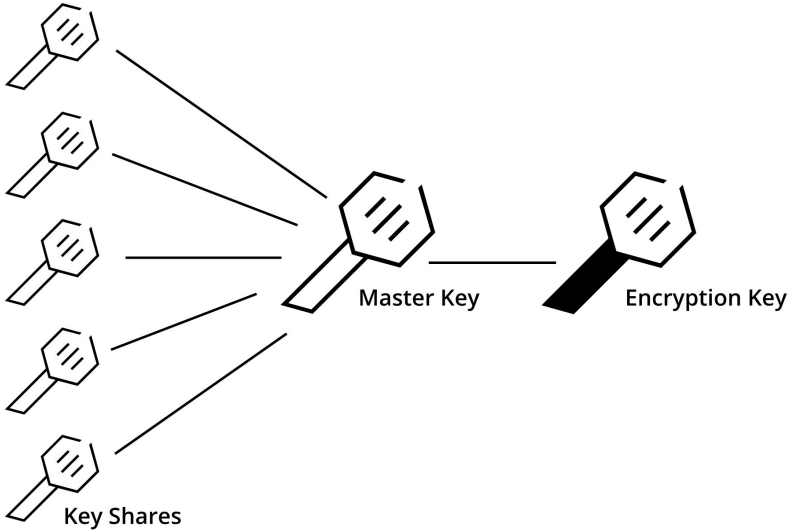


Universität Potsdam

HPI Hasso Plattner Institut
Digital Engineering · Universität Potsdam

Secrets Management

Johannes Kroschewski
Nils Straßenburg
Network Security In Practice - Midterm Presentation

Agenda

- Attack Classification
- Motivation
- Basics
- Challenges
- Existing solutions
- Example: Vault
- Further work

Attack Classification

Johannes Kroschewski
Nils Straßenburg
Network Security In Practice - Midterm Presentation

Attack Classification

- An **attack** is realization of threat, the harmful action aiming to find and exploit the system vulnerability. [1]

- ...rapid growth of cyberspace has also contributed to unethical practices by individuals who are bent on using the technology to exploit others. Such exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks and stealing both data and money is termed as **cyber attack**. [2]

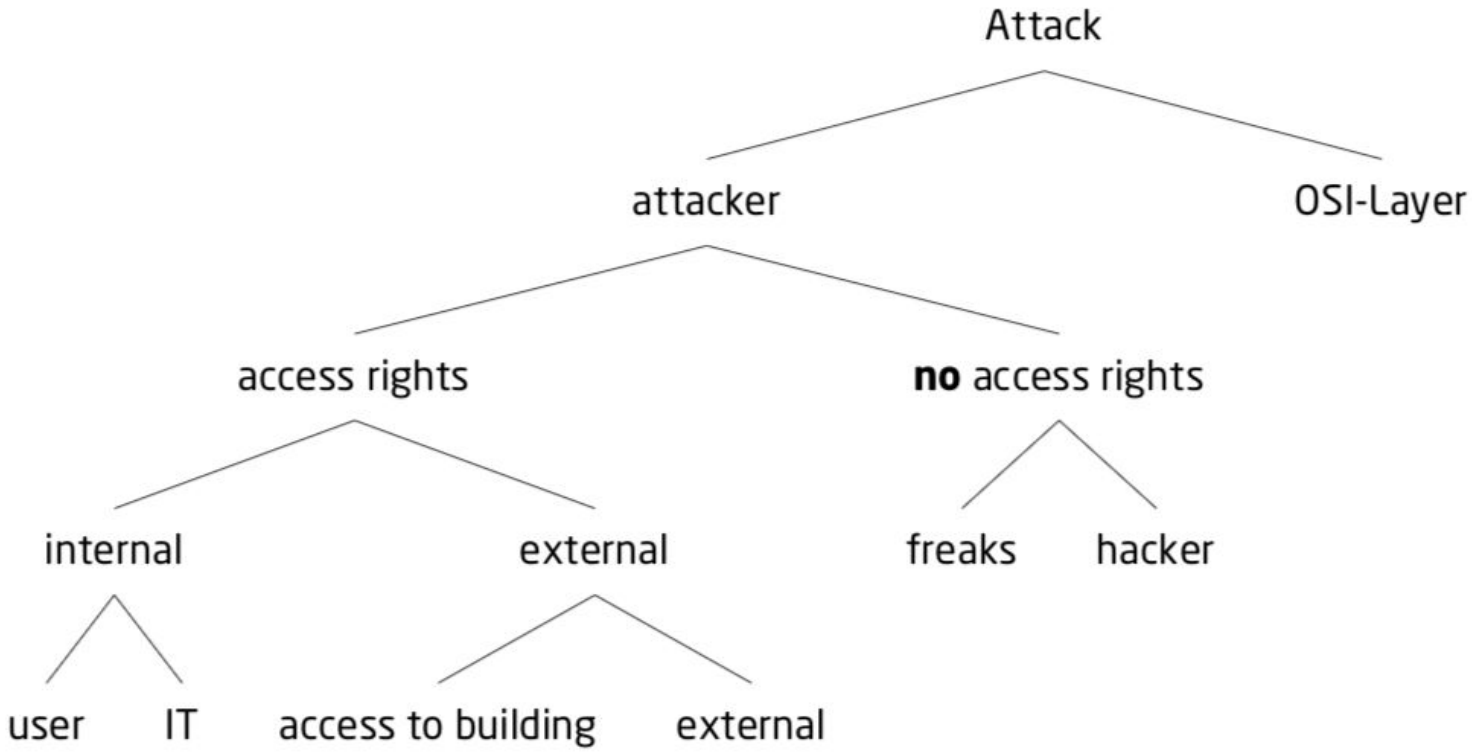
[1] Paulauskas, N., and E. Garsva. "Computer system attack classification." Elektronika ir elektrotechnika 66.2 (2006): 84-87.

