# Man in the Middle attacks

Network Security Lab – University of Trento – 2016-04-27

Jan Wolf Amit Gupta Ali Davanian

Ali Davanian – Amit Kumar Gupta – Jan Helge Wolf

## Section 1 - Introduction and configuration

- Introduction & configuration
- HTTP MitM
- HTTPS MitM
- Defenses

#### Introduction – MitM



#### Introduction – HTTP over TLS

- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
  - Cryptographic protocol to secure communication channels
  - Can be added on top of most communication protocols (HTTP, FTP, SMTP, IMAP, ...)
  - Symmetric cryptography for data encryption
  - Asymmetric cryptography for negotiating symmetric keys and authenticating the communication partner
    - Hierarchy-based public-key infrastructure with Certification Authorities (CAs)
    - HTTPS: Browsers/OSs come preloaded with a list of trusted root certificates, which are used to cryptographically sign intermediate certificates, which sign website certificates
    - Trust chain is verified by the browser during establishment of the secure connection (TLS handshake)
  - Integrity checks for transmitted data

Introduction – Setup (1)

#### Abstract setup:



## Introduction –Setup (2)

- Client/Web server (victim) -
  - Ubuntu 14.04 Desktop
  - Apache httpd
    - "Online banking" application
  - Firefox
    - FoxyProxy
- Man in the Middle (attacker)
  - Ubuntu 14.04 Server
  - mitmproxy
- Laptop
  - Slides

litM Victim/Server (post\_network\_config wird ausgeführt

MitM Attacker (post\_network\_config) ausgeschaltet

state associate

2016-04-27

## Section 2 – HTTP MitM

- Introduction and configuration
- HTTP MitM
  - Passive attack
- HTTPS MitM
  - Problem
  - sslstrip
  - Certificate forgery
- Defenses

#### HTTP MitM passive attack – Step 1

- Open Attacker virtual machine (credentials: attacker/attacker)
- Run mitmproxy on attacker's machine (mitmproxy)



## HTTP MitM passive attack – Step 2 (1)

- Open Victim virtual machine
- Open Firefox
- Activate the proxy
- Visit mybank.com and log in
  - User is user
  - Password is user

× No proxy	× Auto-detect proxy	× System proxy	🗶 Manual	× Autor	natic
Profile:	MitM Proxy	۲			Edi
HTTP Proxy:	192.168.100.2		Port	8080	÷
🐱 Use this pr	oxy server for all protocols				
SSL Proxy:	192.168.100.2		Port	8080	÷
FTP Proxy:	192.168.100.2		Port	8080	÷
SOCKS Host	192.168.100.2		Port	8080	÷
SOCKS v4 O	SOCKS v5 😣 🗆 Remote	DNS			
No Proxy for:					

## HTTP MitM passive attack – Step 2 (2)



## HTTP MitM passive attack – Step 3

- Open the Attacker virtual machine
- Check details of the HTTP POST request to mybank.com and its response (including credentials)

2016-04-18 18:09:	08 <mark>POST</mark> ht	tp://mybank.com/	
	<del>(</del>	<mark>302</mark> text/html 403B 189ms	
Request		Response	Detail
Host:	mybank.co	m	
User-Agent:	Mozilla/5	.0 (X11; Ubuntu; Linux x86_(	64; rv:39.0)
	Gecko/201	00101 Firefox/39.0	
Accept:	text/html	,application/xhtml+xml,appl	ication/xml;q=0.9,*/*;q=
	0.8		
Accept-Language:	en-US,en;	q=0.5	
Accept-Encoding:	gzip, def	late	
Referer:	http://my	bank.com/	
Connection:	keep-aliv	e	
Content-Type:	applicati	on/x-www-form-urlencoded	
Content-Length:	40		
UKLEncoded form			Lm:Auto
username: user			
password: user			
submit: Login			
[2/3]			?:helm_m:hack_[ <b>*:8080</b>
			. norp q. baon P. 10000

## Section 3 – HTTPS MitM

- Introduction and configuration
- HTTP MitM
- HTTPS MitM
  - Problem
  - sslstrip
  - Certificate forgery
- Defenses

#### HTTPS MitM – Problem

- Encrypted protocol -> no trivial MitM possible
- Authenticated protocol -> no TLS termination possible



#### HTTPS MitM – Demonstration

#### • Visit https://ssl.mybank.com with and without proxy (Compare)

← ● https://ssl.mybank.com		C 🛞	
Welcome to MyBank! Username:	Password:	Login	- Without MitM and proxy
	C Sear COUL CONNECTION IS NOT the owner of ssl.mybank.com has configured their we totect your information from being stolen, Firefox ha is website. Co Back	ch ☆ Secure bsite improperly. To is not connected to Advanced	- With MitM and proxy

