ALPACA: Application Layer Protocol Confusion

Analyzing and Mitigating Cracks in TLS Authentication

Full paper at 30th USENIX Security Symposium!

Real World Crypto Symposium 2022

Marcus Brinkmann,[1] Christian Dresen,[2] Robert Merget,[1] Damian Poddebniak,[2] Jens Müller,[1] Juraj Somorovsky,[3] Jörg Schwenk,[1] Sebastian Schinzel[2]

[1] Ruhr University Bochum
[2] Münster University of Applied Sciences
[3] Paderborn University

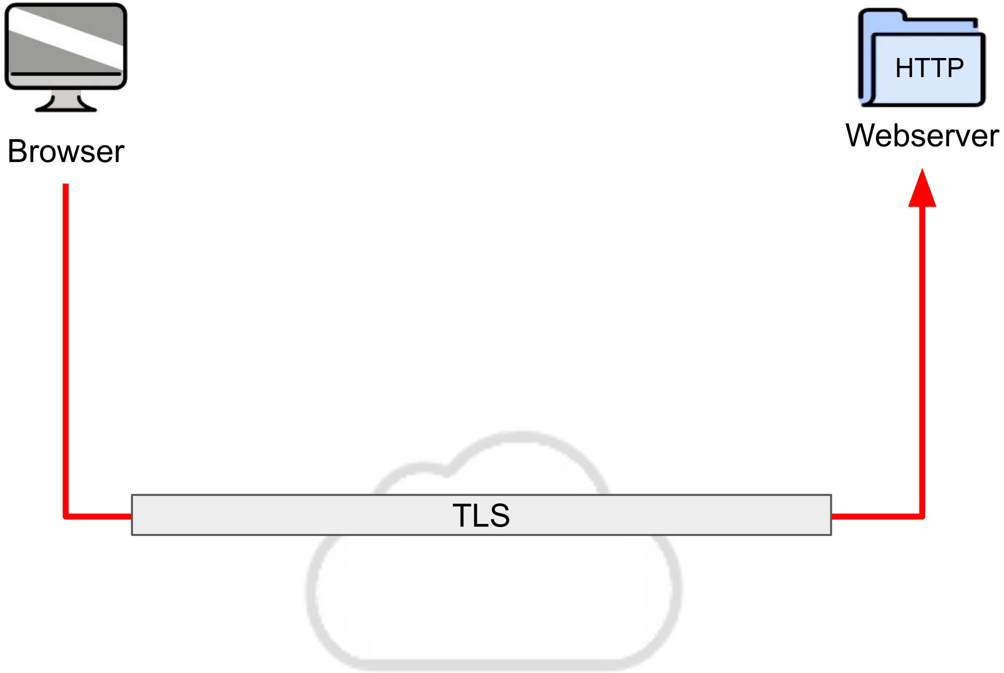
RWC 2021: Raccoon Attack

Sidechannel on TLS-DH(E)
→ Confidentiality

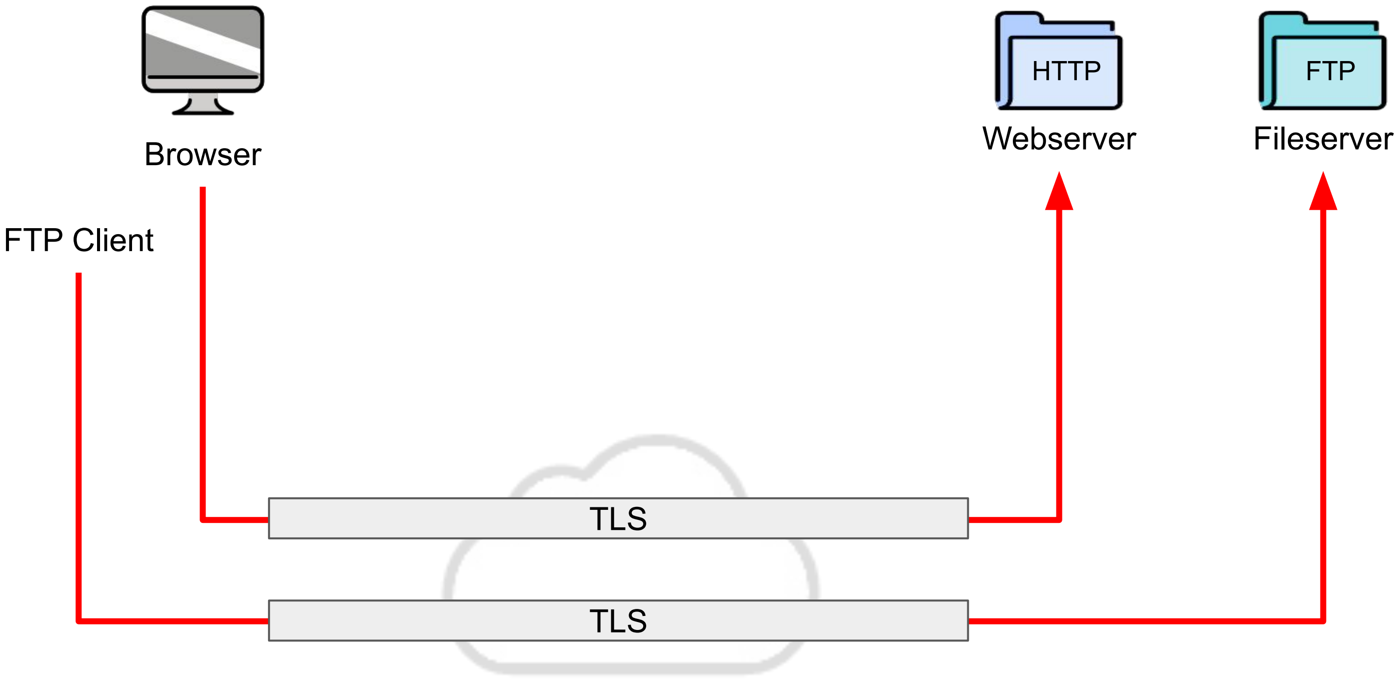
RWC 2022: ALPACA Attack

Gaps in TLS Authentication
→ Application Security

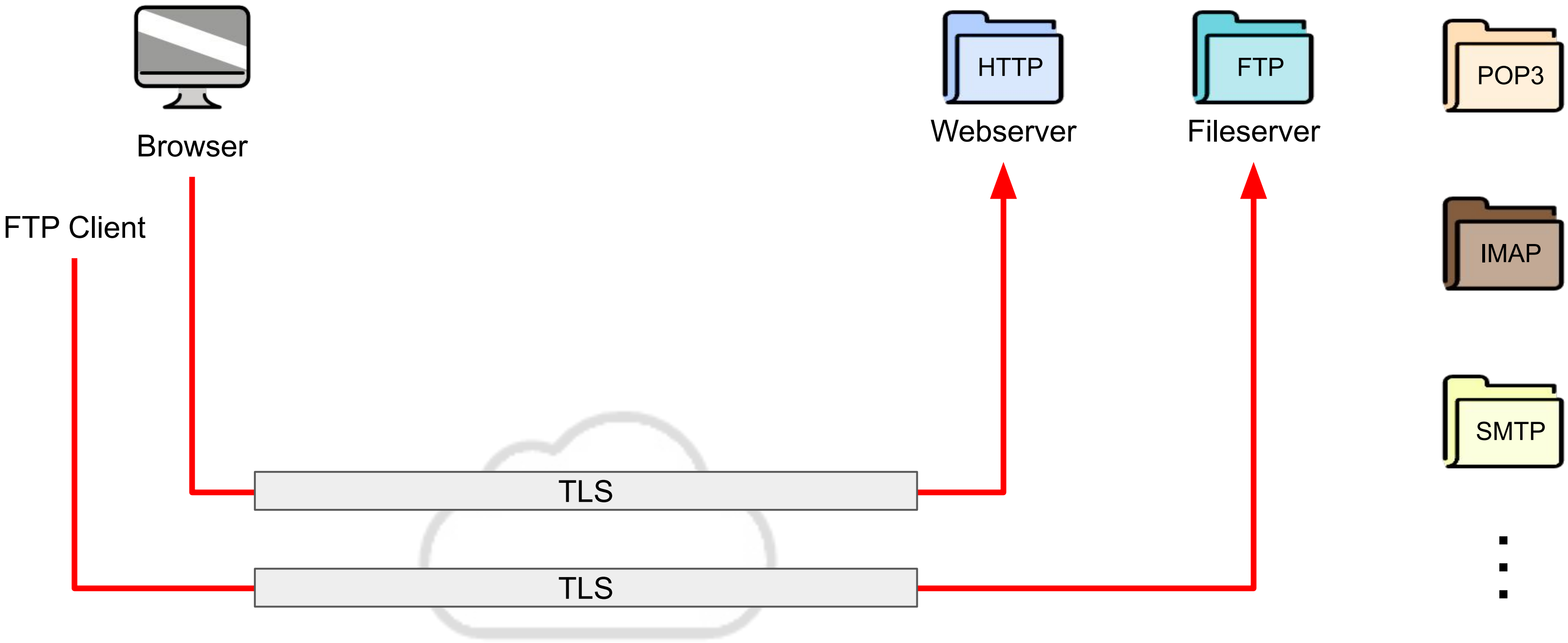
Transport Layer Security (TLS)



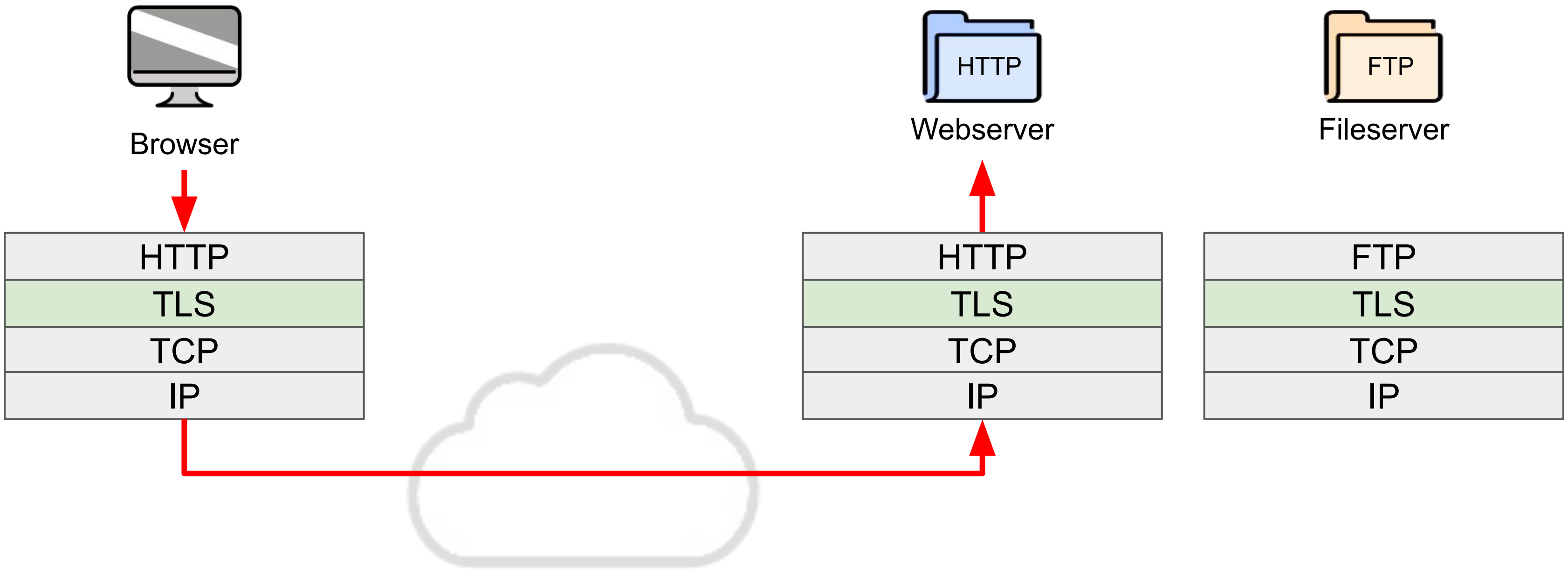
Transport Layer Security (TLS)