[2] Uma, M., and Ganapathi Padmavathi. "A Survey on Various Cyber Attacks and their Classification." IJ Network Security 15.5 (2013): 390-396.

Attack **Classification**

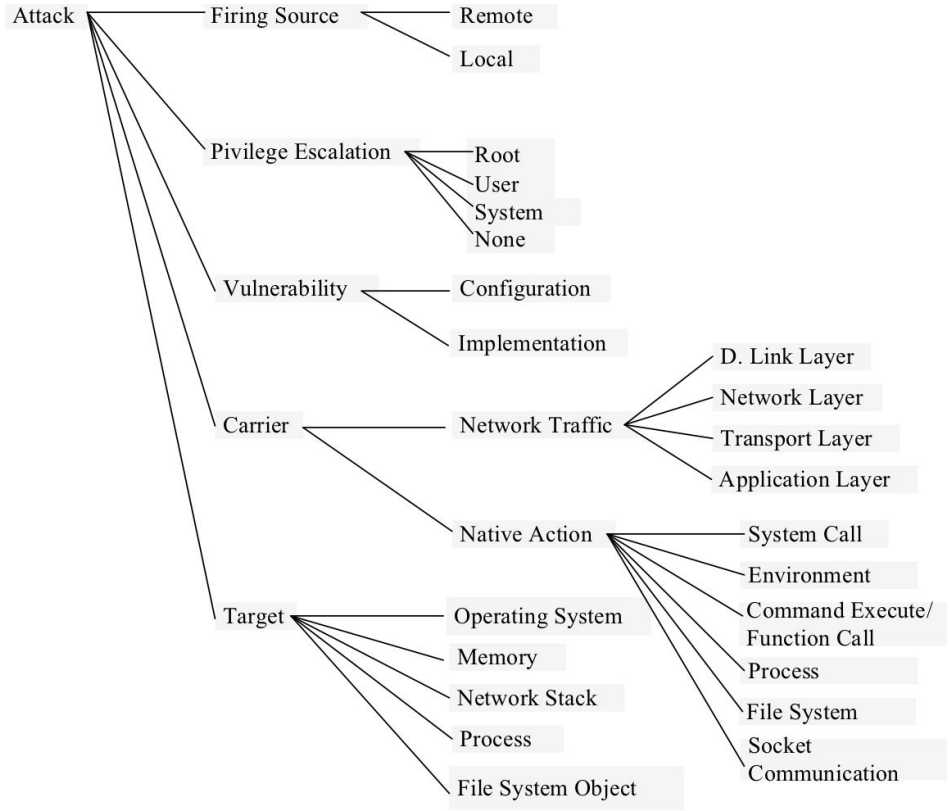
- Searching for a way to classify attacks
- Papers and books told us:
  - Headlines like: stealing passwords, social engineering, ...
  - Description of typical attacks
  - Helps: getting an overview
  - But still: **How could attacks be classified?**
- We as computer scientists like
  - A well structured model with categories
  - Graphs -> trees

