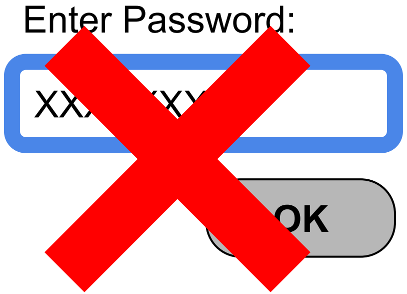
@schlomo@floss.social
@schlomoschapiro

TEKTIT
CONSULTING

Immer diese verflixten Passwörter:

Es geht auch anders!

Continuous Lifecycle



13.–14. November 2024, Continuous Lifecycle Conference, Mannheim
Schlomo Schapiro, Associate Partner / Principal Engineer, Tektit Consulting

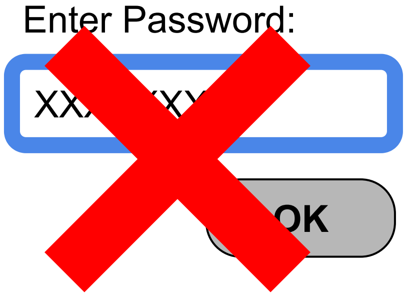
@schlomo@floss.social
@schlomoschapiro

TEKTIT
CONSULTING

Lifting the Curse of Static Credentials

Who needs passwords, anyway?

Continuous Lifecycle

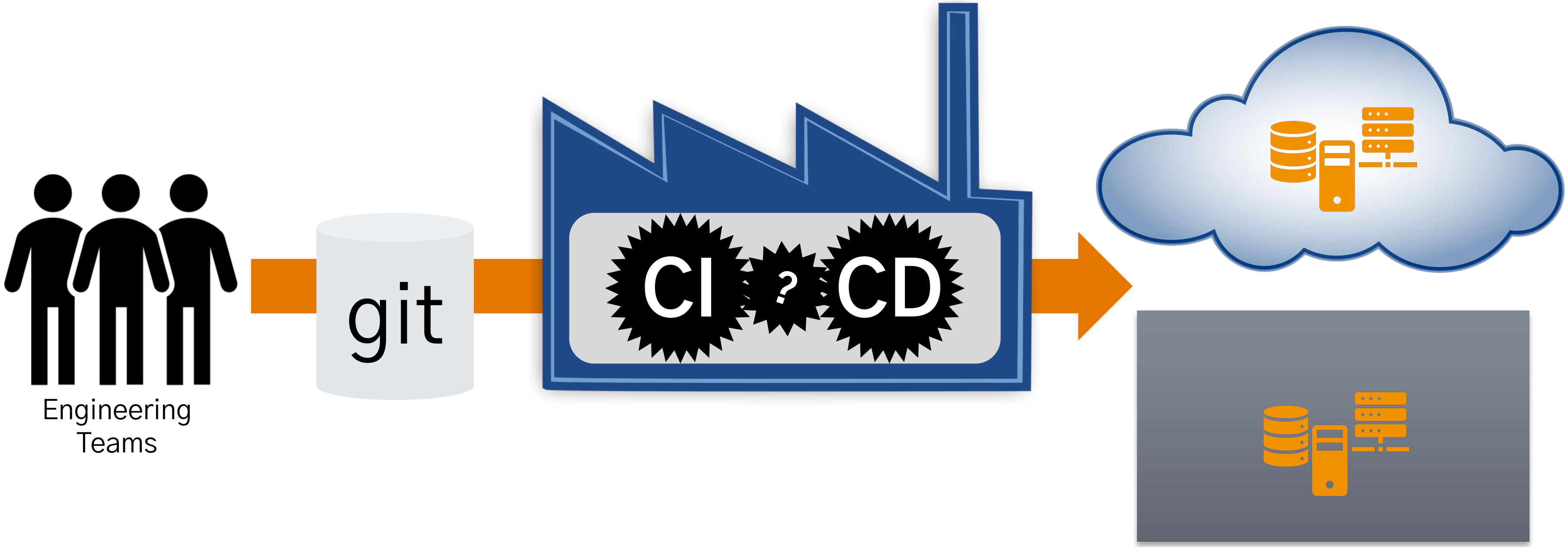


13.–14. November 2024, Continuous Lifecycle Conference, Mannheim
Schlomo Schapiro, Associate Partner / Principal Engineer, Tektit Consulting

Agenda

1. Context: DevOps
2. Why Static Credentials?
3. Why is it a Problem?
4. What about Passkeys?
5. What should we use instead?
6. What prevents us?
7. Let’s make an effort!

Happy DevOps Campers



DevOps is

··· if every person uses the same tool for the same job

··· codified knowledge – everybody contributes his part to common automation

··· if all people have the same privileges in their tooling

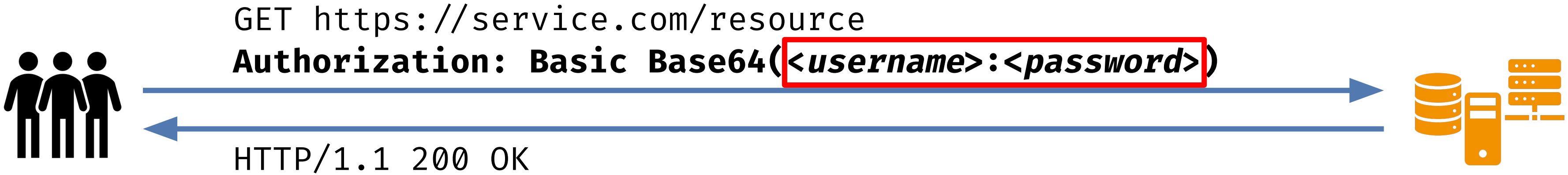
··· if human error is equally possible for Dev and Ops

··· replacing people interfaces by automated decisions and processes ⬅

bit.ly/5devops

... a result

Why Static Credentials?



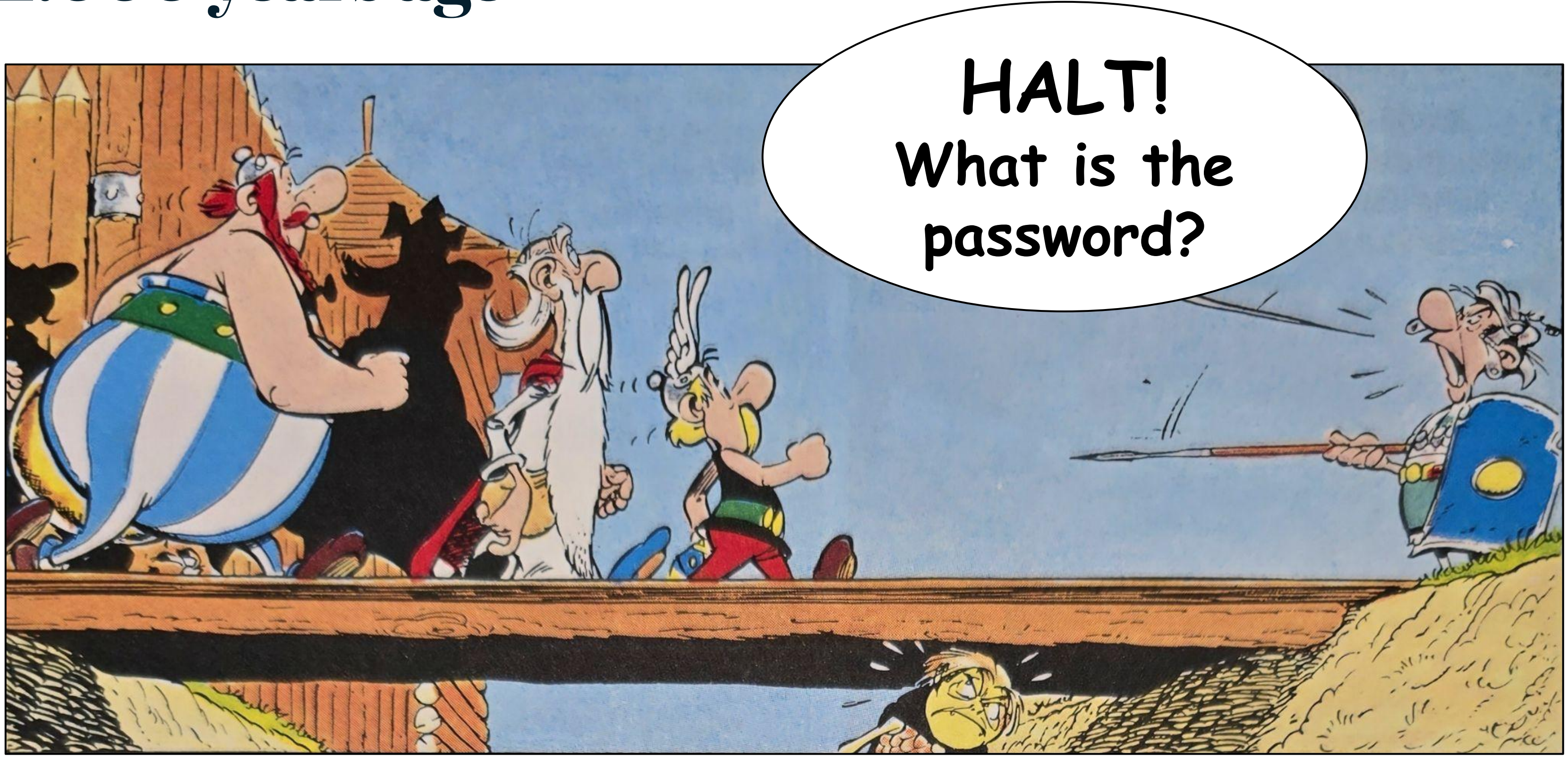
```
GET https://service.com/resource
Authorization: Basic Base64(<username>:<password>)

HTTP/1.1 200 OK

… Content …

… Private Content …
```

