Computer and Network Security

Lecture 22: TLS / Protocols

COMP-5370/6370
Fall 2025


The TLS Protocol

IN THE YEAR 2023, NO PUBLIC-FACING WEBSITE SHOULD NOT SUPPORT & UPGRADE TO HTTPS.

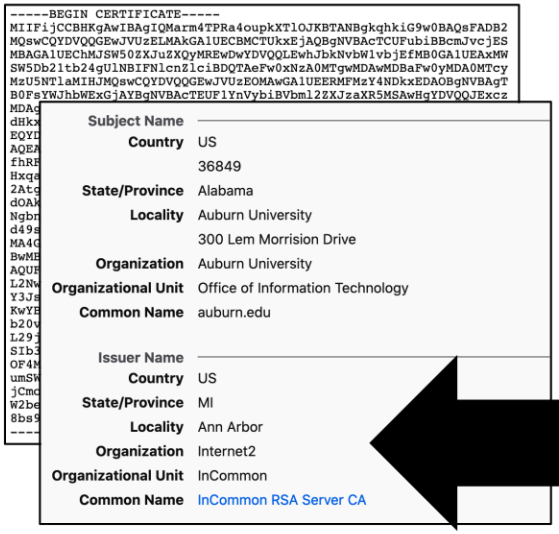
Key Distribution Problem

Key Distribution Problem is the generic name used to reference real-world challenges from a nominally simple need.

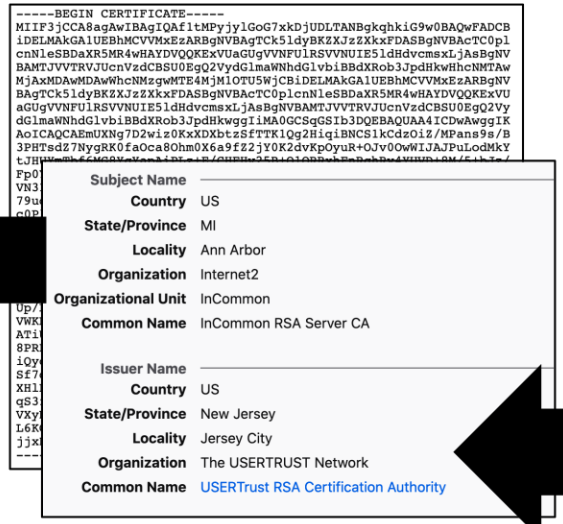
- Is well-known and widely maligned
- Directly applicable to shared secrets
- Also applicable to non-secret provenance

SSL Certificate Chains

Leaf Certificate

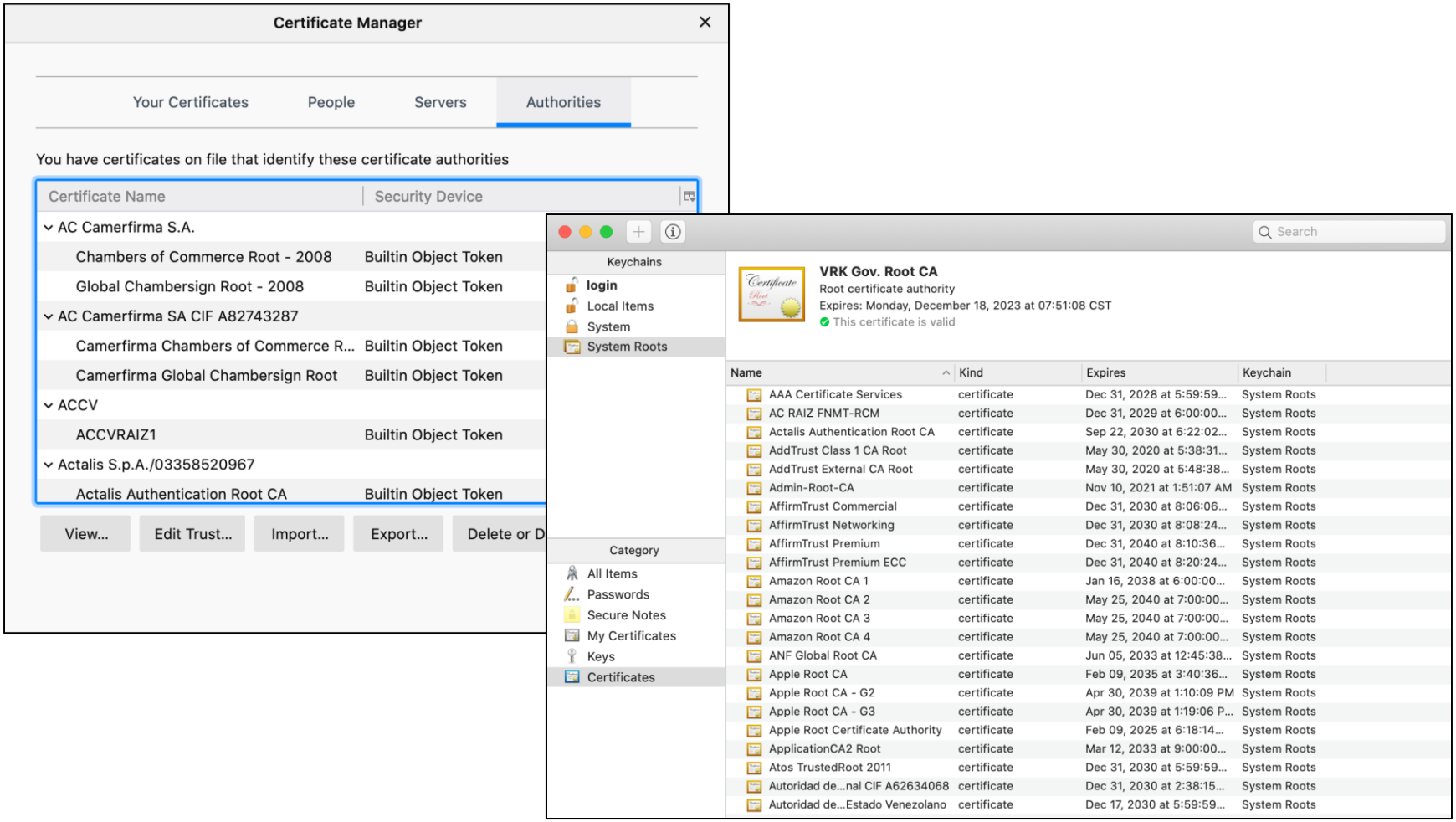


Intermediate Certificate



Root Certificate

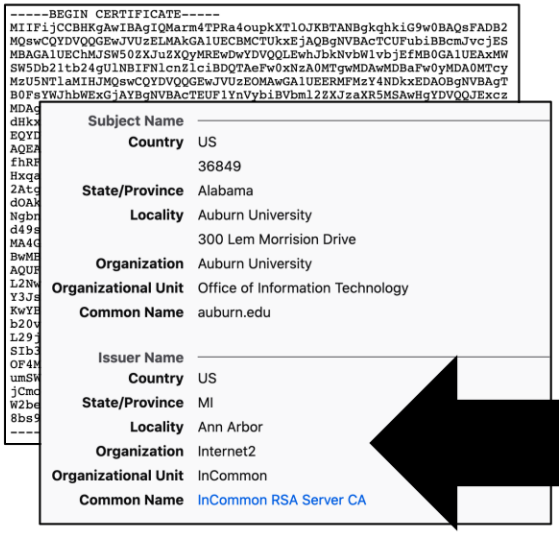
Root Certificate Authorities (Root CAs)



