How prevalent is the operation of DNS security mechanisms?

OARC 35a

Masanori Yajima(Waseda University), Daiki Chiba(NTT),

Yoshiro Yoneya(JPRS), Tatsuya Mori(Waseda University, NICT)

Introduction

- Various DNS security mechanisms have been proposed, standardized, and implemented
  - It is not clear how widespread these mechanisms are in the DNS ecosystem

- We conduct a large-scale measurement analysis of the major DNS security mechanisms
  - DNSSEC, DNS Cookies, CAA, SPF, DMARC, MTA-STS, DANE, and TLS-RPT

- We share the results of the measurement and want to get feedback

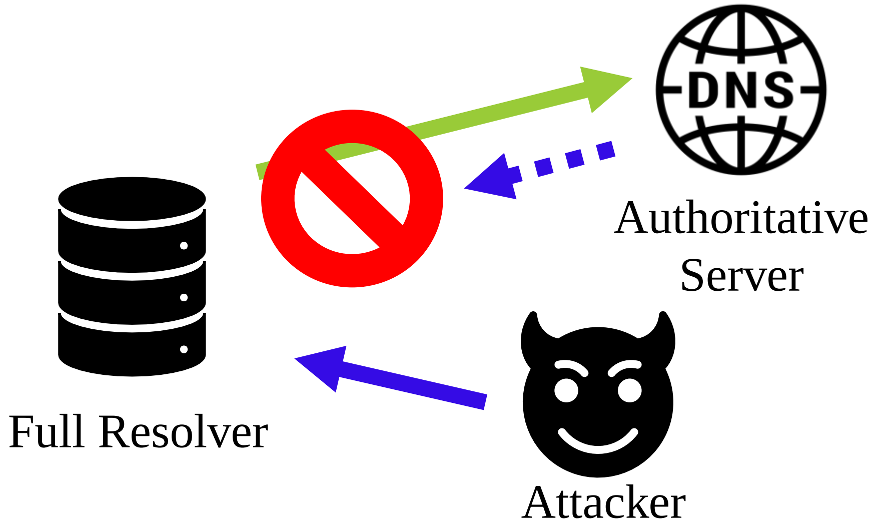
DNS security mechanisms

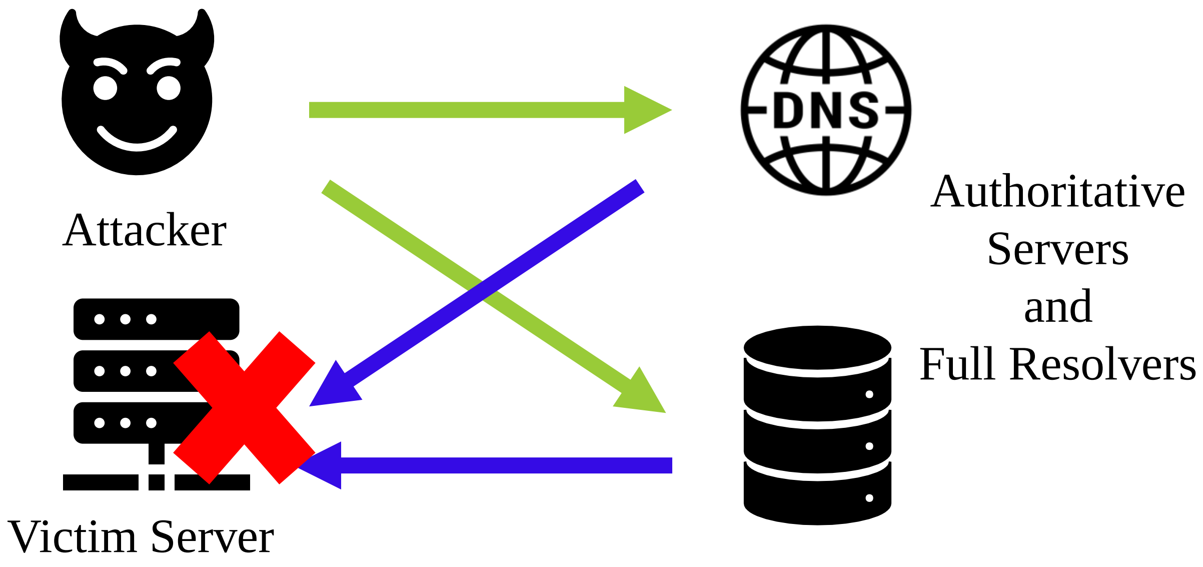
- Security threats targeting DNS can be broadly classified into the following three categories:
  - vulnerabilities of DNS communication
    (DNS cache poisoning attacks, DNS amplification attacks)
  - domain names
    (phishing sites and phishing emails, using spoofed domain names)
  - leakage of privacy information contained in the DNS queries/responses

