So you think you can secure a network


OH SO YOU USE HTTPS
TELL ME MORE ABOUT THE PASSWORDS I'M CATCHING
imgflip.com

Disclaimer

- I cannot be held responsible for whatever happens if you try the experiments demonstrated today.
- I am NOT encouraging anyone to perform any kind of attack against the confidentiality, integrity and/or availability of any system.
- Everything shown in this presentation/workshop/seminar is public domain knowledge and, therefore, the material used for it cannot be considered as the main medium because of which illegal activities were, are or will be performed.

In other words: don’t try this stuff on

Your company/university/favorite cafe’s network. If I’m contacted by the authorities...

Disclaimer

- I cannot be held responsible for whatever happens if you try the experiments demonstrated today.
- I am NOT encouraging anyone to perform any kind of attack against the confidentiality, integrity and/or availability of any system.
- Everything shown in this presentation/workshop/seminar is public domain knowledge and, therefore, the material used for it cannot be considered as the main medium because of which illegal activities were, are or will be performed.

In other words: don’t try this stuff on

Your company/university/favorite cafe’s network.
authorities… I WILL FIND YOU

Nosy twitter...

What's happening?

Marco Chiappetta @lambdacomplete · 19s

this is a nice #wat in python

```
    return getattr(self.client, method)(**params)
TypeError: patch() takes at least 2 arguments (3 given)

----------------------------------------------------------
```

Who to follow · Refresh · View all

Amazon Web Services ...
Followed by H. Yigit Guler a...
Follow

CIA @CIA
Follow

dafuq

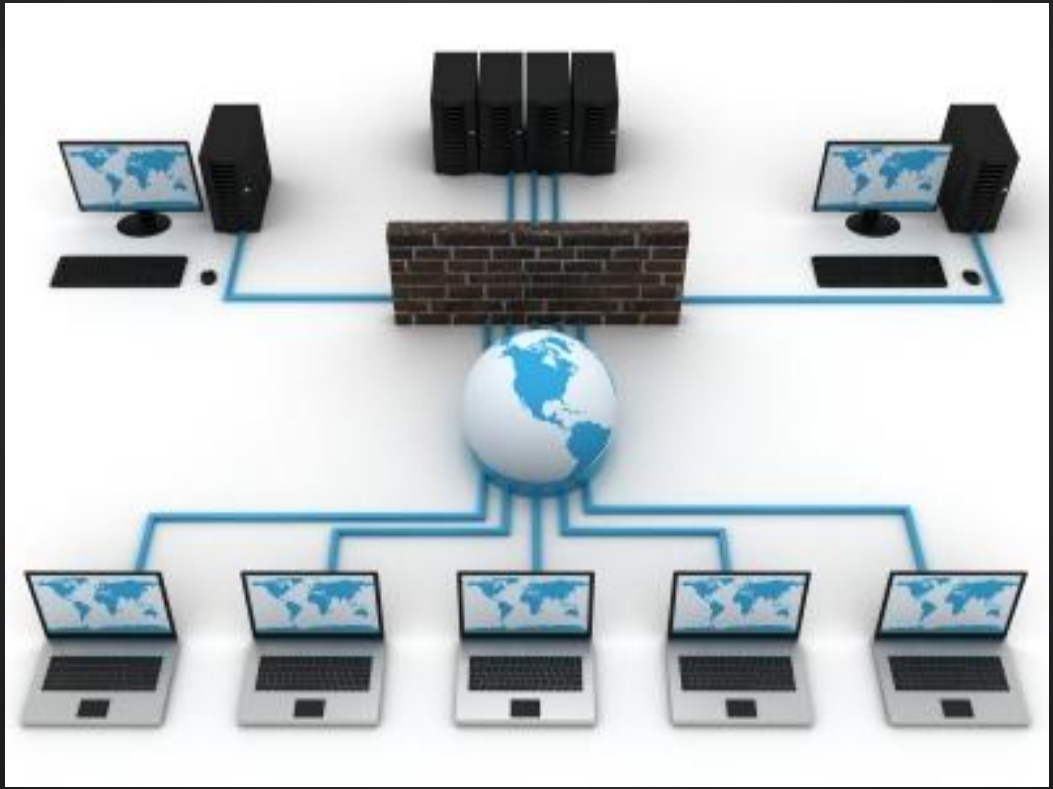
TODO list

- Invade people’s privacy (for educational purposes!).
- “Break” modern security mechanisms (e.g. *https*).
- Show that networks are vulnerable *by design*.

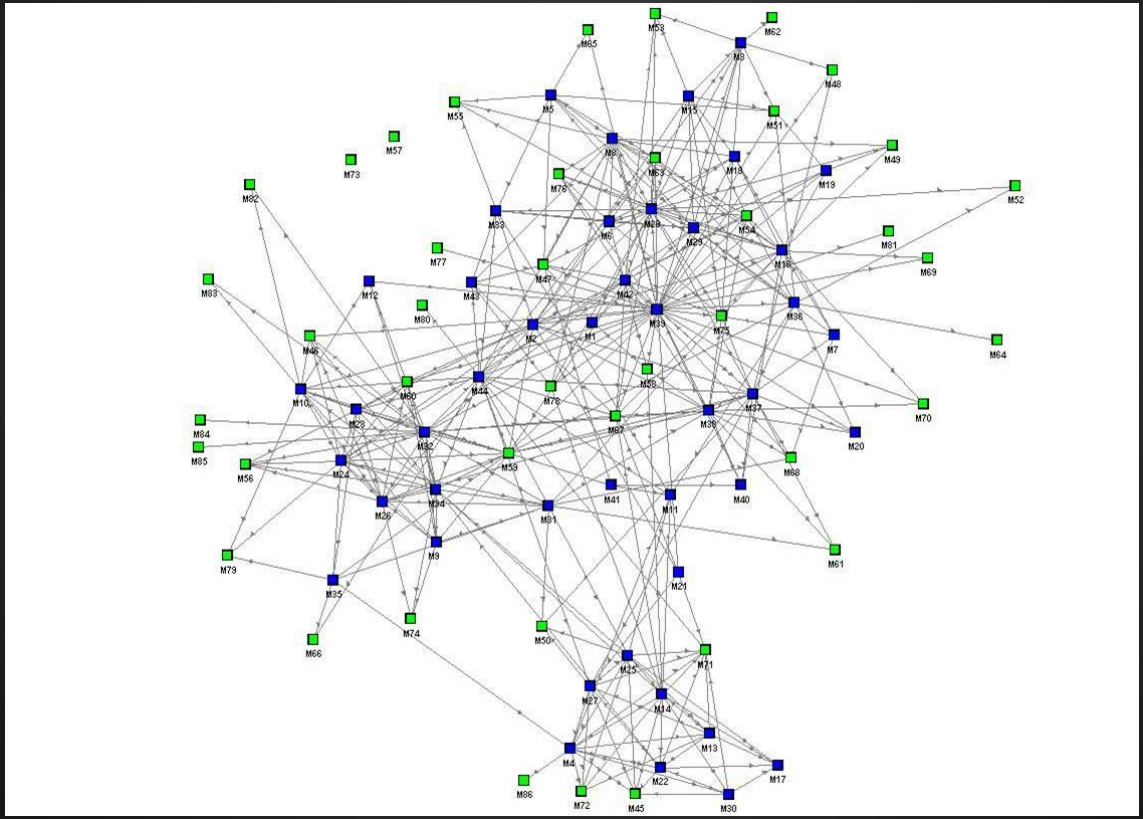
TODO list

- Invade people's privacy (for educational purposes!).
- "Break" modern security mechanisms (e.g. *https*).
- Show that networks ~~are vulnerable *by design*~~ have been vulnerable for the past 20-30 years!

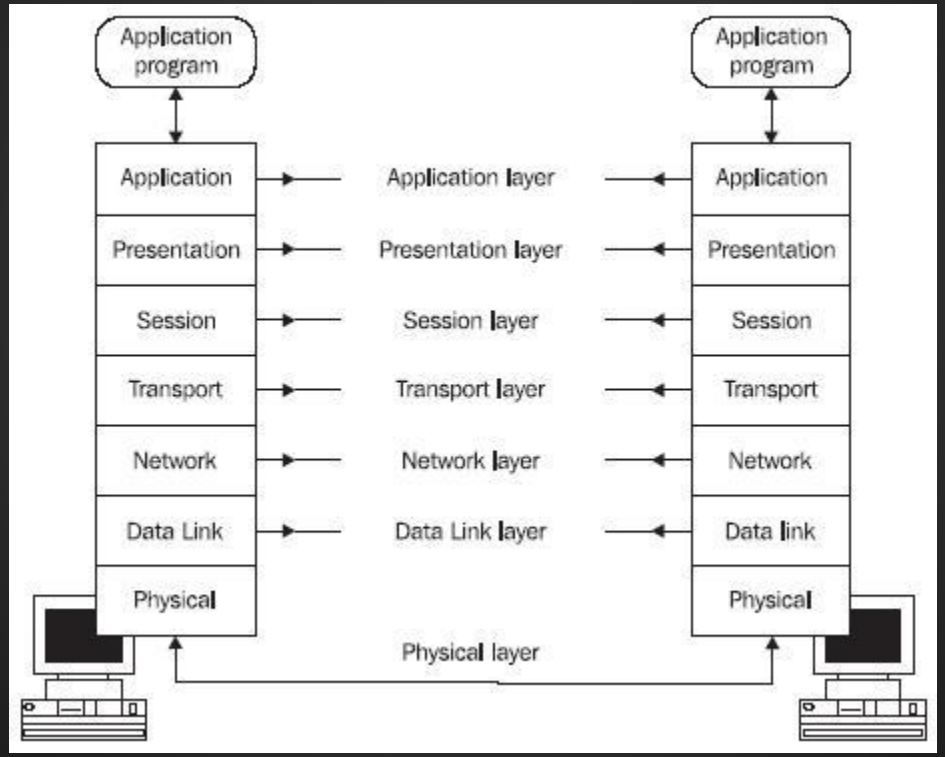
The ideal world...



The real world!



One-slide intro to ISO/OSI



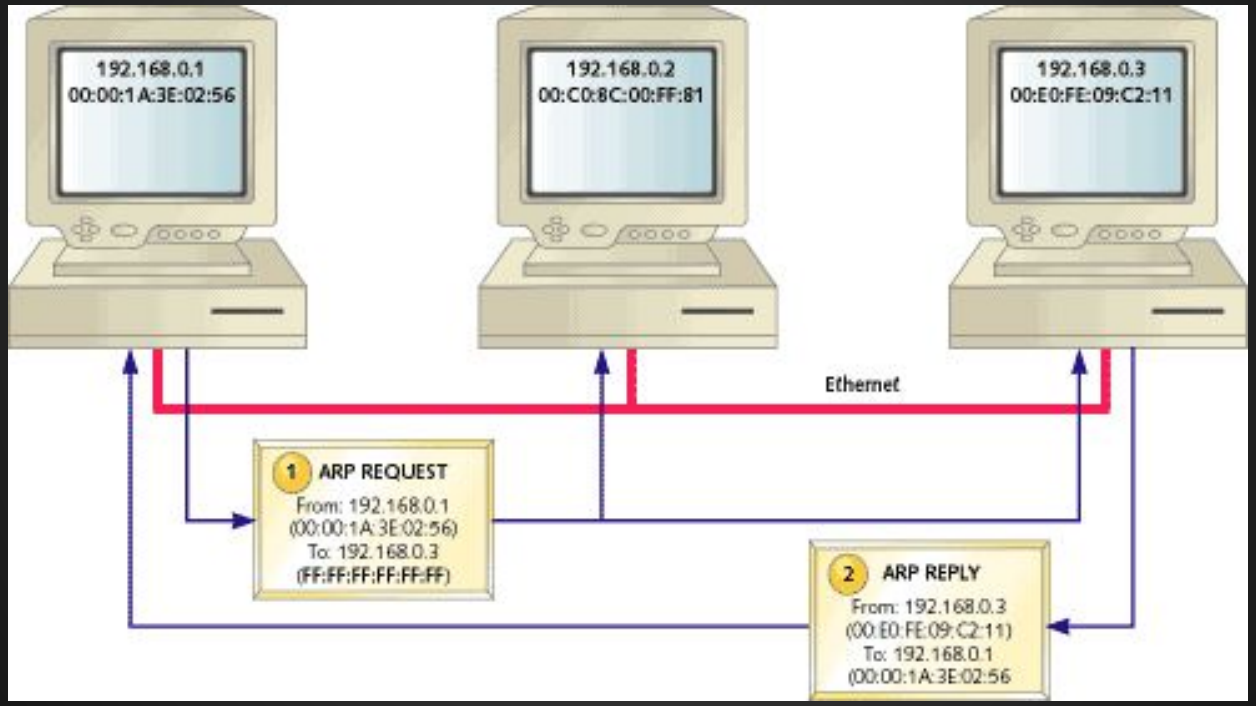
Network and Datalink layers

Question: if IP addresses can be changed, how do we (dynamically) link each IP address to the actual device? And how do we identify these devices in the first place?