## Section 3 – Phase 2

- Introduction and configuration
- HTTP MitM
- HTTPS MitM
  - Problem
  - sslstrip
    - Active attack
  - Certificate forgery
- Defenses

#### HTTPS MitM – sslstrip

- **Problem**: HTTPS is regularly negotiated over HTTP
  - HTTP 30X redirects
  - Client-side redirect (JavaScript, meta-refresh, ...)
  - Form action location
  - Links
- HTTP can be intercepted and manipulated to prevent establishment of encrypted connections

### HTTPS MitM – sslstrip – Step 1

- Open the attacker virtual machine
- Stop mitmproxy by typing:
  - q
  - y
- Typecd ~/mitmproxy/ (Tilde: Alt Gr +)
  - You should see sslstrip.py by typing ls
  - Start mitmproxy with sslstrip:
    - mitmproxy -s sslstrip.py

## HTTPS MitM – sslstrip – Step 2 (1)

- Open the Victim virtual machine
- Open the browser, deactivate the proxy
- Visit ssl.mybank.com
- Check the source code using Firefox inspector (right click -> Inspect element)
- Activate the proxy, refresh the page, and compare the source code
- Log in using known credentials
- HTTPS redirect does not happen
- The website is served in HTTP
- User will observe no error in the browser

## HTTPS MitM – sslstrip – Step 2 (2)



## Section 3 – Phase 2

- Introduction and configuration
- HTTP MitM
- HTTPS MitM
  - Problem
  - sslstrip
    - Active attack
  - Certificate forgery
- Defenses

#### HTTPS MitM – Active Attack – Step 1

- Open the attacker virtual machine
- Press i
- Type ~q | ~s and press Enter to activate interception for all requests and all responses

#### HTTPS MitM – Active Attack – Step 2

- Open Victim virtual machine
- Open the browser
- You should still be logged in to ssl.mybank.com
- Click "Wire transfer"
- Accept the request and the response by pressing a twice on the attacker machine

#### HTTPS MitM – Active Attack – Step 3

• Perform transfer of 10€ to account IT00000000

Finder File Edit View Go Window Help	📧 🜒 🕸 🕲 🛕 😱 🕙 🔹 🔅 53% 🗊 📕 U.S. Tue Apr 19 12:32:14 Amit Gupta 🔍 😑
MitM Victim/Server [Running]	MitM Attacker [Running]
Mozilla Firefox 🗢 🔄 📧	(I) 12:32
http://ssl.mransfer.php × New Tab     ×       • • • • • • • • • • • • • • • • • • •	★ Set http://ssl.mybank.com/
Please enter the details of your wire transfer here: Sender account: IT999999999 Recipient account: IT0000000000 Amount	<ul> <li>← 302 text/html 408B 223ms</li> <li>GET https://ssl.mybank.com/ouerview.php</li> <li>← 200 text/html 474B 25ms</li> <li>GET https://ssl.mybank.com/transfer.php</li> <li>← 200 text/html 430B 80ms</li> </ul>
Description:	
back	
a	[1/4] [scripts:1]?:helv [*:8080]
2	Intercept filter: ~q + ~s

## HTTPS MitM – Active Attack – Step 4 (1)

- Open the intercepted request and manipulate it
  - On the request tab press  ${\rm e}$
  - Press r afterwards, editor opens

Request inter	cented	Response	Detail	
Host:	ssl.mubank.com	neeponeo		
User-Agent:	Mozilla/5.0 (X11;	Ubuntu; Linux x86_64	; ru:39.0)	
	Gecko/20100101 Fi	refox/39.0		
Accept:	text∕html,applica 0.8	tion/xhtml+xml,applic	ation/xml;q=0.9,	,*∕*;q=
Accept-Language:	en-US,en;q=0.5			
Accept-Encoding:	gzip, deflate			
Referer:	http://ssl.mybank	.com/transfer.php		
Cookie:	PHPSESSID=tlb0md1	q65om81g4dduoaftej4		
Connection:	keep-alive			
Content-Type:	application/x-www	-form-urlencoded		
Content-Length:	125			
URLEncoded form				[n:Auto]
srcAccount: IT99	1999999999			
dstAccount: ITOO	00000000			
amount: 290				
description: mont	hly rent to san ba	rtolameo		
submit: Conf	irm transfer			
[2/2] [i:~q	~s][scripts:1]		?:help q:back	[*:8080]
Edit request (coo	kies, <mark>q</mark> uery,path, <mark>u</mark> r	l,header,form,raw bod	y,method)?	