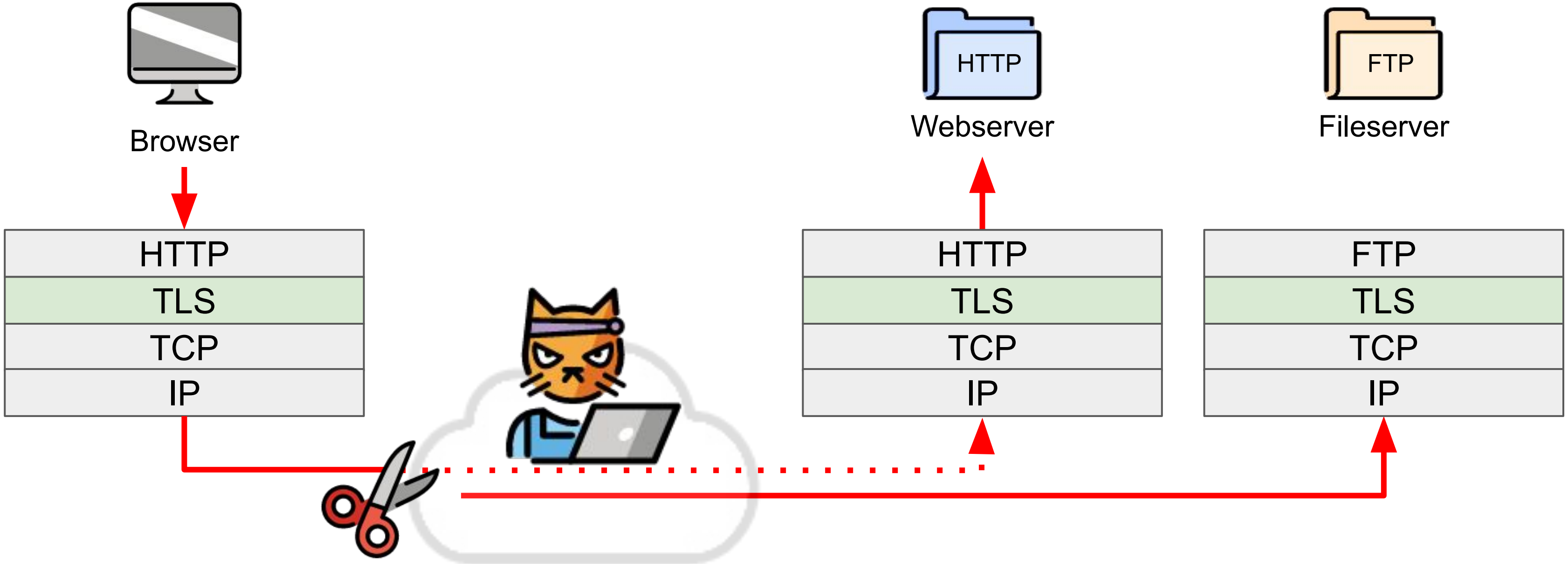
Transport Layer Security (TLS)



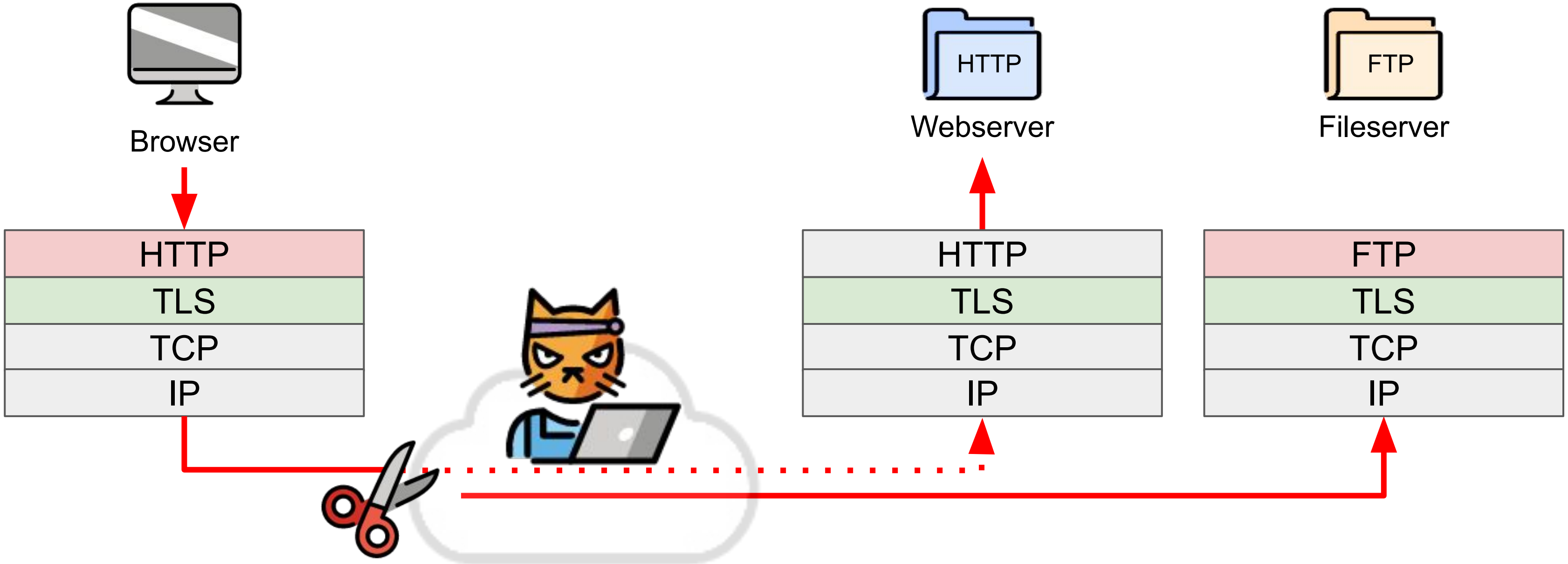
TLS Is Application Independent



TLS-Based Cross-Protocol Attacks



TLS-Based Cross-Protocol Attacks



TLS Server Authentication Has Gaps

Wildcard Certificates

*.bank.com

Multi-Domain Certificates

www.bank.com
ftp.bank.com

Same Hostname

bank.com:443
bank.com:21

Substitute Protocol

Intended Protocol

	HTTP	SMTP	IMAP	POP3	FTP	...
HTTP	-	This work.				