The One!

The One?!?

ARP (Address Resolution Protocol)



ARP (Address Resolution Protocol)

Alice
10.0.0.11
bb:10:fa:ke:34:aa

ARP Cache:

Bob
10.0.0.12
bb:10:fa:ke:34:bb

ARP Cache:

Eve
10.0.0.15
bb:10:fa:ke:34:ee

ARP (Address Resolution Protocol)

ARP (Address Resolution Protocol)

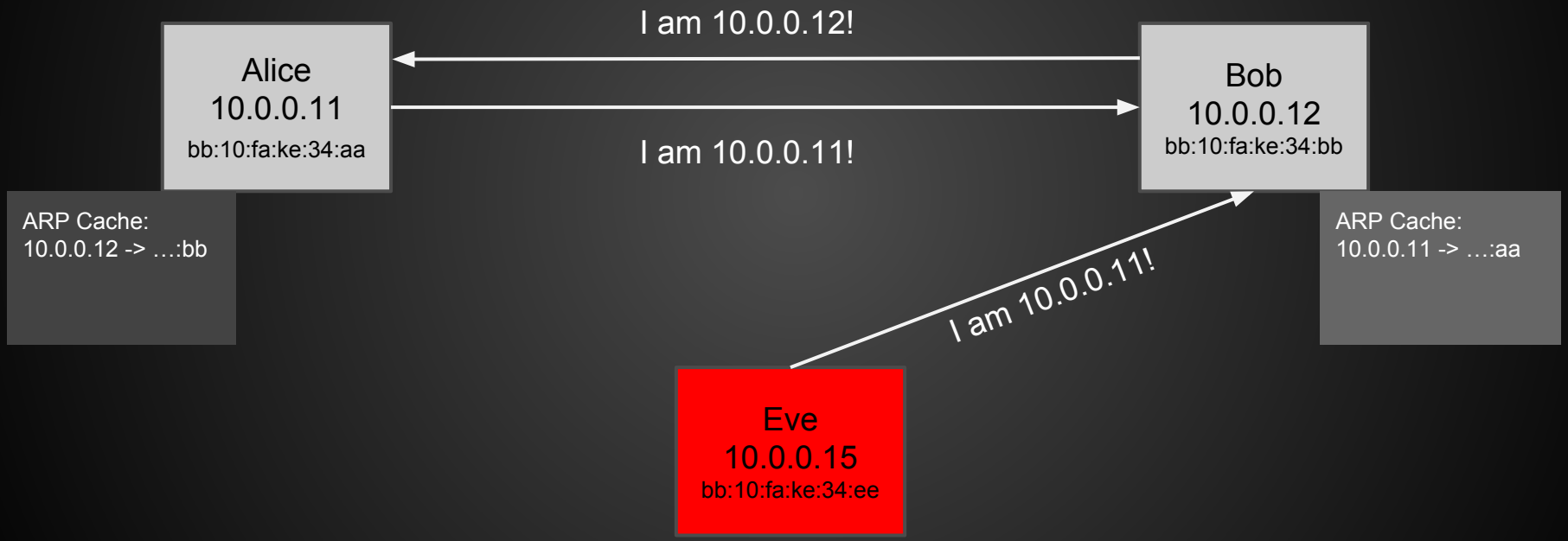
ARP (Address Resolution Protocol)

Time to fuck around

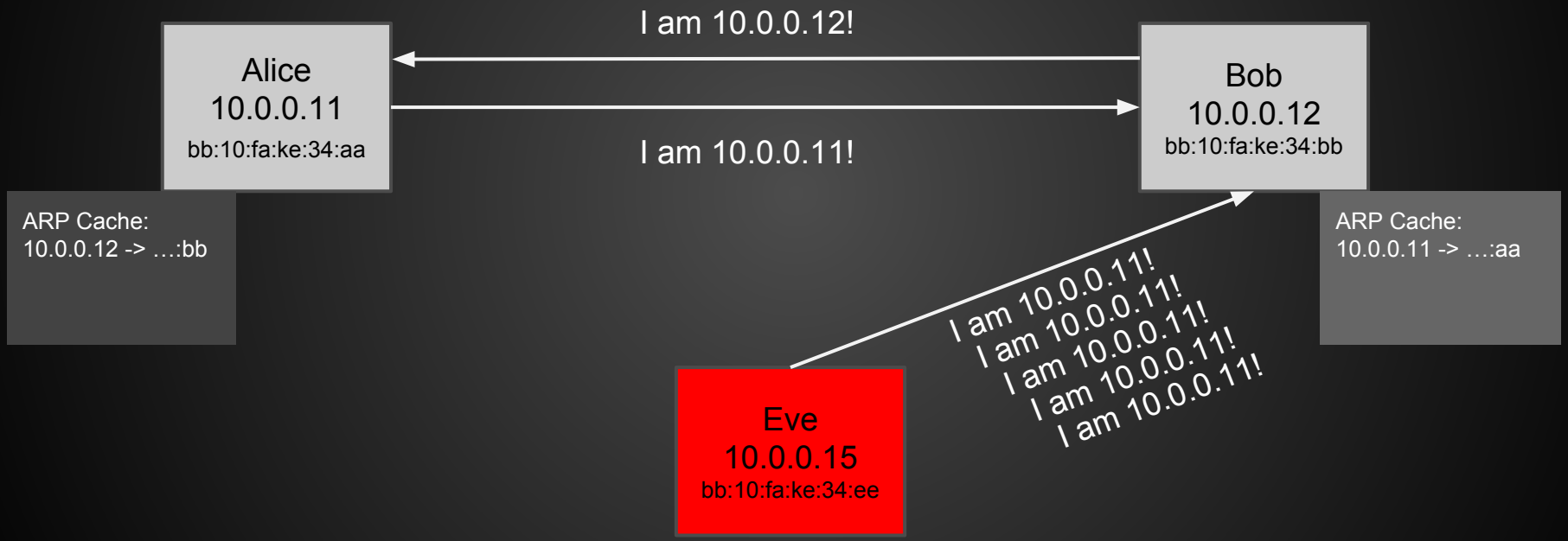
Time to do cool things that we are only going to test in our local network and I promise I won’t disappoint my parents

ARP (Address Resolution Protocol)

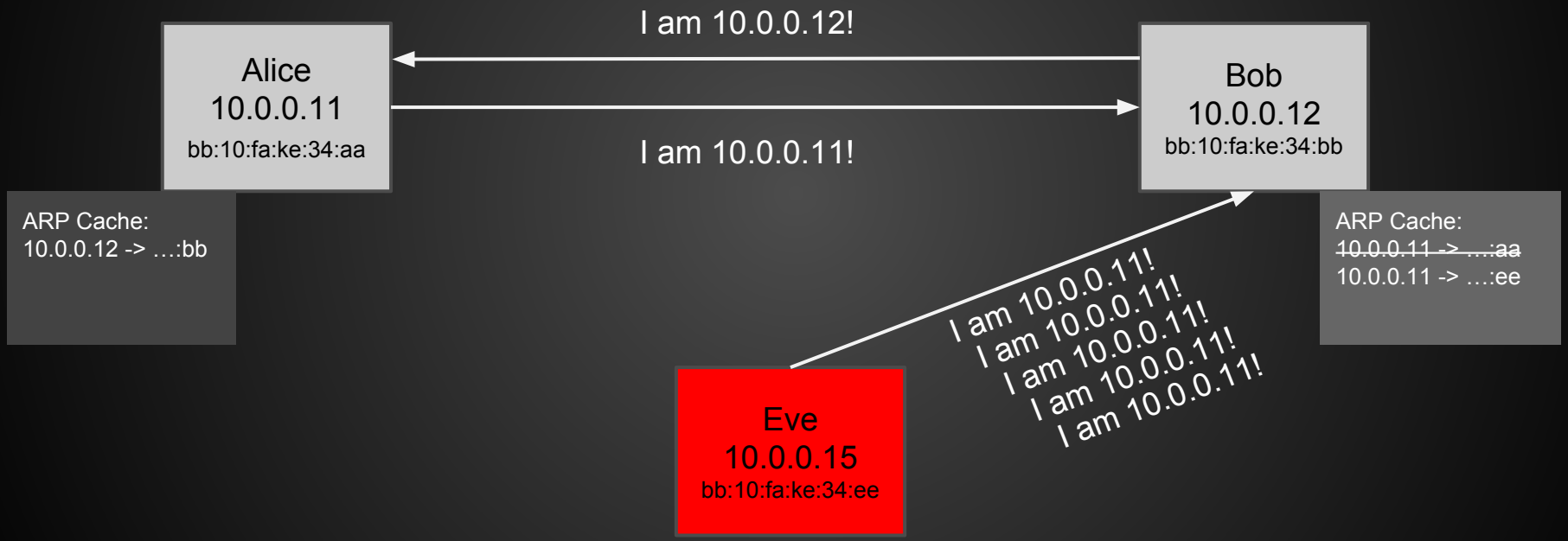
ARP (Address Resolution Protocol)



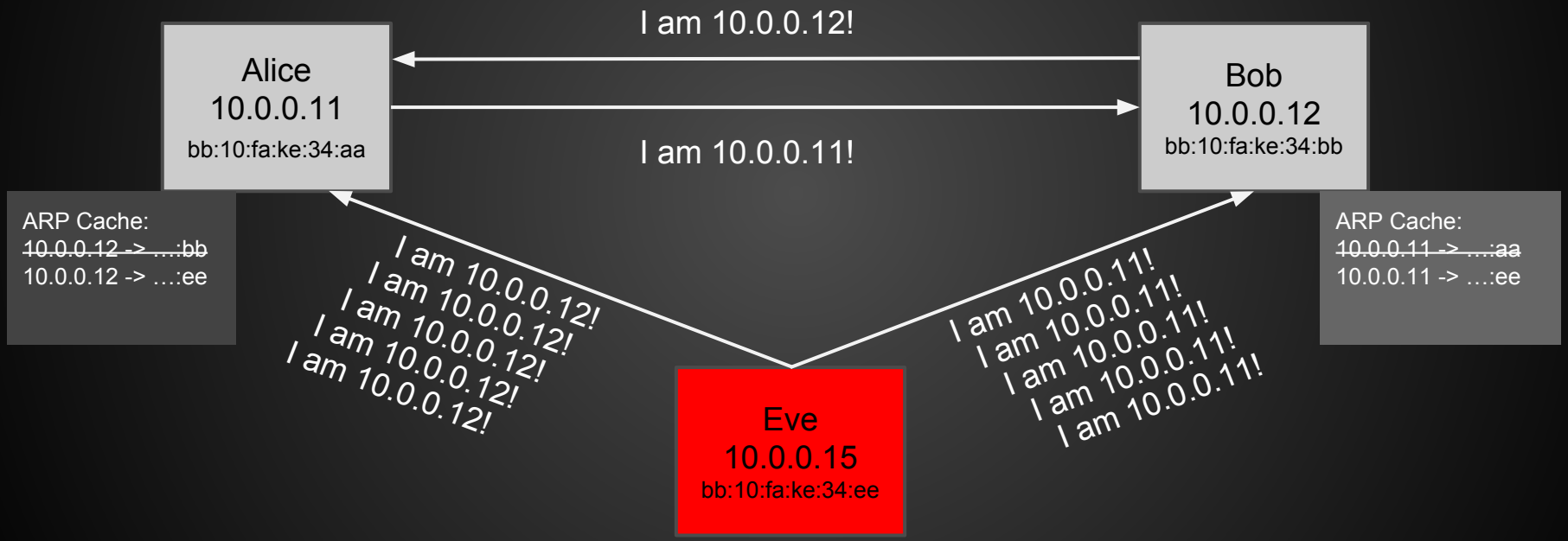
ARP (Address Resolution Protocol)