2016-04-19 13:20:04 POST http://ssl.

## HTTPS MitM – Active Attack – Step 4 (2)

- Manipulate the request as to transfer 500€ to account IT5555555555
  - Replace account IT000000000 by IT555555555
  - Replace amount by 500
  - Press CTRL+X to exit
  - Save changes (y) to default file



## HTTPS MitM – Active Attack – Step 5 (1)

- Press a to accept the manipulated request
- Press Tab to go to the response tab
- On the response tab, press  $\in$
- Press r, editor opens

2016-04-19 13:20:0	4 POST http://ssl.mybank.com/transfer.ph	p	
	← 200 text/html 264B 140s		
Request	Response intercepted	Detail	
Date:	Tue, 19 Apr 2016 11:22:26 GMT		
Server:	Apache/2.4.7 (Ubuntu)		
X-Powered-By:	PHP/5.5.9-1ubuntu4.14		
Expires:	Thu, 19 Nov 1981 08:52:00 GMT		
Cache-Control:	no-store, no-cache, must-revalidate, pos	st-check=0,	
	pre-check=0		
Pragma:	no-cache		
Vary:	Accept-Encod ing		
content-length:	264		
Keep-Alive:	timeout=5, max=100		
Connection:	Keep-Alive		
Content-Type:	text/html		
content-encoding:	gzip		
[decoded gzip] HTM	L		[m:Auto]
<pre><!DOCTYPE html PUE</pre>    </pre>	LIC "-//W3C//DTD HTML 4.0 Transitional//	EN''	
"http://www.w3.org	/TR/REC-html40/loose.dtd">		
<html></html>			
<head></head>			
<style>&#13;</td><td></td><td></td><td></td></tr><tr><td><pre>??.formrow label {</pre></td><td> </td><td></td><td></td></tr><tr><td>???display: inline</td><td>-block; </td><td></td><td></td></tr><tr><td>???width: 200px;&#</td><td>13;</td><td></td><td></td></tr><tr><td>??} </td><td></td><td></td><td></td></tr><tr><td>?</style>			
[272] [i:"q   ~	sllscripts:11	fihelp qiback	L*:80801

## HTTPS MitM – Active Attack – Step 5 (2)

- Deceive the user
  - Replace account IT5555555555 by IT000000000
  - Replace amount by original amount (default 10)
  - Press CTRL+X to exit,
  - Save changes (y) to default file
  - Accept the response by pressing a
  - Press  $\operatorname{q}$  to leave the detail view
- Press i, delete the current intercept filter and press Enter

<html> <head></head></html>	
	<style></td></tr><tr><td></td><td>.formrow label {</td></tr><tr><td></td><td>display: inline-block;</td></tr><tr><td></td><td>width: 200px;</td></tr><tr><td></td><td>}</td></tr><tr><td></td><td></style>
<body></body>	(1)
	<alv la="welcome"> Thank Veret</alv>
	<pre>\/uiv/ /diu class="success"\Your transfer of 290 00%euro; from IT9999999999 to</pre>
I TAAAAAA	MAAA was successful (hr /)/a href="oueruiew_nhn")hack//a)//diu)//hodu)//
html>	$\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{\sqrt{$
~	
~	
~	
~	
~	
~	
~	
~	
TNORT	
INSEE	11 13,13-27 All

