

PASCAL GLOOR

THE DAY WE'VE BEEN HACKED

ABOUT ME

- ▶ Principal Network & Systems Architect
- ▶ 20+ years experience
- ▶ Work for Quickline, 2nd largest cable operator in CH

THIS PRESENTATION _IS_ ABOUT

- ▶ tech stuff
- ▶ legal stuff
- ▶ humans

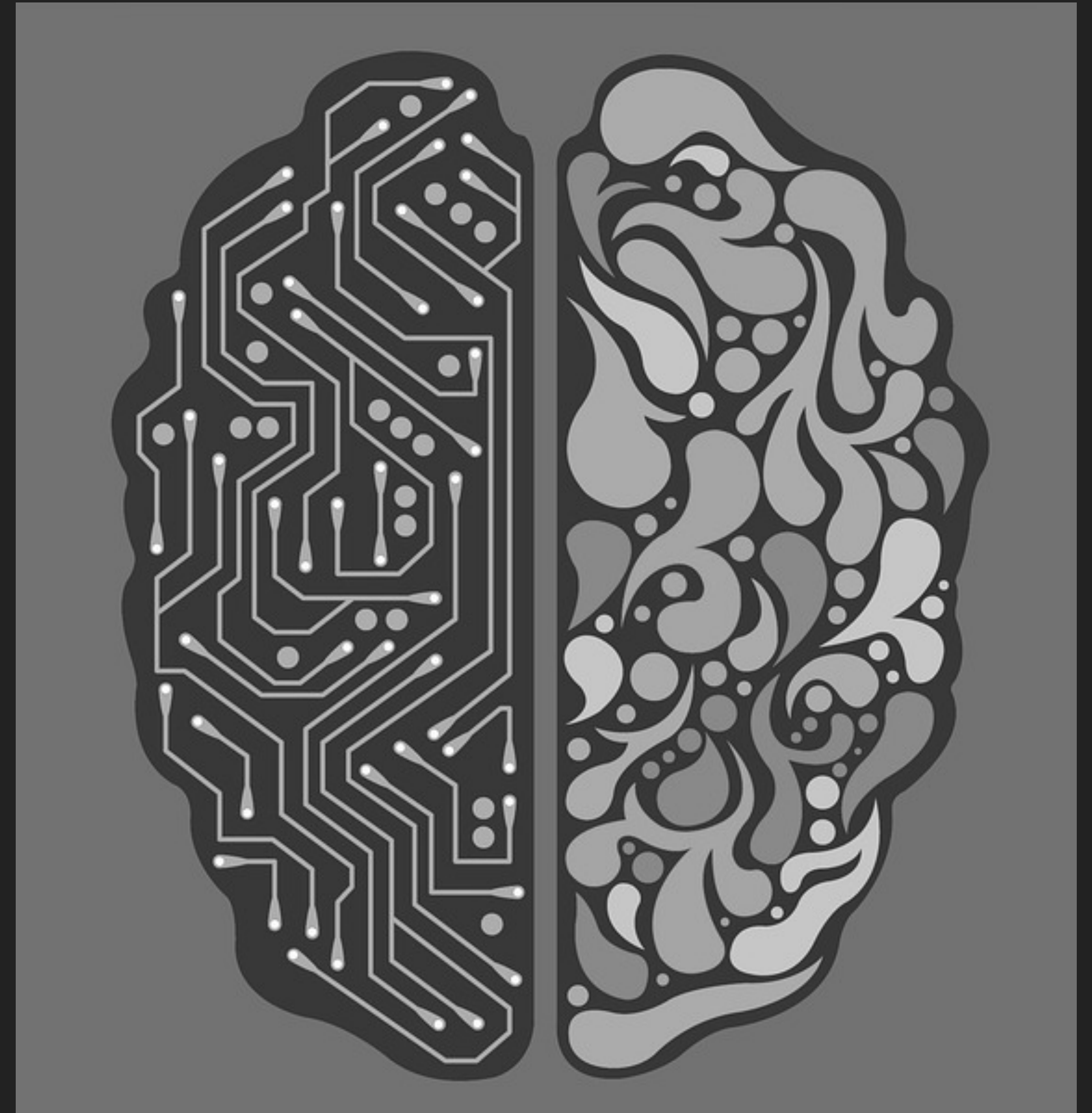
THIS PRESENTATION **_IS NOT_** ABOUT

~~BLOCKCHAIN~~



THIS PRESENTATION **_IS NOT_** ABOUT

~~Machine Learning~~



THIS PRESENTATION **_IS NOT_** ABOUT

~~GDPR~~

