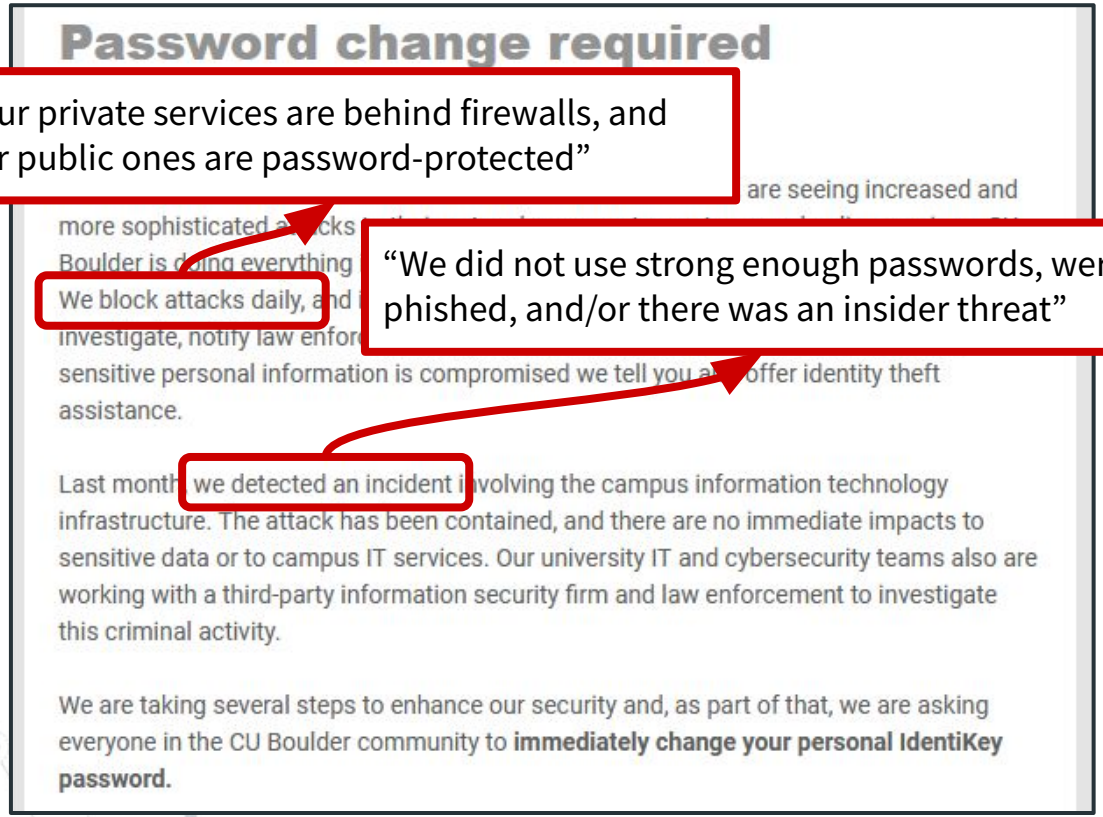
Network Security

Patch notes



"Our private services are behind firewalls, and our public ones are password-protected"

"We did not use strong enough passwords, were phished, and/or there was an insider threat"

Patch notes

Questions from the chat:

- **Q**: Hackers 1995 has the best "hacking through firewall" scenes.

  A: This wasn't a question, but I just wanted anyone reading this to know that it's true and you should watch *Hackers* (1995). Hack the planet!

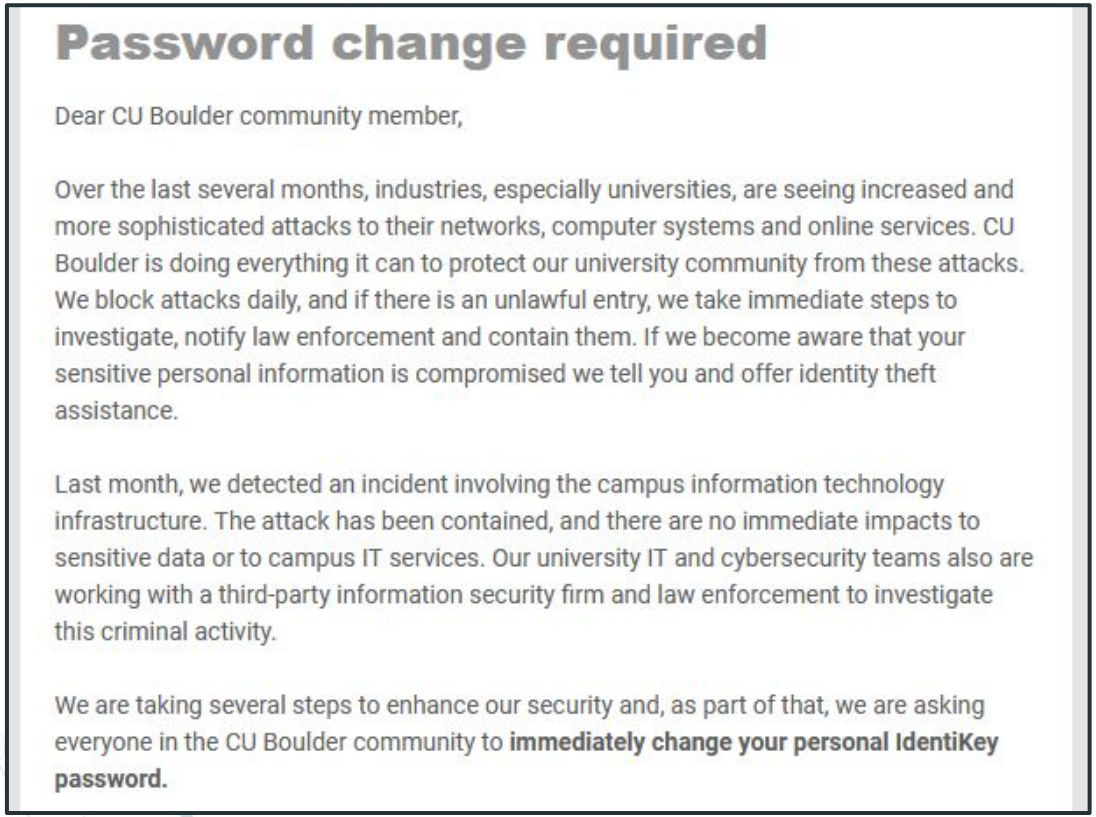
- **Q**: Do we have to partner up for homework?

  A: It is preferred, but you don't have to if you don't want to.

- **Q**: Whenever I run fastcoll, the outputs of the two python files are identical. Why?

  A: They should be different every time, although it can be hard to find the difference in the binary blob. Are the files themselves different? You can tell by taking the SHA-256 hash instead of the MD5 one. If they are the exact same, it's a problem with the command to generate the files. If they are different, but print the same thing, then it is a problem with the Python prefix or suffix you're using.

Patch notes



Password change required

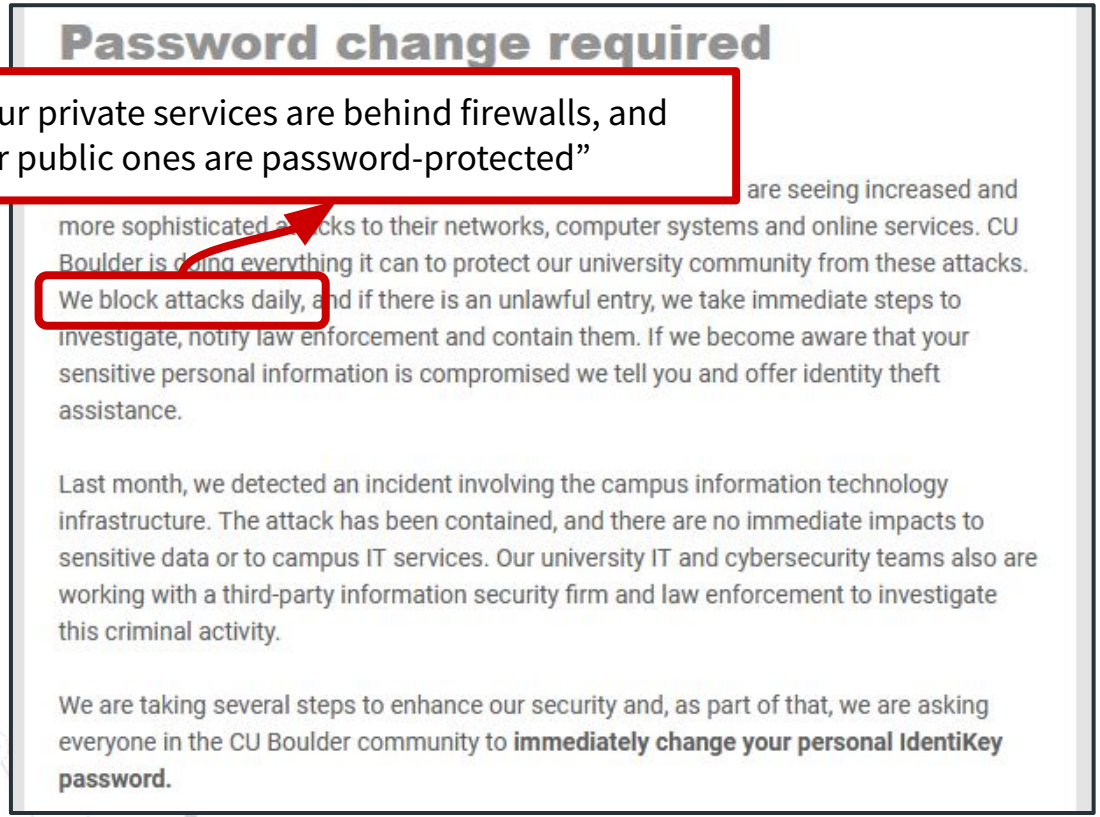
Dear CU Boulder community member,

Over the last several months, industries, especially universities, are seeing increased and more sophisticated attacks to their networks, computer systems and online services. CU Boulder is doing everything it can to protect our university community from these attacks. We block attacks daily, and if there is an unlawful entry, we take immediate steps to investigate, notify law enforcement and contain them. If we become aware that your sensitive personal information is compromised we tell you and offer identity theft assistance.

Last month, we detected an incident involving the campus information technology infrastructure. The attack has been contained, and there are no immediate impacts to sensitive data or to campus IT services. Our university IT and cybersecurity teams also are working with a third-party information security firm and law enforcement to investigate this criminal activity.

We are taking several steps to enhance our security and, as part of that, we are asking everyone in the CU Boulder community to **immediately change your personal IdentiKey password.**

Patch notes



Password change required

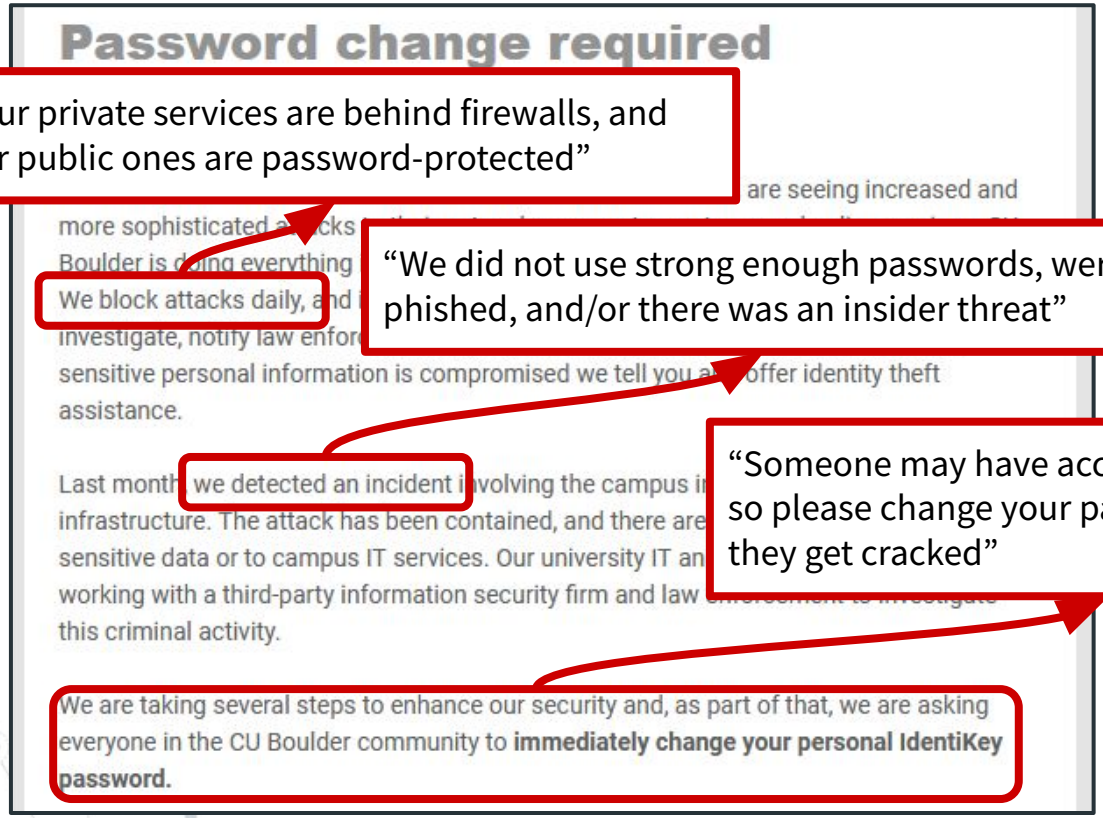
“Our private services are behind firewalls, and our public ones are password-protected”

are seeing increased and more sophisticated attacks to their networks, computer systems and online services. CU Boulder is doing everything it can to protect our university community from these attacks. We block attacks daily, and if there is an unlawful entry, we take immediate steps to investigate, notify law enforcement and contain them. If we become aware that your sensitive personal information is compromised we tell you and offer identity theft assistance.

Last month, we detected an incident involving the campus information technology infrastructure. The attack has been contained, and there are no immediate impacts to sensitive data or to campus IT services. Our university IT and cybersecurity teams also are working with a third-party information security firm and law enforcement to investigate this criminal activity.

We are taking several steps to enhance our security and, as part of that, we are asking everyone in the CU Boulder community to **immediately change your personal IdentiKey password.**

Patch notes



"Our private services are behind firewalls, and our public ones are password-protected"

"We did not use strong enough passwords, were phished, and/or there was an insider threat"

"Someone may have accessed password hashes, so please change your passwords now before they get cracked"

Risk

Risk refresher: Risk = Probability * Severity

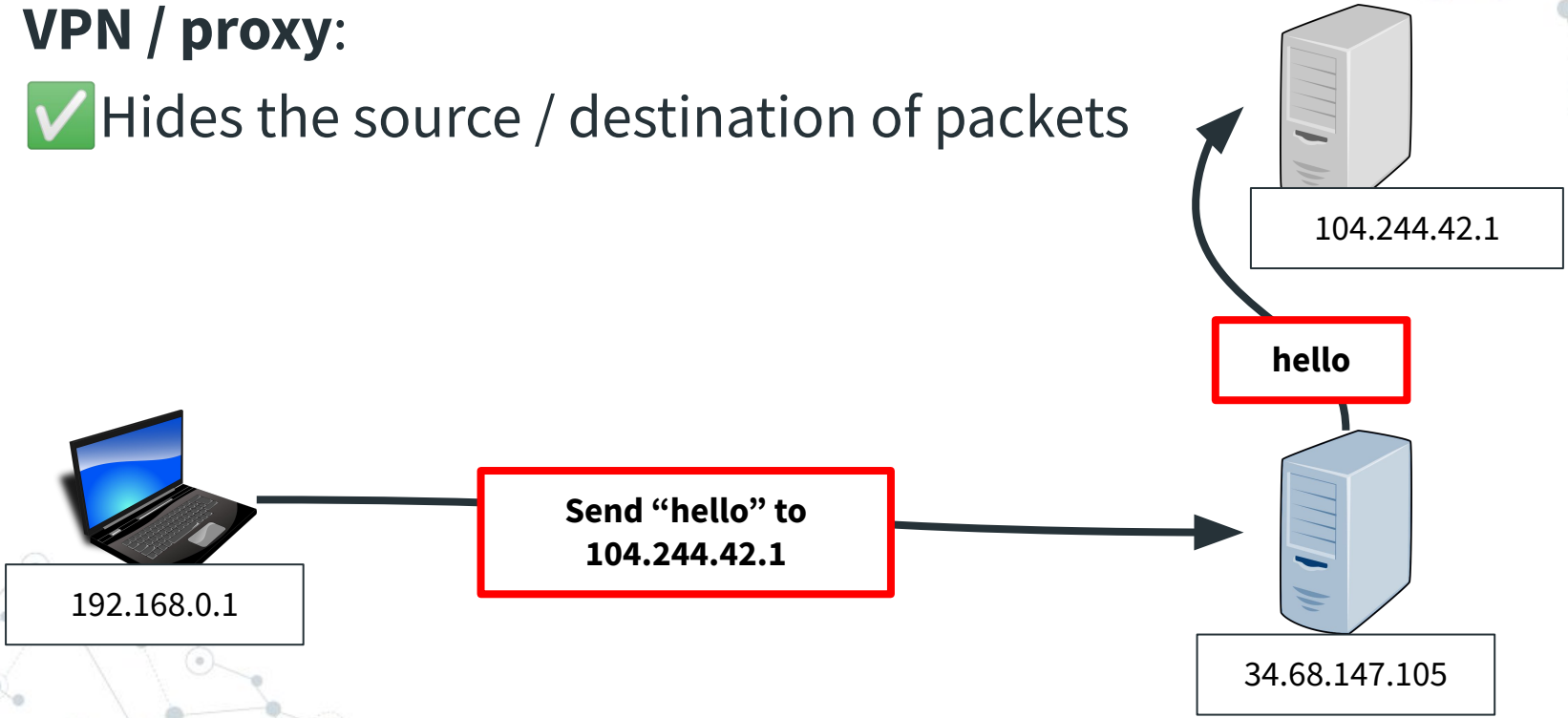
Probability: *How likely an attack is to happen*

Severity: *How much damage it causes*

VPNs

VPN / proxy:

✅Hides the source / destination of packets

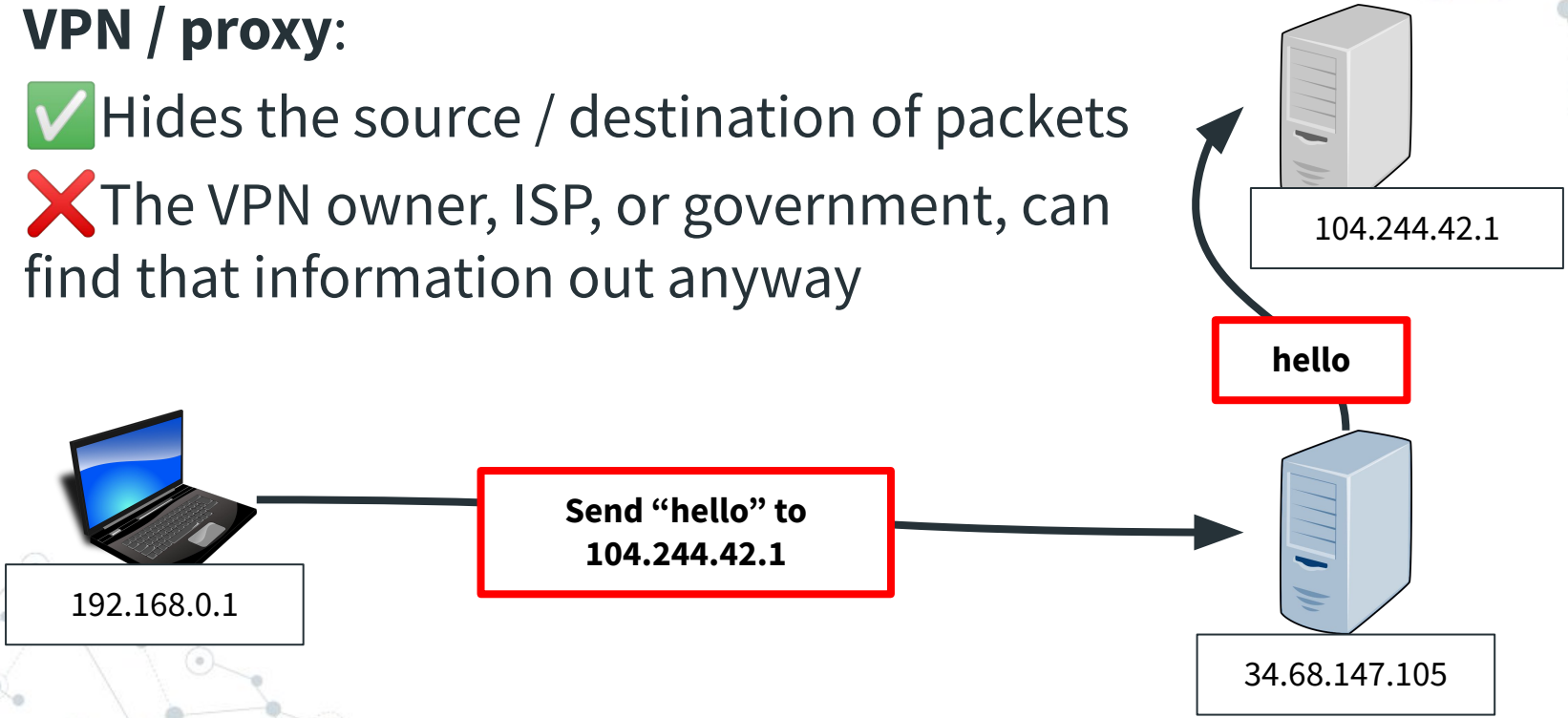


VPNs

VPN / proxy:

