ALPACA: Application Layer Protocol Confusion

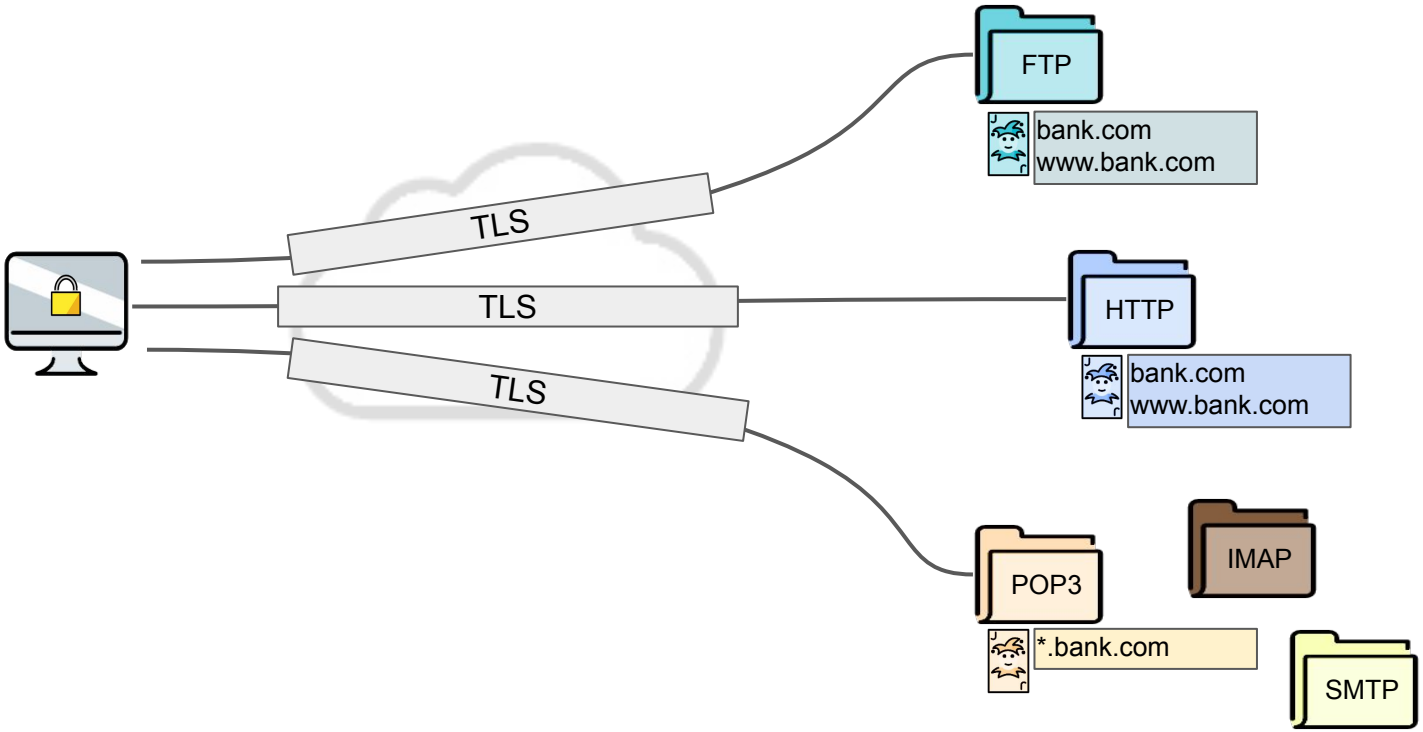
Analyzing and Mitigating Cracks in TLS Authentication

30th USENIX Security Symposium 2021

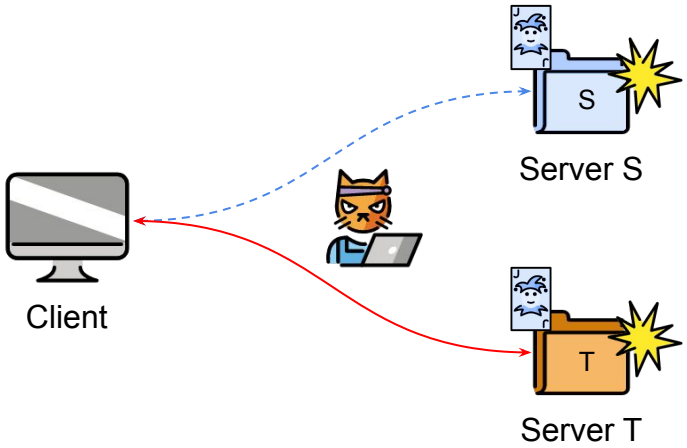
Marcus Brinkmann,[1] Christian Dresen,[2] Robert Merget,[1] Damian Poddebniak,[2] Jens Müller,[1] Juraj Somorovsky,[3] Jörg Schwenk,[1] Sebastian Schinzel[2]