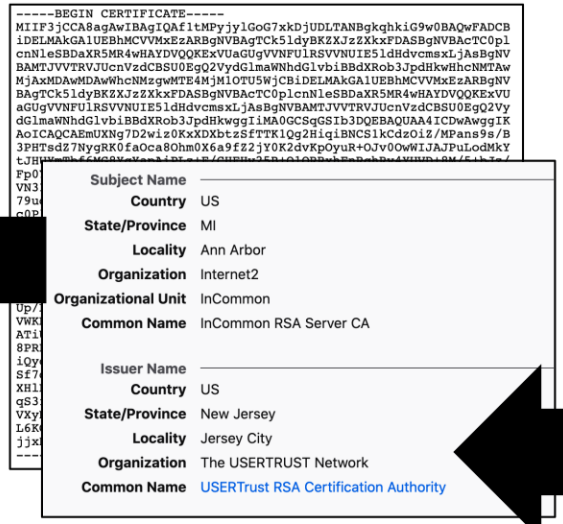
Compromised Root CA

SSL Certificate Chains

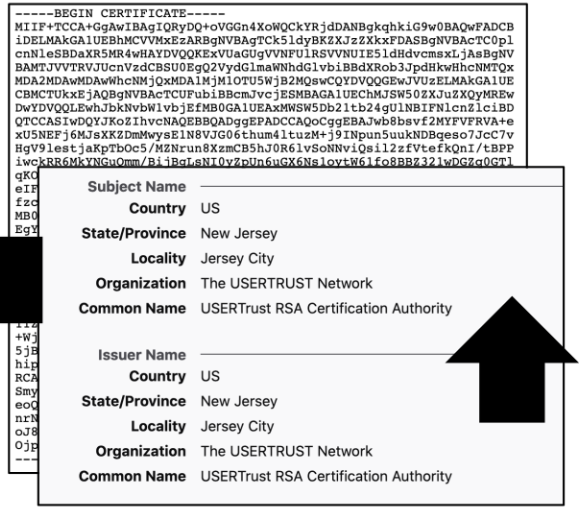
Leaf Certificate



Intermediate Certificate

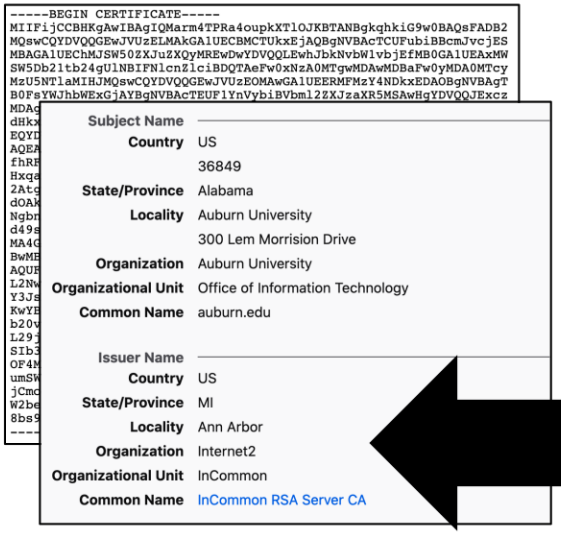


Root Certificate



SSL Certificate Chains

Leaf Certificate

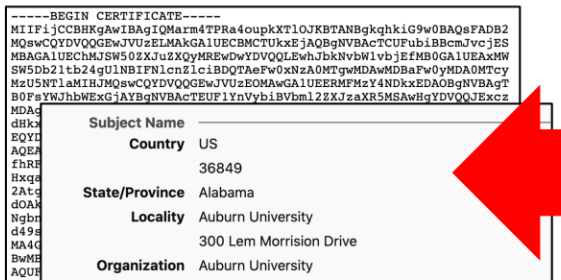


Intermediate Certificate

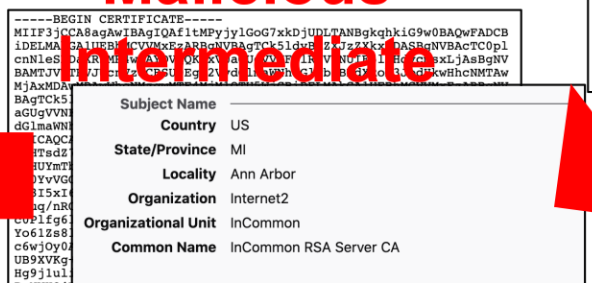
Root Certificate

COMPROMISED

Malicious Leaf

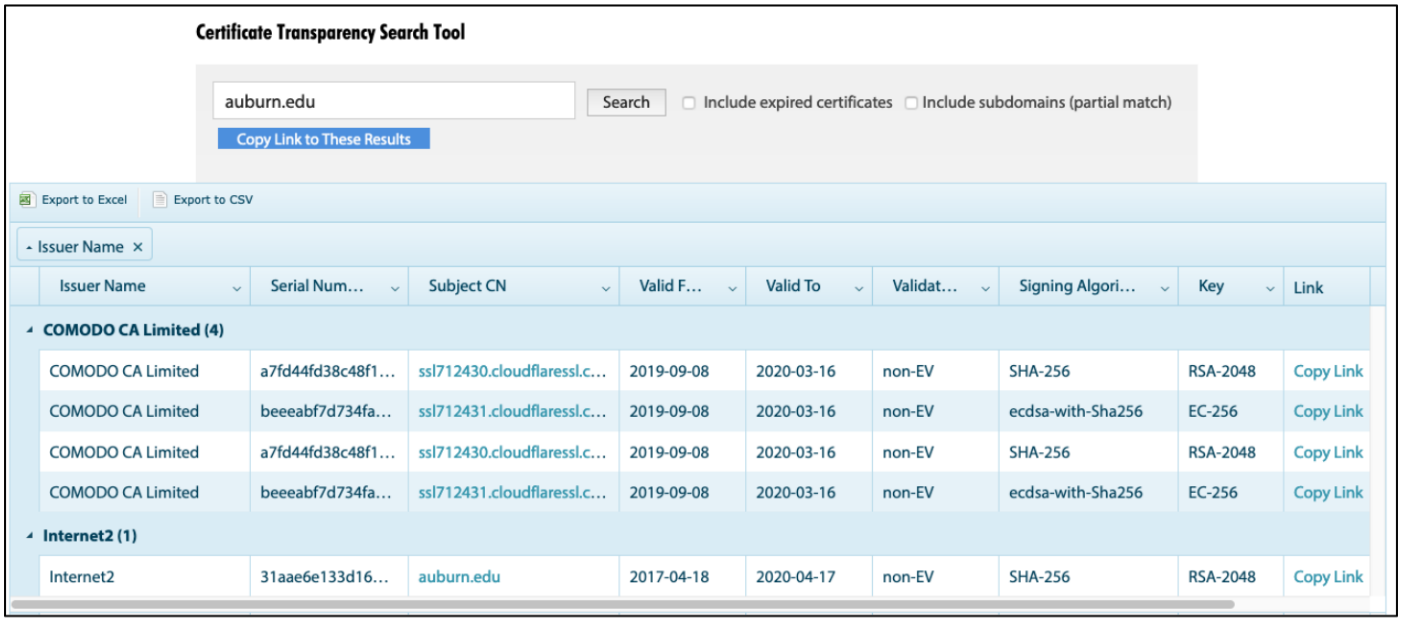


Malicious Intermediate



Certificate Transparency

- When issuing an SSL cert, CA must notify 3rd parties of the details of the certificate
- Will eventually be a repository of all currently-valid SSL certificates.



Certificate Transparency Search Tool

auburn.edu | Search | Include expired certificates | Include subdomains (partial match)

Copy Link to These Results

Export to Excel | Export to CSV

Issuer Name ×

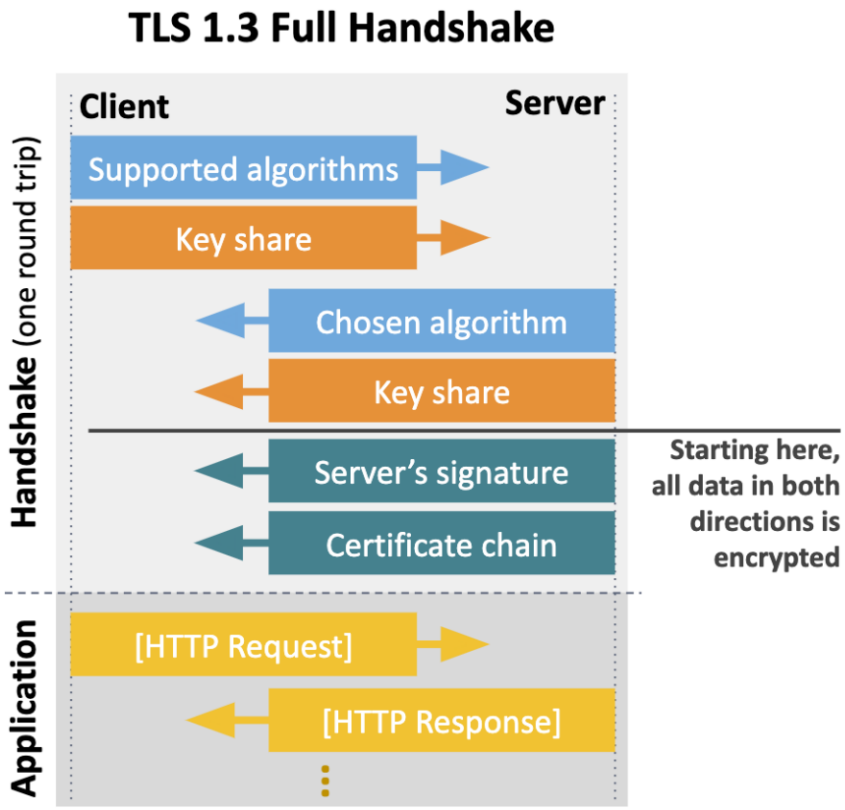
Issuer Name	Serial Num…	Subject CN	Valid F…	Valid To	Validat…	Signing Algori…	Key	Link
COMODO CA Limited (4)								
COMODO CA Limited	a7fd44fd38c48f1…	ssl712430.cloudflaressl.c…	2019-09-08	2020-03-16	non-EV	SHA-256	RSA-2048	Copy Link
COMODO CA Limited	beeeabf7d734fa…	ssl712431.cloudflaressl.c…	2019-09-08	2020-03-16	non-EV	ecdsa-with-Sha256	EC-256	Copy Link
COMODO CA Limited	a7fd44fd38c48f1…	ssl712430.cloudflaressl.c…	2019-09-08	2020-03-16	non-EV	SHA-256	RSA-2048	Copy Link
COMODO CA Limited	beeeabf7d734fa…	ssl712431.cloudflaressl.c…	2019-09-08	2020-03-16	non-EV	ecdsa-with-Sha256	EC-256	Copy Link
Internet2 (1)								
Internet2	31aae6e133d16…	auburn.edu	2017-04-18	2020-04-17	non-EV	SHA-256	RSA-2048	Copy Link