> *“Username & password (or API key) is simple, standard and everybody is using it”*
>
> *Everybody thinks so*

100.000 years ago

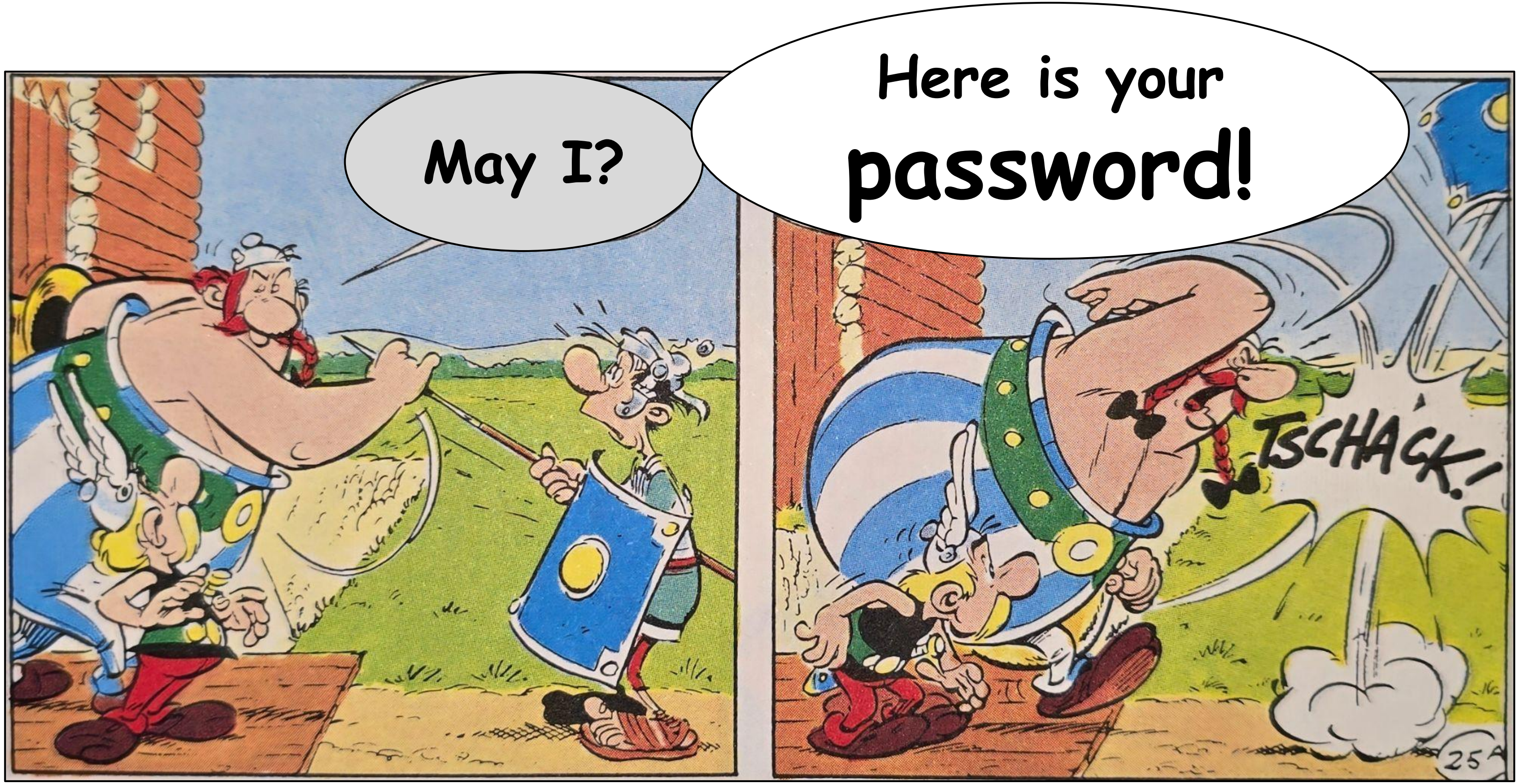
AI generated by Schlomo

2.000 years ago



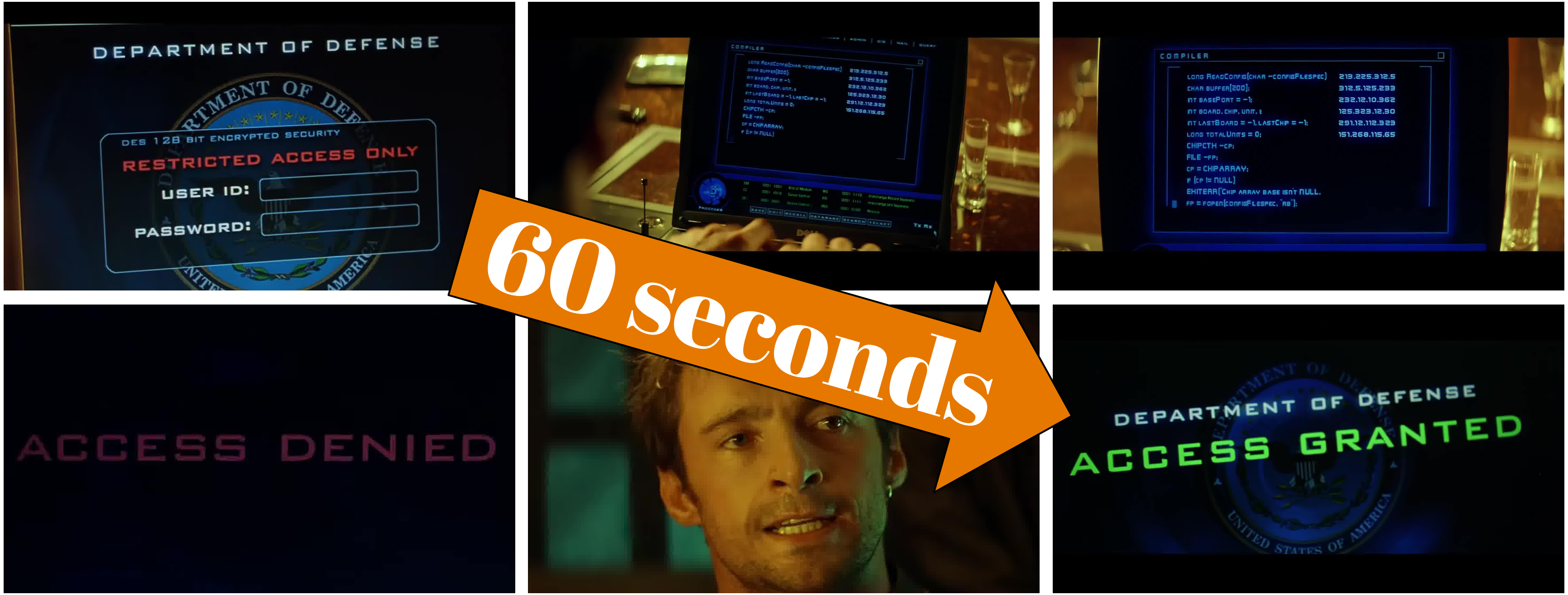
Asterix: Der große Graben

2.000 years ago - brute forcing passwords



TEKTIT CONSULTING

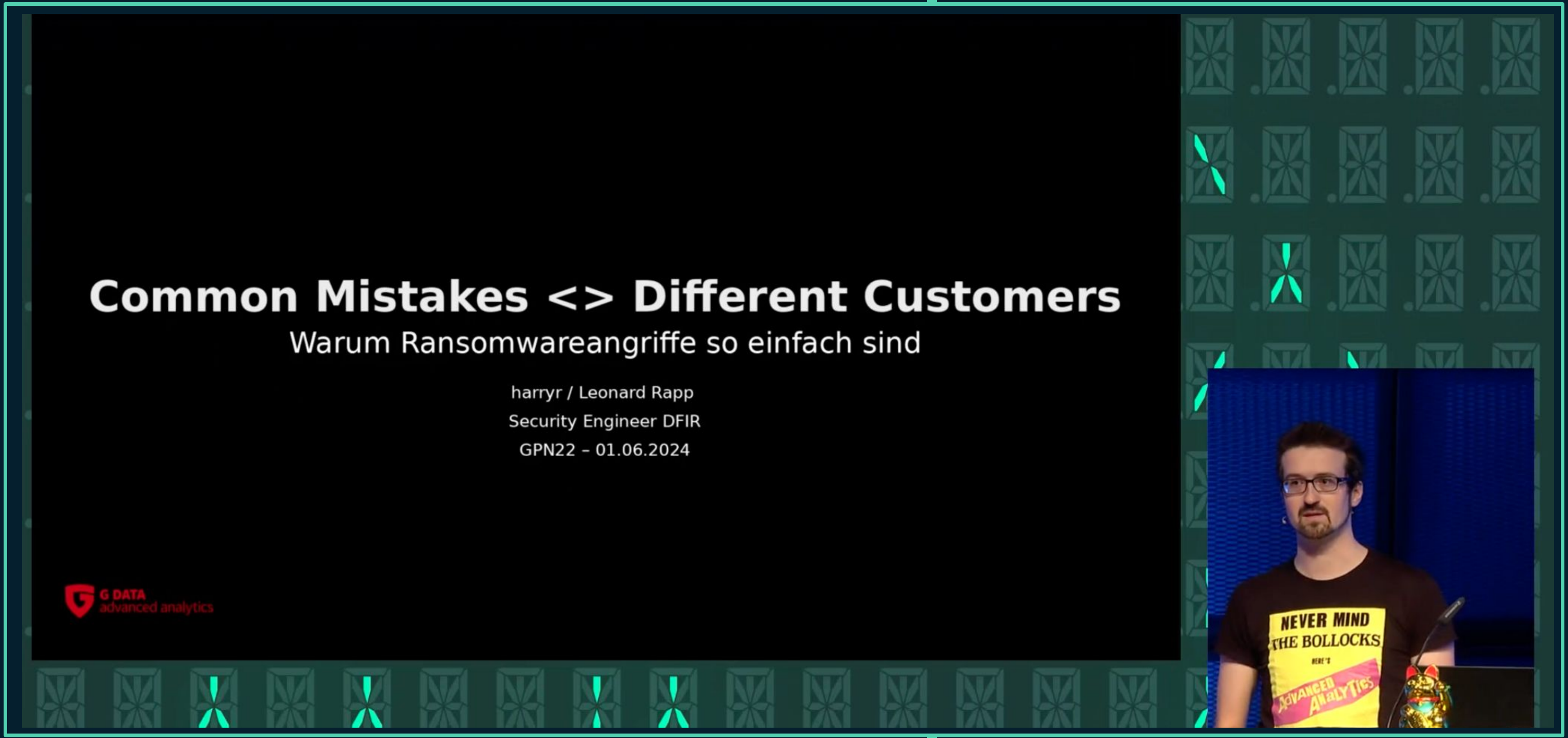
Nowadays



```
LONG READCONFIG(CHAR -CONFIGFILESPEC)     213.225.312.5
CHAR BUFFER[200];                         312.5.125.233
INT BASEPORT = -1;                        232.12.10.362
INT BOARD, CHIP, UNIT, I;                 125.323.12.30
INT LASTBOARD = -1, LASTCHIP = -1;        291.12.112.323
