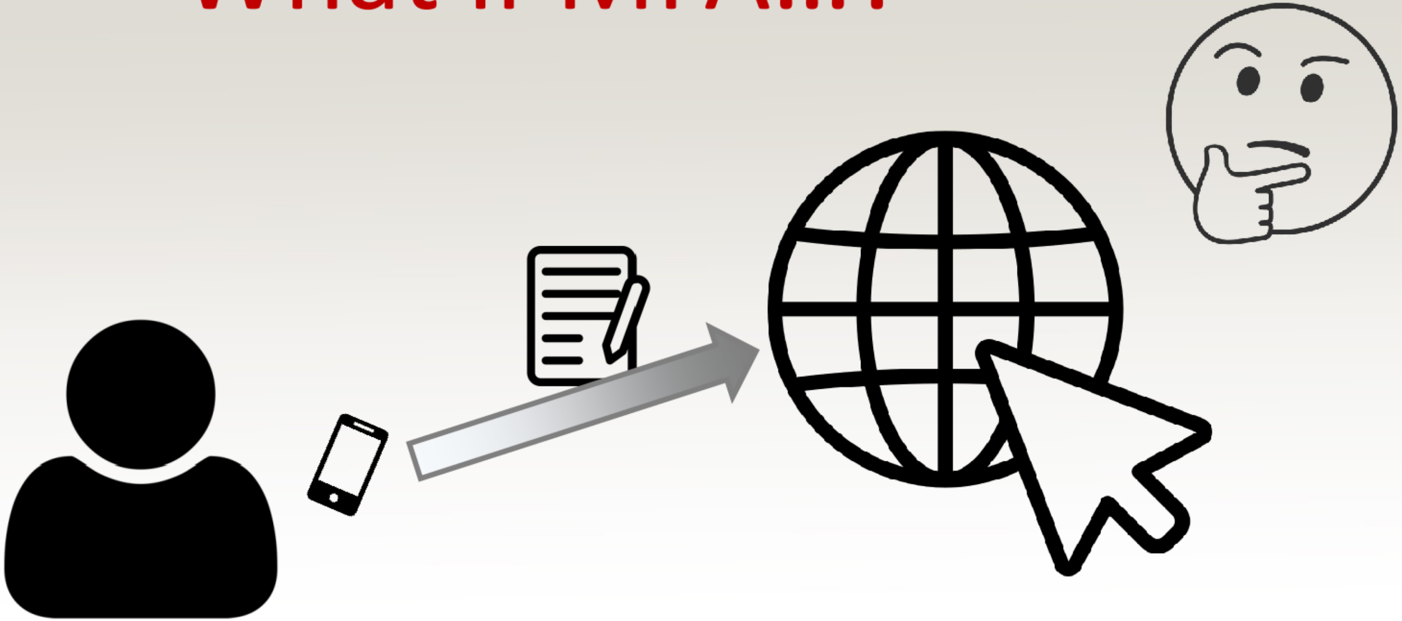
Beyond Classical MFA: Reinforcing Systems in an Evolving Digital Landscape

Swiss Cyber Storm
24th October 2023

Mauro Verderosa

What if MFA…?



Intro

Cyberattacks during latest 12 months

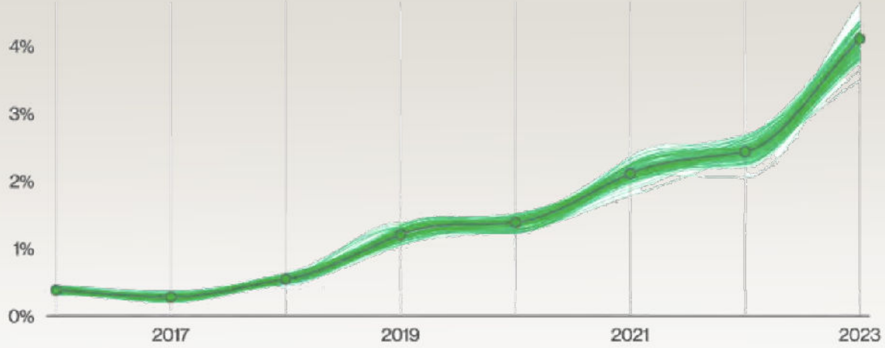
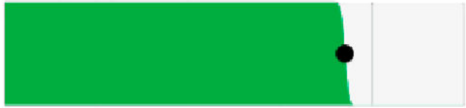
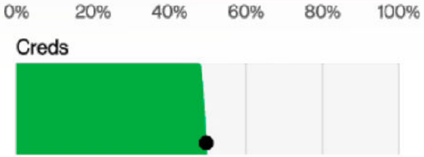


Figure 5. Pretexting incidents over time

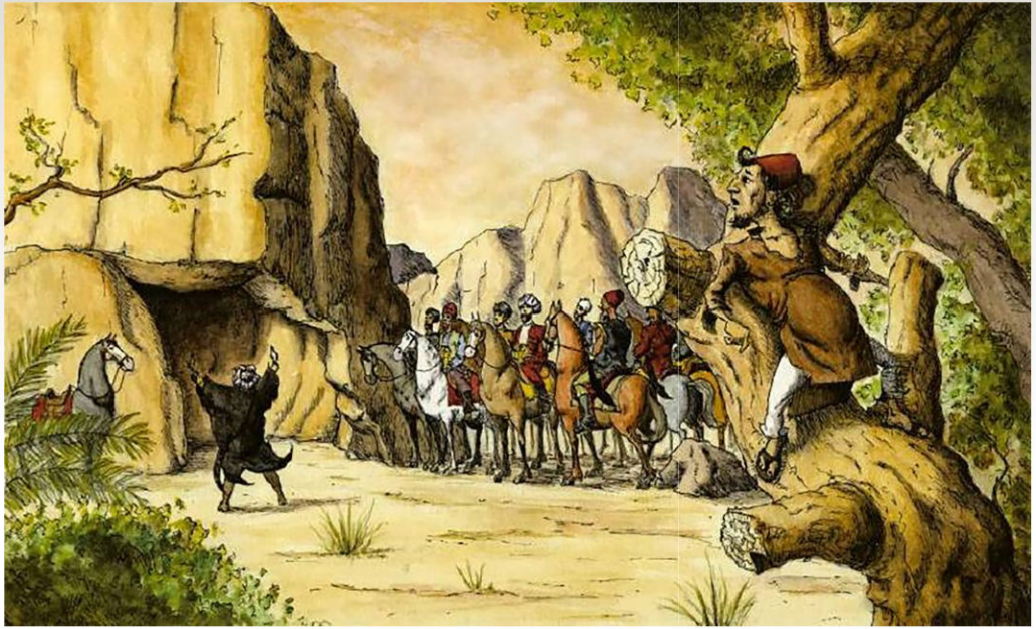
74% of breaches involved a human element (n=4,482)





