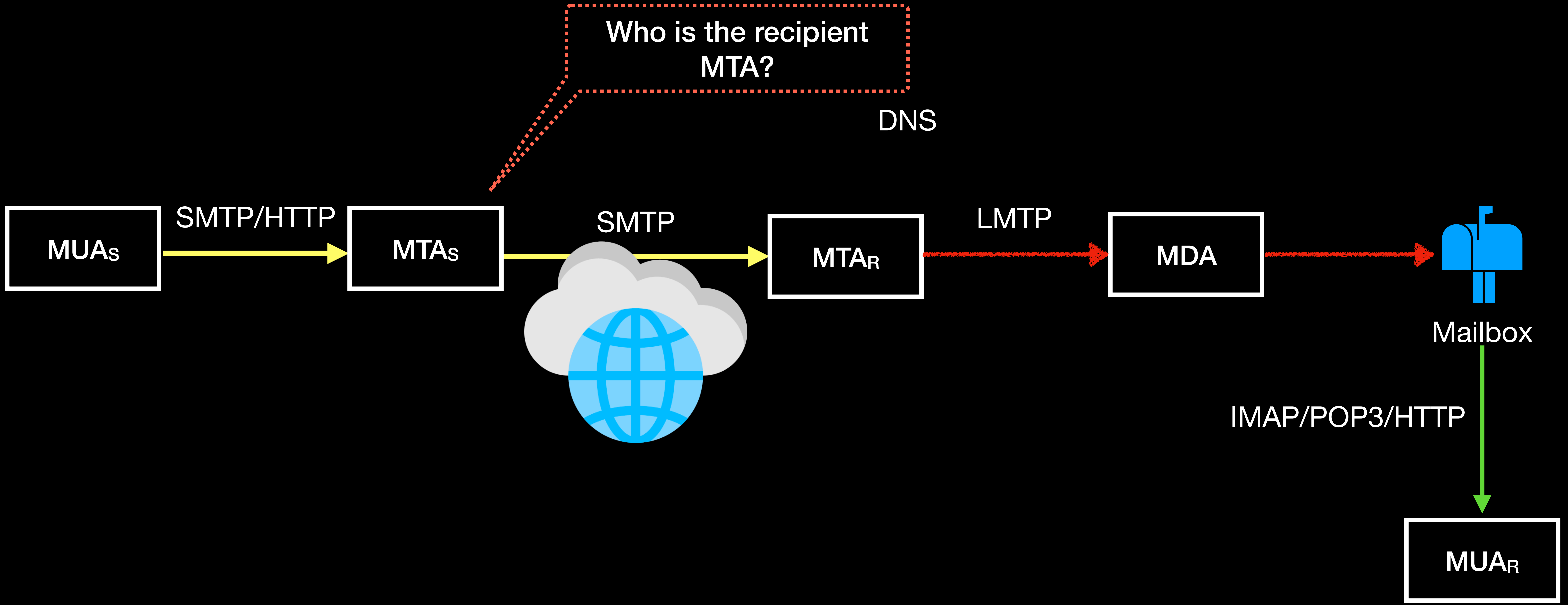
You've Got Report: Measurement and Security Implications of DMARC Reporting

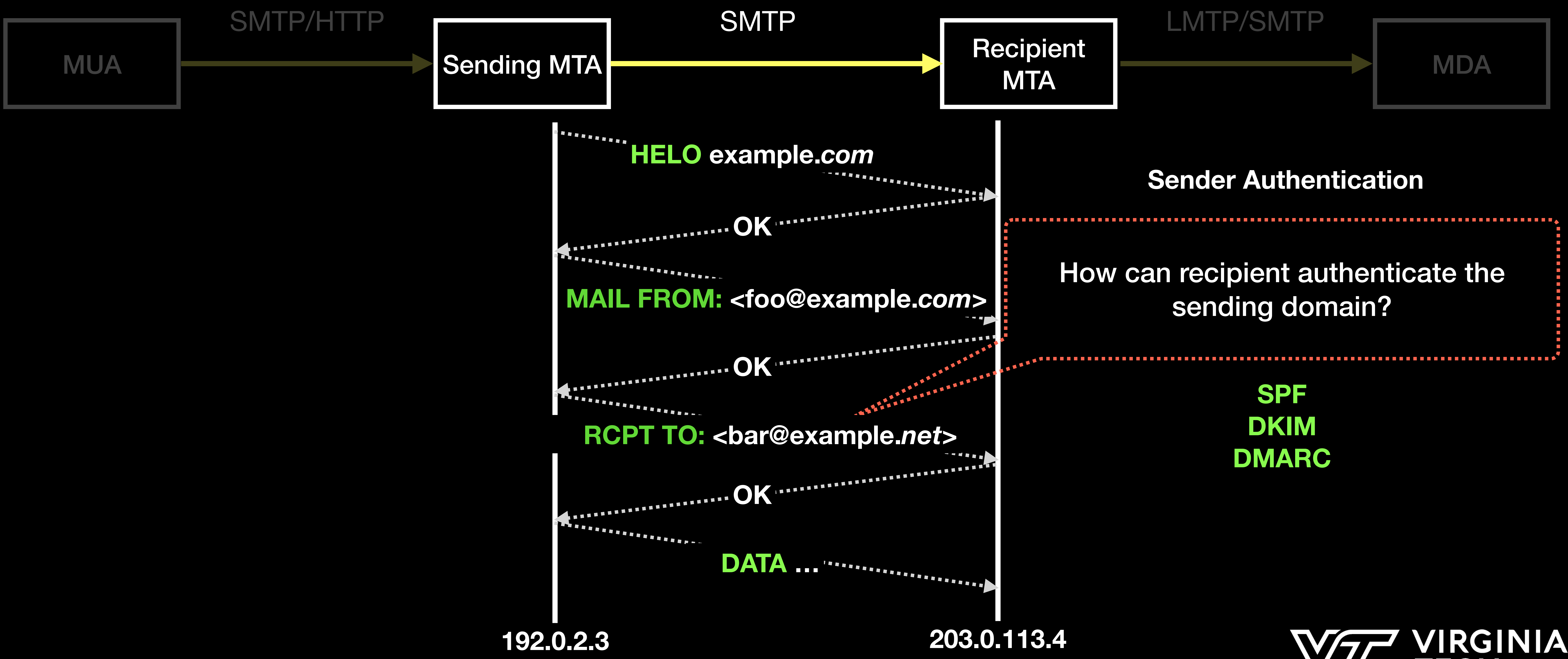
Md. Ishtiaq Ashiq[§], Weitong Li[§],
Tobias Fiebig[†], and Tijay Chung[§]