I can consult for 5000 CHF / day to put this on all your servers

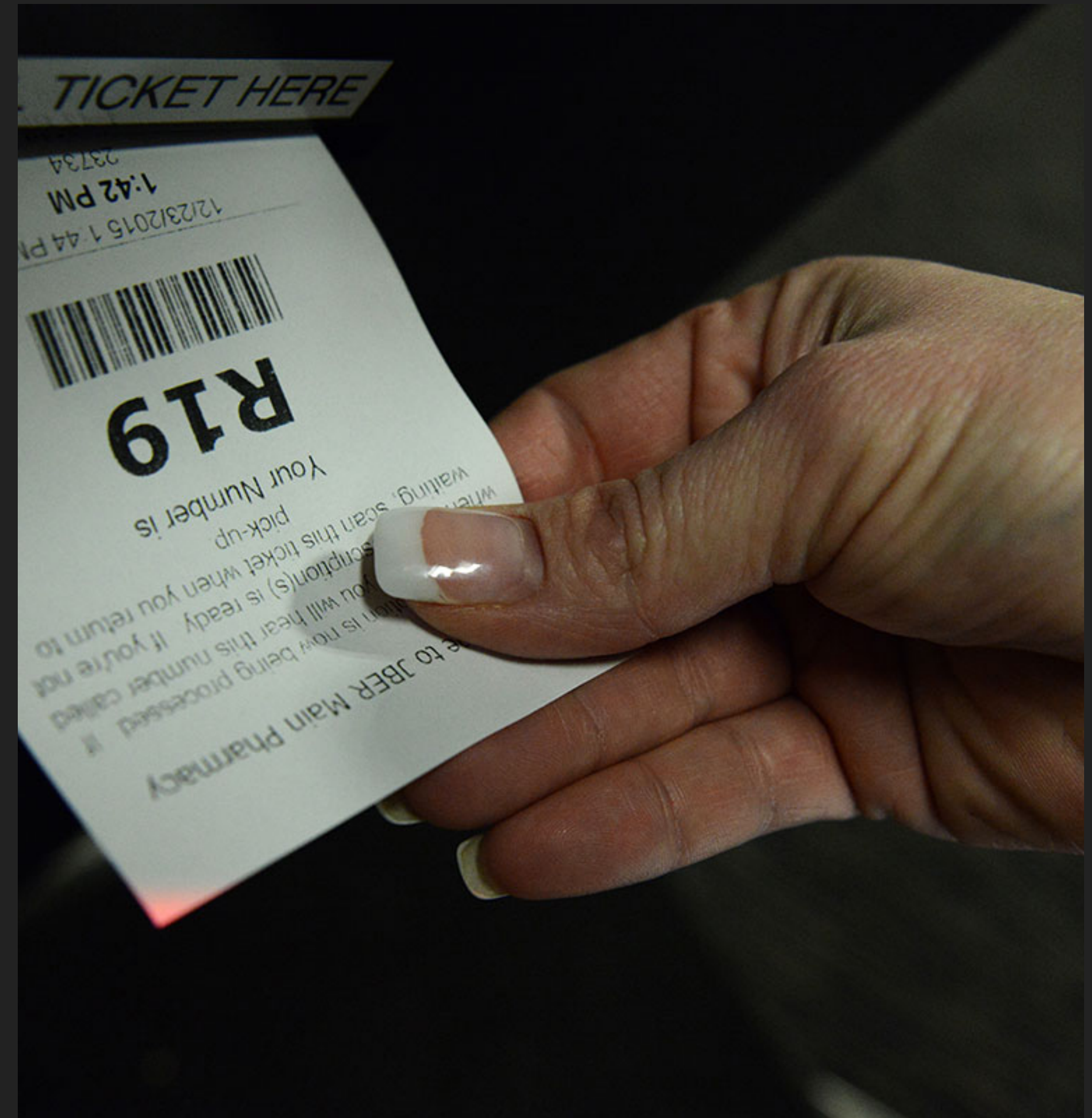
```
root@server:~#alias gdpr_compliant="rm -rf /; sync; halt;"
```


STORY

A stack of five old, worn books with visible spines and titles. The books are arranged vertically, with the top book having a dark cover and the bottom book having a light, textured cover. The spines show signs of age and wear, with some titles like 'CAPTAIN COOK' and 'VOL. 1' visible. The background is a dark, textured surface.