Verizon 2023 Data Breach Investigations Report

The Human Factor



MFA alone is insufficient

Mauro Verderosa

Cybersecurity Specialist and IAM Expert

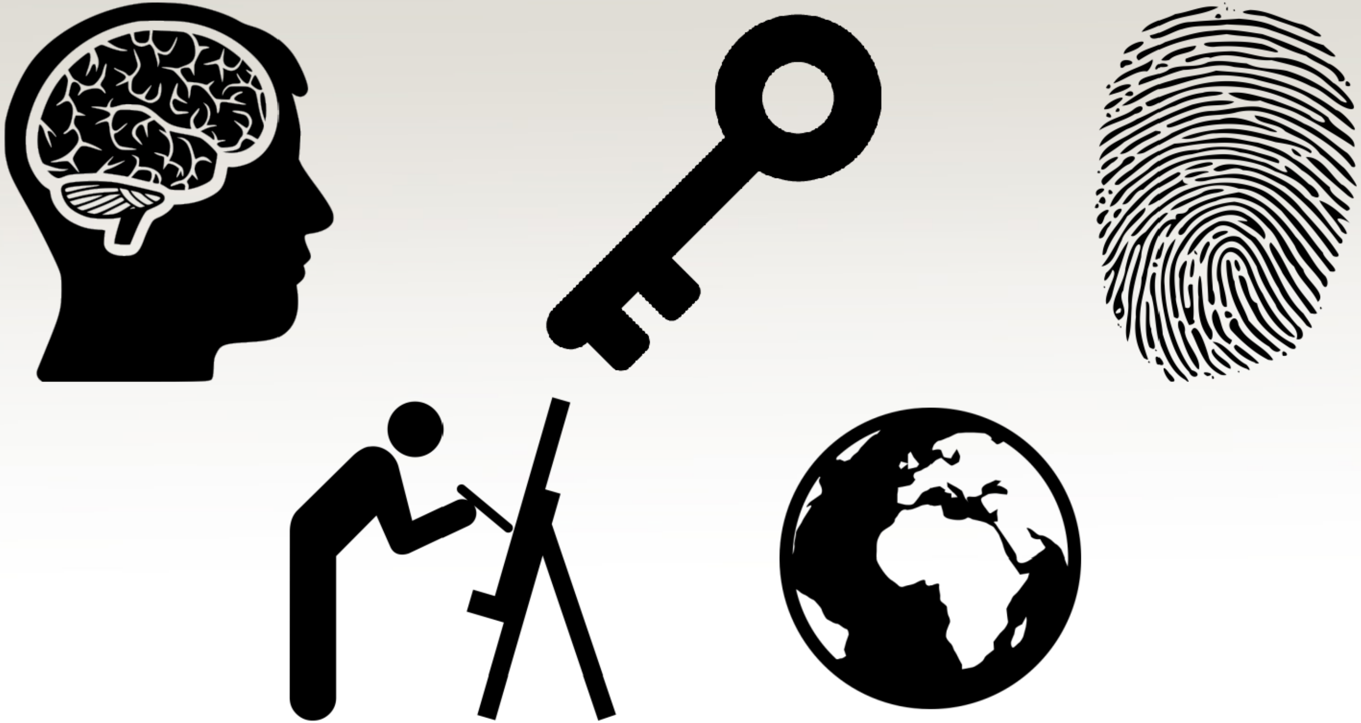
Official (ISC)² trainer
[CISSP, CCSP, HCISPP, CAP, CSSLP]

PSYND
IT SECURITY SERVICES

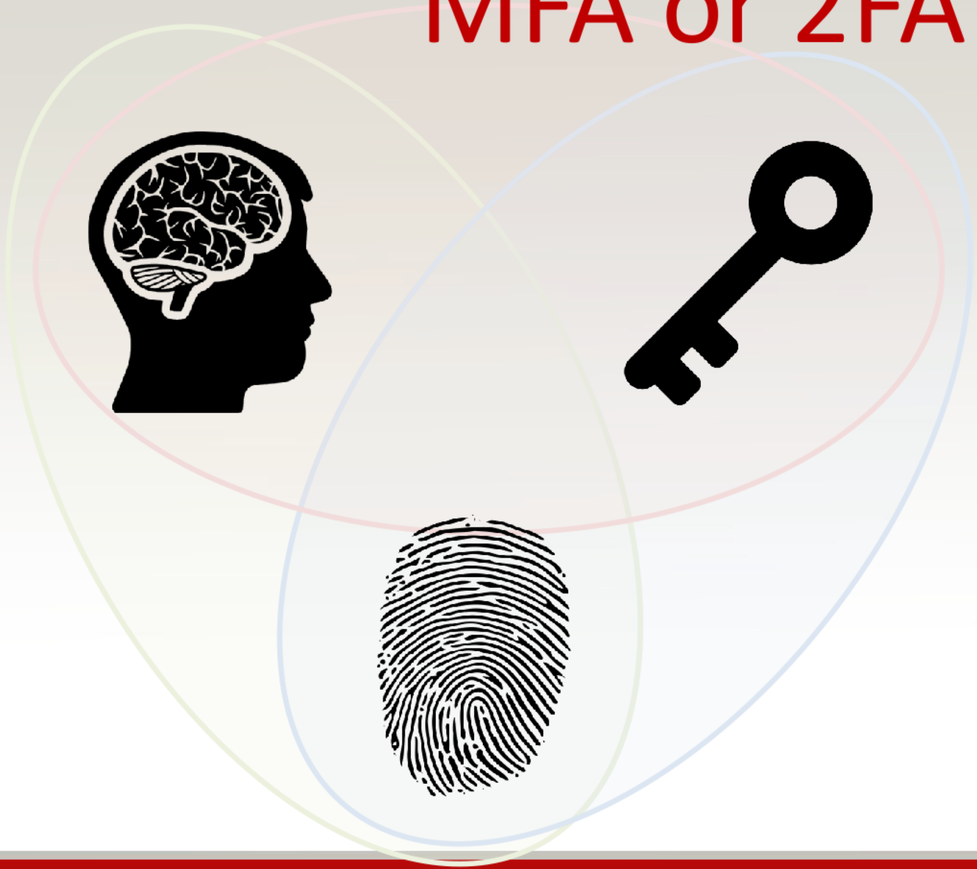
Swiss CyberSecurity

Suisse Romande
Connect | Educate | Inspire | Secure

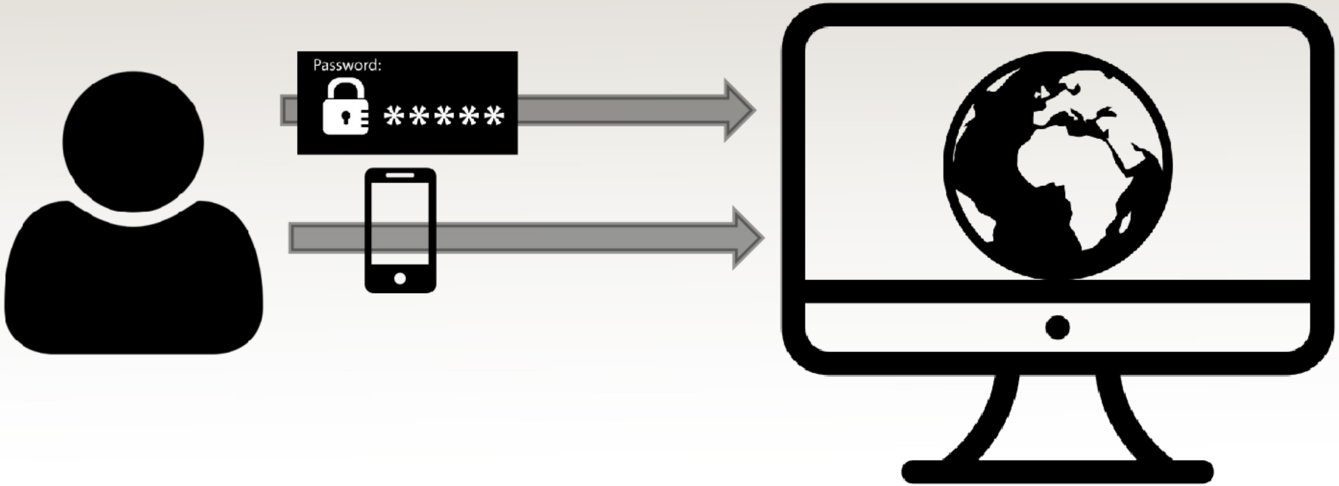
What is MFA?



