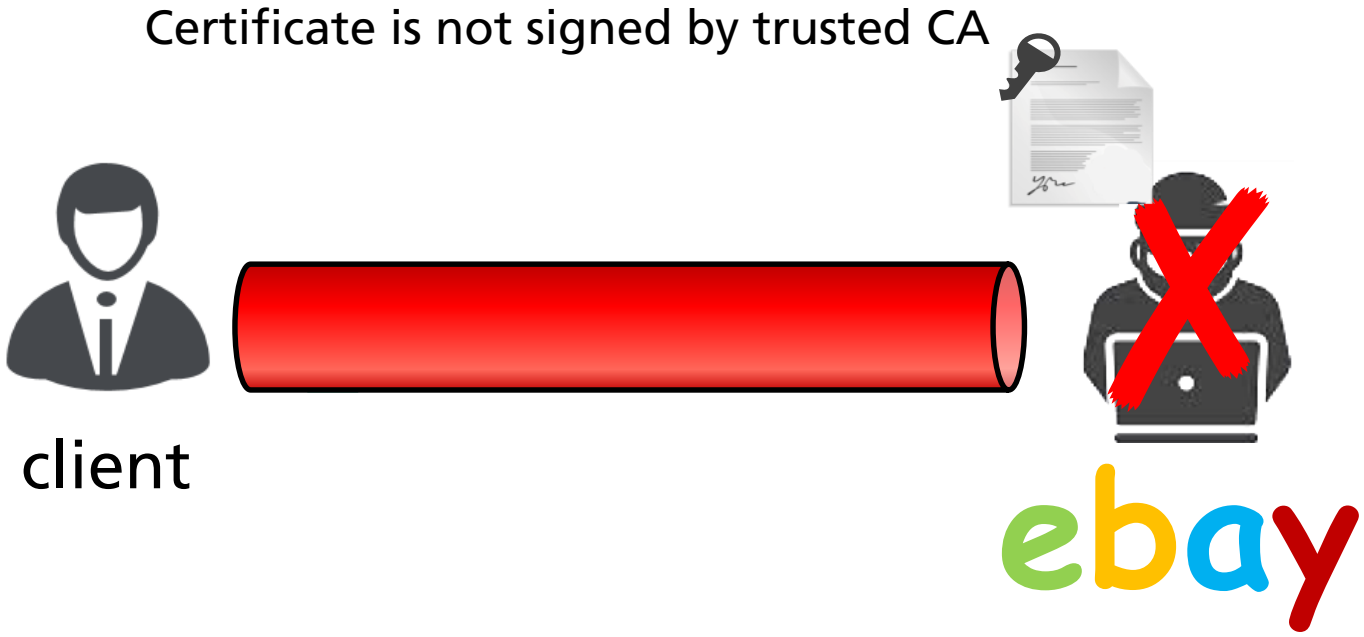


WEB PKI
SECURED COMMUNICATION

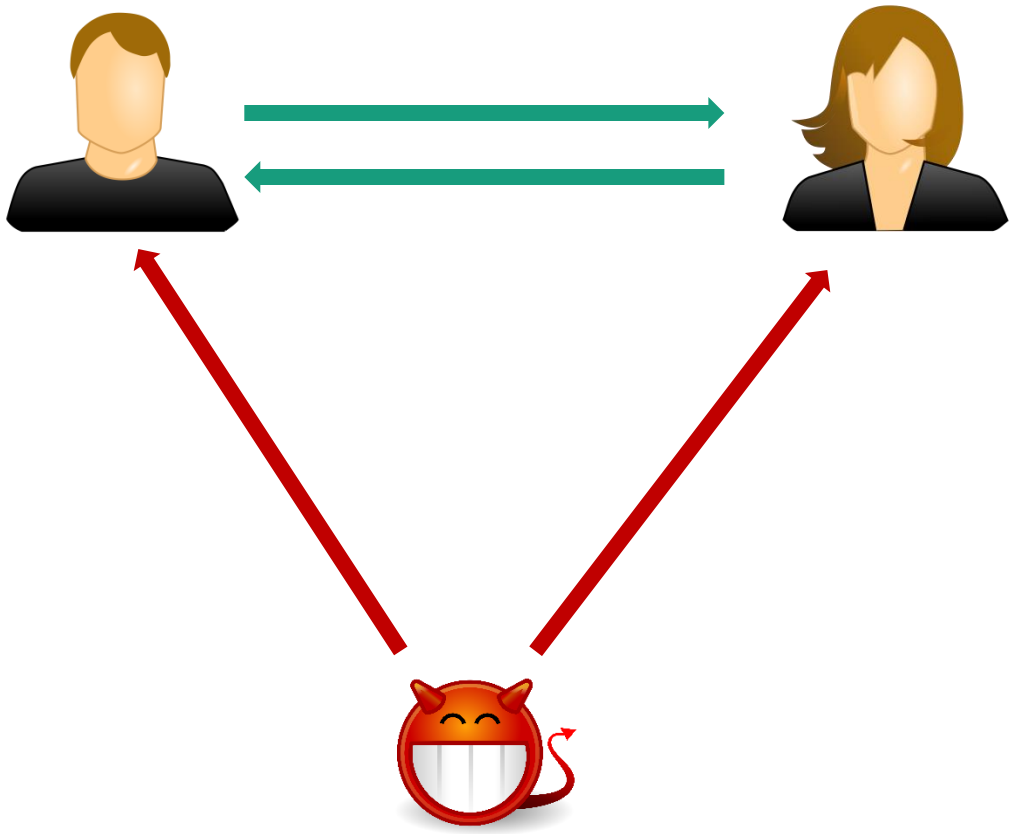
Certificate is signed by trusted CA



WEB PKI
SECURE AGAINST SPOOFING

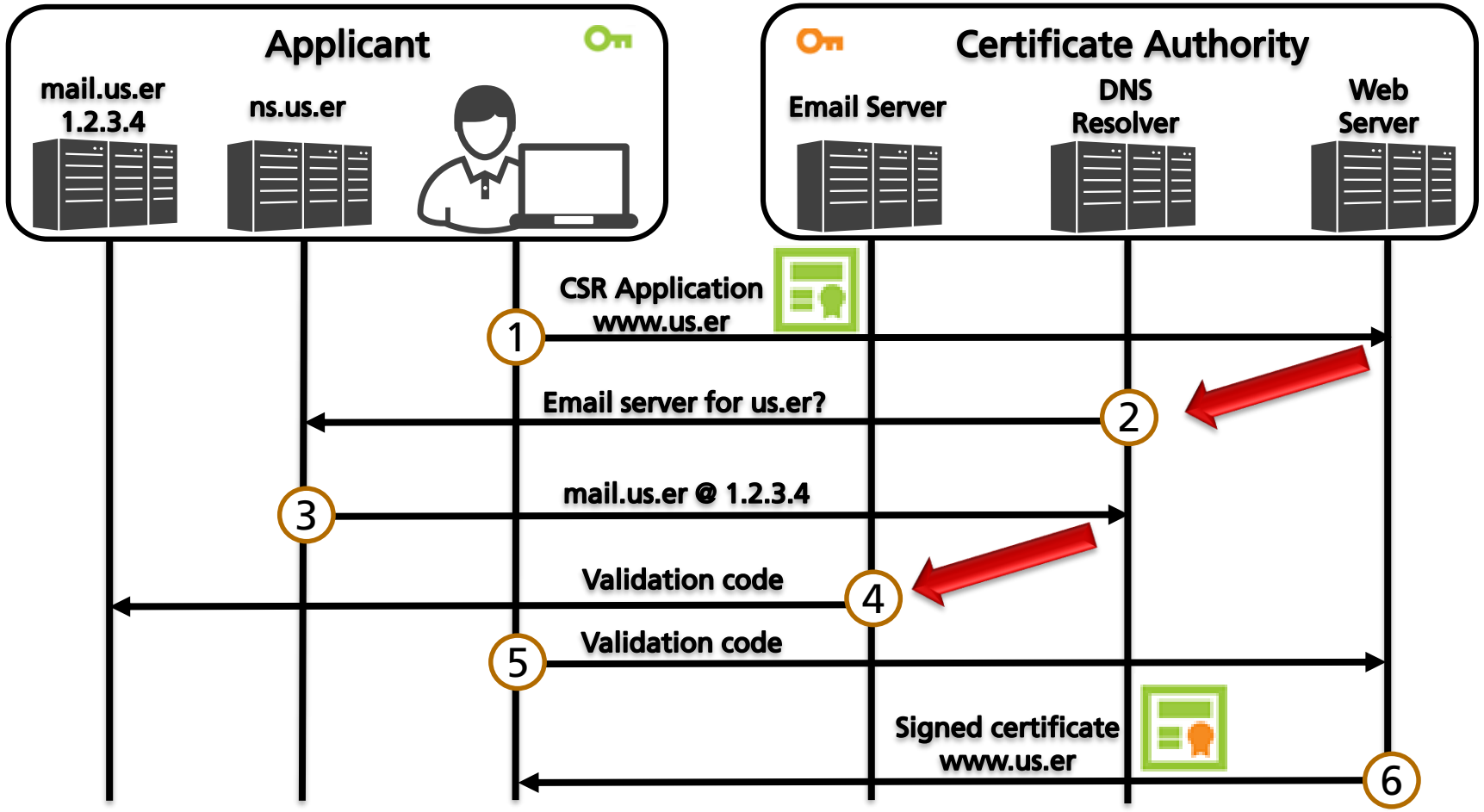


ATTACKER MODEL



- Off-path attacker
  - cannot eavesdrop, block, delay or modify packets in any way
  - injects packets with spoofed sender address
- Means of Attack
  - leverage IP defragmentation cache poisoning
  - to achieve DNS cache poisoning
  - for exploiting Domain Validation