TICKETS

- ▶ ticket about rejected email
- ▶ and another one...
- ▶ and another one...
- ▶ ...

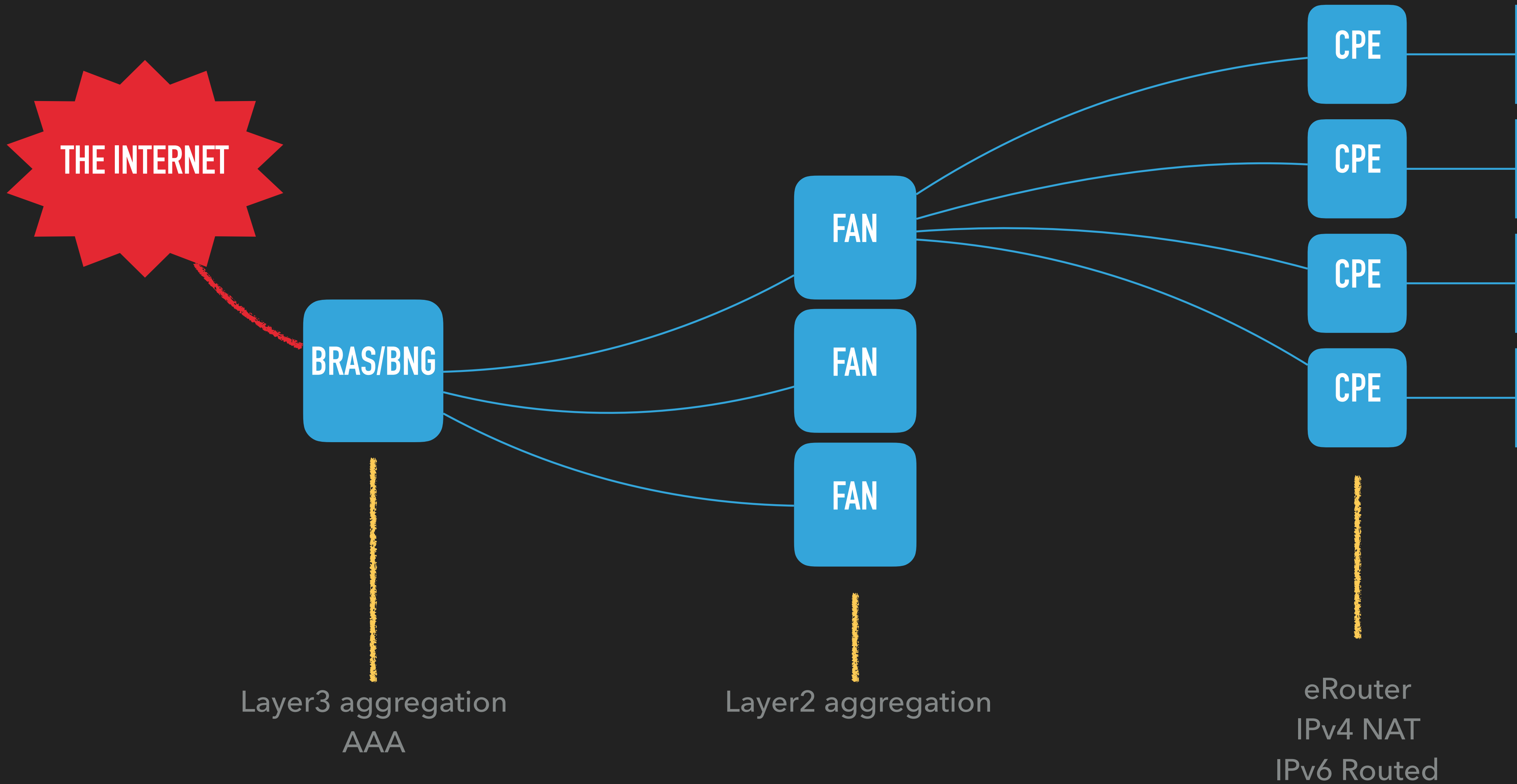


SWISSCOM

- ▶ blacklisted specific range
- ▶ discussion about details with Swisscom
- ▶ mass UCE/SPAM/SCAM email from a specific IP range



NETWORK TOPOLOGY



NETWORK TOPOLOGY

Huawei HG8247H



A dark silhouette of a person in profile, facing right, holding a magnifying glass up to their eye. The person is wearing a long-sleeved shirt and trousers. The background is a dark, solid color.