[§]Virginia Tech, [†]Max Planck Institute for Informatics

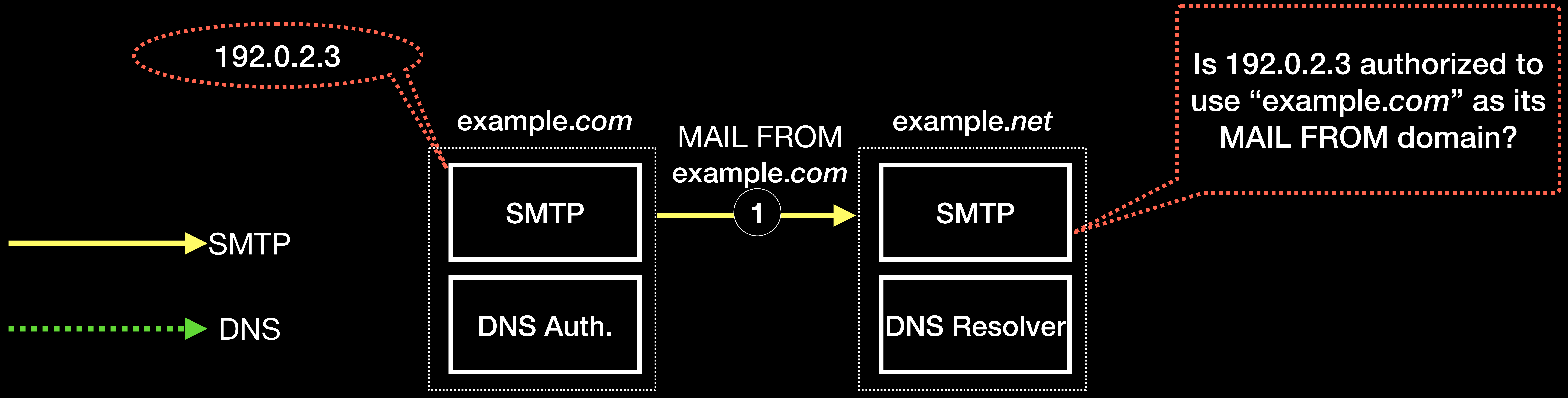
How Email Works



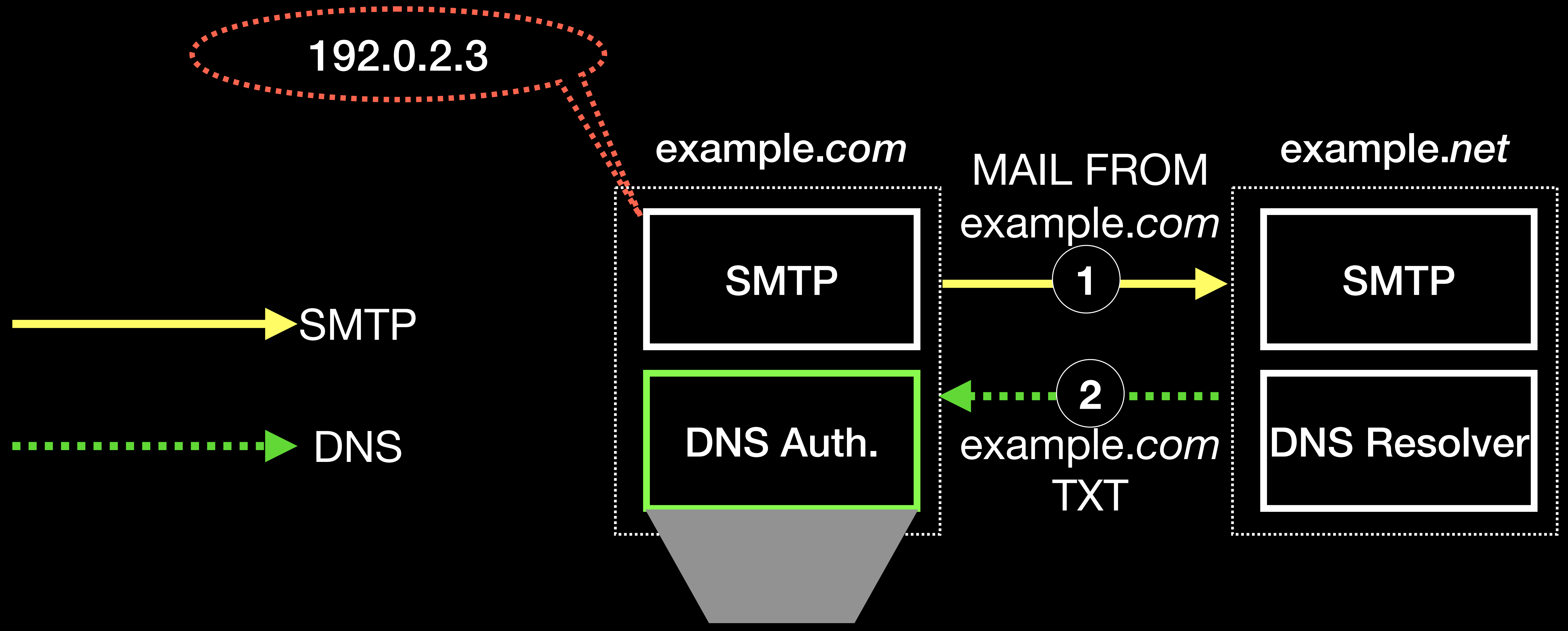
How SMTP Works



SPF (Sender Policy Framework)