MFA or 2FA?



MFA usage

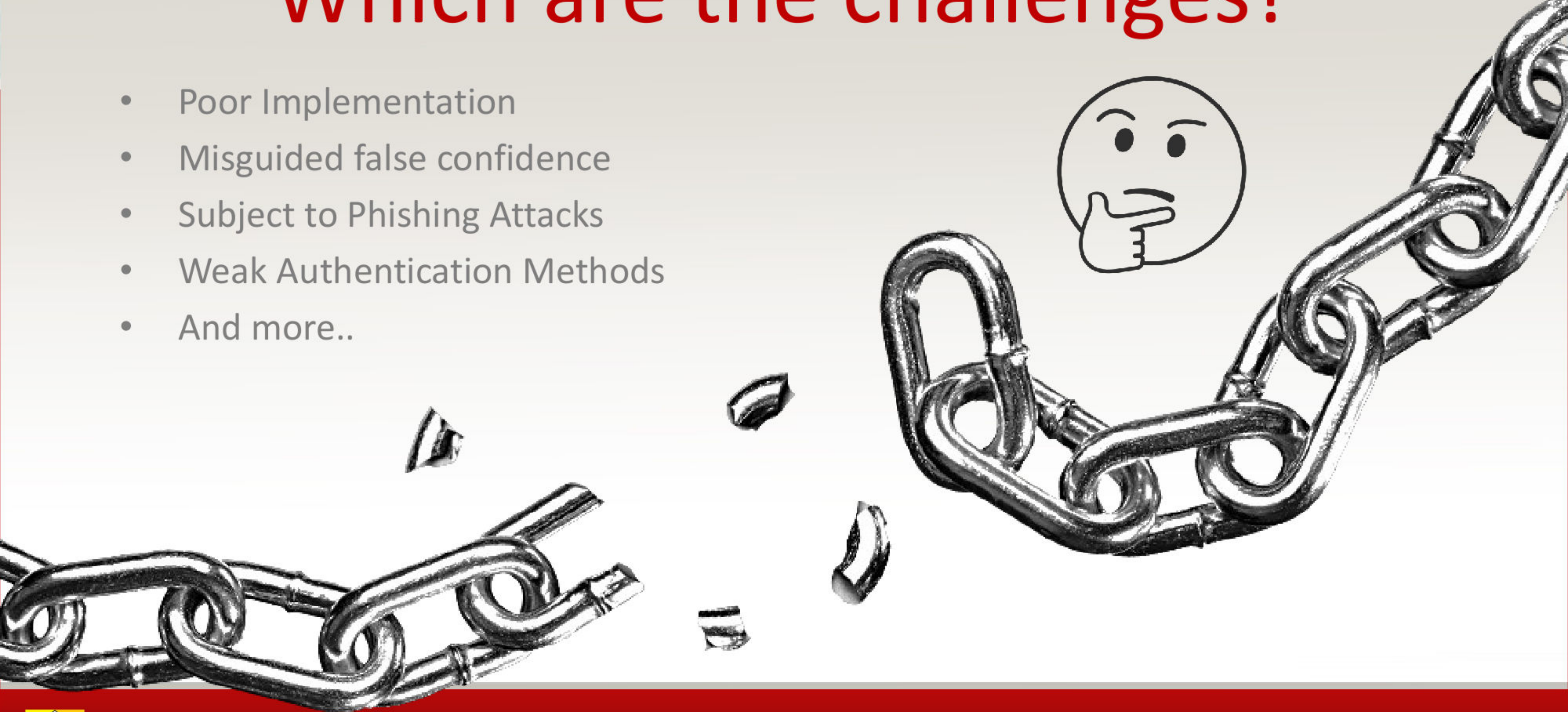


MFA advantages

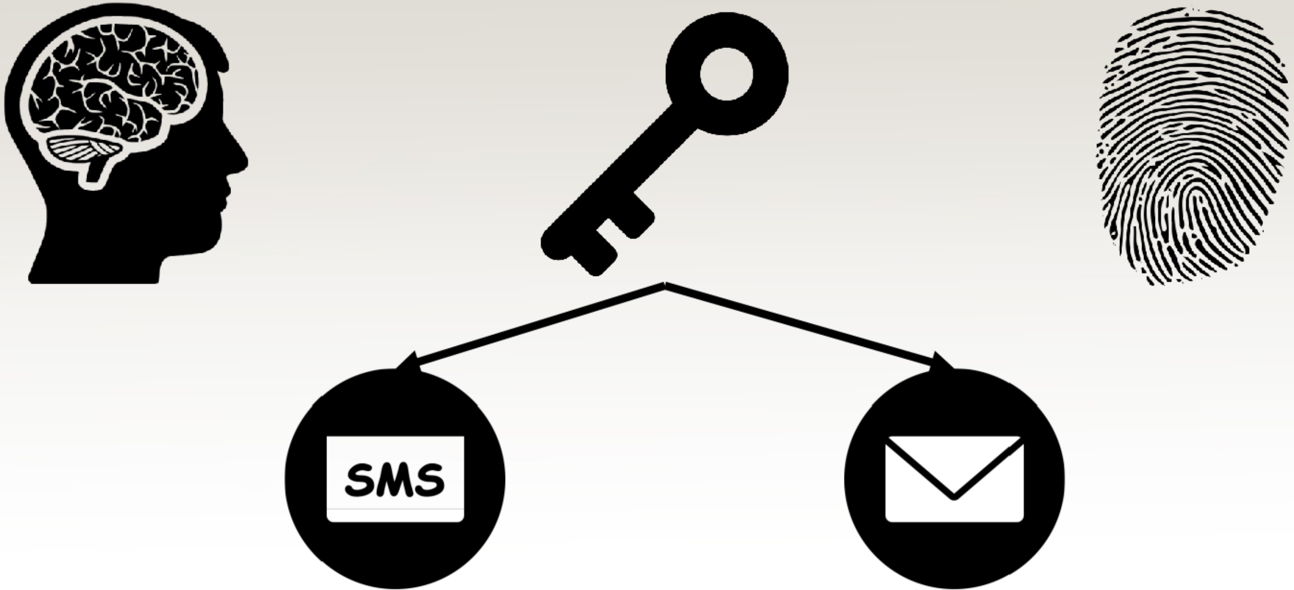
- Enhanced security
- Reduced attack surface
- Reduced data breaches
- Compliance with industry regulations
- Easy to implement
- Remote access protection
- Flexible in authentication method
- Cost-effective security solution
- And more..

Which are the challenges?

- Poor Implementation
- Misguided false confidence
- Subject to Phishing Attacks
- Weak Authentication Methods
- And more..