DNS security mechanisms

- Vulnerabilities of DNS communication
  - (DNS cache poisoning attacks, DNS amplification attacks)

- DNSSEC, DNS Cookie

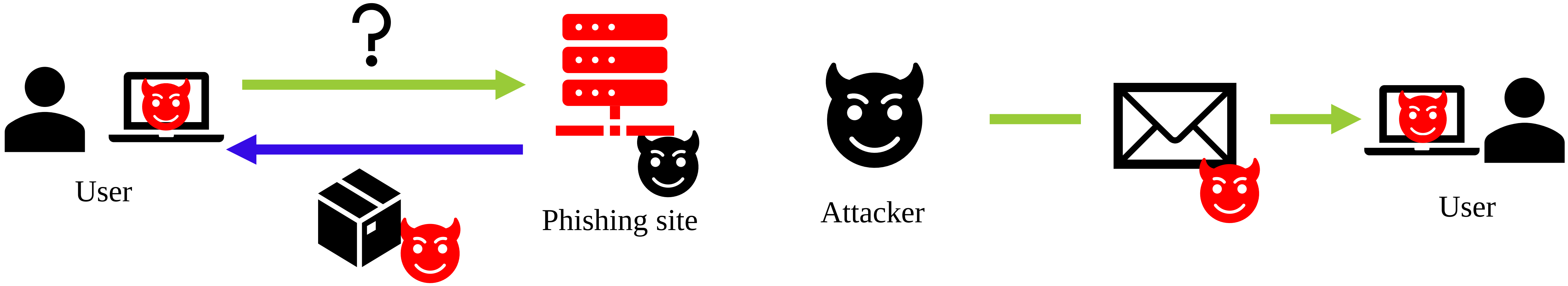




DNS security mechanisms

- Domain names
  - (phishing sites and phishing emails, using spoofed domain names)

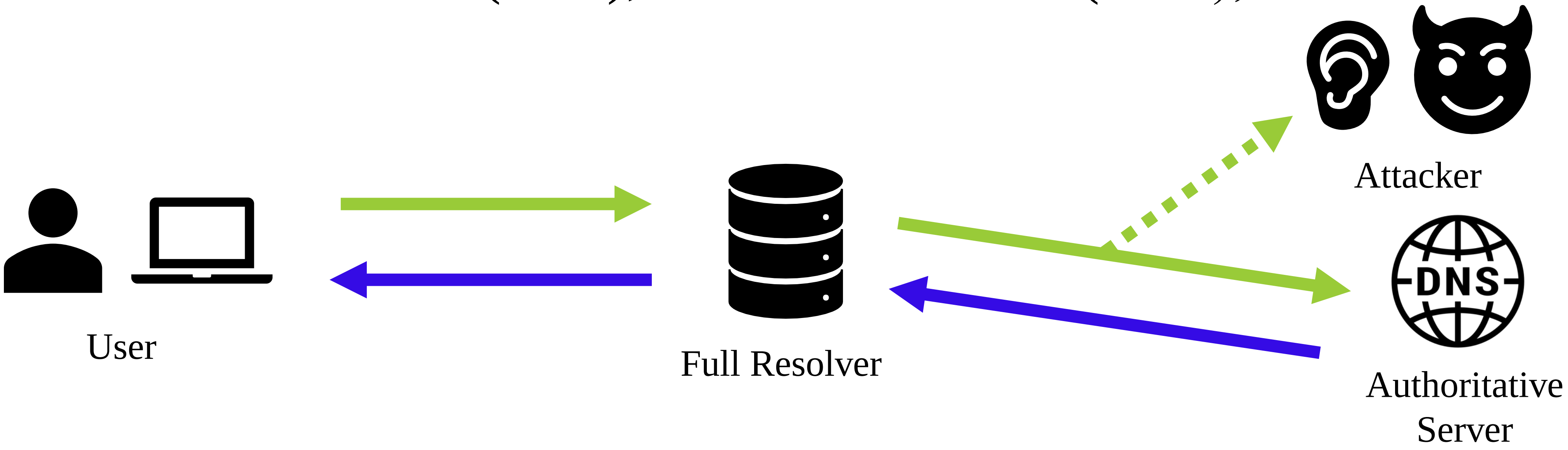
- CAA, SPF, DMARC, MTA-STS, DANE, TLSRPT