CERTIFICATE ISSUANCE WITH DOMAIN VALIDATION

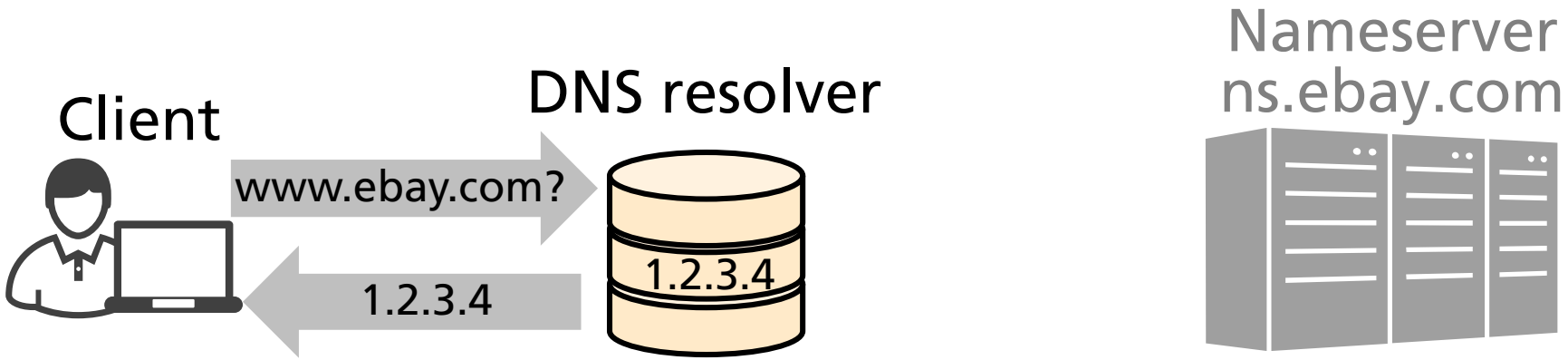


DNS - QUERIES

The yellow pages of the Internet

DNS - QUERIES

If cached the resolver will reply with the cached answer



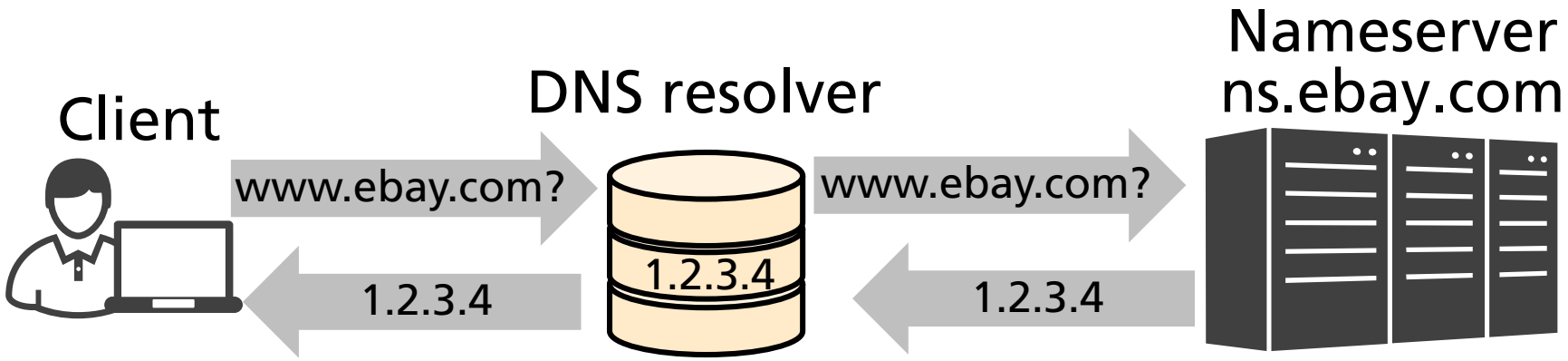
DNS - QUERIES

If not cached the resolver will recursively lookup the answer