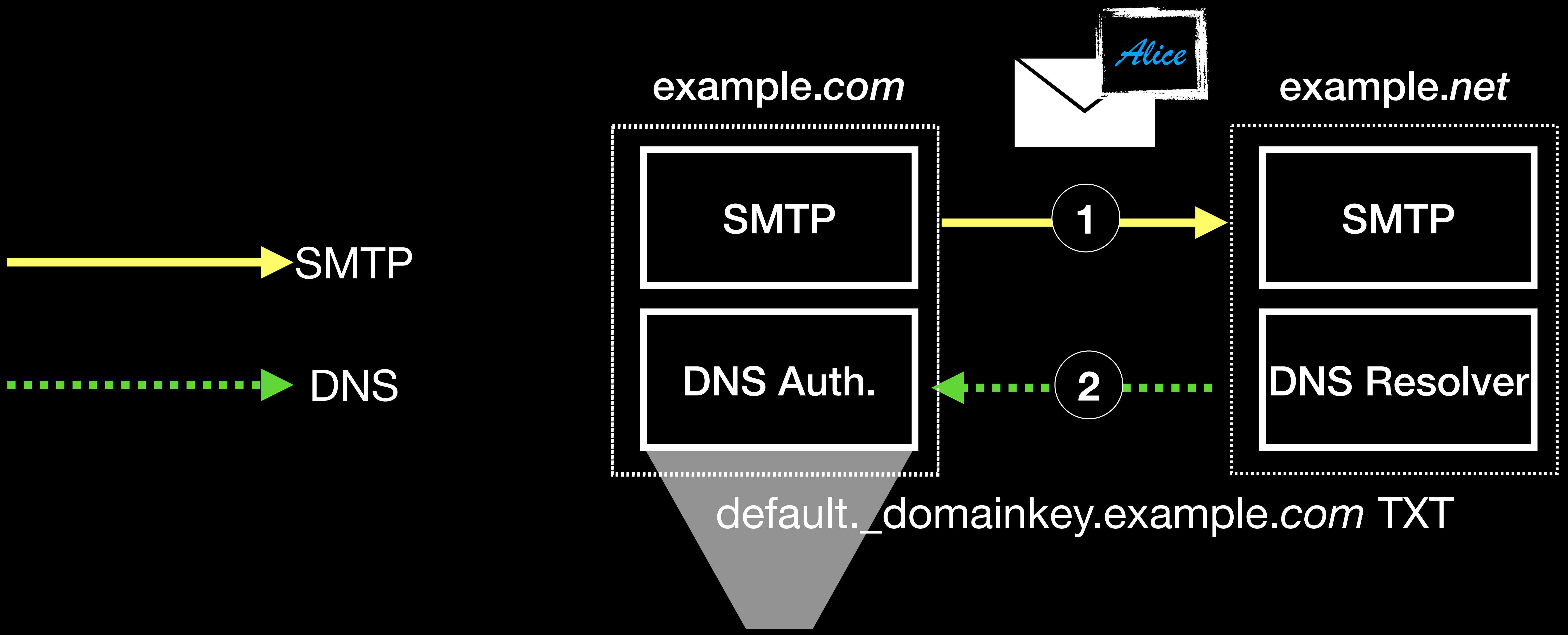


SPF (Sender Policy Framework)



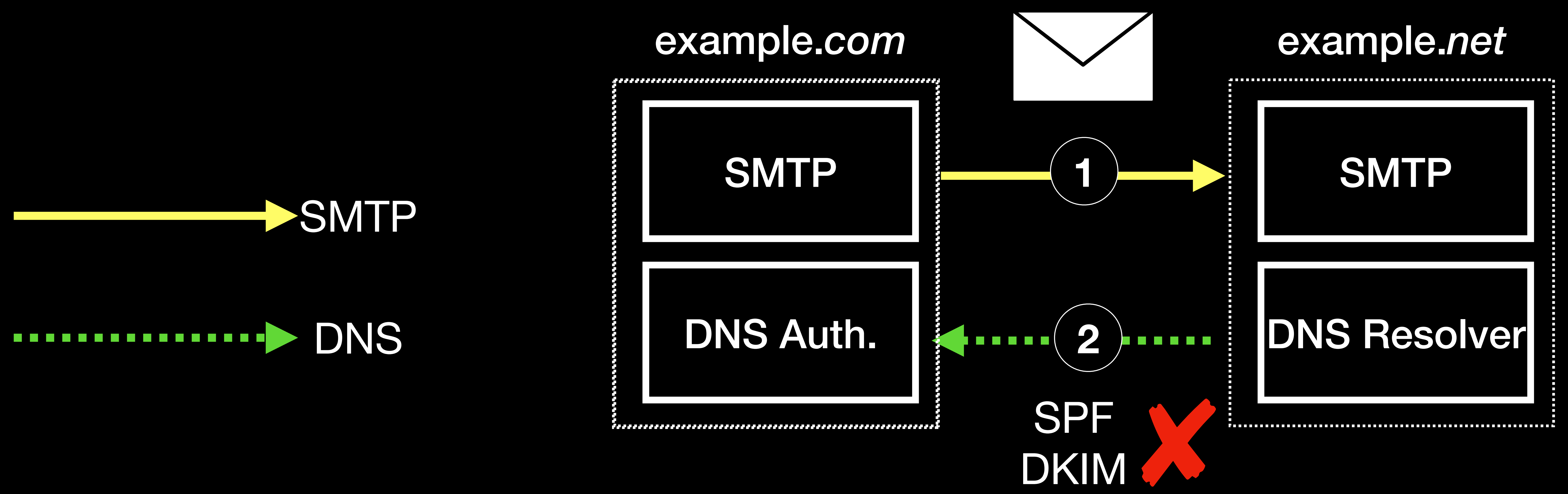
`example.com        TXT                v=spf1 ip4:192.0.2.0/24 -all`

DKIM (DomainKeys Identified Mail)



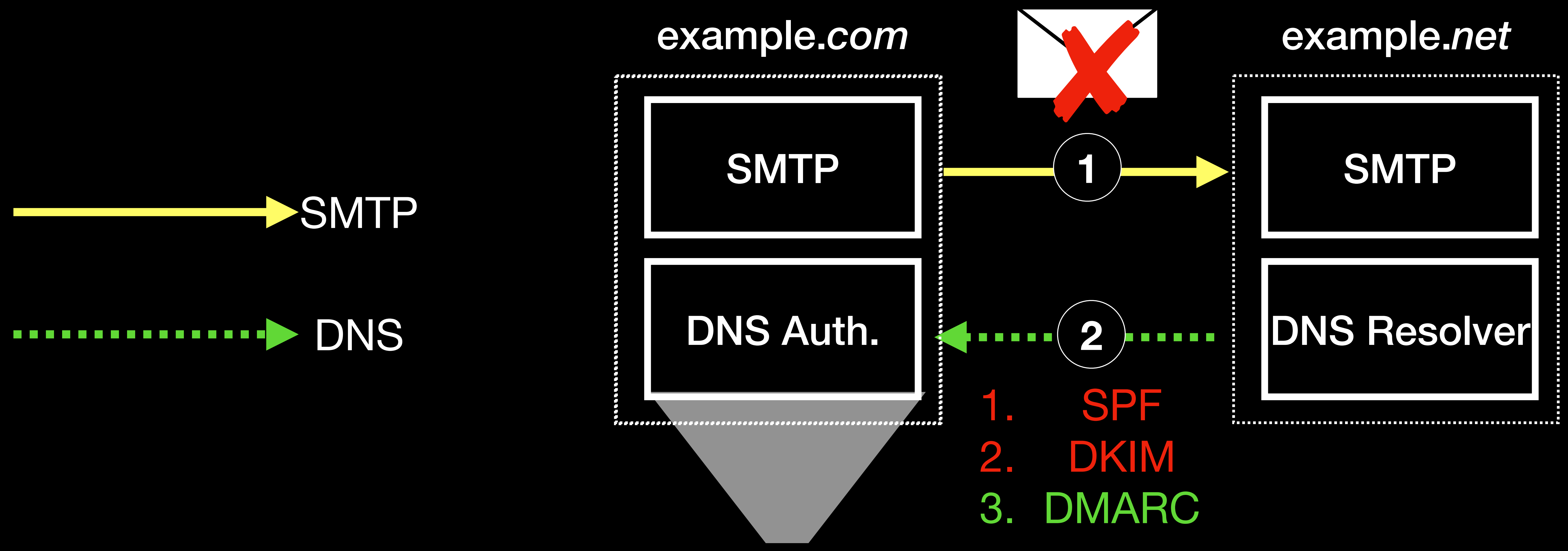
`default._domainkey.example.com  TXT  k=rsa; p=MIGfMAMIGfMA0MIGfMIGfMIGfMIGfMAGCd…`

What happens if SPF/DKIM validation fails?