INVESTIGATION

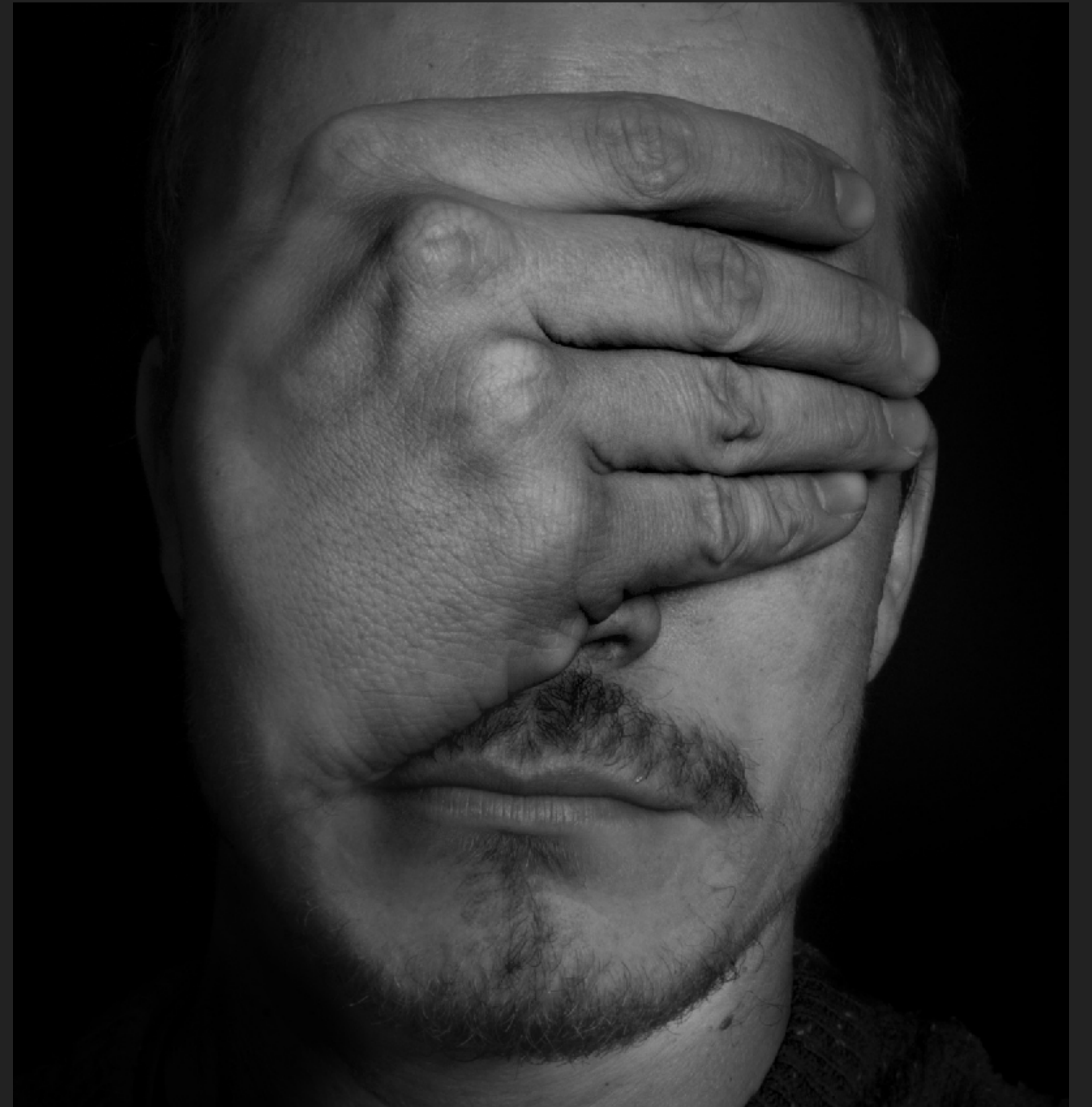
INVESTIGATING THE ORIGIN

- ▶ obviously not customer originated
- ▶ netflow
- ▶ direct tapping
- ▶ netstat-like on the CPE



ASSUMPTIONS

**Assumptions
will make you
blind!**



INVESTIGATING THE ORIGIN

SSH !