Choosing Wrong MFA Component



MITM

Spoofing

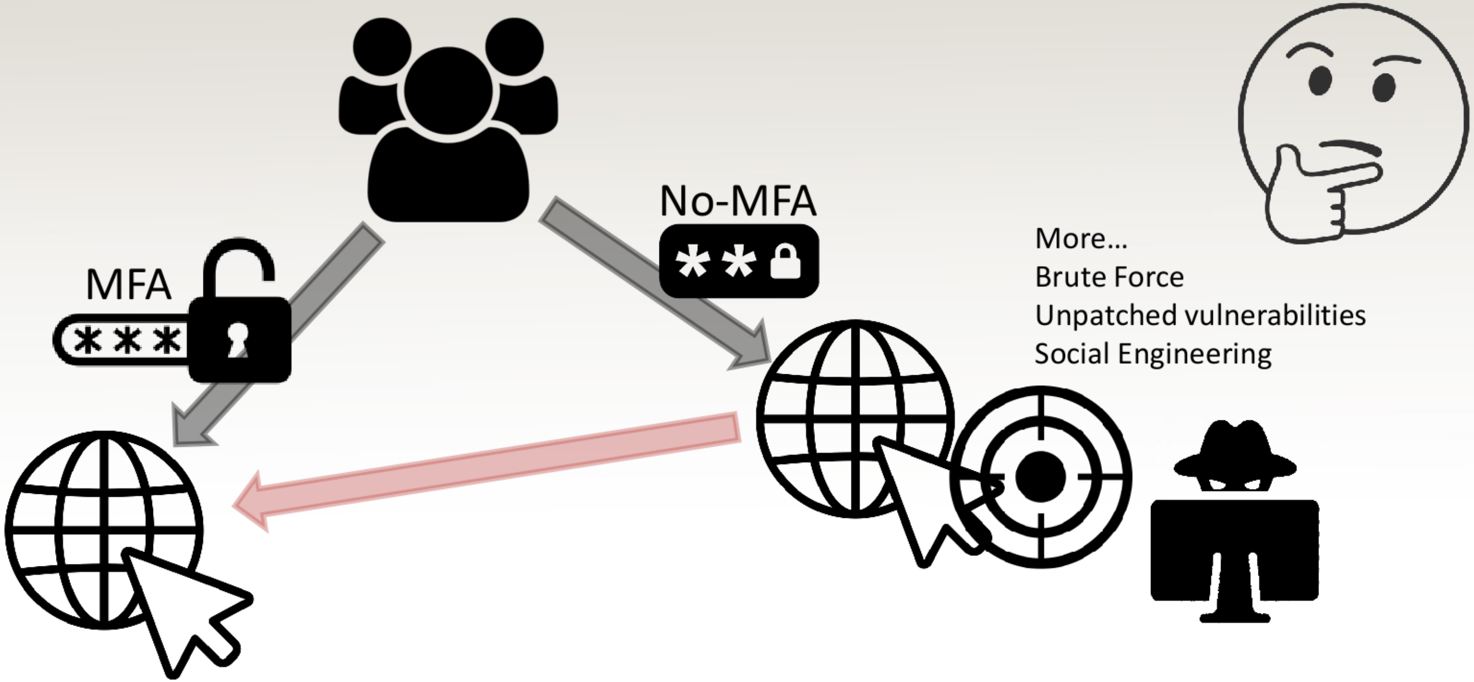
SIM Swap

Phishing

No Encryption

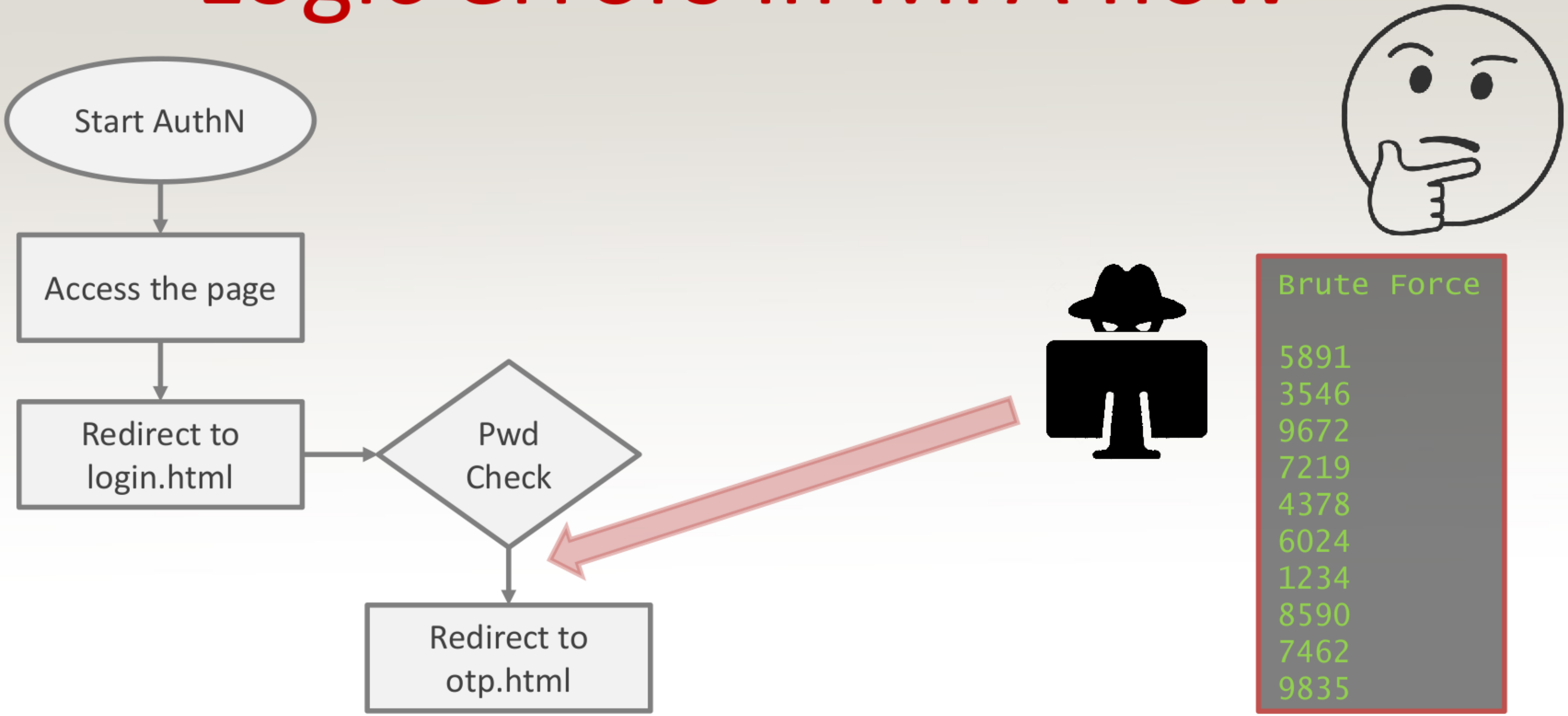
Insecure Email Providers

Inconsistent MFA implementation



More...