LONG TOTALUNITS = 0;                      151.268.115.65
CHIPCTH -CP;
FILE -FP;
CP = CHIPARRAY;
IF (CP != NULL)
EXITERR("CHIP ARRAY BASE ISN'T NULL.
FP = FOPEN(CONFIGFILESPEC, "RB");
```

Swordfish (2001)

Why is it a problem?



Common Mistakes <> Different Customers

Warum Ransomwareangriffe so einfach sind

harryr / Leonard Rapp

Security Engineer DFIR

GPN22 – 01.06.2024

TEKTIT CONSULTING

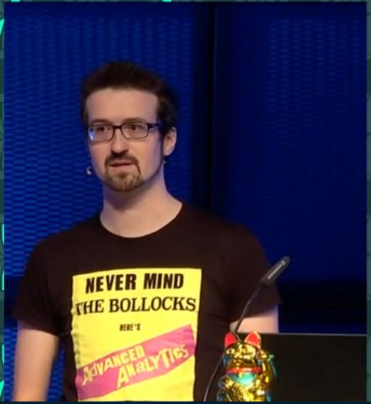
media.ccc.de/v/gpn22-314-common-mistakes-different-customers-warum-ransomware-angriffe-so-einfach-sind

Problem #1:
Patch Management

Problem #2

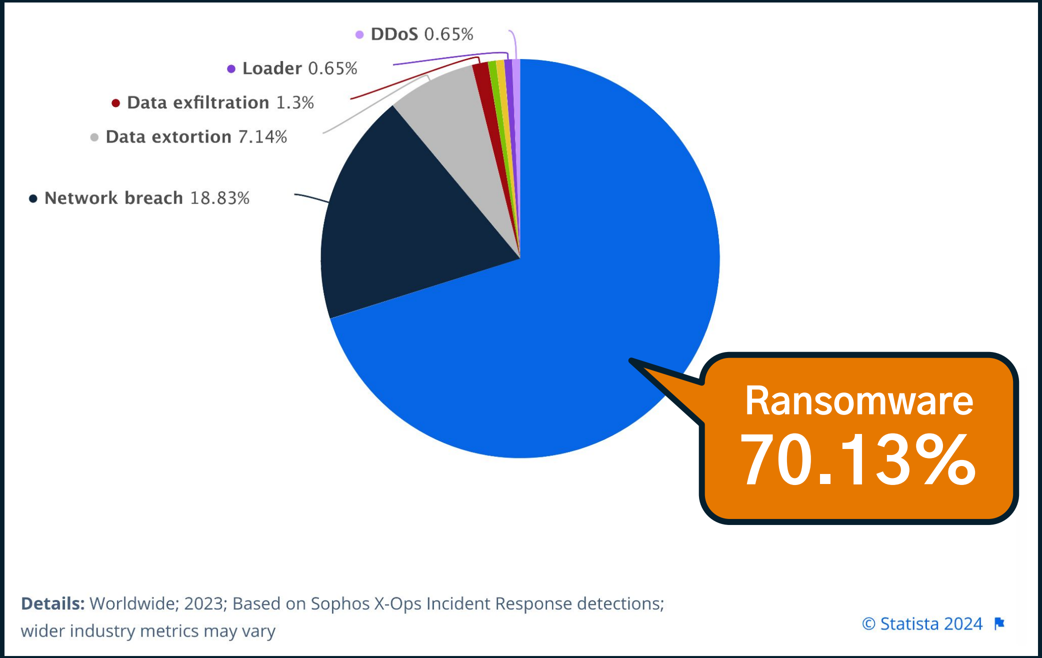
Schwache Passwörter

SOMEONE FIGURED OUT MY PASSWORD,
NOW I HAVE TO RENAME MY DOG.