Attack Classification



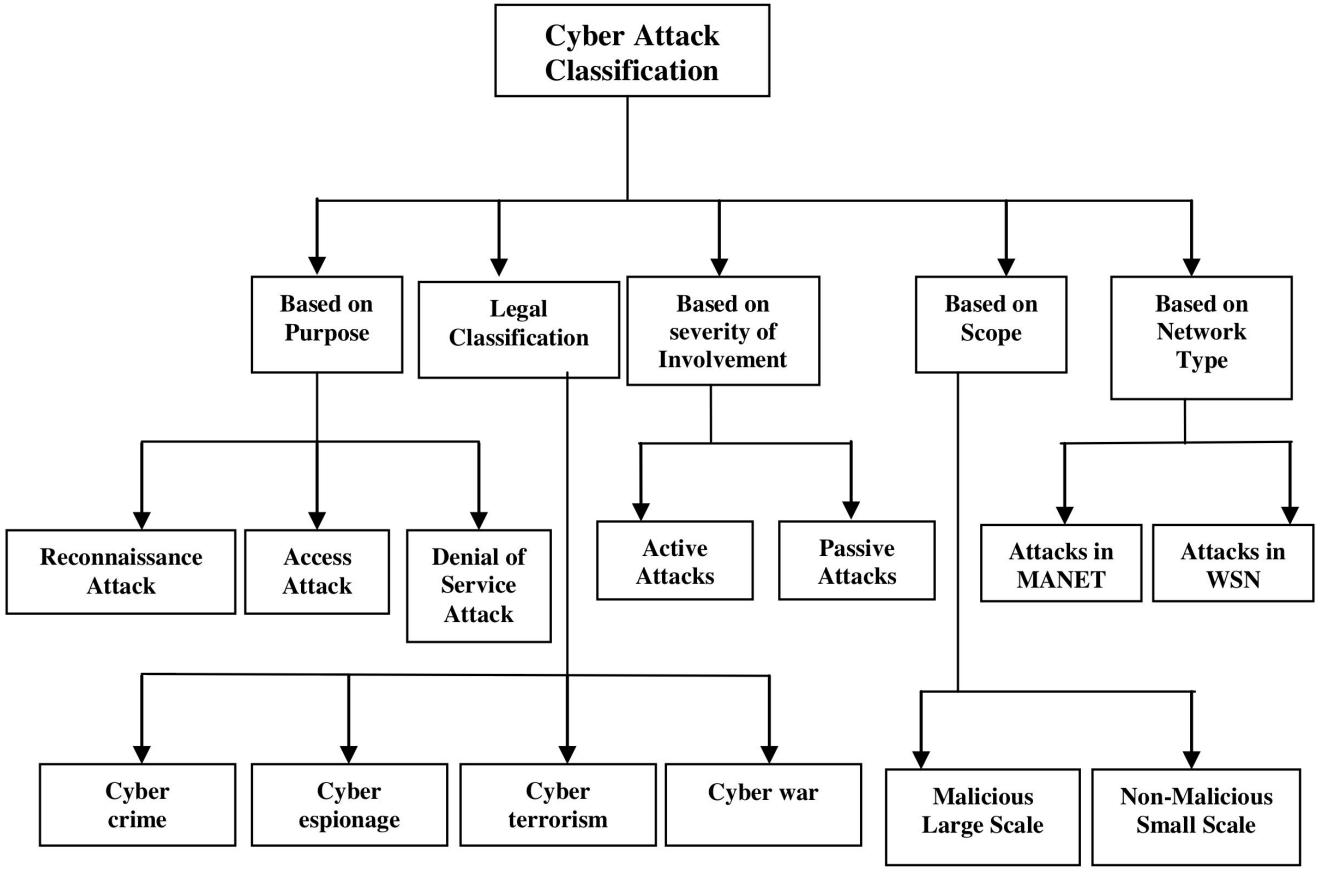
[1] Andreas Hanemann, Sicherheitstechniken in kommunikationsnetzen, Technische Hochschule Lübeck, 2017.

