Sniffing and Not Getting Sniffed

Some Foundations on Communicating Secrets Between Systems

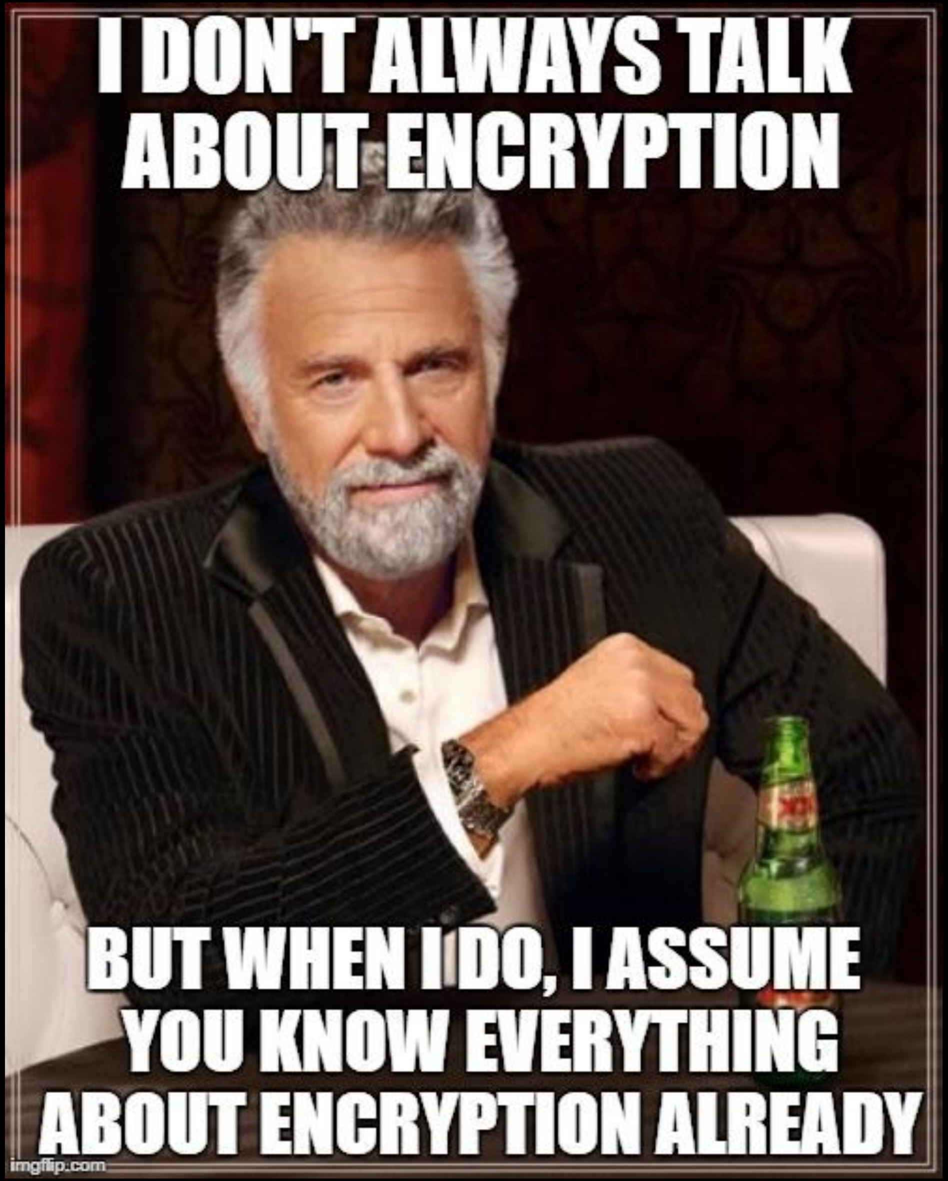
John Haldeman – Hackforge – May 2017

Why?

1) Randy is about to talk to you about let’s encrypt

2) Many people in this domain assume that you already know something about encryption

3) This presentation is going to try to ground you in the base concepts

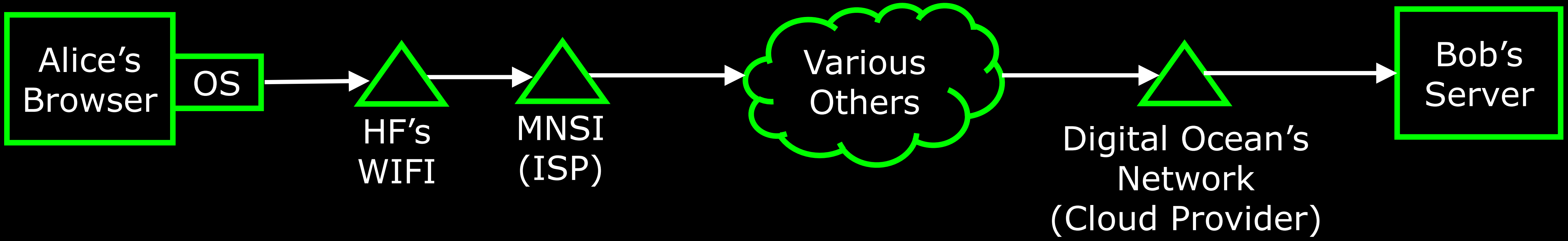

I DON'T ALWAYS TALK ABOUT ENCRYPTION
BUT WHEN I DO, I ASSUME YOU KNOW EVERYTHING ABOUT ENCRYPTION ALREADY
imgflip.com

Topics

- Goals and Problems:
  - Sniffing
  - Man in the Middle
- Classes of Encryption:
  - Symmetric Encryption
  - Asymmetric Encryption
- Certificates
- What SSL/TLS Doesn’t Absolve You From
- Responsibilities in Encryption on the Wire:
  - The User
  - The Application (site/server)
  - OS/Browser
- Sniffing/MITM as a Security Mechanism

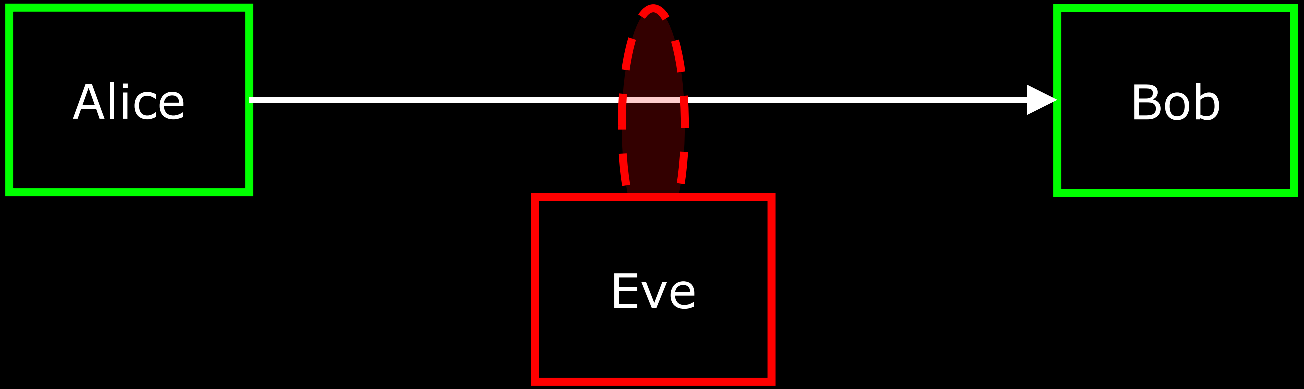
Problem: Intermediaries

Sending Data Through a Network Involves Intermediaries



Sniffing

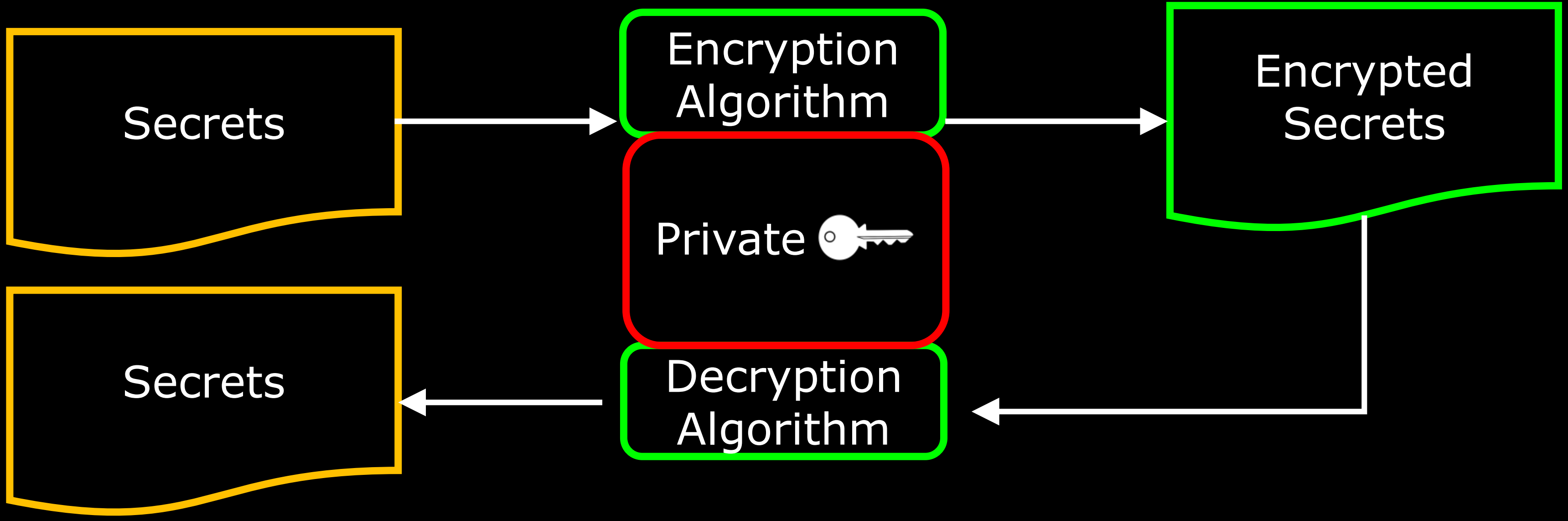
Sniffing is the process of intercepting and making use of the transmitted network data.