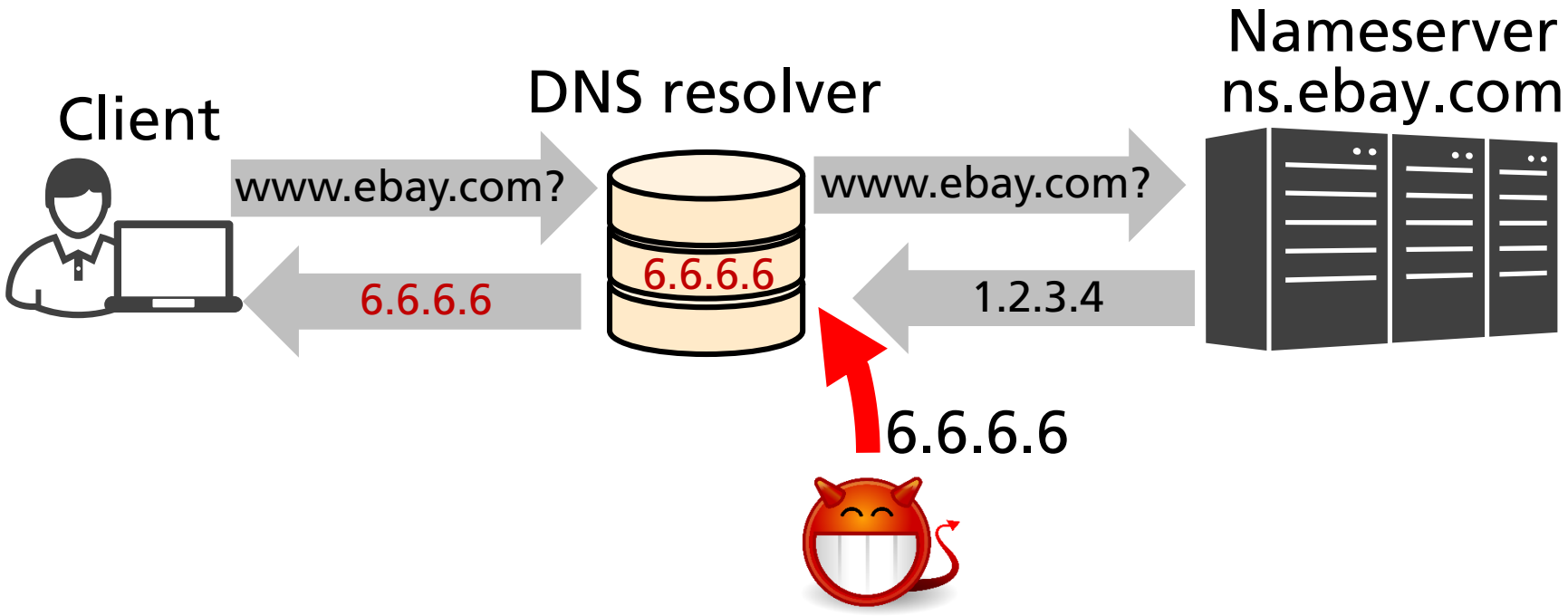
DNS - QUERIES


Client
DNS resolver
Nameserver
ns.ebay.com
www.ebay.com?
www.ebay.com?
1.2.3.4

DNS - QUERIES

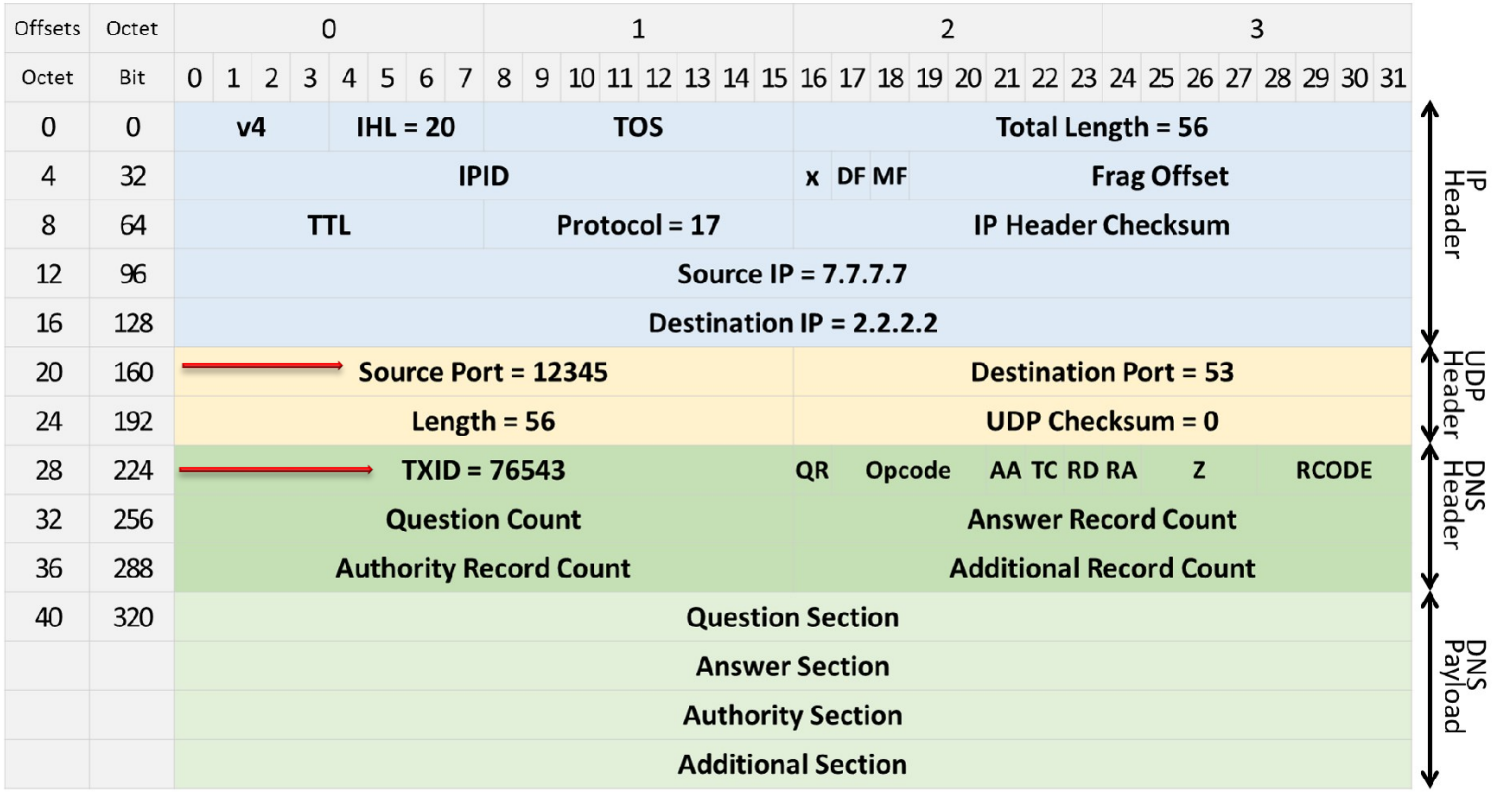

Client
DNS resolver
Nameserver
ns.ebay.com
www.ebay.com?
www.ebay.com?
1.2.3.4
1.2.3.4
1.2.3.4