TEKTIT CONSULTING

Ransomware risk #1



Ransomware
70.13%

Details: Worldwide; 2023; Based on Sophos X-Ops Incident Response detections; wider industry metrics may vary

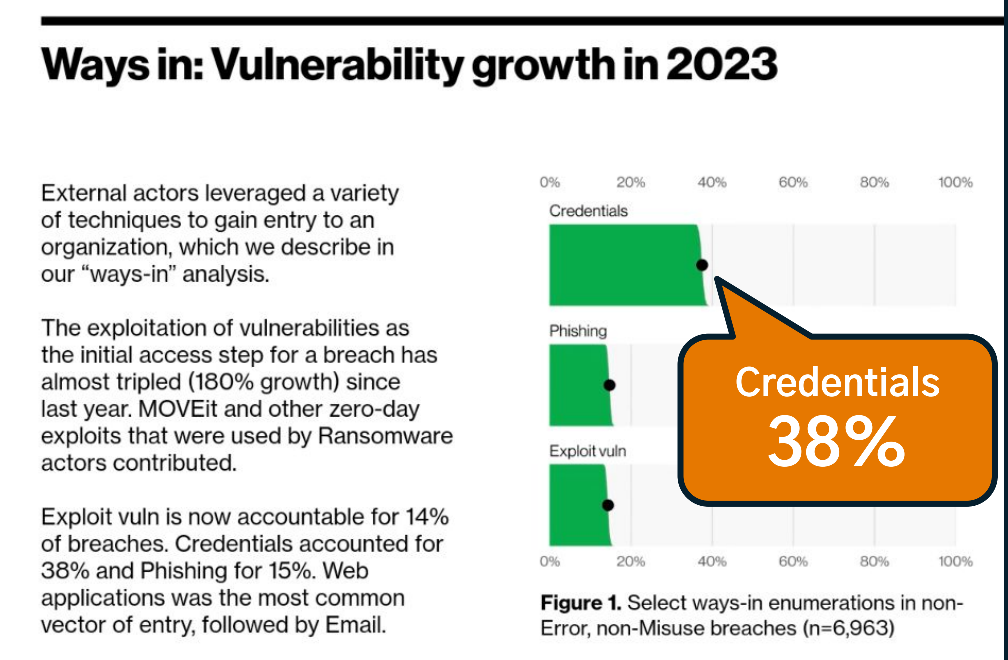
© Statista 2024

Statista: Distribution of detected cyberattacks worldwide in 2023, by type

www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type/

TEKTIT CONSULTING

Credentials problem #1



Ways in: Vulnerability growth in 2023

External actors leveraged a variety of techniques to gain entry to an organization, which we describe in our “ways-in” analysis.

The exploitation of vulnerabilities as the initial access step for a breach has almost tripled (180% growth) since last year. MOVEit and other zero-day exploits that were used by Ransomware actors contributed.

Exploit vuln is now accountable for 14% of breaches. Credentials accounted for 38% and Phishing for 15%. Web applications was the most common vector of entry, followed by Email.

Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

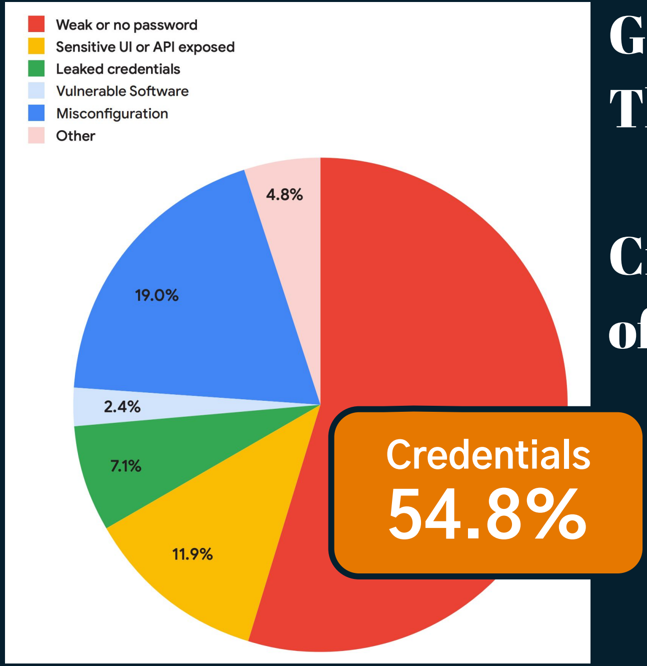
Credentials
38%

2024 Verizon Data Breach Investigations Report (DBIR), key findings

TEKTIT CONSULTING

www.brighttalk.com/webcast/15099/609088 & www.verizon.com/business/resources/reports/dbir/

Cloud IaaS exploits #1



Google Cloud August 2023 Threat Horizons Report:

Credentials factor into over half of incidents in Q1 2023

cloud.google.com/blog/products/identity-security/threat-horizons-report-august-2023/

TEKTIT CONSULTING

My idea:

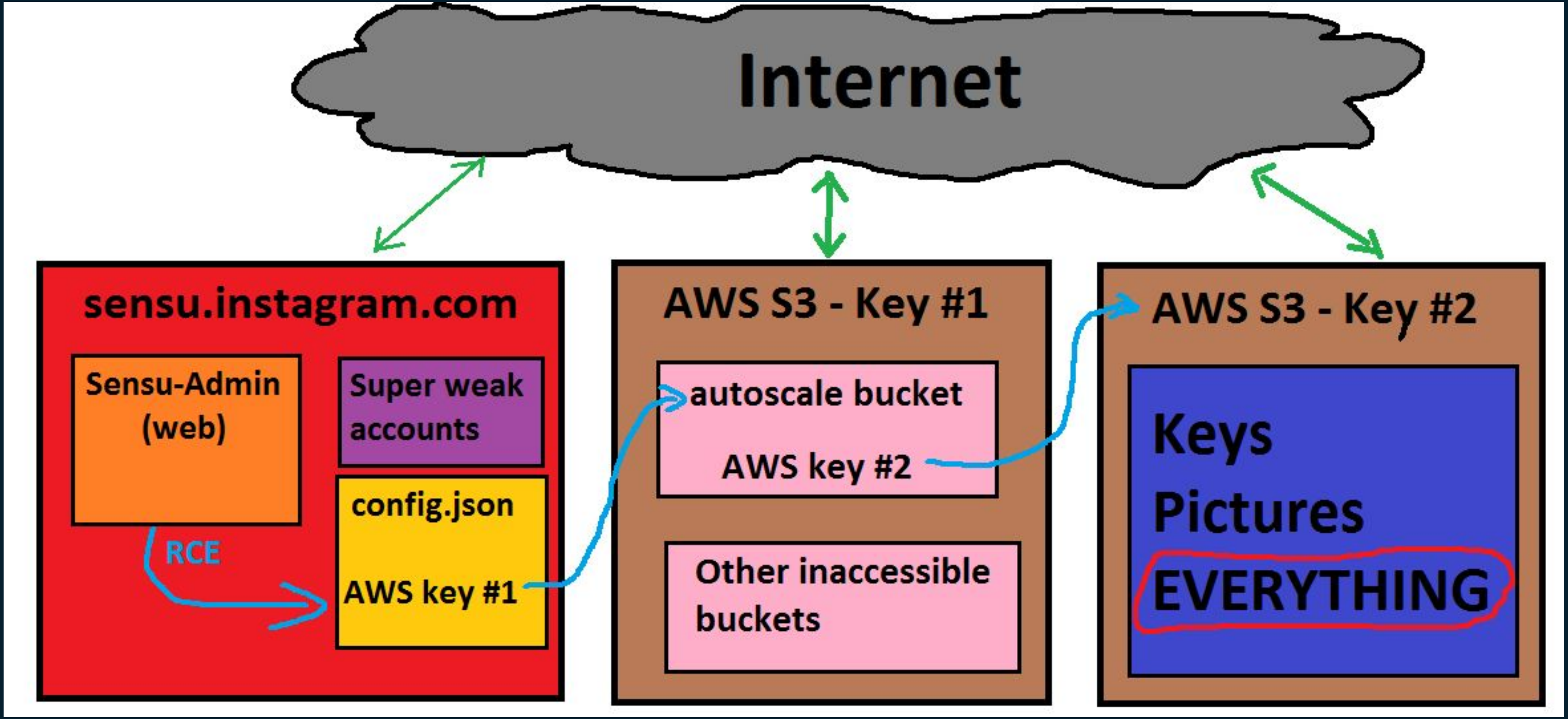
Let’s get rid of ***passwords*** *as much as possible to eliminate this attack vector and significiantly reduce the risks*

TEKTIT CONSULTING

Why is it a problem?