(POSSIBLY) PROPRIETARY IMPLEMENTATION

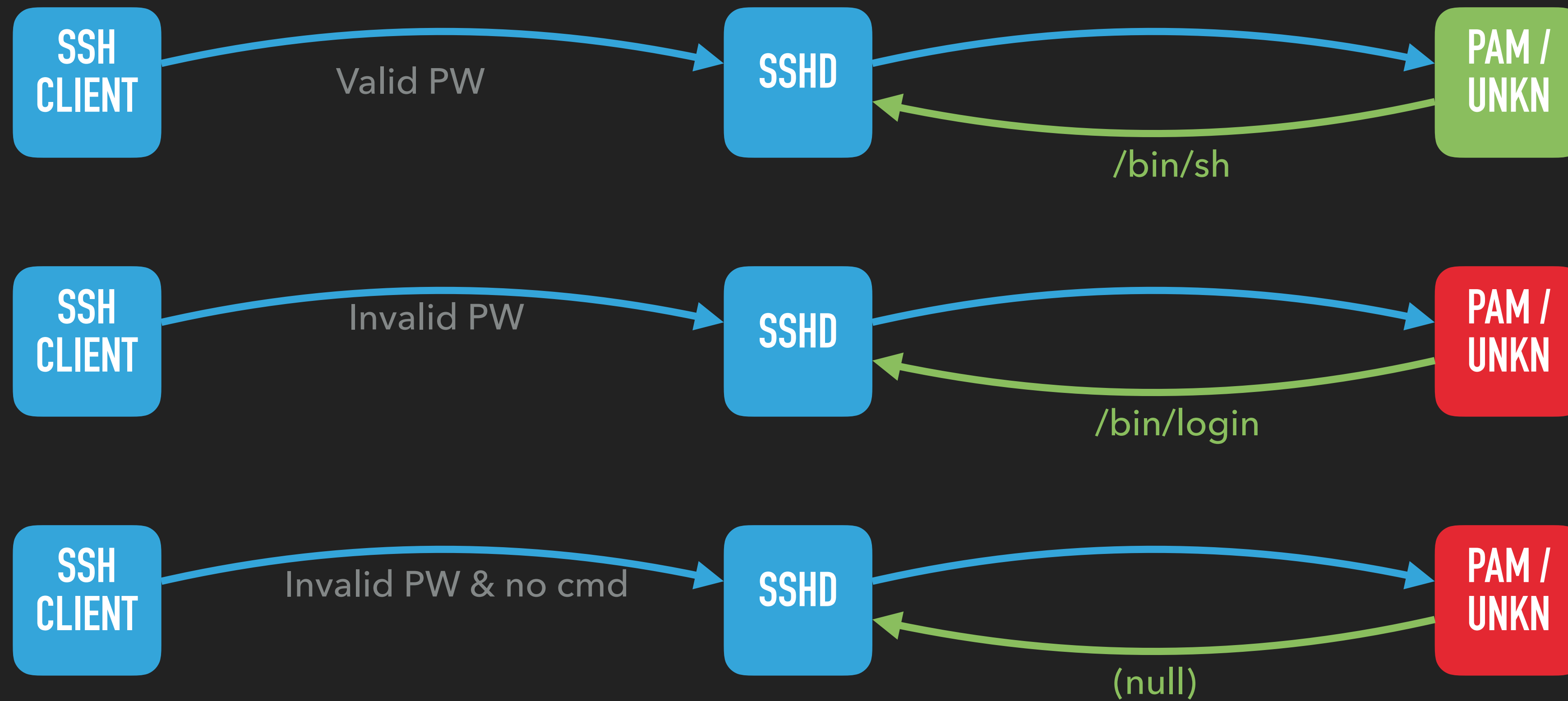
```
root@[REDACTED]:~# ssh root@[REDACTED]  
root@[REDACTED]'s password:  
  
User name or password is wrong, please try it again!  
Login:█
```