Substitute Protocol

Intended Protocol

	HTTP	SMTP	IMAP	POP3	FTP	...
HTTP	-	This work.				
SMTP		-				
IMAP			-			
POP3				-		
FTP					-	
...						-

Mostly unexplored attack surface

Mostly unexplored attack surface

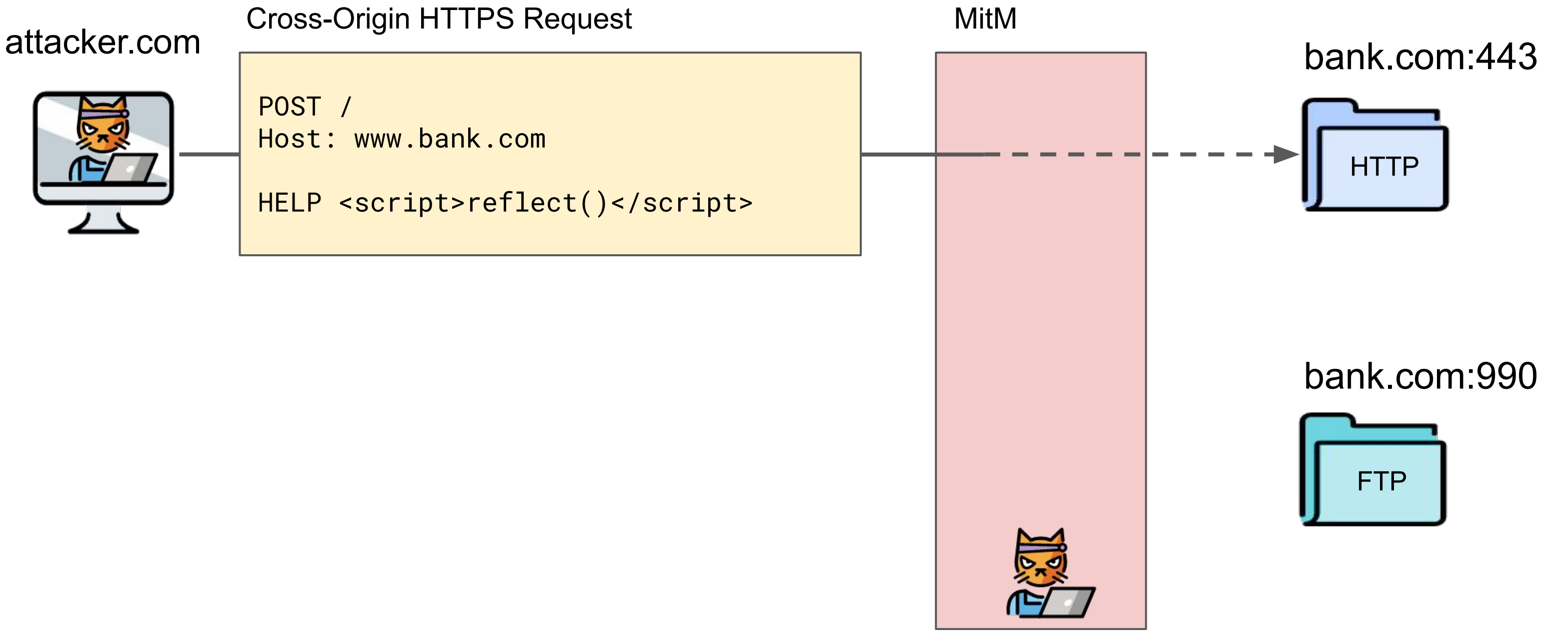
Cross-Protocol Exploit Methods

Reflection

Download

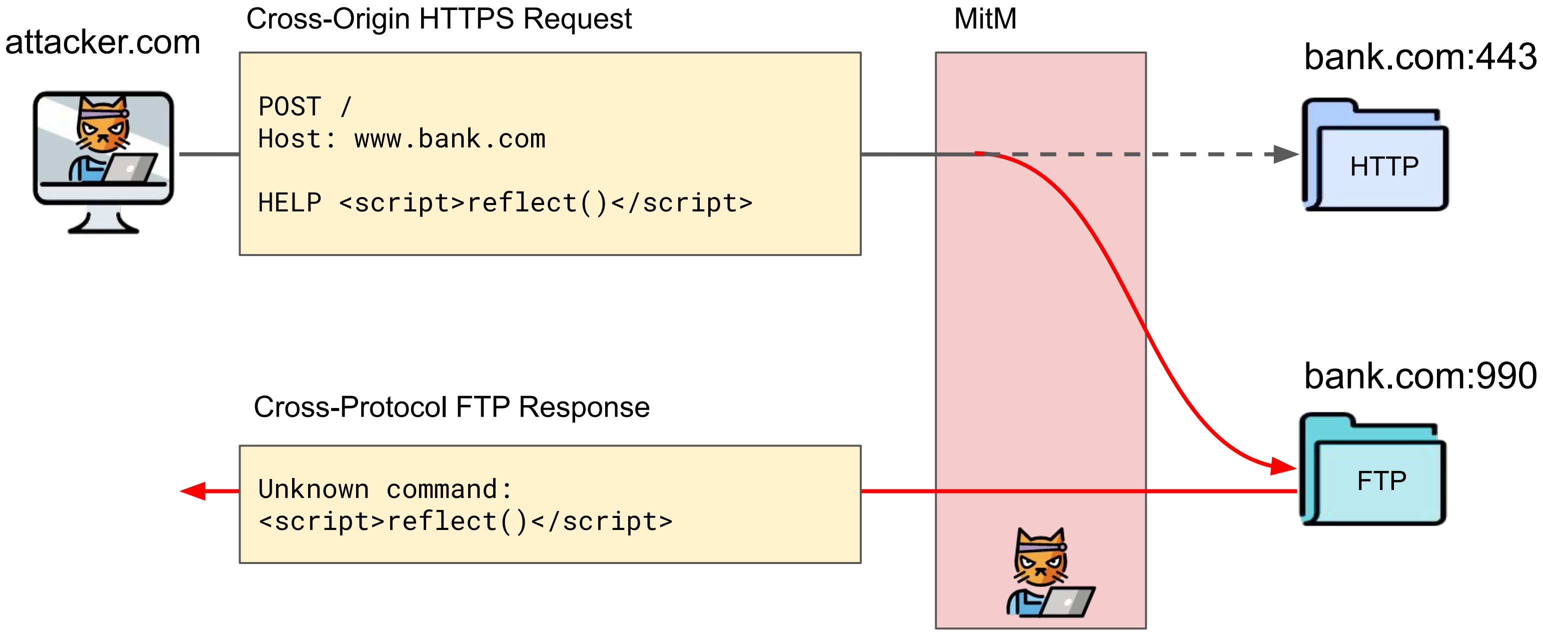
Upload

Reflection Attack on HTTPS Exploiting FTP (Jann Horn, 2015)



```
POST /
Host: www.bank.com

HELP <script>reflect()</script>
```

Reflection Attack on HTTPS Exploiting FTP (Jann Horn, 2015)



attacker.com

Cross-Origin HTTPS Request

```
POST /
Host: www.bank.com

HELP <script>reflect()</script>
```

MitM

bank.com:443

HTTP

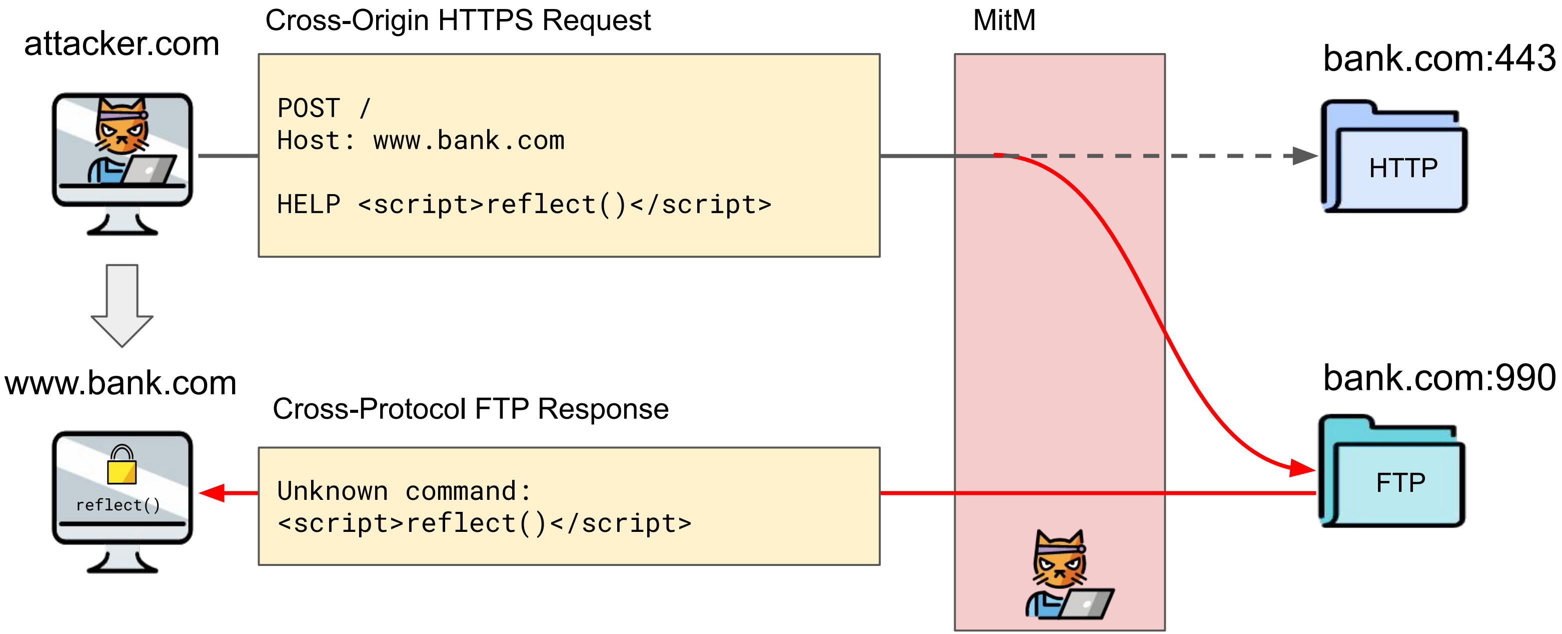
bank.com:990

FTP

Cross-Protocol FTP Response

```
Unknown command:
<script>reflect()</script>
```

Reflection Attack on HTTPS Exploiting FTP (Jann Horn, 2015)



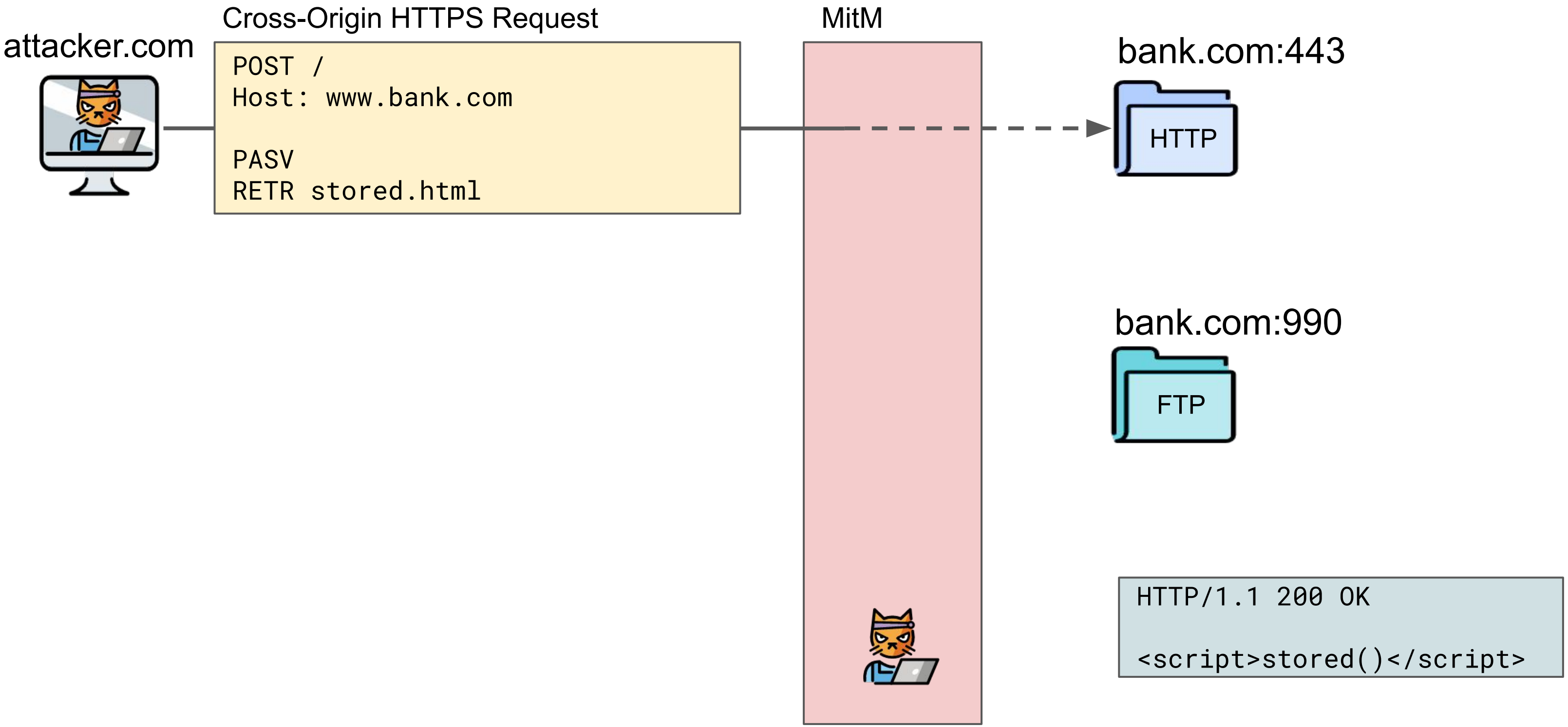
Cross-Origin HTTPS Request

```
POST /
Host: www.bank.com

HELP <script>reflect()</script>
```