Goal: Keep secrets from Eve – She can see the network traffic, but it should not contain sensitive information

Symmetric Encryption

With symmetric encryption, you use a key to encrypt the data and the same key to decrypt it

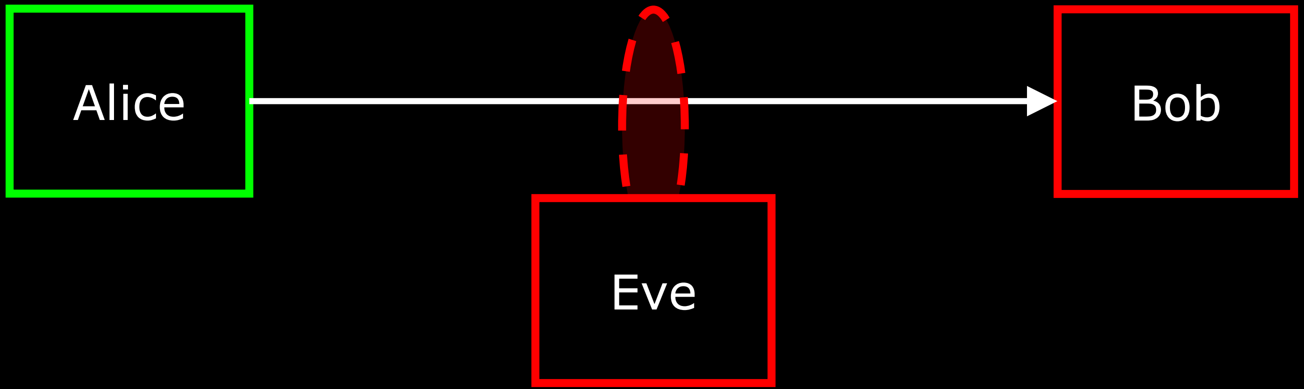


Problem: The private key is a secret. If the target does not know the key, it has to be communicated somehow

Symmetric Encryption

Where is this Useful?

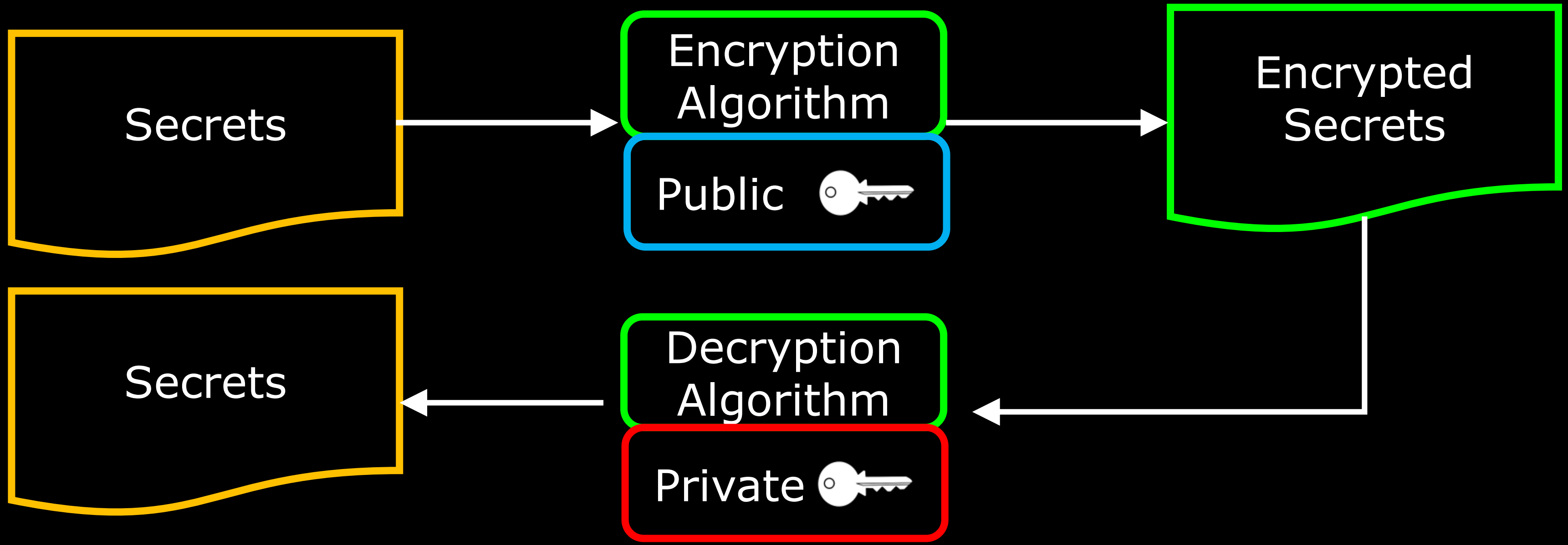
1) If you want Bob to store the data but not know the secrets (eg: Bob is a cloud storage provider)



2) If Alice and Bob don’t need to communicate the secret to each other (eg: the client and server are owned by the same person who manually enters the key)

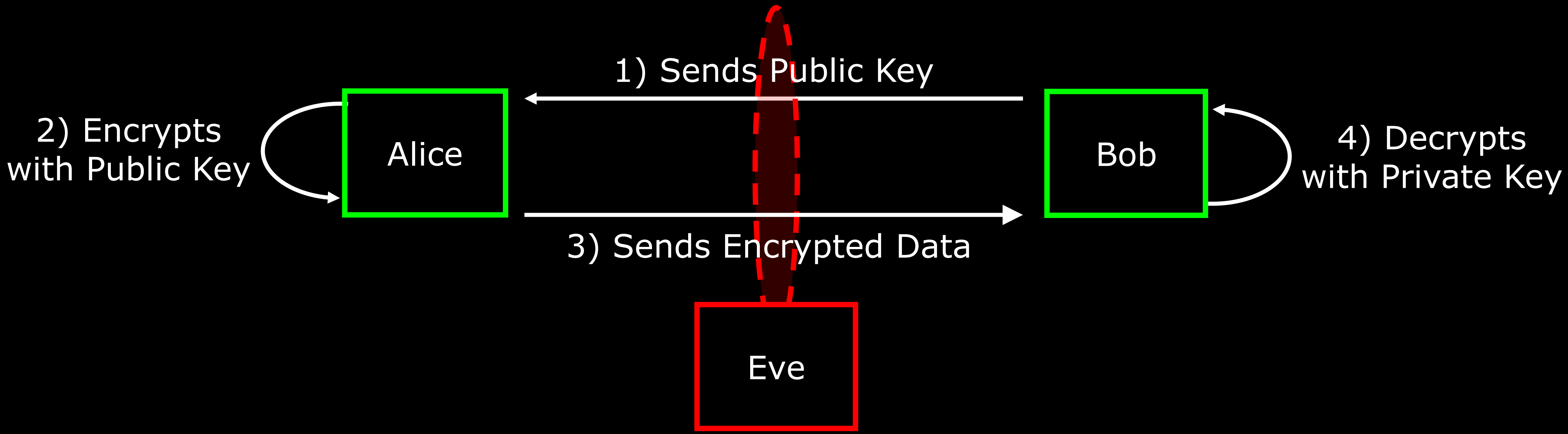
Asymmetric Encryption

With Asymmetric encryption, you use a public key to encrypt data and a secret (private) key to decrypt the data



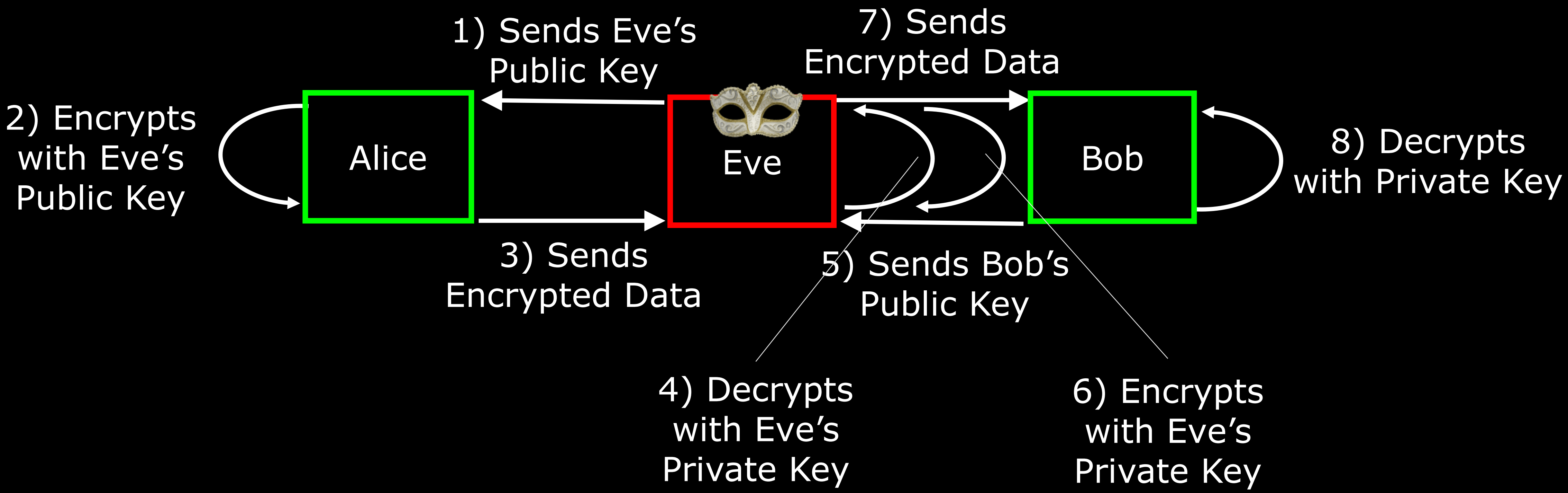
The only (practical) way to decrypt data encrypted with a public key is with its private key

Asymmetric Encryption



If Eve doesn’t control the communication, this is all you need.