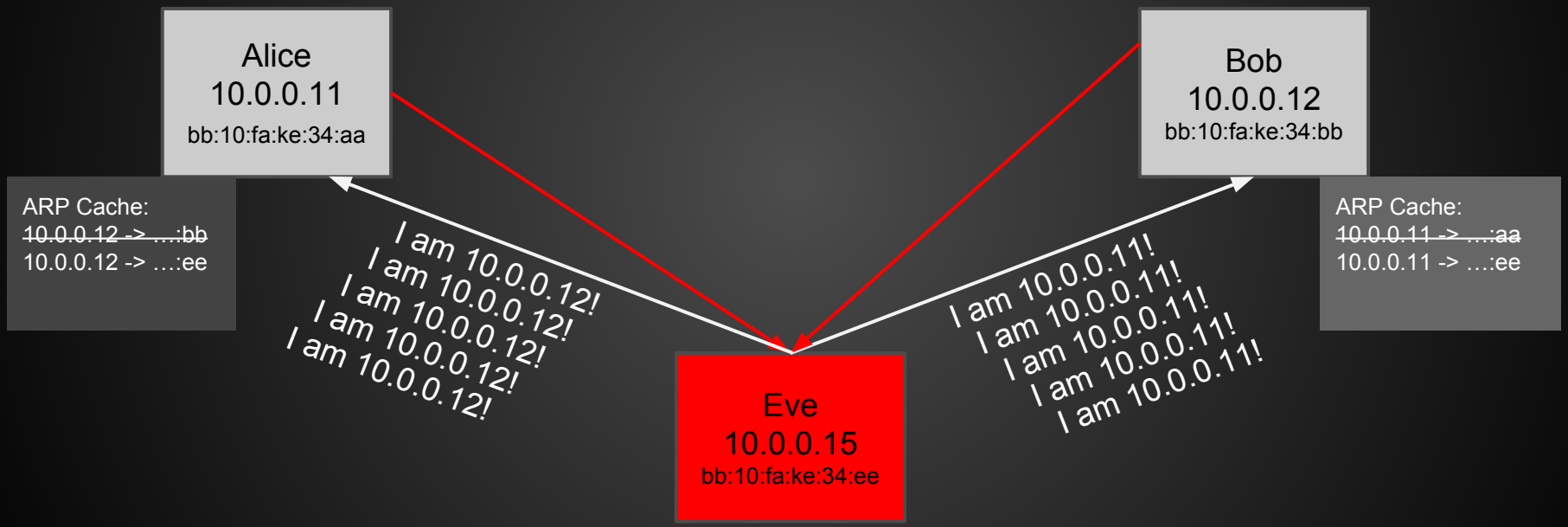
ARP (Address Resolution Protocol)



ARP (Address Resolution Protocol)



ARP (Address Resolution Protocol)



Let’s spoof!

HTTPS, SSL, TLS...WTF?

“If there’s an acronym for it, it must be secure.”
(ancient Chinese proverb)

Some vocabulary (oversimplified!)

- **Encryption**: the process of using a key to hide the content of a message.
- **Decryption**: the process of using a key to reveal the content of an encrypted message.
- **Public key**: a key that can be shared with anyone, can only be used to encrypt.
- **Private key**: a key that shouldn't be shared with anyone and can decrypt messages encrypted with the related public key.
- **Certificate authority (CA)**: trusted entities that uniquely establish the ownership of a particular public key.

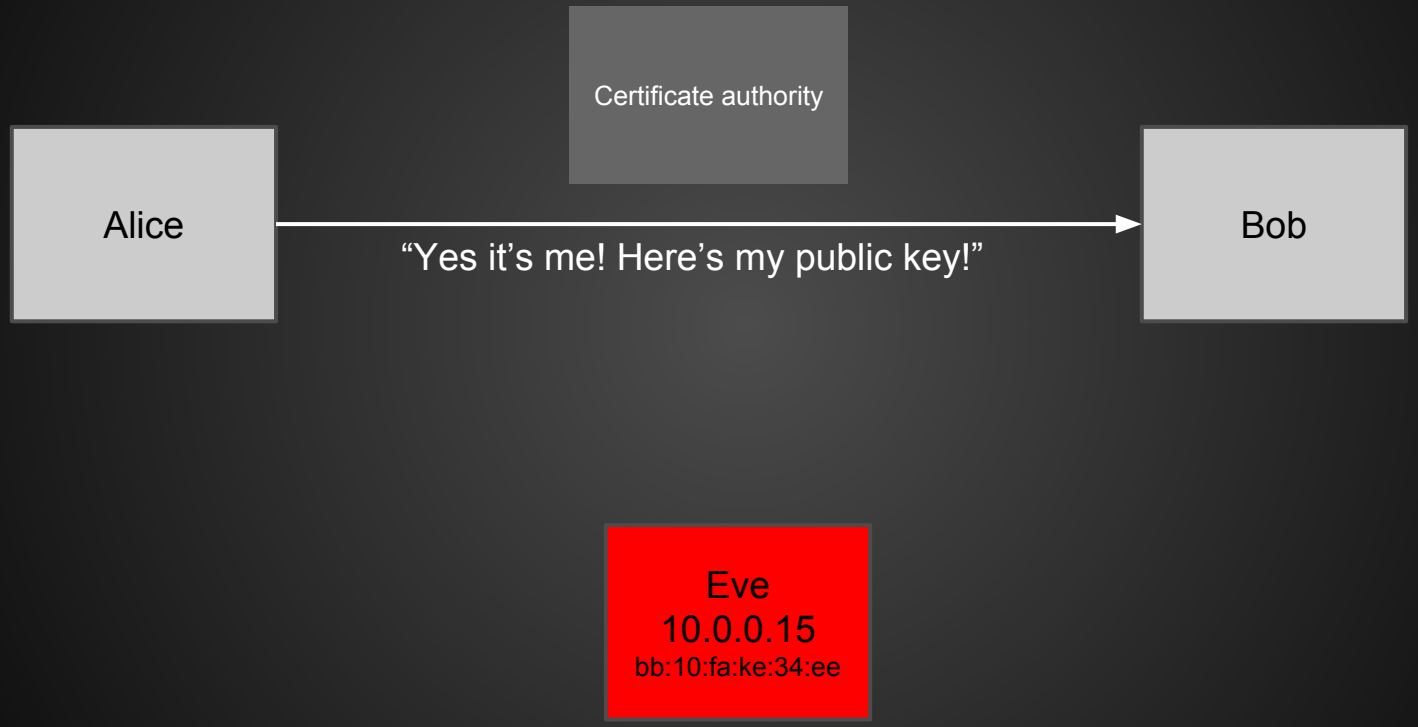
Public and private key go in "pairs", generated together.

Very hard (read "impossible") to find the private key having only the public key.