DNS security mechanisms

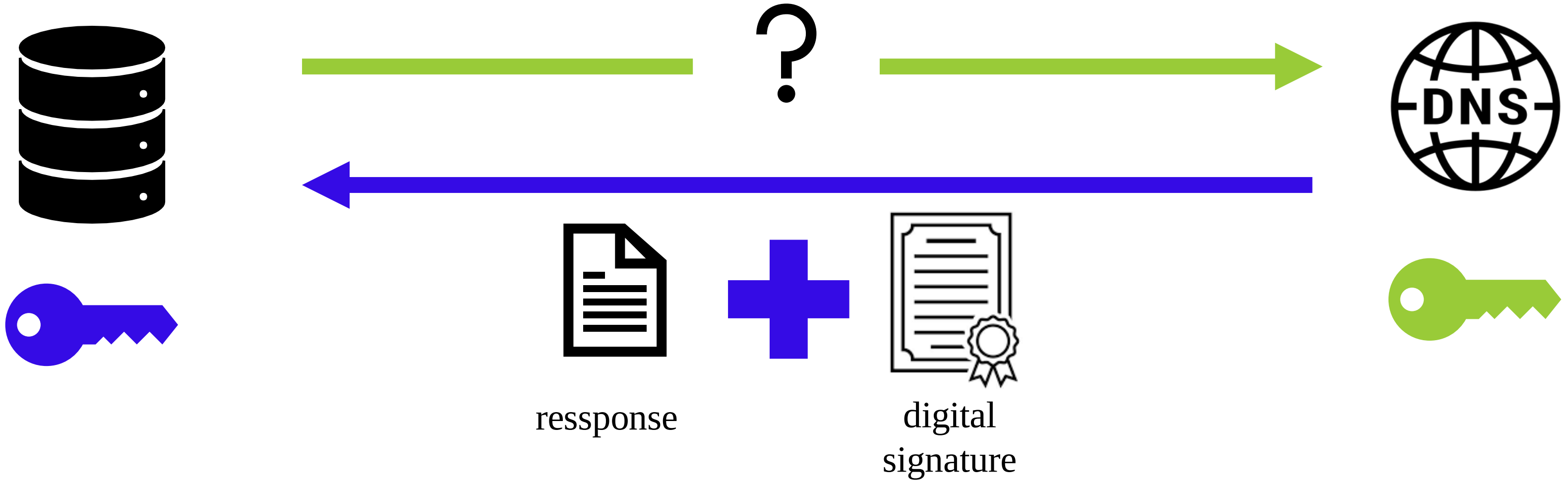
- Leakage of privacy information contained in the DNS queries/responses

- DNS over TLS(DoT), DNS over HTTPS(DoH), …



DNSSEC

- DNSSEC is a mechanism used to assure the integrity of DNS responses
  - By adding a digital signature to a DNS query response, it is possible to verify that the response has not been tampered with