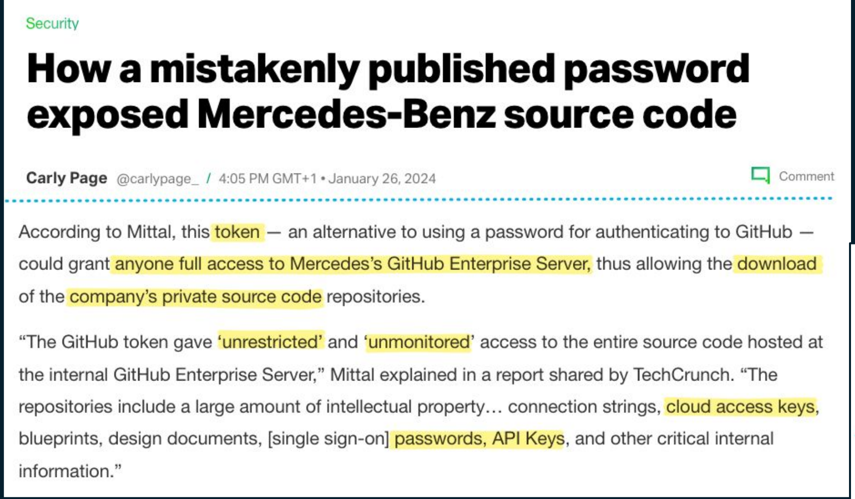
Protecting static credentials is impossible, in “real life”

2015: Instagram's Million Dollar Bug



exfiltrated.com/research-Instagram-RCE.php

2024: Merzedes & BMW



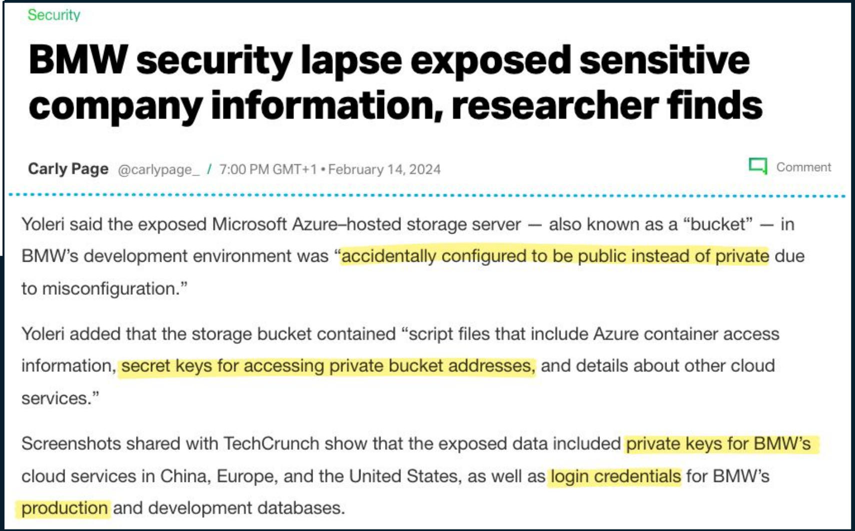
Security

How a mistakenly published password exposed Mercedes-Benz source code

Carly Page @carlypage_ / 4:05 PM GMT+1 • January 26, 2024 Comment

According to Mittal, this token — an alternative to using a password for authenticating to GitHub — could grant anyone full access to Mercedes's GitHub Enterprise Server, thus allowing the download of the company's private source code repositories.

"The GitHub token gave 'unrestricted' and 'unmonitored' access to the entire source code hosted at the internal GitHub Enterprise Server," Mittal explained in a report shared by TechCrunch. "The repositories include a large amount of intellectual property… connection strings, cloud access keys, blueprints, design documents, [single sign-on] passwords, API Keys, and other critical internal information."



Security

BMW security lapse exposed sensitive company information, researcher finds

Carly Page @carlypage_ / 7:00 PM GMT+1 • February 14, 2024 Comment

Yoleri said the exposed Microsoft Azure–hosted storage server — also known as a "bucket" — in BMW's development environment was "accidentally configured to be public instead of private due to misconfiguration."

Yoleri added that the storage bucket contained "script files that include Azure container access information, secret keys for accessing private bucket addresses, and details about other cloud services."

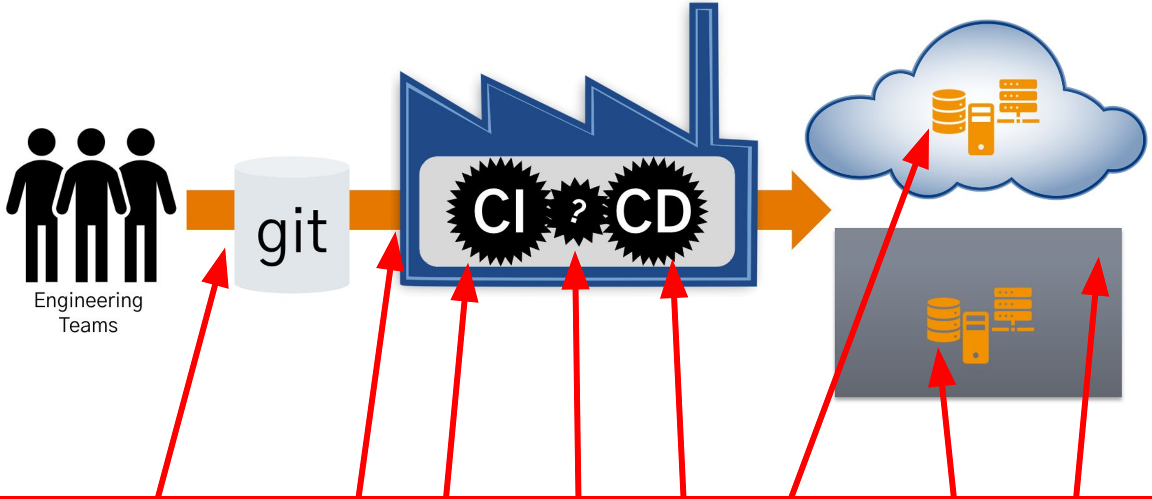
Screenshots shared with TechCrunch show that the exposed data included private keys for BMW's cloud services in China, Europe, and the United States, as well as login credentials for BMW's production and development databases.

techcrunch.com/2024/02/14/bmw-security-lapse-exposed-sensitive-company-information-researcher-finds/
techcrunch.com/2024/01/26/mercedez-benz-token-exposed-source-code-github/

I’m afraid:

Who actually has ***your*** *passwords?*

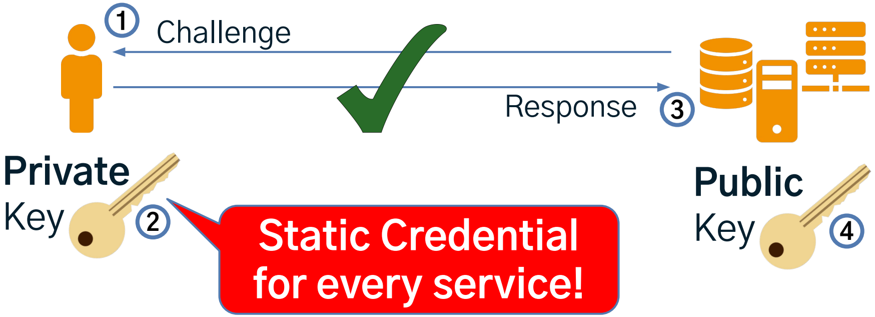
Why is it a DevOps Problem?