Computer and Network Security

Lecture 22: Other Security Protocols

COMP-5370/6370
Fall 2025

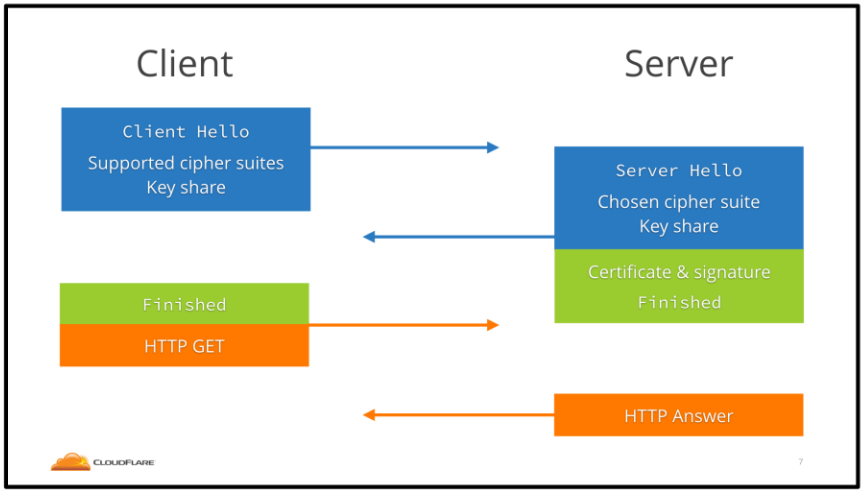
TLS 1.3

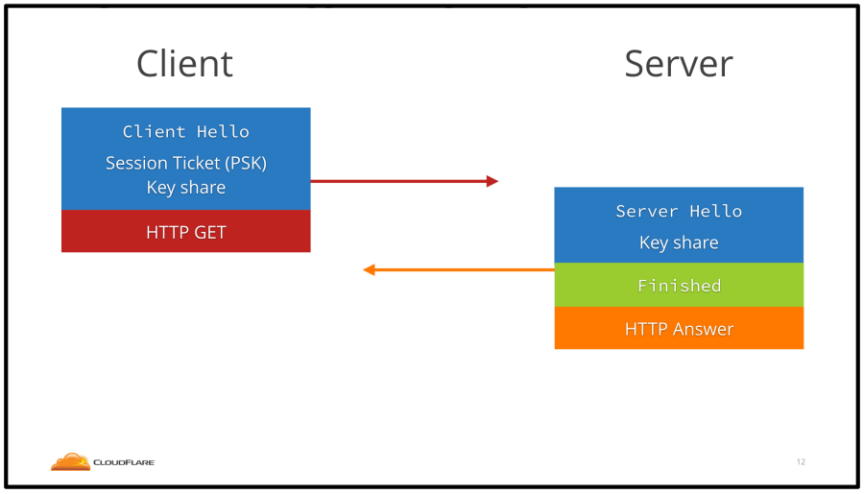


- Single round-trip required for full connection
  - ~100ms latency
- May require additional due to optimistic contents

TLS 1.3 (Early Data)

- TLS 1.3 can send an HTTP request in the first message
  - “early data”
  - “0RTT request”
- Request is protected by previous session’s key material
- Can (but shouldn’t) be processed immediately





https://blog.cloudflare.com/tls-1-3-overview-and-q-and-a/

QUIC

The **QUIC ("quick")** protocol is a UDP-based alternative to TLS designed by Google for experimenting with new ideas.

- Similar to TLS but some major changes
- Heavily contributed to features and structure of HTTP/2 and TLSv1.3
- HTTP/3 uses QUIC instead of TLS
  - Standardized in June 2023 (RFC 9114)

SSH

The **Secure Shell (SSH)** protocol is a widely-used secure channel optimized for terminal-access and administration.

- Significantly different approach from TLS
- Mandatory bi-directional authentication
- PKI-style authentication exists but rarely used
  - Does **NOT** use the same root CAs as TLS
- Almost always Trust on First Use (TOFU) authentication

Trust On First Use

Trust On First Use (TOFU) is an alternative solution to the key-distribution problem where keys are “pinned” after initial connection.

- Similar to HSTS in security trade-offs
  - Assume the very-first connection is safe
  - As long as key doesn’t change, not MitM
- Can be used in almost any protocol but mostly limited to SSH

TLS vs. SSH

TLS

- Client rarely authenticated
- Almost always PKI for auth (CAs + SSL certs)
- Lots of optimization for static(ish) content
- Large number of connections to large number of hosts
  - Minimal/Optimized setup

SSH

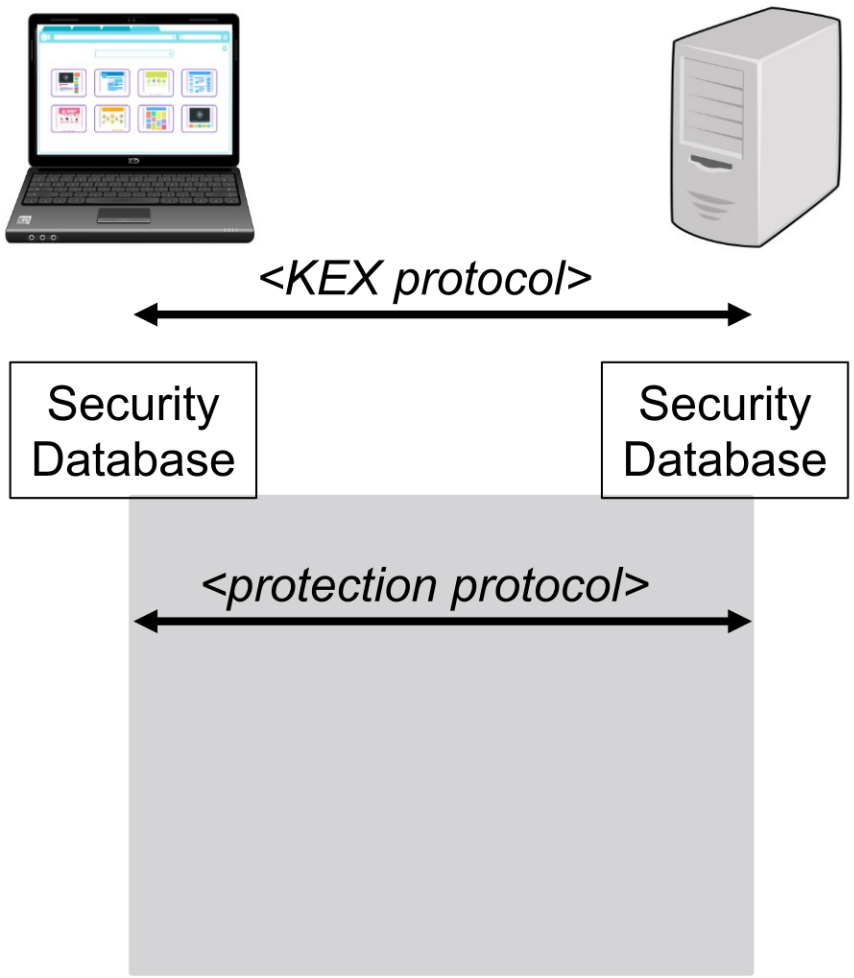
- Forced Bi-directional authentication
- Almost always auth via manual-config + TOFU
- Focused on real-time & bi-directional data
- Small number of connections to small number of hosts
  - Very verbose setup

VPNs

A **Virtual Private Network (VPN)** is a *logical* concept through which a remote client appears on the local network by use of a multiplexed secure channel.