Brute Force
Unpatched vulnerabilities
Social Engineering

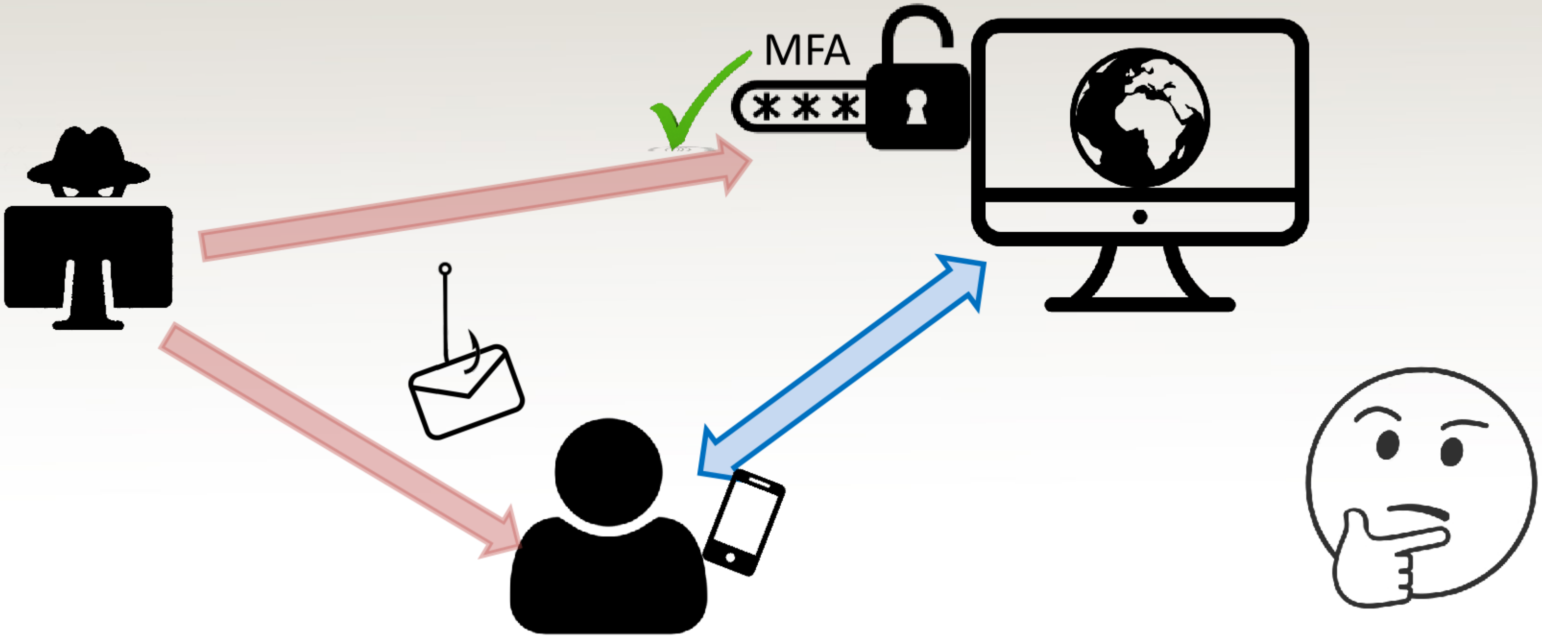
Logic errors in MFA flow



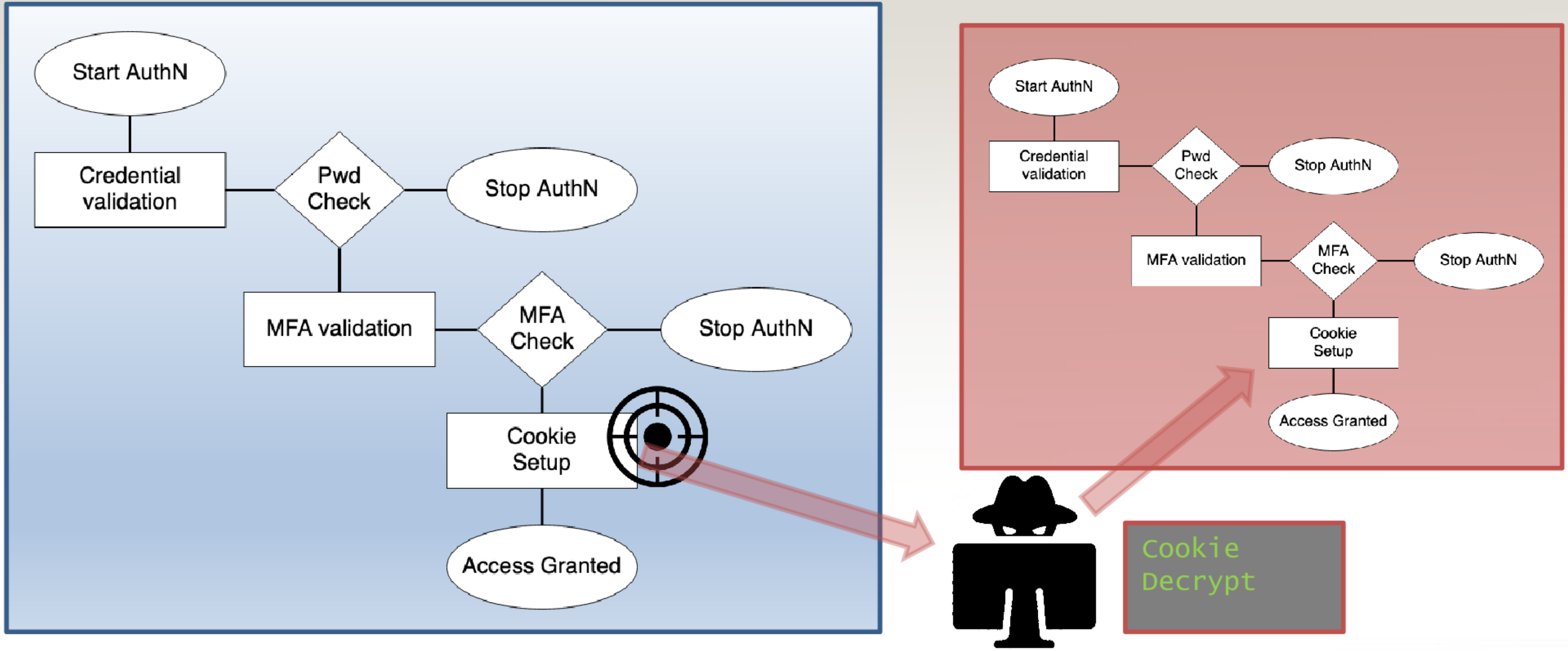
```
Brute Force

5891
3546
9672
7219
4378
6024
1234
8590
7462
9835
```