✅Hides the source / destination of packets

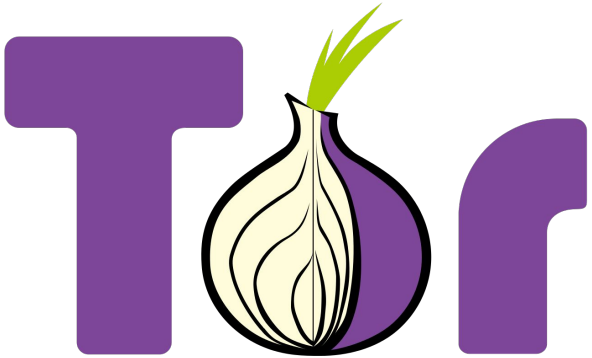
❌The VPN owner, ISP, or government, can find that information out anyway



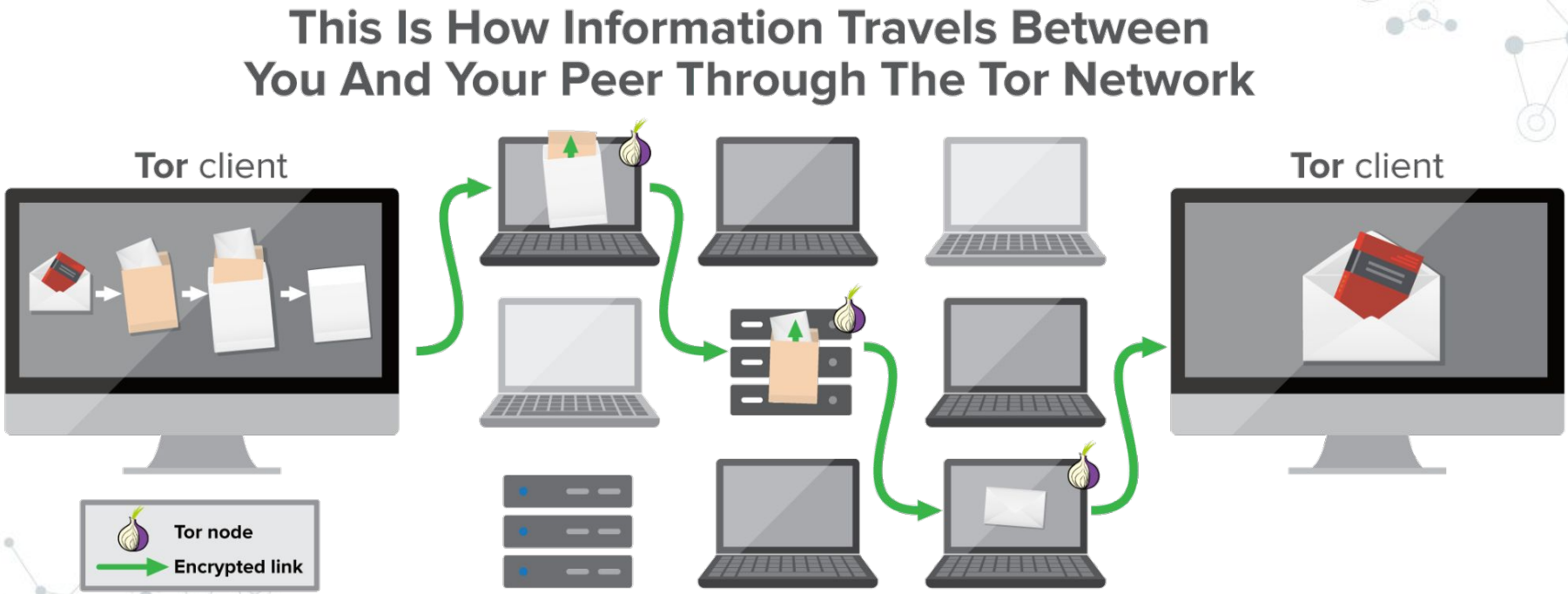
TOR

The Onion Router (TOR): A service that fully commits to user privacy

- Proxy **multiple** times, through multiple servers
- Proxies are owned by **different** volunteers
- Path is chosen **randomly**



TOR



https://s22908.pcdn.co/internet-privacy/wp-content/uploads/sites/2/2016/01/what-is-a-tor-network.png

TOR

The Onion Router (TOR):

- Requires a special web browser to use
- Provides as close to complete privacy as possible

TOR

The Onion Router (TOR):

- Requires a special web browser to use
- Provides as close to complete privacy as possible

TOR

Risk if your browsing history is leaked:

- Severity: **Low**
- Probability: **Nearly zero**

TOR

Risk if your browsing history is leaked:

- Severity: **Low**
- Probability: **Nearly zero**

Mitigation cost: **Constantly slow web browsing**

TOR

Risk if your browsing history is leaked:

- Severity: **Low**
- Probability: **Nearly zero**

Mitigation cost: **Constantly slow web browsing**

This is probably not worth it for most users!

TOR

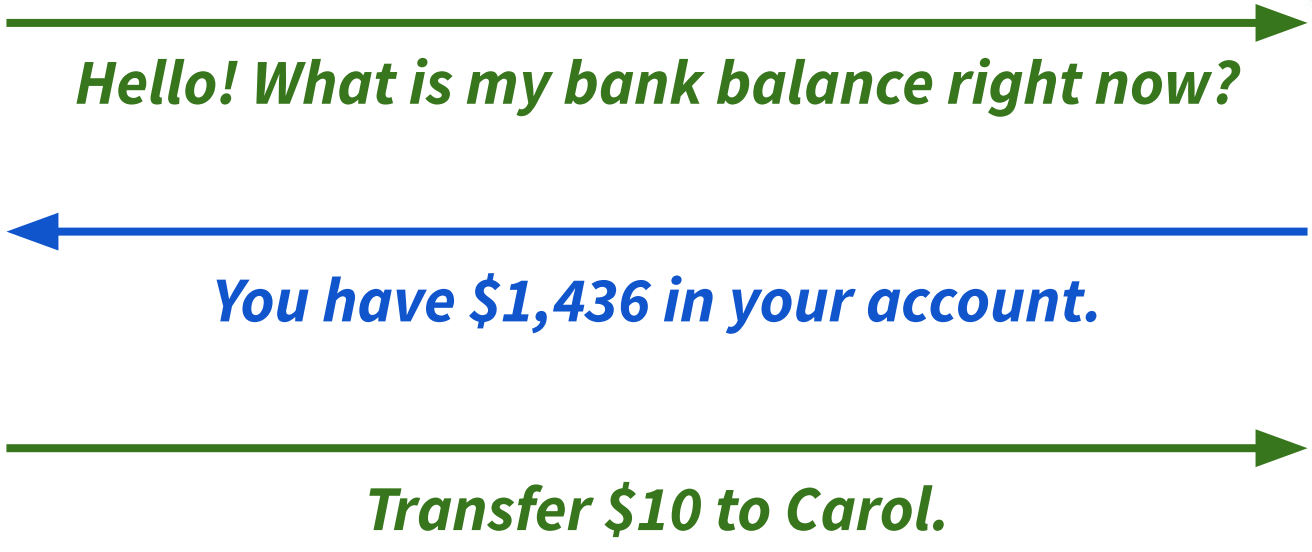
Recap:

TOR, as well as **Web proxies** and **VPNs**, all provide different levels of anonymity on the web.

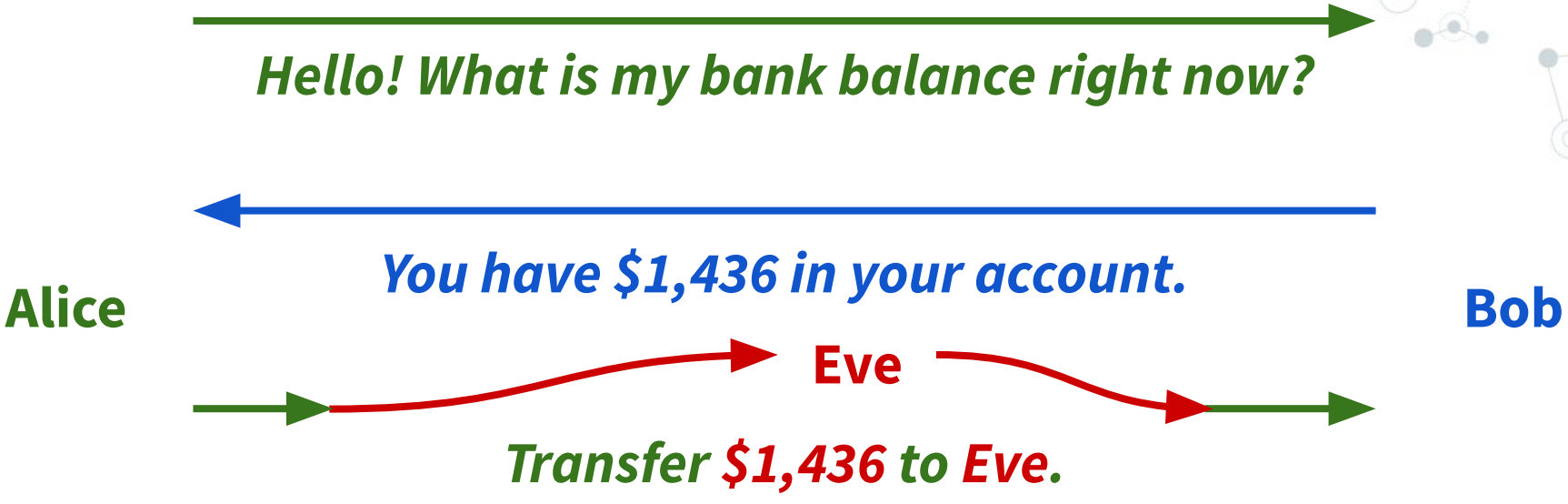
Their security benefits depend entirely on your personal threat model.

Man-in-the-Middle Attacks

Man-in-the-Middle Attacks



Man-in-the-Middle Attacks



Man-in-the-Middle Attacks

How can Eve become a Man-in-the-Middle?

- Own / spoof a WiFi hotspot
- Tap an ethernet cable

https://hackerwarehouse.com/product/gigabit-ethernet-tap/

https://shop.hak5.org/products/wifi-pineapple?variant=32019576094833

Man-in-the-Middle Attacks

How can Eve become a Man-in-the-Middle?

- Host a VPN
- Build a router
- Become an ISP

CenturyLink®

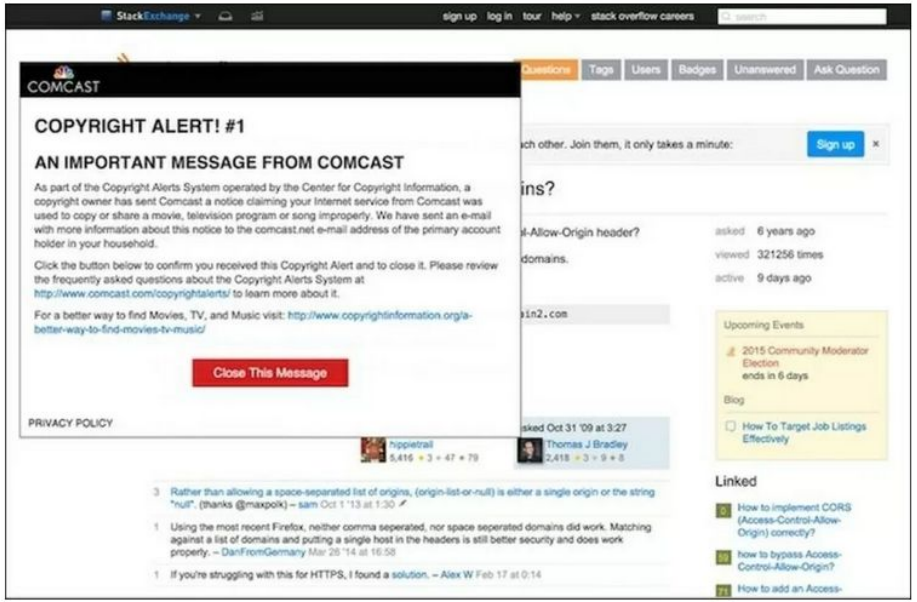
verizon

COMCAST

SECURITY THE WEB

Comcast using man-in-the-middle attack to warn subscribers of potential copyright infringement

By **Shawn Knight** November 23, 2015, 3:00 PM | 7 comments



Comcast has resorted to using what's essentially a man-in-the-middle attack to warn customers that they might be breaking copyright laws. The move, first brought to light

MOST READ

Intel Core i3-12100F
Budget Champ

https://www.techspot.com/news/62887-comcast-using-man-middle-attack-warn-subscribers-potential.html

{* NETWORKS *}

Help! my Belkin router is spamming me

Nagware promotes censorware

John Leyden

Fri 7 Nov 2003 // 14:47 UTC

The marketing geniuses at Belkin, the consumer networking vendor, have dreamed up a new form of spam - ads served to your desktop, by way of its wireless router.

Clem, a former Belkin wireless router user, was perplexed to find machines on his network redirected to an ad for Belkin's new parental control system, following a software update.

Clem initially thought that the browser setting on the machine to which he downloaded the updated software had been changed. But when other machines displayed the same behaviour he realised his router was to blame.

The router would grab a random HTTP connection every eight hours and redirect it to Belkin's (push) advertised web page.

https://www.theregister.com/2003/11/07/help_my_belkin_router/

Man-in-the-Middle Attacks

Meaning:

- Requires physical access or company-scale attacks
- Attacks are easier to attribute

Result: Overall less common than e.g. IP scanning

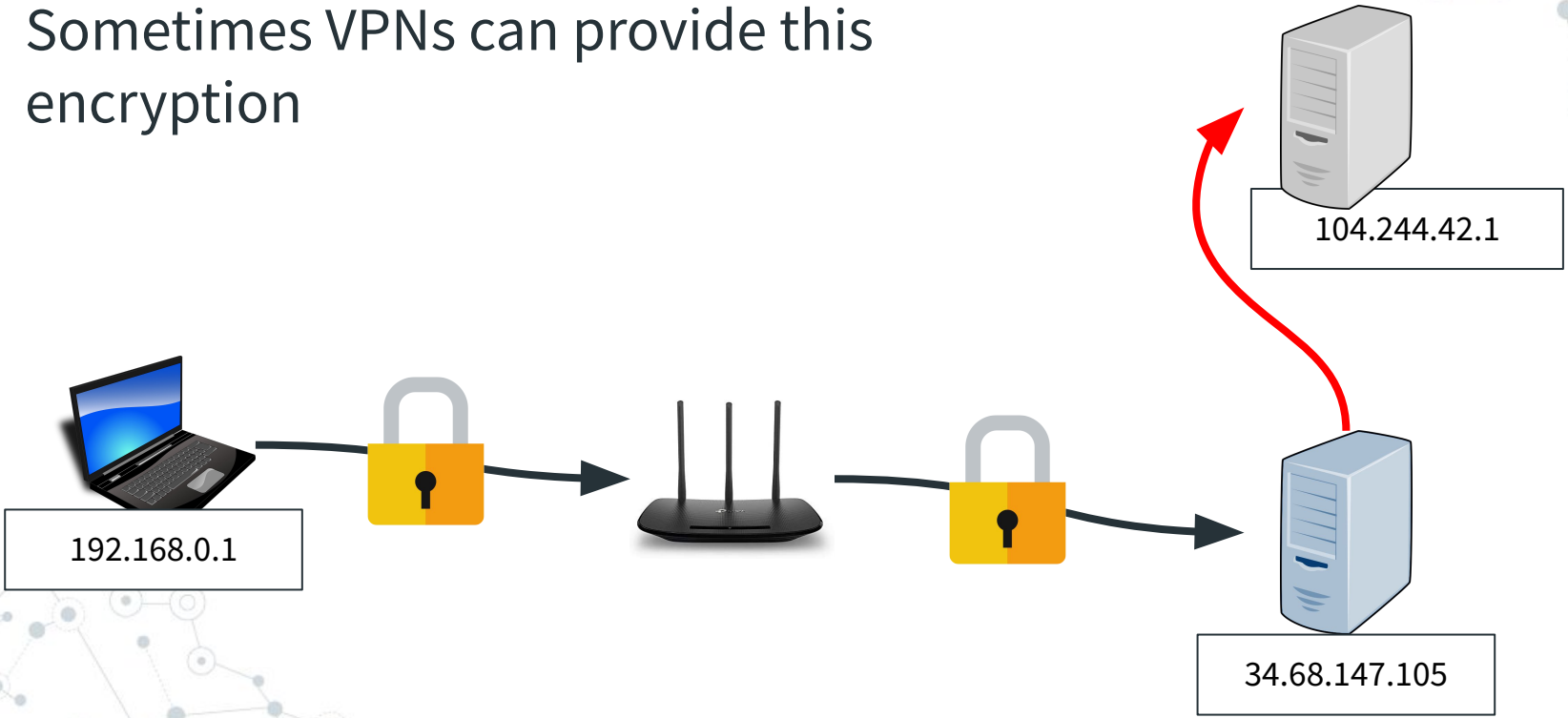
Man-in-the-Middle Attacks

Easy answer: Encrypt!

Unencrypted service	Encrypted version
HTTP	HTTPS
TELNET	SSH
FTP	SFTP
DNS	DNS-over-HTTPS

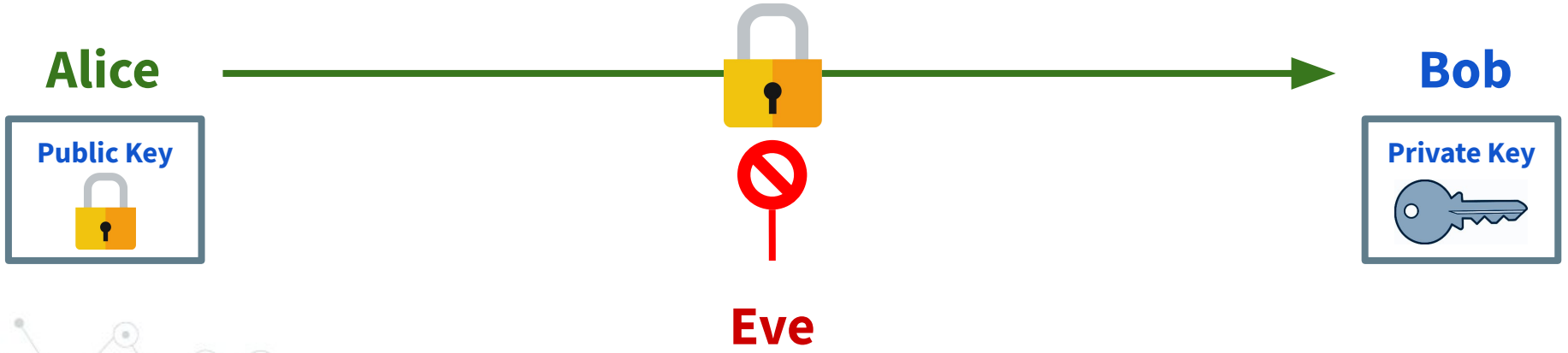
Man-in-the-Middle Attacks

Sometimes VPNs can provide this encryption



Man-in-the-Middle Attacks

We’re safe as long as we encrypt, right?