(POSSIBLY) PROPRIETARY IMPLEMENTATION

```
root@[REDACTED]:~# ssh -D 1080 -N root@[REDACTED]  
root@[REDACTED]'s password:
```

- ▶ -D [bind_address:]port
Specifies a local “dynamic” application-level port forwarding
- ▶ -N
Do not execute a remote command. This is useful for just forwarding ports

(POSSIBLY) PROPRIETARY IMPLEMENTATION



CAUSE

- ▶ SSH open to the world!
- ▶ Misunderstanding, unclear documentation
- ▶ Vendor said "Works as expected"



RESOLUTION

- ▶ Correction of the CPE settings



SOLVED

► Yaaaaayyy!!



LAWFUL INTERCEPT 🤮

- ▶ BÜPF / LSCPT - Federal Law for surveillance of Post and Telecommunications services
- ▶ 6 months of data retention for IP/timestamp to customer association

Der Bundesrat



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Der Bundesrat

Das Portal der Schweizer Regierung

Kontakt

Erweiterte Suche

DEFRITRMEN

Search

Bundesrat

Bundespräsidium

Departemente

Bundeskanzlei

Bundesrecht

Dokumentation

Startseite

Bundesrecht

Systematische Rechtsammlung

Landesrecht

7 Öffentliche Werke – Energie – Verkehr

78 Post- und Fernmeldeverkehr

780.1 Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Systematische Rechtsammlung

Landesrecht

1 Staat – Volk – Behörden

2 Privatrecht – Zivilrechtspflege – Vollstreckung

3 Strafrecht – Strafrechtspflege – Strafvollzug

4 Schule – Wissenschaft – Kultur

5 Landesverteidigung

6 Finanzen

7 Öffentliche Werke – Energie – Verkehr

780.1

alles einblenden

Artikelübersicht

alles ausblenden

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

vom 18. März 2016 (Stand am 1. März 2018)

Die Bundesversammlung der Schweizerischen Eidgenossenschaft, gestützt auf die Artikel 92 Absatz 1 und 123 Absatz 1 der Bundesverfassung¹, nach Einsicht in die Botschaft des Bundesrates vom 27. Februar 2013²,
beschliesst:

1. Abschnitt: Allgemeine Bestimmungen

Art. 1 Sachlicher Geltungsbereich

¹ Dieses Gesetz gilt für die Überwachung des Post- und Fernmeldeverkehrs, die angeordnet und durchgeführt wird:

Zusätzliche Informationen

Dieser Text ist in Kraft.

Abkürzung

BÜPF

Beschluss

18. März 2016

Inkrafttreten

1. März 2018

Quelle

AS 2018 117

Chronologie

Chronologie

Zitate

Zitate


Werkzeug

Sprachenvergleich

Alle Fassungen

LAWFUL INTERCEPT

- ▶ 6 months of data retention for IP/ timestamp to customer association



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesverwaltung admini

Überwachung Post- und Fernmeldeverkehr Ü

Startseite

CCIS 5.3.0 (a6aa, TSP1151)

Neue Suche

Abbrechen

Suchergebnis

Anfrage	Firma	Name	Vorname	Ort	Rufnummer	Mutiert	Benutzer	Status	
7917149	<input type="checkbox"/>					08.06.18 16:48		erledigt	Anzeigen
7915792	<input type="checkbox"/>					07.06.18 14:49		erledigt	Anzeigen
7915638	<input type="checkbox"/>					07.06.18 14:30		pendent bei StrafB	Anzeigen
7887628	<input type="checkbox"/>					18.05.18 08:04		erledigt	Anzeigen
7883585	<input type="checkbox"/>					14.05.18 15:46		erledigt	Anzeigen
7877188	<input type="checkbox"/>					07.05.18 13:56		erledigt	Anzeigen
7875029	<input type="checkbox"/>					04.05.18 12:55		erledigt	Anzeigen
7873248	<input type="checkbox"/>					03.05.18 12:29		erledigt	Anzeigen