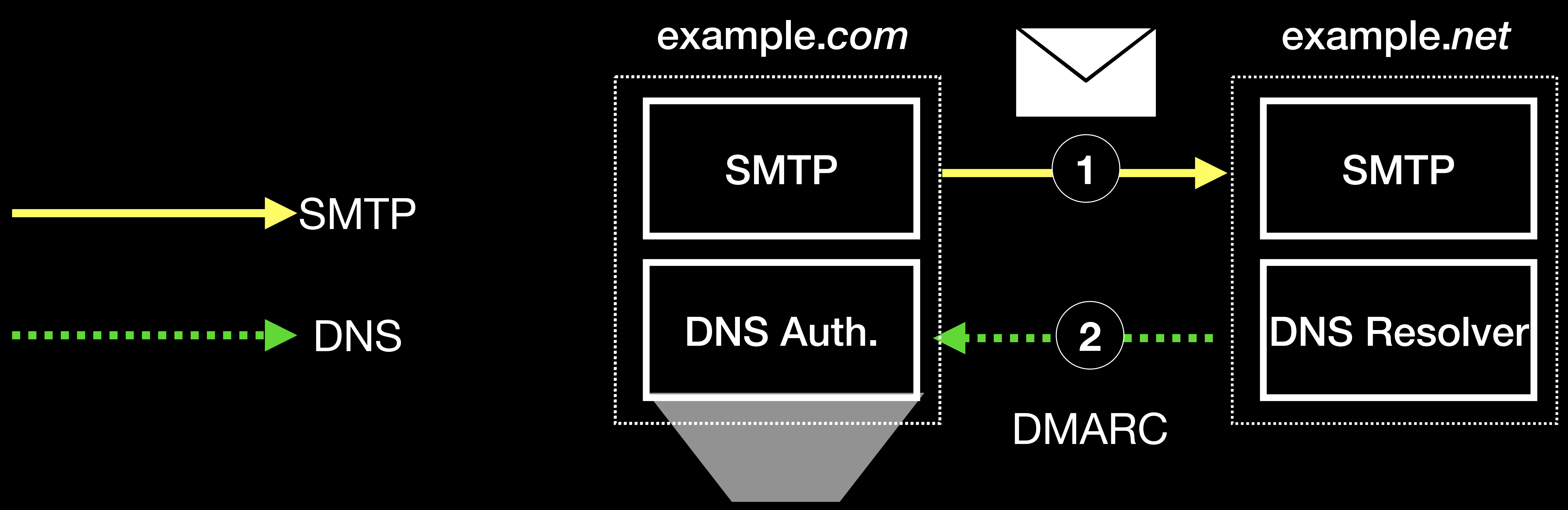
- SPF/DKIM do not tell what actions the receiver has to take when validation fails.

DMARC
(Domain-based Message Authentication, Reporting & Conformance)



_dmarc.example.*com* TXT v=DMARC1; p=reject;

DMARC
(Domain-based Message Authentication, Reporting & Conformance)

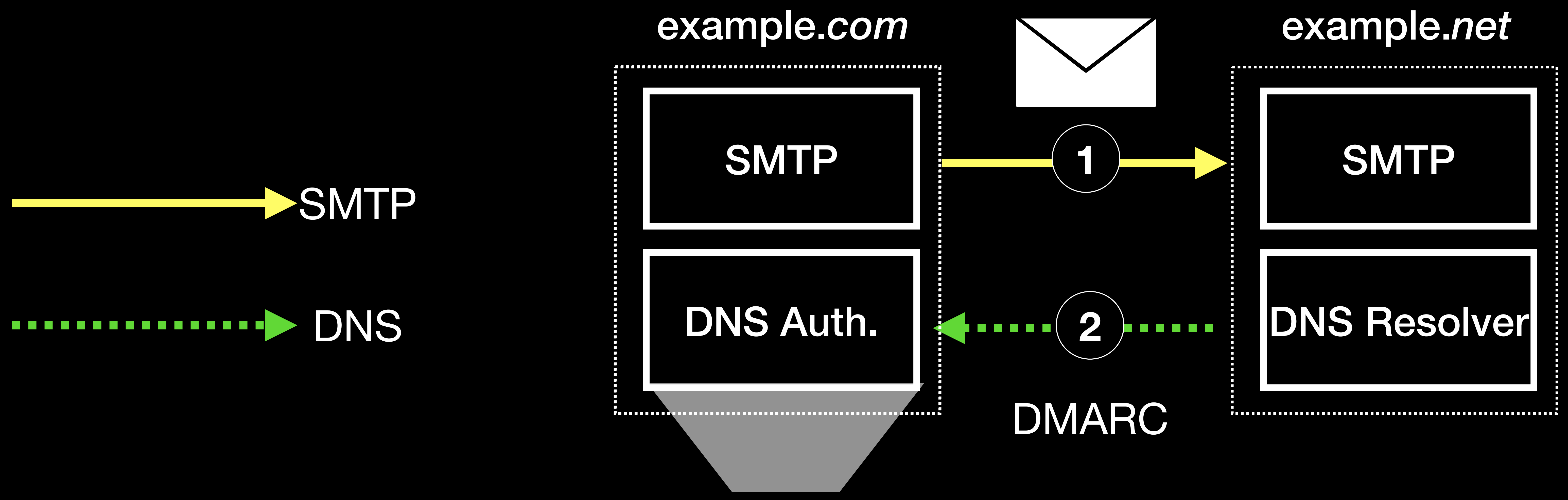


_dmarc.example.*com* TXT v=DMARC1; p=reject; rua=mailto:report@example.*com*

- Contains lots of meta information like source IP, evaluated policy, results, the number of emails, and so on.