Attack Classification

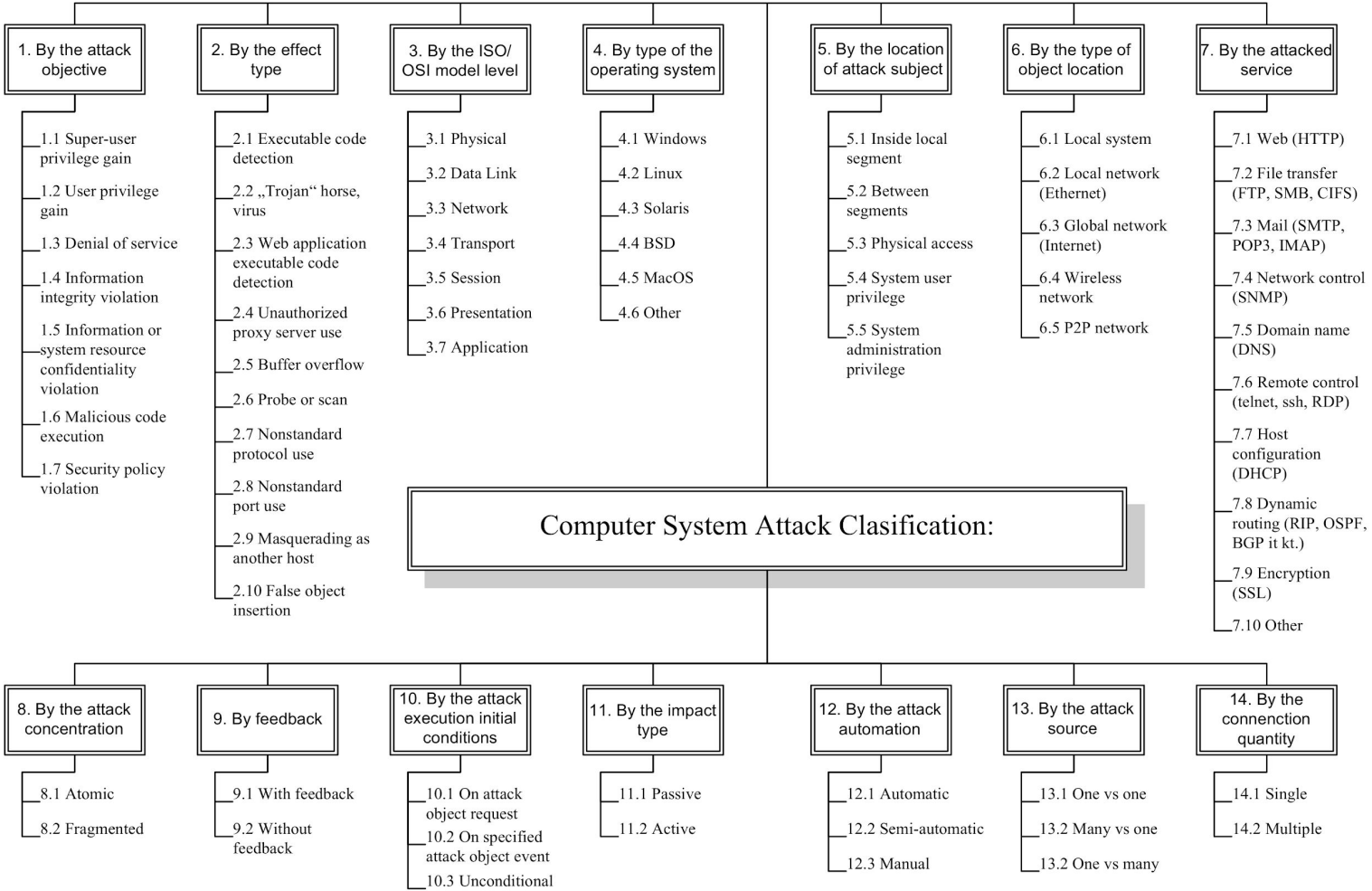


[1] Gadelrab, Mohammed S., et al. "Defining categories to select representative attack test-cases." Proceedings of the 2007 ACM workshop on Quality of protection. ACM, 2007.

Attack Classification



[1] Uma, M., and Ganapathi Padmavathi. "A Survey on Various Cyber Attacks and their Classification." IJ Network Security 15.5 (2013): 390-396.



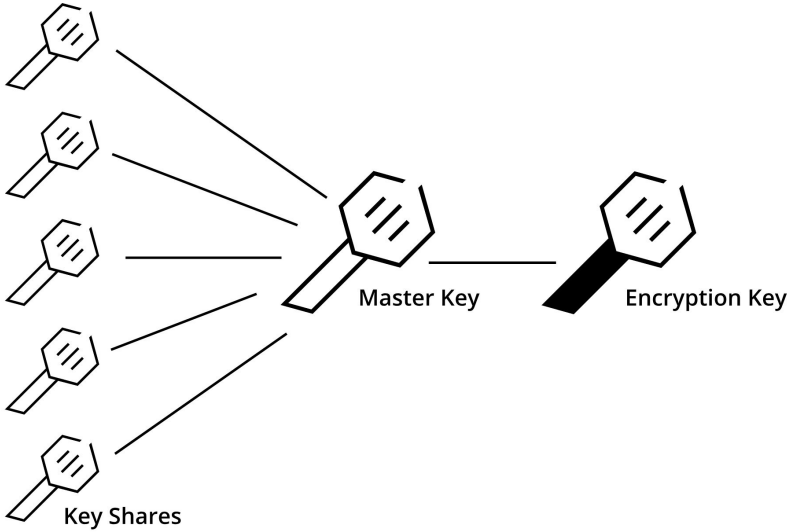
[6] Paulauskas, N., and E. Garsva. "Computer system attack classification." Elektronika ir elektrotechnika 66.2 (2006): 84-87.