MFA Fatigue

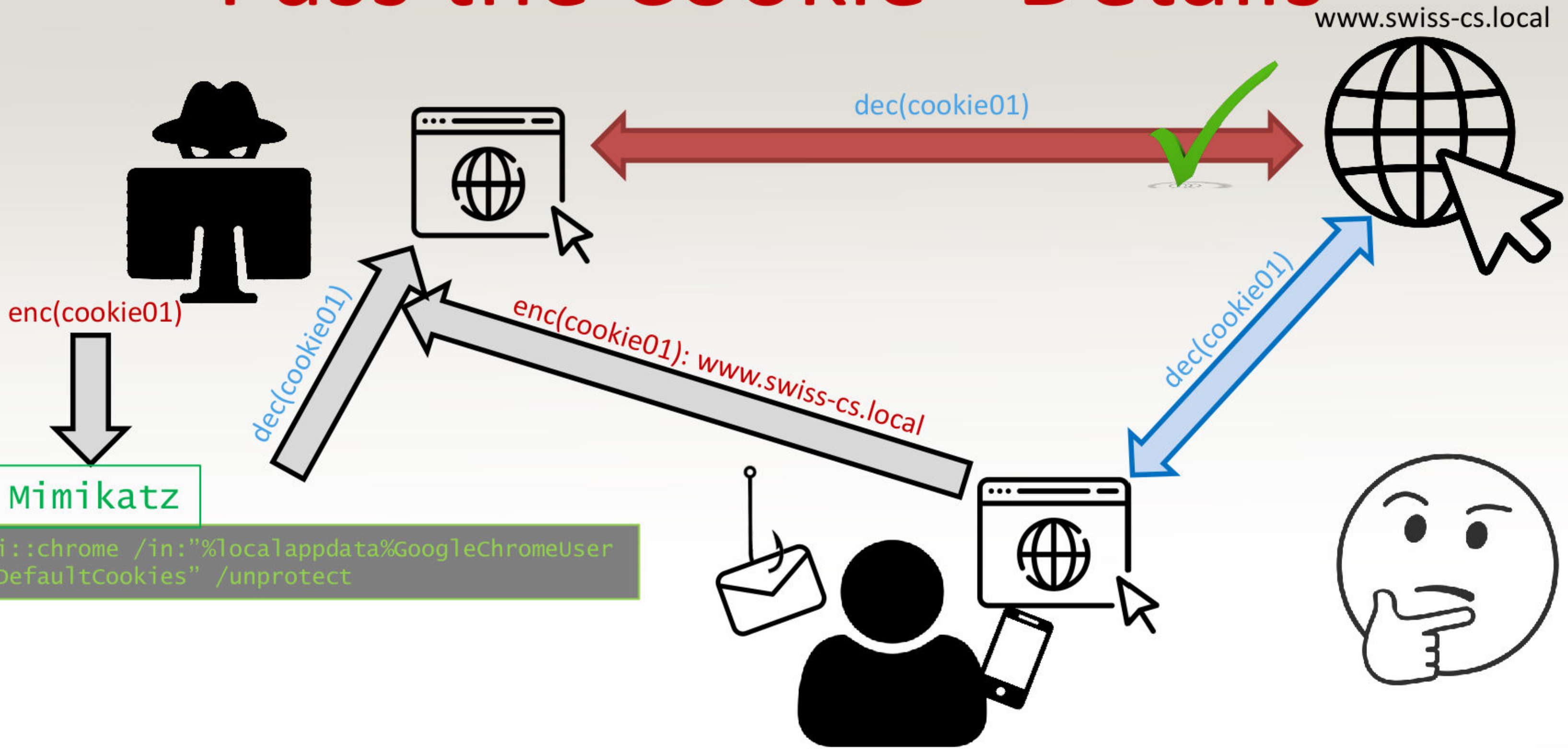


Pass the Cookie



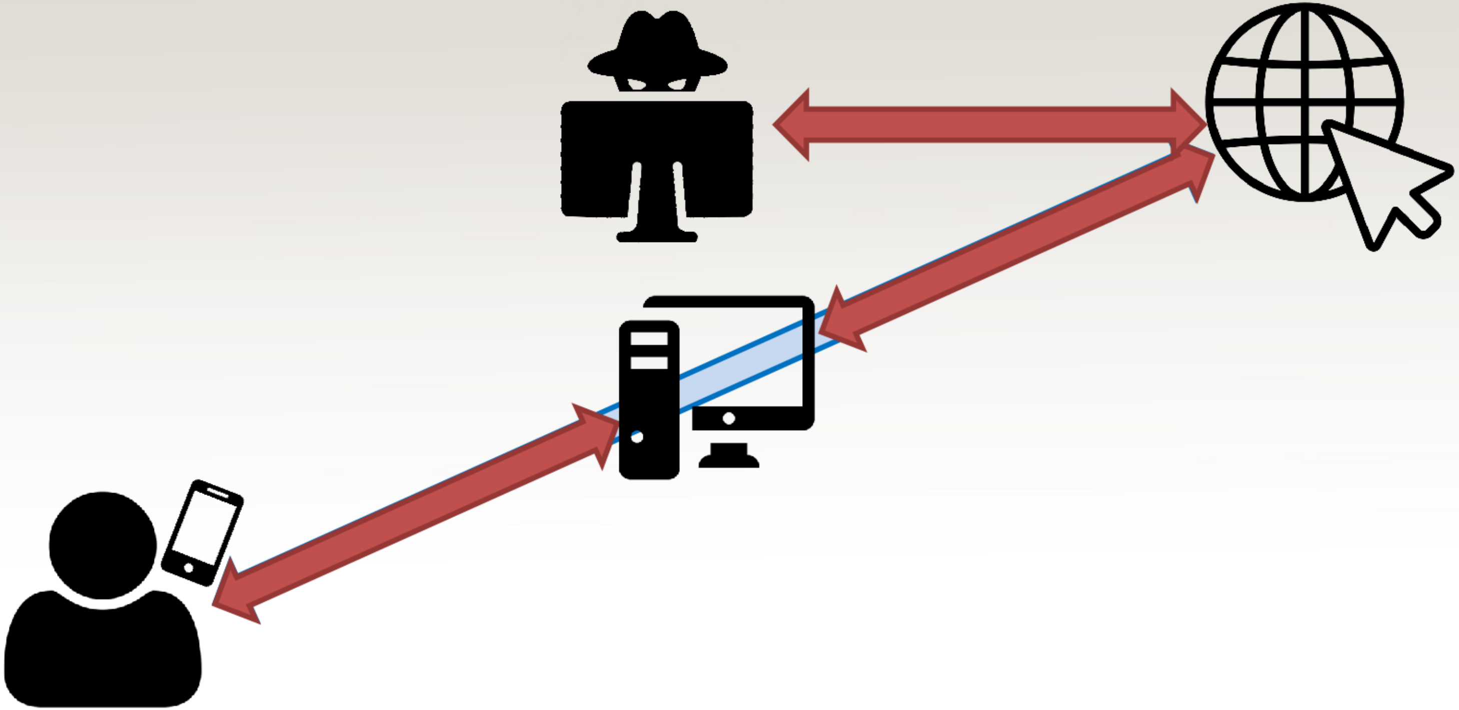
Swiss CyberSecurity

Pass the Cookie - Details

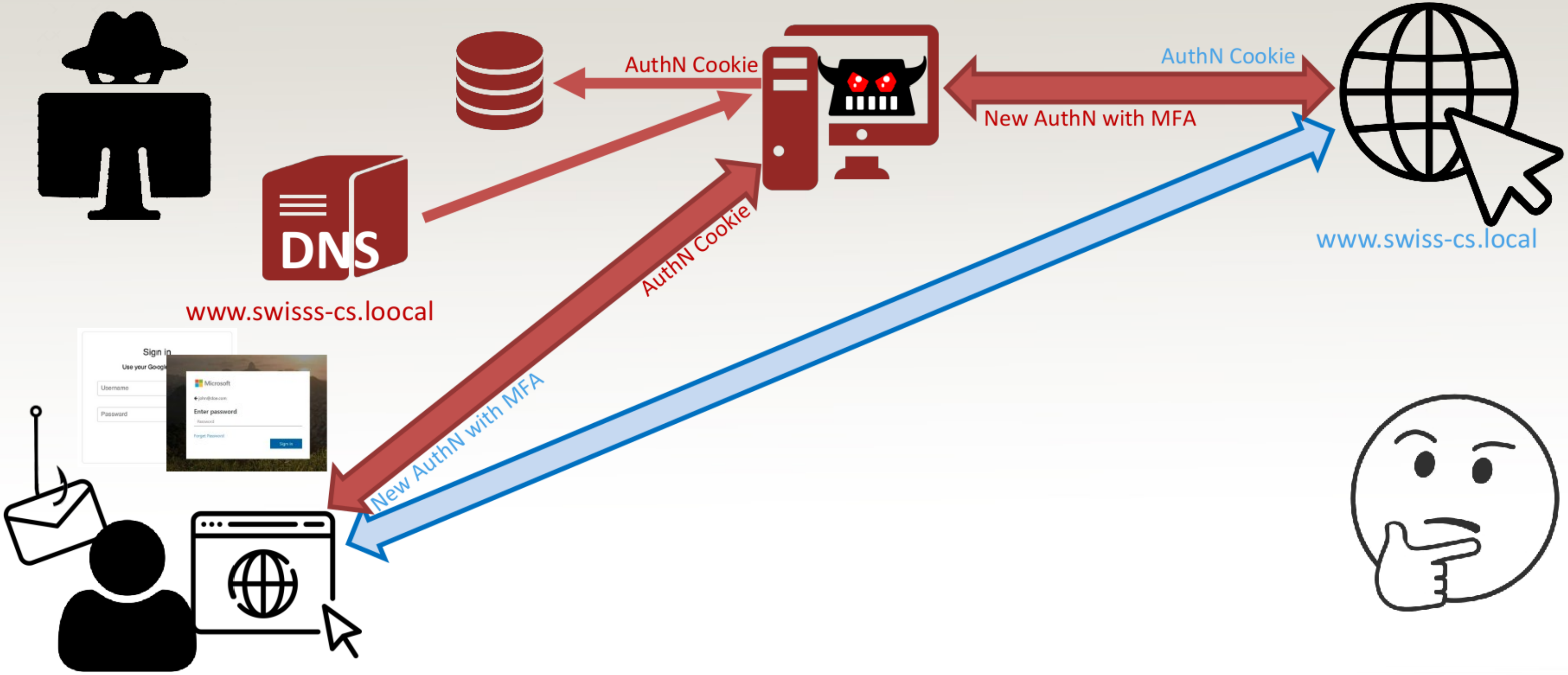


```
dpapi::chrome /in:”%localappdata%GoogleChromeUser
DataDefaultCookies” /unprotect
```