Passwords, Tokens, API Keys, Certificates, SSH Keys …

DevOps is … replacing people interfaces by automated decisions and processes

What about Passkeys?



Passkeys solve important problems:

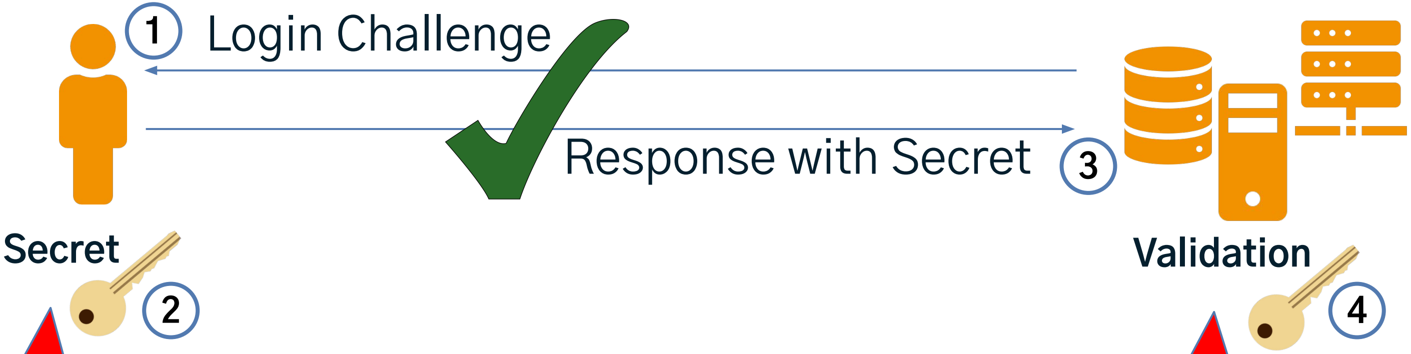
- Challenge–Response protects static credential confidentiality
- API–first design, automation friendly
- Universal standard
- **Effective SSO for consumers**

Passkey shortcomings:

- Security depends on client–side implementation (like with SSH keys)
- Confusing UX
- Lack of management controls for Enterprise or managed environments
- No backup concept – except blind trust to Cloud providers

See "Passkeys: A Shattered Dream" fy.blackhats.net.au/blog/2024–04–26–passkeys–a–shattered–dream/
for a detailed analysis by William (Firstyear) Brown, a 389DS and Kanidm developer

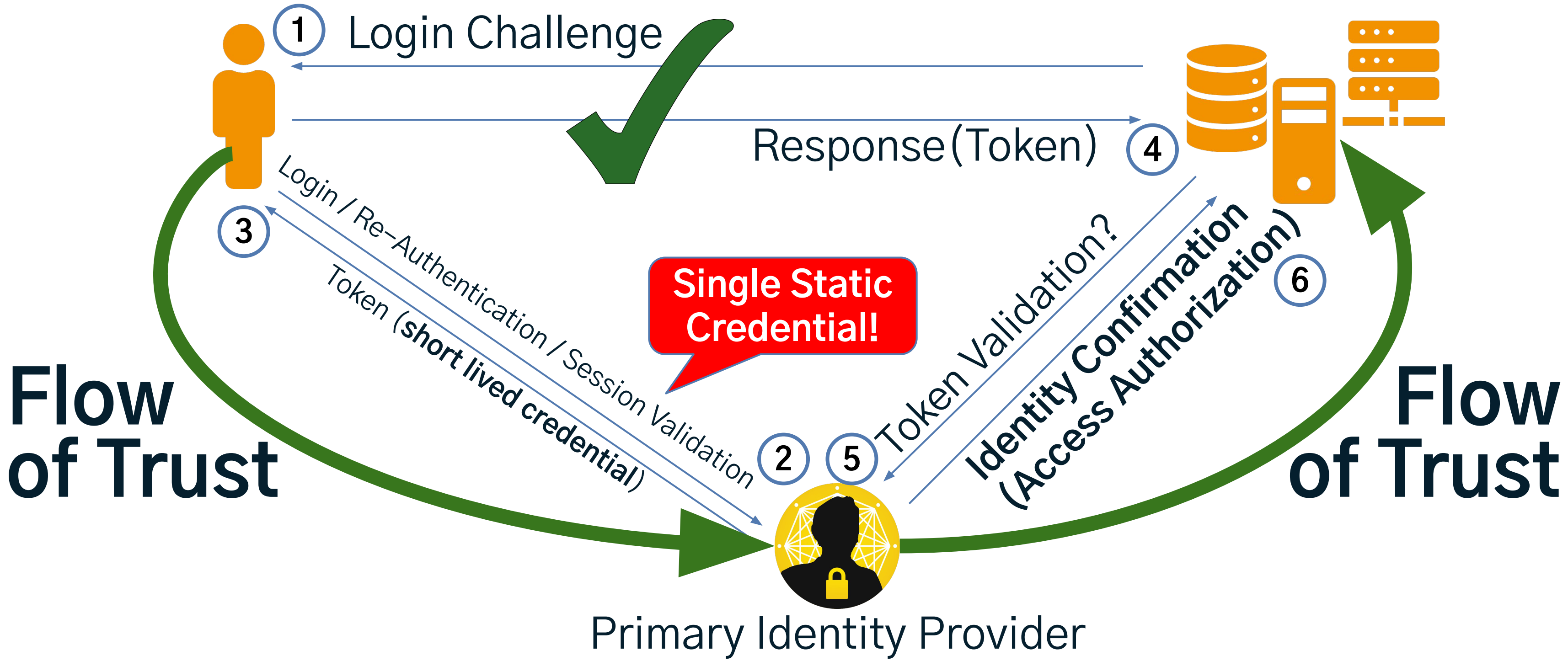
Root Cause: Static Credentials = offline check



Steal the secret and gain access

Anybody with a valid secret is welcome

Solution: **Identity** verification = **online** check



1
Login Challenge
Response(Token)
4
Login / Re-Authentication / Session Validation
3
Token (**short lived credential**)
Single Static Credential!
2
5
Token Validation?
Identity Confirmation (Access Authorization)
6
Flow of Trust
Flow of Trust
Primary Identity Provider

Trusting Digital Identities instead of Secrets

Secrets:

- ➢ can be used by anyone who has them – friend or foe
- ➢ are typically very short and can even be brute forced or guessed
- ➢ for machine- or service-users have to be stored in configuration files from where they can be leaked
- ➢ are hard to remember for humans so that they will write them down somewhere or store them in files
- ➢ typically stay the same over a long period of time
- ➢ don’t include any information about the identity of the bearer or user
- ➢ are hard to rotate on a regular base because the change has to happen in several places at the same time

