MITM Attacks on HTTPS: Another Perspective

MITM Attacks on HTTPS: Another Perspective - GreenD0g, Slideshare.

- Published: 2017-11-20
- Original: <https://www.slideshare.net/GreenD0g/mitm-attacks-on-https-another-perspective/>
- Current location: <https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614>
- Preserved from: https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614 (live) on 2026-08-09
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

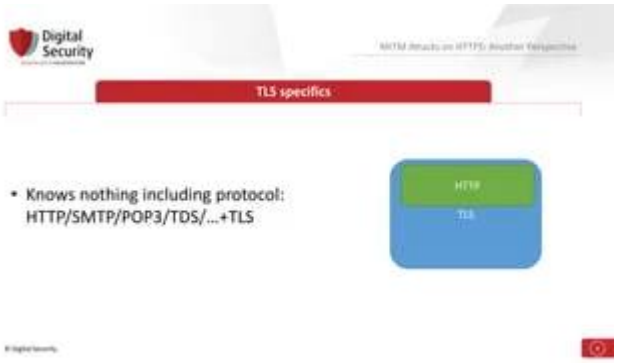
- [1 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#1)
- [2 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#2)
- [3 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#3)
- [4 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#4)
- [5 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#5)
- [6 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#6)
- [7 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#7)
- [8 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#8)
- [9 / 43

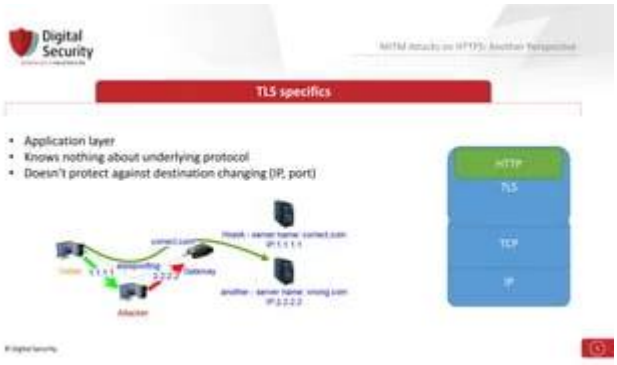
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#9)

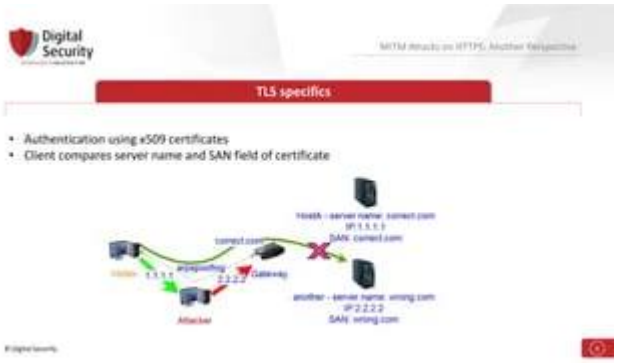
- [10 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#10)
- [11 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#11)
- [12 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#12)
- [13 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#13)
- [14 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#14)
- [15 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#15)
- [16 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#16)
- [17 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#17)
- [18 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#18)
- [19 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#19)
- [20 / 43
](https://www.slideshare.net/slideshow/mitm-attacks-on-https-another-perspective/82373614#20)

![© Digital Security 3 MITM Attacks on HTTPS: Another Perspective HTTPS • TLS (SSL)+ HTTP • Protects against man-in-the-middle attacks • Authentication, Encryption, Integrity – Silver bullet ? • Crypto attacks:

- POODLE, BEAST, CRIME… Hard to exploit](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-3-320.jpg)







Certificates features and limitations

- Doesn't care about port (many services – 1 certificate)
- For a wide range of domain names:
  - Many names in SAN - Subject Alternative Name (+ CN*)
  - Wildcard certificate
- No SNI
- TLS cache **
- HTTP/2 connection sharing**

*Since 58, Chrome doesn't check CN, only SAN (because of RFC)
** http://antoine.delignat-lavaud.fr/doc/www15.pdf

Wildcard names

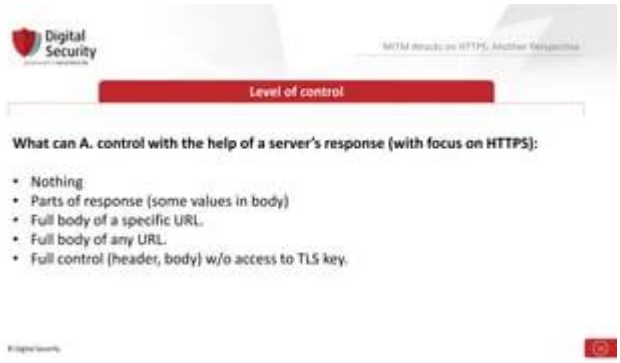
A lot of names in SAN

TLS Redirection

- Group of MitM attacks – misuse of authentication limits and features
- Any protocol
  - Virtual host confusion (http://antoine.delignat-lavaud.fr/doc/www15.pdf)