Eve as a Man in the Middle (MITM)


1) Sends Eve’s Public Key
7) Sends Encrypted Data
2) Encrypts with Eve’s Public Key
Alice
Eve
Bob
8) Decrypts with Private Key
3) Sends Encrypted Data
5) Sends Bob’s Public Key
4) Decrypts with Eve’s Private Key
6) Encrypts with Eve’s Private Key

Eve can Masquerade as Bob! Drat! Foiled!

What’s a Certificate?

A document that includes:

1) The public key
2) Information about the site’s identity
3) A signature verifying the data is accurate

What’s a Signature?

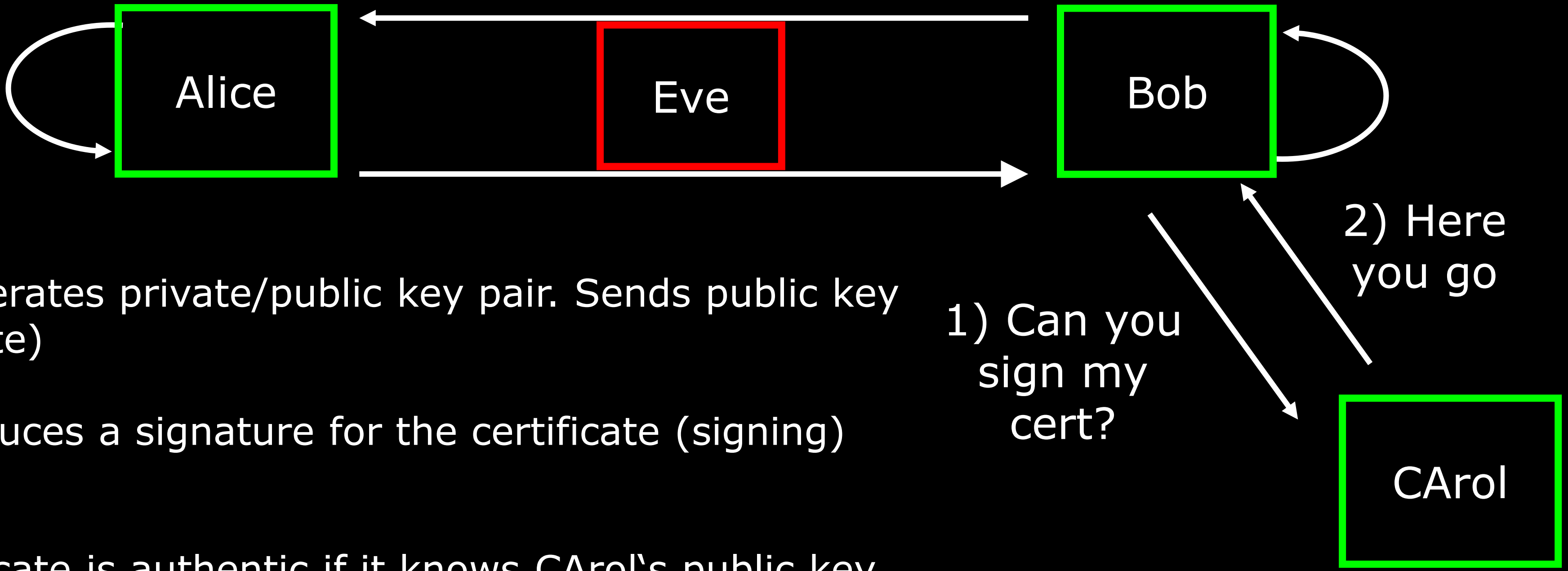
Take a private key from a trusted source

Generate a tag (signature) for a message you would later like to verify

Using the signature and the public key, you can verify the message

So, How Does Alice Confirm Bob's Certificate is Valid (and as a result knows the public key has not been misrepresented by Eve)?

- You Need a Trusted Certificate Source – A Certificate Authority (CA)



Certificate Scheme:

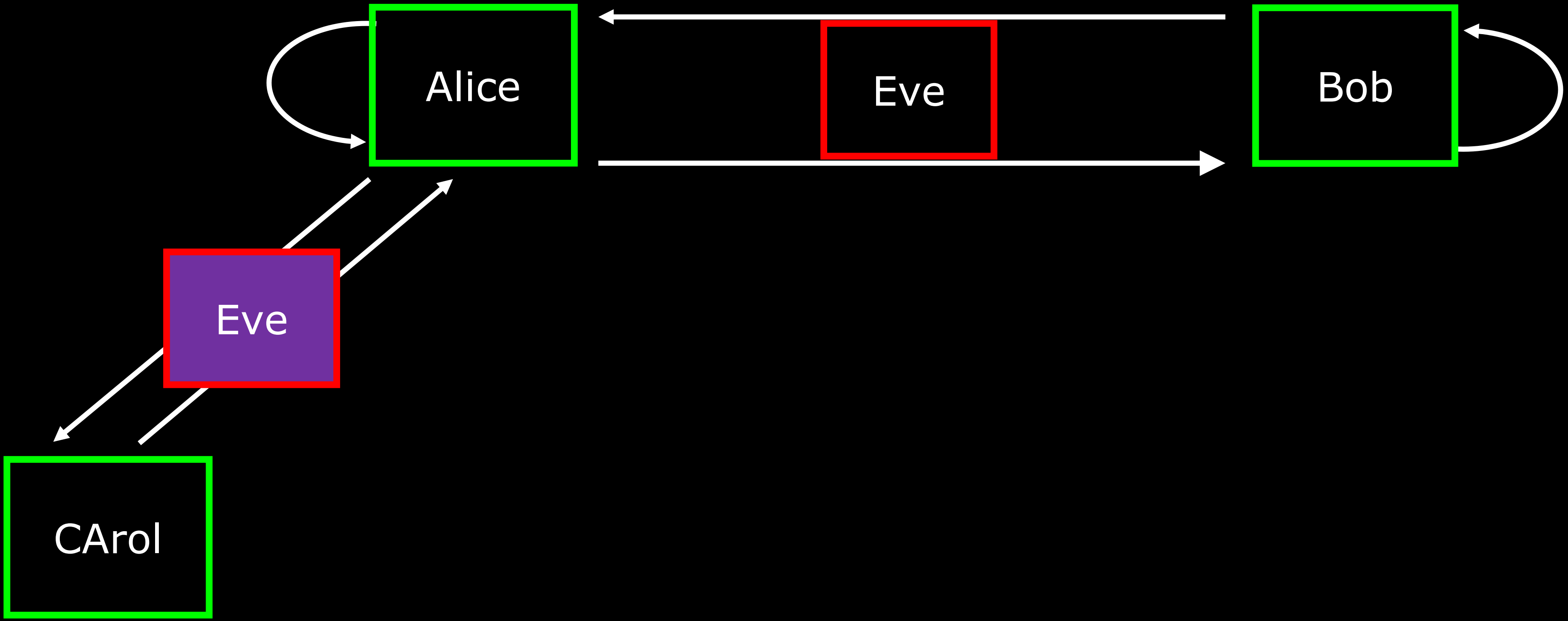
1) Key Generation: Bob generates private/public key pair. Sends public key to CA (inside the certificate)

2) Signing Request: CA produces a signature for the certificate (signing) using it's private key

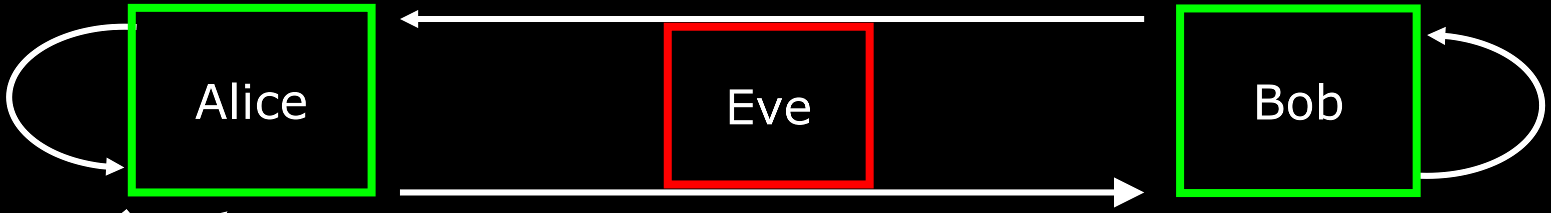
3) Alice can verify the certificate is authentic if it knows CArol's public key

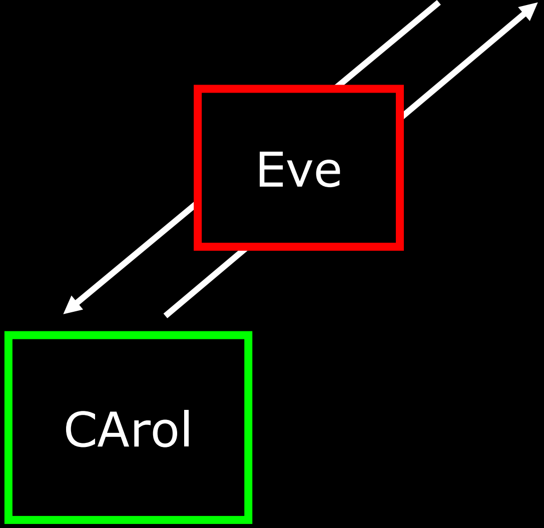
If you’re paying attention…

- Whoa, whoa, whoa – How does Alice key CArol‘s public key in order to verify the signature???