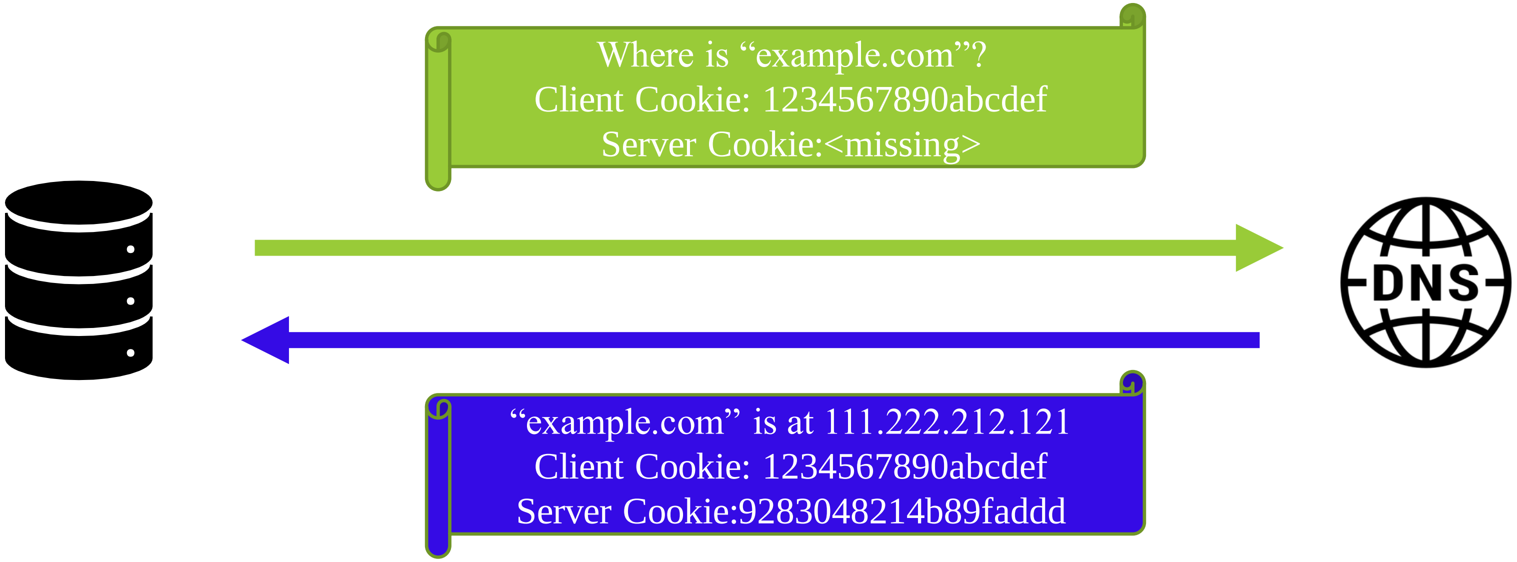
DNSSEC

- DNSSEC only guarantees the integrity of the response
  - It cannot deal with the case in which the other party to the communication has been stealthily switched

- To support DNSSEC, zone owners have to positively configure

DNS Cookies

- DNS Cookies allows both DNS clients and servers to verify that the communicating entities have not been switched
  - The client and server will each validate the DNS Cookies



Where is “example.com”?
Client Cookie: 1234567890abcdef
Server Cookie:<missing>

“example.com” is at 111.222.212.121
Client Cookie: 1234567890abcdef
Server Cookie:9283048214b89faddd

DNS Cookies

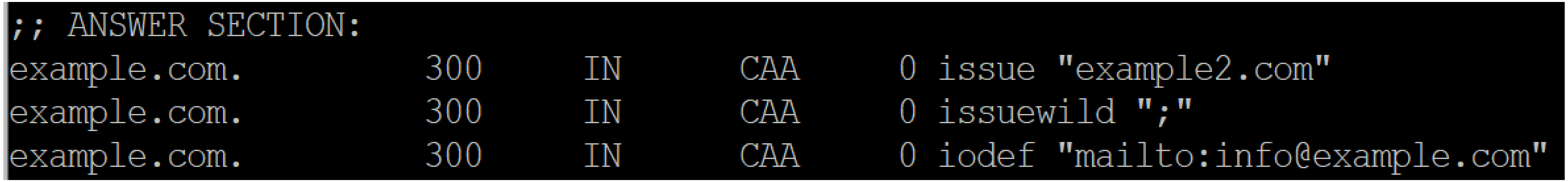
- If the verification fails, the server responds with a BADCOOKIE error and either applies a rate limit or discards the packet