DNS – CACHE POISONING

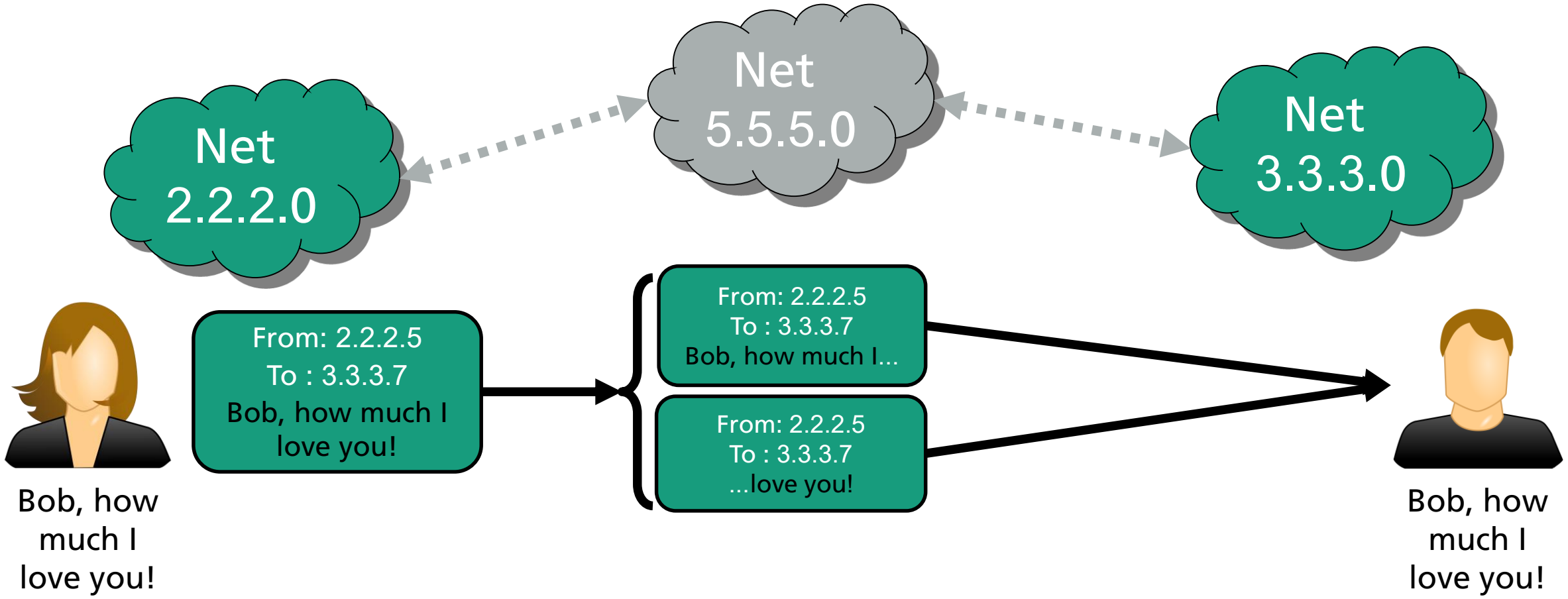


DNS – CHALLENGE RESPONSE SECURITY

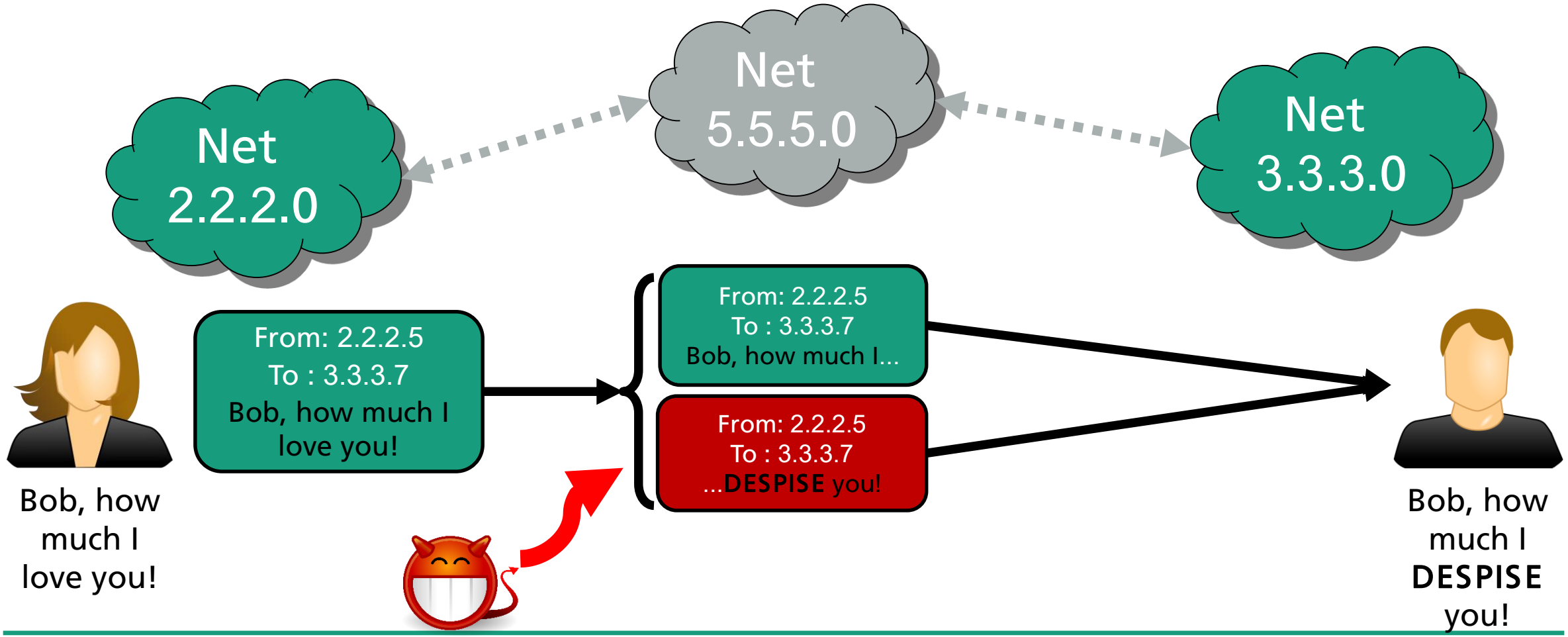
- Prevention mechanisms against off-path attacks
  - UDP source port randomization
  - TXID randomization
  - 32 random bits
- Here: impractical to guess
- Do fragmentation attack instead