Cross-Protocol FTP Response

```
Unknown command:
<script>reflect()</script>
```

Download Attack on HTTPS Exploiting FTP (Jann Horn, 2015)



attacker.com

Cross-Origin HTTPS Request

```
POST /
Host: www.bank.com

PASV
RETR stored.html
```

MitM

bank.com:443

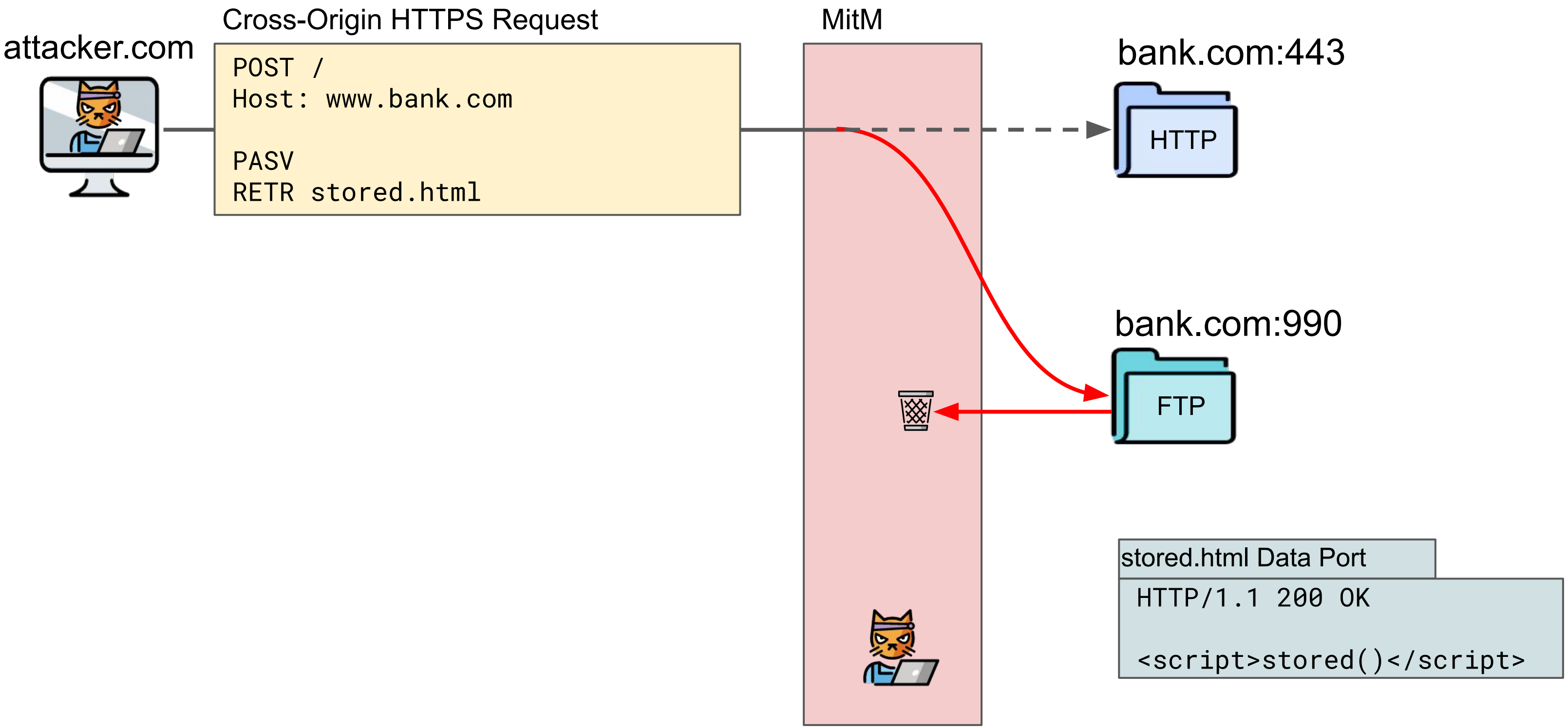
HTTP

bank.com:990

FTP

```
HTTP/1.1 200 OK

<script>stored()</script>
```

Download Attack on HTTPS Exploiting FTP (Jann Horn, 2015)



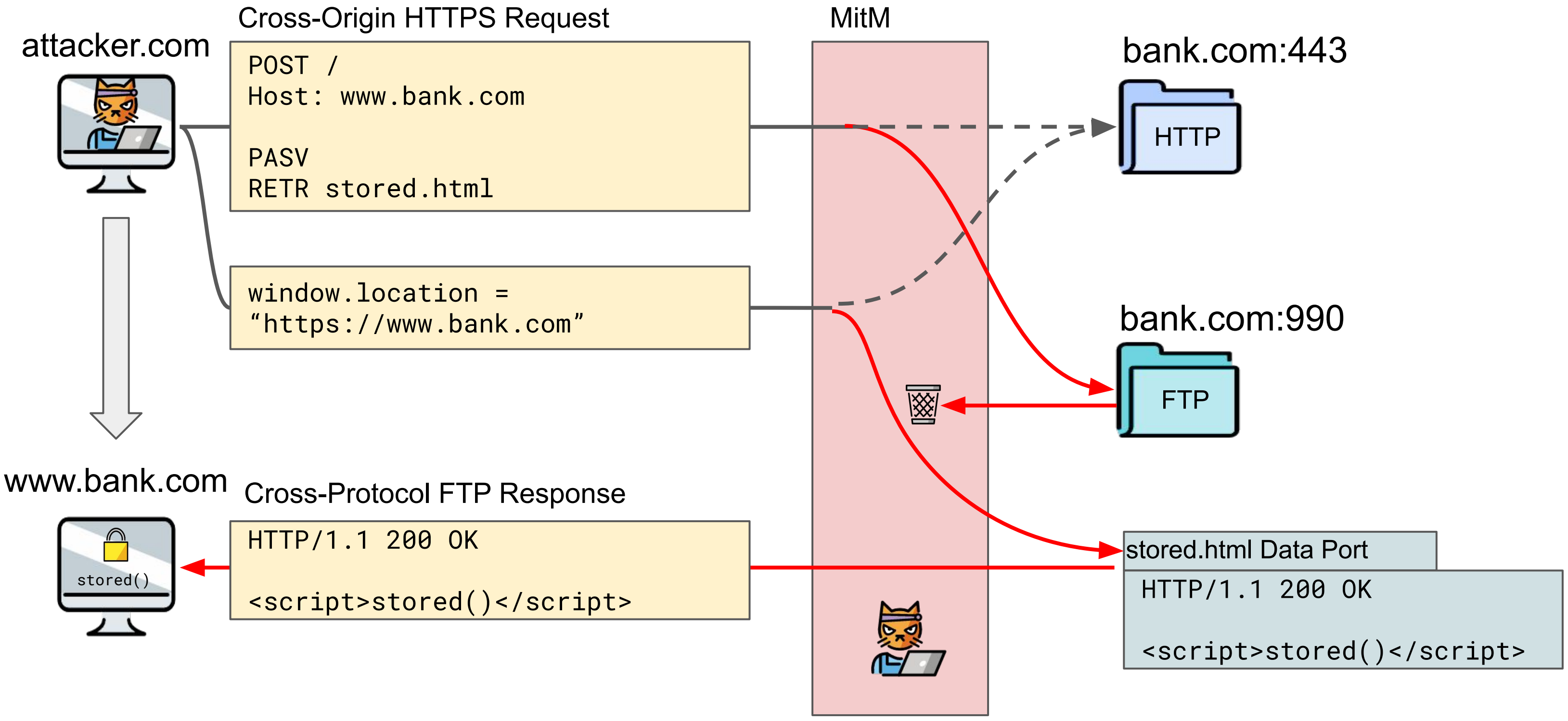
Cross-Origin HTTPS Request

```
POST /
Host: www.bank.com

PASV
RETR stored.html
```

stored.html Data Port

```
HTTP/1.1 200 OK

<script>stored()</script>
```

Download Attack on HTTPS Exploiting FTP (Jann Horn, 2015)



attacker.com

Cross-Origin HTTPS Request

```
POST /
Host: www.bank.com

PASV
RETR stored.html
```

```
window.location =
“https://www.bank.com”
```

MitM

bank.com:443

HTTP

bank.com:990

FTP

www.bank.com

stored()

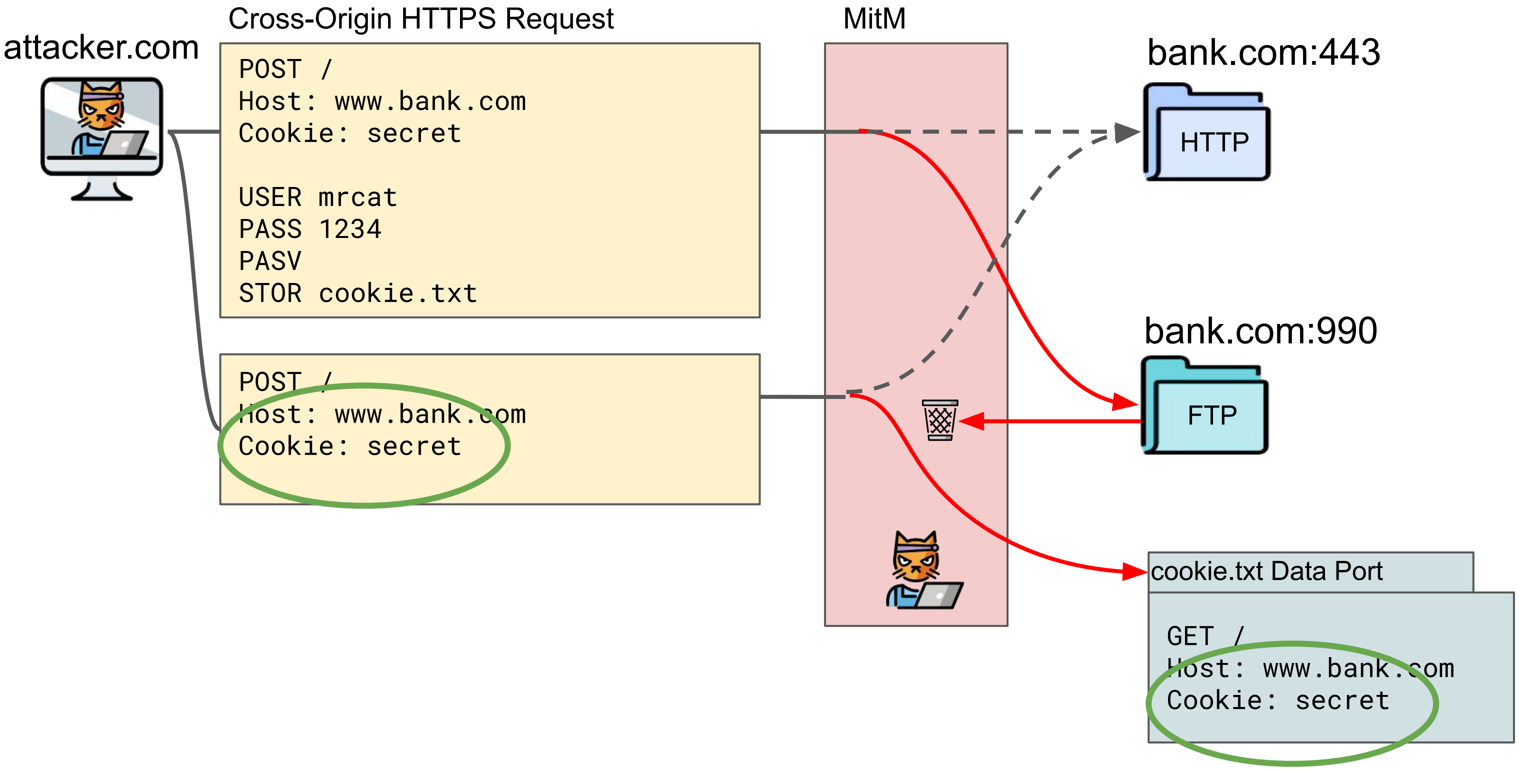
Cross-Protocol FTP Response

```
HTTP/1.1 200 OK

<script>stored()</script>
```