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

TLS Authentication



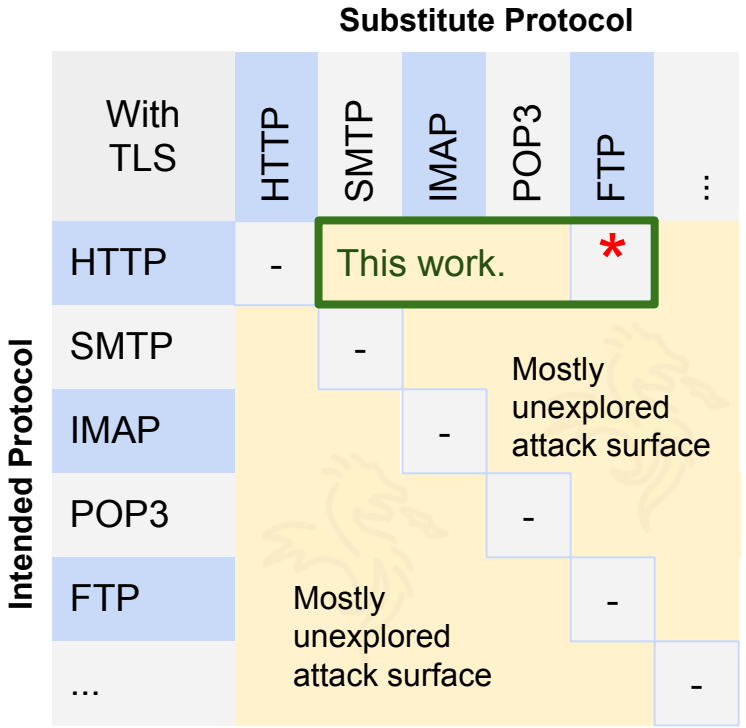
TLS-Based Cross-Protocol Attacks



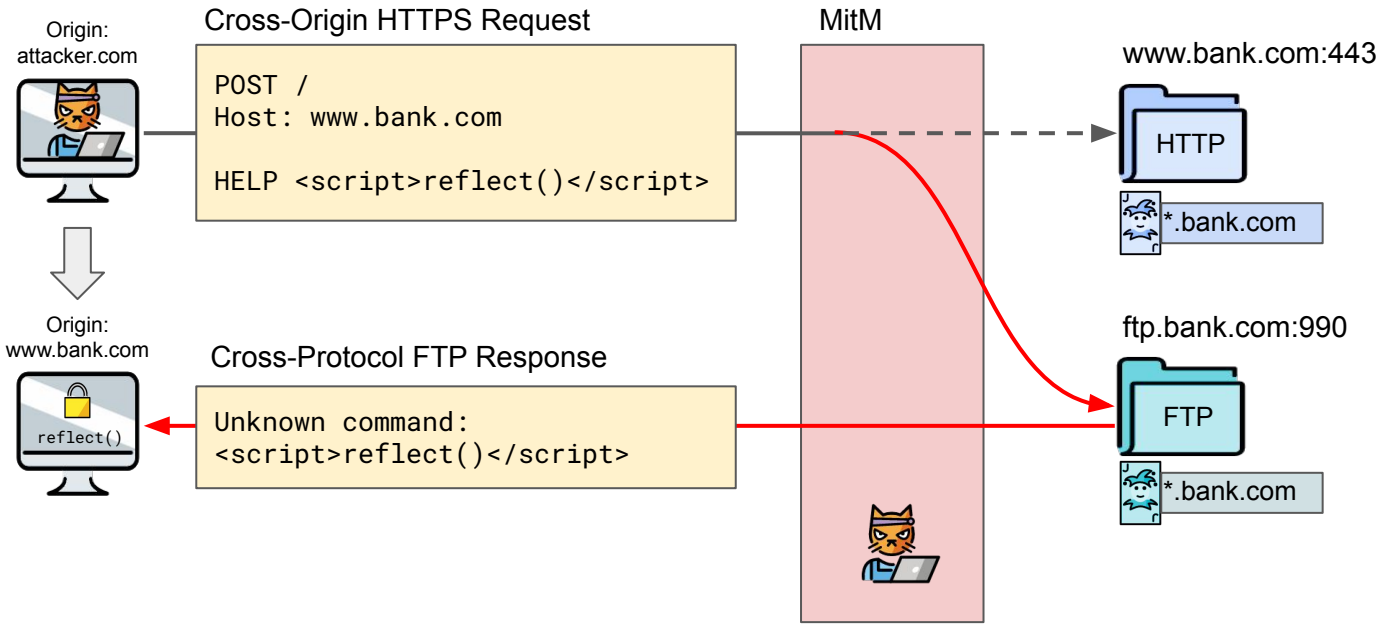
History and Potential of Cross-Protocol Attacks