Man-in-the-Middle Attacks

We're sa

Alice

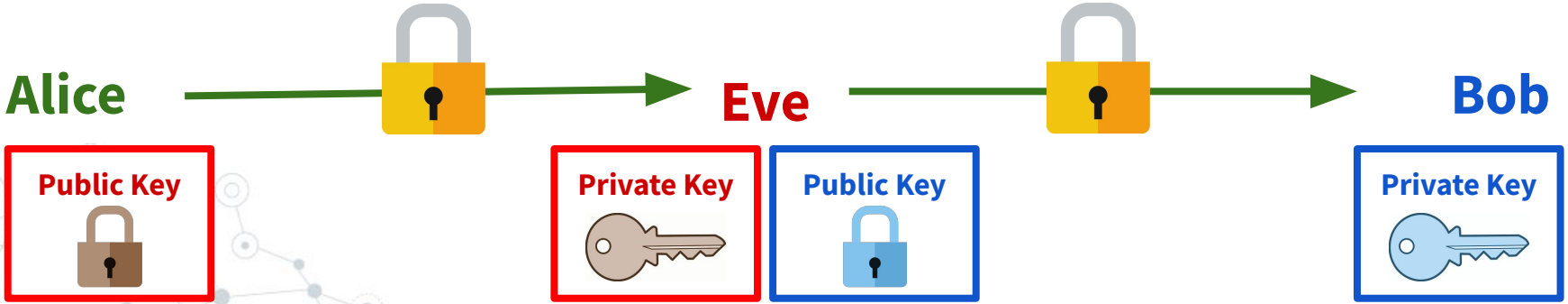
Public Key

Bob

Private Key

Man-in-the-Middle Attacks

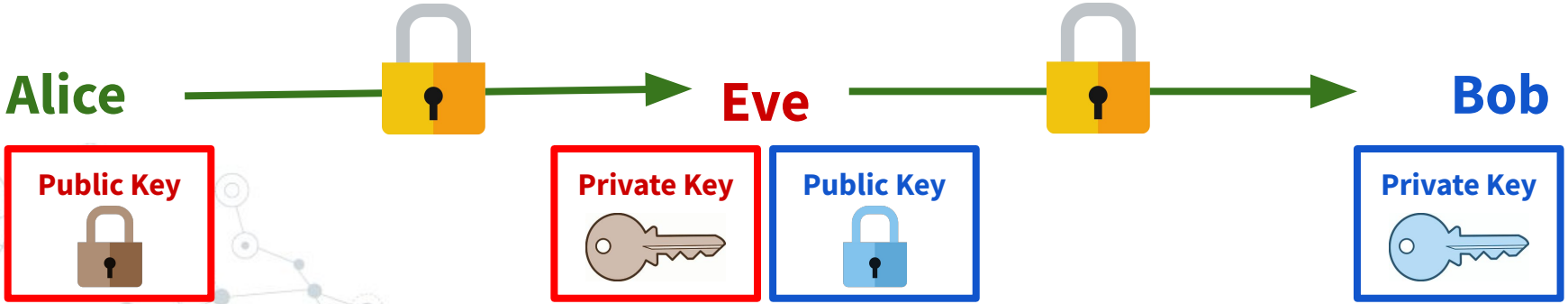
Eve can just make two encrypted channels!



Man-in-the-Middle Attacks

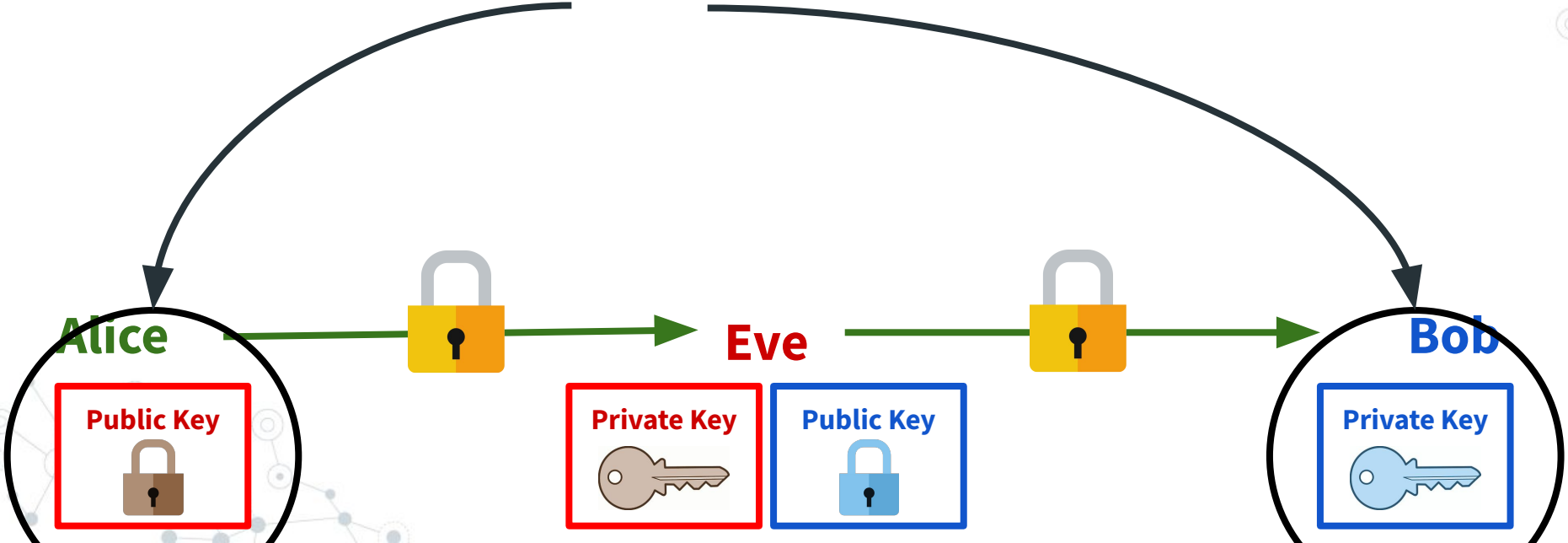
Eve can just make two encrypted channels!

1. Alice encrypts the message for Eve
2. Eve decrypts the message
3. Eve re-encrypts the message for Bob



Man-in-the-Middle Attacks

Solution: Verify the public key… somehow?

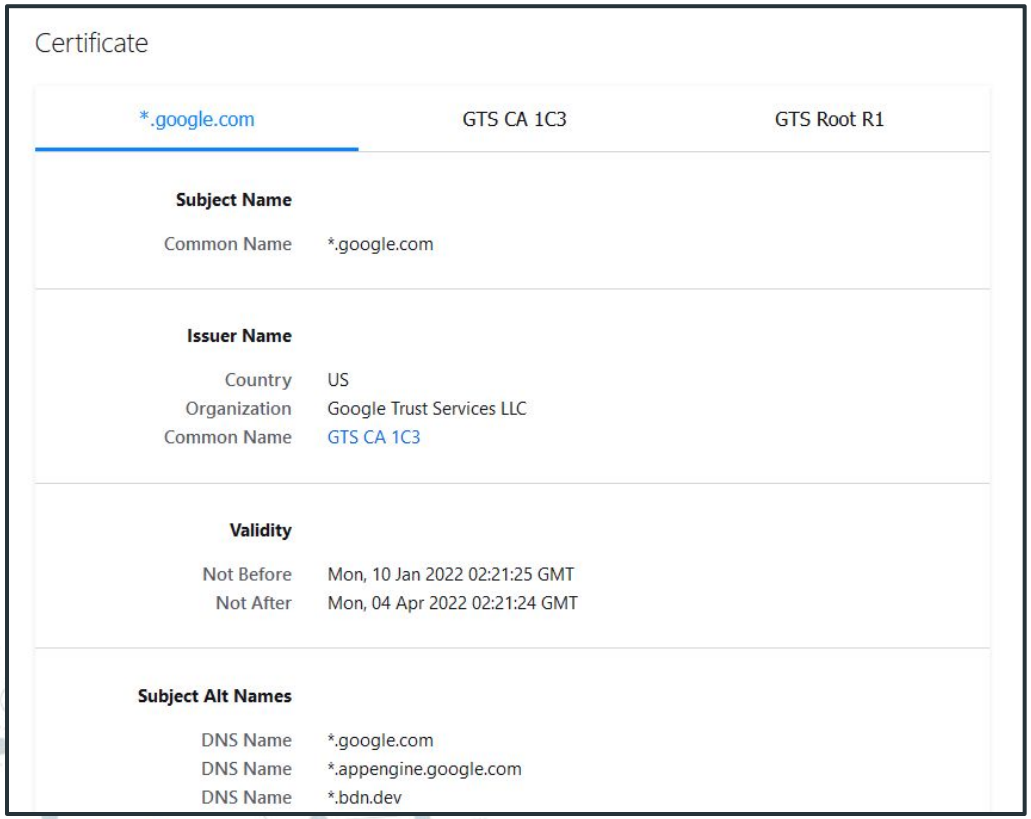


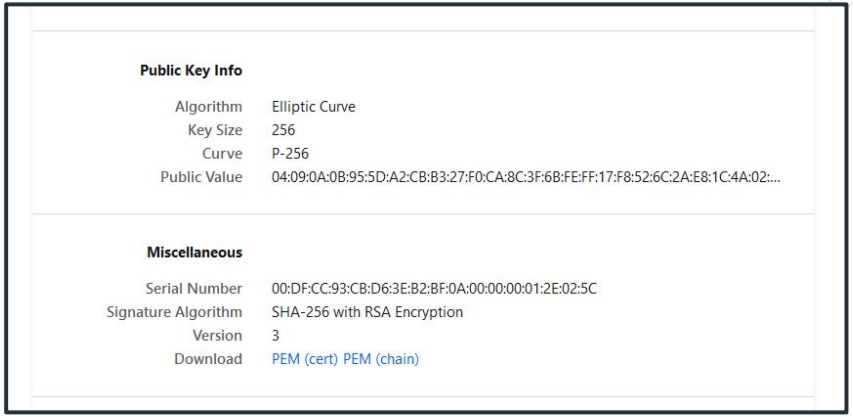
Digital Certificates

Digital Certificate: A record of who owns a public key, digitally signed by one or more parties

Certificate Authority (CA): An online service which verifies the signers of Digital Certificate

Digital Certificates





Digital Certificates

Certificate Authority

Alice

Bob

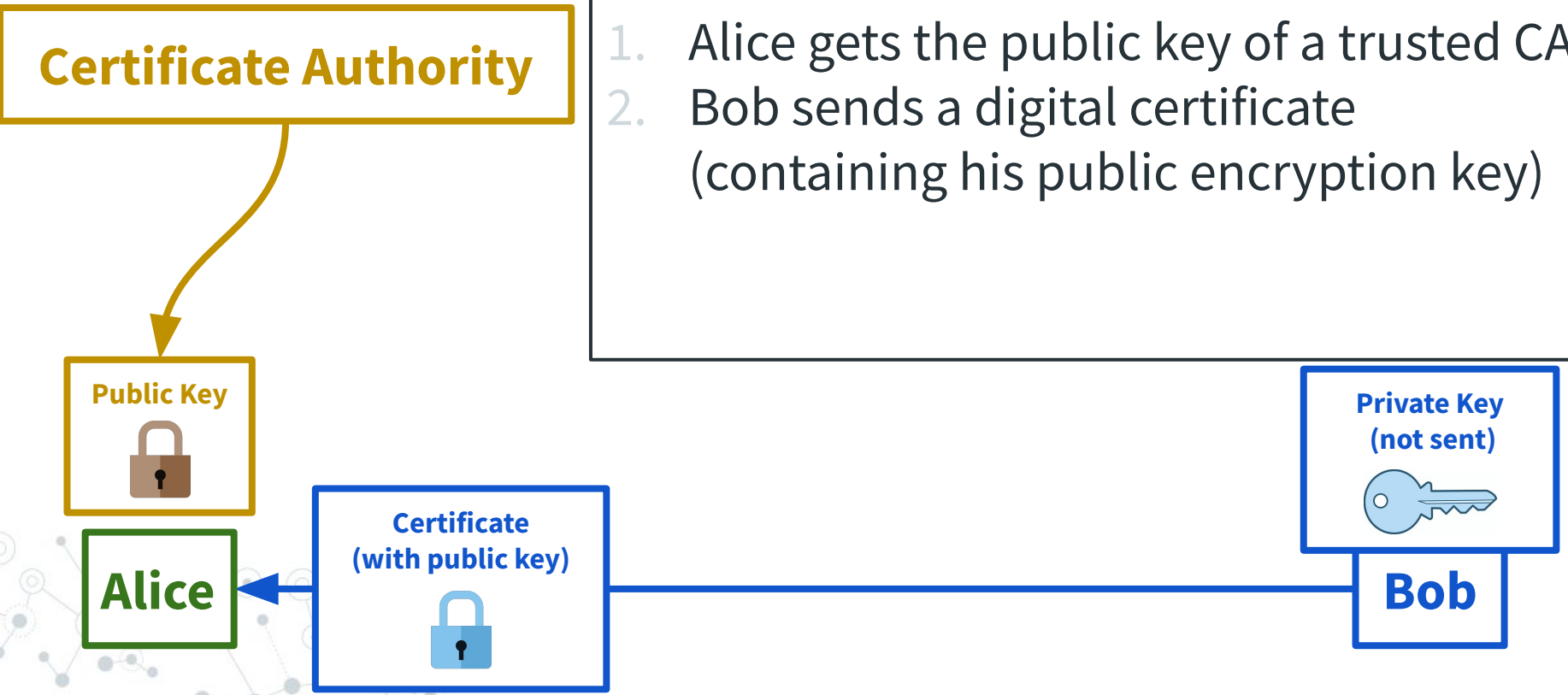
Digital Certificates

1. Alice gets the public key of a trusted CA

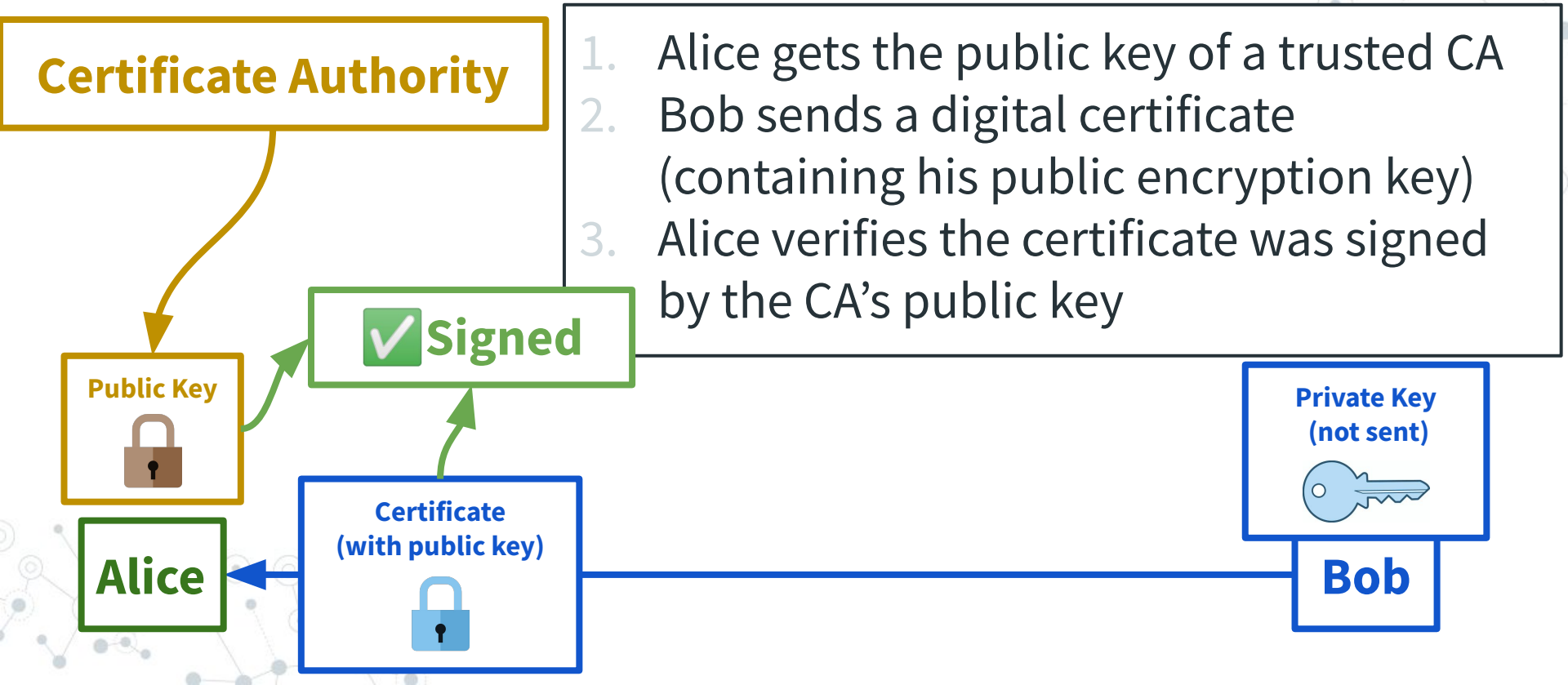
Bob

Digital Certificates

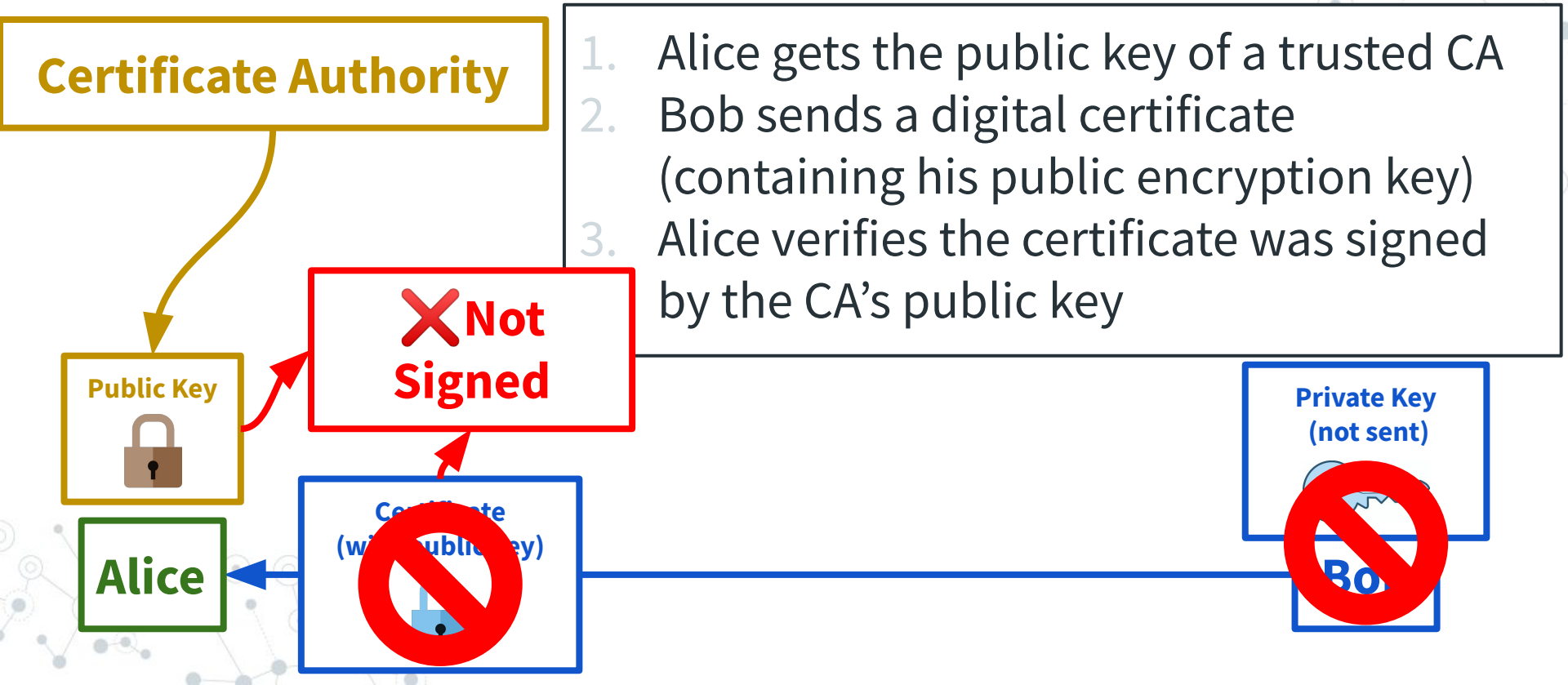
1. Alice gets the public key of a trusted CA
2. Bob sends a digital certificate (containing his public encryption key)