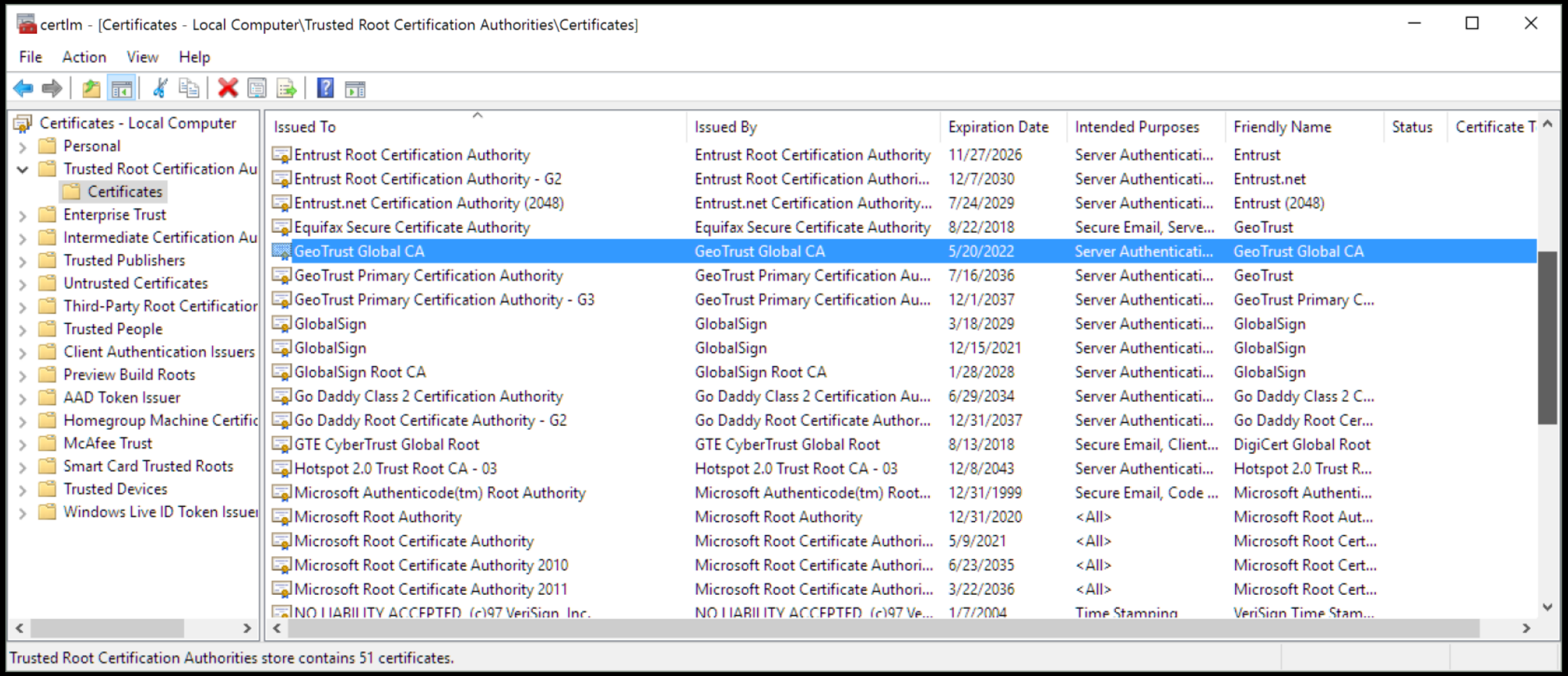


CA Lists





You cheat a bit and pre-distribute CA certificates (which includes their public keys) with the OS/Browser:


certlm - [Certificates - Local Computer\Trusted Root Certification Authorities\Certificates]

File
Action
View
Help
Certificates - Local Computer
Personal
Trusted Root Certification Au
Certificates
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Preview Build Roots
AAD Token Issuer
Homegroup Machine Certific
McAfee Trust
Smart Card Trusted Roots
Trusted Devices
Windows Live ID Token Issuer

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate T
Entrust Root Certification Authority	Entrust Root Certification Authority	11/27/2026	Server Authenticati...	Entrust		
Entrust Root Certification Authority - G2	Entrust Root Certification Authori...	12/7/2030	Server Authenticati...	Entrust.net		
Entrust.net Certification Authority (2048)	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)		
Equifax Secure Certificate Authority	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust		
GeoTrust Global CA	GeoTrust Global CA	5/20/2022	Server Authenticati...	GeoTrust Global CA		
GeoTrust Primary Certification Authority	GeoTrust Primary Certification Au...	7/16/2036	Server Authenticati...	GeoTrust		
GeoTrust Primary Certification Authority - G3	GeoTrust Primary Certification Au...	12/1/2037	Server Authenticati...	GeoTrust Primary C...		
GlobalSign	GlobalSign	3/18/2029	Server Authenticati...	GlobalSign		
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	GlobalSign		
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign		
Go Daddy Class 2 Certification Authority	Go Daddy Class 2 Certification Au...	6/29/2034	Server Authenticati...	Go Daddy Class 2 C...		
Go Daddy Root Certificate Authority - G2	Go Daddy Root Certificate Author...	12/31/2037	Server Authenticati...	Go Daddy Root Cer...		
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	DigiCert Global Root		
Hotspot 2.0 Trust Root CA - 03	Hotspot 2.0 Trust Root CA - 03	12/8/2043	Server Authenticati...	Hotspot 2.0 Trust R...		
Microsoft Authenticode(tm) Root Authority	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...		
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...		
Microsoft Root Certificate Authority	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Authority 2010	Microsoft Root Certificate Authori...	6/23/2035	<All>	Microsoft Root Cert...		
Microsoft Root Certificate Authority 2011	Microsoft Root Certificate Authori...	3/22/2036	<All>	Microsoft Root Cert...		
NO LIABILITY ACCEPTED, (c)97 VeriSign, Inc.	NO LIABILITY ACCEPTED, (c)97 Ve...	1/7/2004	Time Stamping	VeriSign Time Stam...		

Trusted Root Certification Authorities store contains 51 certificates.

What SSL/TLS Doesn’t Absolve You From

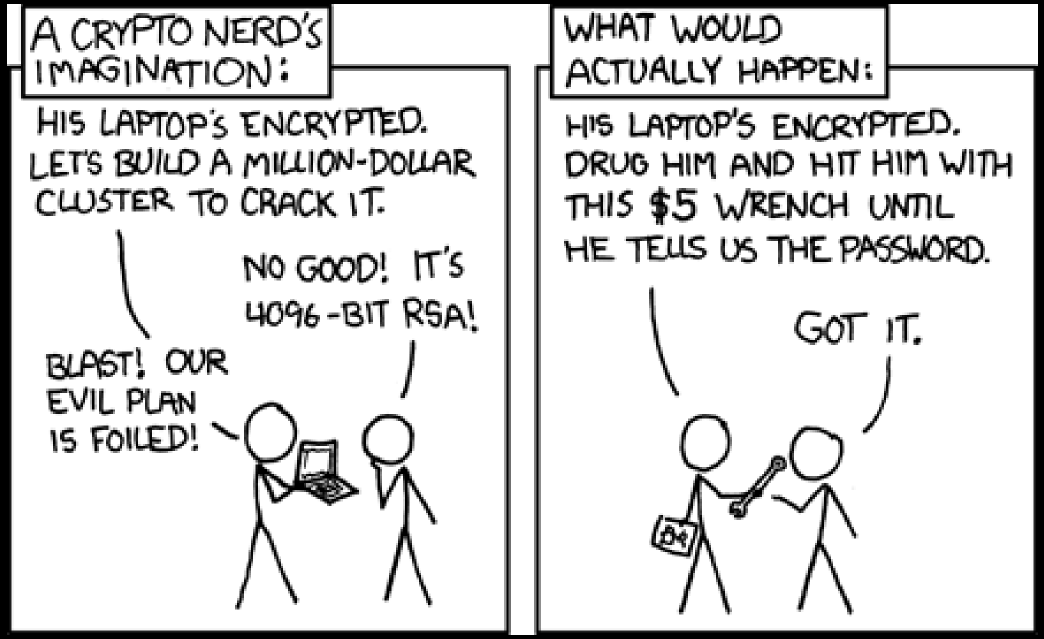
1) Building Secure Applications

2) Having Secure Infrastructure

3) Social Engineering

4) Compromised Clients

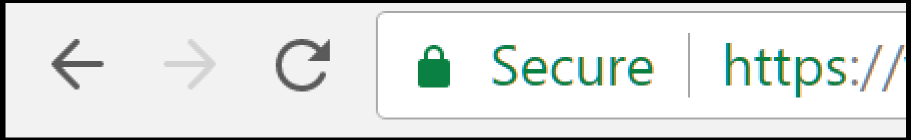
5) Compromised Servers


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

There are no security/privacy panaceas – just because there’s a green lock in your browser, it doesn’t mean you are perfectly safe – just safe from sniffing

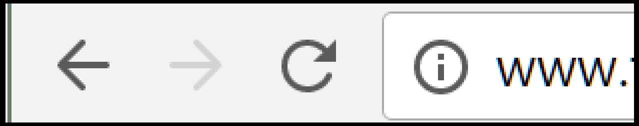
User Responsibilities

- Look for a green lock



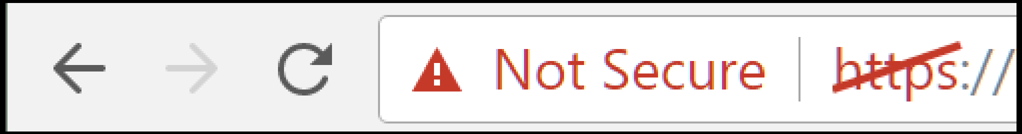
User Responsibilities

- If you don’t see https and a green lock, don’t send anything you would not put on a postcard in the mail (this applies to most emails too):



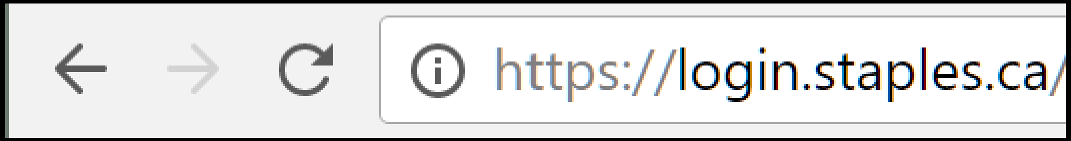
www.