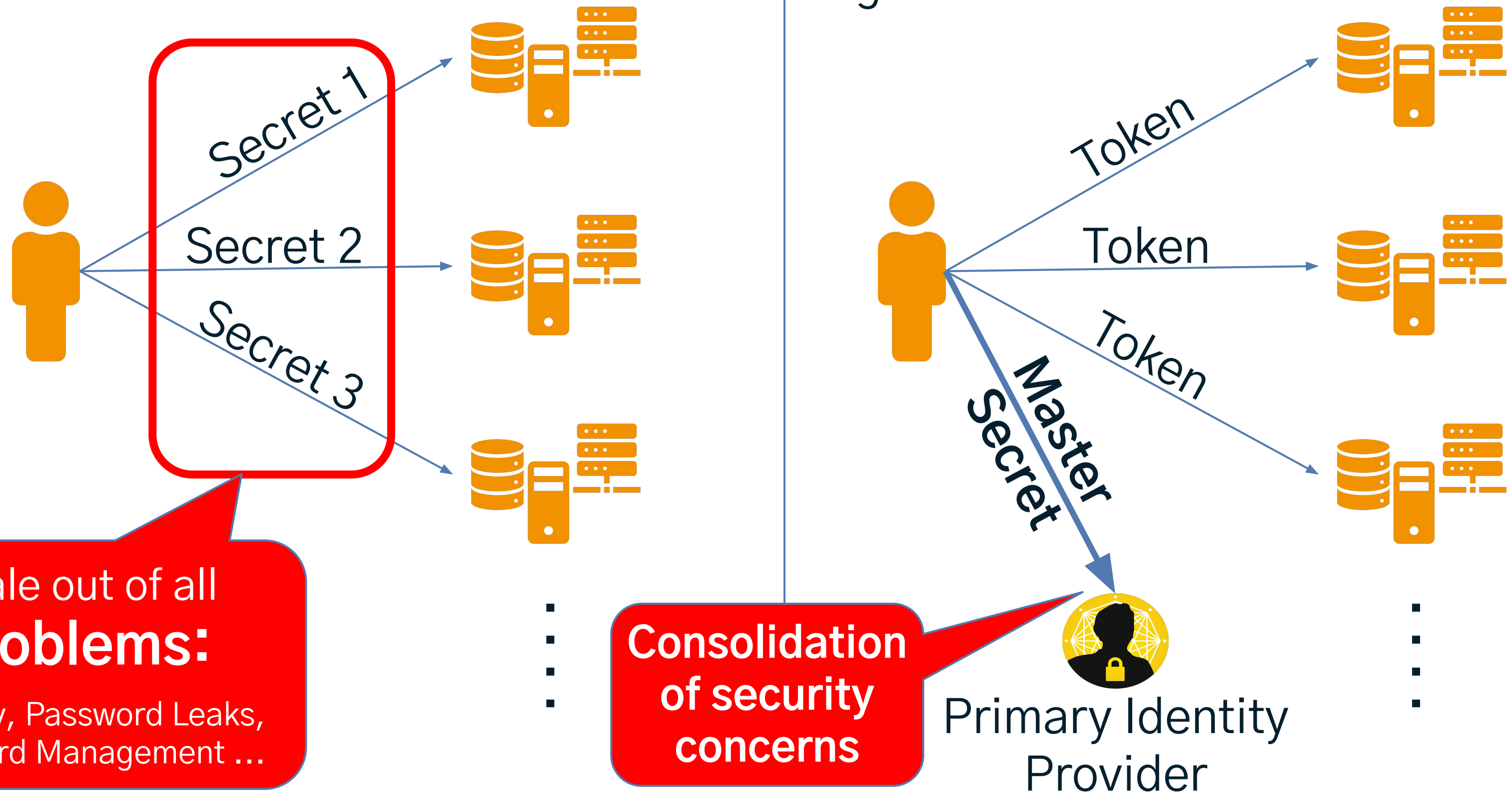
Digital Identities:

- ➢ rely on a strongly protected primary identity
- ➢ can be used only by the owner
- ➢ strong assertion of identity
- ➢ can provide additional personal information
- ➢ provide short-lived / temporary secure credentials for authentication
- ➢ frequent credential rotation by design
- ➢ work for machine authentication with the help of machine identities