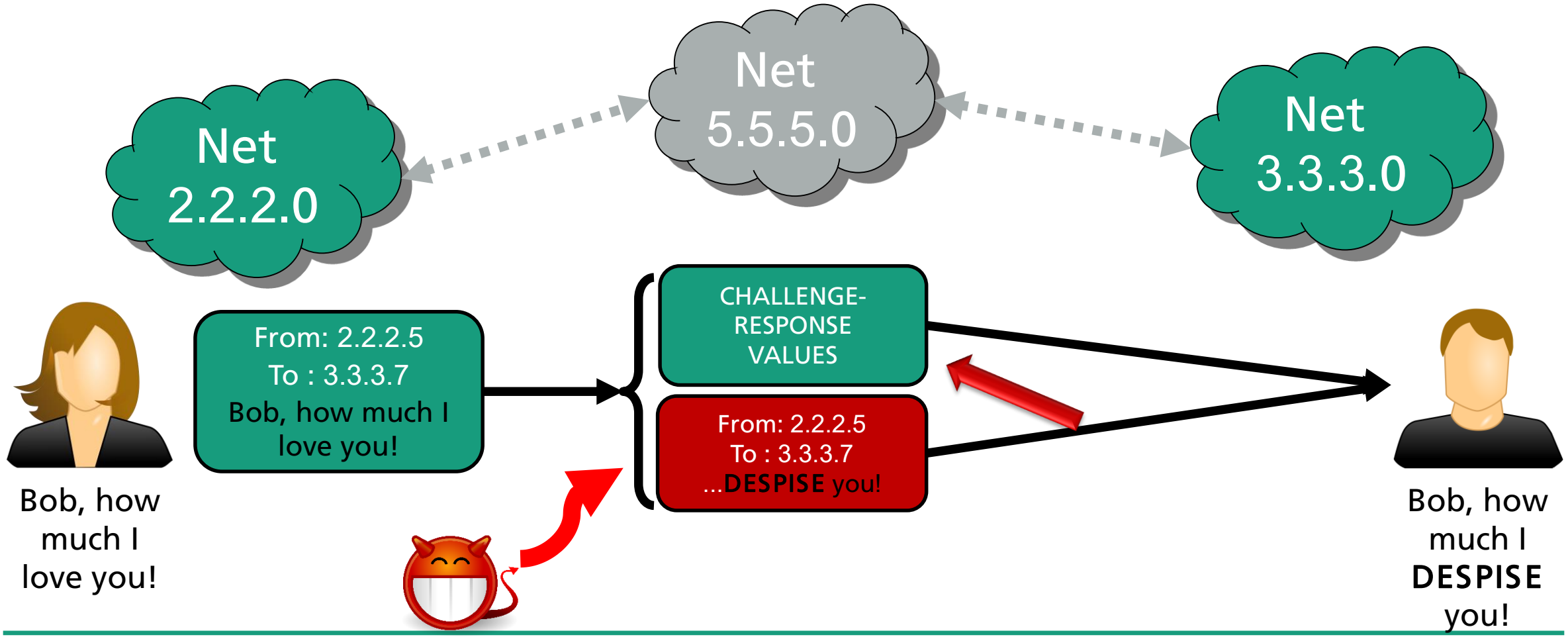
IP FRAGMENTATION



IP DEFRAGMENTATION CACHE POISONING



BYPASSING DNS OFF-PATH SECURITY MECHANISMS



BYPASSING DNS OFF-PATH SECURITY MECHANISMS
FIRST FRAGMENT OF RESPONSE

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	v4				IHL = 20				TOS								Total Length = 85															
4	32	IPID = 23456																x	DF	MF	Frag Offset = 0											
8	64	TTL								Protocol = 17								IP Header Checksum															
12	96	Source IP = 2.2.2.2																															
16	128	Destination IP = 7.7.7.7																															
20	160	Source Port = 53																Destination Port = 12345															
24	192	Length = 65																UDP Checksum = 0x14de															
28	224	TXID = 76543																QR	Opcode = 0			AA	TC	RD	RA	Z				RCODE = 0			
32	256	Question Count = 1																Answer Record Count = 1															
36	288	Authority Record Count = 0																Additional Record Count = 1															
40	320	4								m								a								i							
44	352	l								4								v								i							
48	384	c								t								2								i							
52	416	m								0								Type = A															
56	448	Class = IN																Name (Pointer)															
60	480	Type = A																Class = IN															
64	512	TTL																															

IP Header

UDP Header

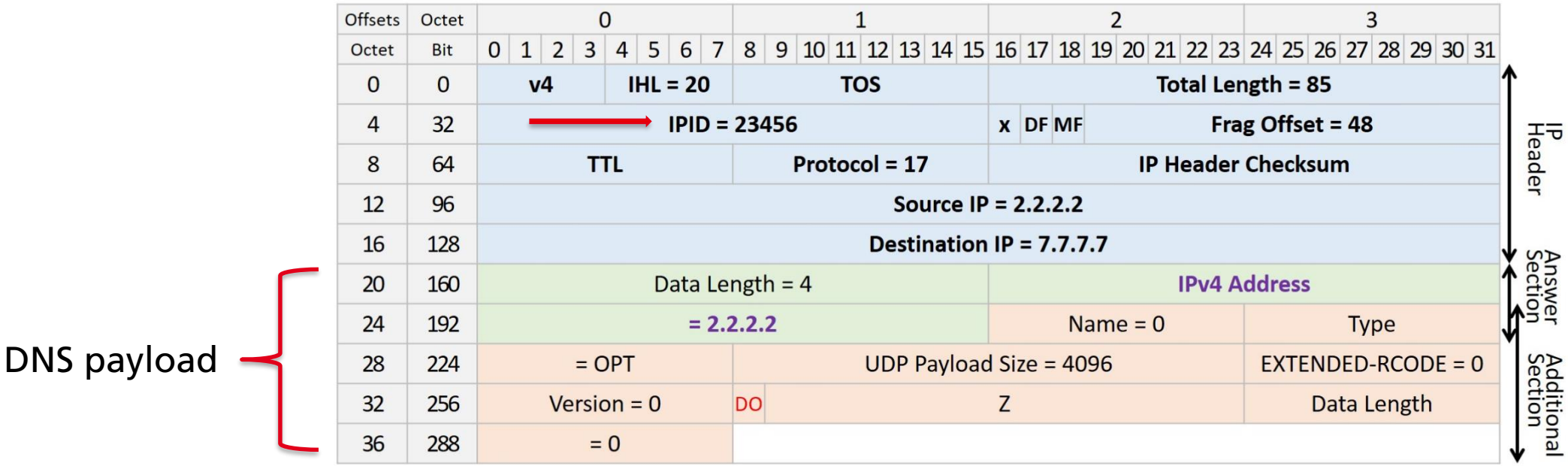
DNS Header

Question Section

Answer Section

- Contains response to the challenge
- and parts of the DNS response
- Challenges
  - Guessing IPID
  - Matching UDP checksum

BYPASSING DNS OFF-PATH SECURITY MECHANISMS SECOND FRAGMENT OF RESPONSE



Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	v4				IHL = 20				TOS								Total Length = 85															
4	32	IPID = 23456																x	DF	MF	Frag Offset = 48											
8	64	TTL								Protocol = 17								IP Header Checksum															
12	96	Source IP = 2.2.2.2																															
16	128	Destination IP = 7.7.7.7																															
20	160	Data Length = 4																IPv4 Address															
24	192	= 2.2.2.2																Name = 0								Type							
28	224	= OPT								UDP Payload Size = 4096																EXTENDED-RCODE = 0							
32	256	Version = 0								DO	Z															Data Length							
36	288	= 0																															

- UDP checksum can be matched using true fragment
- IPID usually is guessable counter

CAUSING FRAGMENTATION WITH ICMP

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	v4				IHL = 20				TOS								Total Length = 56															
4	32	IPID																x	DF	MF	Frag Offset											
8	64	TTL								Protocol = 1								IP Header Checksum															
12	96	Source IP = 6.6.6.6																															
16	128	Destination IP = 2.2.2.2																															
20	160	Type = 3								Code = 4								ICMP Checksum															
24	192	Unused																MTU = 100															
28	224	v4				IHL = 20				TOS								Total Length = 76															
32	256	IPID																x	DF	MF	Frag Offset											
36	288	TTL								Protocol = 17								IP Header Checksum															
40	320	Source IP = 2.2.2.2																															
44	352	Destination IP = 7.7.7.7																															
48	384	Source Port = 53																Destination Port = 12345															
52	416	Length = 56																UDP Checksum = 0															