- As a user, you probably shouldn’t go to sites that look like this:



Not Secure ~~https~~://

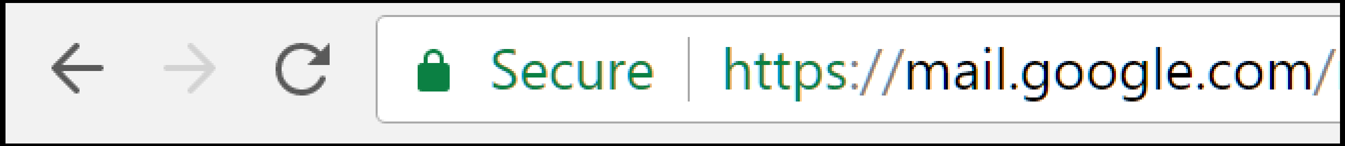
- This is kind of mostly sort of encrypted (*sigh*):



https://login.staples.ca/

User Responsibilities

- Look at the Domain Name – Make Sure it makes sense. That’s what’s been verified by the CA



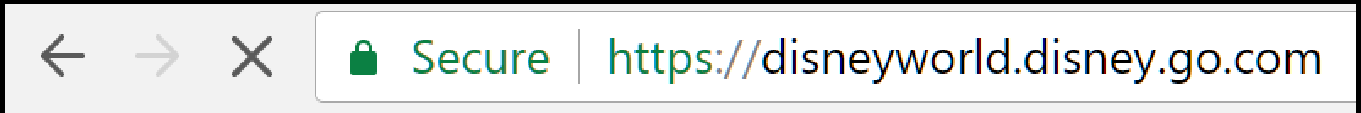
Secure | https://mail.google.com/

Application Responsibilities

- Consider erring on the side of encrypting – Let’s Encrypt aims to make this as easy/cheap as possible

- Keep your servers secure (certs are only as good as the secrets on the server)

- Pet Peeve: Don’t get cute with your domain names (this is Disneyworld’s actual home page):



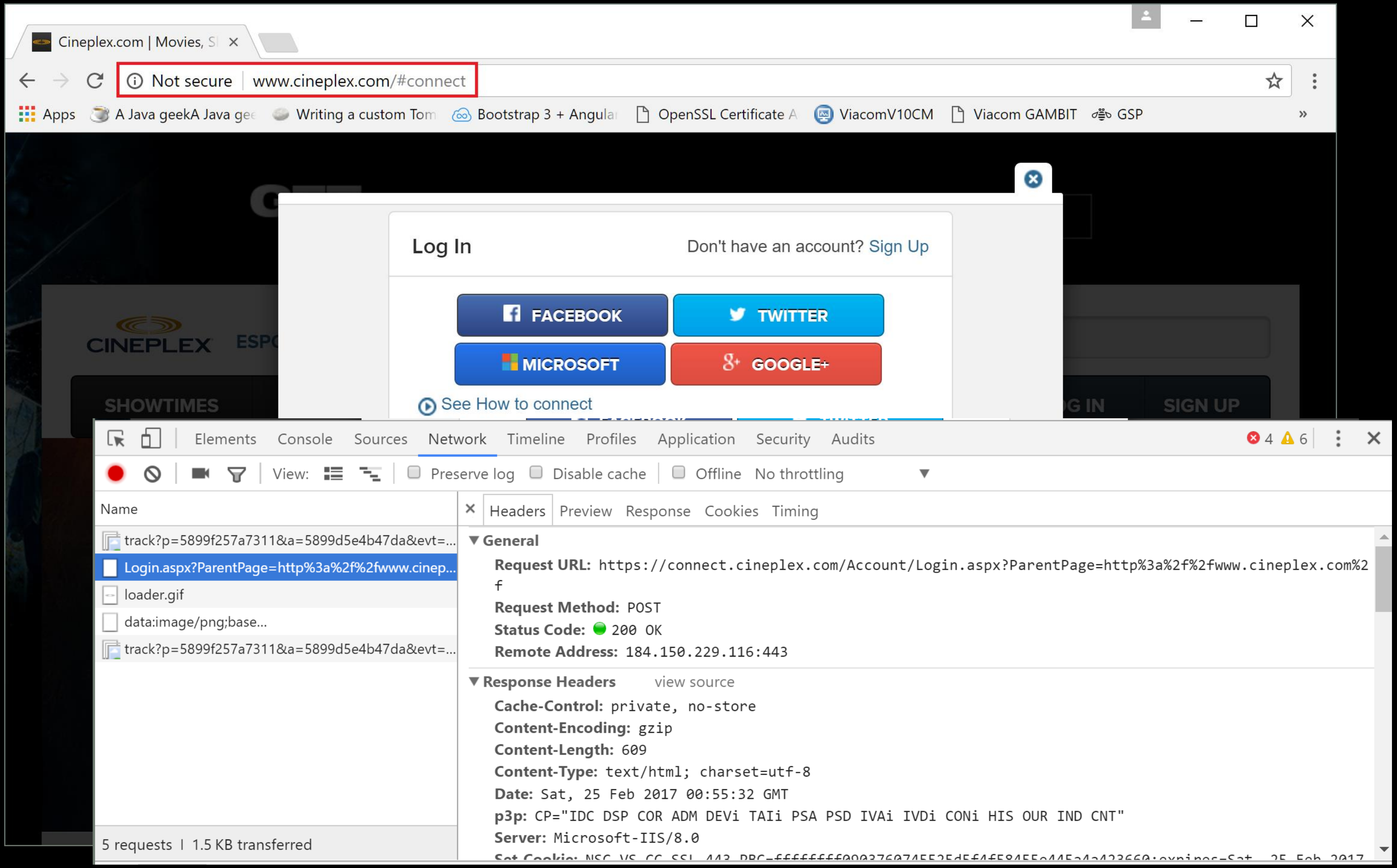
Secure | https://disneyworld.disney.go.com

  - There’s a kind of attack that uses legitimate-looking domain names that are actually malicious. For example stuff like the following is designed to look like Facebook but isn’t:
    - facebook-fb.com
    - facebook.account.com

Application Responsibilities

- Another Pet Peeve – Hidden HTTPS requests for logins behind plain old http sites

- The certificate information and user participation in security is eliminated here



```
Name
track?p=5899f257a7311&a=5899d5e4b47da&evt=...
Login.aspx?ParentPage=http%3a%2f%2fwww.cinep...
loader.gif
data:image/png;base...
track?p=5899f257a7311&a=5899d5e4b47da&evt=...
5 requests | 1.5 KB transferred
```