VIRGINIA TECH

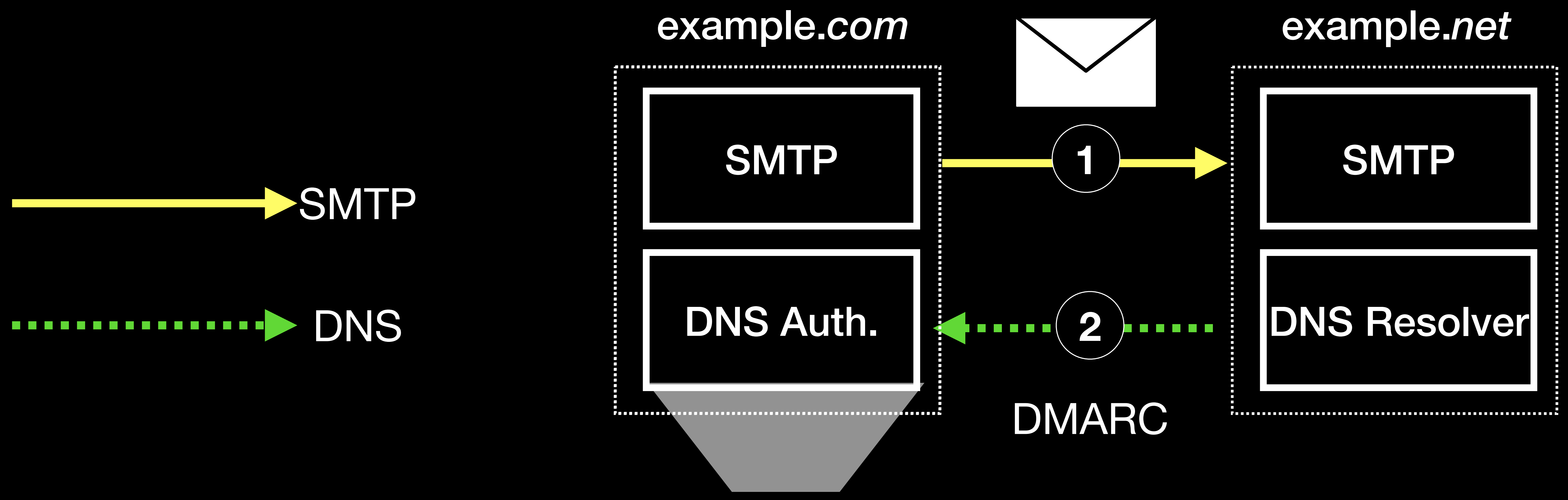
DMARC
(Domain-based Message Authentication, Reporting & Conformance)



_dmarc.example.*com* TXT v=DMARC1; p=reject; rua=mailto:report@example.*com*

- Helps sender identify and address threats promptly

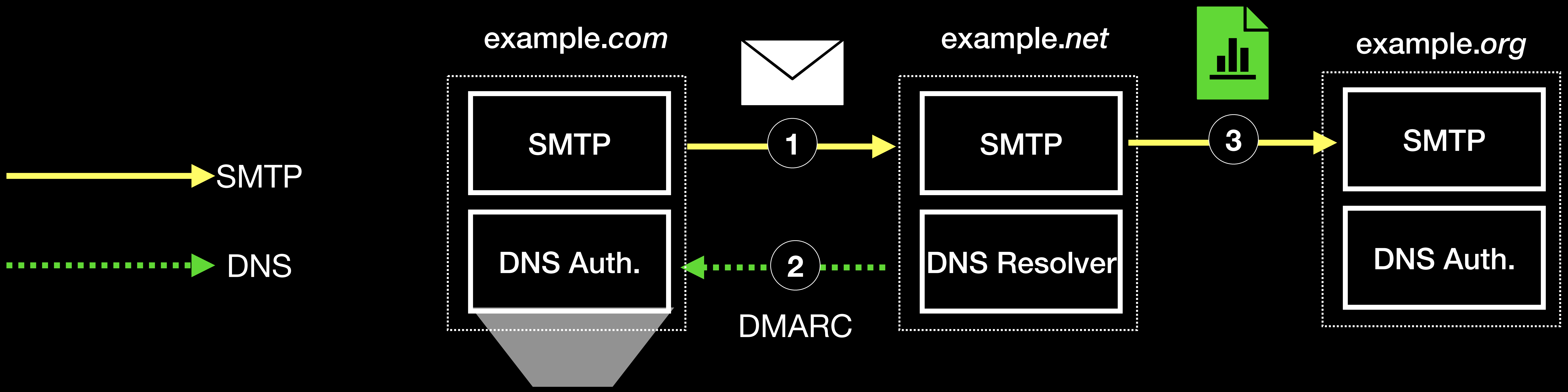
DMARC
(Domain-based Message Authentication, Reporting & Conformance)



_dmarc.example.com TXT v=DMARC1; p=reject; rua=mailto:report@example.org

- XML formatted, thus not user-friendly – thus 80% of the report recipient address is an external domain.

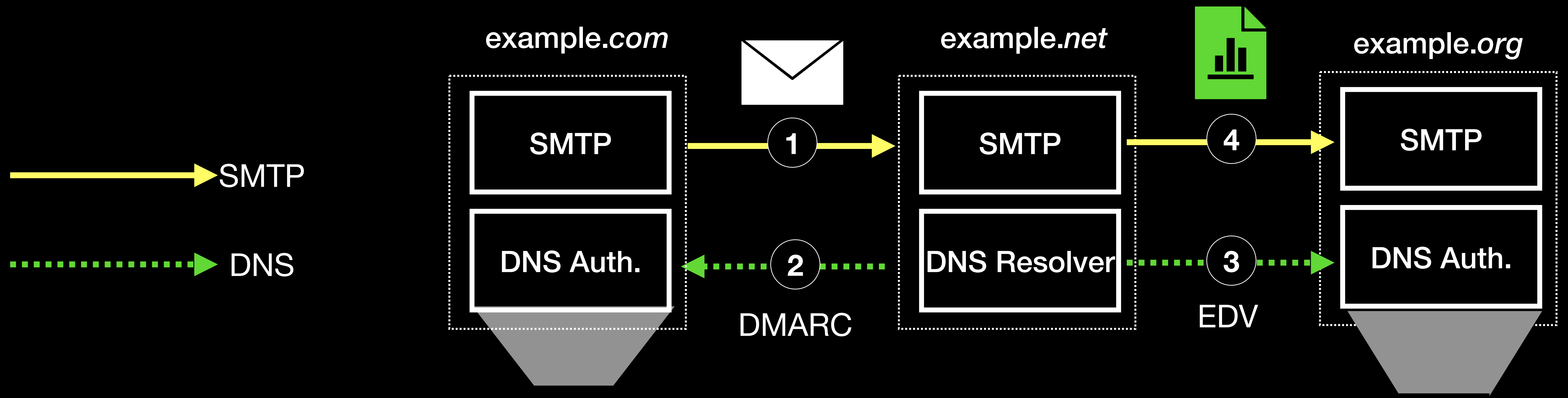
DMARC report w/ external domains



_dmarc.example.*com* TXT v=DMARC1; p=reject; rua=mailto:report@example.*org*

How does example.*net* know that example.*org* has agreed to receive the report?