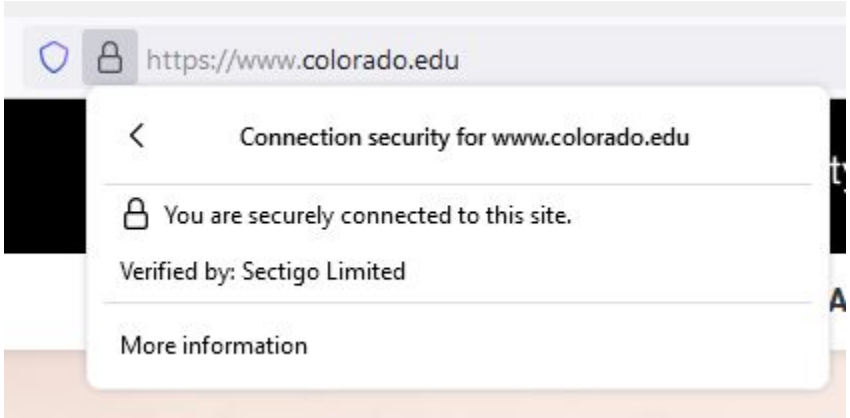
Digital Certificates



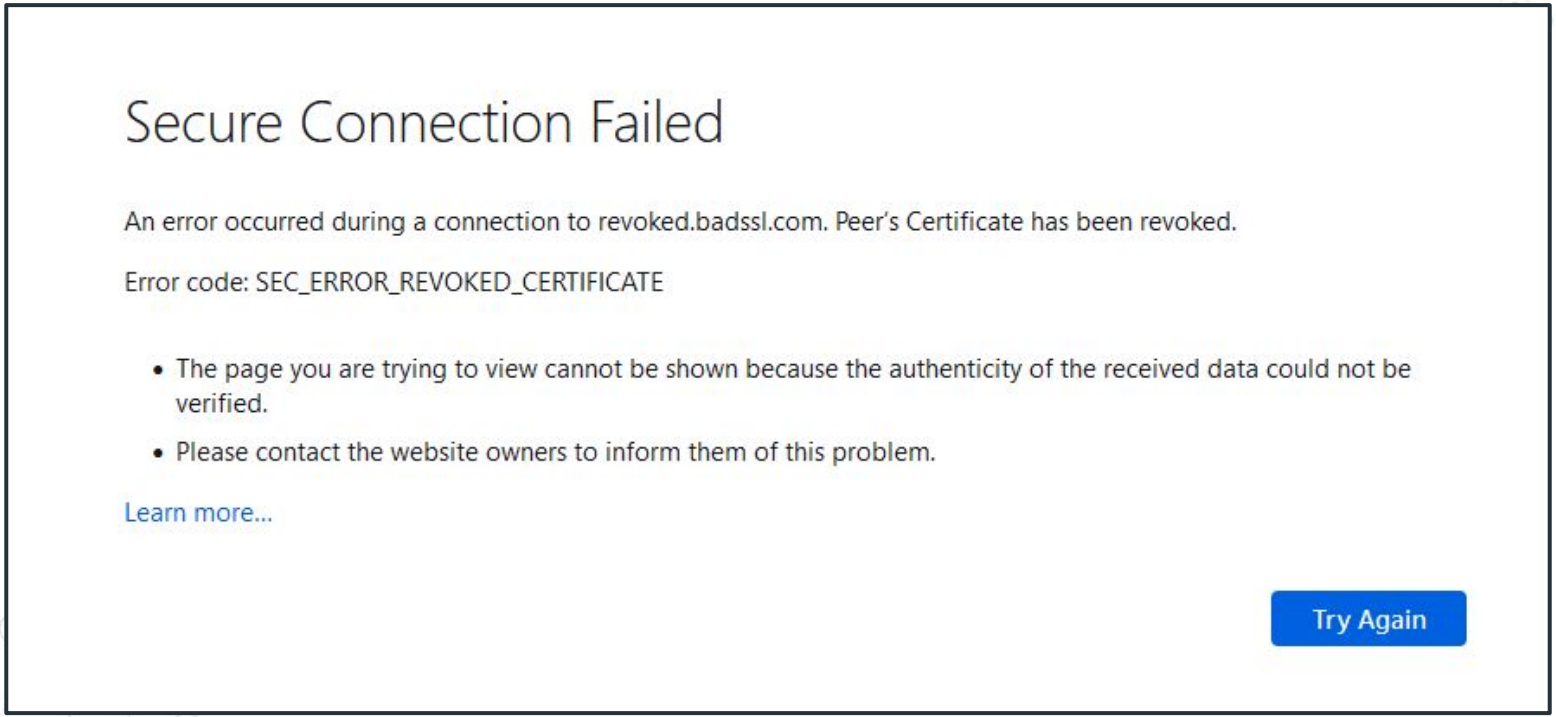
Digital Certificates



Digital Certificates



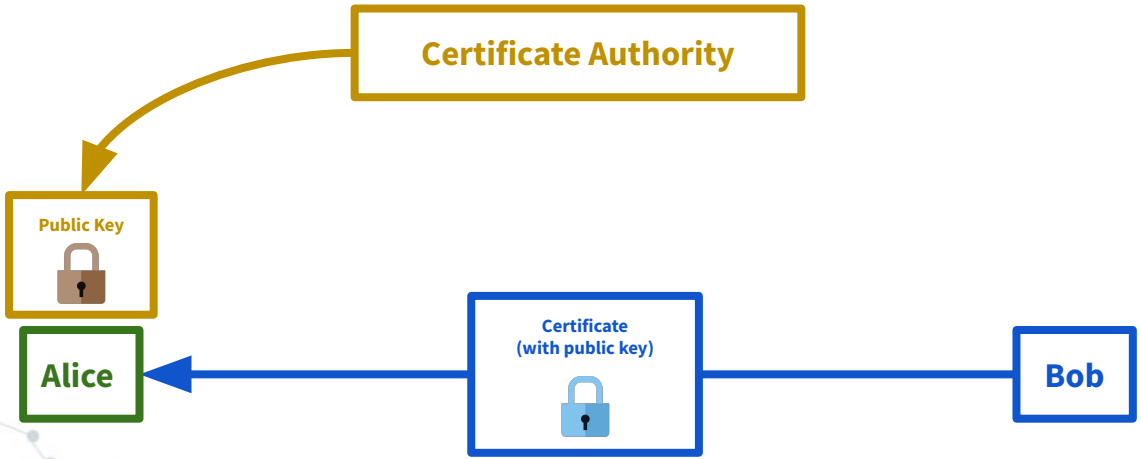
Digital Certificates



https://badssl.com/

Digital Certificates

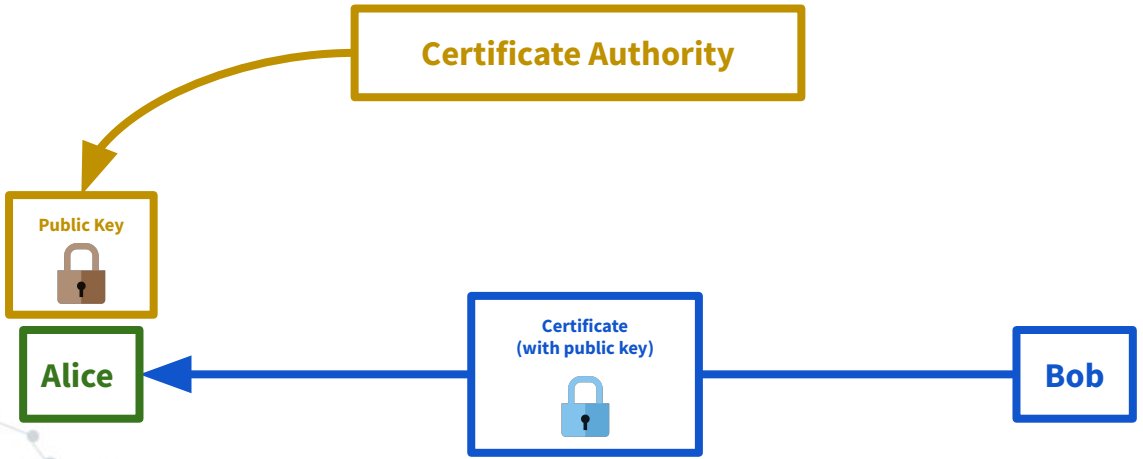
Q: How can Alice safely get the CA's public key?



Digital Certificates

Q: How can Alice safely get the CA's public key?

A: It is often hard-coded into the browser / computer / phone / car during manufacture!



Digital Certificates

Root Certificate: A certificate that is trusted without being signed (often hard-coded into a browser or OS)

Chain of Trust: A chain of signed CAs, each verifying the next, starting with a Root CA.

Recap

Digital Certificate: Proves who owns a public key

Chain of Trust: A chain of signed certificates

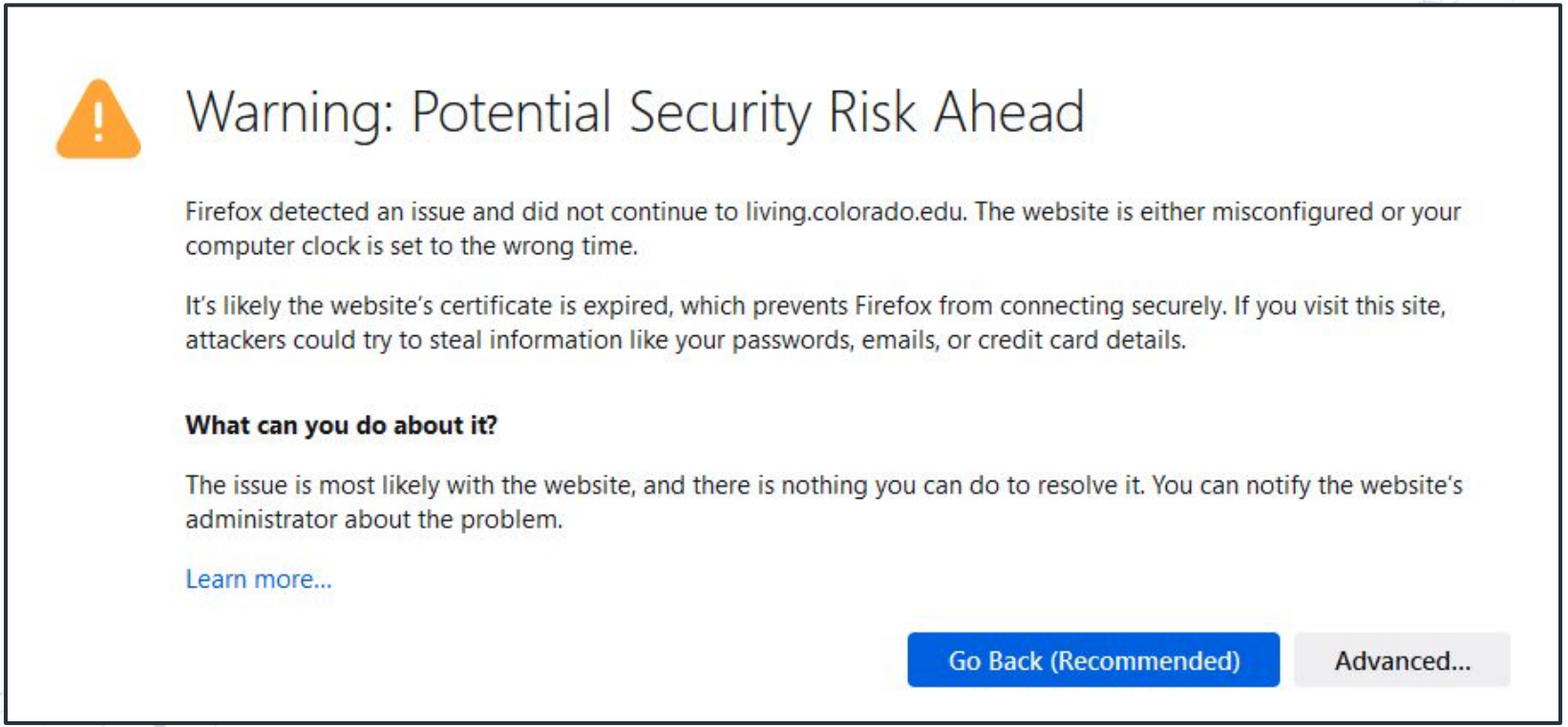
Root Certificate: A certificate you trust to be accurate, even though it is not signed

Digital Certificates

Notes on Certificates:

- Normally associated with one or more domain names (e.g. *.google.com)
- Can be revoked if the private key is leaked or stolen
- Given an expiration date

Digital Certificates

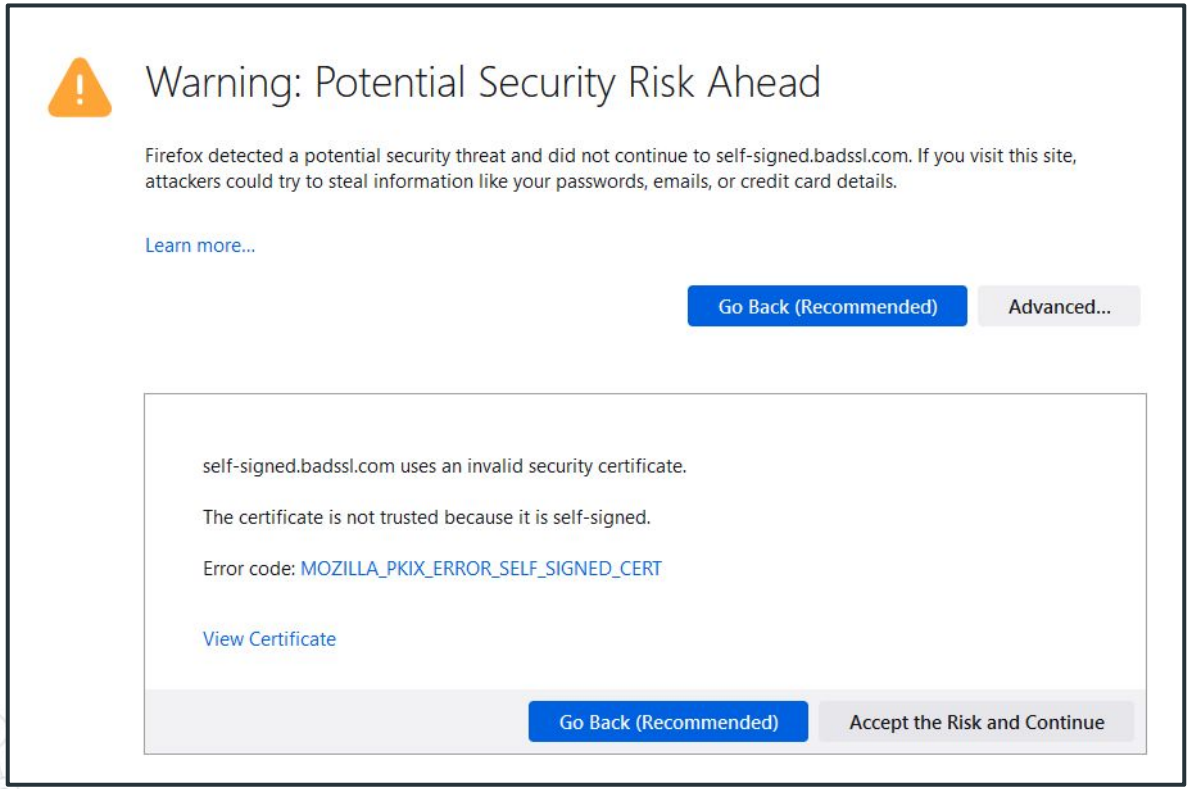


Digital Certificates

Self-signed certificates: Digital Certificates that were not verified by a Certificate Authority

- Still allow encryption, but the owner cannot be verified

Digital Certificates



https://self-signed.badssl.com/

Digital Certificates

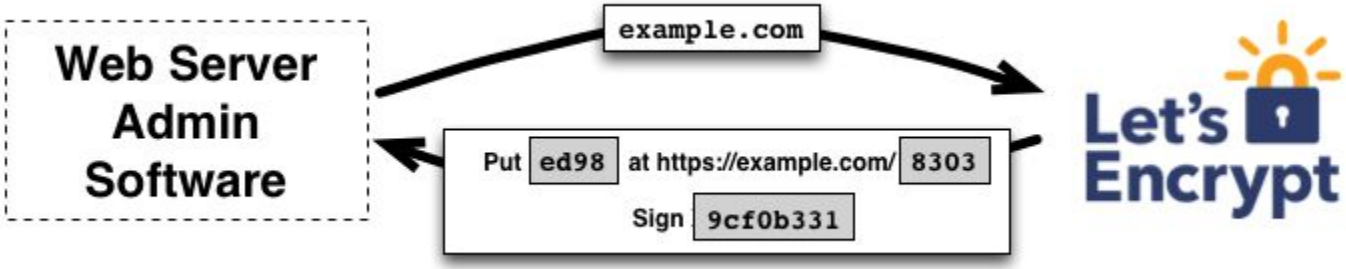
How do Certificate Authorities verify a domain's identity?

1. Physically interacting with a representative

Digital Certificates

How do Certificate Authorities verify a domain's identity?

1. Physically interacting with a representative
2. Can be verified automatically from the server whose public key is in question



https://letsencrypt.org/how-it-works/

Digital Certificates

```
alexander@sandbox:~$ sudo certbot --nginx
Saving debug log to /var/log/letsencrypt/letsencrypt.log

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: csci3403.com
2: demo.csci3403.com
3: insecure.csci3403.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 1
Requesting a certificate for csci3403.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/csci3403.com-0001/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/csci3403.com-0001/privkey.pem
This certificate expires on 2022-05-08.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for csci3403.com to /etc/nginx/sites-enabled/default
Congratulations! You have successfully enabled HTTPS on https://csci3403.com
```

Digital Certificates

```
alexander@sandbox:~$ sudo certbot --nginx
Saving debug log to /var/log/letsencrypt/letsencrypt.log

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: csci3403.com
2: demo.csci3403.com
3: insecure.csci3403.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 1
Requesting a certificate for csci3403.com

Successfully received certificate.
Certificate is saved at: /etc/letsencrypt/live/csci3403.com-0001/fullchain.pem
Key is saved at:         /etc/letsencrypt/live/csci3403.com-0001/privkey.pem
This certificate expires on 2022-05-08.
These files will be updated when the certificate renews.
Certbot has set up a scheduled task to automatically renew this certificate in the background.

Deploying certificate
Successfully deployed certificate for csci3403.com to /etc/nginx/sites-enabled/default
Congratulations! You have successfully enabled HTTPS on https://csci3403.com
```

Digital Certificates

```
alexander@sandbox:~$ sudo certbot --nginx
Saving debug log to /var/log/letsencrypt/letsencrypt.log

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: csci3403.com
2: demo.csci3403.com
3: insecure.csci3403.com
4: notmydomain.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 4
Requesting a certificate for notmydomain.com

Certbot failed to authenticate some domains (authenticator: nginx). The Certificate A
  Domain: notmydomain.com
  Type:   unauthorized
  Detail: Invalid response from https://www.hugedomains.com/domain_profile.cfm?d=notm

Hint: The Certificate Authority failed to verify the temporary nginx configuration ch

Some challenges have failed.
```

Digital Certificates

```
alexander@sandbox:~$ sudo certbot --nginx
Saving debug log to /var/log/letsencrypt/letsencrypt.log

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: csci3403.com
2: demo.csci3403.com
3: insecure.csci3403.com
4: notmydomain.com
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 4
Requesting a certificate for notmydomain.com

Certbot failed to authenticate some domains (authenticator: nginx). The Certificate A
  Domain: notmydomain.com
  Type:   unauthorized
  Detail: Invalid response from https://www.hugedomains.com/domain_profile.cfm?d=notm

Hint: The Certificate Authority failed to verify the temporary nginx configuration ch

Some challenges have failed.
```

Digital Certificates

Q: What if a certificate authority makes a mistake?

Digital Certificates

Q: What if a certificate authority makes a mistake?

A:

NEWS

DigiNotar dies from certificate hack caper

'Unlikely many are going to shed tears' over Dutch company's demise, says security researcher

By Gregg Keizer

Senior Reporter, Computerworld | SEP 21, 2011 4:09 PM PST

The Dutch company that was hacked earlier this summer by certificate thieves has gone bust and shut down, its U.S.-based owner said Tuesday.

https://www.computerworld.com/article/2511297/diginotar-dies-from-certificate-hack-caper.html

Digital Certificates

Malicious Root Certificates

- Allows an attacker to impersonate any domain
- **Extremely** high effort
  - Requires compromising a CA whose sole job is to prevent this

Digital Certificates

Malicious Root Certificates

- Allows an attacker to impersonate any domain
- **Extremely** high effort
  - Requires compromising a CA whose sole job is to prevent this
  - Alternatively, requires root access on a device

NSA disguised itself as Google to spy, say reports

If a recently leaked document is any indication, the US National Security Agency -- or its UK counterpart -- appears to have put on a Google suit to gather intelligence.

Edward Moyer
Sept. 12, 2013 2:19 p.m. PT

The flag of the NSA.

Here's one of the latest tidbits on the NSA surveillance scandal (which seems to be generating nearly as many blog items as there are phone numbers in the spy agency's data banks).

https://www.cnet.com/news/nsa-disguised-itself-as-google-to-spy-say-reports/

Google, Mozilla Drop Trust in Chinese Certificate Authority CNNIC

Author:
Dennis Fisher

April 2, 2015 / 7:59 am

3 minute read

Share this article:

UPDATE–Google has taken the unusual step of completely removing trust from Chrome for the Chinese certificate authority CNNIC in the wake of an incident in which certificates issued by the CA were misused. Mozilla followed suit on Thursday, also removing CNNIC from its trust store.

https://threatpost.com/google-drops-trust-in-chinese-certificate-authority-cnnic/111974/

Kazakhstan government is intercepting HTTPS traffic in its capital

This marks the third time since 2015 that the Kazakh government is mandating the installation of a root certificate on its citizens' devices.