Secure connections

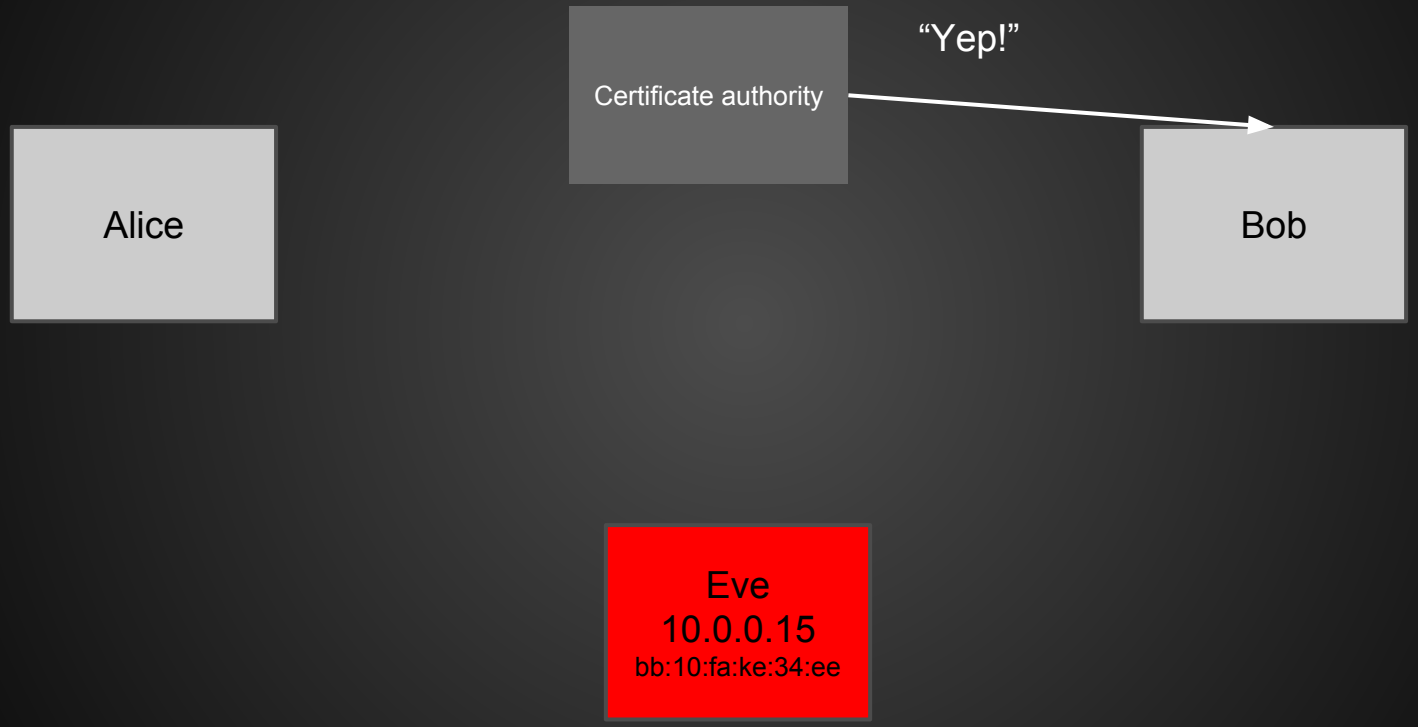
Secure connections

Secure connections

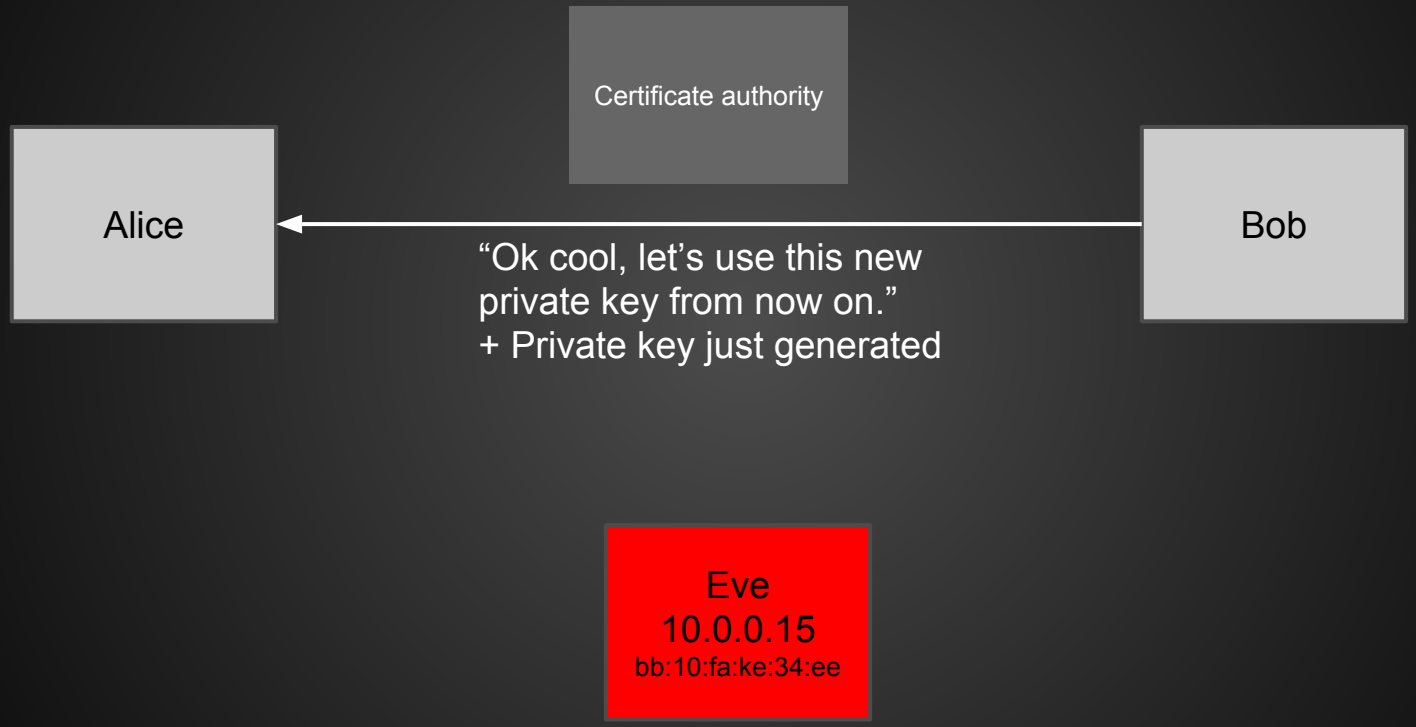


Secure connections

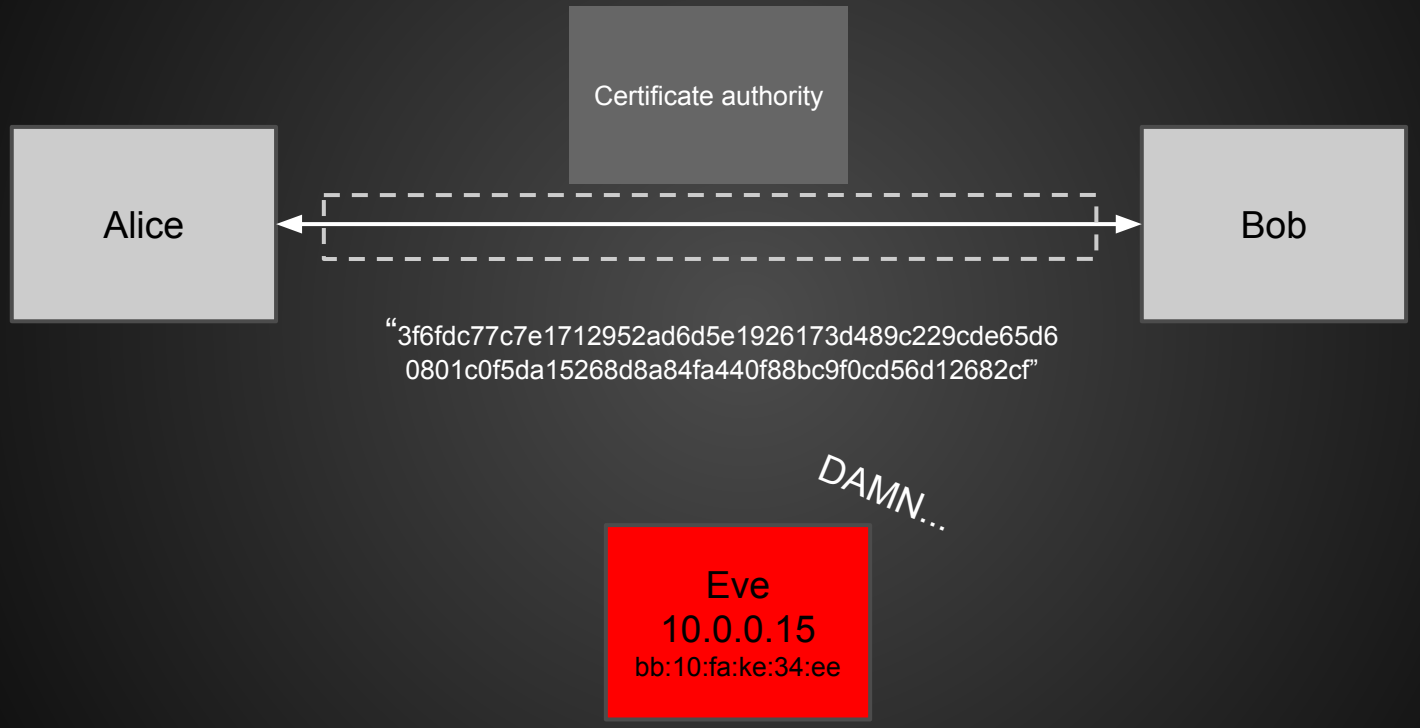
Secure connections



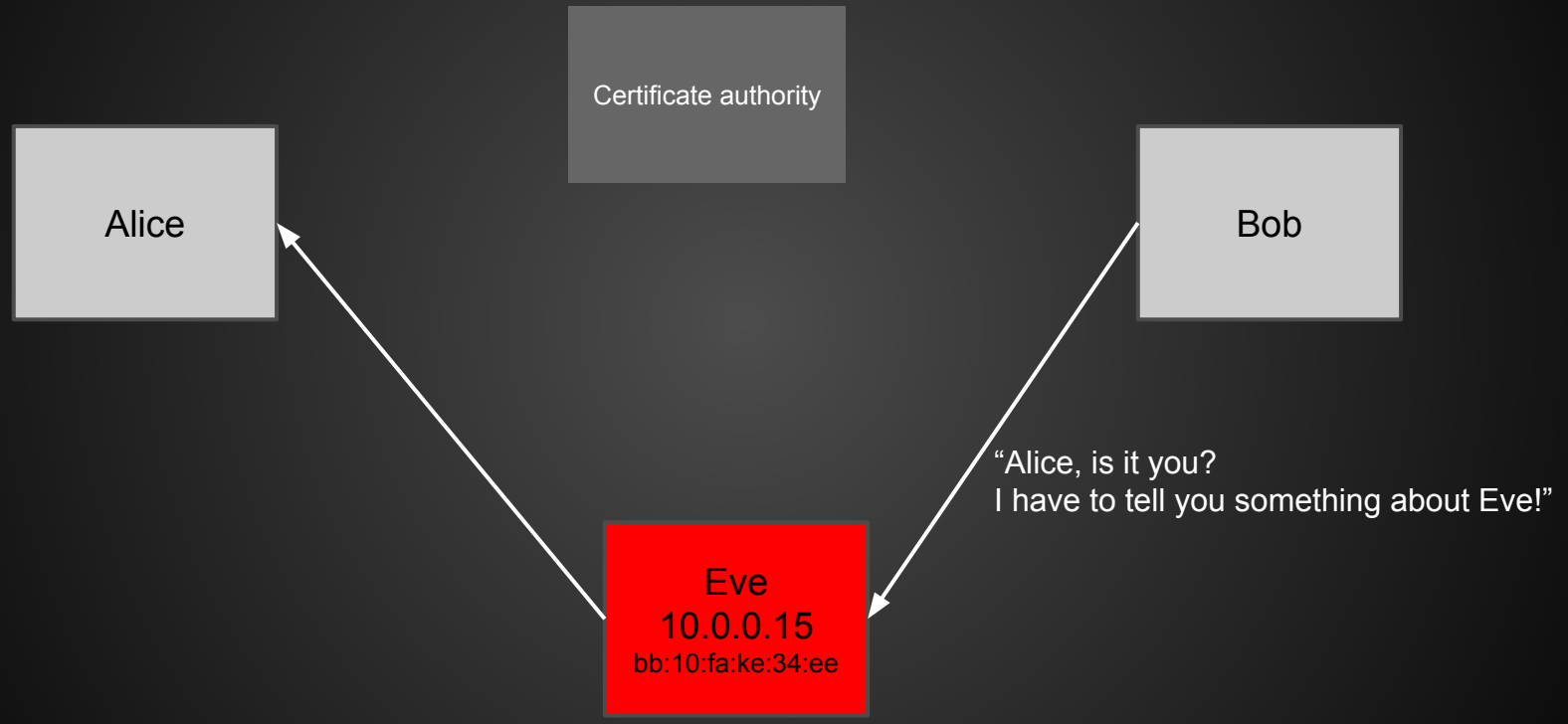
Secure connections



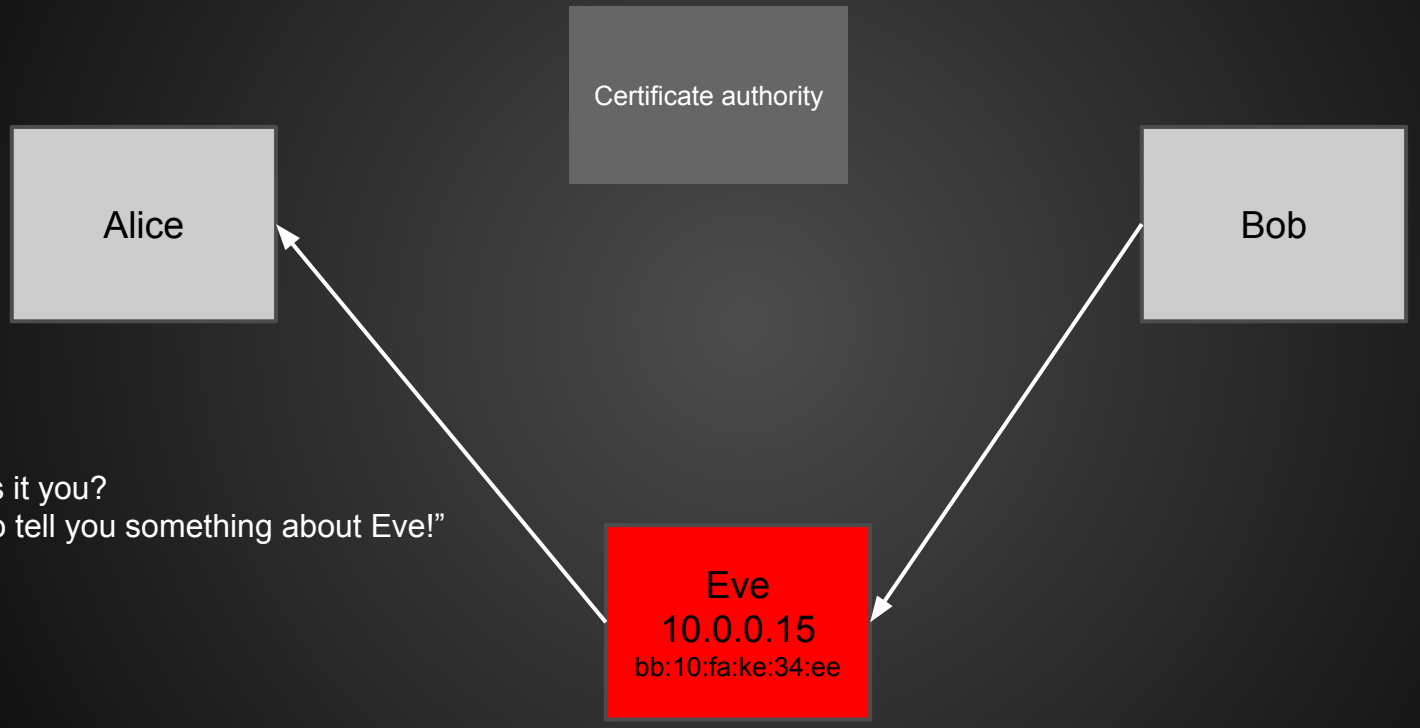
Secure connections



Secure connections (with ARP spoofing)