Trusting Digital Identities instead of Secrets

Secrets

Digital Identities

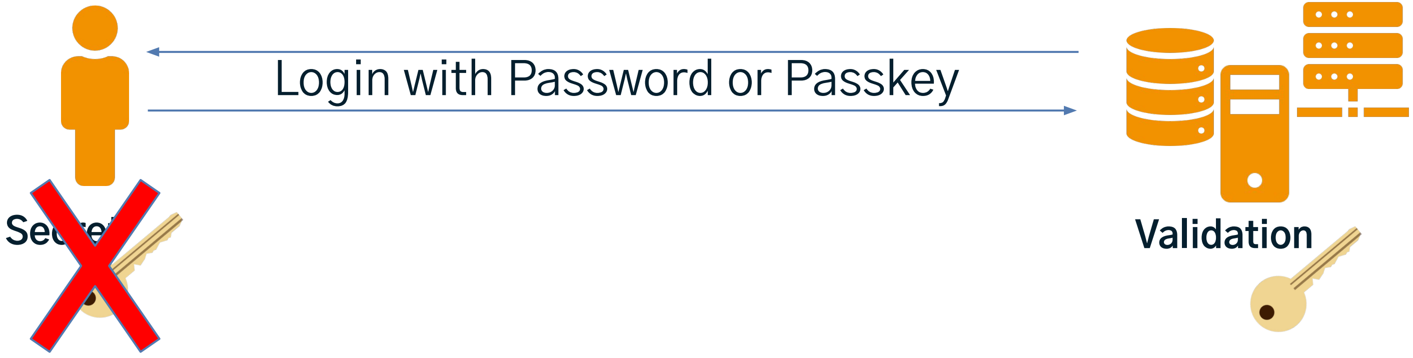


Scale out of all **problems:**

Security, Password Leaks, Password Management …

Consolidation of security concerns

The Lost Password Problem

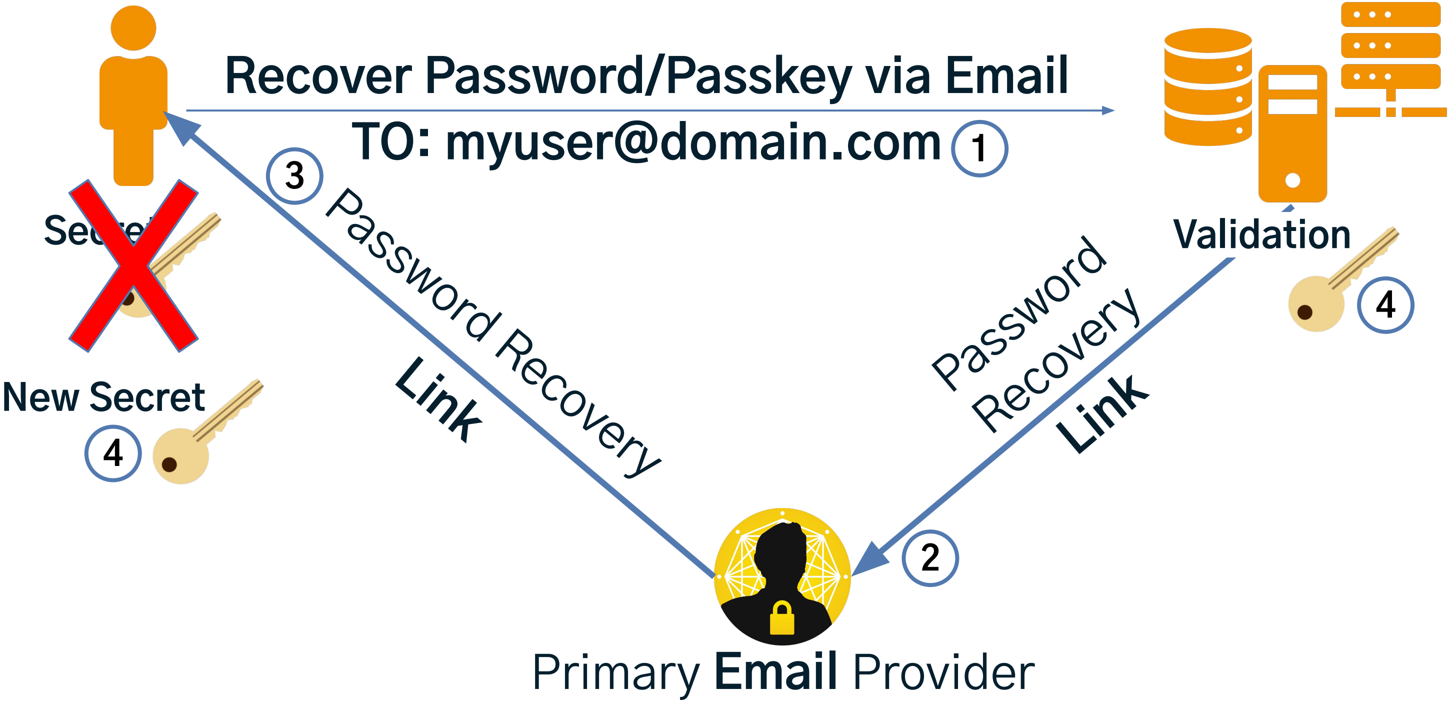


Login with Password or Passkey

Secret

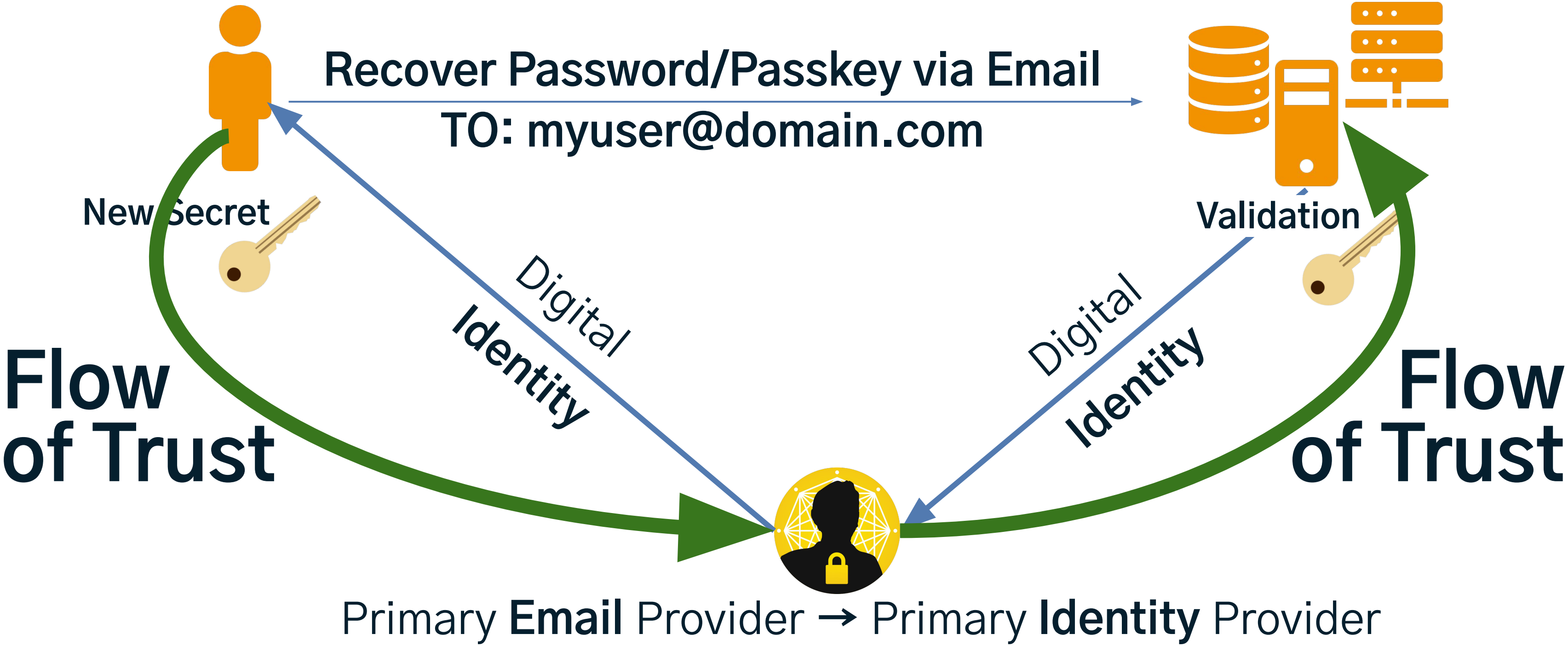
Validation

Solution: Email Password Reset



TEKTIT CONSULTING

Email as Identity → ~~Poor Man's~~ Consumer SSO



Practical Advice

What should we do instead for Consumers?

- **Accept** the fact, that your primary email is your **digital identity**
- Use **strong protection** for your primary email (multi–factor authentication)
- Use password managers, trust your primary browser
- Take care of **backup and disaster recovery** for your email
  - must use own domain instead of big provider (no gmail.com, outlook.com, web.de ...)
  - local provider, to recover access via letter & copy of ID
  - off–cloud backup of email content separate from your regular work environment
    → Outlook is **not** a backup!
  - what happens when you are gone? Think about "digital continuity" for your family

What should we do instead for Enterprise?

- **Eradicate static credentials** for all internal systems – on premise & Cloud
- Use **strong protection** (multi-factor authentication)
- Use your primary **account** as **only digital identity**
- Use password managers, trust your primary browser
- SSO with **pass-through authentication**, federated logins
- Use **machine identities** for machine communication
- off-cloud **backup** and offline **disaster recovery** capabilities
- … and, **learn** from the mistakes of others!

Use existing Identity Federation Solutions!

Examples:

- Desktop Windows/Mac/Linux: Kerberos pass-through authentication
- Websites: SAML2, SCIM, OpenID Connect ...
- Mobile Apps sign-in: iOS with Apple ID, Android with Google Account
- Customer/Consumer: Email Magic Link & Passkeys
- Kubernetes: SPIFFE/SPIRE
- AWS: Identity Federation & IAM Roles for Service Accounts
- GCP: Workload Identity Federation
- Azure: Microsoft Entra Workload ID
- GitHub: IAM with SAML for single sign-on (SSO)
- GitHub Actions: Workload Identity Federation for Deployments
- ...

Fixing the basics is really hard → Hands-Off Ops

- No manual changes in production
- Dev & Ops have same permissions in production: None by Default
- Automate the ***hard*** stuff:
  - Compliance & governance
  - Distributed rolling upgrades
  - Consistent Backup & Disaster Recovery
  - Everything in your stack
- Test Driven Everything
- Standardized Tooling
- Remove static credentials
- **Fix the Basics!**

GitOps

The Role of GitOps in IT Strategy v2

Schlomo Schapiro, 21.09.2022, DevOpsDays 2022

schlomo.schapiro.org

TEKTIT CONSULTING

Lifting the Curse of Static Credentials:

Let’s get out of the stone age,
and start the future!
Resolve the biggest security problems!

Read more in my blog at 🌐schlomo.schapiro.org

1. Lifting the Curse of Static Credentials
schlomo.schapiro.org/2016/05/lifting-curse-of-static-credentials.html
2. Eliminating the Password of Shared Accounts
schlomo.schapiro.org/2017/06/eliminating-password-of-shared-accounts.html
3. A Login Security Architecture Without Passwords
schlomo.schapiro.org/2022/02/login-security-architecture-without-passwords.html

Q&A — How may I help you?

schlomo.schapiro.org

We are not consultants. We are Partners, Coaches, Humans, Enablers, Catalysts, Sparring Partners, Experts … and sometimes a little annoying.

I focus on **IT strategy**, IT governance, technology and architecture management, security and compliance automation, related organisational changes, business continuity, open source and cloud technologies – and I'm available as a Principal Engineer or Technical Product Owner for short-term / interim support.

Examples:

- ➢ **Business-IT alignment & leveraging**, developing required skills and abilities for 21st century IT, leverage AI
- ➢ **SaaS compliance & governance**, data possession vs. ownership, IAM, integrations, backup & DR, shadow IT
- ➢ **Compliance Automation**, finding the "golden path" to a "golden state" via **Platform Engineering**
- ➢ **Secrets Management** for Datacenter, Cloud Infrastructure, IaaS/PaaS/SaaS
- ➢ **Open Source**, from usage to contribution, writing policies, using SBOM, establishing Open Source Stewardship
- ➢ **Good Engineering Practices**, GitOps, test driven development, good architecture decisions, known tech strategy
- ➢ **Business Continuity and Disaster Recovery** for office, Cloud infrastructure, data center & SaaS, with quality assurance, emergency communication & collaboration, hot & cold standby, no-restore solution, ransomware protection, Linux Disaster Recovery / Bare Metal Restore with "Relax and Recover (rear)" Open Source tooling

schlomo.schapiro@tektitconsulting.com