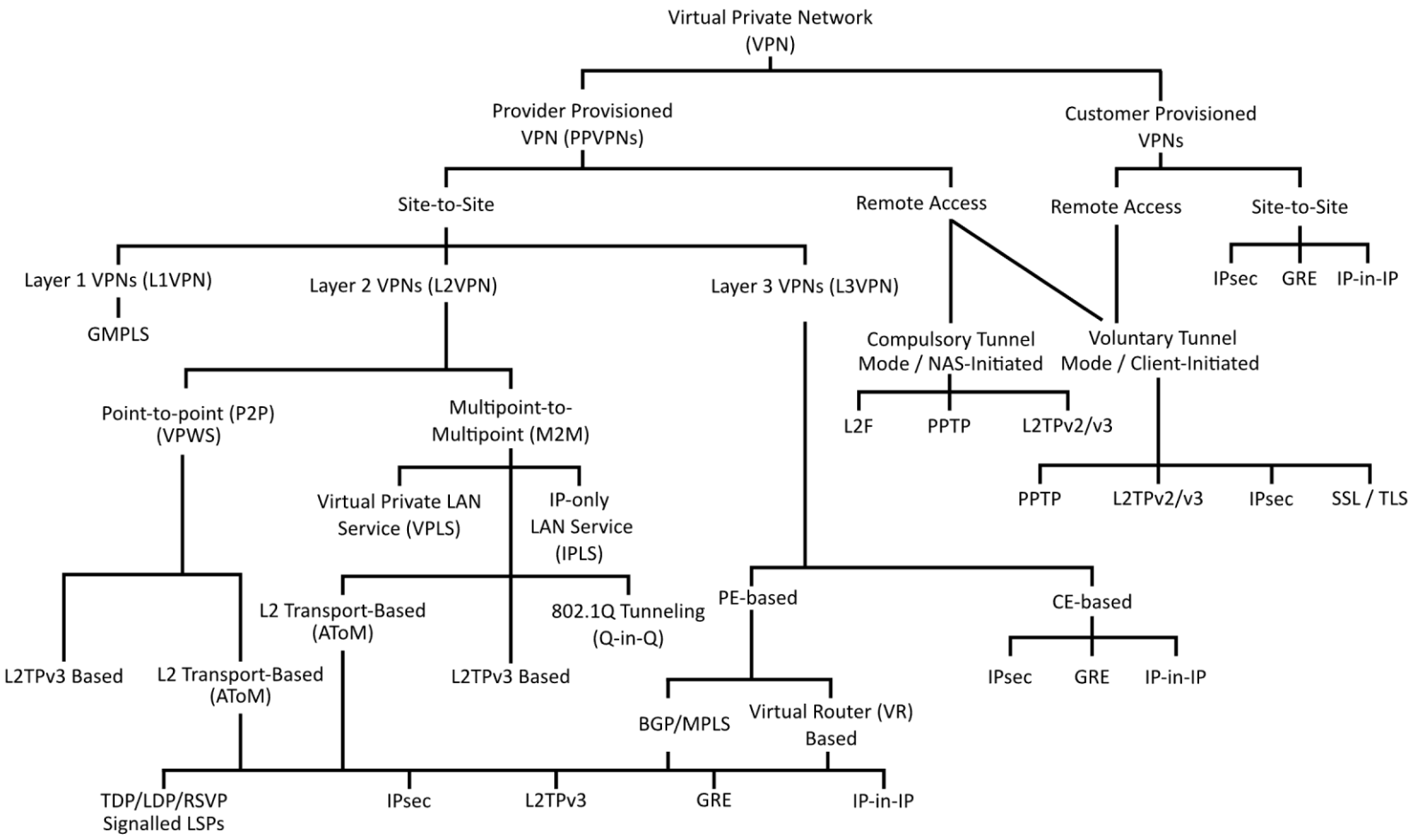
- Many different protocols can be used

Decoupled Design



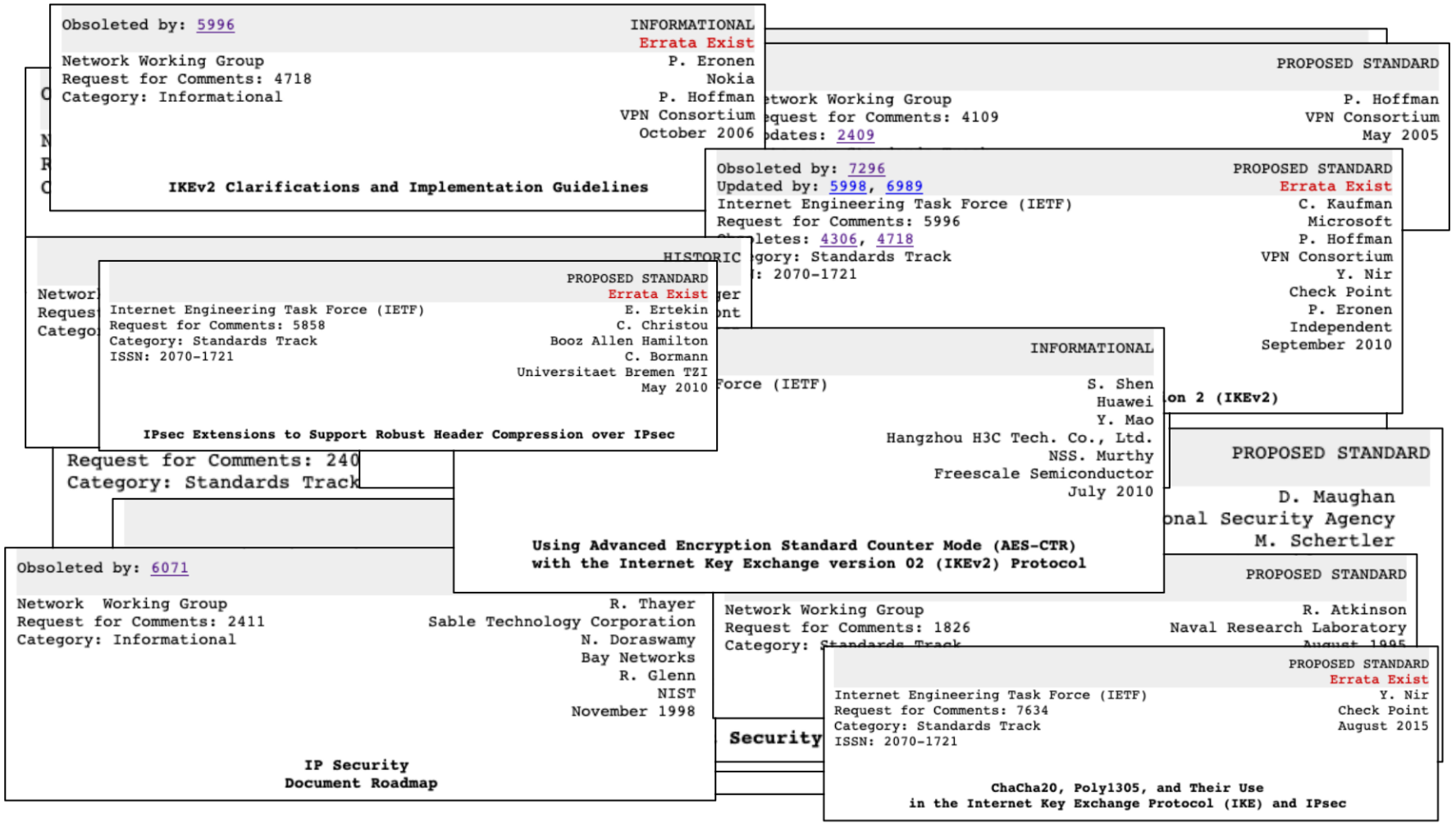
- Attempted to explicitly decouple responsibilities
- Can mix-and-match protocols for needs
  - Think of as a “security protocol stack”
- Revolves around ”Security Associations”

Types of VPNs



VPN Specifications

VPN Specifications



Obsoleted by: 5996 — INFORMATIONAL, Errata Exist
Network Working Group — P. Eronen, Nokia
Request for Comments: 4718 — P. Hoffman, VPN Consortium
Category: Informational — October 2006
IKEv2 Clarifications and Implementation Guidelines

PROPOSED STANDARD
P. Hoffman, VPN Consortium, May 2005

Obsoleted by: 7296
Updated by: 5998, 6989
PROPOSED STANDARD, Errata Exist
Internet Engineering Task Force (IETF) — C. Kaufman, Microsoft
Request for Comments: 5996 — P. Hoffman, VPN Consortium
Obsoletes: 4306, 4718 — Y. Nir, Check Point
Category: Standards Track — P. Eronen, Independent
ISSN: 2070-1721 — September 2010

PROPOSED STANDARD, Errata Exist
Internet Engineering Task Force (IETF) — E. Ertekin, C. Christou, Booz Allen Hamilton, C. Bormann, Universitaet Bremen TZI
Request for Comments: 5858 — May 2010
Category: Standards Track
ISSN: 2070-1721
IPsec Extensions to Support Robust Header Compression over IPsec

INFORMATIONAL
S. Shen, Huawei
Y. Mao, Hangzhou H3C Tech. Co., Ltd.
NSS. Murthy, Freescale Semiconductor
July 2010
Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol

PROPOSED STANDARD
D. Maughan
M. Schertler

Obsoleted by: 6071
Network Working Group — R. Thayer, Sable Technology Corporation
Request for Comments: 2411 — N. Doraswamy, Bay Networks
Category: Informational — R. Glenn, NIST
November 1998
IP Security Document Roadmap

PROPOSED STANDARD
Network Working Group — R. Atkinson, Naval Research Laboratory
Request for Comments: 1826

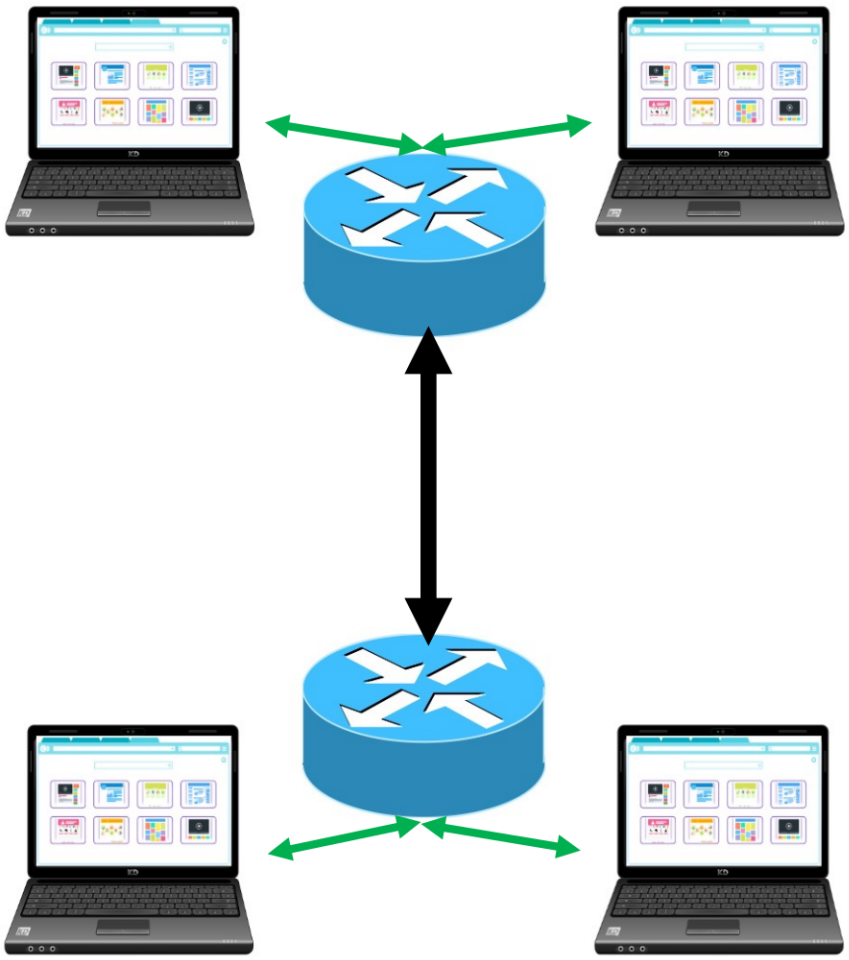
PROPOSED STANDARD, Errata Exist
Internet Engineering Task Force (IETF) — Y. Nir, Check Point
Request for Comments: 7634 — August 2015
Category: Standards Track
ISSN: 2070-1721
ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec

VPNs

A **Virtual Private Network (VPN)** is a *logical* concept through which a remote client appears on the local network by use of a multiplexed secure channel.