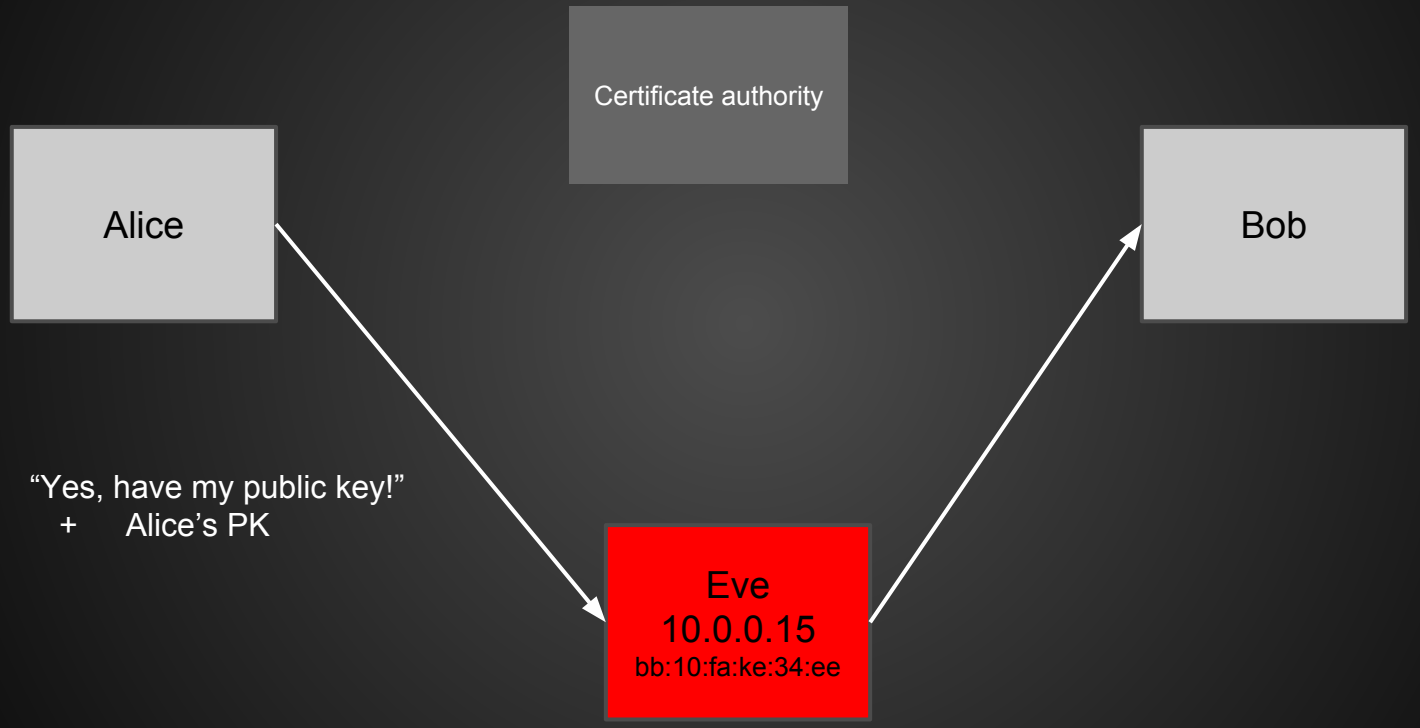


Secure connections (with ARP spoofing)

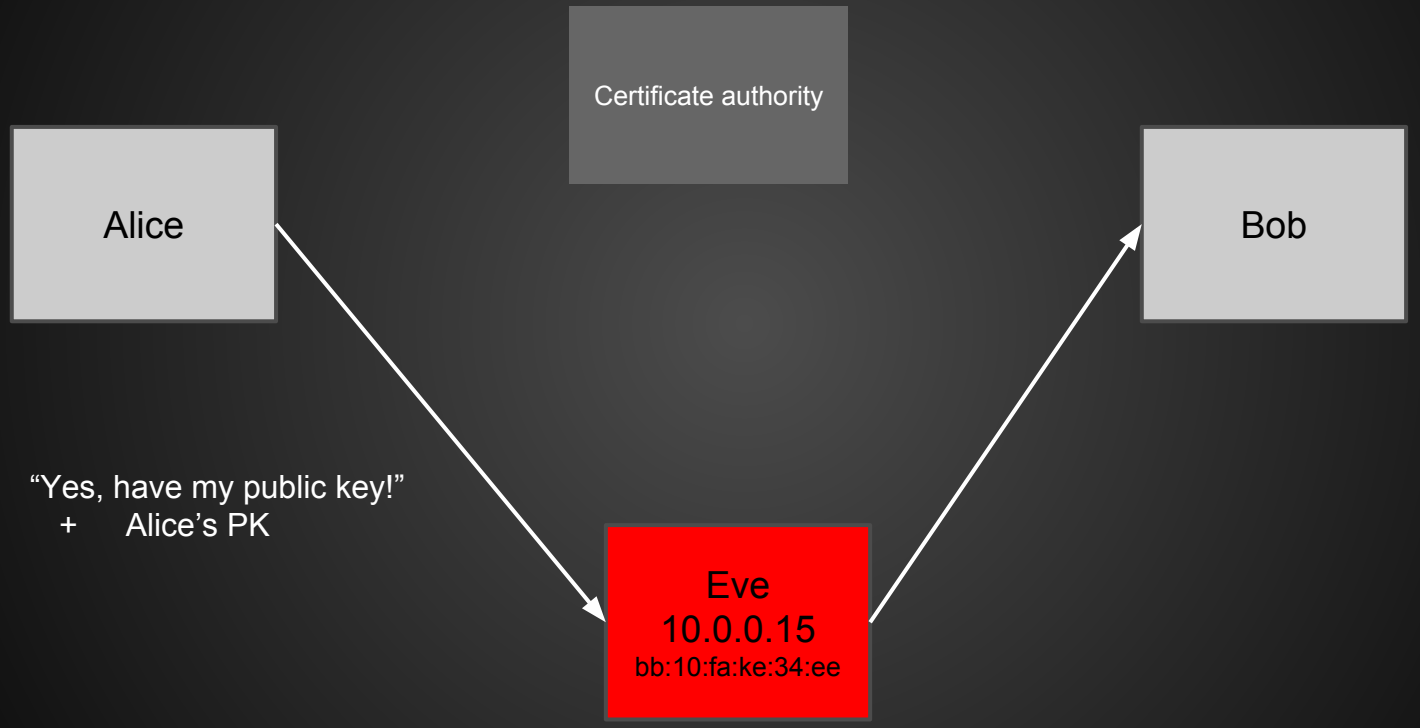


“Alice, is it you?
I have to tell you something about Eve!”

Secure connections (with ARP spoofing)

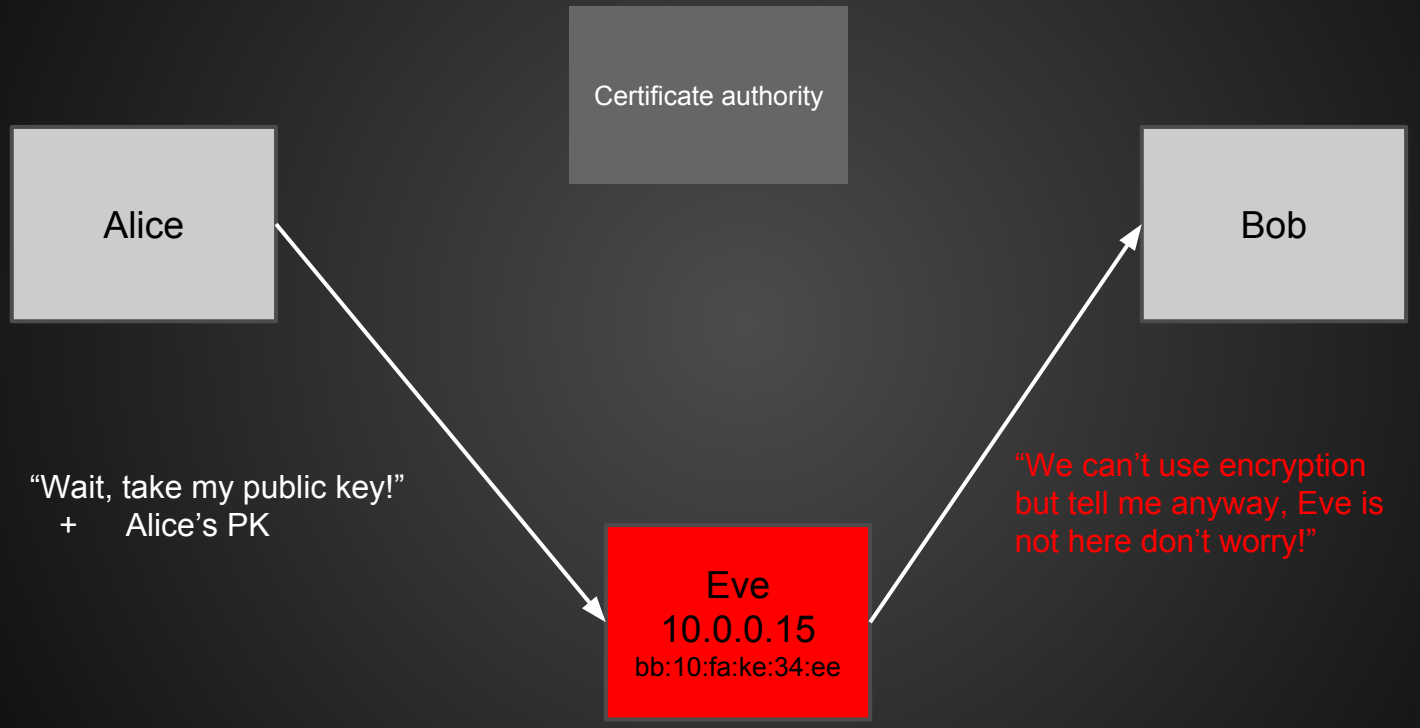


Secure connections (with ARP spoofing)