IP Header

ICMP Header

IP Header

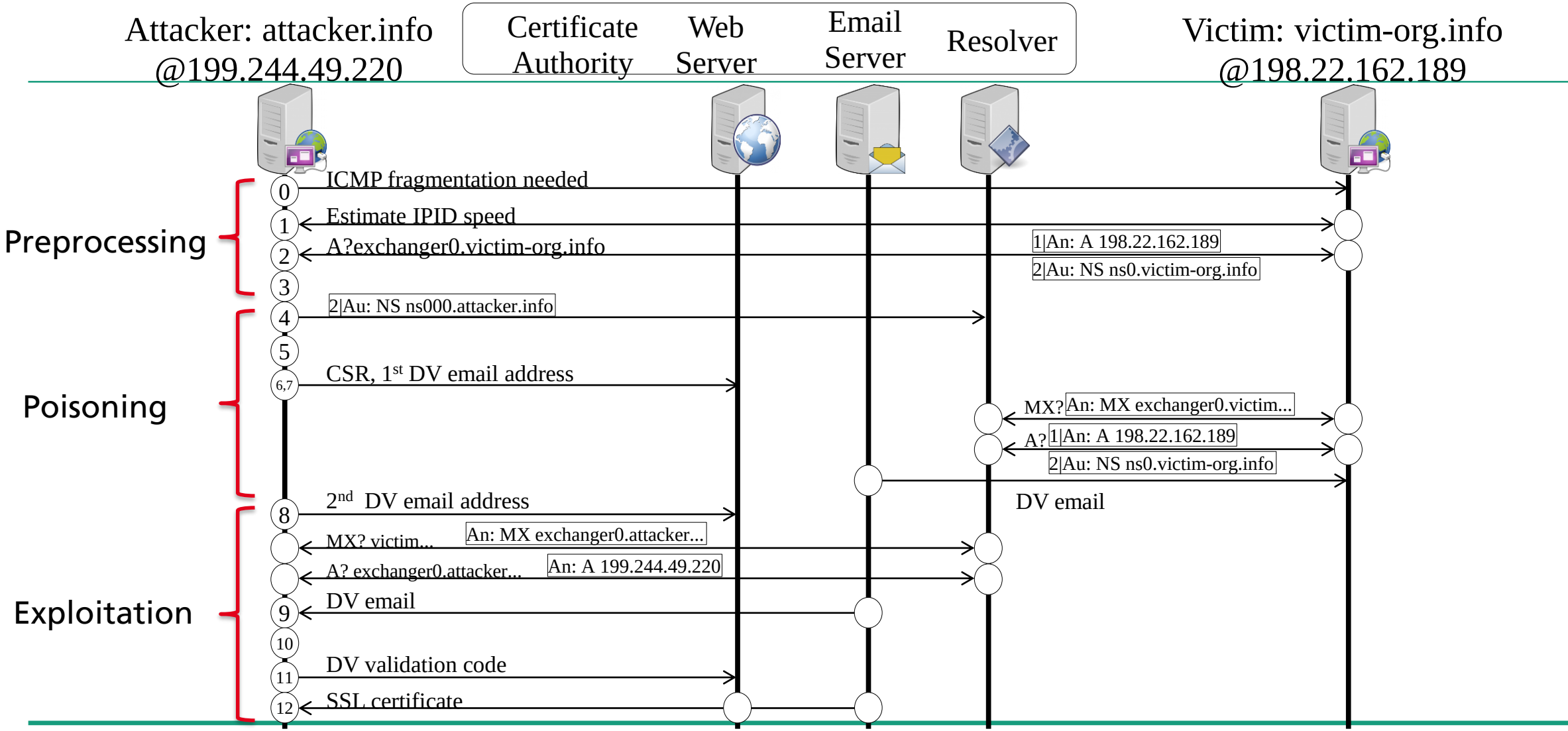
UDP Header

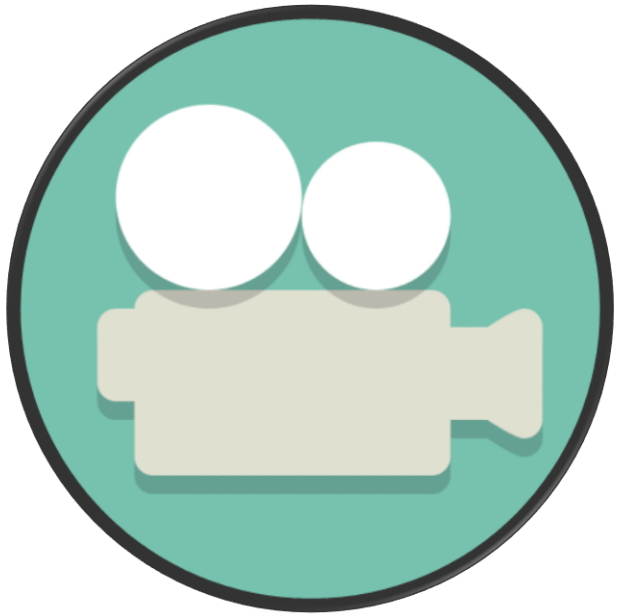
- Type=3
  - "Destination unreachable"
- Code=4
  - "Fragmentation needed and DF set"

AGENDA

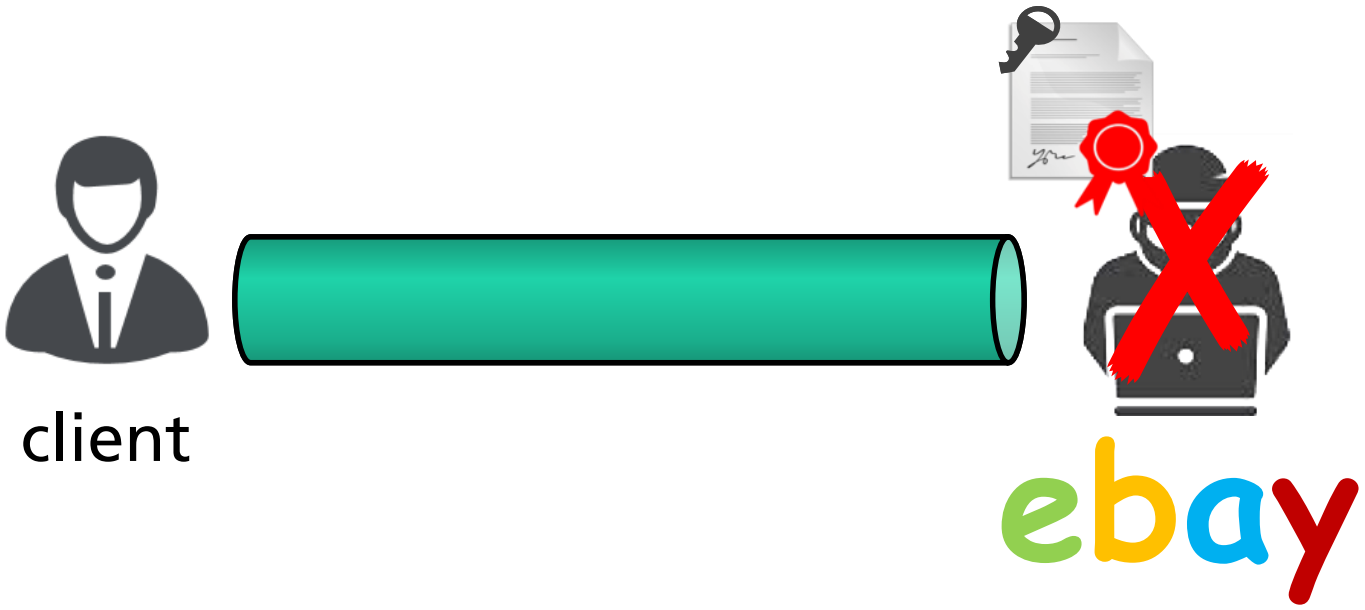
- Objectives
- ➢ Attacking
- Impact
- Mitigation
- Summary