HTTP (w/o TLS)
Jochen Topf (2001), The HTML Form Protocol Attack

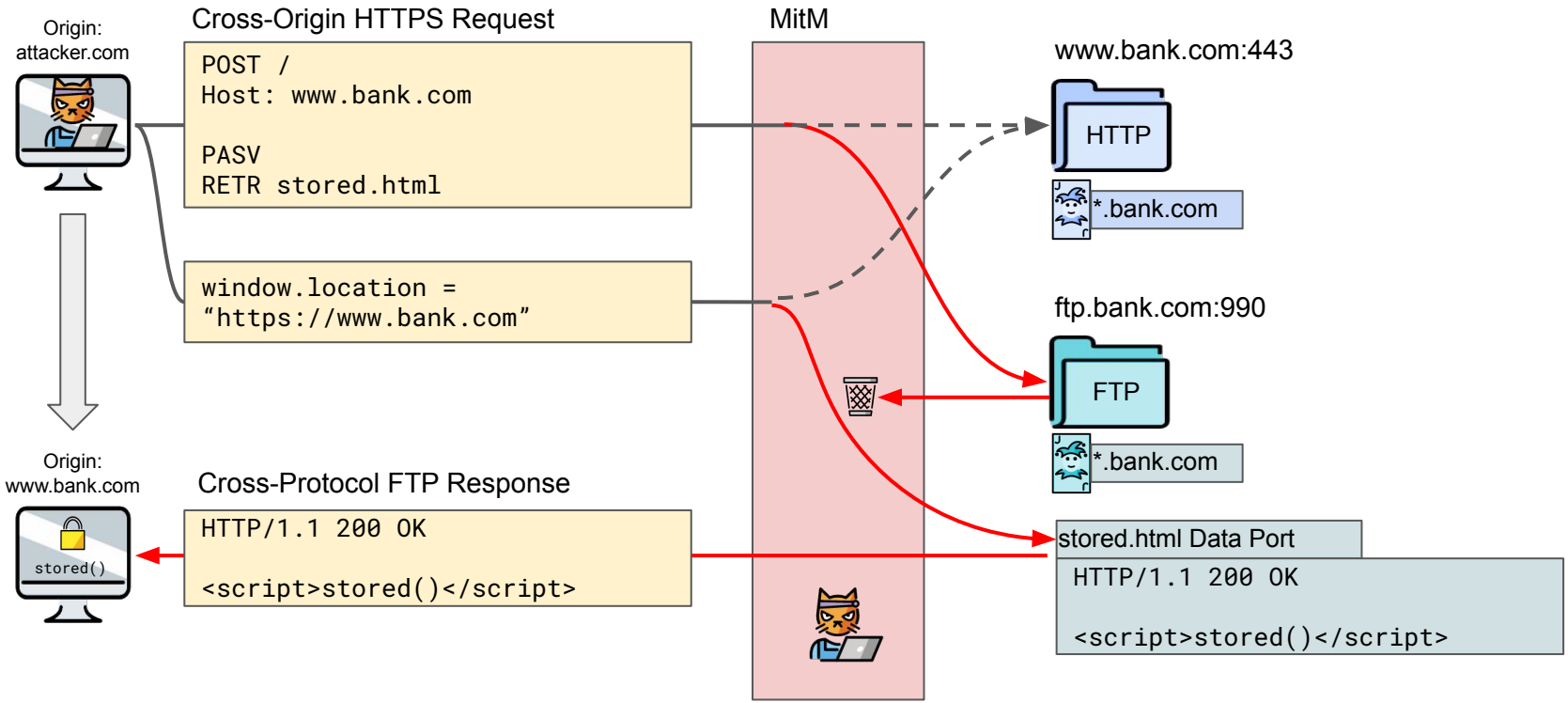
HTTPS (w/ TLS) *
Jann Horn (2015), Two cross-protocol MitM attacks on browsers