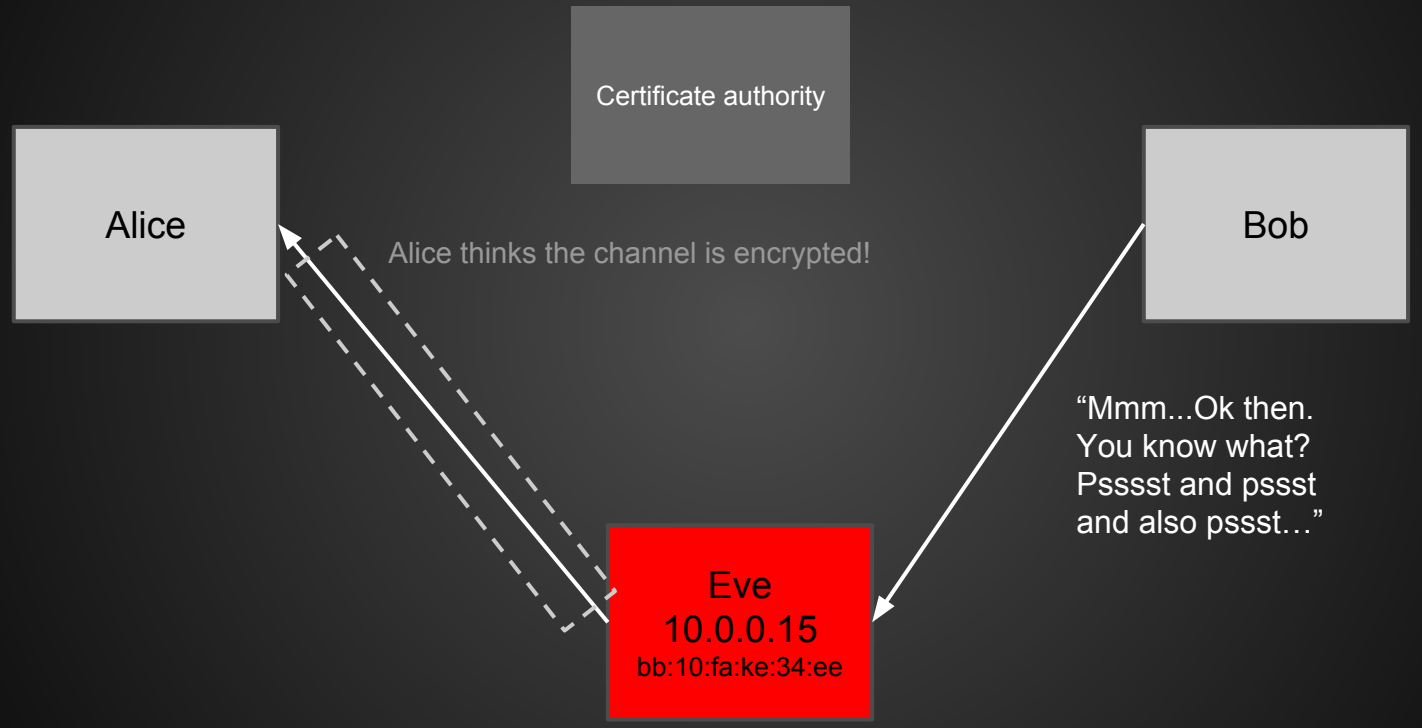


“Mmm...If I change the key the CA will tell Bob it’s not Alice’s...”

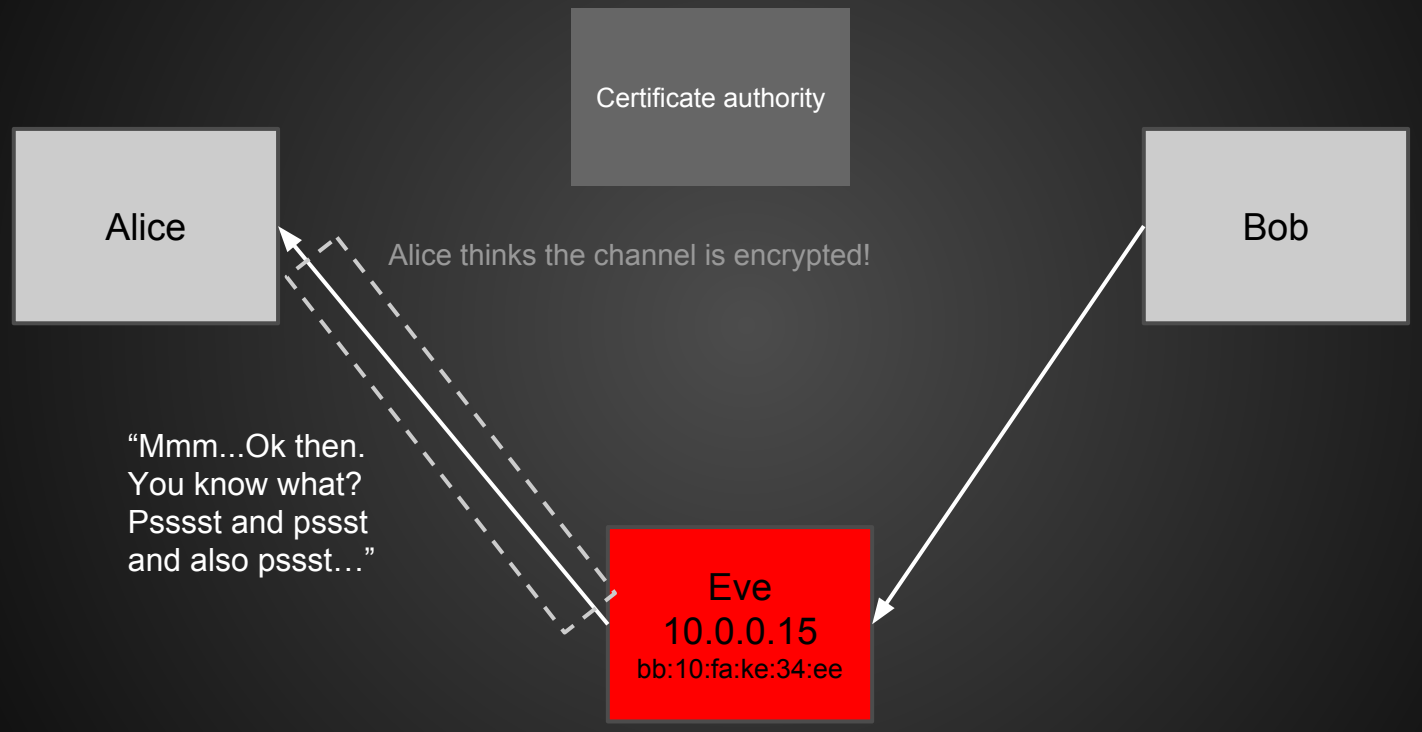
Secure connections (with ARP spoofing)



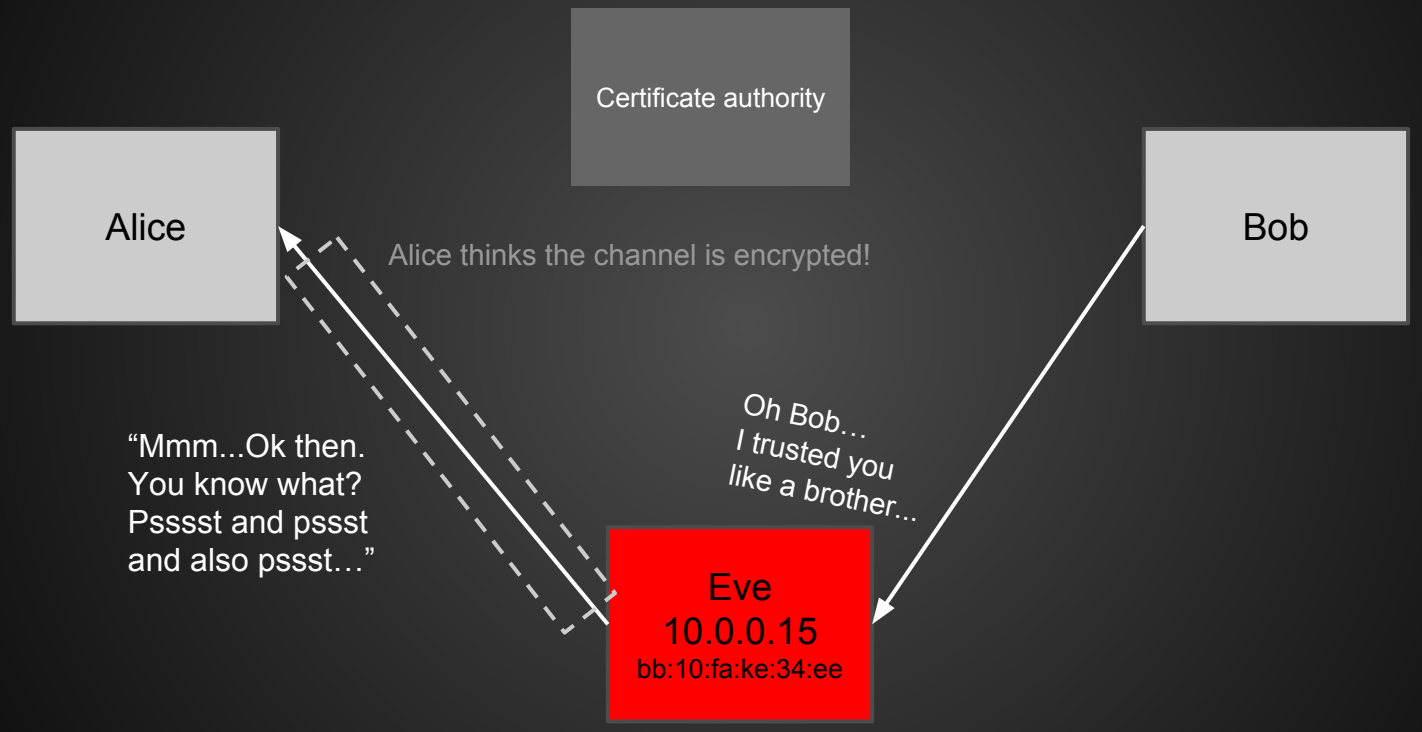
Secure connections (with ARP spoofing)



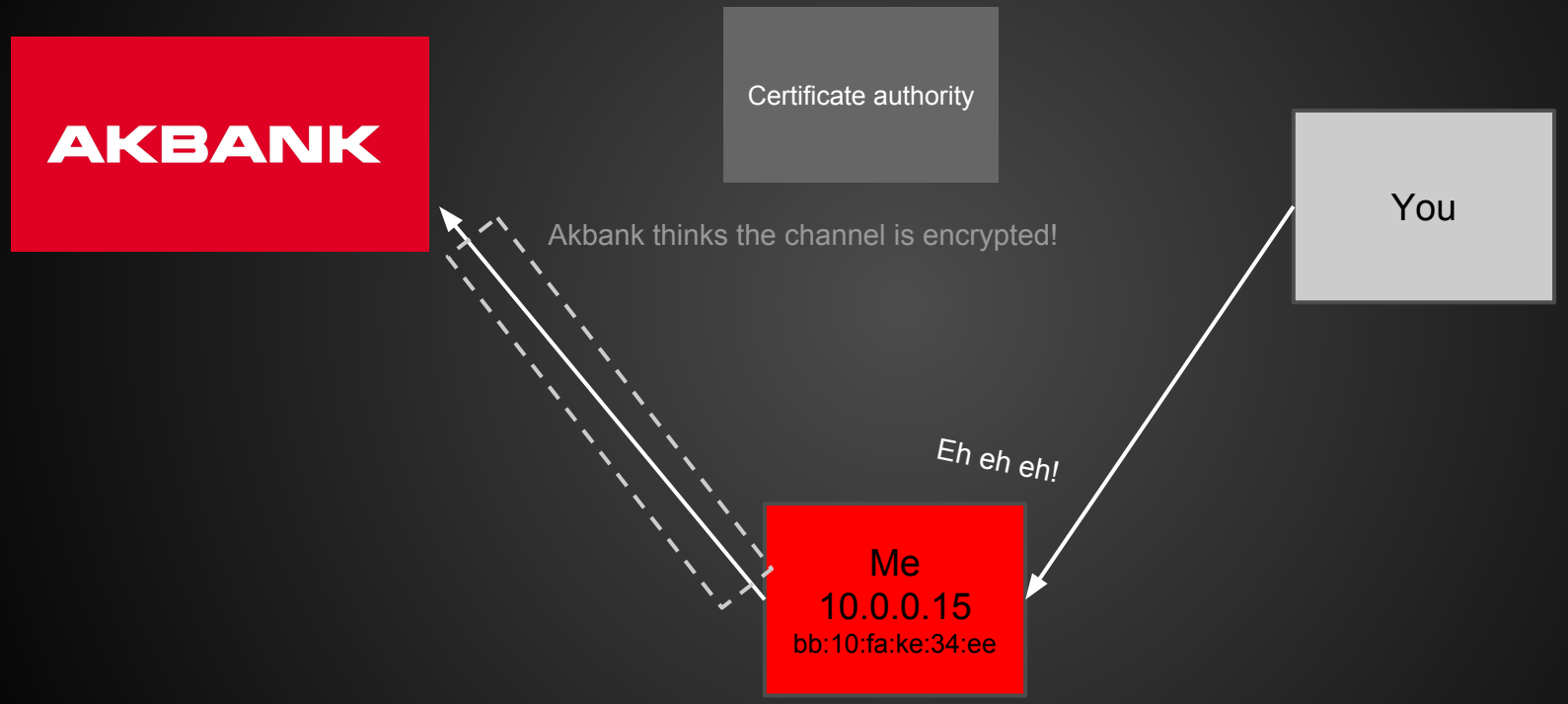
Secure connections (with ARP spoofing)