- Difficulty of supporting DNS Cookies depends on DNS software implementation and default setting

CAA

- DNS certification authority authorization (CAA) prevents third parties from issuing TLS server certificates without permission

- The administrator of a domain name can specify the certification authority (CA) that is allowed to issue TLS certificates for the registered domain name



```
;; ANSWER SECTION:
example.com.            300     IN      CAA     0 issue "example2.com"
example.com.            300     IN      CAA     0 issuewild ";"
example.com.            300     IN      CAA     0 iodef "mailto:info@example.com"
```

Example of CAA RR

CAA

- CAA RR is required when issuing of TLS server certificates

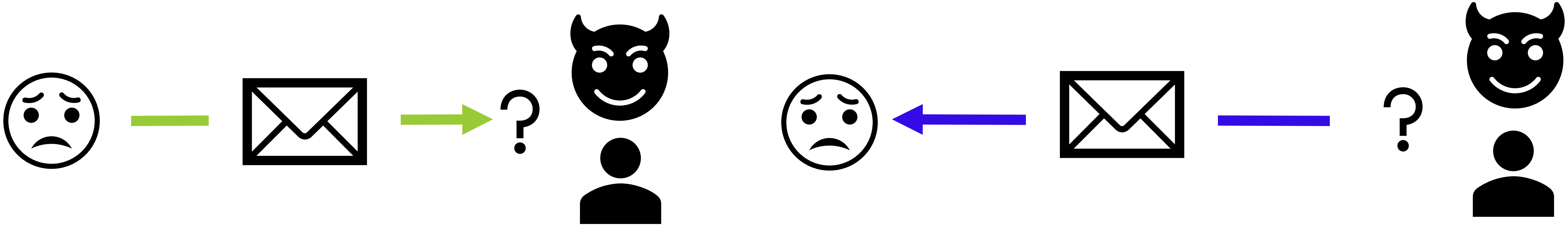
- CAA RR enable Client to distinguish whether communication with the target domain name can be encrypted or not

- CAA should be used with DNSSEC

Mail security mechanisms

- There are many security mechanisms which enhance the security functionalities for e-mail communication
  - SPF, DMARC, MTA-STS, DANE, and TLSRPT

- These mechanisms mitigate threats posed by phishing e-mails



Mail security mechanisms

- DNSSEC signing is strongly recommended for DMARC and DANE

- Mail security mechanisms are indicators of some functions:

Mechanisms	Indicator of
SPF, DMARC	sender authentication is enabled for emails
MTA-STS, TLSRPT	implementing instructions for encryption of email delivery and reporting on its downgrade.
DANE(TLSA)	distribute securely the server certificate public key used for communications other than HTTPS

DNS security mechanisms

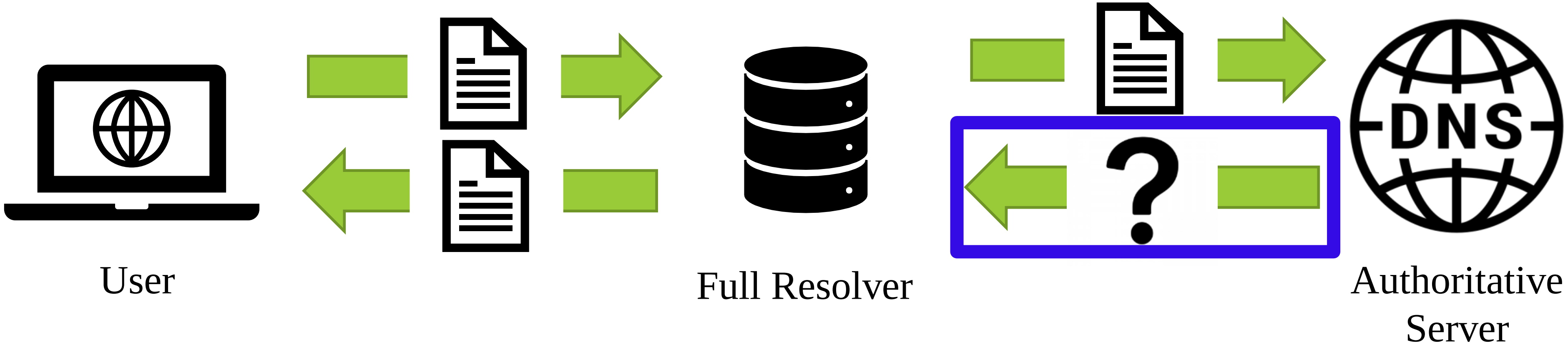
- DNS Security Mechanisms need to configure DNS Records:

Table: DNS records used for configuring DNS security mechanisms.

	Configure	Target domain name	RR	Signature
DNSSEC	Server	<domain name>	RRSIG(, etc)	n/a
DNS Cookies	Server	n/a	n/a	n/a
CAA	Server	<domain name>	CAA	n/a
SPF	Server	<domain name>	TXT	v=spf1…
DMARC	Receiver	_dmarc.<domain name>	TXT	v=DMARC1…
MTA-STS	Receiver	_mta-sts.<domain name>	TXT	v=STSv1…
DANE	Receiver	_25._tcp.<domain name>	TLSA	n/a
TLSRPT	Receiver	_smtp._tls.<domain name>	TXT	v=TLSRPTv1…

Method

- The IP addresses corresponding to each domain name are examined
- If we observe that at least one IP address operates the mechanism, then we determine that the entire domain name is compliant with the security mechanism



Data set

- Root: 1 domain, 13 IP
- TLDs
  - (the legacy) gTLD : 22 domains, 110 IP
  - ccTLD: 254 domains, 993 IP
- Popular domains(from Tranco List): 9999 domains, 12,318 IP

- We focus on IPv4 addresses

Result – Core DNS infrastructures

- Security mechanisms used to counter threats to DNS communication have a high adoption rate in servers involved in the core of the DNS

DNS Servers	DNSSEC[%]	DNS Cookies[%]	CAA [%]	MX[%]	SPF[%]	DMARC[%]	MTA-STS[%]	DANE [%]	TLSRPT [%]
ROOT	**100.00**	**100.00**	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ccTLD	**56.69**	**81.10**	0.00	6.30	0.00	0.00	0.00	0.00	0.00
gTLD	**100.00**	**45.45**	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Top 10	0.00	20.00	30.00	90.00	100.00	88.89	33.33	0.00	33.33
Top 100	4.00	21.00	48.00	86.00	96.51	84.88	5.81	0.00	5.81
Top 1K	9.20	13.80	22.70	88.10	92.85	74.01	1.48	0.57	1.82
Top 5K	8.60	18.58	14.90	87.76	89.86	58.49	0.75	0.84	0.98
Top 10K	7.67	17.40	12.98	86.75	88.66	54.09	0.51	0.84	0.74

Result – Popular domains

- The rate for domain names used on the web remains low at 4-20%

DNS Servers	DNSSEC[%]	DNS Cookies[%]	CAA [%]	MX[%]	SPF[%]	DMARC[%]	MTA-STS[%]	DANE [%]	TLSRPT [%]
ROOT	100.00	100.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ccTLD	56.69	81.10	0.00	6.30	0.00	0.00	0.00	0.00	0.00
gTLD	100.00	45.45	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Top 10	**0.00**	**20.00**	30.00	90.00	100.00	88.89	33.33	0.00	33.33
Top 100	**4.00**	**21.00**	48.00	86.00	96.51	84.88	5.81	0.00	5.81
Top 1K	**9.20**	**13.80**	22.70	88.10	92.85	74.01	1.48	0.57	1.82
Top 5K	**8.60**	**18.58**	14.90	87.76	89.86	58.49	0.75	0.84	0.98
Top 10K	**7.67**	**17.40**	12.98	86.75	88.66	54.09	0.51	0.84	0.74