stored.html Data Port

```
HTTP/1.1 200 OK

<script>stored()</script>
```

Upload Attack on HTTPS Exploiting FTP



```
POST /
Host: www.bank.com
Cookie: secret

USER mrcat
PASS 1234
PASV
STOR cookie.txt
```

```
POST /
Host: www.bank.com
Cookie: secret
```

```
GET /
Host: www.bank.com
Cookie: secret
```

Exploit Methods and Protocols

		Application Protocol			
		FTP	SMTP	IMAP	POP3
Exploit Method	Upload	✓	✓	✓	✗
	Download	✓	✗	✓	✓
	Reflection	✓	✓	✓	✓

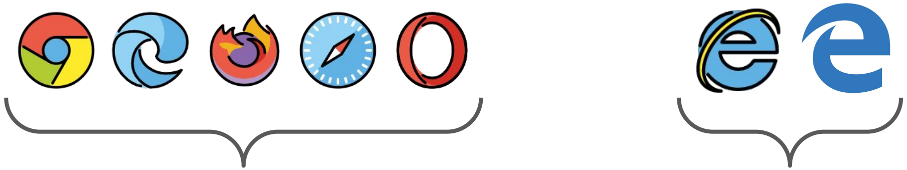
Research Questions

Are cross-protocol attacks still possible today?

How many servers are affected by cross-protocol attacks?

How can cross-protocol attacks be prevented?

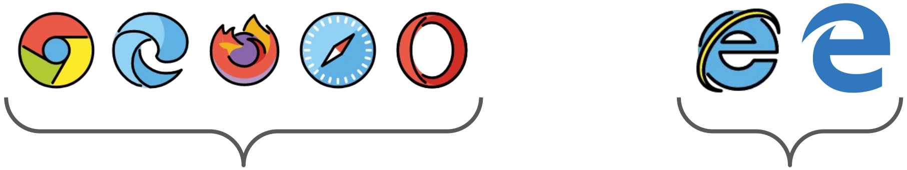
Evaluation of Browsers and Servers



- FTP Upload Attack
- FTP Download Attack

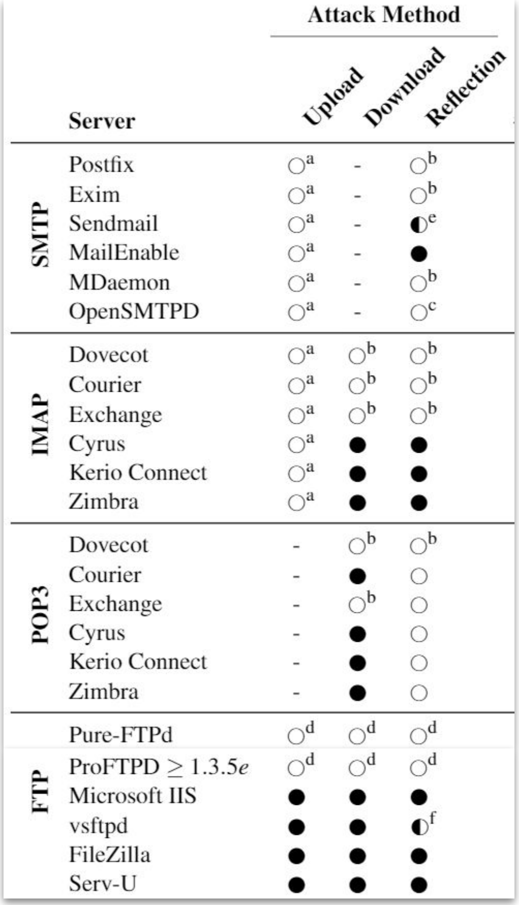
- All exploit methods.

Evaluation of Browsers and Servers



- FTP Upload Attack
- FTP Download Attack

- All exploit methods.



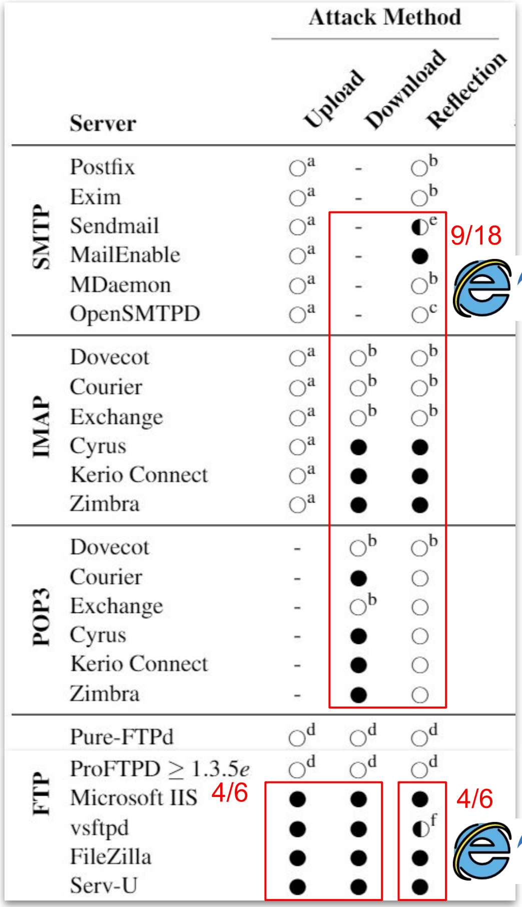
		Attack Method		
	Server	Upload	Download	Reflection
SMTP	Postfix	○[a]	-	○[b]
	Exim	○[a]	-	○[b]
	Sendmail	○[a]	-	◐[e]
	MailEnable	○[a]	-	●
	MDaemon	○[a]	-	○[b]
	OpenSMTPD	○[a]	-	○[c]
IMAP	Dovecot	○[a]	○[b]	○[b]
	Courier	○[a]	○[b]	○[b]
	Exchange	○[a]	○[b]	○[b]
	Cyrus	○[a]	●	●
	Kerio Connect	○[a]	●	●
	Zimbra	○[a]	●	●
POP3	Dovecot	-	○[b]	○[b]
	Courier	-	●	○
	Exchange	-	○[b]	○
	Cyrus	-	●	○
	Kerio Connect	-	●	○
	Zimbra	-	●	○
FTP	Pure-FTPd	○[d]	○[d]	○[d]
	ProFTPD $\geq 1.3.5e$	○[d]	○[d]	○[d]
	Microsoft IIS	●	●	●
	vsftpd	●	●	◐[f]
	FileZilla	●	●	●
	Serv-U	●	●	●

Evaluation of Browsers and Servers

- FTP Upload Attack
- FTP Download Attack

- All exploit methods.

13 out of 24 application servers can be exploited for at least one HTTPS cross-protocol attack method with at least one browser.



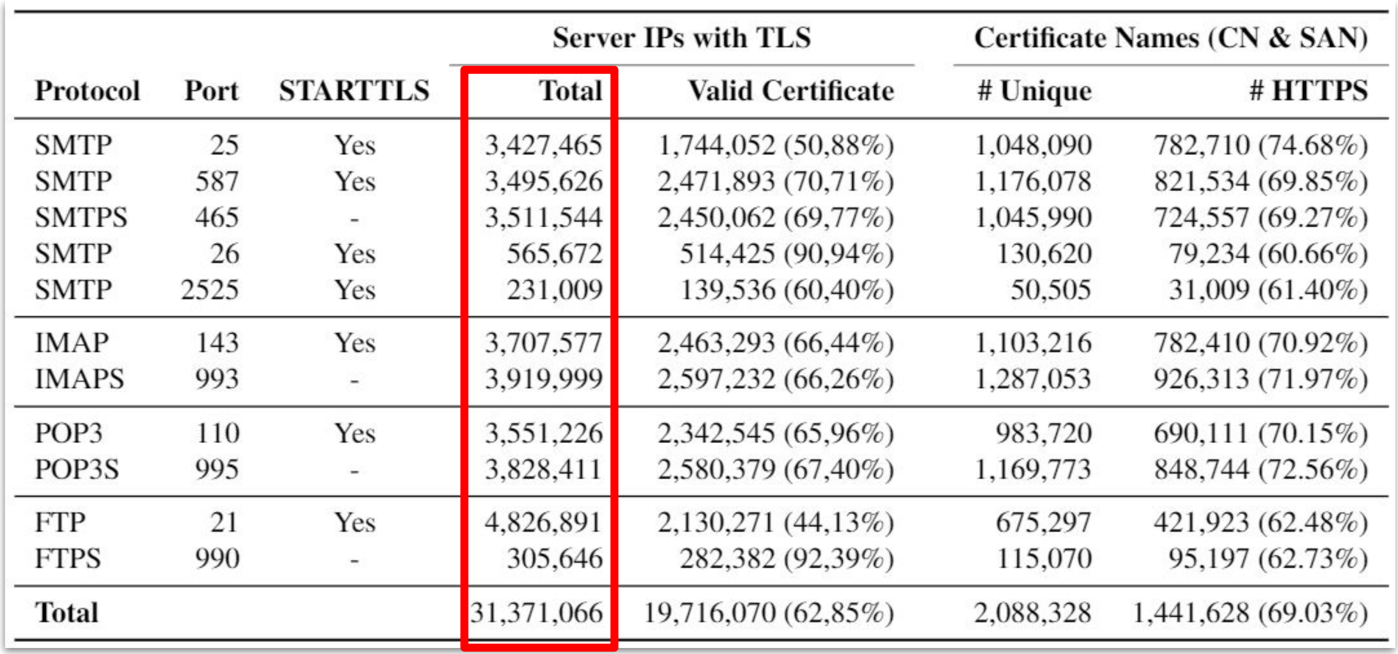
	Server	Attack Method Upload	 Download	 Reflection
SMTP	Postfix	○[a]	-	○[b]
	Exim	○[a]	-	○[b]
	Sendmail	○[a]	-	◐[e]
	MailEnable	○[a]	-	●
	MDaemon	○[a]	-	○[b]
	OpenSMTPD	○[a]	-	○[c]
IMAP	Dovecot	○[a]	○[b]	○[b]
	Courier	○[a]	○[b]	○[b]
	Exchange	○[a]	○[b]	○[b]
	Cyrus	○[a]	●	●
	Kerio Connect	○[a]	●	●
	Zimbra	○[a]	●	●
POP3	Dovecot	-	○[b]	○[b]
	Courier	-	●	○
	Exchange	-	○[b]	○
	Cyrus	-	●	○
	Kerio Connect	-	●	○
	Zimbra	-	●	○
FTP	Pure-FTPd	○[d]	○[d]	○[d]
	ProFTPD $\geq$ 1.3.5*e*	○[d]	○[d]	○[d]
	Microsoft IIS	●	●	●
	vsftpd	●	●	◐[f]
	FileZilla	●	●	●
	Serv-U	●	●	●