Secure connections (with ARP spoofing)



Secure connections (with ARP spoofing)



Any volunteer?

:)

Some notes

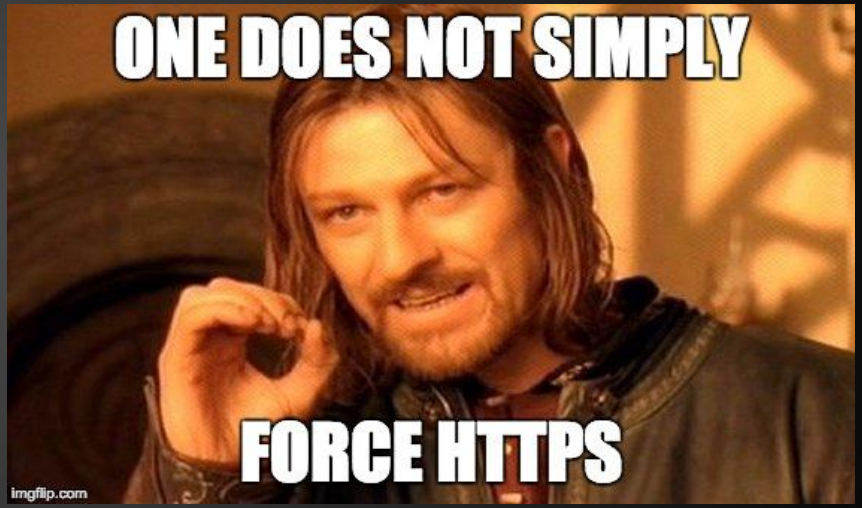
- If the request is directed to an HTTPS URL we can only replace the certificate (and trigger the RSOD).
- If the browser “knows” that a website is supposed to be accessed via HTTPS it will try to do so.
- Client isolation is a “solution” (see WiSpotter).

“We are good man, we redirect all requests to HTTPS”

A story about lack of awareness

Ways to “force” HTTPS

1. HTTP 30X from the server (useless since we intercept the requests)
2. Disable unencrypted server (impractical in most cases)
3. Force the browser to use HTTPS (no control from the server and... How many of you do it anyway?)
4. Force the browser to look up the domain in a list and determine whether to allow unencrypted connections (HSTS)



Internal redirect with HSTS

Certificate authority

Bob

GET google.com

Eve
10.0.0.15
bb:10:fa:ke:34:ee

Internal redirect with HSTS

Certificate authority

Bob

GET google.com

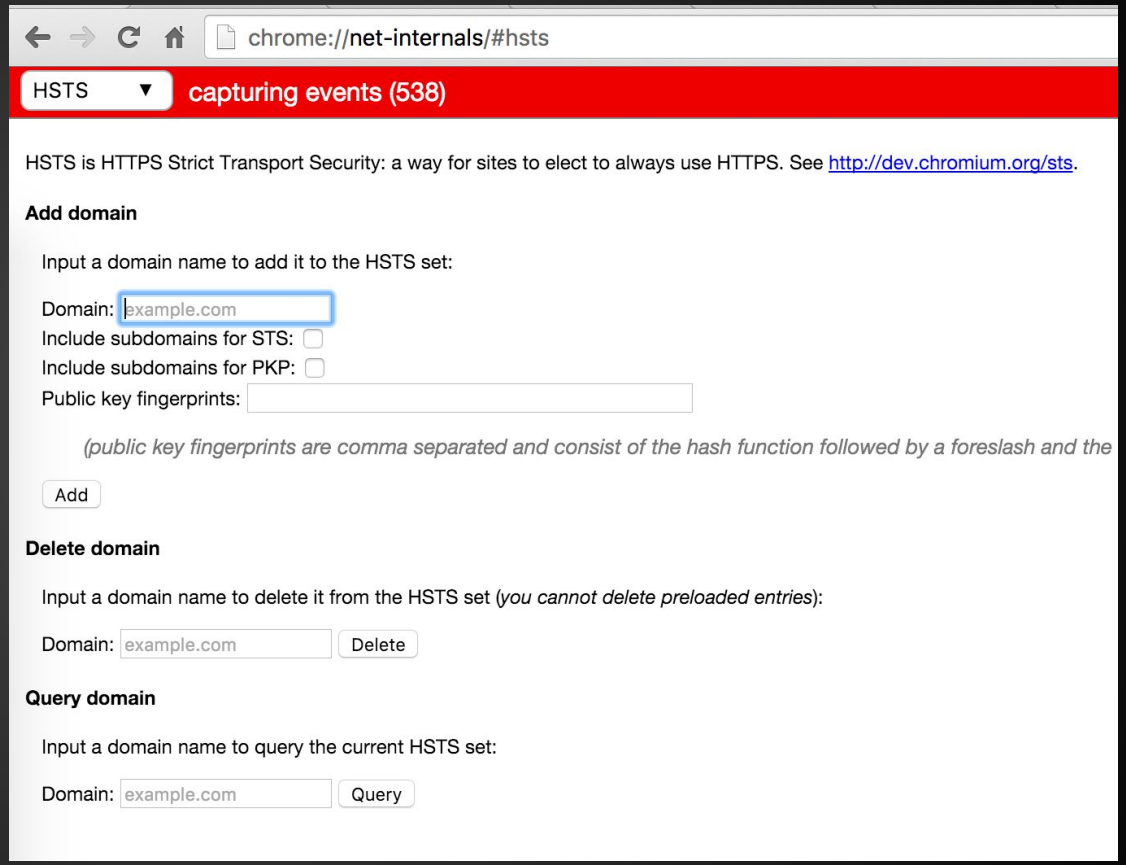
Eve
10.0.0.15
bb:10:fa:ke:34:ee

▼General
Request URL: http://facebook.com/
Request Method: GET
Status Code: 307 Internal Redirect

▼Response Headers
Location: https://facebook.com/
Non-Authoritative-Reason: HSTS

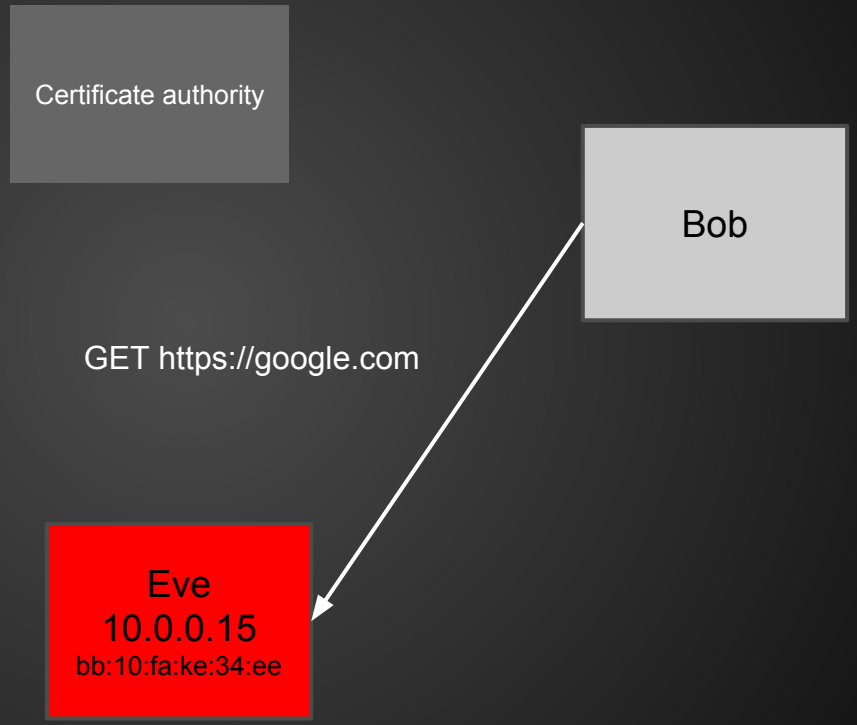
HSTS

New browsers come with a built-in list of websites that *cannot* (meh) use unencrypted connections. Example on Chrome ->



HSTS...less?


Google


Certificate authority
Bob
GET https://google.com
Eve
10.0.0.15
bb:10:fa:ke:34:ee

HSTS...less?

Certificate authority

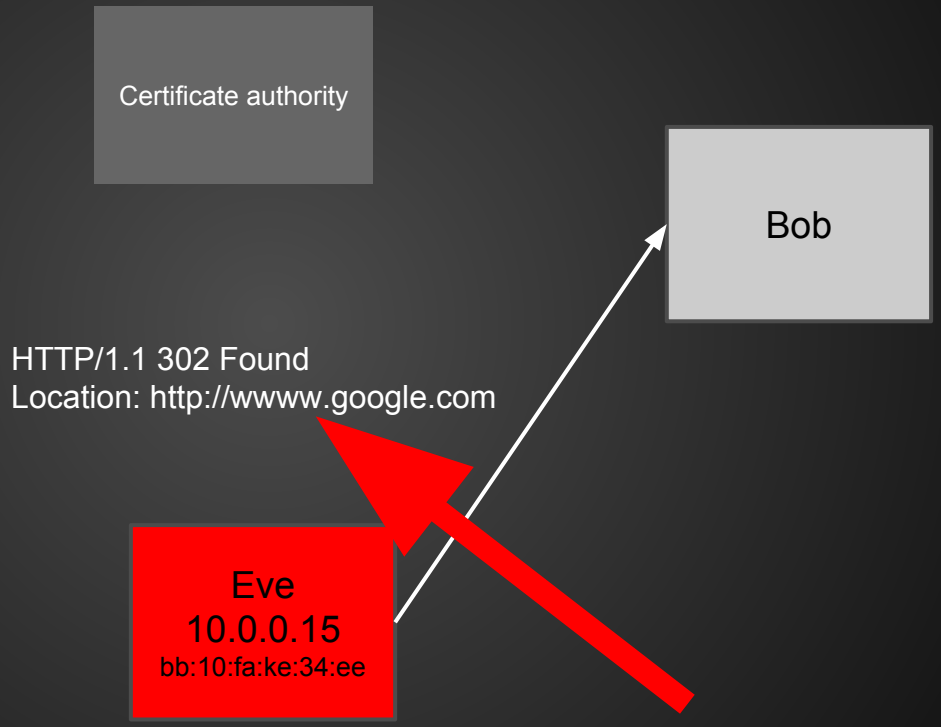
Bob

HTTP/1.1 302 Found
Location: https://wwww.google.com

Eve
10.0.0.15
bb:10:fa:ke:34:ee

HSTS...less?