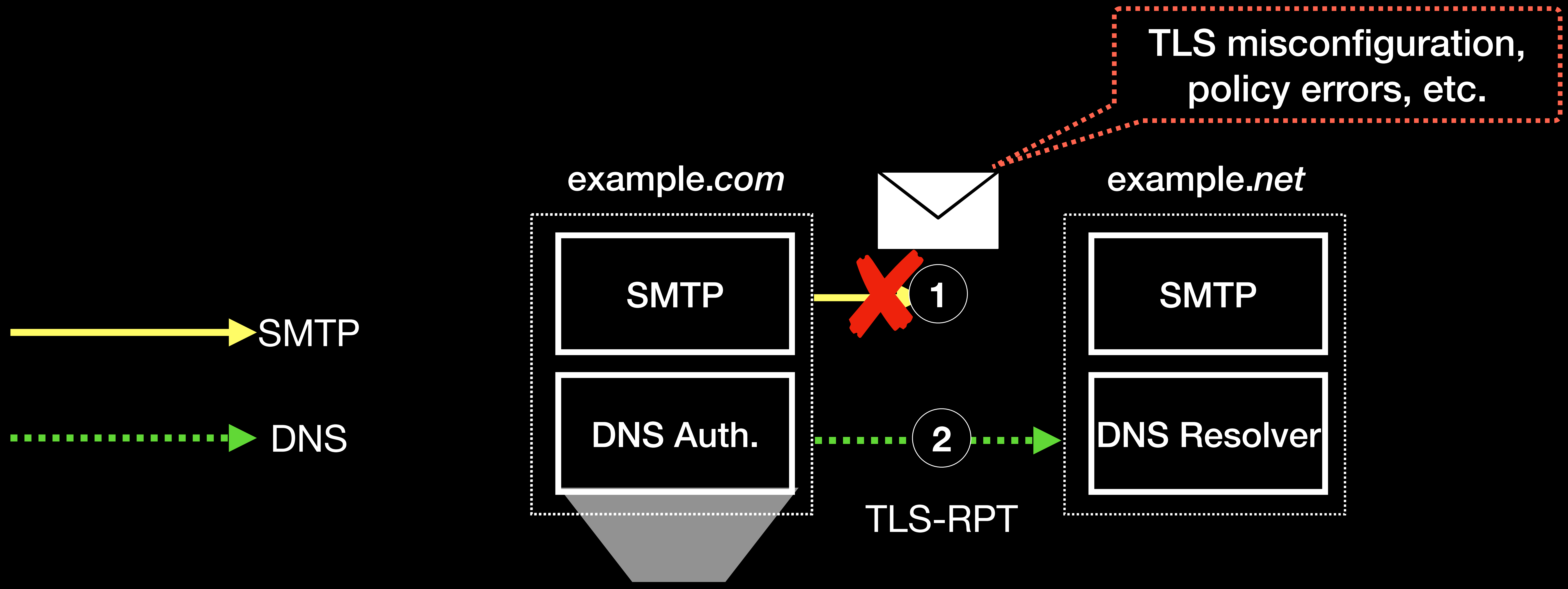
DMARC report w/ External Destination Verification (EDV)



_dmarc.example.*com* TXT v=DMARC1; p=reject; rua=mailto:report@example.*org*

example.*com*._report._dmarc.example.*org* TXT v=DMARC1

SMTP TLS Reporting



_smtp._tls.example.*net*   TXT   v=TLSRPTv1; rua=mailto:report@example.*org*

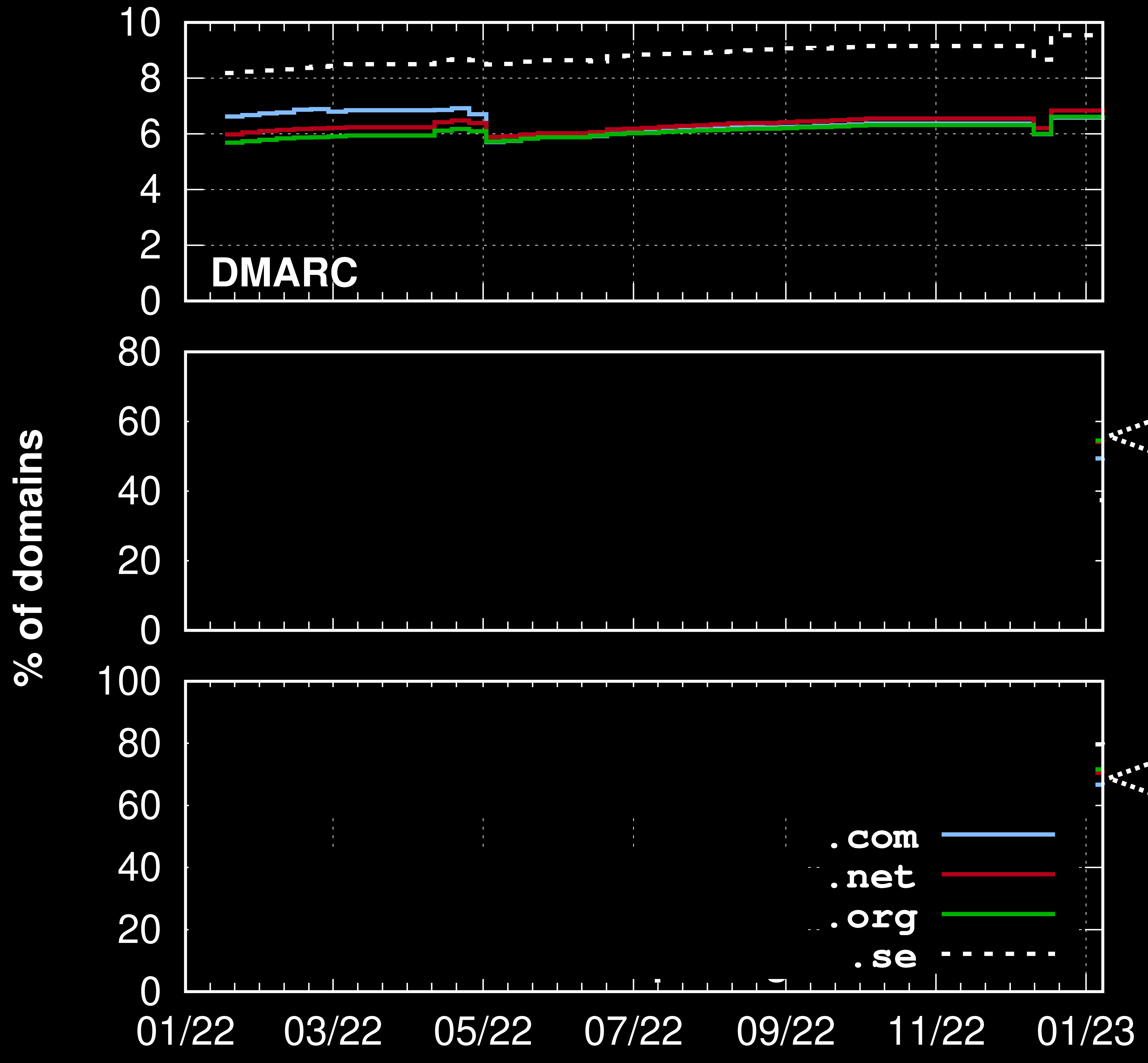
- Senders compatible with MTA-STS or DANE can share success and failure statistics with the receivers
  - Helps receivers fix their TLS configuration, MTA-STS or DANE policy, etc.

Research Questions

Measurement

- How many domains use DMARC?
  - How many of them use DMARC Reporting?
- How many receivers send DMARC reports?