## HTTPS MitM – Active Attack – Step 5 (3)

Mith Victin/Server [Running]       Mith Altacker [Running]         Mozilla Firefox       Constraints	Finder	File Edit	View	Go Windo	ow Help							) 💝	◄ 🖓 🔽 🛦 🍳	* 🤶 22% 🕞	📕 U.S. F	Fri Apr 22 12:16:2	7 Amit Gupta	् ≡
Mozilla Firefox       Image: The state of					MitM Victim/S	Server [Rui	nning]						100	Mit	tM Attacker	r [Running]		
<pre>http://sslmransfer.php * tew Tab * + Request Fri, 22 Apr 2016 03:57:33 GMT Server: Apachez 4.7: (Uburtu) Fri, 22 Apr 2016 03:57:33 GMT Server: Apachez 4.7: (Uburtu) Frize: Thu, 12 Congratulations!! Your transfer of 290,00€ from IT9999999999 to IT0000000000 was successful. Dete: Frize: Thu, 10:55: 9-100 must -revalidate, post-check=0, pre-check=0 pre-check=</pre>	Mozilla	Firefox							🔶 En		<b>●</b> )) 11	:59 🔱	2016-04-22 12:13:	39 POST https://	/ssl.mybai ext/html/2	nk.com/transfer 248B 59 8s	.php	
Congratulations!!       Fxpires:       Tw. 19 Nov 1981 08:52:00 GMT         Your transfer of 290,00€ from IT999999999 to IT000000000 was successful.       pre-check=0         pack       no-cache         wack       no-cache         war       no-cache         log:       log:         image:       cache-line:         log:       log:         image:       cache         log:       log:         image:       log:	0	http://ss	l.mran mybank.c	sfer.php ×	New Tab er.php	▼ (	× ع ۹	+	>	÷	合 »		Request Date: Server: X-Powered-Bu:	Fri, 22 Apr 20 Apache/2.4.7 ( PHP/5.5.9-1ubu	Respon 016 09:57 (Ubuntu) (ntu4.14	nse :39 GMT	Deta	1
Connection:       Keep-Alive         Content-Type:       text/html         Content-Type:       text/html         Image: Content-Type:       t		Congratu Your tran <u>back</u>	lations! Isfer of	‼ 290,00€ 1	from IT999	9999999	9 to IT00	00000	0000 w	as su	ccessfu	1.	Expires: Cache-Control: Pragma: Vary: content-length: Keen-Alive:	Thu, 19 Nov 19 no-store, no-c pre-check=0 no-cache Accept-Encodin 248 timeout=5. max	081 08:52 cache, mus ng c=100	:00 GMT st-revalidate,	post-check=0	
(?DOCTYPE htnl PUBLIC ''-/W3C//DTD HTML 4.0 Transitional//EN''         ''http://www.w3.org/TR/REC-htm140/loose.dtd''>         (htm1)         (htm2)         (style>         ???formrow label {         ???display: inline-block;         ???width: 200px;         ???width: 200px;         ???width: 200px;         ???width: 200px;         ???width: 200px;         ???bead>         [5/5]       [i:~q + ~s][scripts:1]         ?:help q:back [*:8080													Connection: Content-Type: content-encoding: [decoded_gzin] HT	Keep-Alive text/html gzip	(-100			[m:Auto]
<pre></pre>													<pre><!DOCTYPE html PU "http://www.w3.or <html>    </pre>	BLIC "-//W3C//DT g/TR/REC-html40/	ID HIML 4 /loose.dta	.0 Transitional d">	//EN''	
???width: 200px;         ??/width:													<head> <style>&#13; ??.formrow label ???displau: inlin</td><td>{  e-block; </td><td></td><td></td><td></td><td></td></tr><tr><td>[5/5]       [i:~q + ~s][scripts:1]       ?:help q:back [*:8080         [2]       [2]       [2]       [2]         [3]       [2]       [2]       [2]         [4]       [2]       [2]       [2]         [5/5]       [1:~q + ~s][scripts:1]       ?:help q:back [*:8080         [5/5]       [1:~q + ~s][scripts:1]       ?:help q:back [*:8080</td><td>A</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>???width: 200px;& ??}  ?</style></head>	#13;				
	a,												[5/5] [i:~q]	~s][scripts:1]		<b>a</b> a <b>a a a a </b>	?:help q:ba	ıck [*:8080] ▼ Left Ж

#### Section 3 – Phase 3

- Introduction and configuration
- HTTP MitM
- HTTPS MitM
  - Problem
  - sslstrip
  - Certificate forgery
- Defenses

## HTTPS MitM – Certificate forgery (1)

- What is a signature?
  - The signature proves the authenticity of the certificate

२ 🏡 ≟ 🐵 🔘 🔶 https://www.google.it/?gfe\_rd=cr&ei=TM4XV8TIIdOo8wf4k4nqAQ 💽 Certificate  $\times$ R f Elements Console Sources Network Timeline Security >>> General Details Certification Path Security Overview Overview Certificate Information 200 Ð Main Origin This certificate is intended for the following purpose(s): • Ensures the identity of a remote computer Reload to view details Proves your identity to a remote computer This page is secure (valid HTTPS). •1.3.6.1.4.1.11129.2.5.1 Valid Certificate The connection to this site is using a valid, trusted server certificate. Issued to: \*.google.com View certificate Issued by: Google Internet Authority G2 Secure TLS connection The connection to this site is using a strong protoc Valid from 4/7/2016 to 6/30/2016 version and cipher suite. Google Se Secure Resources Issuer Statement All resources on this page are served securely.