Steal the AuthN Cookie



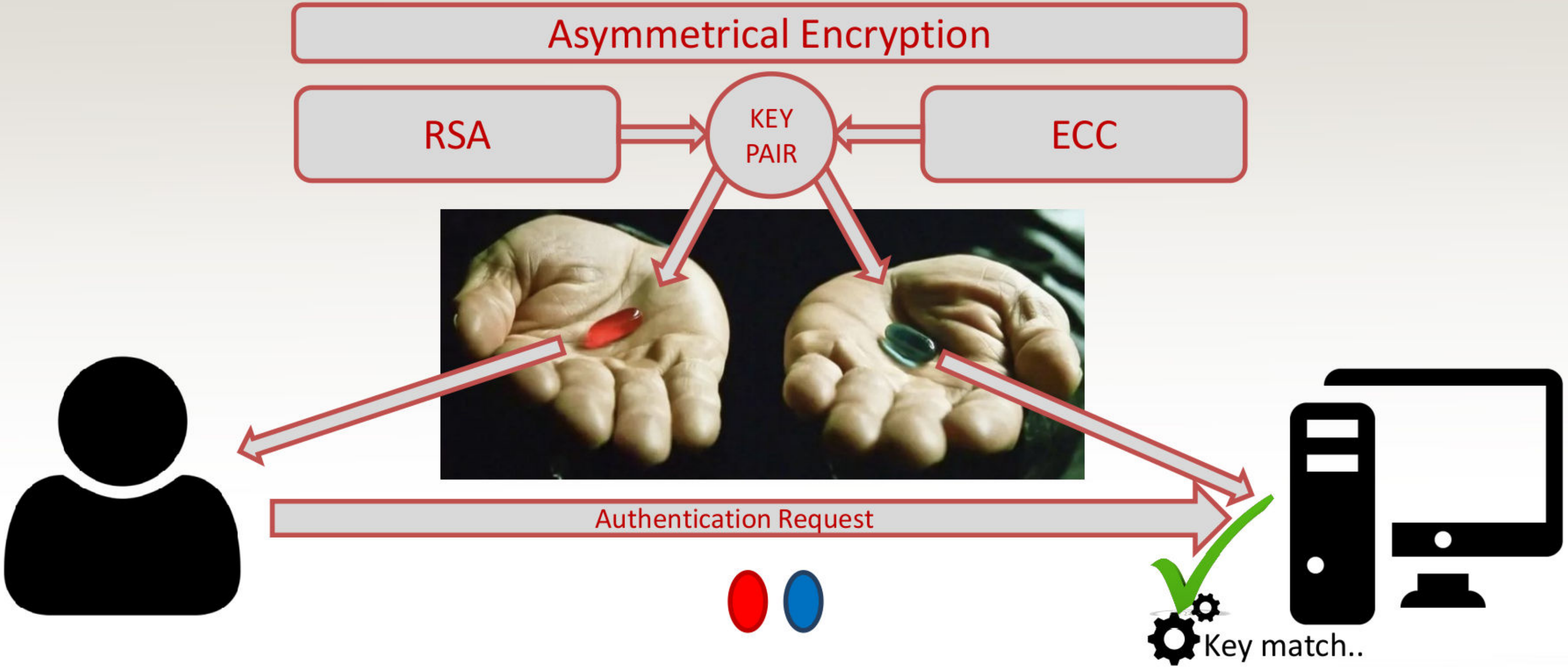
Steal the AuthN Cookie - Details



What went wrong and why?

- What went wrong so far and why?