- Many different protocols can be used
- IKE+IPSec is a common implementation
- Can connect two remote-networks as 1

Site-to-Site VPN



- VPN is handled by network nodes
  - *"A long ethernet cable"*
- Clients are unaware of its existence due to being handled by network infrastructure

VPNs

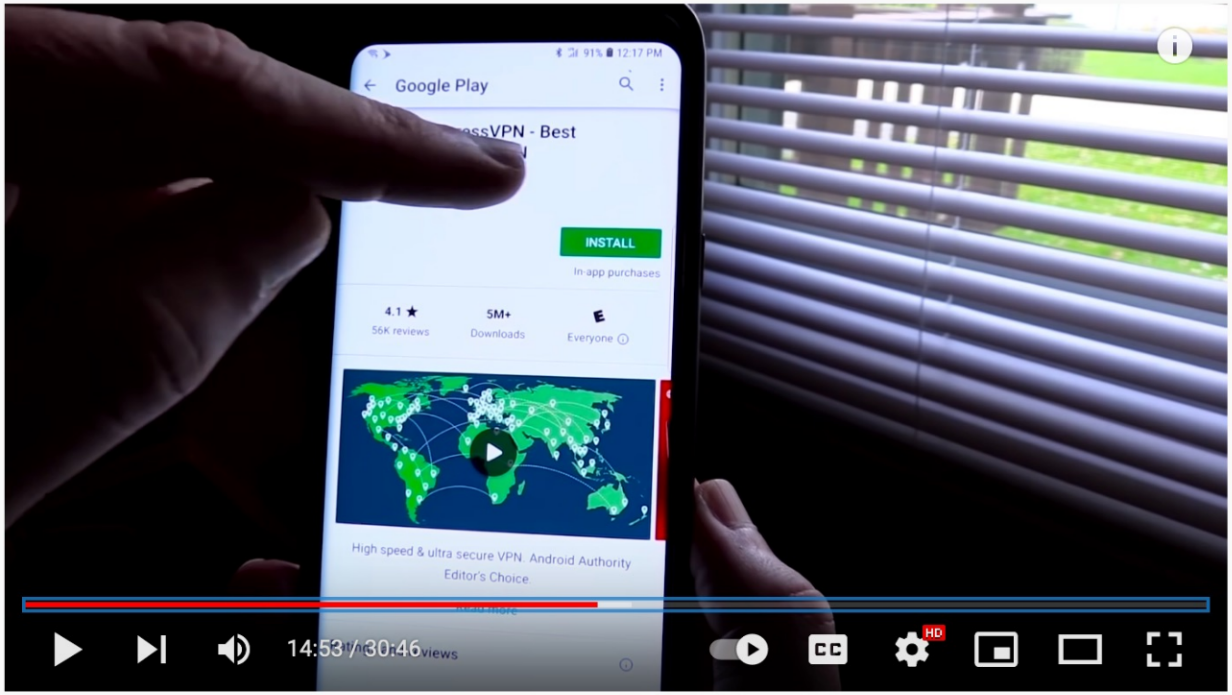
A **Virtual Private Network (VPN)** is a *logical* concept through which a remote client appears on the local network by use of a multiplexed secure channel.

- Many different protocols can be used
- IKE+IPSec is a common implementation
- Can connect two remote-networks as 1
- Can be used on a client-server construction

YouTube

Search

SIGN IN



Nostalgia Critic S12 • E29

The Lion King - Nostalgia Critic

1,708,198 views • Jul 17, 2019

43K 3.2K SHARE SAVE ...

Channel Awesome

1.27M subscribers

SUBSCRIBE

Go to https://expressvpn.com/nostalgiacritic, to take back your Internet privacy TODAY and find out how you can get 3 months free.

SHOW MORE

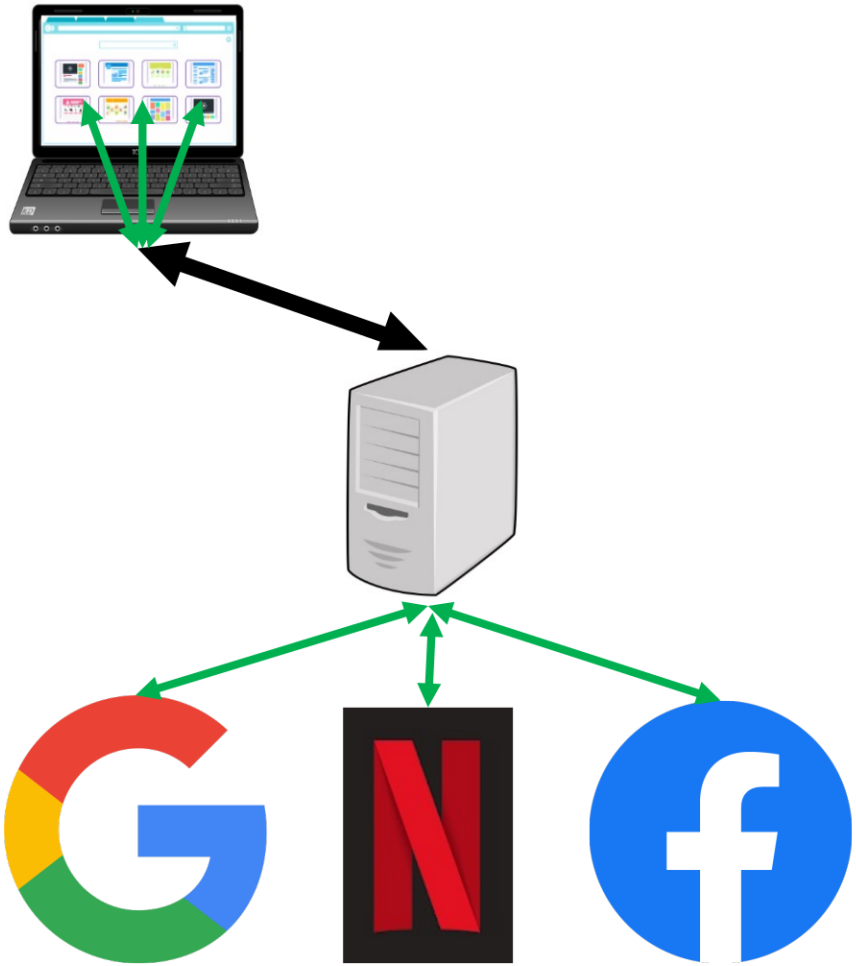
ExpressVPN

The best anon protection

ExpressVPN's core mission is to enab with the help of a VPN. We're not onl **transparent** about the information w **connection logs**. And we invite inde and technology.

kward to ust

Remote-Access VPN



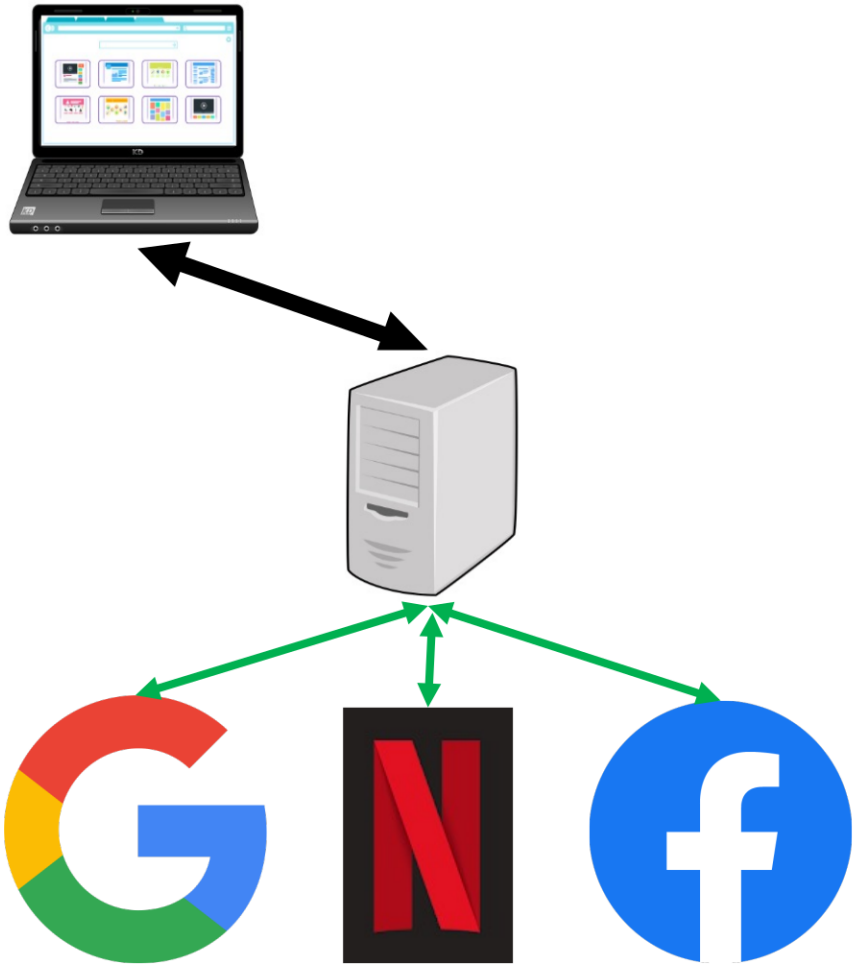
- The type you are normally accustomed to thinking about

What are VPN Trade-Offs?