Written by **Catalin Cimpanu**, Contributor
Posted in Zero Day on December 6, 2020 | Topic: Security

Wind develops flag of the Republic of Kazakhstan in background of capital Nur-Sulta

RELATED

AirTag use in theft and stalking prompts Apple to update its safety guide

Apple allows unlisted entries in App Store once its approval is gained

Russian APT Primitive Bear attacks Western government department in Ukraine through job hunt

NEWSLETTERS

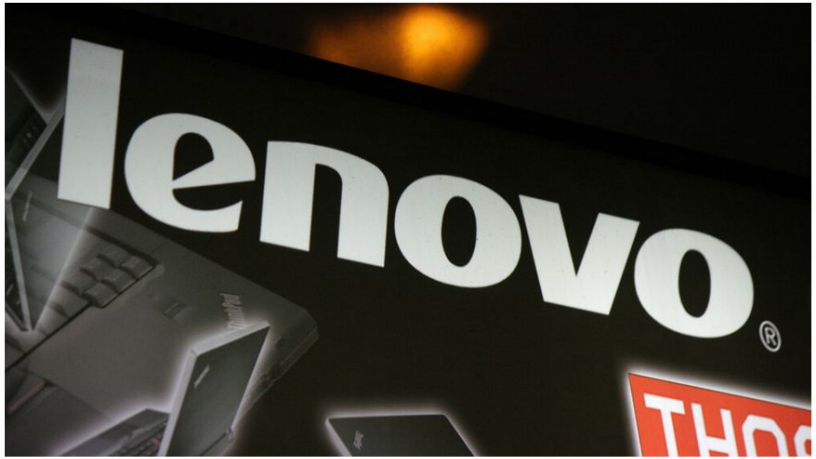
ZDNet Security

Your weekly update on security around the globe, featuring research, threats, and more.

Your email address SUBSCRIBE

https://www.zdnet.com/article/kazakhstan-government-is-intercepting-https-traffic-in-its-capital/

Lenovo caught installing adware on new computers



STORY BY
Owen Williams

It looks like Lenovo has been installing adware onto new consumer computers from the company that activates when taken out of the box for the first time.

The adware, named Superfish, is reportedly installed on a number of Lenovo's consumer laptops out of the box. The software injects third-party ads on Google searches and websites without the user's permission.

Popular on TNW today

1. This futuristic EV promises a mind-melting 1,000km range on a single charge
2. Northern Europe's founders lack ambition — here's what we should do
3. How to disable the in-app browser on the Gmail app for Android
4. The US tech scene is becoming decentralized — the time is ripe for new startup cities
5. Astronomers discovered a new asteroid sharing Earth's orbit – here's why it matters

https://thenextweb.com/news/lenovo-caught-installing-adware-new-computers

Digital Certificates

Internal Certificate Authorities

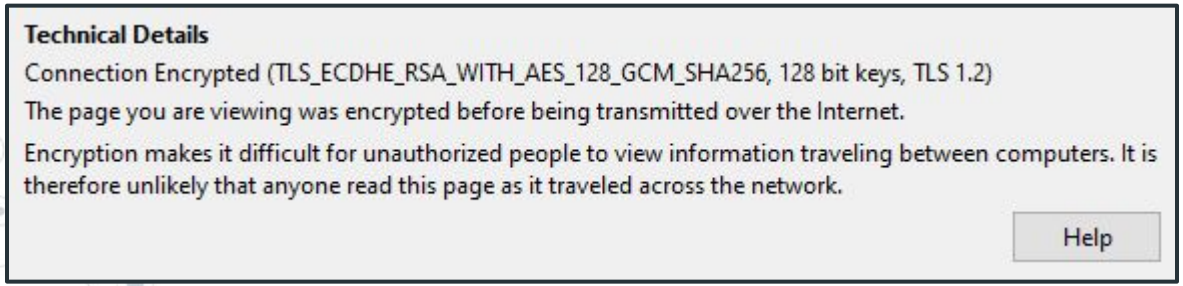
- Companies can use internal CAs to secure their own devices
  - Requires installing an additional root cert
  - Easy if the organization provides hardware

Jargon

Public Key Infrastructure (PKI): Umbrella term for the various protocols and organizations needed to run this

Transport Layer Security (TLS): A protocol for verifying a digital certificate, then encrypting traffic

- Often relies on AES and RSA (but can use different symmetric/asymmetric key algorithms as well)



Recap

Concepts

- Public Key Infrastructure
- Roots of Trust

Jargon

- Digital Certificate
- Certificate Authority
- Transport Layer Security (TLS)

Other options

A “**Web of Trust**”: Literally meeting face-to-face and exchanging public keys.

https://en.wikipedia.org/wiki/Key_signing_party

Other options

A “**Web of Trust**”: Literally meeting face-to-face and exchanging public keys.

Problem:

Very few people are going to do this.

https://en.wikipedia.org/wiki/Key_signing_party

Other options

Trust On First Use: Record the public key the first time, and alert if it changes.

```
$ ssh csci3403.com
The authenticity of host 'csci3403.com (34.68.147.105)' can't be established.
ECDSA key fingerprint is SHA256:kTk6kTG6gywLUNV7j3ynAkjtw2gL7S4yyPDFRPSHgb4.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Other options

Trust On First Use: Record the public key the first time, and alert if it changes.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
4e:10:42:39:53:85:7f:89:81:dc:d7:84:8d:79:e7:6d.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /root/.ssh/known_hosts:44
  remove with: ssh-keygen -f "/root/.ssh/known_hosts" -R 10.86.115.66
ECDSA host key for 10.86.115.66 has changed and you have requested strict checking.
Host key verification failed.
```

Other options

Trust On First Use: Record the public key the first time, and alert if it changes.

- First use can still be MitM’d

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
4e:10:42:39:53:85:7f:89:81:dc:d7:84:8d:79:e7:6d.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /root/.ssh/known_hosts:44
  remove with: ssh-keygen -f "/root/.ssh/known_hosts" -R 10.86.115.66
ECDSA host key for 10.86.115.66 has changed and you have requested strict checking.
Host key verification failed.
```

Other options

Trust On First Use: Record the public key the first time, and alert if it changes.

- First use can still be MitM’d
- Leads to “warning fatigue”

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
4e:10:42:39:53:85:7f:89:81:dc:d7:84:8d:79:e7:6d.
Please contact your system administrator.
Add correct host key in /root/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /root/.ssh/known_hosts:44
  remove with: ssh-keygen -f "/root/.ssh/known_hosts" -R 10.86.115.66
ECDSA host key for 10.86.115.66 has changed and you have requested strict checking.
Host key verification failed.
```

Questions?

Client trust

Patch notes

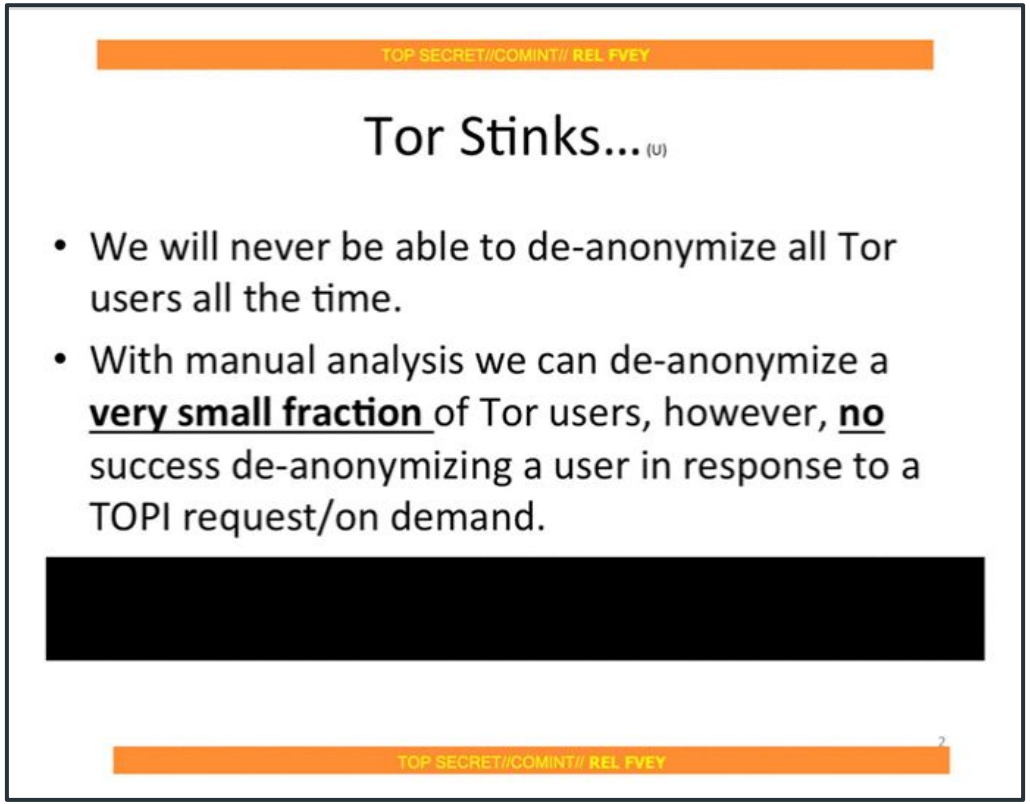
Project 1: Due 2/15 (next Tuesday)

This lecture is image is image / example heavy.
Descriptions are in the speaker notes.

Patch notes

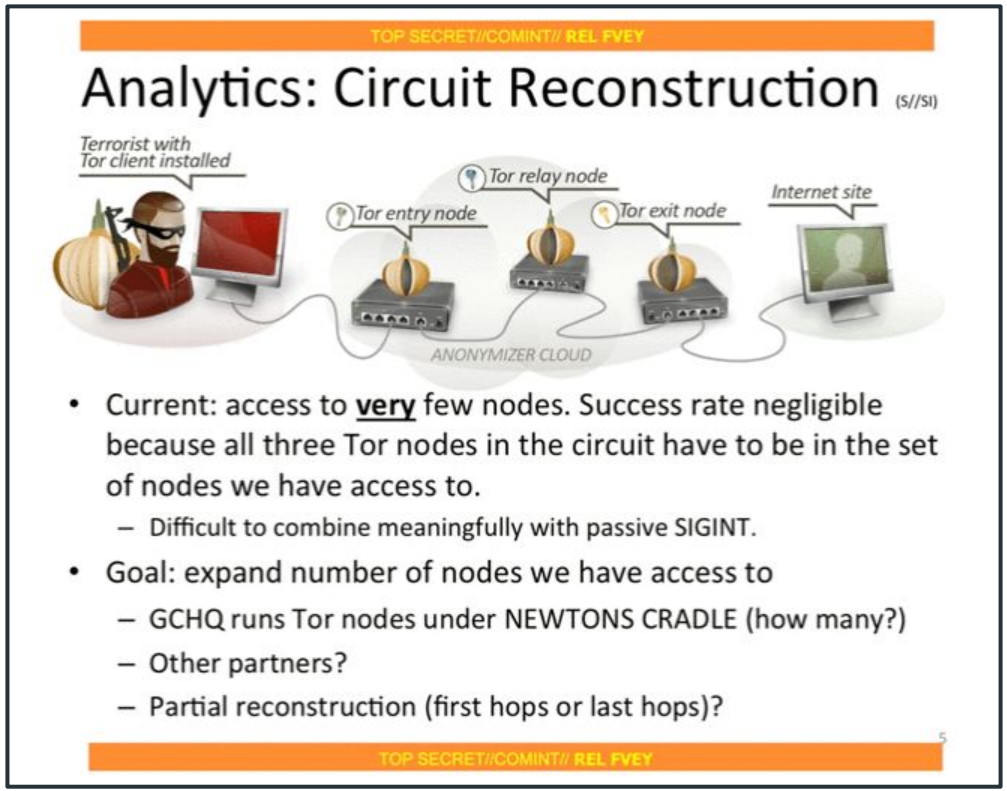
Questions from the chat: Can’t the government just host or take over a lot of TOR nodes?

Patch notes



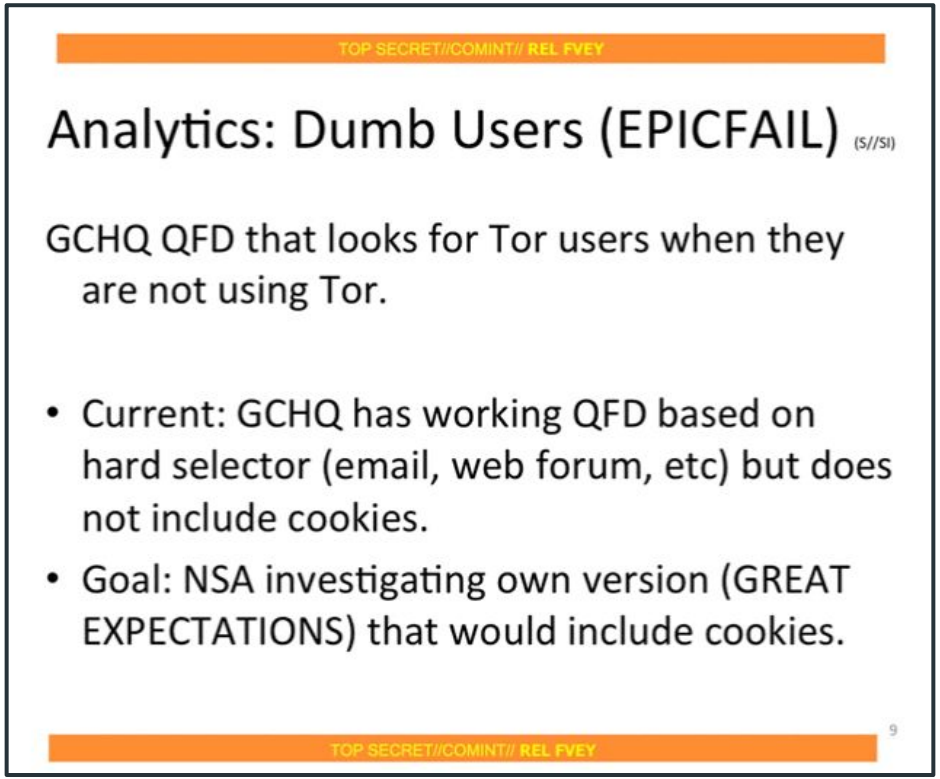
https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

Patch notes



https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

Patch notes



https://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

Patch notes

Questions from the chat: Can’t the government just host or take over a lot of TOR nodes?

A: Sounds like yes, but it appears that other attacks are proving easier.

Patch notes

Questions from the chat:

- **Q**: Can we use zero-knowledge proofs to confirm identities, rather than certificate authorities?

  A: Not yet. As far as I'm aware, nobody has come up with a way of proving identity without revealing any information about the identity of the person in question (such as whether or not they own a particular private key, or are trusted by a CA) and therefore it would not be a zero-trust proof. In fact, I am not aware of any widespread, practical use of those proofs at the moment.

- **Q**: What about a decentralized CA?

  A: The CA system is already decentralized. A CA's existence is based entirely on a consensus from whoever is using them: consensus at an individual level (e.g. you) or an organization level (e.g. Mozilla). There is no official blockchain-esque protocol to manage it, if that's what you mean, but it relies on the same principal of consensus, albeit at a human level rather than an automated one.

- **Q**: Could we use some kind of physical, OSI Layer 2 version of TOR to hide which entry node we use?

  A: The trouble with anything lower than the IP layer is it requires physical data transmission- you would need to have a lot of actual, physical routers, which connect to the internet through different paths… the logistics of this would be nearly impossible, and purchasing and assembling dozens of routers across a wide physical area would almost certainly draw more attention than just using TOR normally.

Certificates

```
During handling of the above exception, another exception occurred:
Traceback (most recent call last):
File "...\filepath\script.py", line 23, in
response = requests.get("https://csci3403.com")
requests.exceptions.SSLError:
Max retries exceeded with url: /login.cgi (Caused by
SSLError(SSLCertVerificationError(1,
    '[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed:
unable to get local issuer certificate (_ssl.c:1076)'
))
```

Certificates

Disabling certificate checking (very few reasons to do this):

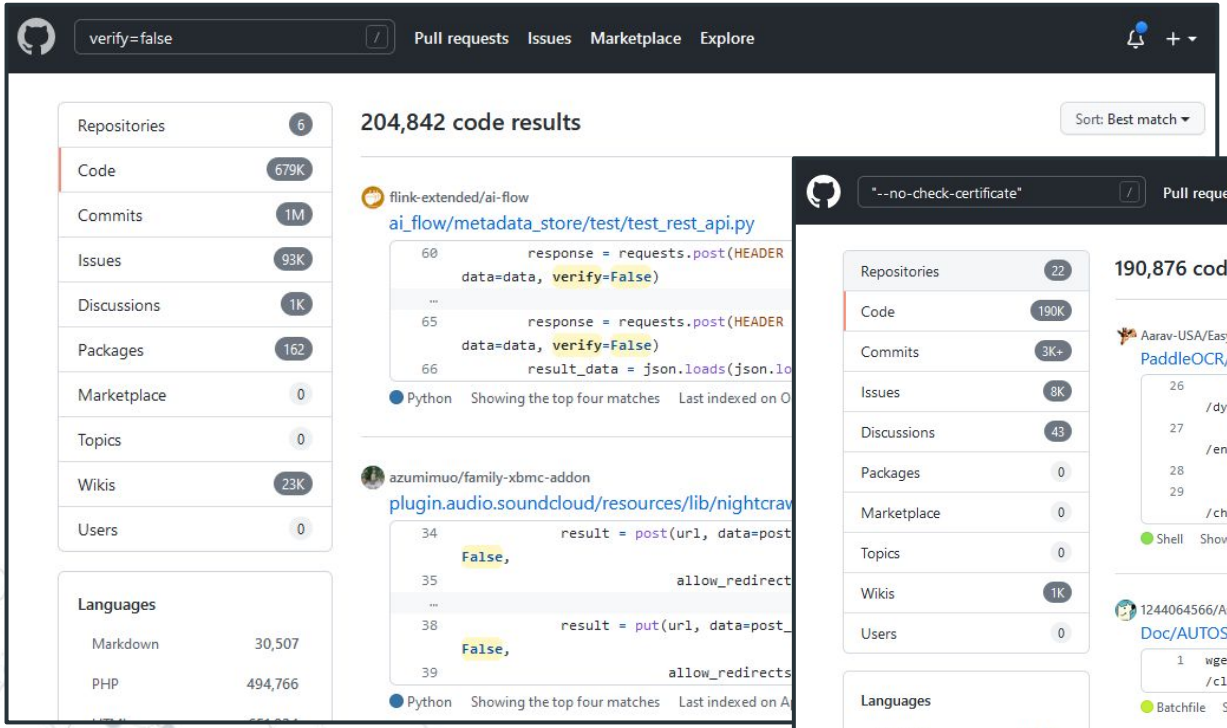
wget/curl:

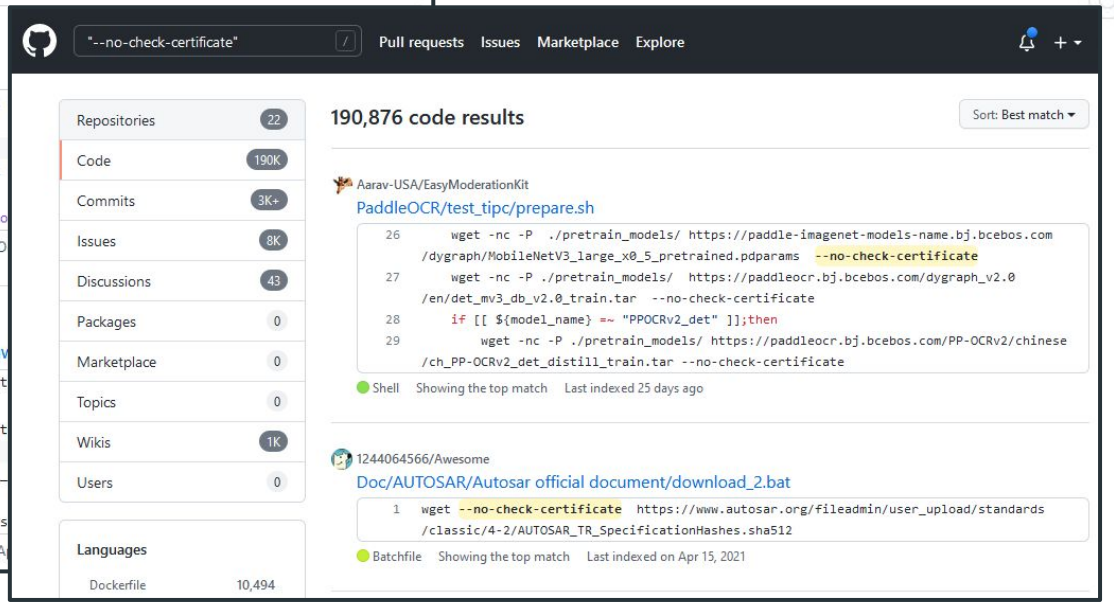
```
wget --no-check-certificate google.com
curl --insecure google.com
```

Python:

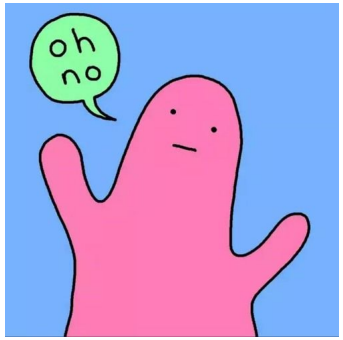
```
requests.get('google.com', verify=False)
```

Certificates





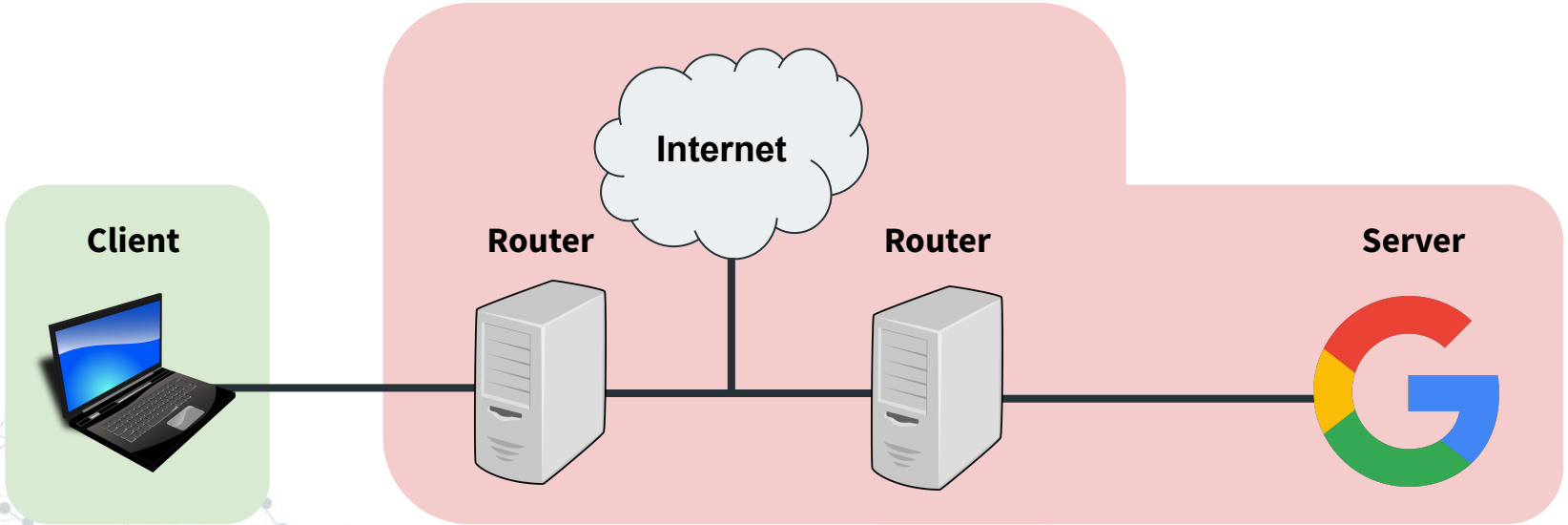
[...] ***there are also some valid use cases where you need to ignore server SSL certs****. One good example is when communicating with network devices such as local network equipment such as* ***routers, access-points, wireless bridge radios, and IoT devices****.*



https://jcutrer.com/python/requests-ignore-invalid-ssl-certificates

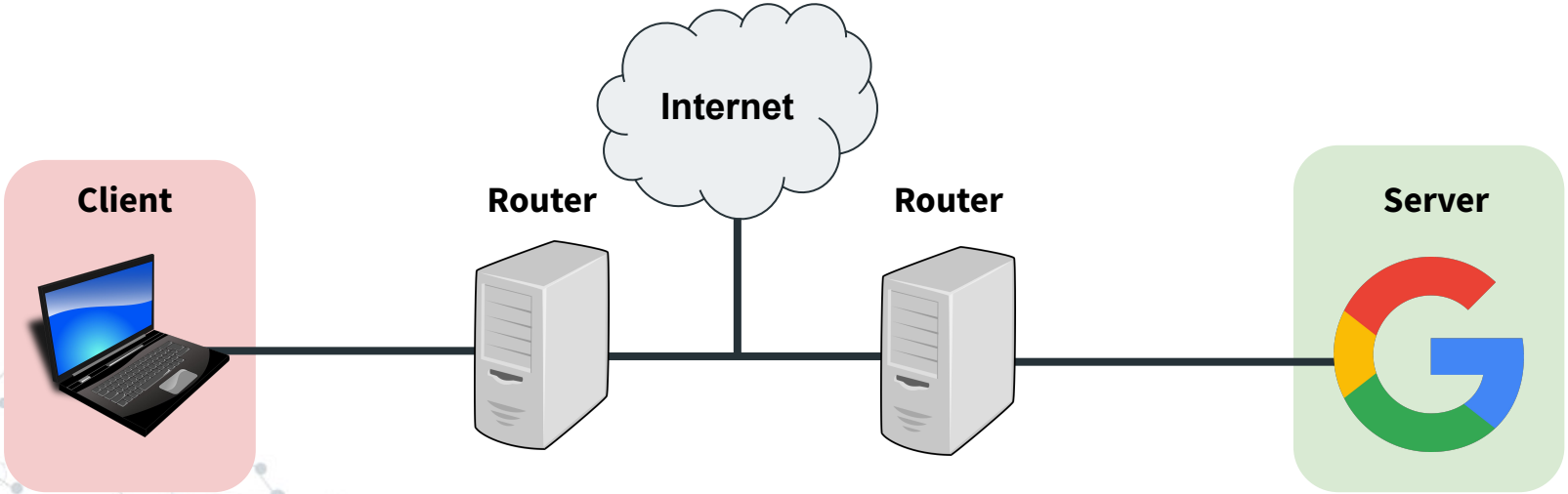
Client Trust

Most topics so far: Security concerns in between connections, and data leaked to the server



Client Trust

Today: Trusting the client, from the perspective of the server



Client Trust

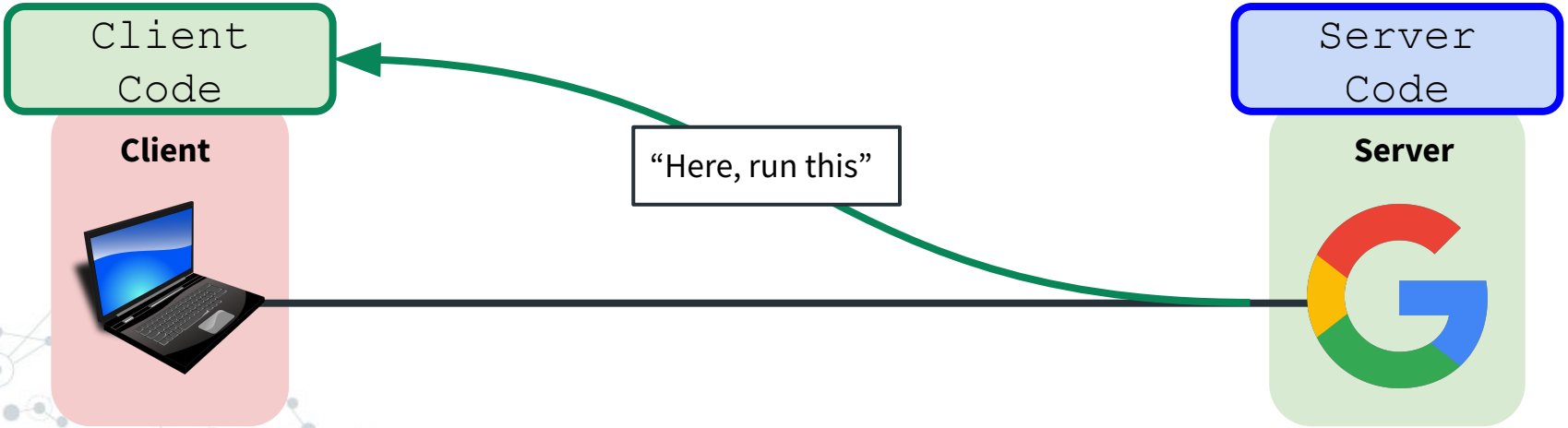
Client-side Trust: Broad term for trusting information from a client, which could be spoofed or altered.

Vulnerabilities arise when a client is given too much trust.

Client Trust

How this normally works:

- Server sends client code as well
- Client runs code, which exchanges data



Client Trust

Client (HTML):

```
<form id="chat-form">
    <input type="text" maxlength="200" placeholder="Enter message">
</form>
```

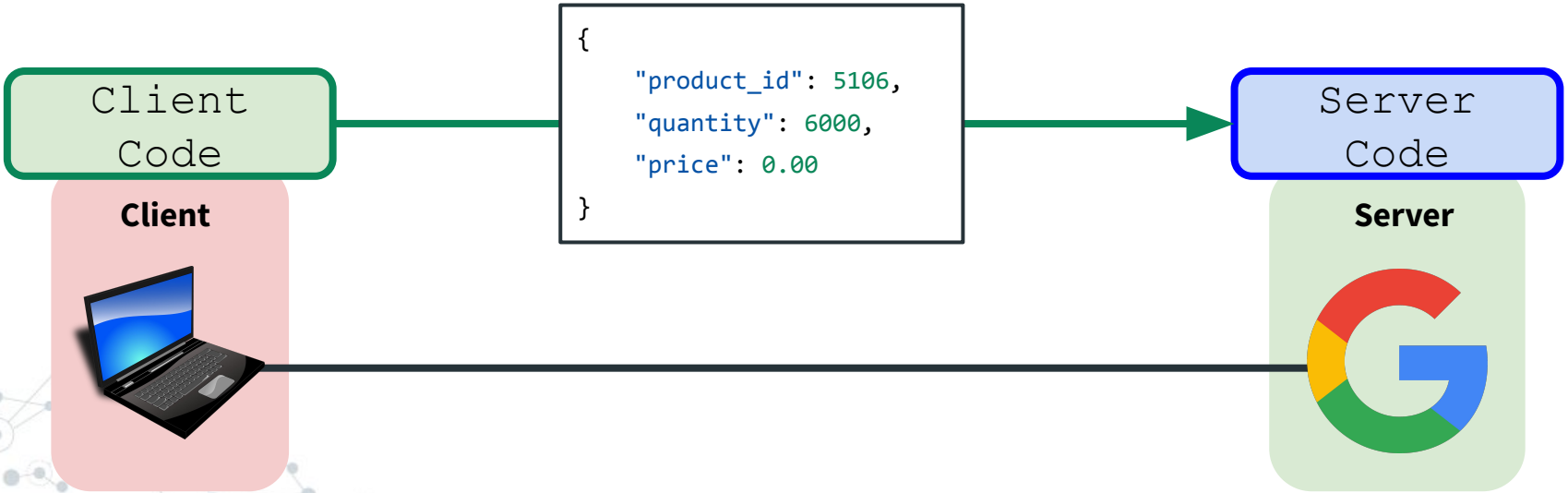
Server (Python):

```
def handle_chat_message(message):
    logger.info(f'{user.username} says: {message}')
```

Client Trust

Problem #1: Client-side validation

- You cannot trust client-side code!



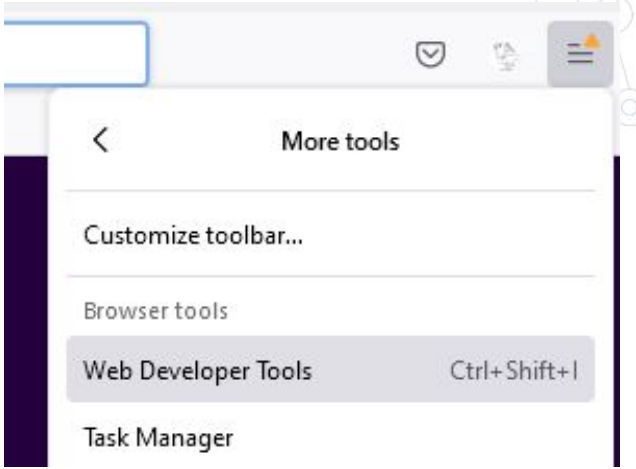
Client Trust

https://www.unknowncheats.me/forum/fall-guys-ultimate-knockout/413549-fall-guys-sharp.html

Client Trust

Accessing client-side code is easier than you might expect:

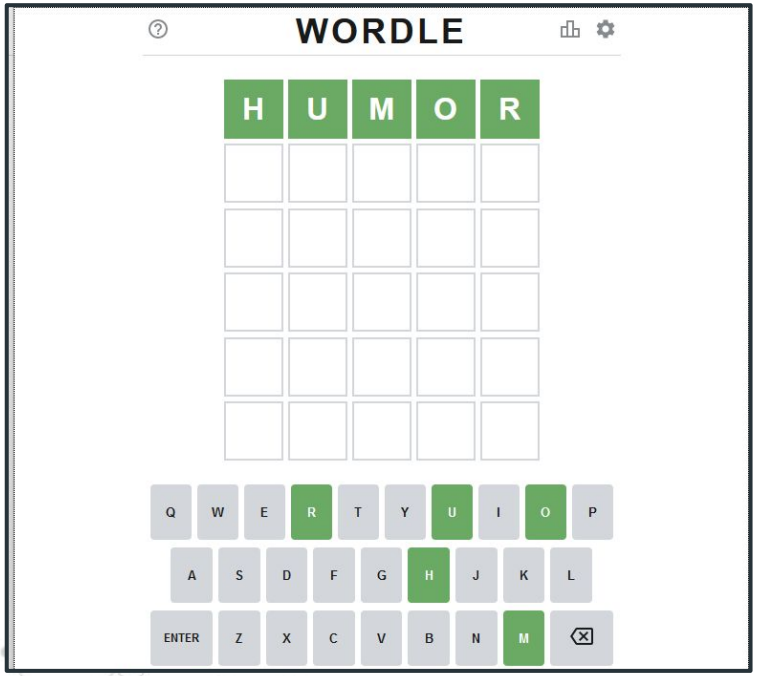
- Program / app code: May require disassembly
- Web code: Literally right there



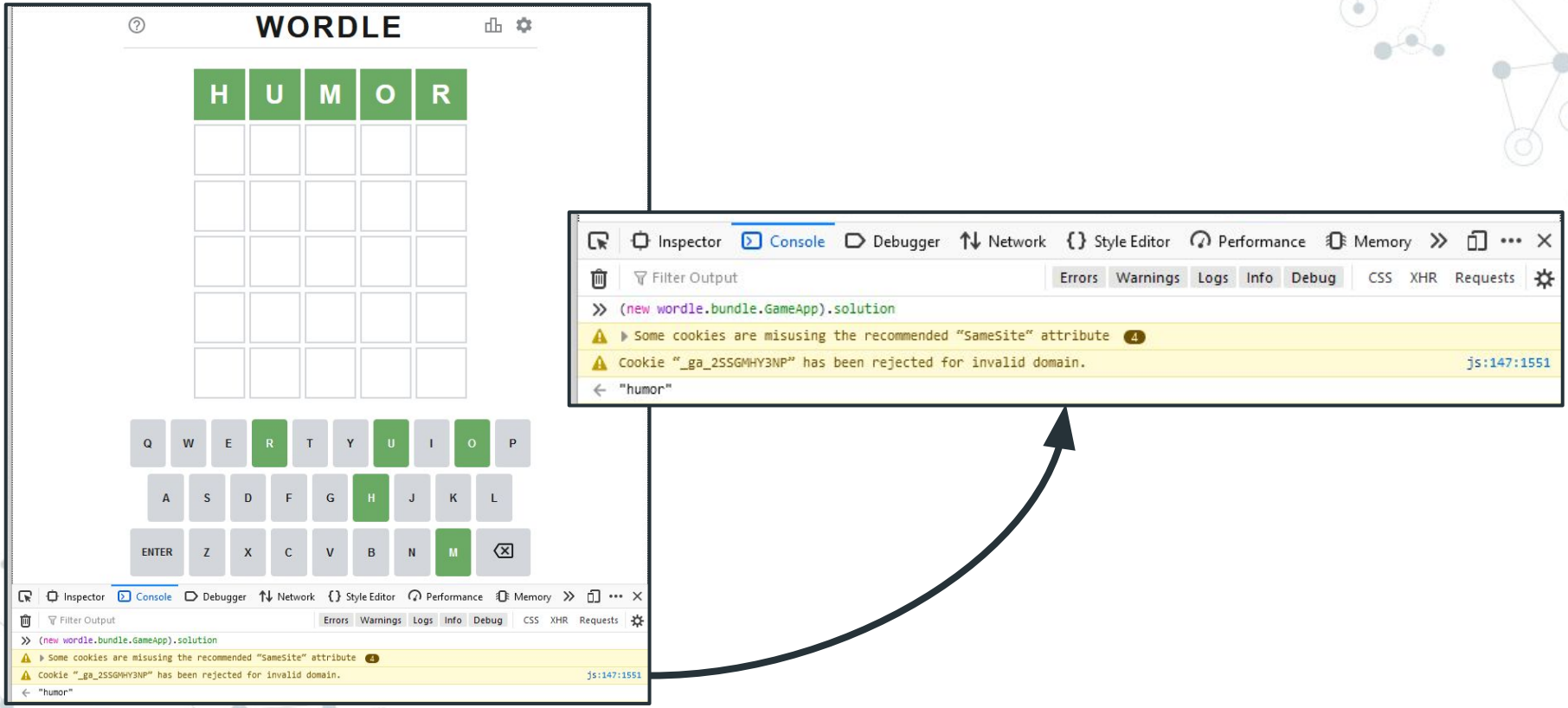
Client Trust

[Developer tools demo]

Client Trust



Client Trust



Client Trust

Alternative to digging through code: View network traffic

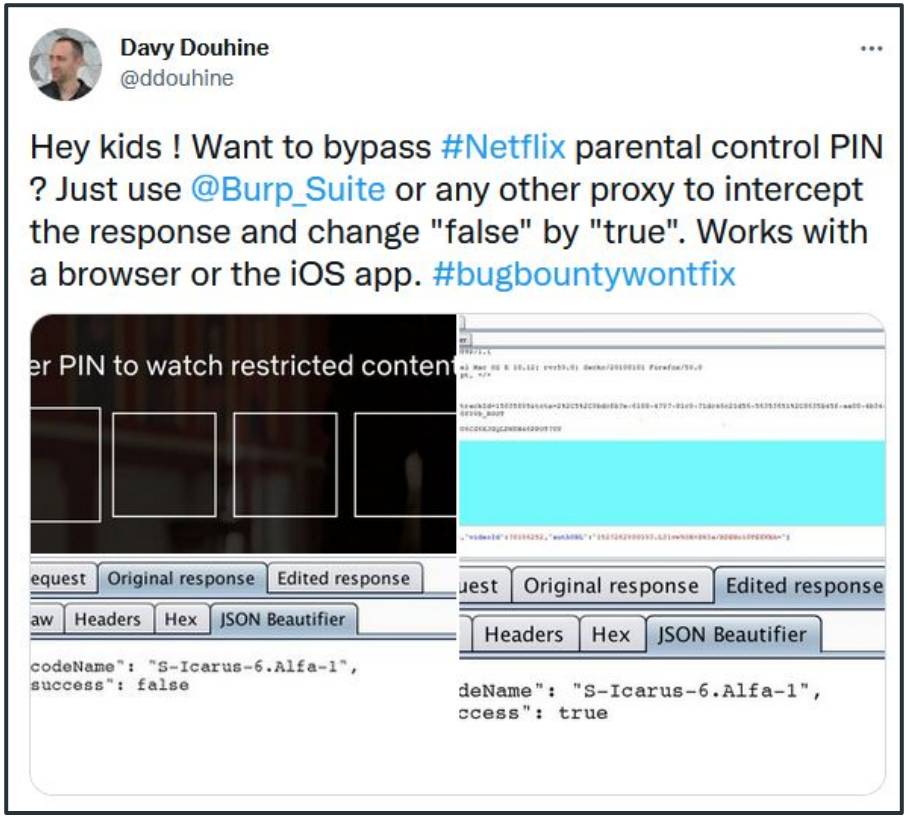
- The client Man-in-the-Middles their own traffic and modifies it

#	Host	Method	URL	Params	Edited	Status	Length	MIME type
1	https://incoming.telemetry.mozi...	POST	/submit/firefox-desktop/baseline/1/2e...			200	618	text
2	https://signaler-pa.clients6.goo...	OPTIONS	/punctual/multi-watch/channel?VER=8...	✓		200	577	HTML
3	https://signaler-pa.clients6.goo...	GET	/punctual/multi-watch/channel?VER=8...	✓				
5	https://docs.google.com	GET	/presentation/d/1xs3qhtSyKY78i_b5xZF...	✓				
6	https://www.google.com	GET	/complete/search?client=firefox&q=cl	✓		200	795	JSON
7	https://www.google.com	GET	/complete/search?client=firefox&q=cla	✓		200	766	JSON
8	https://www.google.com	GET	/complete/search?client=firefox&q=clas	✓		200	778	JSON
9	https://www.google.com	GET	/complete/search?client=firefox&q=cl...	✓		200	774	JSON