9/18

4/6

4/6

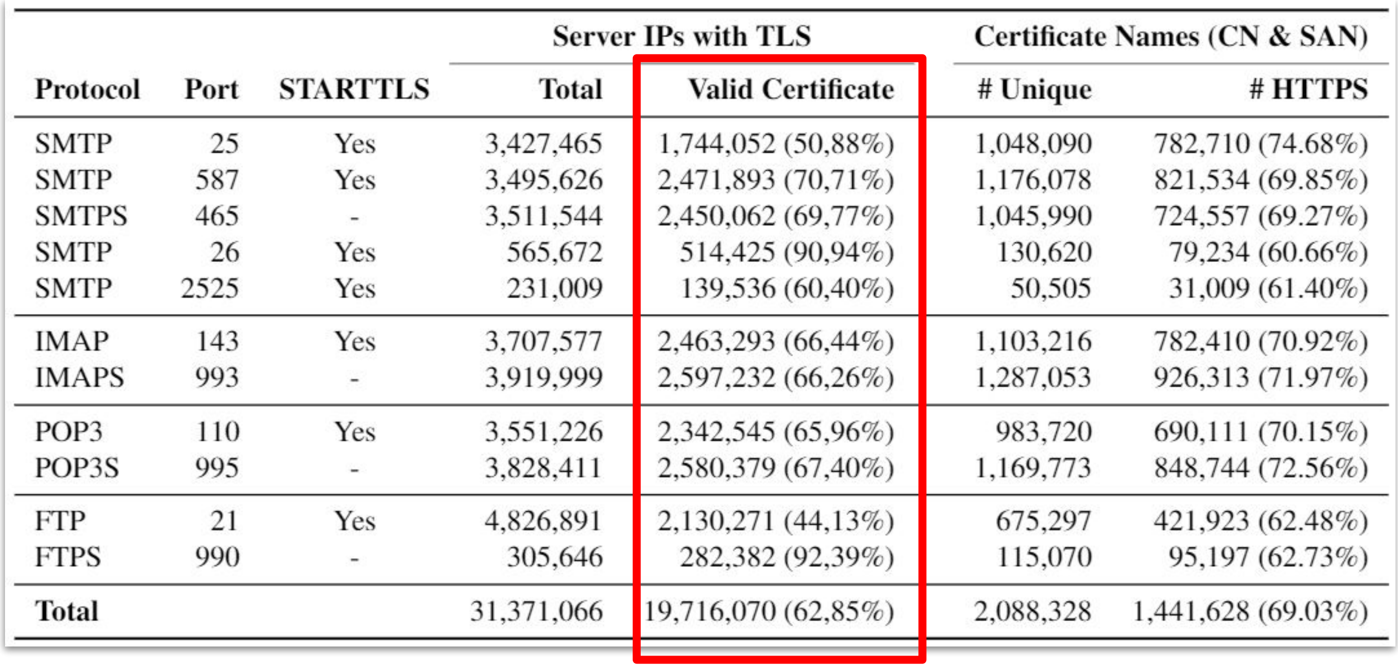
Internet-Wide Scan for Vulnerable Web Servers



			Server IPs with TLS		Certificate Names (CN & SAN)	
Protocol	**Port**	**STARTTLS**	**Total**	**Valid Certificate**	**# Unique**	**# HTTPS**
SMTP	25	Yes	3,427,465	1,744,052 (50,88%)	1,048,090	782,710 (74.68%)
SMTP	587	Yes	3,495,626	2,471,893 (70,71%)	1,176,078	821,534 (69.85%)
SMTPS	465	-	3,511,544	2,450,062 (69,77%)	1,045,990	724,557 (69.27%)
SMTP	26	Yes	565,672	514,425 (90,94%)	130,620	79,234 (60.66%)
SMTP	2525	Yes	231,009	139,536 (60,40%)	50,505	31,009 (61.40%)
IMAP	143	Yes	3,707,577	2,463,293 (66,44%)	1,103,216	782,410 (70.92%)
IMAPS	993	-	3,919,999	2,597,232 (66,26%)	1,287,053	926,313 (71.97%)
POP3	110	Yes	3,551,226	2,342,545 (65,96%)	983,720	690,111 (70.15%)
POP3S	995	-	3,828,411	2,580,379 (67,40%)	1,169,773	848,744 (72.56%)
FTP	21	Yes	4,826,891	2,130,271 (44,13%)	675,297	421,923 (62.48%)
FTPS	990	-	305,646	282,382 (92,39%)	115,070	95,197 (62.73%)
Total			31,371,066	19,716,070 (62,85%)	2,088,328	1,441,628 (69.03%)

Total number of application servers with TLS support (IPv4).

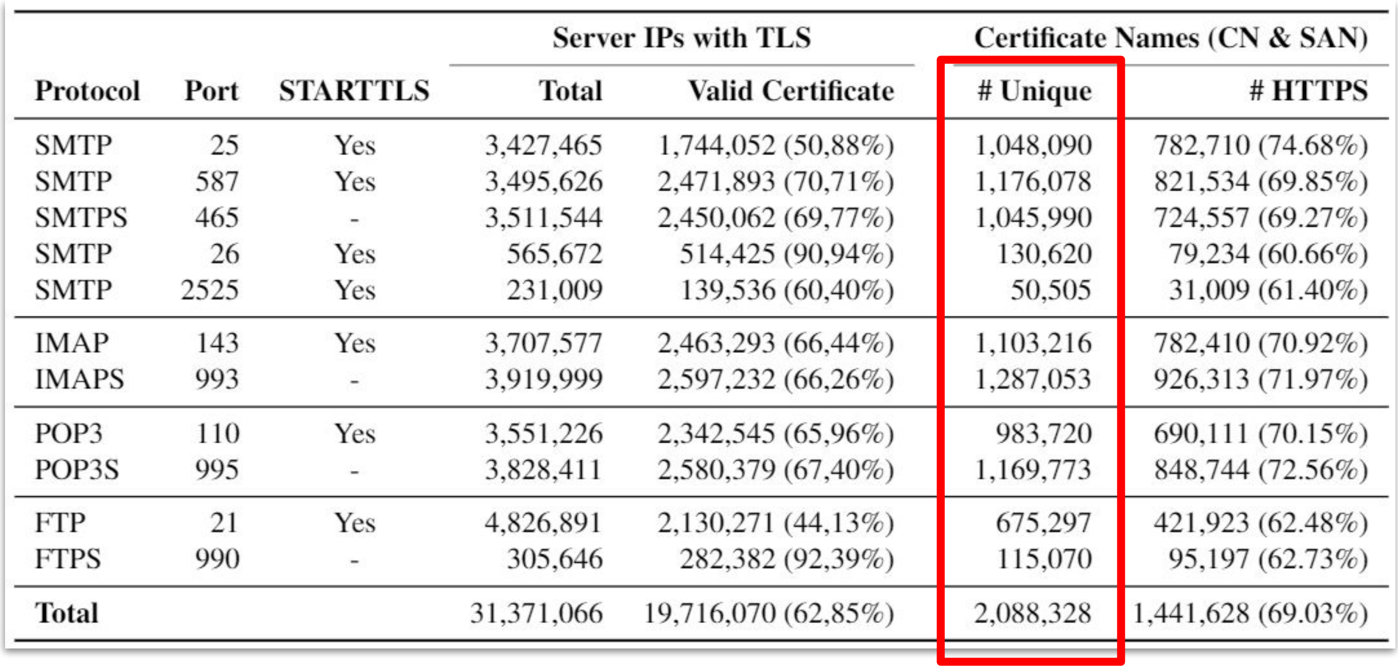
Internet-Wide Scan for Vulnerable Web Servers



			Server IPs with TLS		Certificate Names (CN & SAN)	
Protocol	**Port**	**STARTTLS**	**Total**	**Valid Certificate**	**# Unique**	**# HTTPS**
SMTP	25	Yes	3,427,465	1,744,052 (50,88%)	1,048,090	782,710 (74.68%)
SMTP	587	Yes	3,495,626	2,471,893 (70,71%)	1,176,078	821,534 (69.85%)
SMTPS	465	-	3,511,544	2,450,062 (69,77%)	1,045,990	724,557 (69.27%)
SMTP	26	Yes	565,672	514,425 (90,94%)	130,620	79,234 (60.66%)
SMTP	2525	Yes	231,009	139,536 (60,40%)	50,505	31,009 (61.40%)
IMAP	143	Yes	3,707,577	2,463,293 (66,44%)	1,103,216	782,410 (70.92%)
IMAPS	993	-	3,919,999	2,597,232 (66,26%)	1,287,053	926,313 (71.97%)
POP3	110	Yes	3,551,226	2,342,545 (65,96%)	983,720	690,111 (70.15%)
POP3S	995	-	3,828,411	2,580,379 (67,40%)	1,169,773	848,744 (72.56%)
FTP	21	Yes	4,826,891	2,130,271 (44,13%)	675,297	421,923 (62.48%)
FTPS	990	-	305,646	282,382 (92,39%)	115,070	95,197 (62.73%)
Total			31,371,066	19,716,070 (62,85%)	2,088,328	1,441,628 (69.03%)

Total number of application servers with valid certificates accepted by a browser.