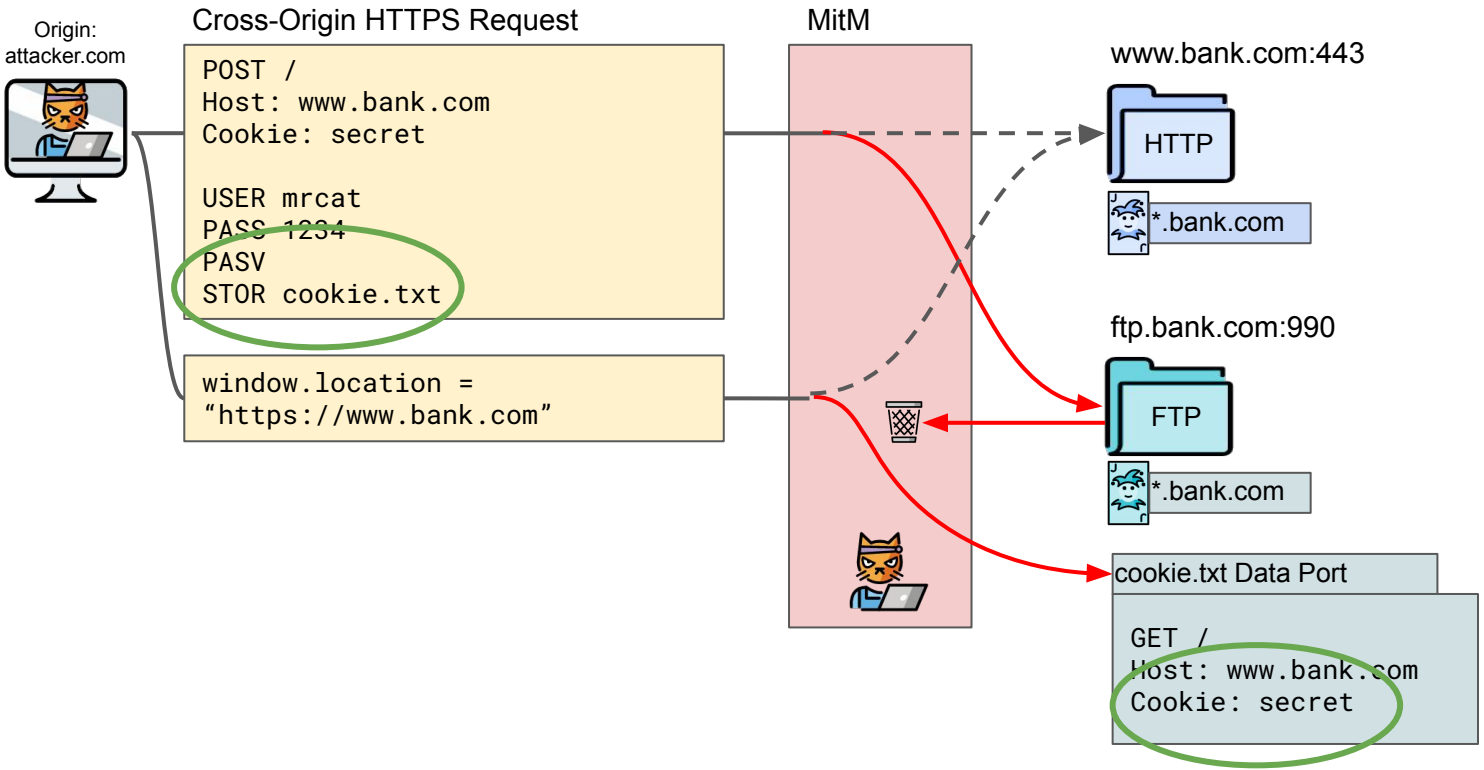
Reflection Attack on HTTPS Exploiting FTP (Jann Horn, 2015)



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



Upload Attack on HTTPS Exploiting FTP



Attack Methods and Protocols

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

Some attacks are also possible in a pure web attacker model (no MitM). See Sec. 8 for details.