Client Trust

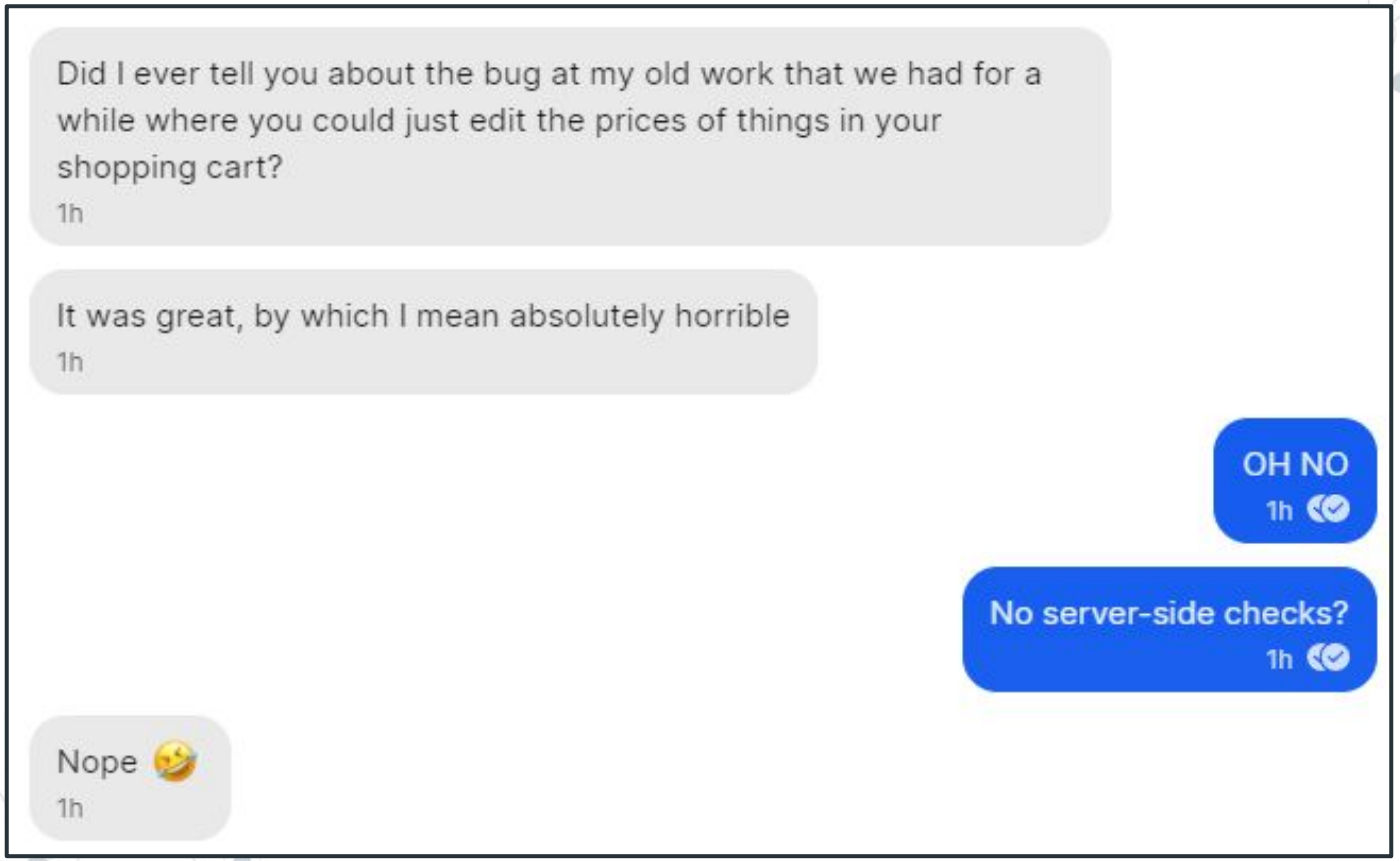
[BURP Suite demo]

Client Trust

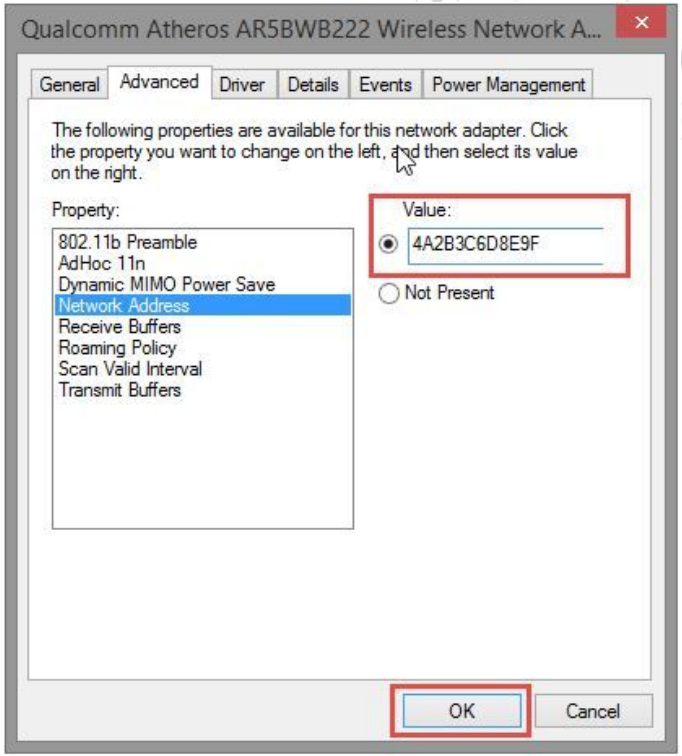


https://twitter.com/ddouhine/status/1000048649802534912

Client Trust



Client Trust



https://www.thewindowsclub.com/change-mac-address-in-windows

Client Trust

Common sources of client-side validation:

- Validating input format
  - e.g. User email validation, password length checks
- Important calculations
  - e.g. Amazon order cost, video game health
- “Disabled” controls
  - e.g. greyed-out buttons

Client Trust

IP spoofing: Modify the source IP address of packets

Client Trust

IP spoofing: Modify the source IP address of packets

Q #1: Why not spoof the destination IP as well?

Client Trust

IP spoofing: Modify the source IP address of packets

Q #1: Why not spoof the destination IP as well?

- Goes to the wrong place

Client Trust

IP spoofing: Modify the source IP address of packets

Q #1: Why not spoof the destination IP as well?

- Goes to the wrong place

Q #2: How could this cause harm?

Client Trust

IP spoofing: Modify the source IP address of packets

Q #1: Why not spoof the destination IP as well?

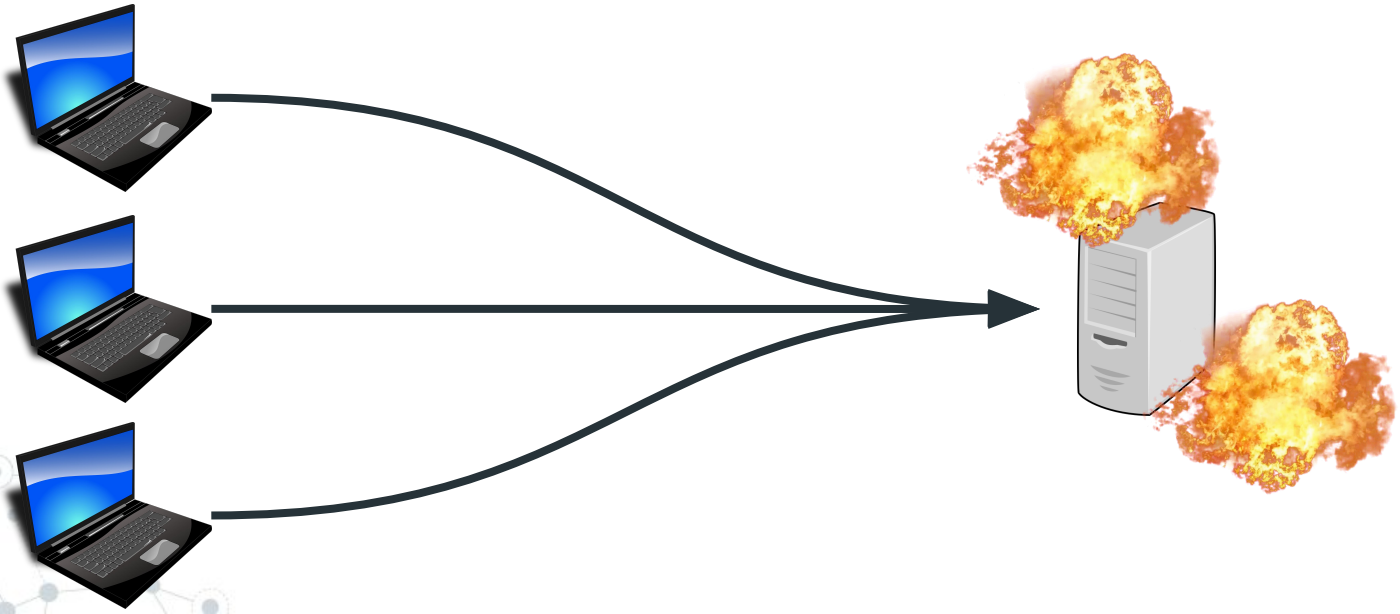
- Goes to the wrong place

Q #2: How could this cause harm?

- Response gets sent to a third party

Client Trust

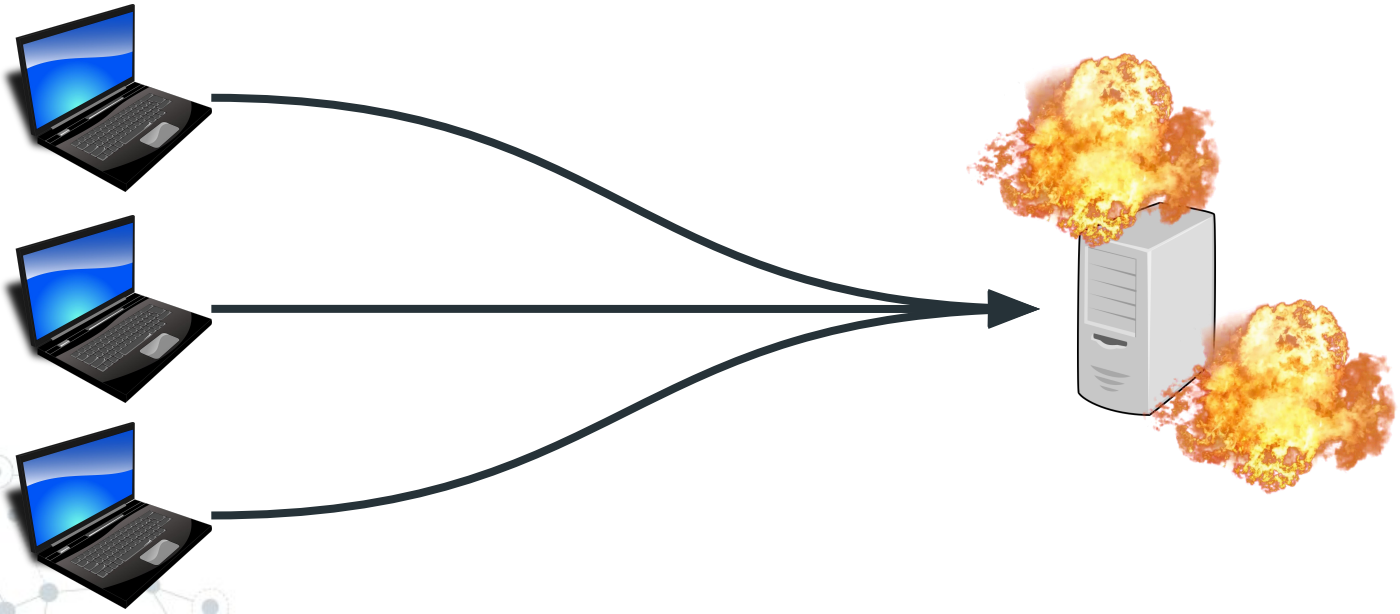
DoS attack: Overwhelm a server with spam packets



Client Trust

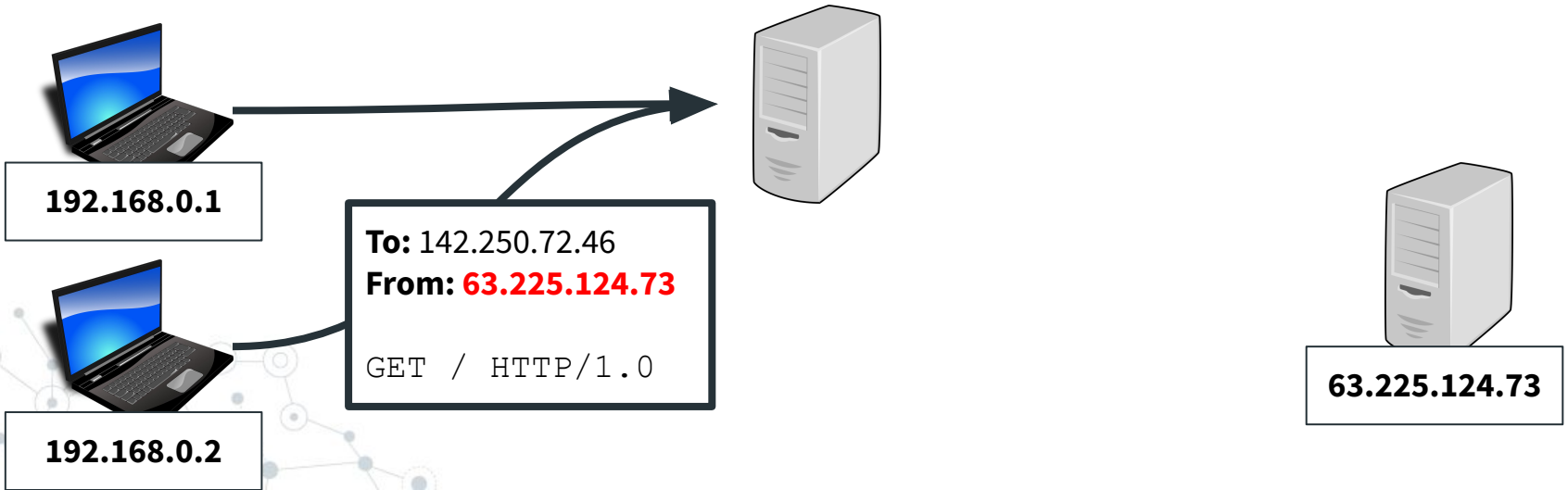
DoS attack: Overwhelm a server with spam packets

- Difficulty for attackers: Need a lot of computing power



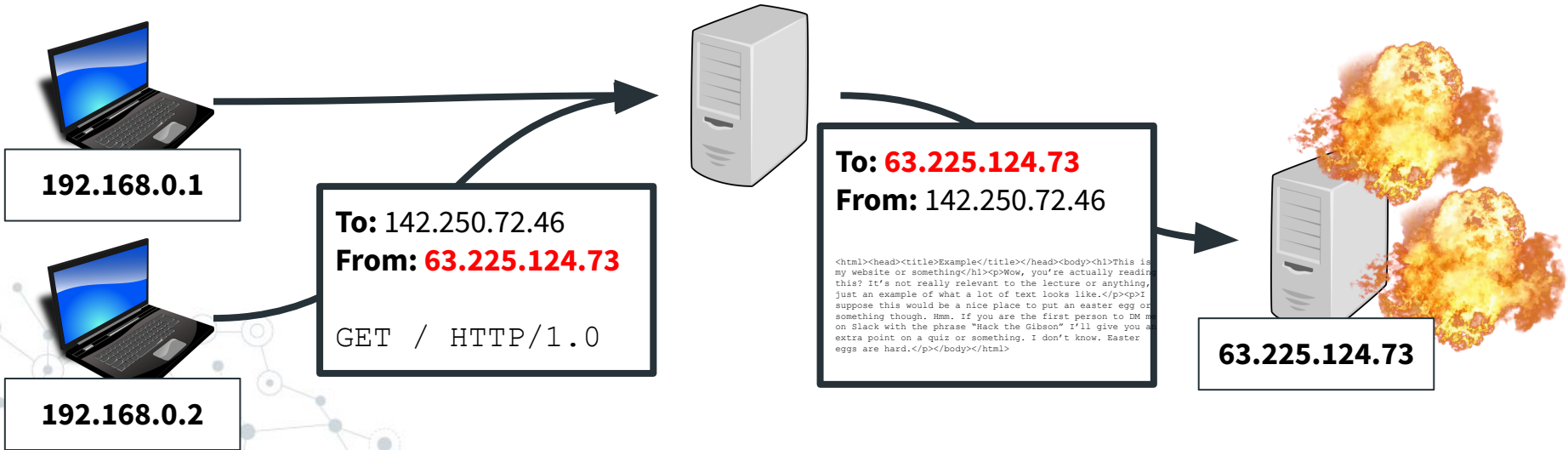
Client Trust

Reflected DoS attack: Attackers spoof their IP, sending responses to the wrong server



Client Trust

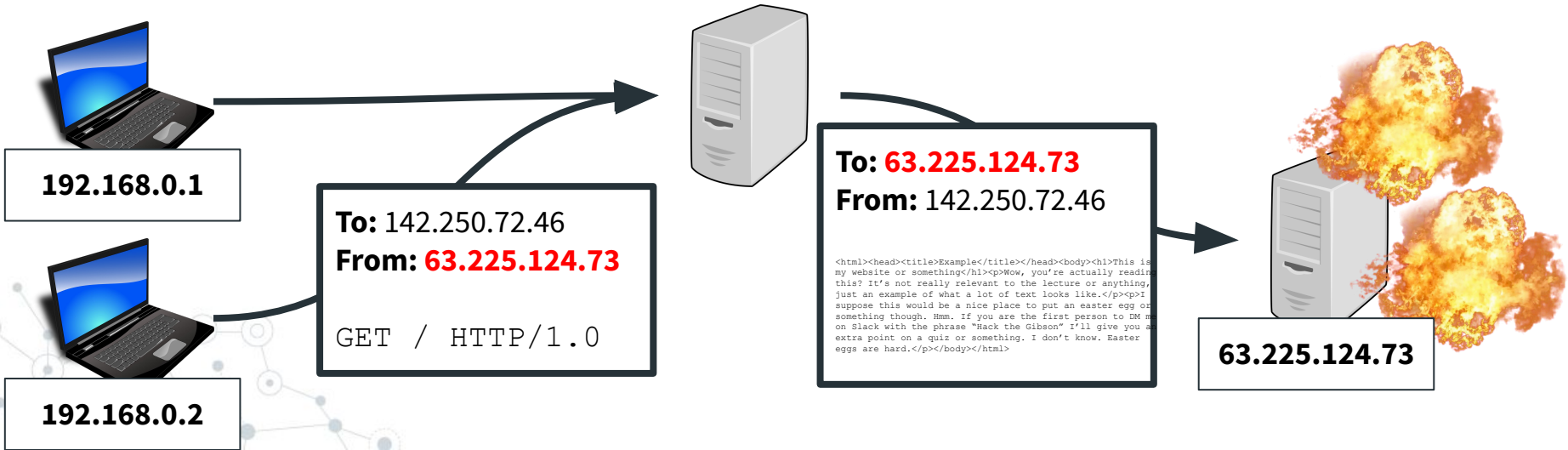
Reflected DoS attack: Attackers spoof their IP, sending responses to the wrong server



Client Trust

Reflected DoS attack: Attackers spoof their IP, sending responses to the wrong server

- Power depends on ratio of request / response size



Client Trust

Mitigations:

- Verify important calculations server-side!
- Rate-limit repeated messages

```
<form id="chat-form">
    <input type="text" maxlength="200" placeholder="Enter message">
</form>
```

```
def handle_chat_message(message):
    if len(message) > 200:
        logger.info('chat_error', 'Message was too long.')
    else
        logger.info(f'{user.username} says: {message}')
```