Result – Mail security mechanisms(1)

- SPF and DMARC have a higher adoption rate than other security mechanisms

DNS Servers	DNSSEC[%]	DNS Cookies[%]	CAA [%]	MX[%]	SPF[%]	DMARC[%]	MTA-STS[%]	DANE [%]	TLSRPT [%]
ROOT	100.00	100.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ccTLD	56.69	81.10	0.00	6.30	0.00	0.00	0.00	0.00	0.00
gTLD	100.00	45.45	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Top 10	0.00	20.00	30.00	90.00	**100.00**	**88.89**	33.33	0.00	33.33
Top 100	4.00	21.00	48.00	86.00	**96.51**	**84.88**	5.81	0.00	5.81
Top 1K	9.20	13.80	22.70	88.10	**92.85**	**74.01**	1.48	0.57	1.82
Top 5K	8.60	18.58	14.90	87.76	**89.86**	**58.49**	0.75	0.84	0.98
Top 10K	7.67	17.40	12.98	86.75	**88.66**	**54.09**	0.51	0.84	0.74

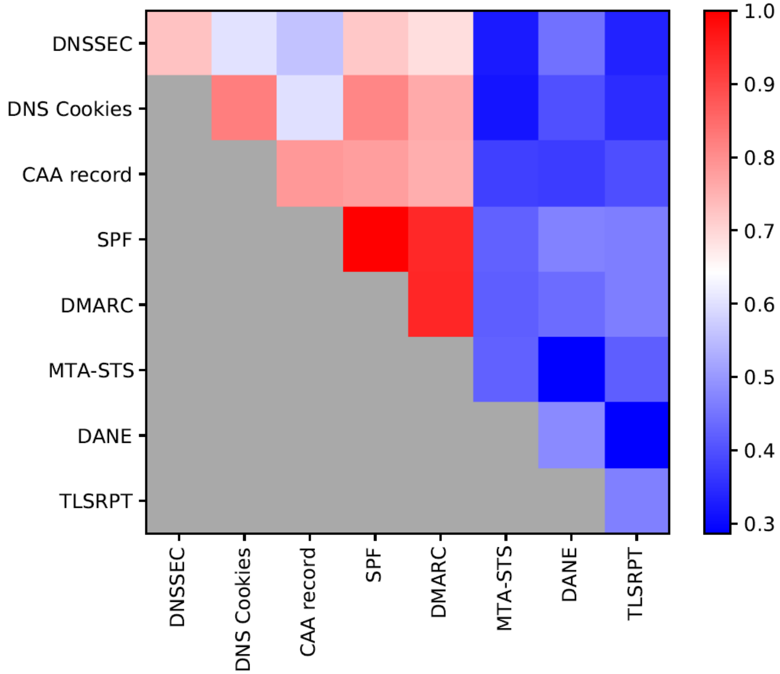
Result – Mail security mechanisms(2)

- The adoption rate of DANE is less than 1%, regardless of its popularity

DNS Servers	DNSSEC[%]	DNS Cookies[%]	CAA [%]	MX[%]	SPF[%]	DMARC[%]	MTA-STS[%]	DANE [%]	TLSRPT [%]
ROOT	100.00	100.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
ccTLD	56.69	81.10	0.00	6.30	0.00	0.00	0.00	0.00	0.00
gTLD	100.00	45.45	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Top 10	0.00	20.00	30.00	90.00	100.00	88.89	33.33	**0.00**	33.33
Top 100	4.00	21.00	48.00	86.00	96.51	84.88	5.81	**0.00**	5.81
Top 1K	9.20	13.80	22.70	88.10	92.85	74.01	1.48	**0.57**	1.82
Top 5K	8.60	18.58	14.90	87.76	89.86	58.49	0.75	**0.84**	0.98
Top 10K	7.67	17.40	12.98	86.75	88.66	54.09	0.51	**0.84**	0.74