Research Questions

Are cross-protocol attacks still possible today?

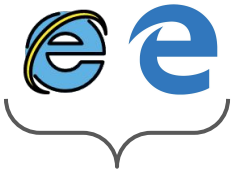
How many servers are affected by cross-protocol attacks?

How can cross-protocol attacks be prevented?

Evaluation of Browsers and Application Servers

Not tolerant to protocol noise.

- FTP Upload Attack
- FTP Download Attack



Tolerant to protocol noise.

- All attack 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]	-	◐[c]
	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 ≥ 1.3.5*e*	○[d]	○[d]	○[d]
	Microsoft IIS	●	●	●
	vsftpd	●	●	◐[f]
	FileZilla	●	●	●
	Serv-U	●	●	●

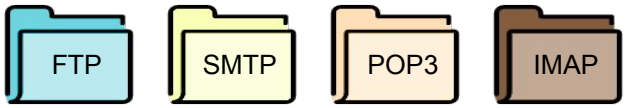
9/18

4/6

4/6

All evaluations, exploits, and proof-of-concept code are in the artifacts to our paper.

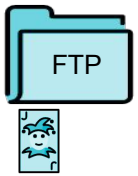
Internet-Wide Scan for Vulnerable Web Servers

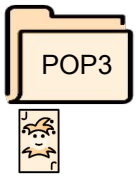


Protocol	Port	STARTTLS	Server IPs with TLS		Certificate Names (CN & SAN)	
			Total	Valid Certificate	# Unique	# HTTPS
SMTP	25	Yes	3,427,465	1,744,052 (50,88%)	1,048,090	782,710 (74.68%)
SMTP	587	Yes	3,495,626	2,471,893 (70,71%)	1,176,078	821,534 (69.85%)
SMTPS	465	-	3,511,544	2,450,062 (69,77%)	1,045,990	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

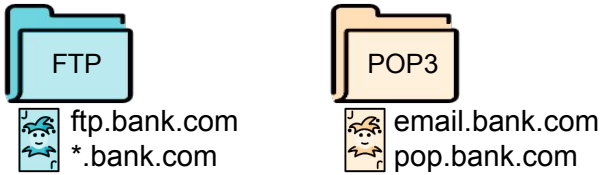




			Server IPs with TLS		Certificate Names (CN & SAN)	
Protocol	**Port**	**STARTTLS**	**Total**	**Valid Certificate**	**# Unique**	**# HTTPS**
SMTP	25	Yes	3,427,465	1,744,052 (50,88%)	1,048,090	782,710 (74.68%)
SMTP	587	Yes	3,495,626	2,471,893 (70,71%)	1,176,078	821,534 (69.85%)
SMTPS	465	-	3,511,544	2,450,062 (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.

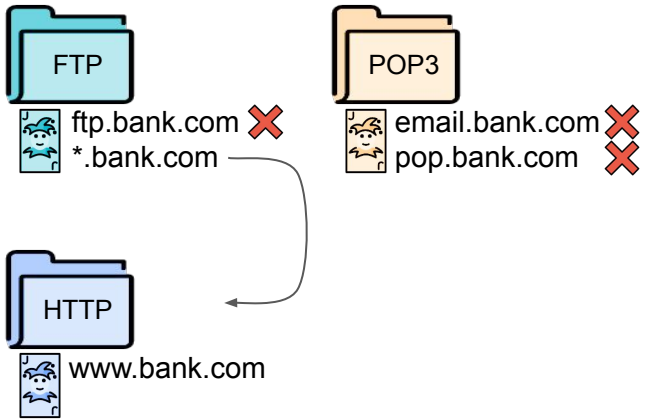
Internet-Wide Scan for Vulnerable Web Servers



Protocol	Port	STARTTLS	Server IPs with TLS		Certificate Names (CN & SAN)	
			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 the Common Name (CN) and Subject Alternative Name (SAN) fields of all valid certificates.