Recap

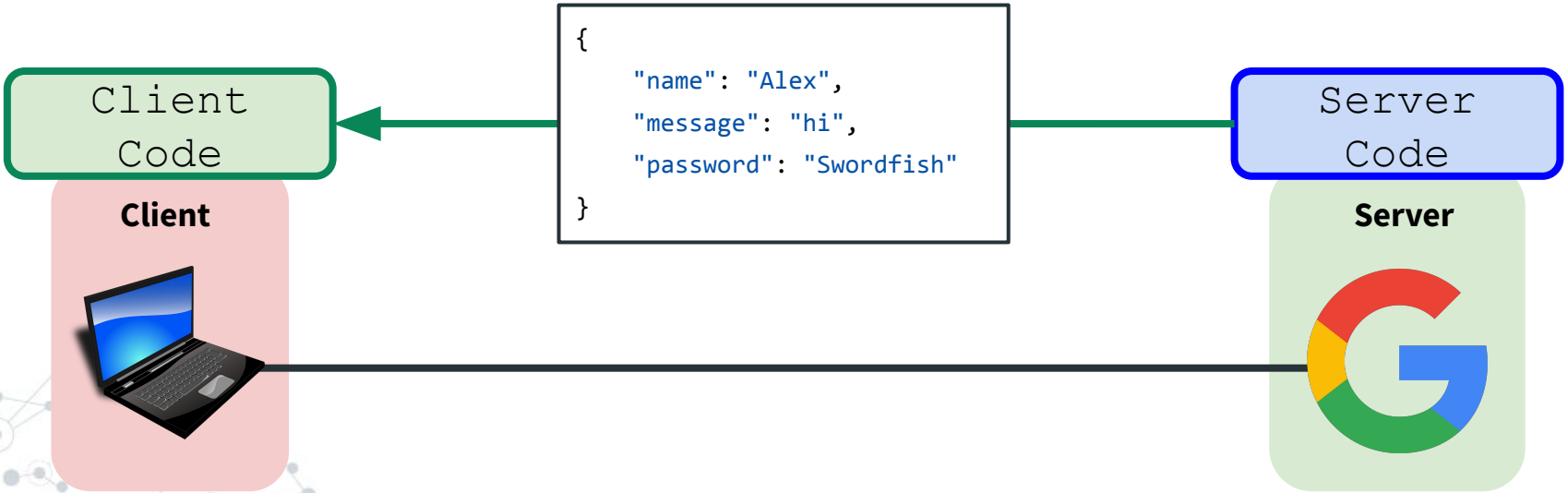
Client-side trust: Often dangerous and abusable

- Client-side checks should be verified server-side

Reflected DoS: Attackers can trick websites into overwhelming each other by spoofing their IP address

Client Trust

Problem #2: Blindly sending information to a client



Client Trust

2020 Grindr Hack:

1. Attacker initiates a password reset for the victim

Client Trust

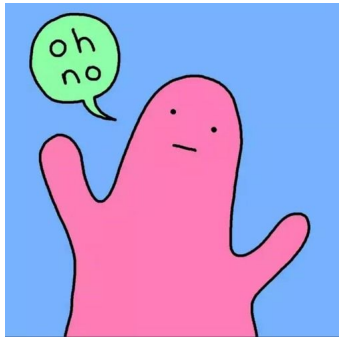
2020 Grindr Hack:

1. Attacker initiates a password reset for the victim
2. Grindr sends a code to the victim’s email

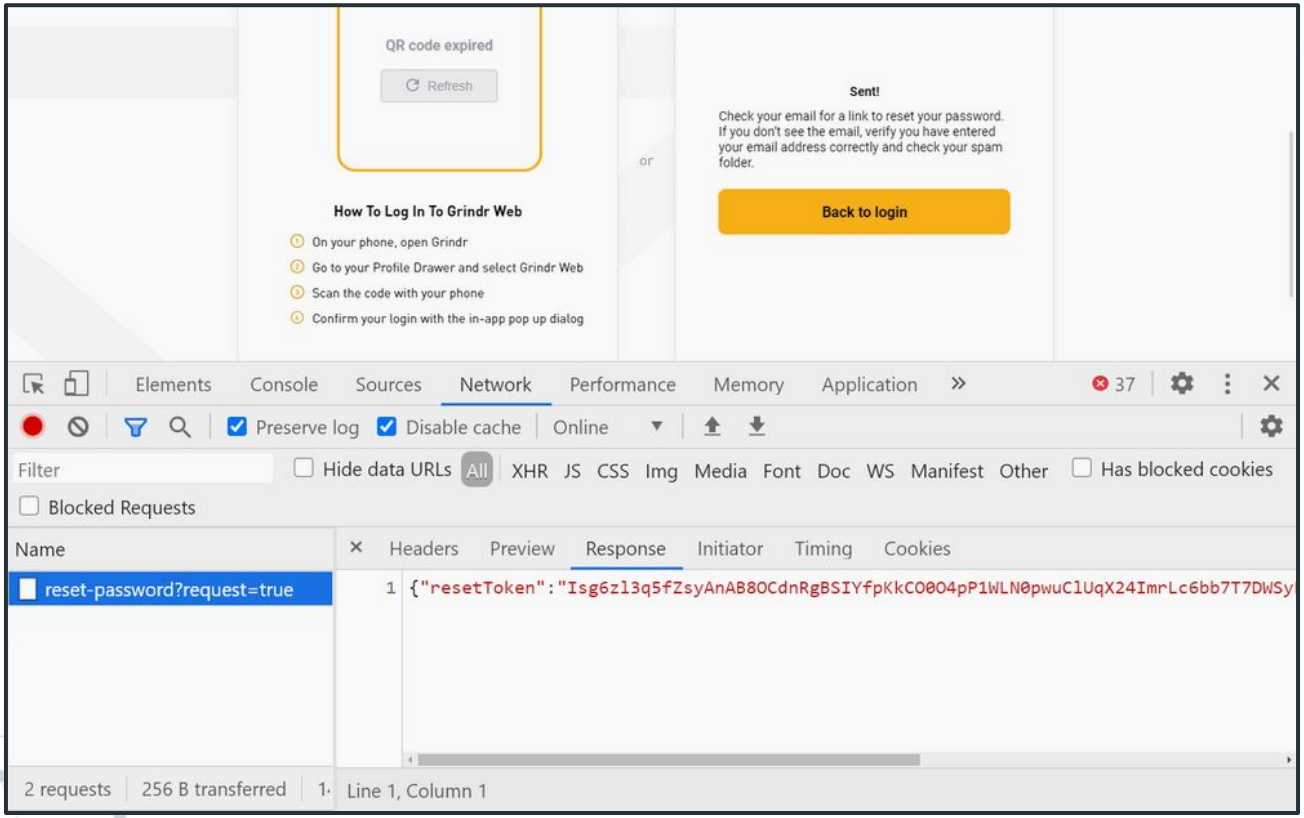
Client Trust

2020 Grindr Hack:

1. Attacker initiates a password reset for the victim
2. Grindr sends a code to the victim's email
3. …and also the page telling them to check their email

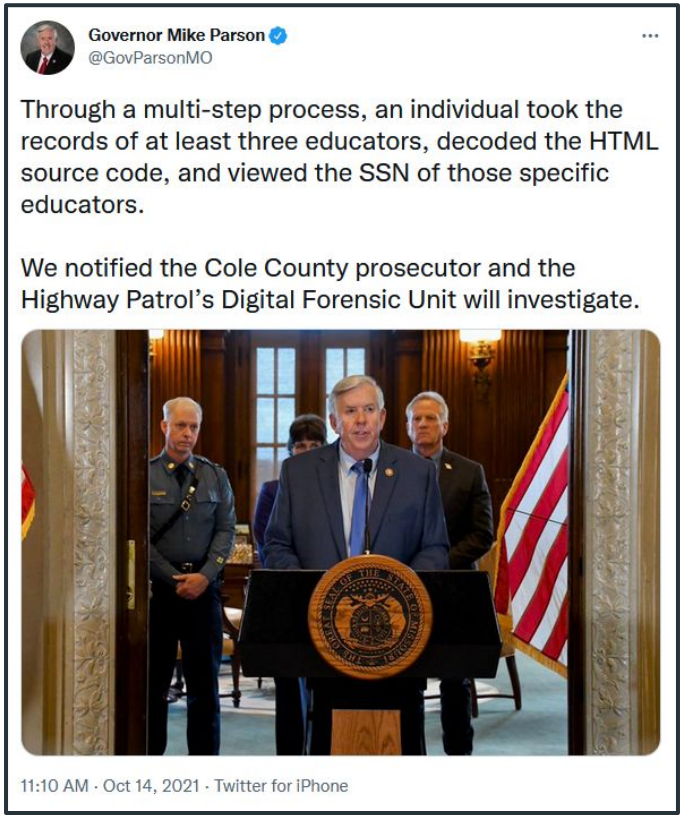


Client Trust



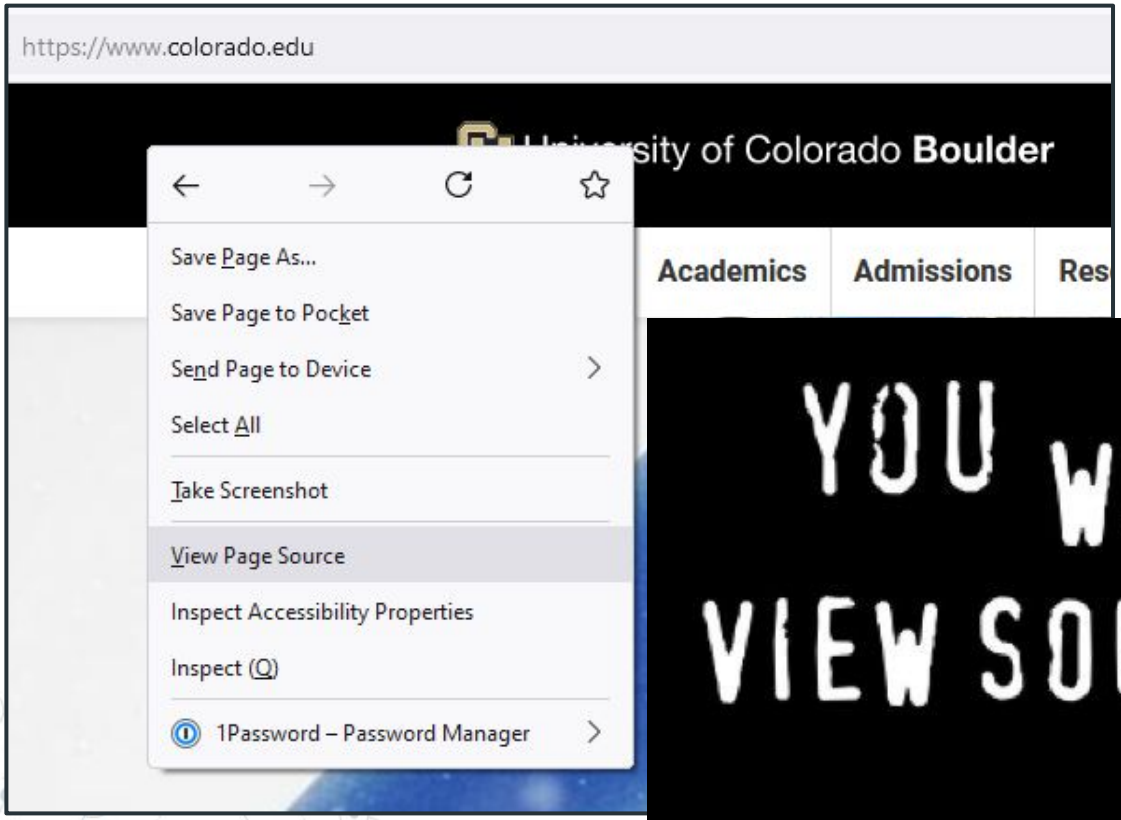
https://techcrunch.com/2020/10/02/grindr-account-hijack-flaw/

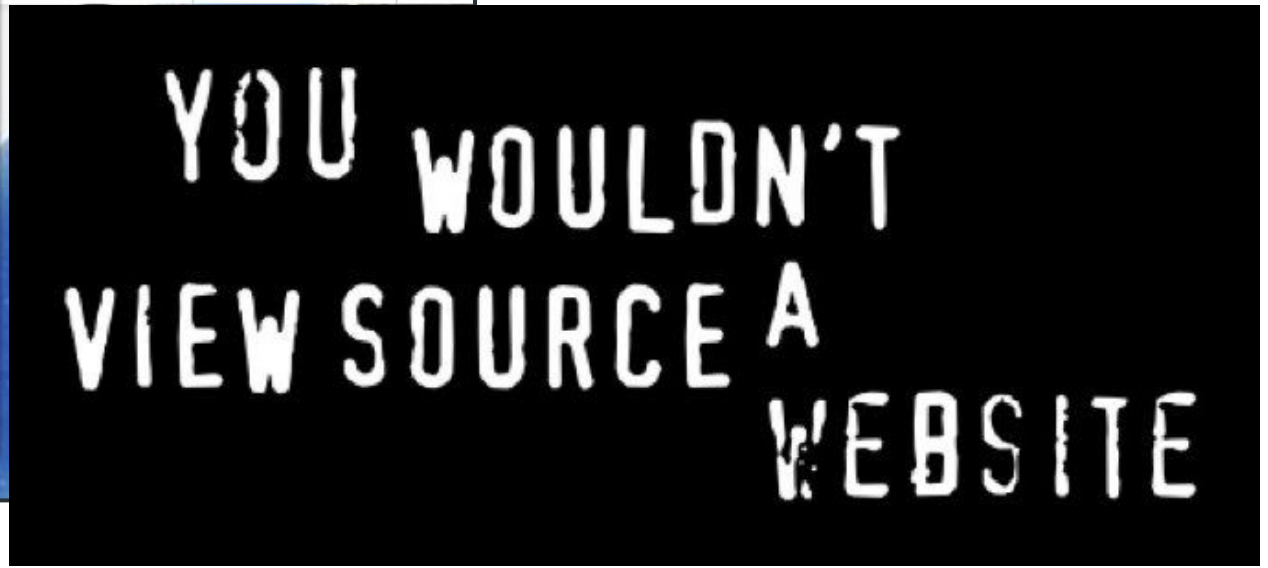
Client Trust



https://twitter.com/GovParsonMO/status/1448697768311132160

Client Trust

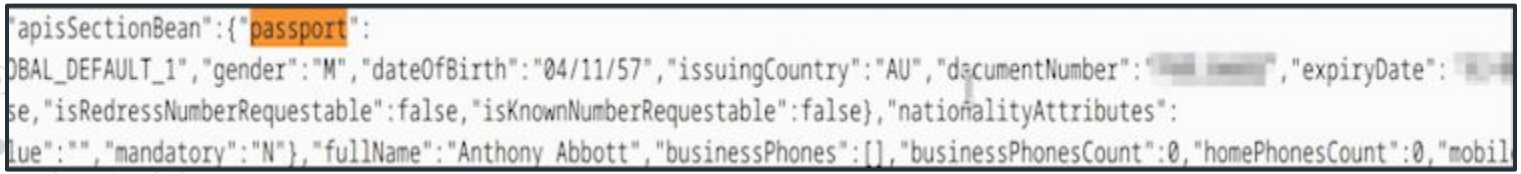




Client Trust

Q: Why is this information sent client-side?

A: Lazy coding practices, normally. Often everything is sent to the client, rather than picking and choosing data.



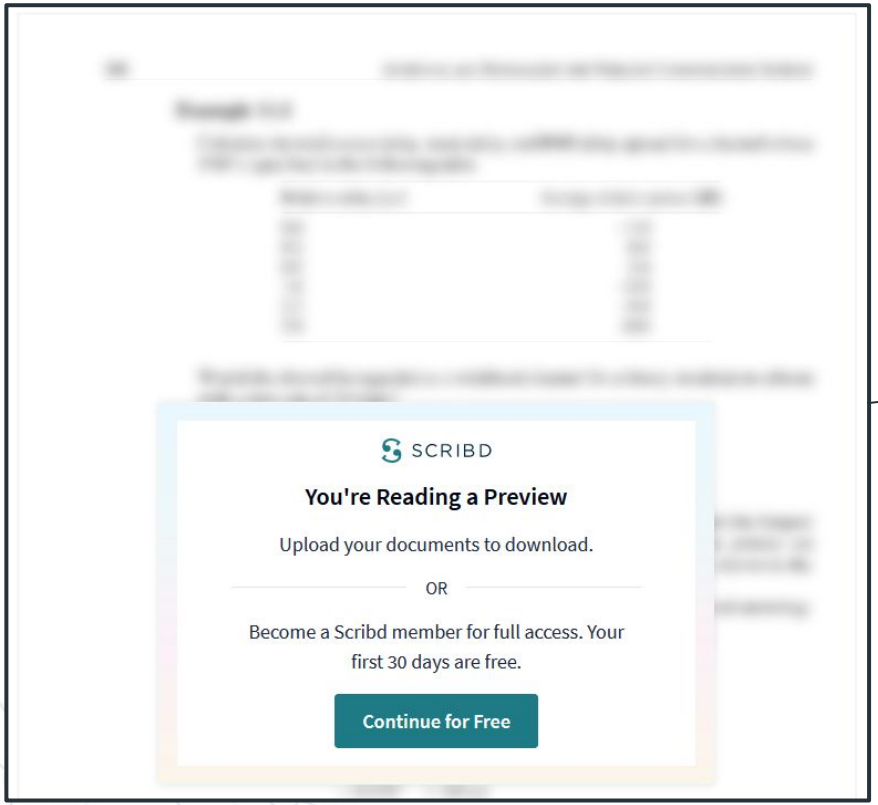
https://mango.pdf.zone/finding-former-australian-prime-minister-tony-abbotts-passport-number-on-instagram

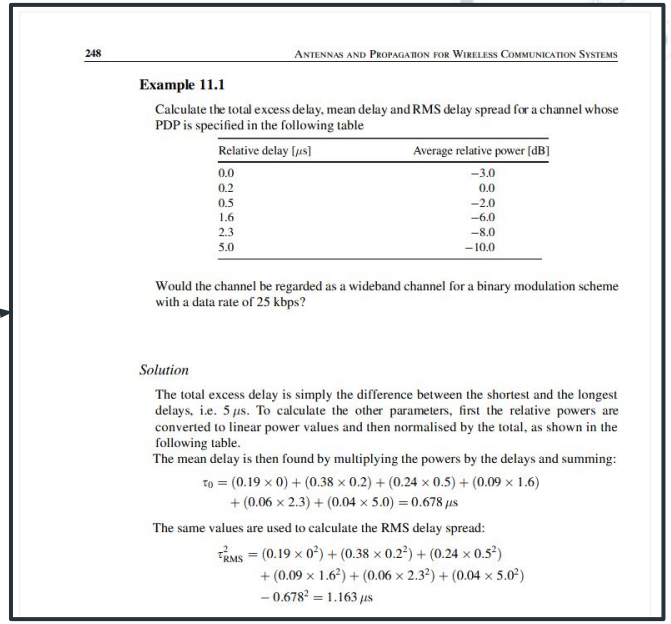
Client Trust

Security Through Obscurity: Hoping that an attacker does not discover available information, rather than preventing them from accessing it

- Almost always a bad idea

Client Trust





248 ANTENNAS AND PROPAGATION FOR WIRELESS COMMUNICATION SYSTEMS

Example 11.1

Calculate the total excess delay, mean delay and RMS delay spread for a channel whose PDP is specified in the following table

Relative delay [μs]	Average relative power [dB]
0.0	−3.0
0.2	0.0
0.5	−2.0
1.6	−6.0
2.3	−8.0
5.0	−10.0

Would the channel be regarded as a wideband channel for a binary modulation scheme with a data rate of 25 kbps?

Solution

The total excess delay is simply the difference between the shortest and the longest delays, i.e. 5 μs. To calculate the other parameters, first the relative powers are converted to linear power values and then normalised by the total, as shown in the following table.
The mean delay is then found by multiplying the powers by the delays and summing:

$$\tau_0 = (0.19 \times 0) + (0.38 \times 0.2) + (0.24 \times 0.5) + (0.09 \times 1.6) + (0.06 \times 2.3) + (0.04 \times 5.0) = 0.678\,\mu s$$

The same values are used to calculate the RMS delay spread:

$$\tau_{RMS}^2 = (0.19 \times 0^2) + (0.38 \times 0.2^2) + (0.24 \times 0.5^2) + (0.09 \times 1.6^2) + (0.06 \times 2.3^2) + (0.04 \times 5.0^2) - 0.678^2 = 1.163\,\mu s$$

https://www.scribd.com/document/73106647/Antennas-and-Propagation-for-Wireless-Communication-Systems-2nd-Ed

Client Trust

Expert Answer

This problem has been solved!

See the answer

https://www.chegg.com/homework-help/questions-and-answers/please-complete-risk-matrix-based-information-second-image-need-graph-q91501055

Client Trust

https://twitter.com/rombik_su/status/1491526725976657924

Client Trust

Mitigations:

- Easy answer: Only send non-confidential data to client

Client Trust

Mitigations:

- Easy answer: Only send non-confidential data to client
- Real-life answers:
  - Security outreach and education
  - Threat modeling
  - Some framework or type system that prevents data from crossing the client boundary?

Recap

Security Through Obscurity: Hiding data rather than securing it

Sending sensitive information to a client:

- You should not do this

Recap

Security Through Obscurity: Hiding data rather than securing it

Sending sensitive information to a client:

- You should not do this
- Engineers will absolutely keep doing this

Recap

Security Through Obscurity: Hiding data rather than securing it

Sending sensitive information to a client:

- You should not do this
- Engineers will absolutely keep doing this
  - On the plus side, good job security for us!

Questions?