Passwordless Authentication



Asymmetrical Encryption

RSA

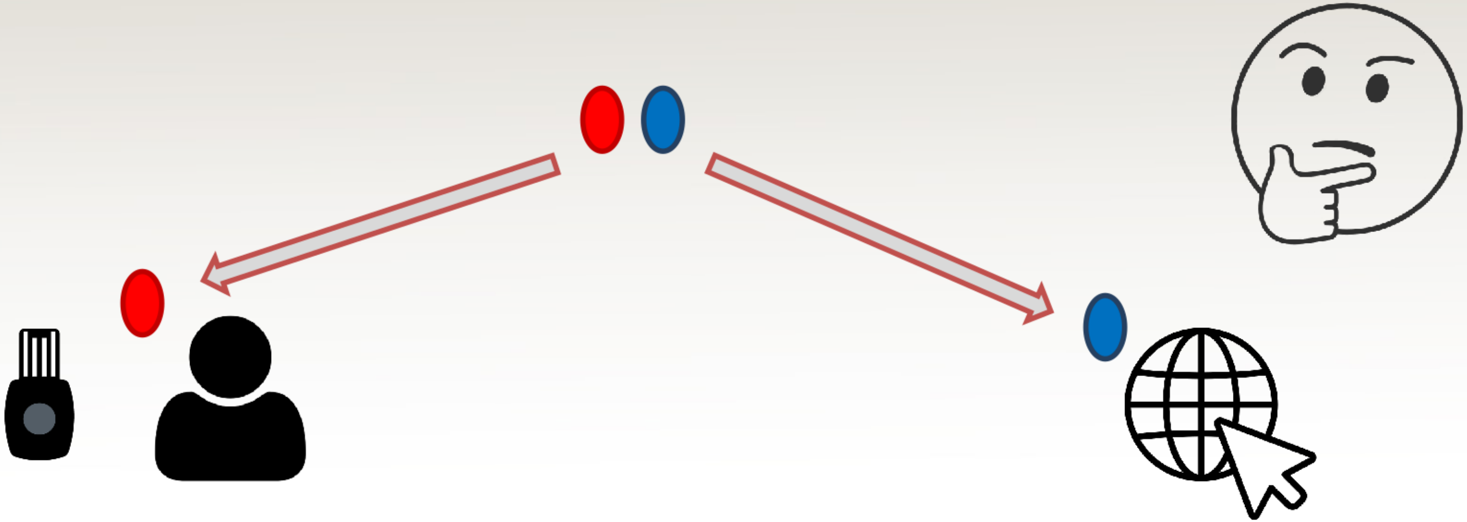
KEY PAIR

ECC

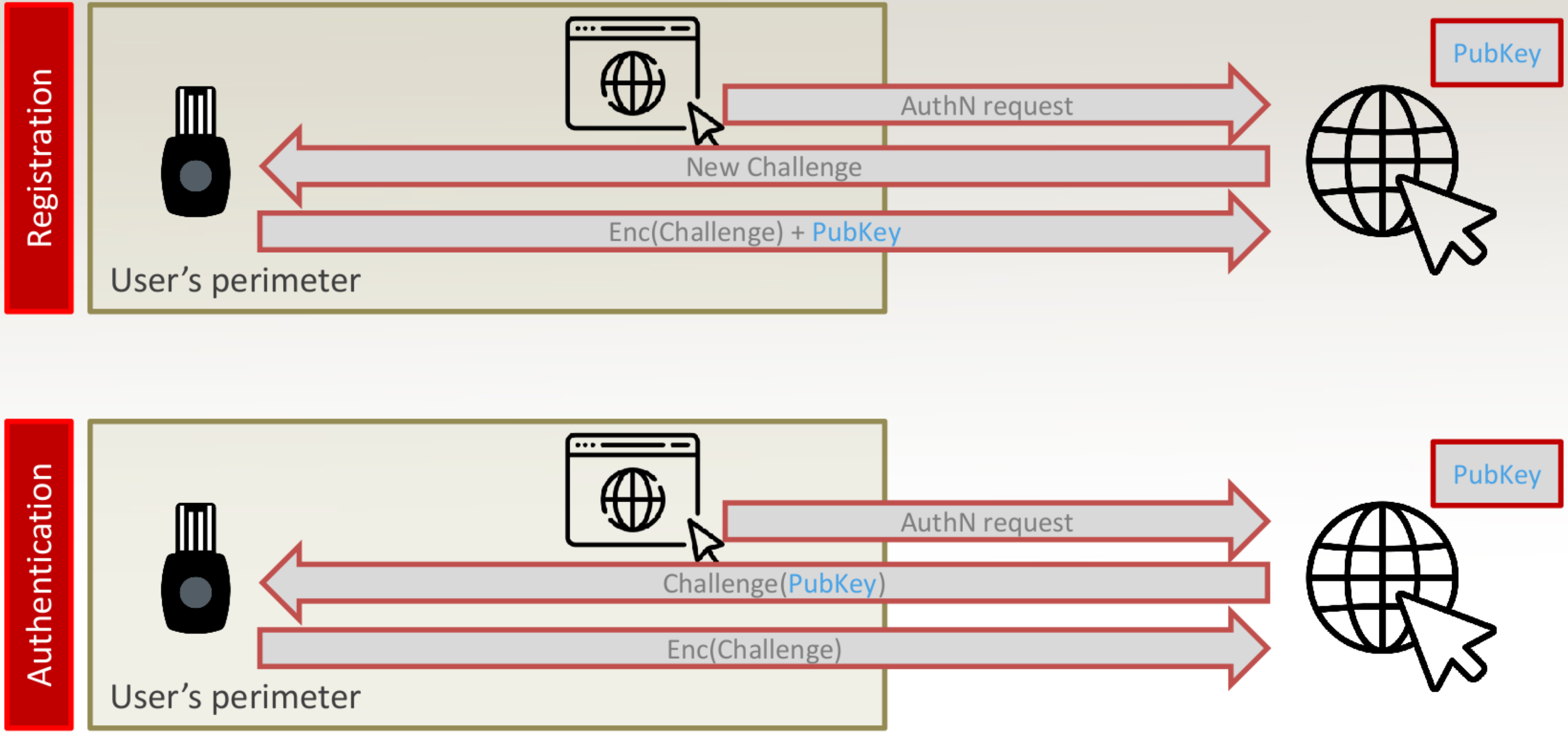
Authentication Request

Key match..

How do I use asym keys?



FIDO2

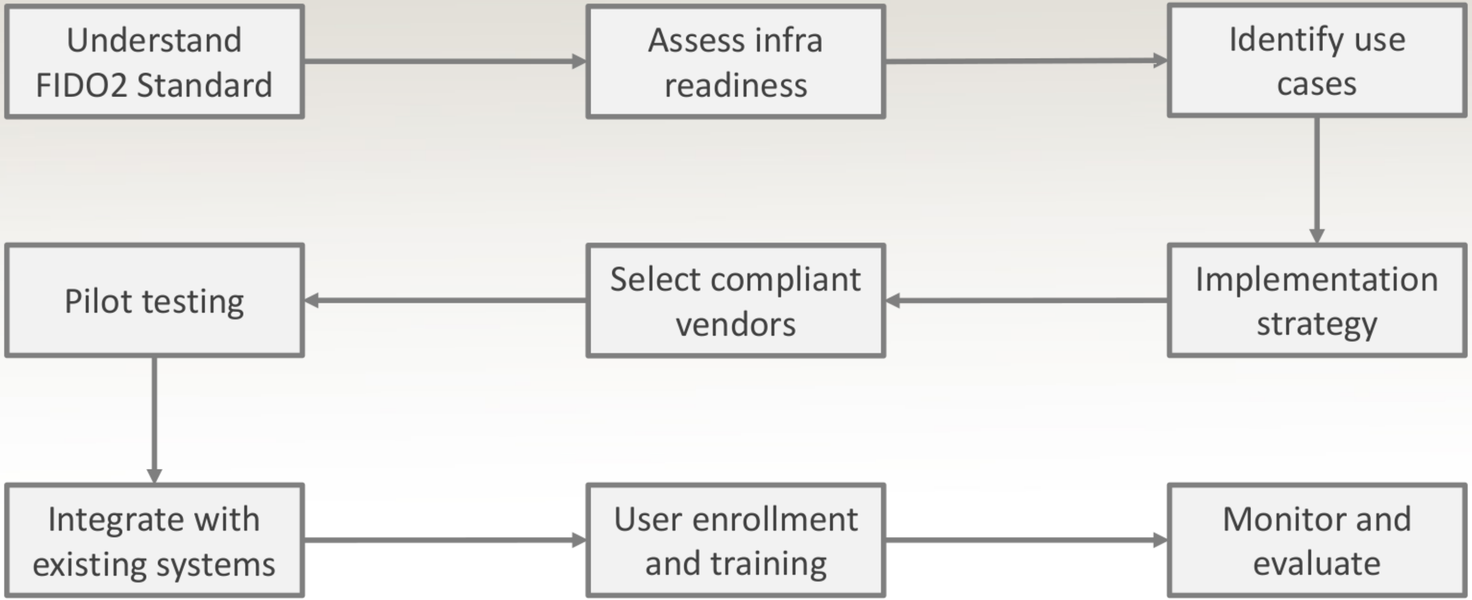


Registration
PubKey
AuthN request
New Challenge
Enc(Challenge) + PubKey
User's perimeter
Authentication
PubKey
AuthN request
Challenge(PubKey)
Enc(Challenge)
User's perimeter

Problem solved?

- Laptops could be stolen
- Hardware tokens could be lost
- Hardware tokens could malfunction or get broken
- Humans are unpredictable..

How to start


Understand FIDO2 Standard
Assess infra readiness
Identify use cases
Implementation strategy
Select compliant vendors
Pilot testing
Integrate with existing systems
User enrollment and training
Monitor and evaluate

Hurdles

- Some systems may not support phishing-resistant MFA
- It may be difficult to deploy phishing-resistant MFA to all staff members at once
- There may be concerns that users will resist a migration to phishing-resistant MFA
- Many others..

Swiss CyberSecurity

www.swiss-cybersecurity.ch

Swiss-CyberSecurity.ch/upcoming-events
Swiss-CyberSecurity.ch/mlist