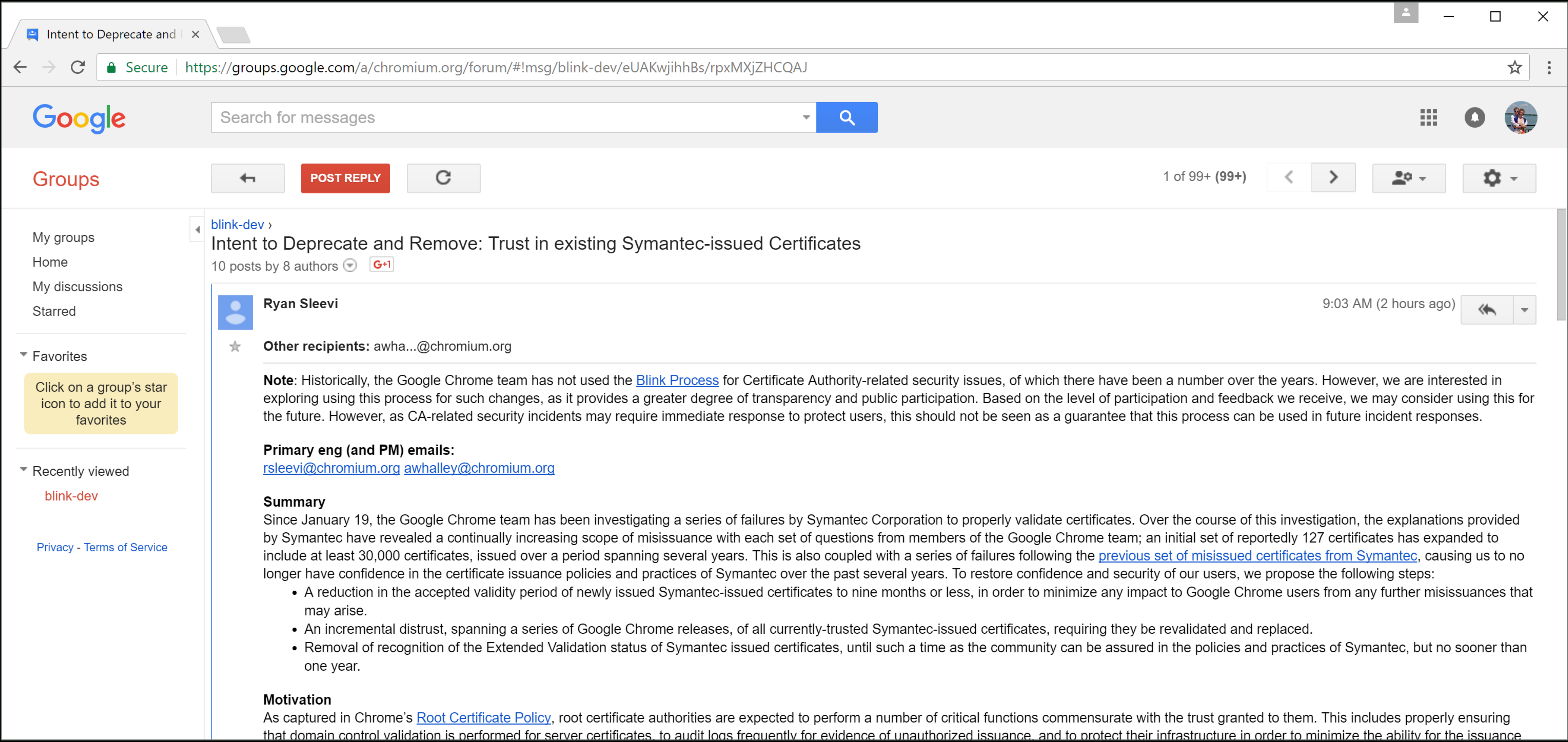
```
▼ General
   Request URL: https://connect.cineplex.com/Account/Login.aspx?ParentPage=http%3a%2f%2fwww.cineplex.com%2
   f
   Request Method: POST
   Status Code: ● 200 OK
   Remote Address: 184.150.229.116:443
▼ Response Headers     view source
   Cache-Control: private, no-store
   Content-Encoding: gzip
   Content-Length: 609
   Content-Type: text/html; charset=utf-8
   Date: Sat, 25 Feb 2017 00:55:32 GMT
   p3p: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
   Server: Microsoft-IIS/8.0
   Set-Cookie: NSC_VS_CC_SSL_443_PRC=ffffffff0903760745525d5f4f58455e445a4a423660;expires=Sat, 25 Feb 2017
```

OS/Browser Vendor Responsibilities

- Make sure your list of CAs is good

Superfish™
Search Visually

- Lenovo’s Superfish Incident (2015):
  - 3rd Party Software pre-loaded by Lenovo Injected a Root CA certificate onto certain Lenovo laptop models
  - The newly registered CA was effectively local – the private key for the CA was placed on every machine with superfish on it
  - In effect, anyone with superfish loaded was exposed to MITM attacks
  - This was done to inject ***ads*** into encrypted websites…


Intent to Deprecate and
Secure
https://groups.google.com/a/chromium.org/forum/#!msg/blink-dev/eUAKwjihhBs/rpxMXjZHCQAJ
Google
Search for messages
Groups
POST REPLY
1 of 99+ (99+)
My groups
Home
My discussions
Starred
Favorites
Click on a group's star icon to add it to your favorites
Recently viewed
blink-dev
Privacy - Terms of Service
blink-dev ›
G+1

Intent to Deprecate and Remove: Trust in existing Symantec-issued Certificates

10 posts by 8 authors

Ryan Sleevi

9:03 AM (2 hours ago)

Other recipients: awha...@chromium.org

Note: Historically, the Google Chrome team has not used the Blink Process for Certificate Authority-related security issues, of which there have been a number over the years. However, we are interested in exploring using this process for such changes, as it provides a greater degree of transparency and public participation. Based on the level of participation and feedback we receive, we may consider using this for the future. However, as CA-related security incidents may require immediate response to protect users, this should not be seen as a guarantee that this process can be used in future incident responses.

Primary eng (and PM) emails:
rsleevi@chromium.org awhalley@chromium.org

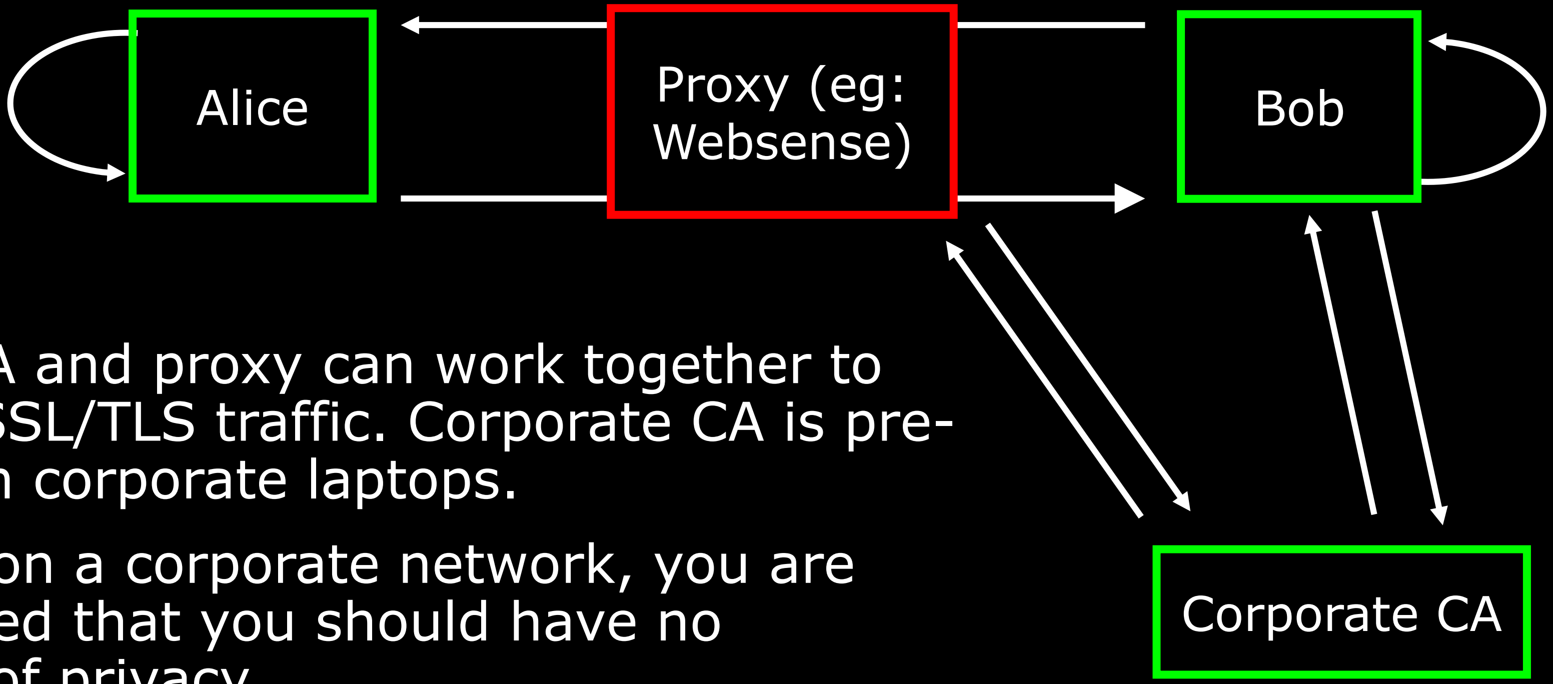
Summary
Since January 19, the Google Chrome team has been investigating a series of failures by Symantec Corporation to properly validate certificates. Over the course of this investigation, the explanations provided by Symantec have revealed a continually increasing scope of misissuance with each set of questions from members of the Google Chrome team; an initial set of reportedly 127 certificates has expanded to include at least 30,000 certificates, issued over a period spanning several years. This is also coupled with a series of failures following the previous set of misissued certificates from Symantec, causing us to no longer have confidence in the certificate issuance policies and practices of Symantec over the past several years. To restore confidence and security of our users, we propose the following steps:

- A reduction in the accepted validity period of newly issued Symantec-issued certificates to nine months or less, in order to minimize any impact to Google Chrome users from any further misissuances that may arise.
- An incremental distrust, spanning a series of Google Chrome releases, of all currently-trusted Symantec-issued certificates, requiring they be revalidated and replaced.
- Removal of recognition of the Extended Validation status of Symantec issued certificates, until such a time as the community can be assured in the policies and practices of Symantec, but no sooner than one year.