What are the advantages and disadvantages of using a VPN?

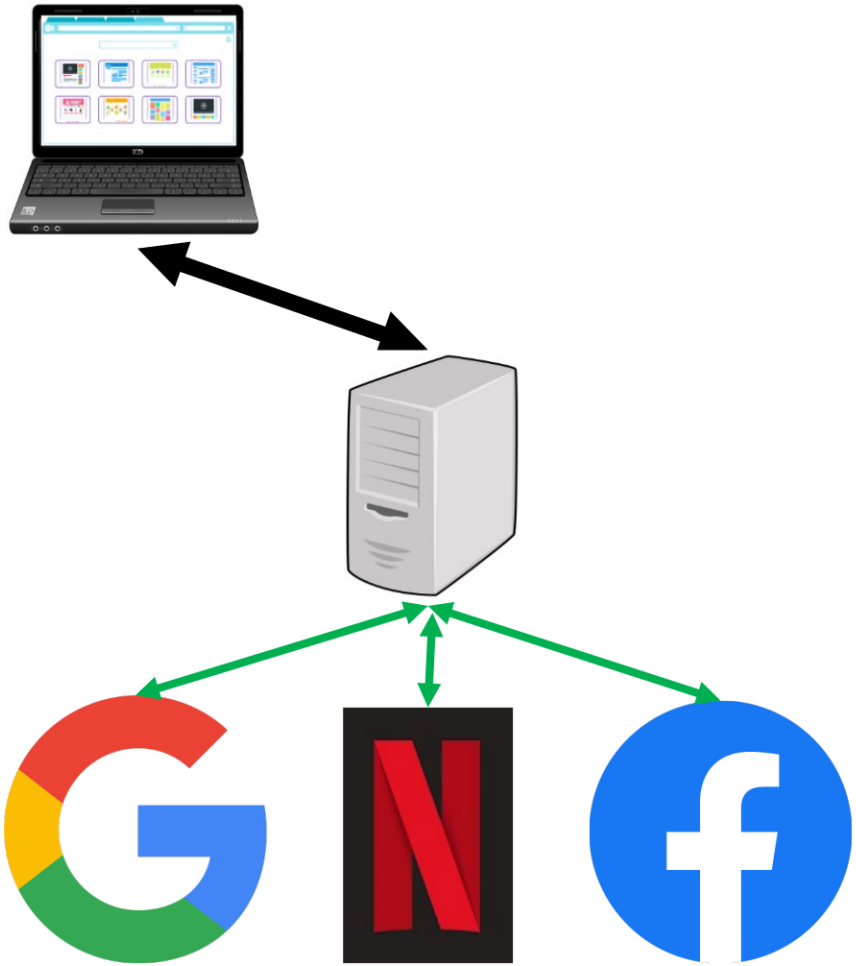
(discuss)

VPN Upsides



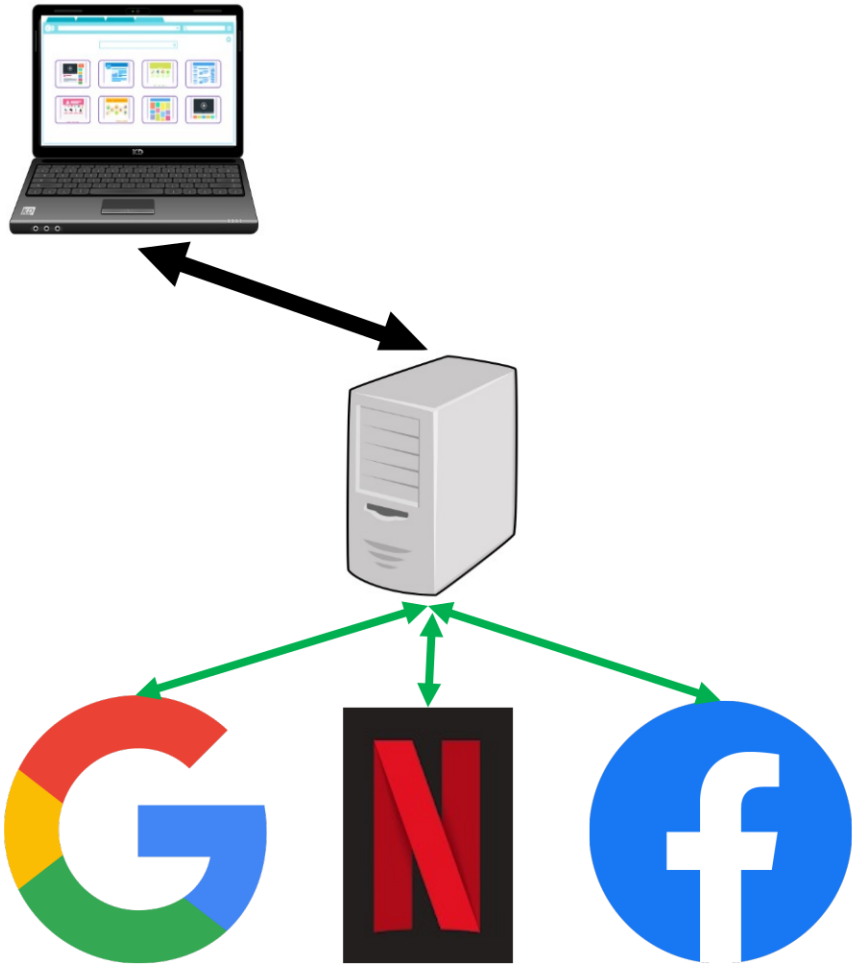
- Allow obfuscation of client's source
  - Source-ASN may leak identity
  - Hide the client's geolocation

VPN Upsides



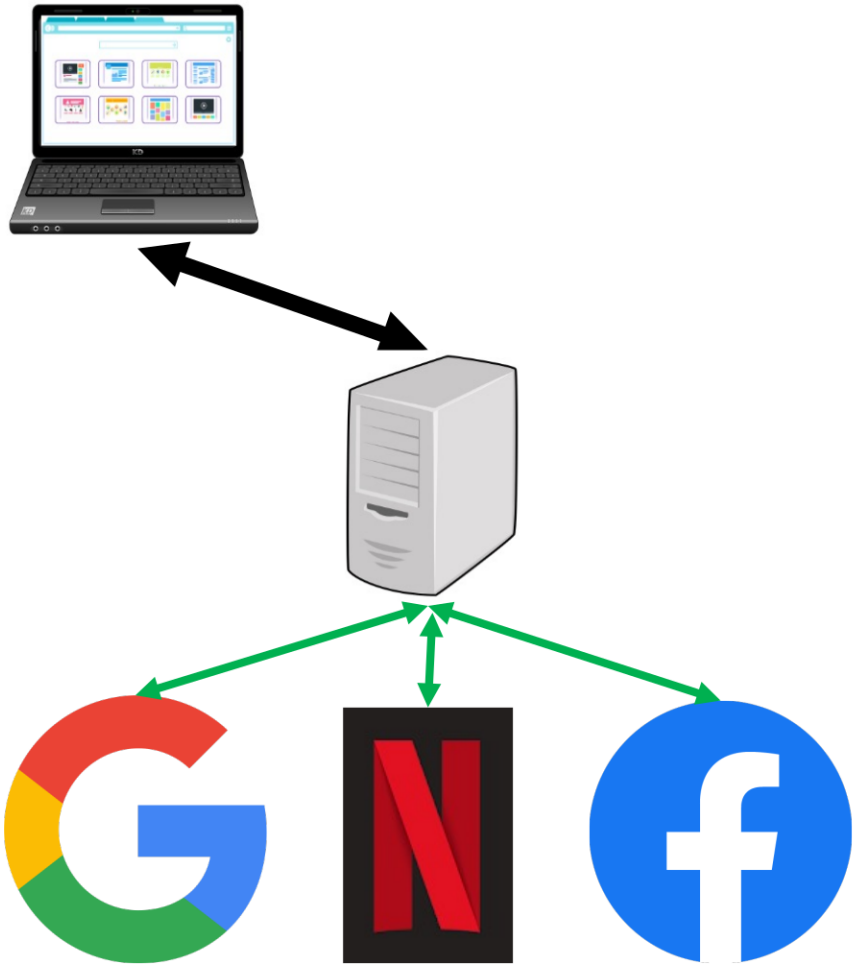
- Mixes client's traffic with all other users of VPN's traffic