Secrets Management

J. Kroschewski
N. Straßenburg
January 14, 2018
Chart **9**

Attack Classification - The Perfect Model

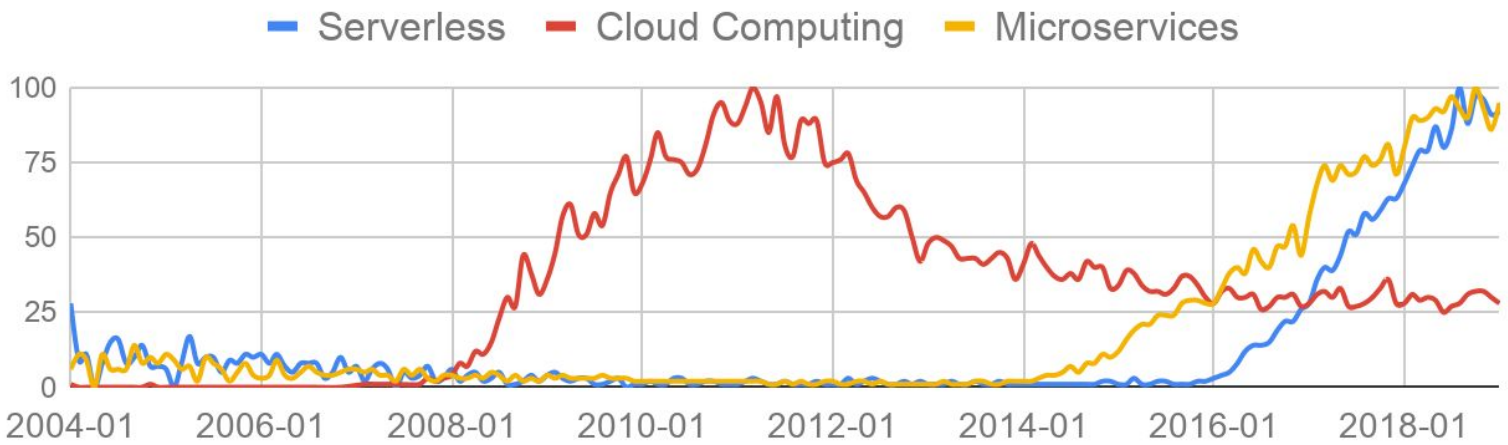
- Is there *the* perfect model for attack classification?
  - No!
- Which model is chosen should depend on points like:
  - The architecture
  - The use case
  - The definition of attack
- Always keep the context in mind:
  - E.g. when you just want to analyse/model costs that you have in consequence of an security issue it is not of interest to classify the attacker in detail



Secrets Management

Johannes Kroschewski
Nils Straßenburg
Network Security In Practice - Midterm Presentation