Motivation
As captured in Chrome's Root Certificate Policy, root certificate authorities are expected to perform a number of critical functions commensurate with the trust granted to them. This includes properly ensuring that domain control validation is performed for server certificates, to audit logs frequently for evidence of unauthorized issuance, and to protect their infrastructure in order to minimize the ability for the issuance

Proxying to Allow/Deny/Modify

- It’s common practice on a lot of corporate networks (and on home “Internet Security Packages”) to proxy their users and attempt to try prevent bad things from happening. They do this with proxies and local certificates/CAs (hmmmm…….)
- Done to protect corporate networks while providing users access to the internet

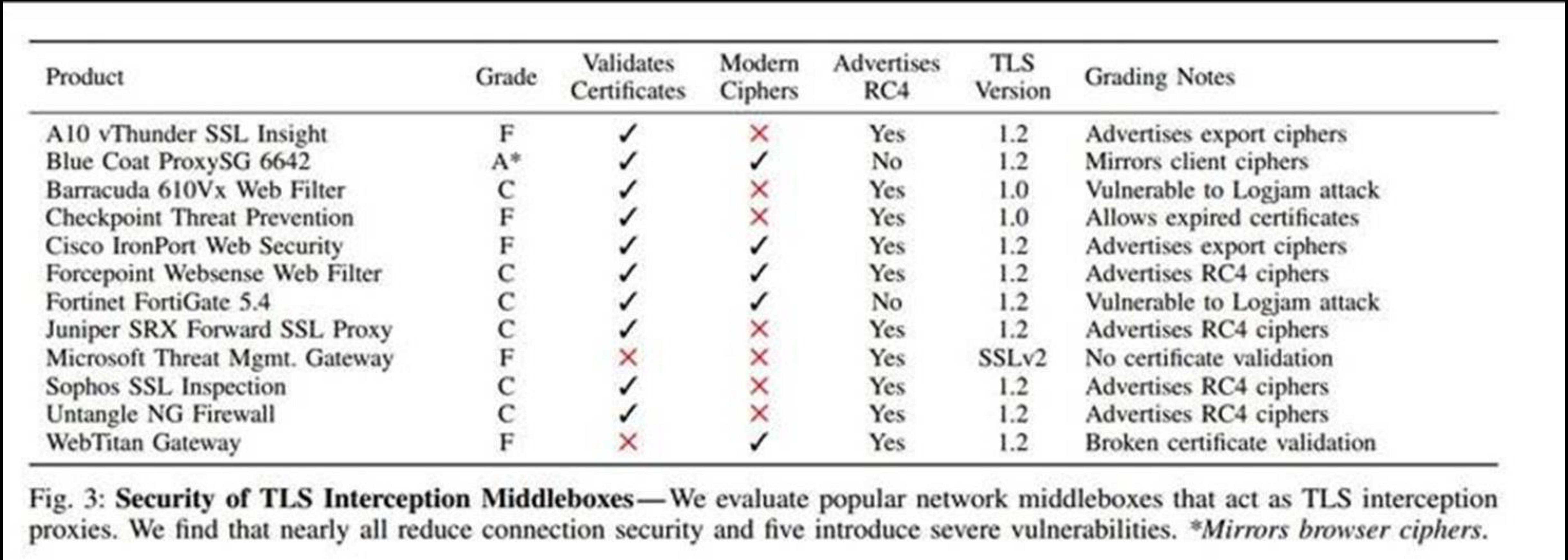


Corporate CA and proxy can work together to expose the SSL/TLS traffic. Corporate CA is pre-registered on corporate laptops.

This is why, on a corporate network, you are often informed that you should have no expectation of privacy.

Benevolent MITMing done poorly

https://jhalderm.com/pub/papers/interception-ndss17.pdf

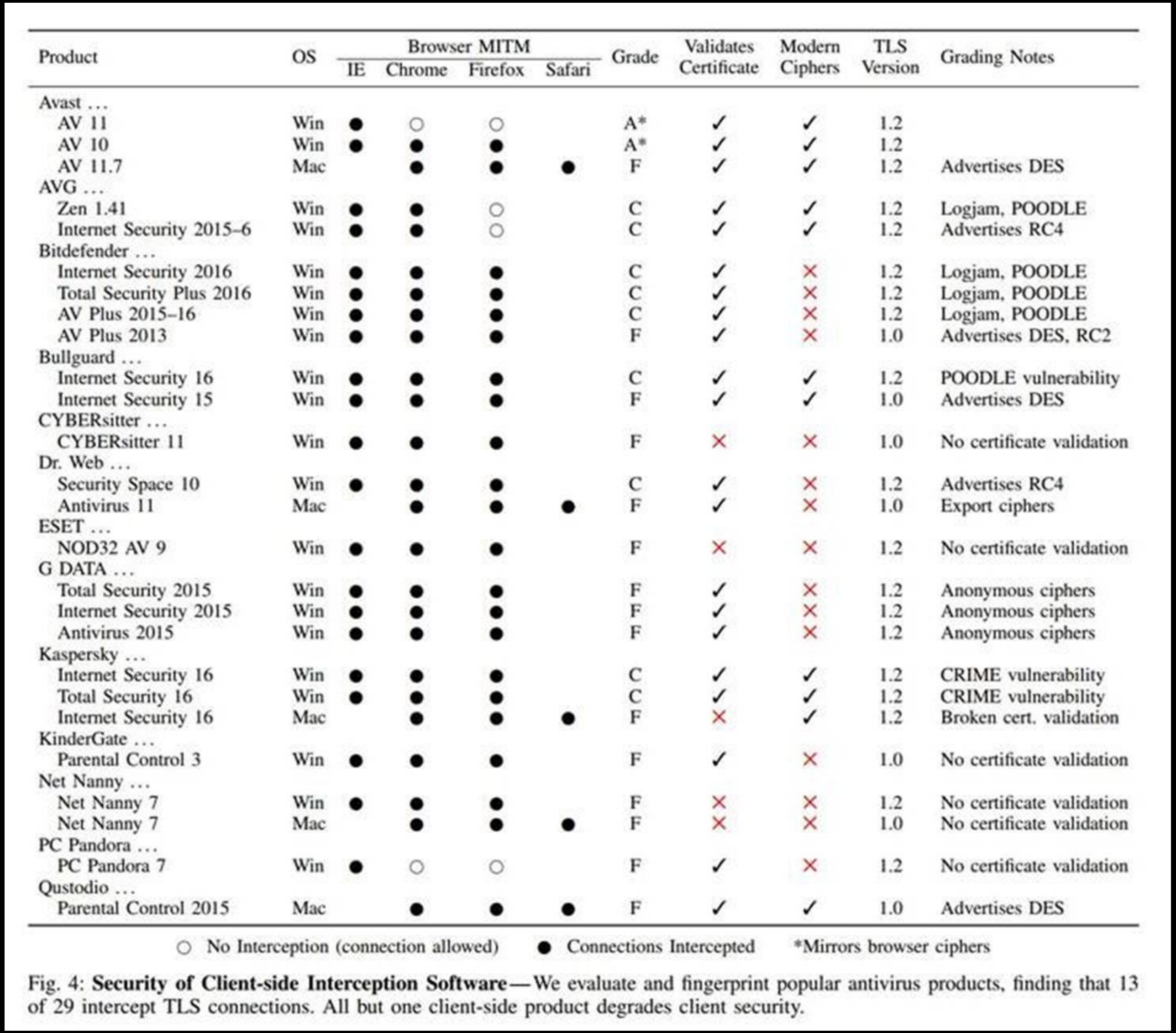


Product	Grade	Validates Certificates	Modern Ciphers	Advertises RC4	TLS Version	Grading Notes
A10 vThunder SSL Insight	F	✓	✗	Yes	1.2	Advertises export ciphers
Blue Coat ProxySG 6642	A*	✓	✓	No	1.2	Mirrors client ciphers
Barracuda 610Vx Web Filter	C	✓	✗	Yes	1.0	Vulnerable to Logjam attack
Checkpoint Threat Prevention	F	✓	✗	Yes	1.0	Allows expired certificates
Cisco IronPort Web Security	F	✓	✓	Yes	1.2	Advertises export ciphers
Forcepoint Websense Web Filter	C	✓	✓	Yes	1.2	Advertises RC4 ciphers
Fortinet FortiGate 5.4	C	✓	✓	No	1.2	Vulnerable to Logjam attack
Juniper SRX Forward SSL Proxy	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
Microsoft Threat Mgmt. Gateway	F	✗	✗	Yes	SSLv2	No certificate validation
Sophos SSL Inspection	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
Untangle NG Firewall	C	✓	✗	Yes	1.2	Advertises RC4 ciphers
WebTitan Gateway	F	✗	✓	Yes	1.2	Broken certificate validation

Fig. 3: **Security of TLS Interception Middleboxes**—We evaluate popular network middleboxes that act as TLS interception proxies. We find that nearly all reduce connection security and five introduce severe vulnerabilities. **Mirrors browser ciphers.*

Benevolent MITMing done poorly

https://jhalderm.com/pub/papers/interception-ndss17.pdf



Product	OS	Browser MITM				Grade	Validates Certificate	Modern Ciphers	TLS Version	Grading Notes
		IE	Chrome	Firefox	Safari					
Avast …										
AV 11	Win	●	○	○		A*	✓	✓	1.2	
AV 10	Win	●	●	●		A*	✓	✓	1.2	
AV 11.7	Mac		●	●	●	F	✓	✓	1.2	Advertises DES
AVG …										
Zen 1.41	Win	●	●	○		C	✓	✓	1.2	Logjam, POODLE
Internet Security 2015–6	Win	●	●	○		C	✓	✓	1.2	Advertises RC4
Bitdefender …										
Internet Security 2016	Win	●	●	●		C	✓	✗	1.2	Logjam, POODLE
Total Security Plus 2016	Win	●	●	●		C	✓	✗	1.2	Logjam, POODLE
AV Plus 2015–16	Win	●	●	●		C	✓	✗	1.2	Logjam, POODLE
AV Plus 2013	Win	●	●	●		F	✓	✗	1.0	Advertises DES, RC2
Bullguard …										
Internet Security 16	Win	●	●	●		C	✓	✓	1.2	POODLE vulnerability
Internet Security 15	Win	●	●	●		F	✓	✓	1.0	Advertises DES
CYBERsitter …										
CYBERsitter 11	Win	●	●	●		F	✗	✗	1.0	No certificate validation
Dr. Web …										
Security Space 10	Win	●	●	●		C	✓	✗	1.2	Advertises RC4
Antivirus 11	Mac		●	●	●	F	✓	✗	1.0	Export ciphers
ESET …										
NOD32 AV 9	Win	●	●	●		F	✗	✗	1.2	No certificate validation
G DATA …										
Total Security 2015	Win	●	●	●		F	✓	✗	1.2	Anonymous ciphers
Internet Security 2015	Win	●	●	●		F	✓	✗	1.2	Anonymous ciphers
Antivirus 2015	Win	●	●	●		F	✓	✗	1.2	Anonymous ciphers
Kaspersky …										
Internet Security 16	Win	●	●	●		C	✓	✓	1.2	CRIME vulnerability
Total Security 16	Win	●	●	●		C	✓	✓	1.2	CRIME vulnerability
Internet Security 16	Mac		●	●	●	F	✗	✓	1.2	Broken cert. validation
KinderGate …										
Parental Control 3	Win	●	●	●		F	✓	✗	1.0	No certificate validation
Net Nanny …										
Net Nanny 7	Win	●	●	●		F	✗	✗	1.2	No certificate validation
Net Nanny 7	Mac		●	●	●	F	✗	✗	1.0	No certificate validation
PC Pandora …										
PC Pandora 7	Win	●	○	○		F	✓	✗	1.2	No certificate validation
Qustodio …										
Parental Control 2015	Mac		●	●	●	F	✓	✓	1.0	Advertises DES