Simplest example

- **Attacker (A) controls files on HostB**
- A. uploads own new_version.exe on HostB
- Autoupdate on Victim (V) requests a new version of software: https://www.correct.com/new_version.exe
- A. MitMs and redirect to HostB
- Autoupdate downloads and runs A's exe file



![© Digital Security 16 MITM Attacks on HTTPS: Another Perspective Common example – XSS XSS on HostB (Part of body)

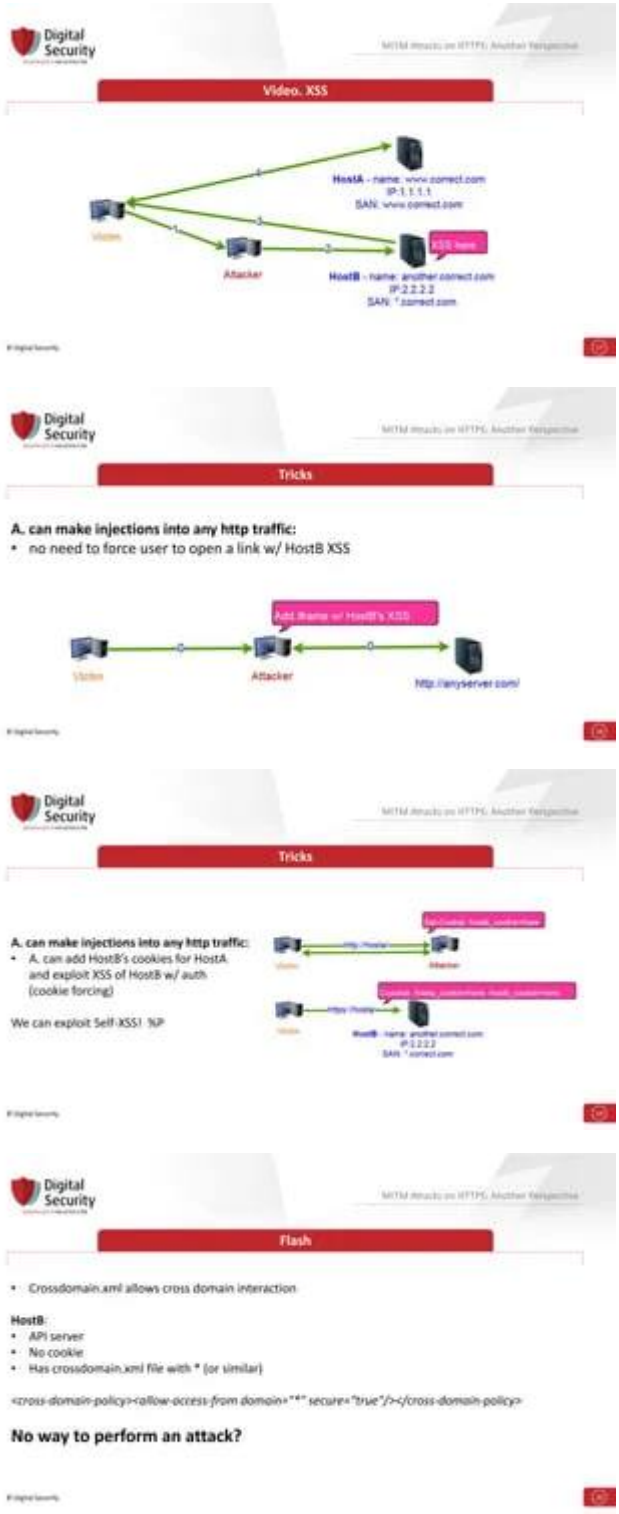
1. V. request to HostA + xss of HostB

https://www.correct.com/xss_of_hostb_here

1. A. MitMs and changes an IP
2. HostB responses with A's JS
3. V. executes JS (context of HostA)
4. A. stops the MitM attack

5. JS can interact with HostA in a usual

way Browser knows nothing about MitM!](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-16-320.jpg)



![© Digital Security 21 MITM Attacks on HTTPS: Another Perspective Flash Crossdomain.xml w/ * on HostB (nothing)