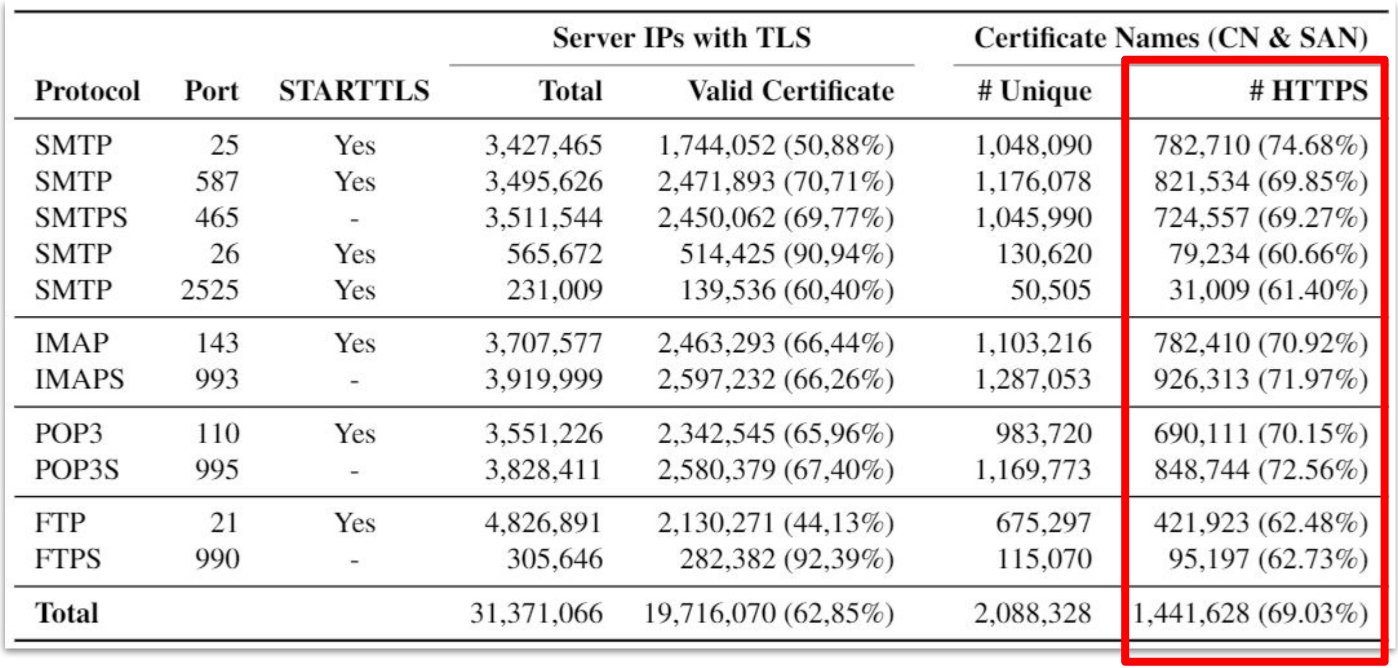
Internet-Wide Scan for Vulnerable Web Servers



			Server IPs with TLS		Certificate Names (CN & SAN)	
Protocol	**Port**	**STARTTLS**	**Total**	**Valid Certificate**	**# Unique**	**# HTTPS**
SMTP	25	Yes	3,427,465	1,744,052 (50,88%)	1,048,090	782,710 (74.68%)
SMTP	587	Yes	3,495,626	2,471,893 (70,71%)	1,176,078	821,534 (69.85%)
SMTPS	465	-	3,511,544	2,450,062 (69,77%)	1,045,990	724,557 (69.27%)
SMTP	26	Yes	565,672	514,425 (90,94%)	130,620	79,234 (60.66%)
SMTP	2525	Yes	231,009	139,536 (60,40%)	50,505	31,009 (61.40%)
IMAP	143	Yes	3,707,577	2,463,293 (66,44%)	1,103,216	782,410 (70.92%)
IMAPS	993	-	3,919,999	2,597,232 (66,26%)	1,287,053	926,313 (71.97%)
POP3	110	Yes	3,551,226	2,342,545 (65,96%)	983,720	690,111 (70.15%)
POP3S	995	-	3,828,411	2,580,379 (67,40%)	1,169,773	848,744 (72.56%)
FTP	21	Yes	4,826,891	2,130,271 (44,13%)	675,297	421,923 (62.48%)
FTPS	990	-	305,646	282,382 (92,39%)	115,070	95,197 (62.73%)
Total			31,371,066	19,716,070 (62,85%)	2,088,328	1,441,628 (69.03%)

Unique hostnames in all valid certificates, guessing www for *.

Internet-Wide Scan for Vulnerable Web Servers

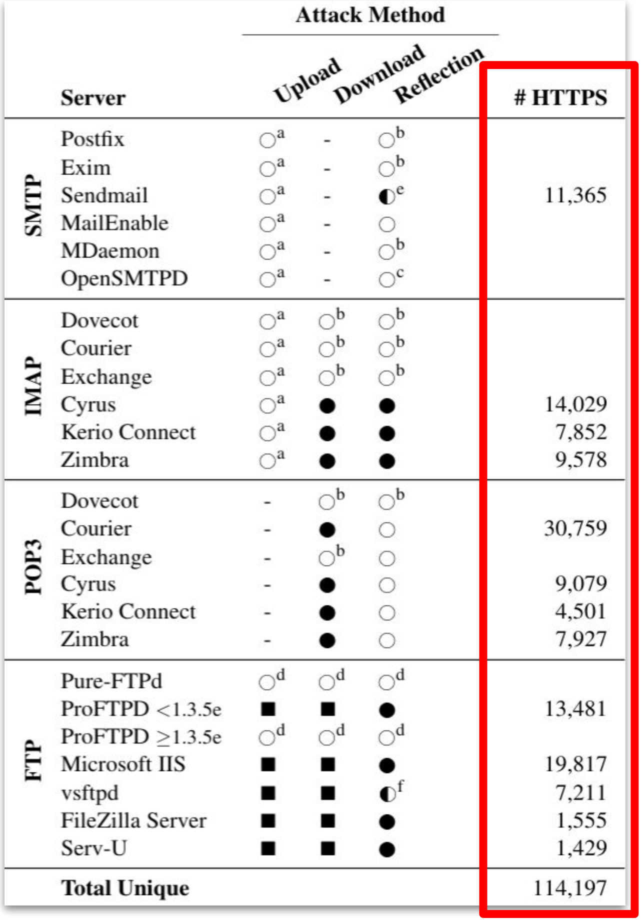


			Server IPs with TLS		Certificate Names (CN & SAN)	
Protocol	Port	STARTTLS	Total	Valid Certificate	# Unique	# HTTPS
SMTP	25	Yes	3,427,465	1,744,052 (50,88%)	1,048,090	782,710 (74.68%)
SMTP	587	Yes	3,495,626	2,471,893 (70,71%)	1,176,078	821,534 (69.85%)
SMTPS	465	-	3,511,544	2,450,062 (69,77%)	1,045,990	724,557 (69.27%)
SMTP	26	Yes	565,672	514,425 (90,94%)	130,620	79,234 (60.66%)
SMTP	2525	Yes	231,009	139,536 (60,40%)	50,505	31,009 (61.40%)
IMAP	143	Yes	3,707,577	2,463,293 (66,44%)	1,103,216	782,410 (70.92%)
IMAPS	993	-	3,919,999	2,597,232 (66,26%)	1,287,053	926,313 (71.97%)
POP3	110	Yes	3,551,226	2,342,545 (65,96%)	983,720	690,111 (70.15%)
POP3S	995	-	3,828,411	2,580,379 (67,40%)	1,169,773	848,744 (72.56%)
FTP	21	Yes	4,826,891	2,130,271 (44,13%)	675,297	421,923 (62.48%)
FTPS	990	-	305,646	282,382 (92,39%)	115,070	95,197 (62.73%)
Total			31,371,066	19,716,070 (62,85%)	2,088,328	1,441,628 (69.03%)

1.4M web servers are vulnerable to a general TLS cross-protocol attack with at least one application server.

Vulnerable Web Servers with Exploitable Application Servers

114,197 web servers can be attacked with at least one exploitable application server.



		Attack Method			
	Server	Upload	Download	Reflection	# HTTPS
SMTP	Postfix	○[a]	-	○[b]	
	Exim	○[a]	-	○[b]	
	Sendmail	○[a]	-	◐[e]	11,365
	MailEnable	○[a]	-	○	
	MDaemon	○[a]	-	○[b]	
	OpenSMTPD	○[a]	-	○[c]	
IMAP	Dovecot	○[a]	○[b]	○[b]	
	Courier	○[a]	○[b]	○[b]	
	Exchange	○[a]	○[b]	○[b]	
	Cyrus	○[a]	●	●	14,029
	Kerio Connect	○[a]	●	●	7,852
	Zimbra	○[a]	●	●	9,578
POP3	Dovecot	-	○[b]	○[b]	
	Courier	-	●	○	30,759
	Exchange	-	○[b]	○	
	Cyrus	-	●	○	9,079
	Kerio Connect	-	●	○	4,501
	Zimbra	-	●	○	7,927
FTP	Pure-FTPd	○[d]	○[d]	○[d]	
	ProFTPD <1.3.5e	■	■	●	13,481
	ProFTPD ≥1.3.5e	○[d]	○[d]	○[d]	
	Microsoft IIS	■	■	●	19,817
	vsftpd	■	■	◐[f]	7,211
	FileZilla Server	■	■	●	1,555
	Serv-U	■	■	●	1,429
	Total Unique				114,197

Application Layer Countermeasures

Detect Protocols

```
◂ 220 smtp.bank.com ESMTP
Postfix
▸ GET /
◂ 221 2.7.0 Error: I can
break rules, too. Goodbye.
Connection closed by
foreign host.
```

Limit Syntax Errors

```
◂ 220 smtp.bank.com ESMTP
Exim
▸ GET /
◂ 500 unrecognized command
▸ Host: bank.com
◂ 500 unrecognized command
▸ Connection: keep-alive
◂ 500 unrecognized command
▸ Cache-Control: max-age=0
◂ 500 Too many
unrecognized commands
Connection closed by
foreign host.
```

Avoid Reflection

```
◂ 220 smtp.bank.com ESMTP
sendmail
▸ <script>alert(1);</script>
◂ 500 5.5.1 Command
unrecognized:
~~“<script>alert(1);</script>”~~
```