LAWFUL INTERCEPT

- ▶ Massive requests for LEA (ÜPF) in the following months
- ▶ Unsuccessful arrangement with MELANI & ÜPF
- ▶ Comment all request explaining the unlikelihood that the customer was responsible



success Ln

Failure Dr

LESSONS LEARNED

TECH LESSONS

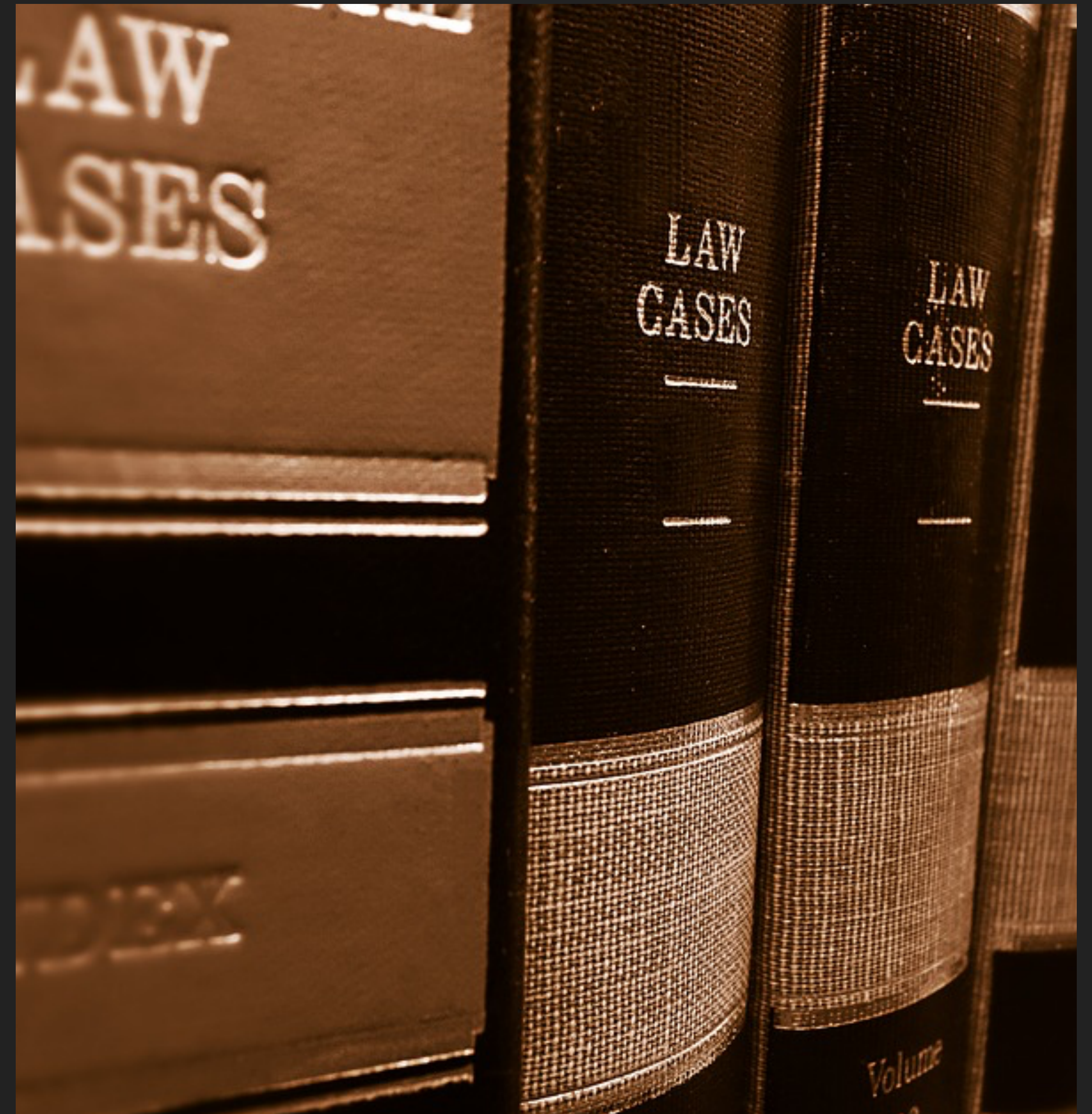
- ▶ DO NOT DEPLOY IN A HURRY !
- ▶ Quick portscan with different CPE configs