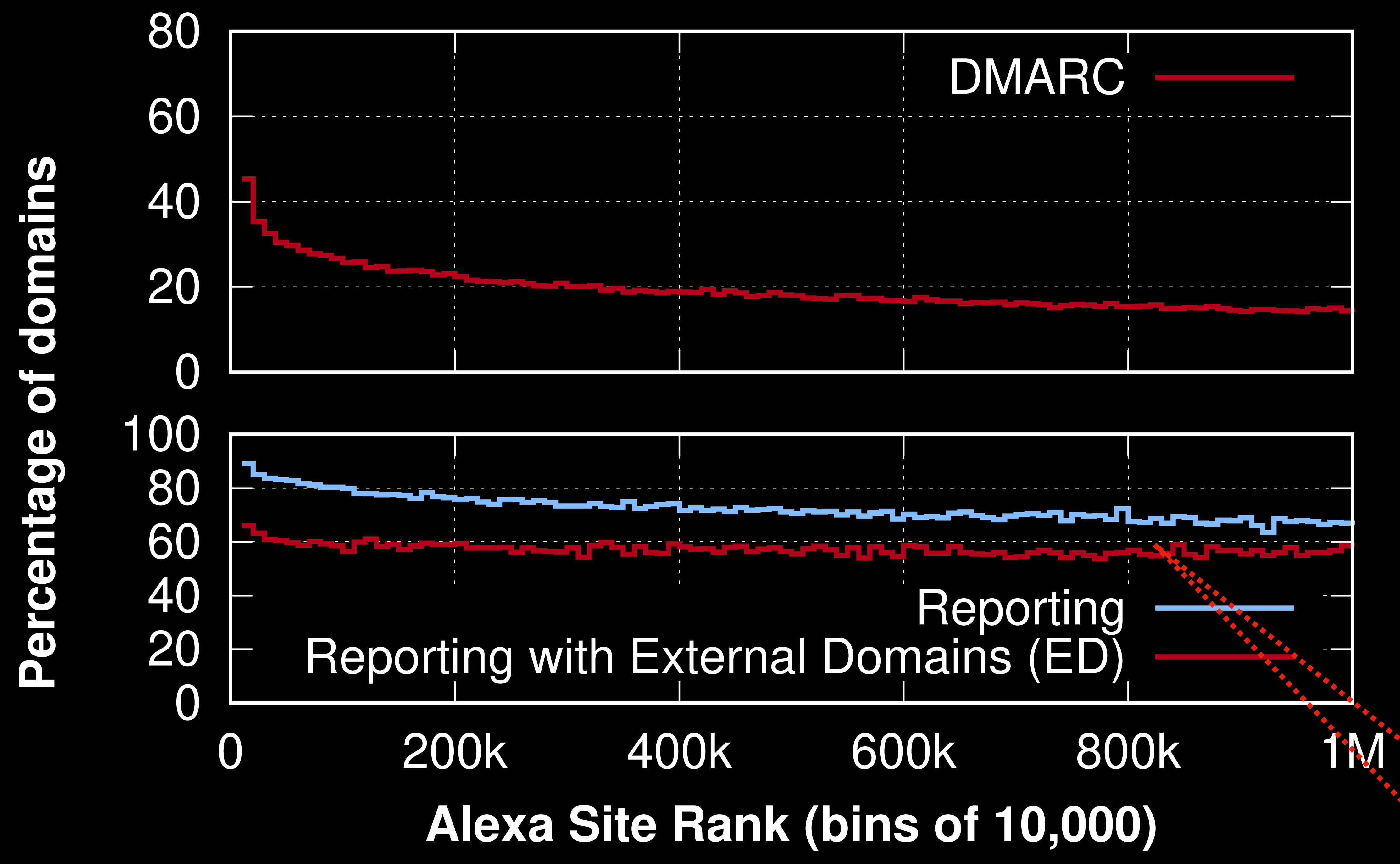
Status Quo (all domains)



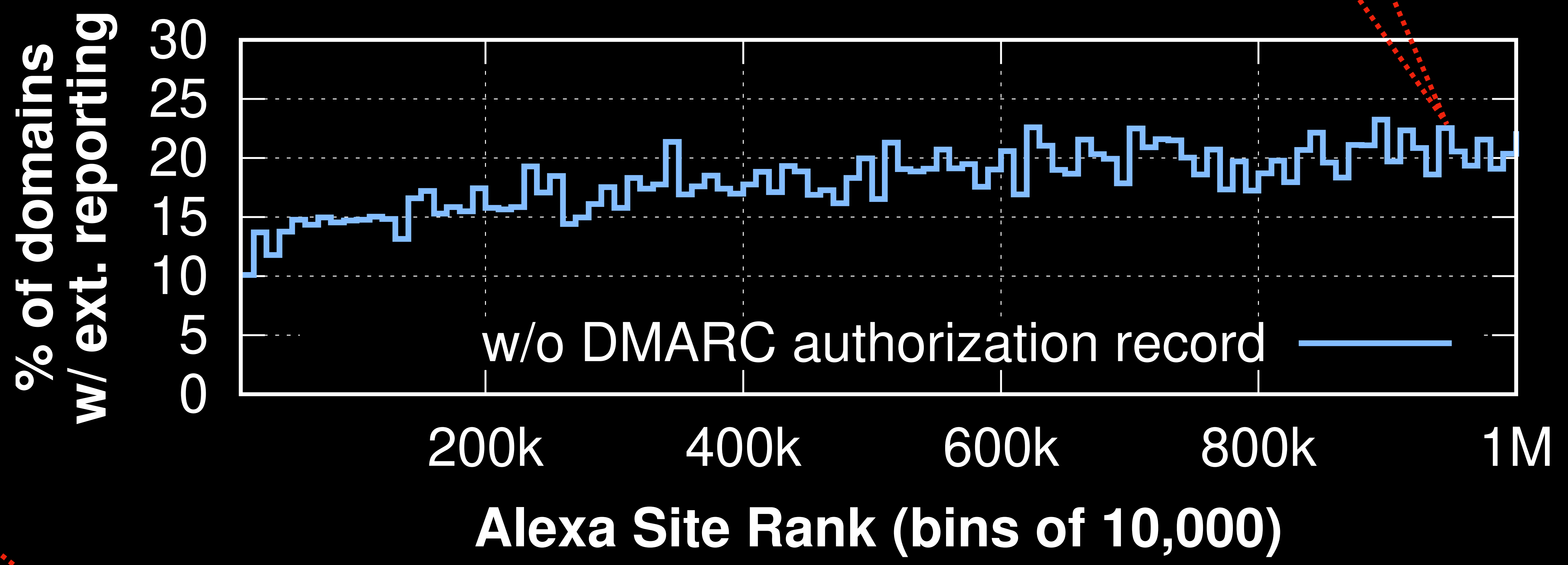
More than 50% of them uses DMARC reporting

The majority specify external domains to receive and process the report

Status Quo (popular domains)



Nearly 20% of domains that use external domains, do not have EDV authorization record



Again, more than 50% of them uses DMARC reporting

VIRGINIA TECH

Research Questions

Attacker's Perspective

Misconfigurations?

- Do SMTP servers in the wild have EDV check?
  - How about popular email hosting providers?

Ambiguities?

- Do SMTP servers in the wild have EDV check?
    - How about popular email hosting providers?