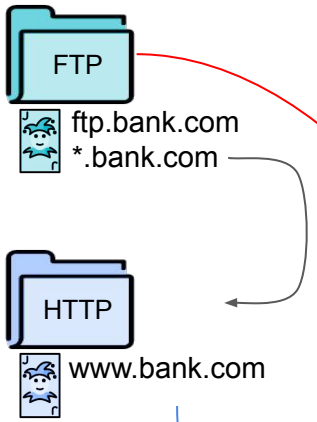
Internet-Wide Scan for Vulnerable Web Servers



			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 web servers on port 443 among unique names (*=www).
1.4M web servers are vulnerable to a general TLS cross-protocol attack with at least one application server (SMTP, IMAP, POP3, or FTP).

Vulnerable Web Servers with Exploitable Application Servers



		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

For the 1.4M web servers, we tried to identify the application servers with a banner scan to see they are exploitable based on our lab eval.

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

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

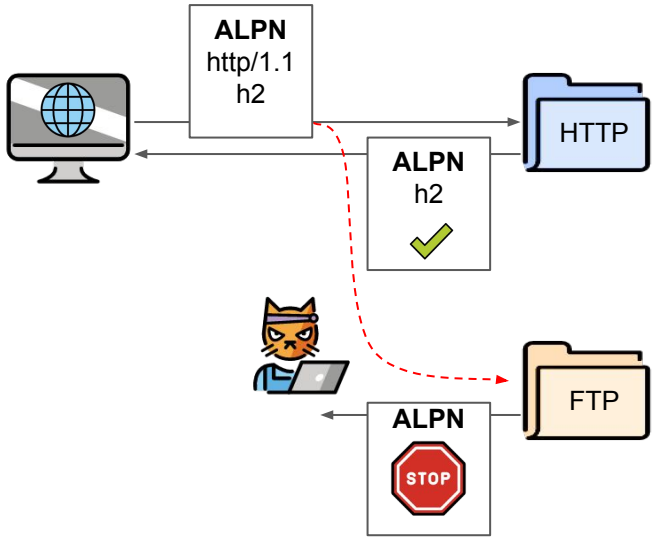
TLS-Based Countermeasures: Application Layer Protocol Negotiation (ALPN)

Server implements strict ALPN:

- It can not be exploited for cross-protocol attacks on clients with ALPN (e.g. browsers).
- It can still accept connections by clients without ALPN (legacy compatibility).

Client and server implement strict ALPN:

- All known and unknown cross-protocol attacks on this connection are prevented.



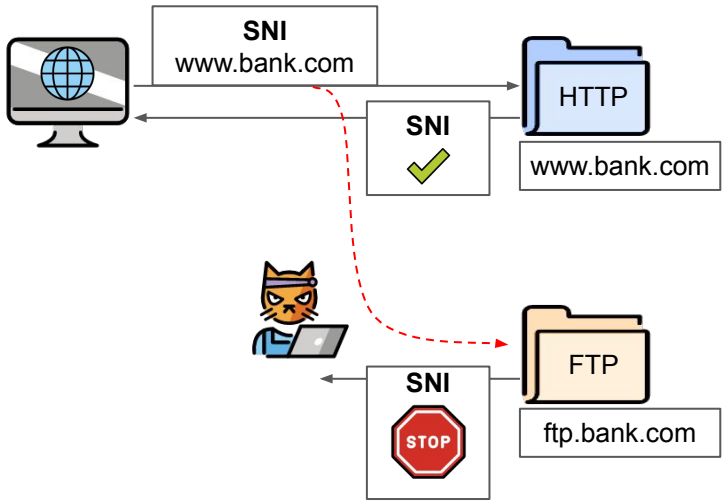
TLS-Based Countermeasures: Server Name Indication (SNI)

Server implements strict SNI:

- Cross-hostname attacks are prevented.

Useful, because servers for different protocols are often located on different hostnames:
www.bank.com vs. ftp.bank.com

Also mitigates some same-protocol host confusion attacks, see Delignat-Lavaud et al. (2015), Zhang et al. (2020).



Conclusions

Implementations of TLS authentication should be extended to prevent cross-protocol attacks.

Deployment of ALPN and SNI countermeasures requires a long-term community effort.

Measurements of the TLS landscape should include ALPN and SNI implementations.

Same-protocol, same-host, cross-port attacks can not be prevented with TLS at the current time.

Future research topics:

- Find more examples for cross-protocol attacks.
- Find similar attacks for other security layers, such as DTLS, IPsec.

Thank you for listening!
Any questions?

alpaca-attack.com
lambdafu
marcus.brinkmann@rub.de