Motivation - Movement - Cloud Computing

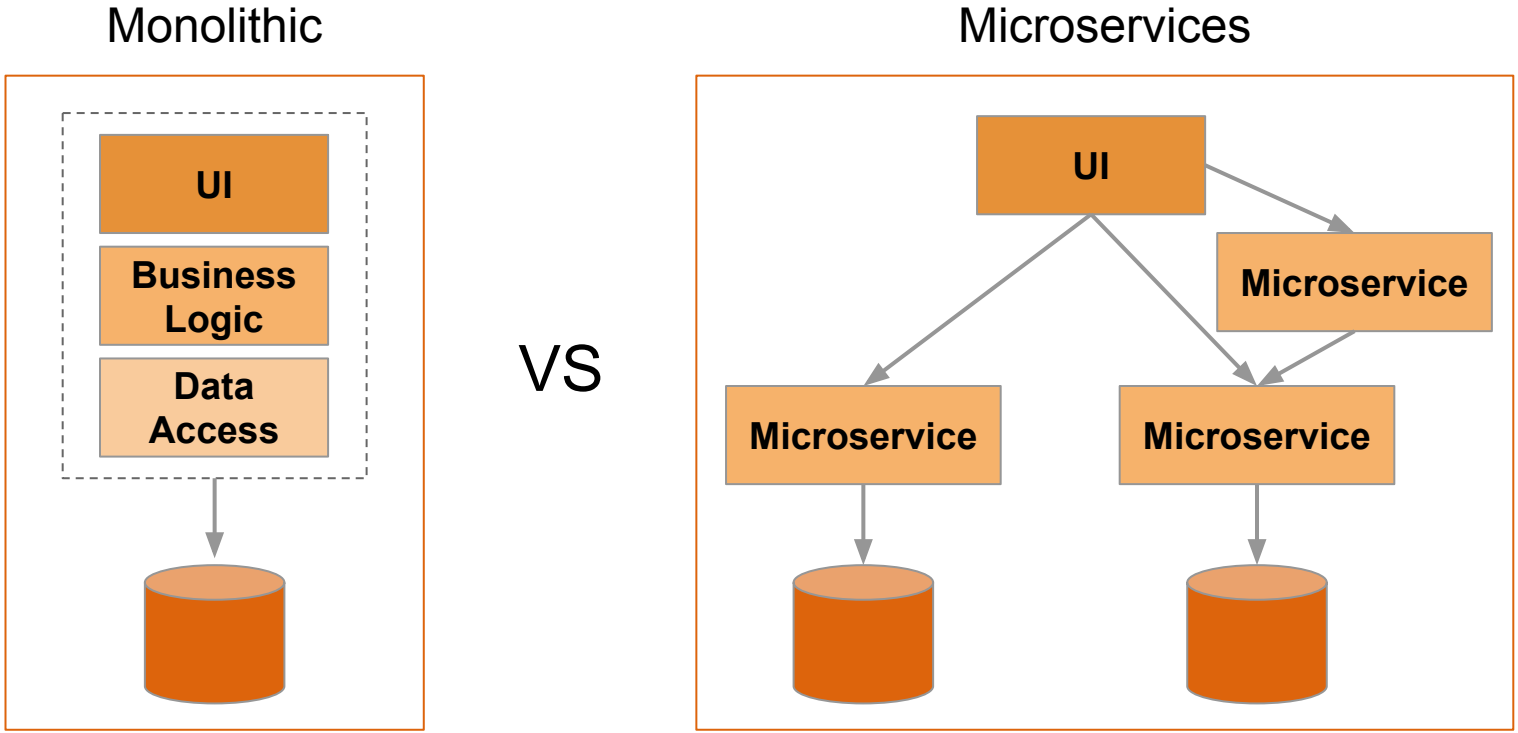


Interest over Time

"The IBM Institute for Business Value found that most enterprises — **85%** — already operate in multicloud environments." October 19, 2018 [7]

[7] Survey: Most companies use multicloud, but far less have tools for management

Motivation - Movement - Building Applications



Motivation - Challenges you should think about

- Move to the cloud
  - Breaks the assumption that the network parameter is secure
- In a world of extreme decentralization, how can you ...
  - distribute a secret to its application?
  - update a secret?
  - revoke a secret?
- Breaches happen, no security is perfect
  - How do you detect that a breach happened?
  - What data was accessed?
    - Employees are involved in **71%** of all cybersecurity incidents in healthcare [8]

[8] Verizon's 2018 Data Breach Investigations Report

Secrets Management - Basics - Secrets

- What is a secret?
  - Anything that grants access
- More precisely: anything that can be used to
  - **Authenticate**
  - **Authorize**
- For example
  - Username and password
  - API Token
  - Certificates

Secrets Management - Basics - Anti Patterns

- Do secrets change over time?
  - Ideally, yes!
  - If secrets not changing over time, they are not secrets for very long
- Secret sprawl: secrets are defined everywhere
  - Hardcoded in application
  - In config files
  - GitHub, Dropbox, Wiki, ...
- Sharing of credentials
  - Every app uses the **same** username and password
- Save passwords in plain text
- ...

Secrets Management - Definition

- Distribution of secrets to the end application?
  - E.g.: server needs access to DB
- Update secrets?
  - E.g.: credentials should not last forever
- Revoke secrets?
  - E.g.: manage to case that a system is compromised
- Define a **life cycle** of a secret ...