- Is RFC 7489 unambiguous for reporting?
    - What happens when there are duplicate addresses in ***rua*** tag?
    - Is there a limit to the number of addresses in ***rua*** tag?

Experiments

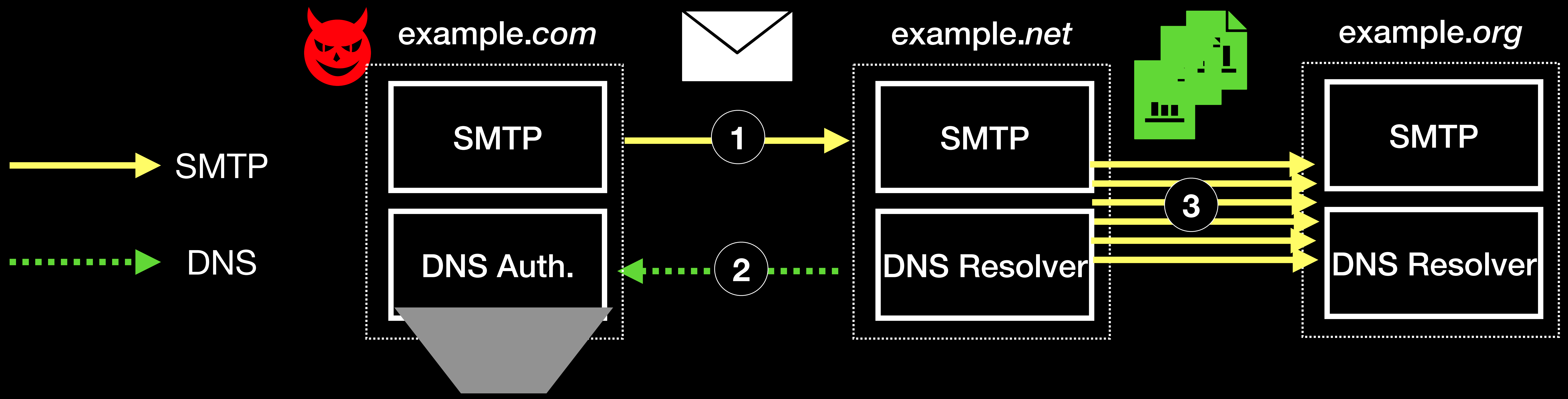
No	Name	Type	RData
Exp. 1	_dmarc.a.com	TXT	v=DMARC1; p=none; rua=mailto:admin1@a.com, ... , mailto:admin50@a.com
Exp. 2	_dmarc.a.com	TXT	v=DMARC1; p=none; rua=mailto:admin@a.com, ... , mailto:admin@a.com
Exp. 4	_dmarc.a.com	TXT	v=DMARC1; p=none; rua=mailto:admin@a.com, mailto:admin@b.com
Exp. 6	_dmarc.a.com	TXT	v=DMARC1; p=none; rua=mailto:admin@a.com
	_smtp._tls.a.com	TXT	v=TLSRPTv1; rua=mailto:admin@b.com

Result

EHP	Report Size (B)	# of addr.	EDV	Duplication Check		SMTP TLS Reporting (Exp. 6)
			Check (Exp. 4)	Addr. (Exp. 2)	Domain (Exp. 1)	
Google	3,962	50	✗	✗	✗	●
Yahoo	4,626	50	✗	✗	✗	✗
QQ	3,628	50	✗	✗	✗	✗
FastMail	4,839	10	●	✗	✗	✗
OpenDMARC	2,238	8-12*	✗	✗	✗	-
Rspamd	2,320	50	●	●	✗	-

*** OpenDMARC restricts DNS records to a maximum of 255 characters.**

Attack 1



_dmarc.example.*com* TXT v=DMARC1; p=reject; rua=mailto:report@example.*org*, mailto:report@example.*org* …

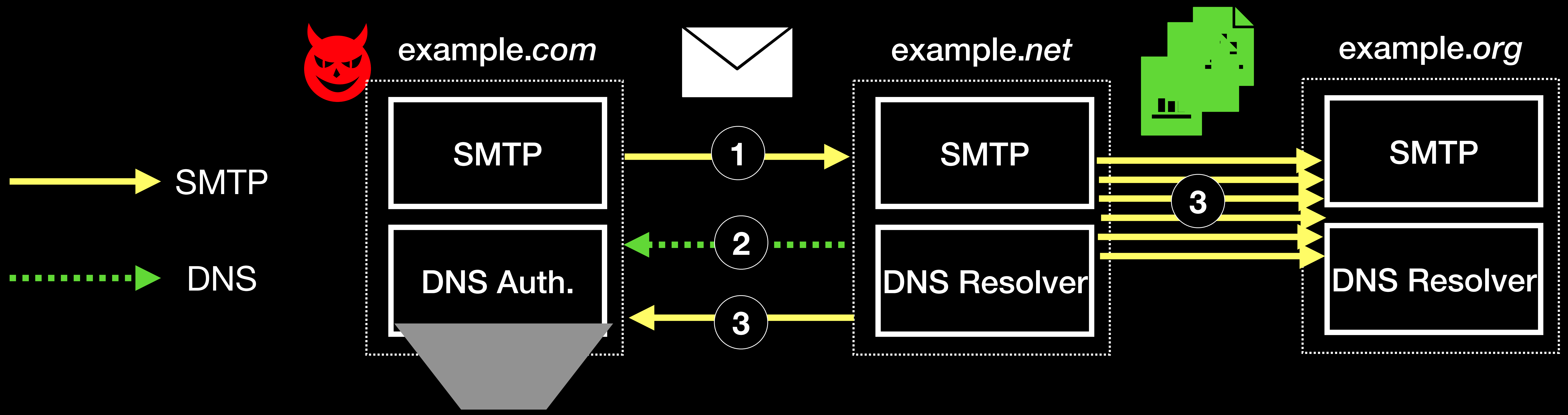
$$F = \frac{R}{200} \times M$$

R: Report Size
M: # of rua tags

Google Workspace, Yahoo, and QQ do not check EDV and do not have duplication check; So, amplification factor achievable by using them as reflector is 950x, 1150x, and 900x

VIRGINIA TECH

Attack 2



_dmarc.example.*com*	TXT	v=DMARC1; p=reject; rua=mailto:report1@s1.example.*com*; … 50 addresses
_smtp._tls.s1.example.*com*	TXT	v=TLSRPTv1; rua=mailto:report1@example.*org*, mailto:report2@example.*org*; …

$$F = \frac{R}{200} \times M^2$$

R: Report Size
M: # of rua tags

Google workspace can be used as a reflector and achievable amplification factor is 1,460x

Conclusion

- First comprehensive study of the DMARC reporting ecosystem
  - DMARC reporting and the lived practice of how it is implemented–holds the potential for annoying Denial-of-Service attacks
  - SMTP TLS reporting can also be combined to raise the attack factor
- Qualitative study
- Recommendations for future iterations on RFC7489

iashiq5@vt.edu
ashiq5.github.io

VIRGINIA TECH