Google


Certificate authority
Bob
HTTP/1.1 302 Found
Location: http://wwww.google.com
Eve
10.0.0.15
bb:10:fa:ke:34:ee

HSTS...less?

Certificate authority

??? WTF is wwww.google.com??

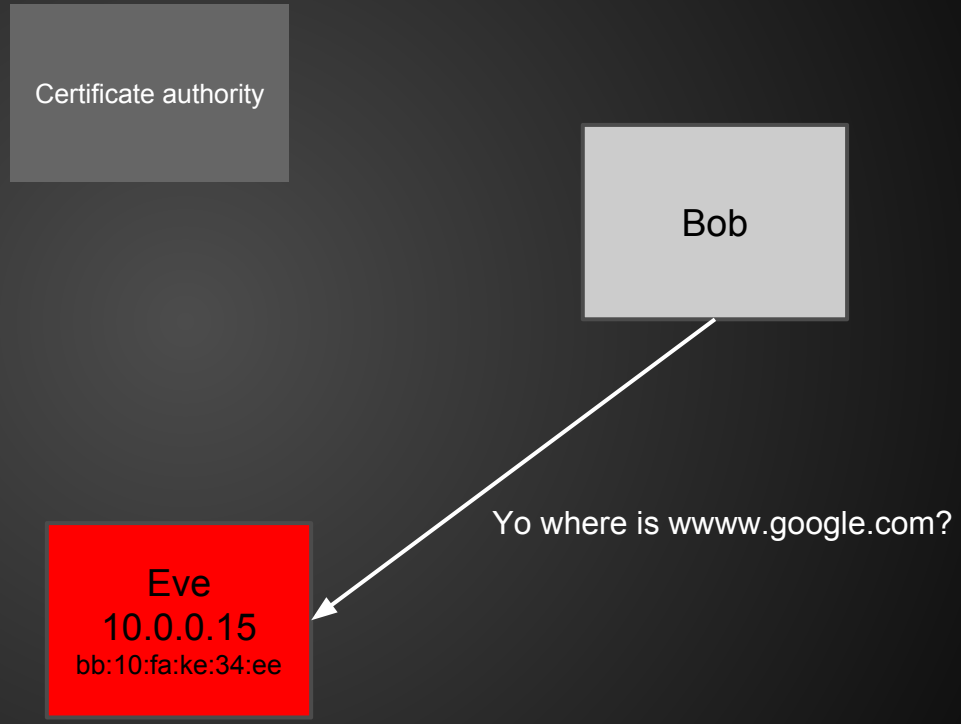
Bob

HTTP/1.1 302 Found
Location: http://wwww.google.com

Eve
10.0.0.15
bb:10:fa:ke:34:ee

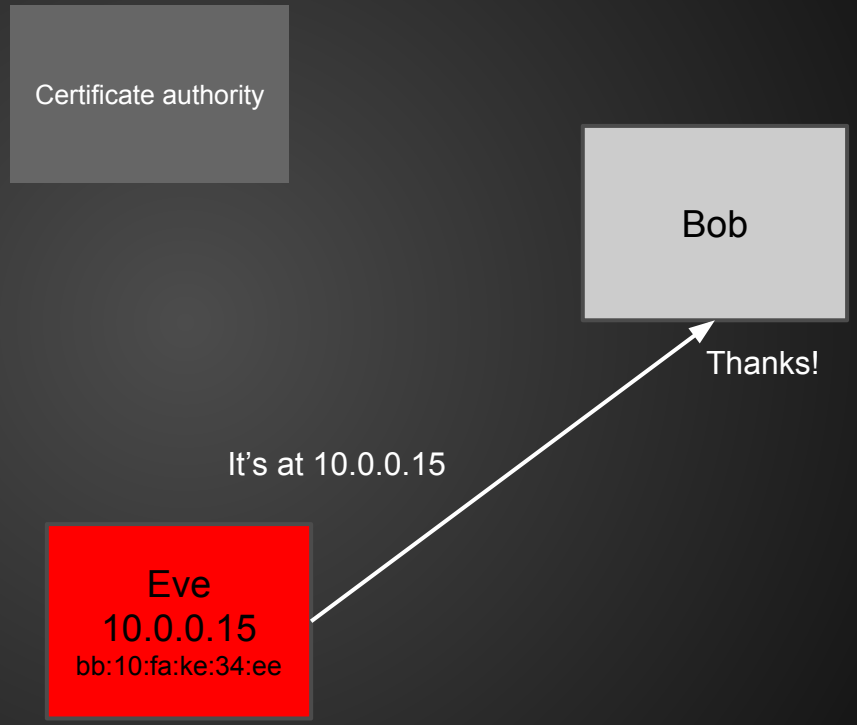
HSTS...less?


Google


Certificate authority
Bob
Yo where is wwww.google.com?
Eve
10.0.0.15
bb:10:fa:ke:34:ee

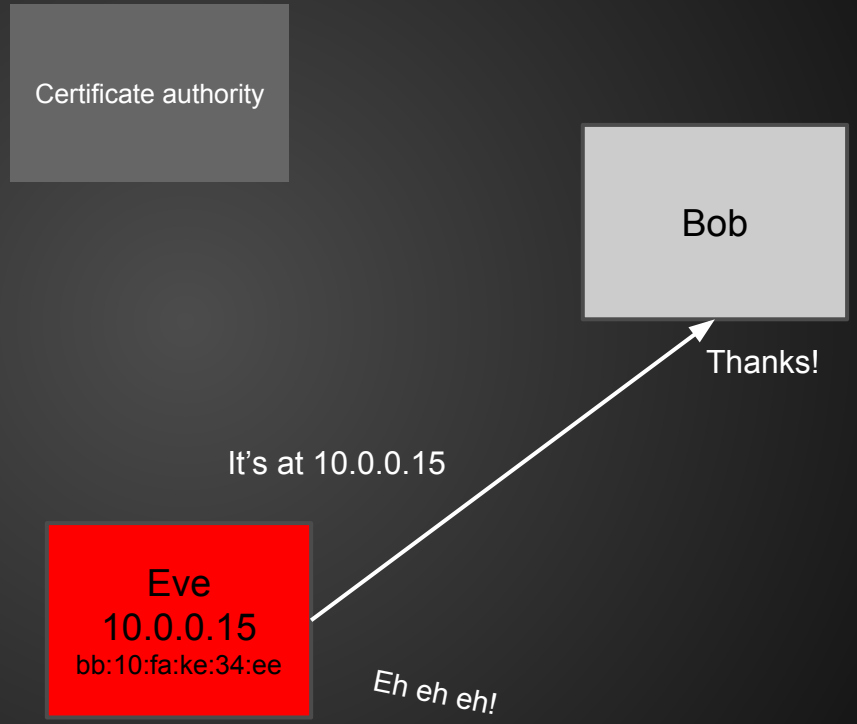
HSTS...less?


Google


Certificate authority
Bob
Thanks!
It's at 10.0.0.15
Eve
10.0.0.15
bb:10:fa:ke:34:ee

HSTS...less?


Google


Certificate authority
Bob
Thanks!
It's at 10.0.0.15
Eve
10.0.0.15
bb:10:fa:ke:34:ee
Eh eh eh!

HSTS...less?

Certificate authority

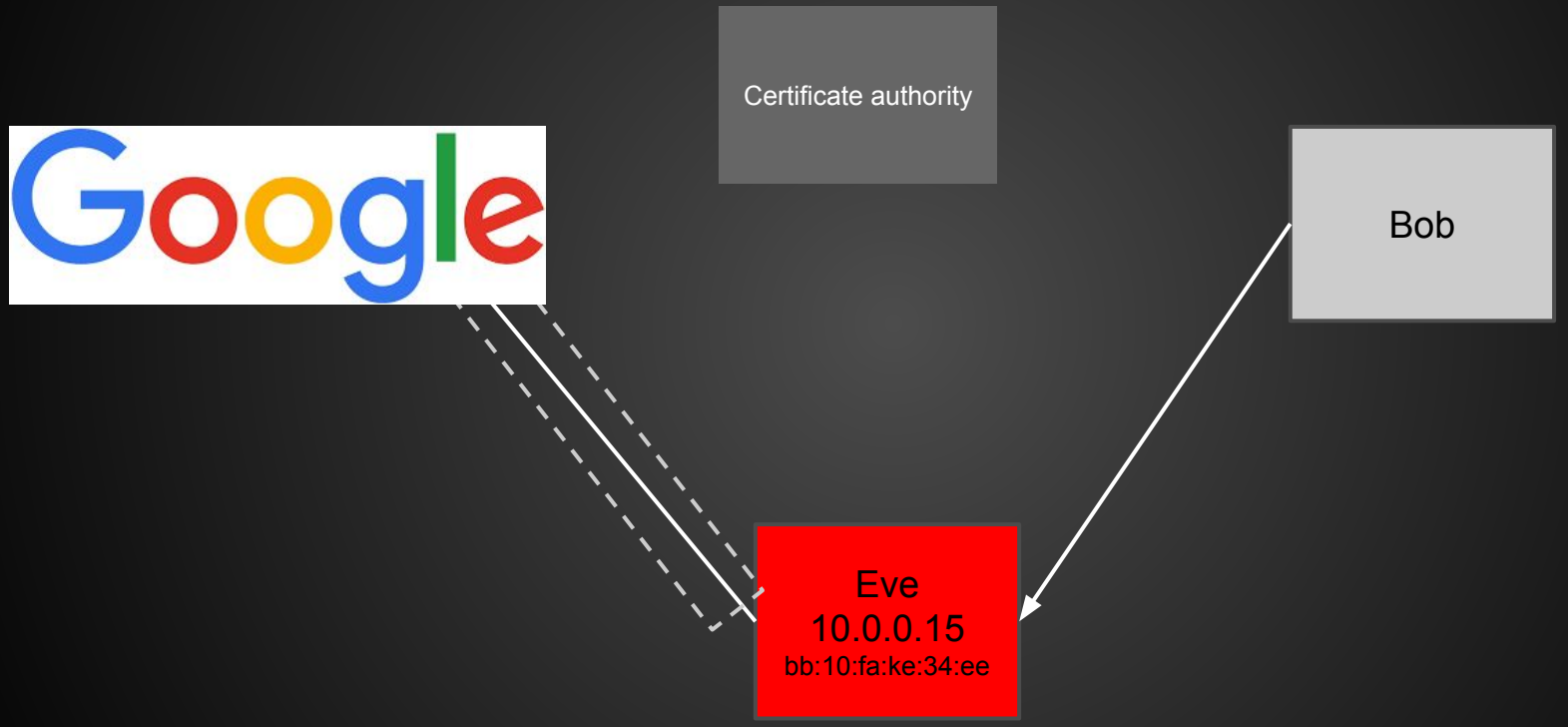
Bob

GET wwww.google.com

NOT IN THE HSTS!!

Eve
10.0.0.15
bb:10:fa:ke:34:ee

And the game continues...



References

- MITMf https://github.com/byt3bl33d3r/MITMf
- Kinda tutorial http://null-byte.wonderhowto.com/how-to/defeating-hsts-and-bypassing-https-with-dns-server-changes-and-mitmf-0162322/
- Kali Linux https://www.kali.org/

Remember the disclaimer!

Do you think GSM is better?

That’s for another story...