LEGAL LESSONS

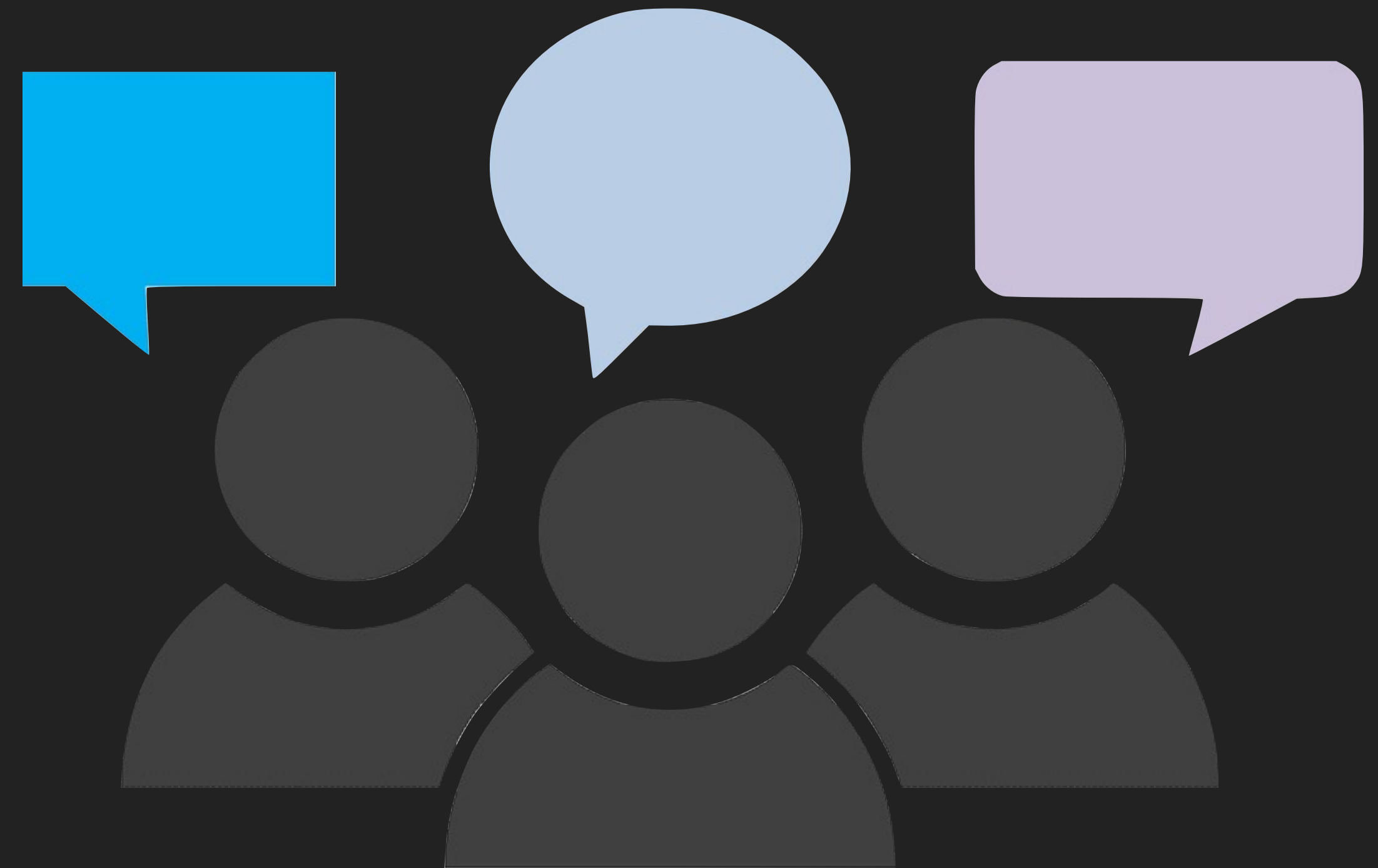
```
if ( true_positive > 0 ) {  
    process_request();  
} else {  
    reject();  
    messy_legal_case();  
}
```

translated quote by Prof. Dr.
Simon Schlauri



PLAN BREACHES

- ▶ inform the public (website, press release)
- ▶ inform the affected customers!



QUESTIONS?

PASCAL GLOOR @SPALET75

THANK YOU