VPN Upsides



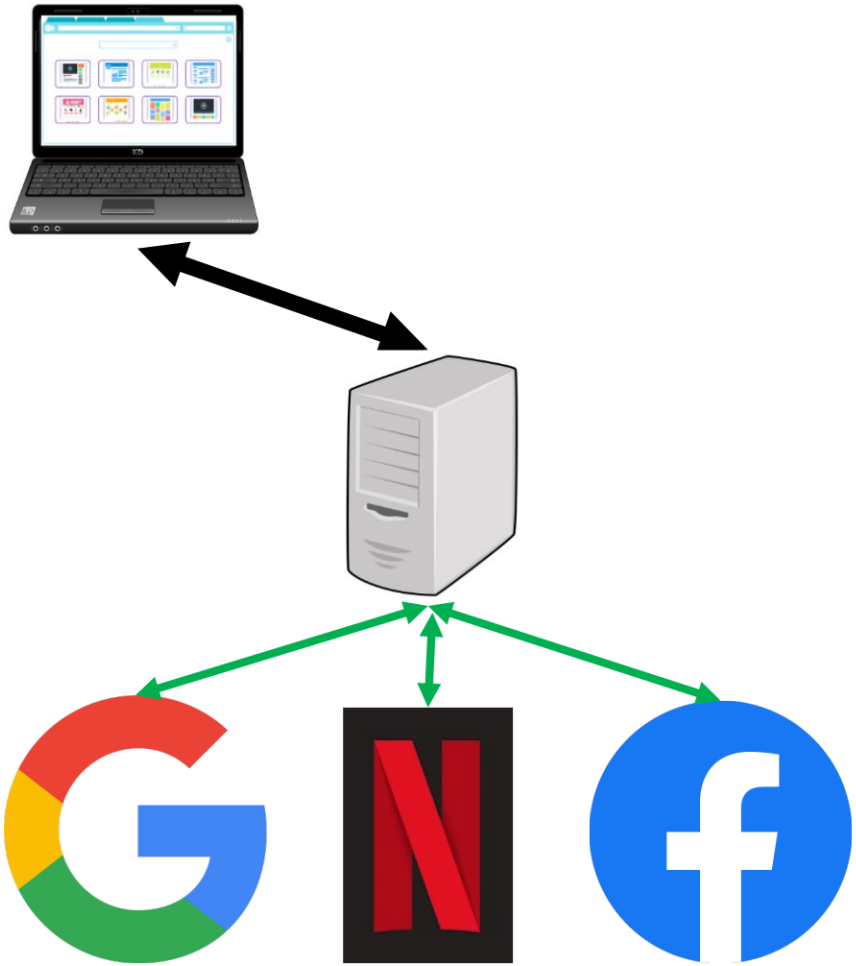
- Prevents client-side “last mile” network attacks
  - Wifi sniffing
  - ISP interference

VPN Downsides



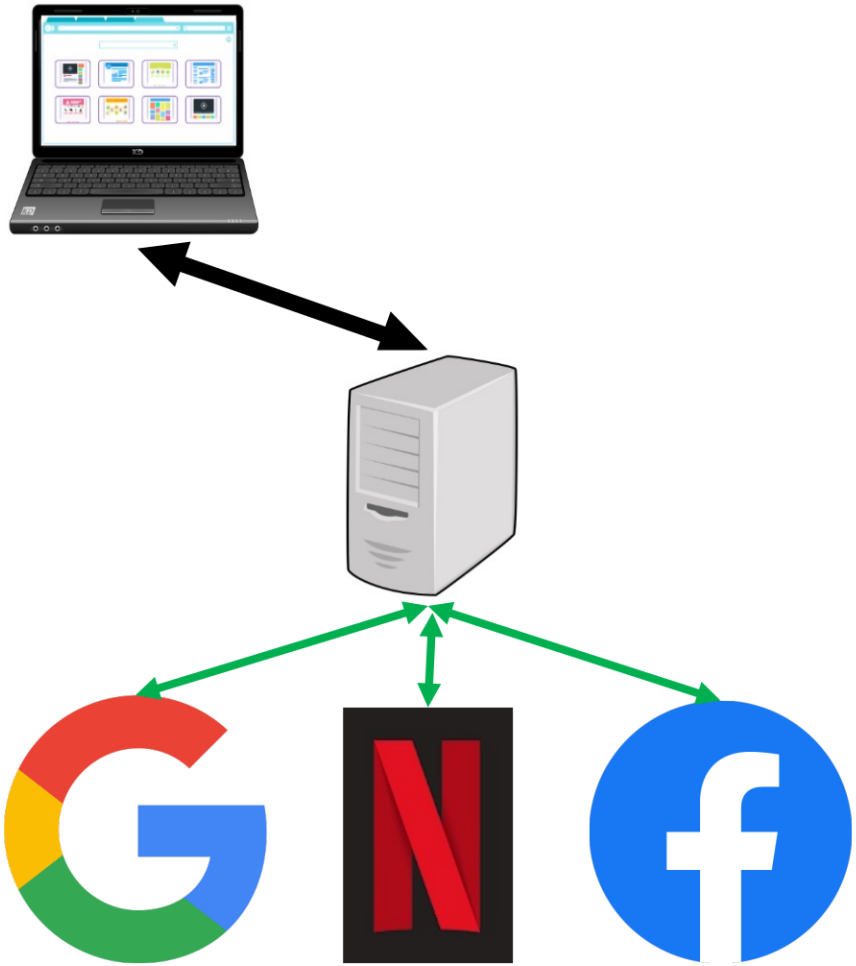
- Large amount of trust in VPN server
  - See all traffic
  - Can inject traffic

VPN Downsides



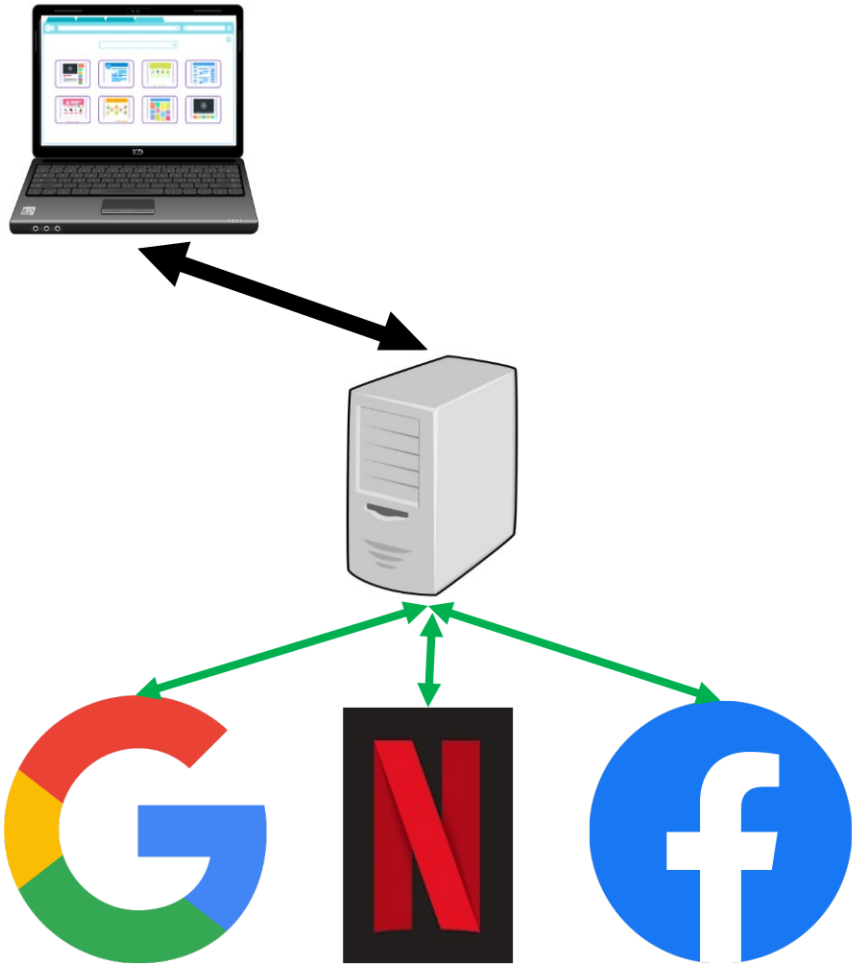
- Privacy properties are often **greatly** exaggerated

VPN Downsides



- Server-side network attacker can dox
- Server-side implementation can be *forced to* dox

VPN Downsides



BLEEPINGCOMPUTER

Home › News › Security › Cyberstalking Suspect Arrested After VPN Providers Shared Logs With the FBI