Building a process around these points is Secrets Management

Secrets Management - Related Work

- There are literally no papers about Secrets Management
- Some patents that were helpful:
  - Method and system for generation and management of secret key of public key cryptosystem, 1998 [9]
  - Scalable and automated secret management, 2012 [10]
  - Method for obtaining vetted certificates by microservices in elastic cloud environments, 2016 [11]
- Many custom solutions in industry
  - Are Security + Scheduling their core competencies?

[9] Method and system for generation and management of secret key of public key cryptosystem

[10] Scalable and automated secret management

[11] Method for obtaining vetted certificates by microservices in elastic cloud environments

Secrets Management - Distinction

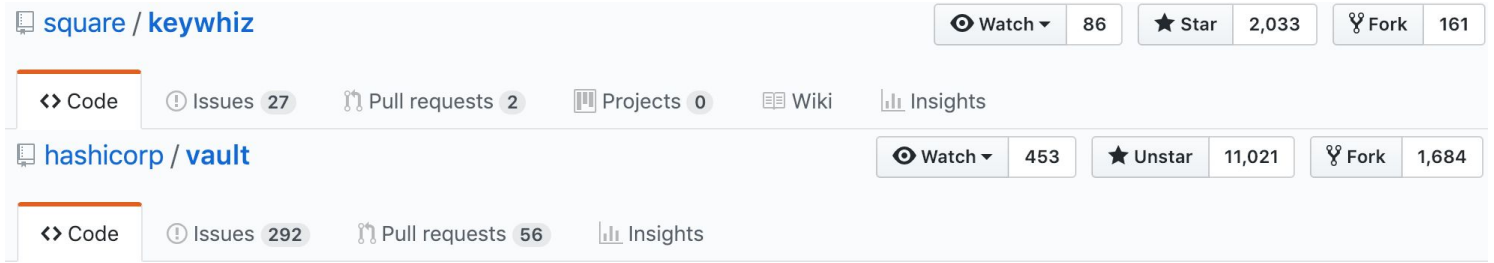
- What's different to password managers, e.g Keepass, Keychain, 1Password?
  - How are secrets managed for server applications?
    - Web Server talks to a database
- Secure Cloud Storage solutions?
  - Securing secrets and application data?
  - Considering multi-cloud strategies?
  - Does it define a life cycle for a secret?
- Does a centralized solution like *zookeeper*, *consule* help?
  - None of them are designed to keep everything secret
  - They are assuming they are used for much less information

Secrets Management - Attack Classification?

- Specific attack classification necessary?
  - Actually a “normal” software product
  - En-/Decrypts data
  - Saves encrypted data
- Attack classification for software discussed already
- Special attack classification just for cryptography?
  - Security is either broken
    - Collision found, Quantum computers, P = NP, ...
  - or brute force is used

Secrets Management - Existing Solutions

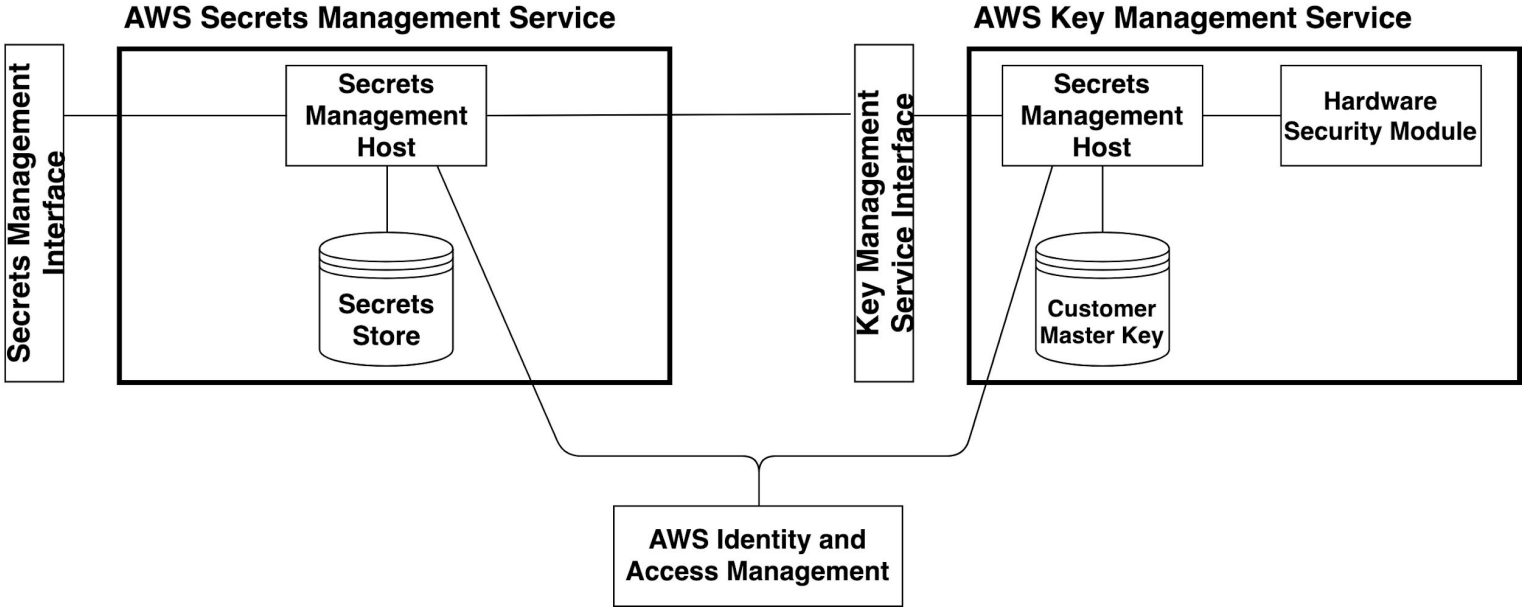
- Orchestrators
  - Docker-Swarm, Kubernetes, AWS, Apache Mesos, ...
- Open Source