Certificate-Based Countermeasures

No Wildcard Certificates

*.bank.com

🚫

No Multi-Domain Certificates

www.bank.com
ftp.bank.com

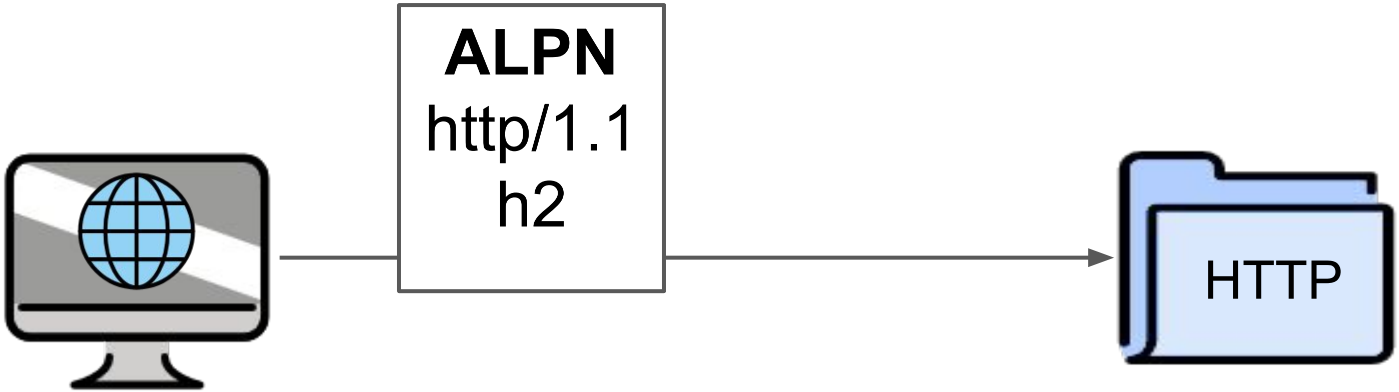
🚫

No Shared Hostnames

bank.com:443
bank.com:21

🚫

Application Layer Protocol Negotiation (ALPN)

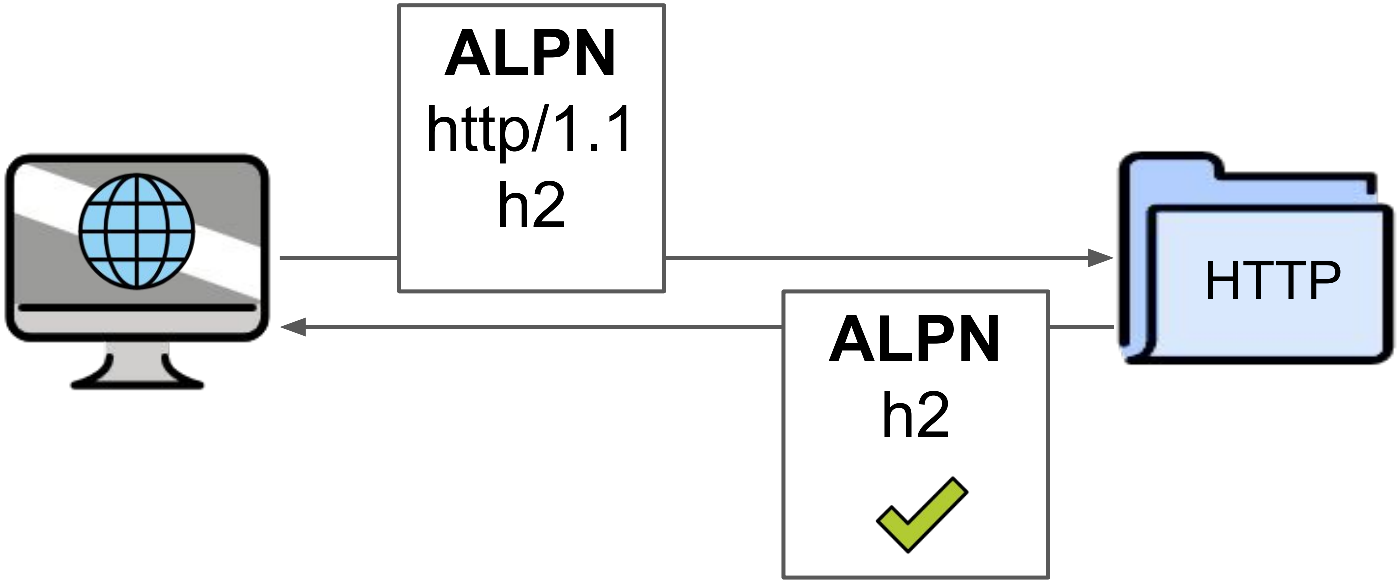


ALPN

http/1.1

h2

Application Layer Protocol Negotiation (ALPN)



ALPN

http/1.1

h2

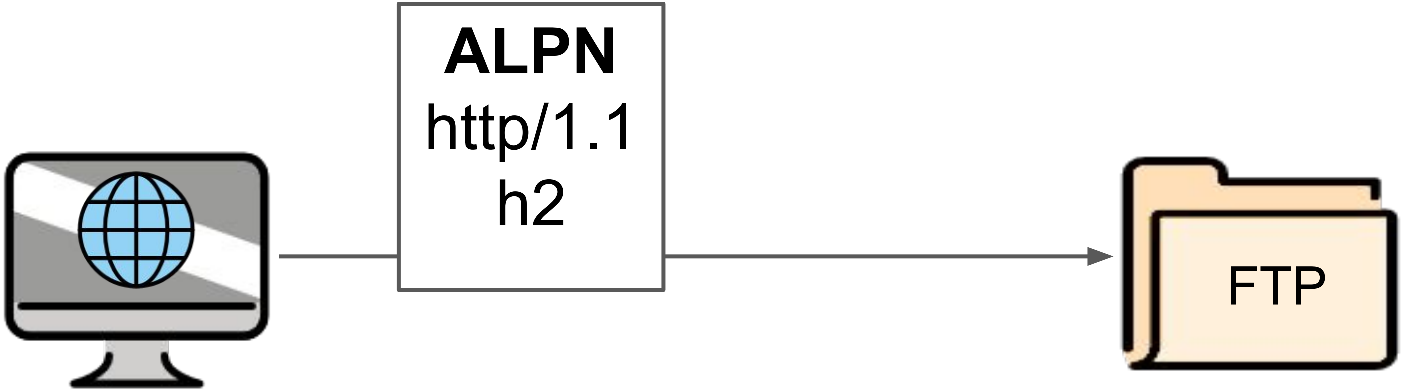
HTTP

ALPN

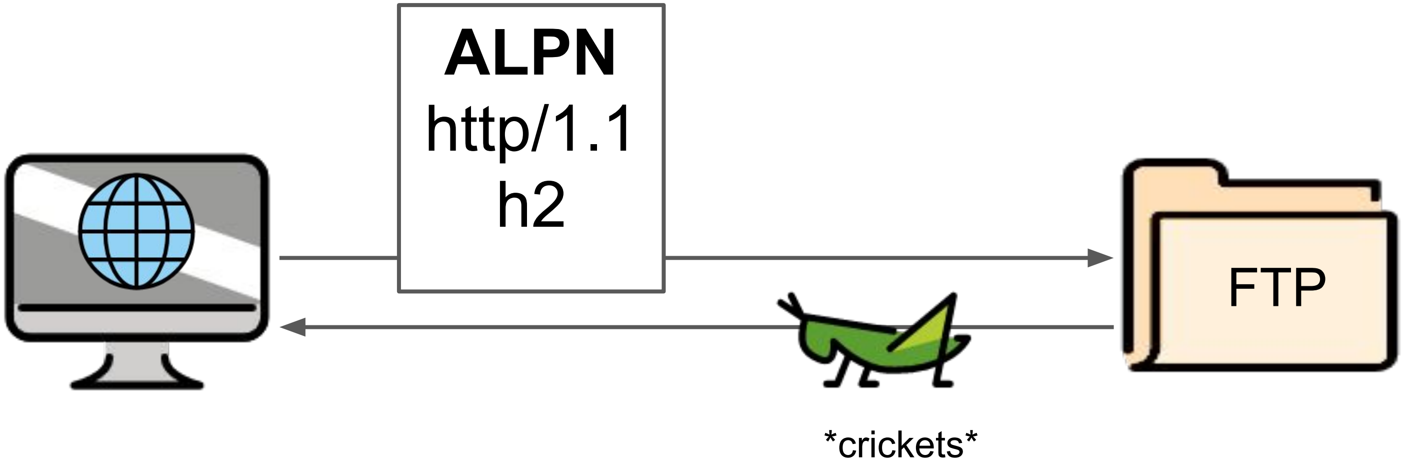
h2

✓

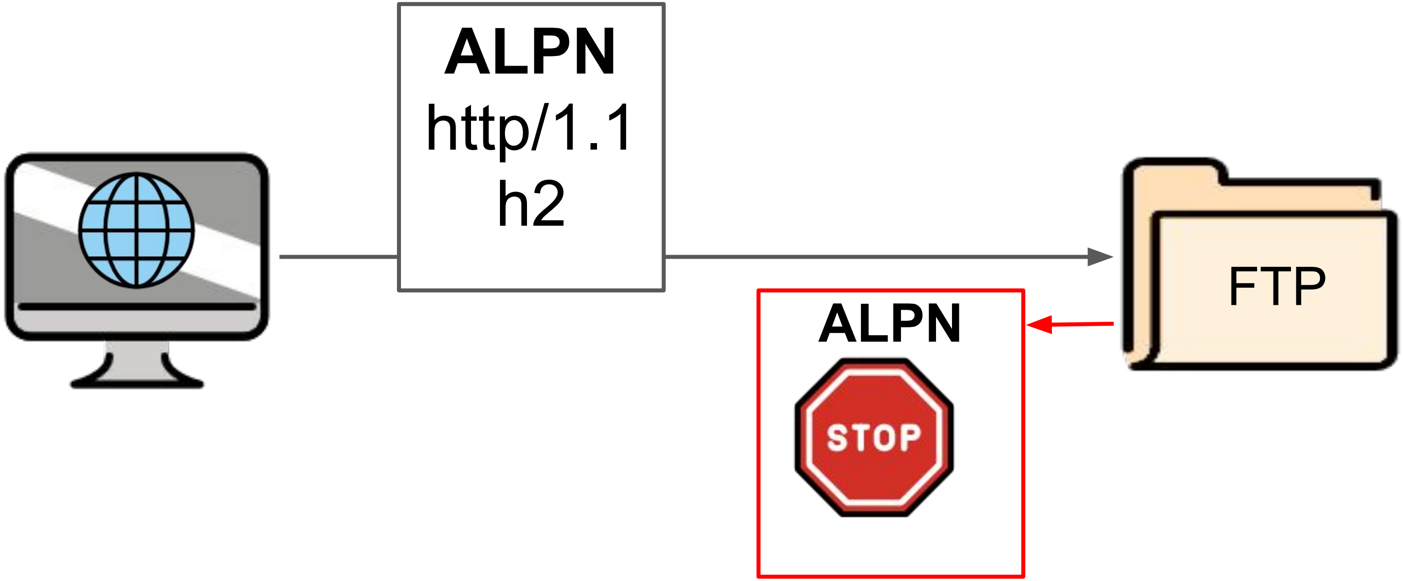
ALPN Is Often Ignored



ALPN Is Often Ignored



Recommended: Strict ALPN Validation



Conclusions

Cross-protocol attacks are still possible today!

We found 114k web servers with an exploitable FTP or Email server.

Strict ALPN and SNI can prevent these attacks.

More cross-protocol attacks?
Binary protocols, DTLS, IPsec, ...

Thank you for listening!
Any questions?

⌂ alpaca-attack.com
🐦 lambdafu
✉ marcus.brinkmann@rub.de