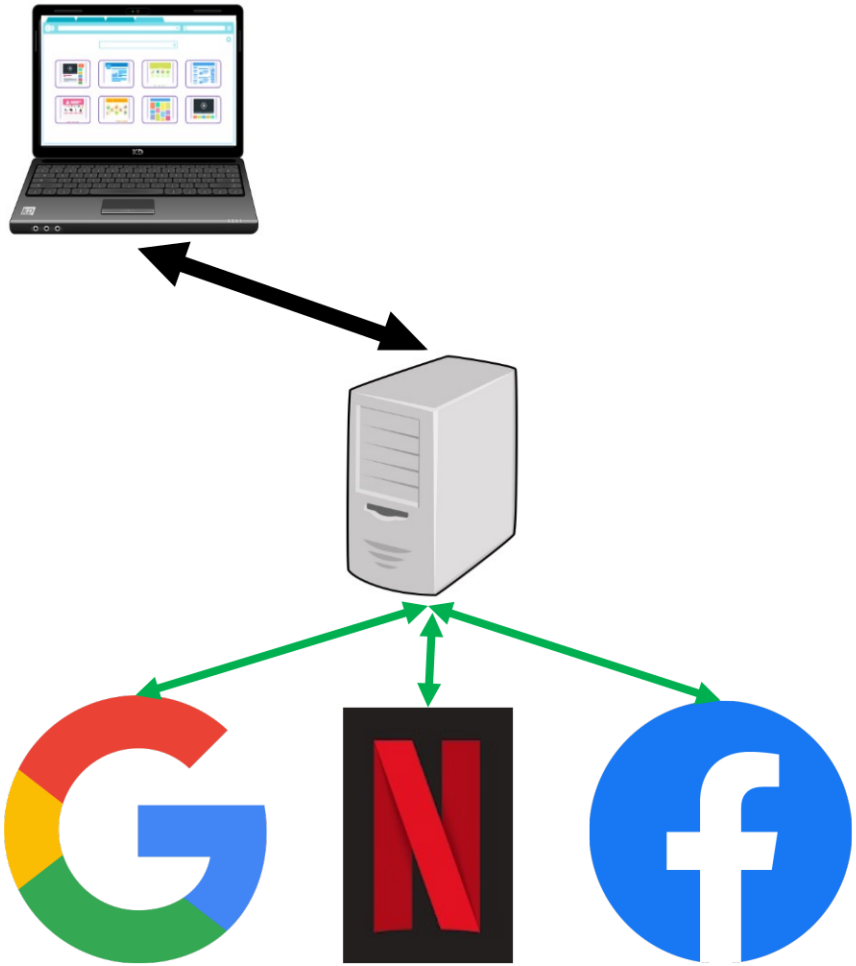
Cyberstalking Suspect Arrested After VPN Providers Shared Logs With the FBI

By Catalin Cimpanu

October 7, 2017 08:55 AM 10

VPN providers often advertise their products as a method of surfing the web anonymously, claiming they never store logs of user activity, but a recent criminal case shows that at least some, do store user activity logs.

VPN Downsides



malwarebytes LABS

Search Labs

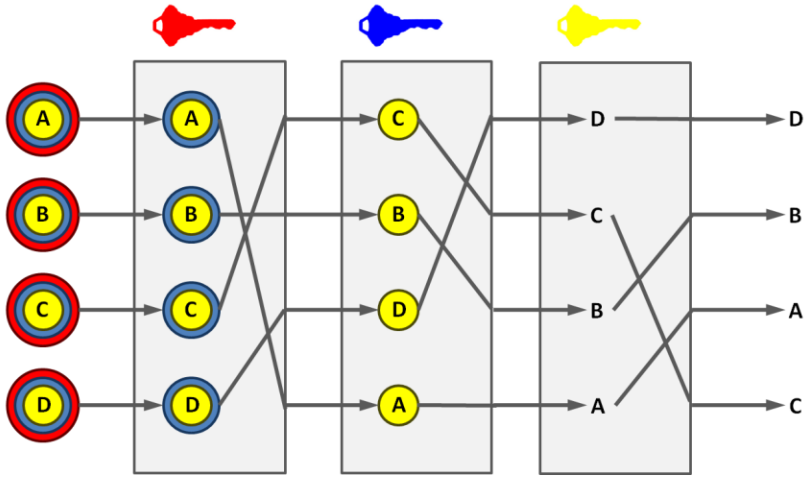
SUBSCRIBE

21 million free VPN users' data exposed

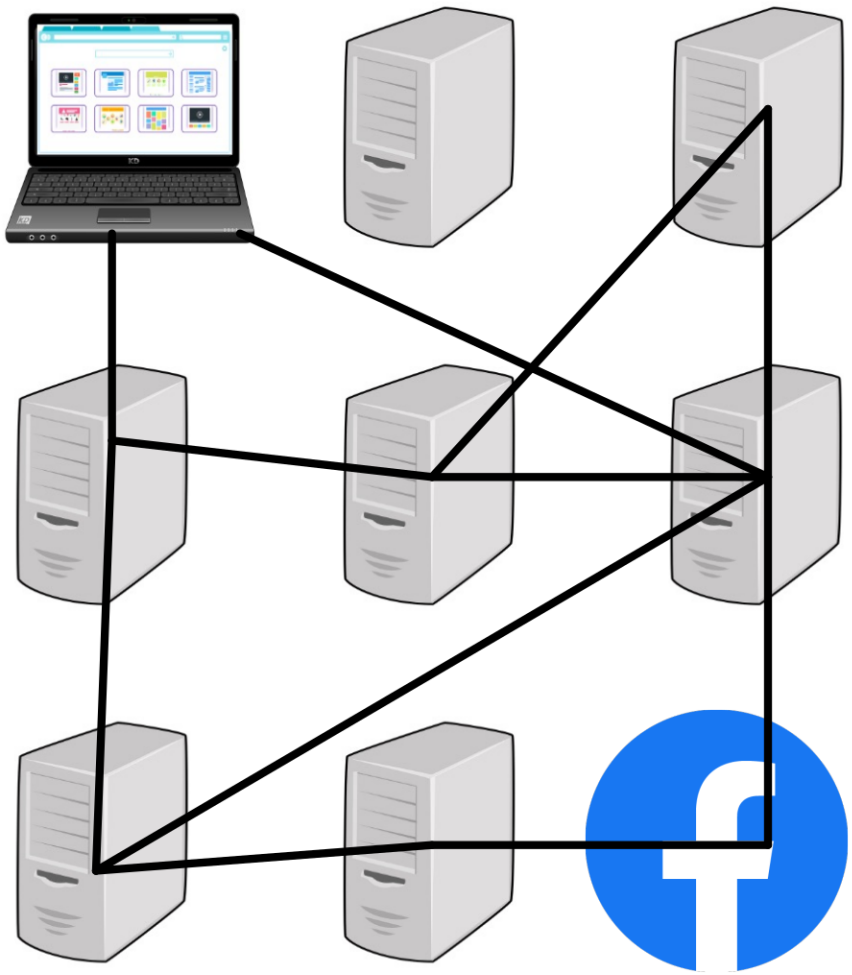
Posted: March 3, 2021 by David Ruiz
Last updated: March 5, 2021

Mix Networks

Mix Networks (Mix-Nets) are a type of high-latency anonymous network which relies on bounces among nodes with other messages for protections.

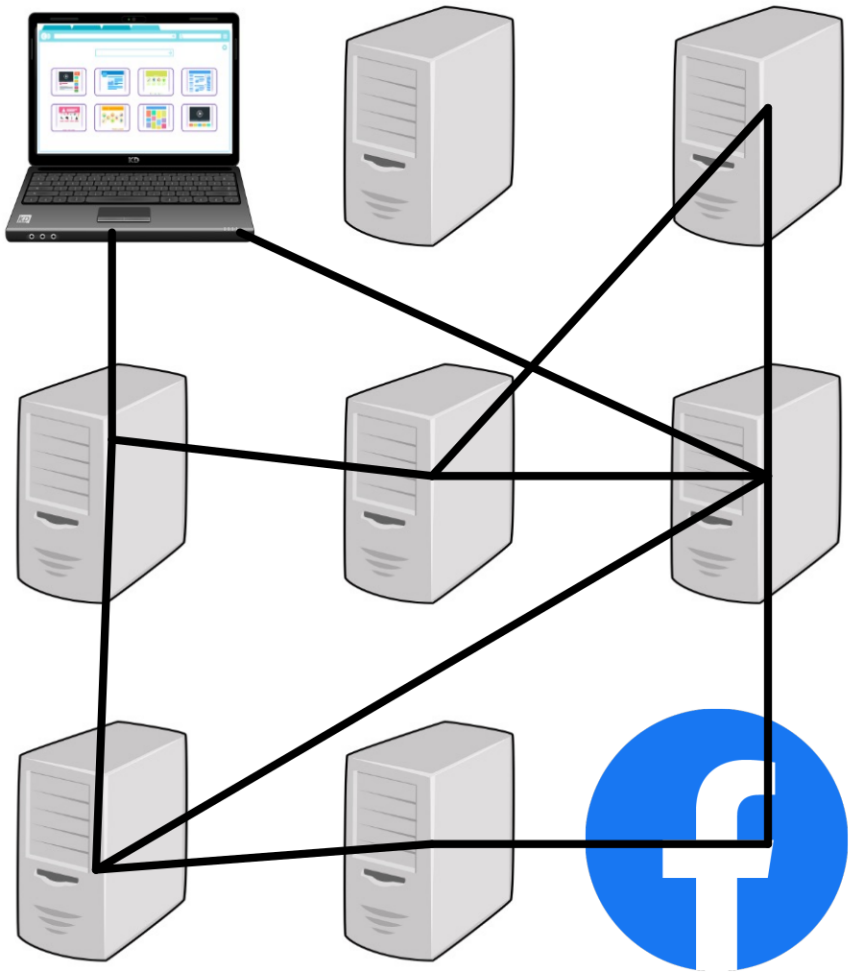


Mix-Nets



- Client sends message to network
- Nodes delay random amount of time
- Nodes sends random selection of nodes
- Repeat

Mix-Net Downsides



- Extremely Slow
- Require large networks and high through-put
- Non-linear scaling

Computer and Network Security

Lecture 22: TLS / Protocols

COMP-5370/6370
Fall 2025