○ No Interception (connection allowed) ● Connections Intercepted *Mirrors browser ciphers

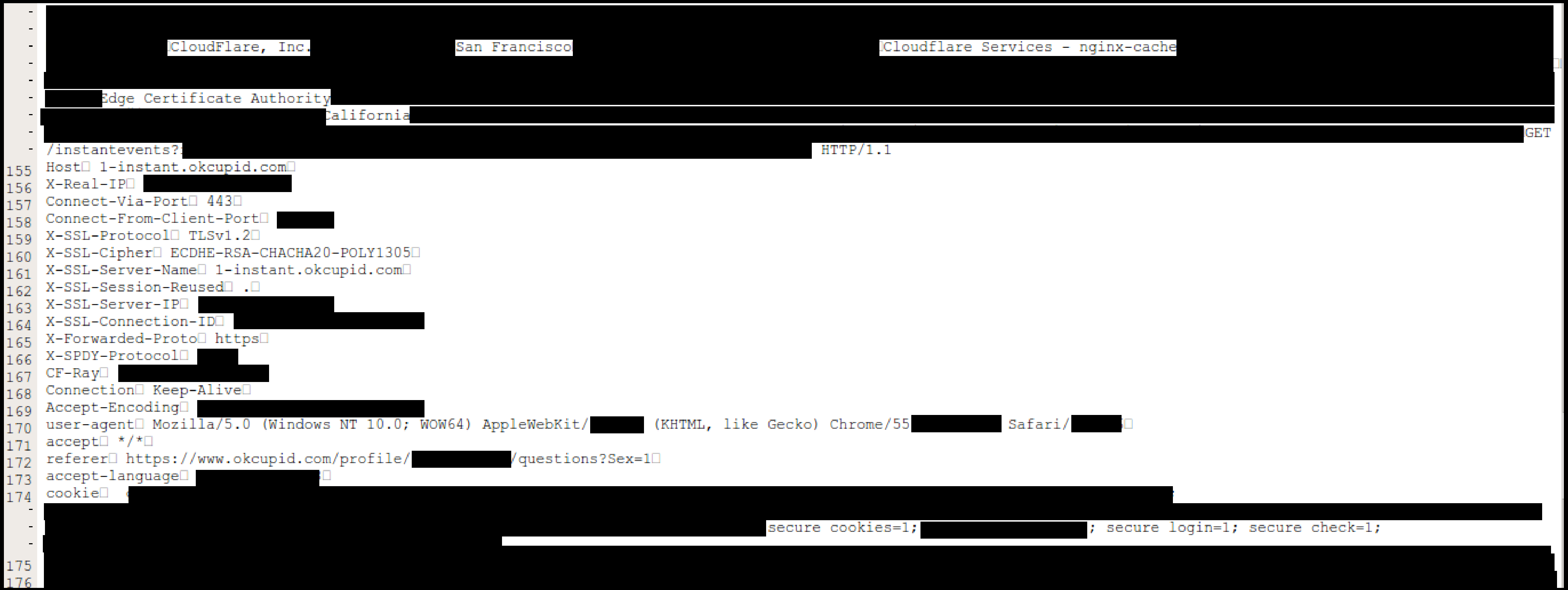
Fig. 4: **Security of Client-side Interception Software**—We evaluate and fingerprint popular antivirus products, finding that 13 of 29 intercept TLS connections. All but one client-side product degrades client security.

Benevolent MITMing Gone Horribly Wrong

- Cloudflare Reverse Proxies:
  - We’ll help you host and manage security (DDoS attacks, SSL management, Scraping)
  - Oh, that scraping protection feature (Scrapeshield)? It had a bug in it that injects random parts of Cloudflare server memory into the responses of scrapers (if the html was formatted a certain way)
  - Sensitive data exposed – if you used the feature or not – Whatever happened to be in memory!

Why Cloudflare, Why!?!?!

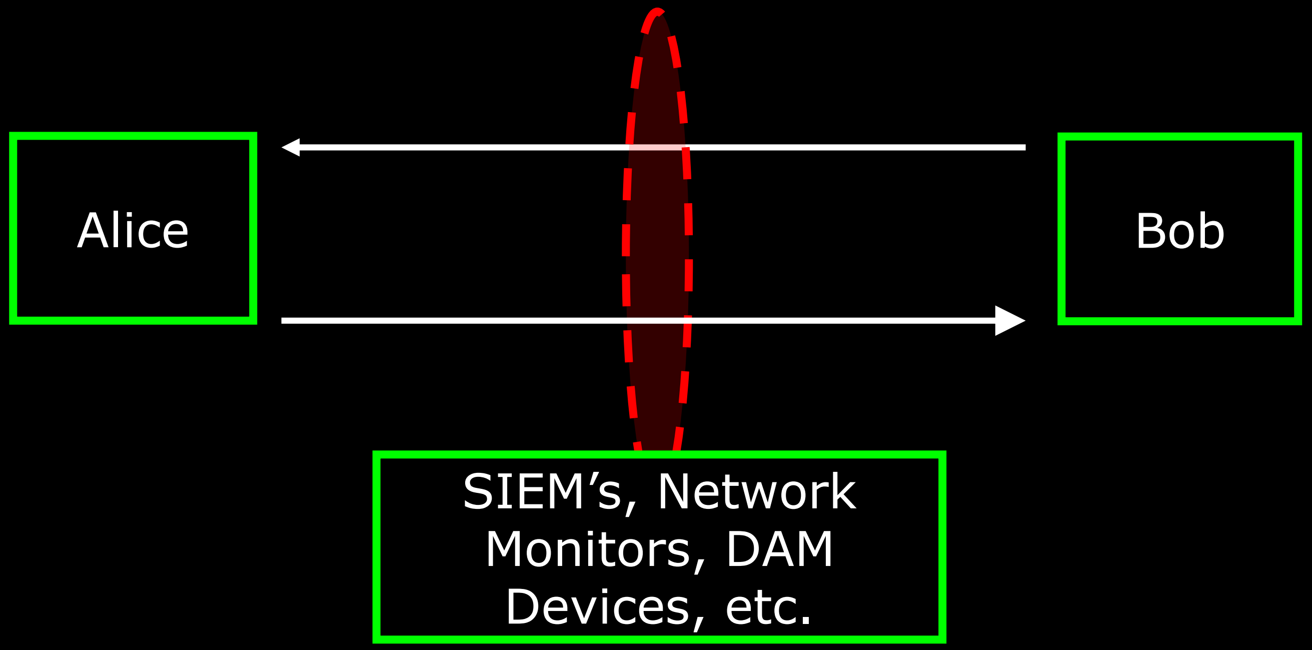
- Sample of Data Exposed:



```
[redacted]CloudFlare, Inc.[redacted]San Francisco[redacted]Cloudflare Services - nginx-cache[redacted]
[redacted]Edge Certificate Authority[redacted]
[redacted]California[redacted]
[redacted]GET
/instantevents?[redacted] HTTP/1.1
Host□ 1-instant.okcupid.com□
X-Real-IP□ [redacted]
Connect-Via-Port□ 443□
Connect-From-Client-Port□ [redacted]
X-SSL-Protocol□ TLSv1.2□
X-SSL-Cipher□ ECDHE-RSA-CHACHA20-POLY1305□
X-SSL-Server-Name□ 1-instant.okcupid.com□
X-SSL-Session-Reused□ .□
X-SSL-Server-IP□ [redacted]
X-SSL-Connection-ID□ [redacted]
X-Forwarded-Proto□ https□
X-SPDY-Protocol□ [redacted]
CF-Ray□ [redacted]
Connection□ Keep-Alive□
Accept-Encoding□ [redacted]
user-agent□ Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/[redacted] (KHTML, like Gecko) Chrome/55[redacted] Safari/[redacted]□
accept□ */*□
referer□ https://www.okcupid.com/profile/[redacted]/questions?Sex=1□
accept-language□ [redacted]□
cookie□ [redacted]
[redacted]secure cookies=1; [redacted]; secure login=1; secure check=1;
[redacted]
```

Sniffing as an Audit Mechanism

- Intercept, parse, and report on events in the network



Wrap Up

- Keeping Secrets from Intermediaries:
  - Use Asymmetric Encryption to Keep Secrets (solves sniffing)
  - Use Certificates to Authenticate the Server (solves MITM)
- That’s not where security ends:
  - Everyone has to use it right
  - Intermediaries are not the only threat
- Benevolent Intermediaries can be used to monitor networks

Membership

Like this presentation?

It couldn’t have happened without Hackforge.

You should join so that we can continue presenting them: http://hackf.org/