Result – Co-occurence

- The co-occurrence scores of SPF and DMARC, DNS Cookies and SPF, and CAA and SPF are high



Result – Adoption rates against difficulty

- We study the relationship between setup difficulty and adoption rate for each security mechanism

- The evaluation indicators were set as the table:

No.	Description	Point
1	DNS resource records need to be configured.	1
2	DNS server configuration needs to be changed.	2
3	Mail server configuration needs to be changed.	2
4	Web server configuration needs to be changed.	2
5	A third-party intermediary is required.	3

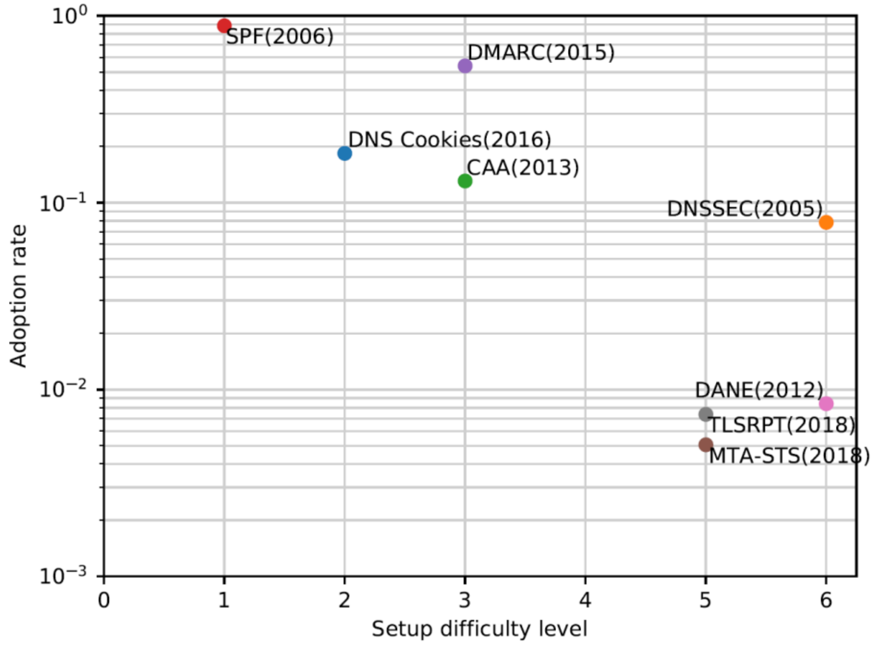
Result – Adoption rates against difficulty

- As a result, the setting difficulty is as the table:

Mechanisms	Indicators No.					Difficulty Level
	1	2	3	4	5	
SPF	1					1
DNS Cookies		2				2
DMARC	1		2			3
CAA	1			2		3
MTA-STS	1		2	2		5
TLSRPT	1		2	2		5
DNSSEC	1	2			3	6
DANE	1	2			3	6

Result – Adoption rates against difficulty

- The lower the difficulty level is, the higher the adoption rate
  - Even when the difficulty level is high, mechanisms proposed relatively earlier have a higher adoption rate than newer mechanisms



Discussion

- The security level of a DNS can be significantly improved by properly configuring the security mechanisms analyzed in this study
- Domain name administrators should review the configuration of these mechanisms on a regular basis
- The key to increasing the adoption rate of security mechanisms lies in their ease of setup.

Future work

- Conduct a human study on domain name administrators
  - approaches such as surveys, interviews, or focus groups
- Study of new DNS security mechanisms to be standardized in the future
- Investigate whether the security mechanisms that operate in DNS clients and full resolvers are correctly configured and operated

Conclusion

- We conducted a large-scale measurement study on the adoption rates of major DNS security mechanisms
  - DNSSEC, DNS Cookies, CAA, SPF, DMARC, MTA-STS, DANE, and TLSRPT

- Core DNS infrastructures such as root servers and TLD servers had high adoption rates of DNSSEC and DNS Cookies

- Mechanisms that were easier to configure tended to have higher adoption rates

Questions? Comments?

Masanori Yajima

y-masa22@nsl.cs.waseda.ac.jp