## HTTPS MitM – Certificate forgery (2)

- Authentic certificate
  - If the certificate authority's signature is in your computer
- Forged certificate
  - Unknown signer -> error in your browser
- Am I secure if I don't see the error?
  - Rogue CA might be listed as trustworthy by your computer
    - Lenovo Superfish example from class
- We do the same here and install the certificate authority manually

## HTTPS MitM – Certificate forgery – Step 1 (1)

- Open the victim virtual machine
- Open the browser
- Make sure the proxy is set
- Open mitm.it
- Choose "other"
- Check the first box and click ok

## HTTPS MitM – Certificate forgery – Step 1 (2)

🗲 🕅 mitm.it		C 🍕 🔍 Search	☆ 自 ♥ ♦ 俞
mitmproxy			
Apple	Click to install the n	nitmproxy certificate:	Other
	Downloading Certificate		
	<ul> <li>You have been asked to trust a new Certificate A</li> <li>Do you want to trust "mitmproxy" for the follow</li> <li>Trust this CA to identify websites.</li> <li>Trust this CA to identify email users.</li> <li>Trust this CA to identify software developers</li> <li>Before trusting this CA for any purpose, you shop procedures (if available).</li> <li>View Examine CA certificate</li> </ul>	ving purposes? ;. puld examine its certificate and its policy and	
		Cancel OK	

## HTTPS MitM – Certificate forgery – Step 2

- Recall the earlier error message when visiting https://ssl.mybank.com while using the proxy
- Visit https://ssl.mybank.com again while the proxy is active

← ▲ https://ssl.mybank.com		C	] 🛞 [	Without MitM and proxy
Welcome to MyBank!			$\sim$	
Username:	Password:	Login		<ul> <li>With MitM and proxy</li> </ul>

### Section 4 - Defenses

- Introduction and configuration
- HTTP MitM
- HTTPS MitM
- Defenses

## HTTP Strict Transport Security (HSTS)

- HTTP header codified in RFC 6797 (Nov 2012)
- "TLS Supercookie"
- Based on Trust-on-First-Use model
  - User visits HTTPS website
  - Server responds with HSTS header, indicating a time period
  - Browser stores this information and will reject all non-HTTPS connections to this domain
- Browser preload possible

## HTTP Public Key Pinning

- HTTP header codified in RFC 7469 (Apr 2015)
- Also called Certificate Pinning
- Based on Trust-on-First-Use model
  - User visits HTTPS website
  - Server responds with HPKP header, indicating
    - the SHA-256 hash of its public key,
    - the SHA-256 hash of a backup public key,
    - a time period
  - Browser stores this information and will reject all HTTPS connections to this domain if the presented public key does not match
- Browser preload for popular websites

## ...and of course

- Don't trust unknown hotspots
- Certainly don't trust unknown certificates
- There's no way you're going to trust an unknown Certification Authority
  - ...right?

Your Certificates	People Se	ervers	Authorities	Others					
You have certific	ates on file	that io	dentify these	certifica	te aut	horities:			
Certificate Nan	ne			Securi	ty Dev	vice			E\$
▶(c) 2005 TÜRKT	RUST Bilgi İ	letişim	ve Bilişim						A
▶A-Trust Ges. f. S	Sicherheitss	ystem	e im elektr						=
▶AC Camerfirma	a S.A.								
►AC Camerfirma	a SA CIF A82	274328	7						
▶ACCV									
▶Actalis S.p.A./(	0335852096	7							
AddTrust AB									
▶AffirmTrust									
▶Agencia Catala	na de Certi	ficacio	(NIF Q-080						
►AS Sertifitseer	imiskeskus								
▶Atos									
▶Autoridad de C	Certificacior	n Firma	profesion						
▶Baltimore									
Buypass AS-98	3163327								ͺ
<u>V</u> iew	<u>E</u> dit Trust		mport	E <u>x</u> port		Delete	or Distrus	t	
									01/
									OK

## References

- TLS: RFC 5246 (https://tools.ietf.org/html/rfc5246)
- HSTS: RFC 6797 (https://tools.ietf.org/html/rfc6797)
- HPKP: RFC 7469 (https://tools.ietf.org/html/rfc7469)
- sslstrip: native software (https://moxie.org/software/sslstrip/) and original Blackhat talk (https://www.youtube.com/watch?v=MFol6IMbZ7Y), both by Moxie Marlinspike
- mitmproxy: https://mitmproxy.org/