1. V . opens A's swf
2. Swf sends request to HostA
3. Flash checks crossdomain.xml

4. A. MitMs and changes an IP
5. HostB responses w/ crossdomain.xml
6. Swf is allowed to interact w/ HostA
7. A. stops the MitM attack
8. SWF can interact with HostA in a

usual way](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-21-320.jpg)

![© Digital Security 24 MITM Attacks on HTTPS: Another Perspective Cross protocol - IE

1. V. sends the POST request w/ JS payload to “any_url.html on” to

HostA

1. A. MitMs and changes an IP
2. HostB reflects the request
3. IE interprets it as HTTP/0.9
4. “.html” forces IE to parse as html
5. V. executes JS (in the context of HostA)
6. A. stops the MitM attack
7. JS can interact with HostA in a usual way](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-24-320.jpg)

![© Digital Security 26 MITM Attacks on HTTPS: Another Perspective Cross protocol – Other browsers (FF, Chrome) A. wants to steal Basic Auth header or HttpOnly cookie A. has XSS on HostA (can execute JS in it's context) (Nothing)

1. JS sends a request to HostA
2. A. MitMs and changes IP
3. HostB reflects the request

-Browser interprets it as HTTP/0.9, text/plain

- JS is allowed to read response (same origin)](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-26-320.jpg)

![© Digital Security 27 MITM Attacks on HTTPS: Another Perspective JavaScript +DOM Web app w/ JQuery uses load() to get content Text-based service that reflects requests on HostB (Nothing) or file uploading is possible

1. A. sets a cookie w/ xss on HostA (cookie forcing)

Set-Cookie: test=<script src="…">

1. V. opens HostA. Jquery is loaded.
2. For other requests load() is used
3. load sends a request to HostA
4. A. MitMs and changes an IP
5. HostB reflects the request

-Browser interprets it as HTTP/0.9, text/plain

- Jquery.load parses it and execute our XSS payload
- Our JS can interact with HostA in a usual way](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-27-320.jpg)

![© Digital Security 28 MITM Attacks on HTTPS: Another Perspective REST API V. is a web app that checks auth (for 200 OK) using HostA REST API Text-based service that reflects requests on HostB (Nothing) or it returns 200 OK for any requests

1. A. tries to auth on V
2. V. sends request to HostA to check auth
3. A. MitMs and changes an IP
4. HostB reflects all the request
5. Curl interprets it as HTTP/0.9 *

6. Curl returns CURLE_OK
7. A. is authenticated
8. https://github.com/curl/curl/issues/467](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-28-320.jpg)

![© Digital Security 32 MITM Attacks on HTTPS: Another Perspective Browsers behavior <script src="script.js"> and headers:

- no browser cares about Content-Disposition header
- IE doesn't care about Content-Type header (without nosniff)
- FF, Chrome, Edge dont't execute script only if Content-Type is from

"image" family (without nosniff)

- with X-Content-Type-Options, all the browsers require correct

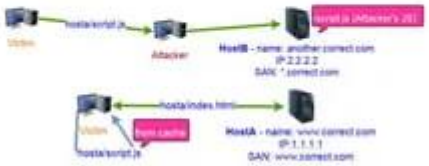
Content-Type](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-32-320.jpg)

1. V. request to HostA + script.js of HostB
2. A. MitMs and changes IP
3. HostB responses with A’s JS
4. V. caches JS for url:

https://hosta/script.js

- A. stops mitm attack
- A. forces V. to open HostA
- V. parses html from HostA
- But takes script.js from its cache, cause it’s there and still fresh
- V. executes JS (in the context of HostA)
- JS can interact with HostA in a usual way](https://image.slidesharecdn.com/httpschecked-171120115606/85/MITM-Attacks-on-HTTPS-Another-Perspective-36-320.jpg)

Active content substitution



Active content substitution - Trick

A. can upload files on HostB, but w/ "uninteresting" Content-Type or Content-Disposition
(specific path)

How can we manipulate with a path?
Depends on technologies

- RPO
- Default error page w/ relative scripts
  https://hostA/anything_here/lalala/ -> anything_here/lalala/script.js
- IE HostHeader injection
- ...

What else?

- HTTPS 2 HTTP redirect
- Reverse Proxy misrouting (CDNs)
- Certificate Pinning
- Client Cert auth "bypass"
- CSP bypass
- Crypto attacks
- Another Protocols
- ...

Conclusion

TLS Redirection

- Based on TLS features
- Based on your imagination and circumstances
- For any protocol (but works best for HTTPS)
- Not so hard to exploit
- You can get something from nothing (or misuse safe stuff)

Conclusion

TLS Redirection

- "New" approach of attacking TLS secured protocols
- The security level of web service equals to the security level of the weakest service with common certificate
- Based on the certificate of the weakest service