ATTACKER ISSUES FRAUDULENT CERTIFICATE





USING IT



Our certificate is signed by a trusted CA.

AGENDA

- Objectives
- Attacking
- Impact
- Mitigation
- Summary

EFFECTS ON VICTIMS

- For victim users
  - Injected malware
  - Theft of credentials, sensitive data, identity, …
- Loss of reputation and trust
  - For victim CA
  - and target domain

VULNERABILITIES IN THE WILD

- We tested 17 CAs that perform Domain Validation
  - Covering > 95% of the certificate market
- Found 5 vulnerable
- Only one vulnerable CA is sufficient to obtain the target certificate
  - Usually it does not matter, which CA signed it

➢ Web PKI security is undermined

AGENDA

- Objectives
- Attacking
- Impact
- ➢ Mitigation
- Summary

PRECONDITIONS FOR THE ATTACK

- Domain Validation
  - Is offered in the first place
- IP fragmentation allowed
  - for victim name server of target domain
  - in CA network
- DNS via UDP

MITIGATION TECHNIQUES

- Disable Domain Validation?
  - Would leave us only with much more expensive alternatives
- Suppress IP Fragmentation?
  - Would disconnect some networks
- Force DNS over TCP?
  - Off-path TCP injection attacks do exist
  - Also: Short-lived BGP prefix hijacks for MITM DNS cache poisoning are on the rise

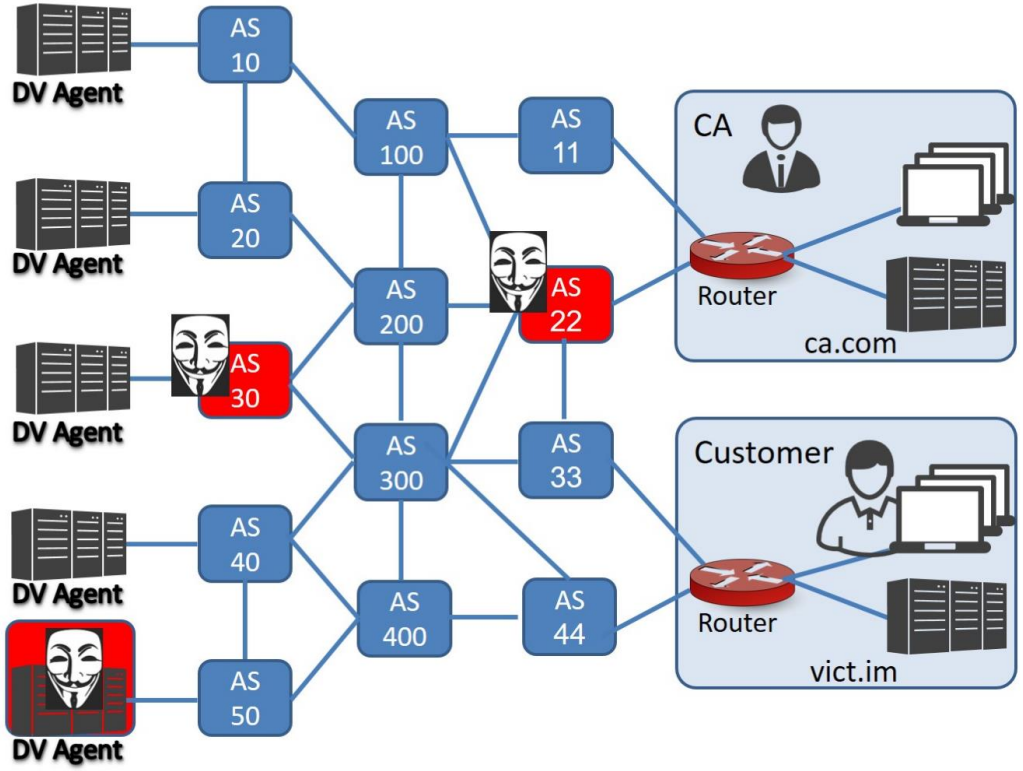
MITIGATION TECHNIQUES

- We need MITM resilient Domain Validation

- DoH / DoT?
  - Securing a PKI with the very same PKI?

- DNSSEC?
  - The way to go
  - But still not properly deployed since mid-90s!

DROP-IN REPLACEMENT DOMAIN VALIDATION++



- Uses orchestrator that evaluates voting from hardened DV agents
  - each performing the DNS part
- Communicates via HTTPS
  - Using out-of-pki certificates
- Over (mostly) non-overlapping paths through the internet

➢ For more details, visit pki.cad.sit.fraunhofer.de

AGENDA

- Objectives
- Attacking
- Impact
- Mitigation
- ➢ Summary

SUMMARY

- Off-path attack against Domain Validation
- Using DNS cache poisoning and IP defragmentation cache poisoning
- To acquire fraudulent certificates for domains under foreign operation

➢ Web PKI, which is meant to provide security against strong MITM attackers, relies on a weak building block that can be circumvented even by a weak off-path attacker.

FURTHER INFORMATION

pki.cad.sit.fraunhofer.de