A tool for secrets management, encryption as a service, and privileged access management https://www.vaultproject.io/

- Hardware Security Module (HSM)
  - Compliance requirements (e.g. FIPS 140)?
  - Very pricy!

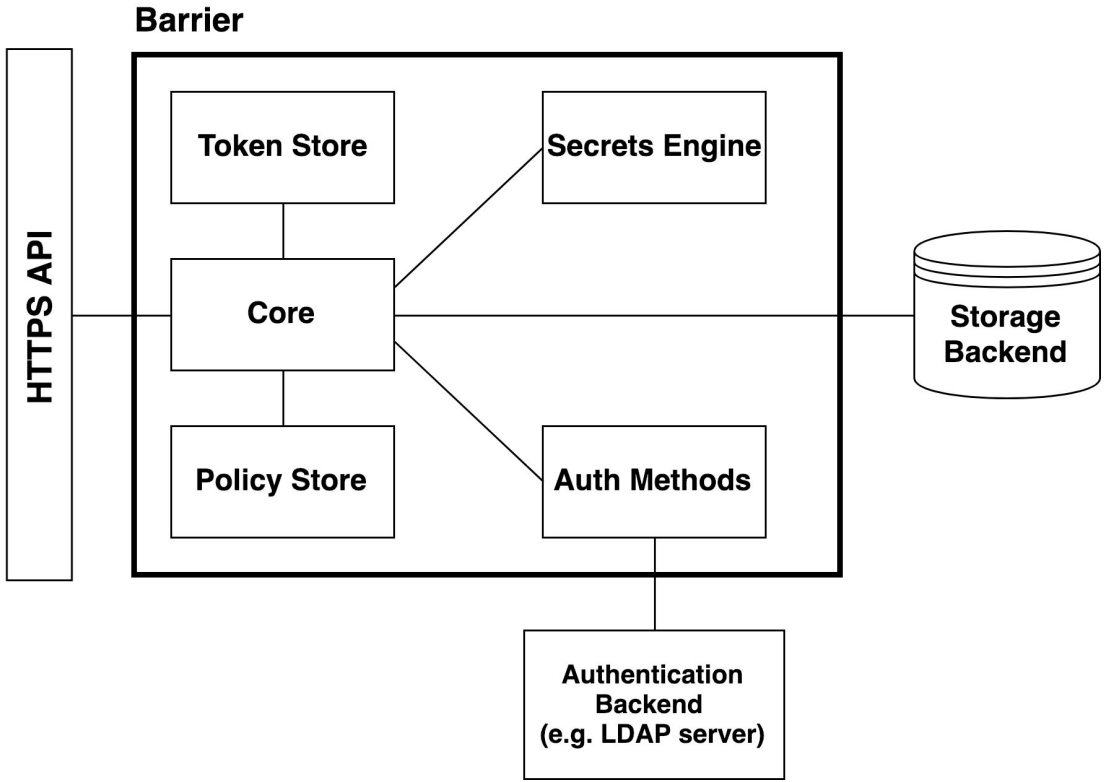
Secrets Management - Example - AWS



[12] AWS Key Management Service Cryptographic Details (August 2018)

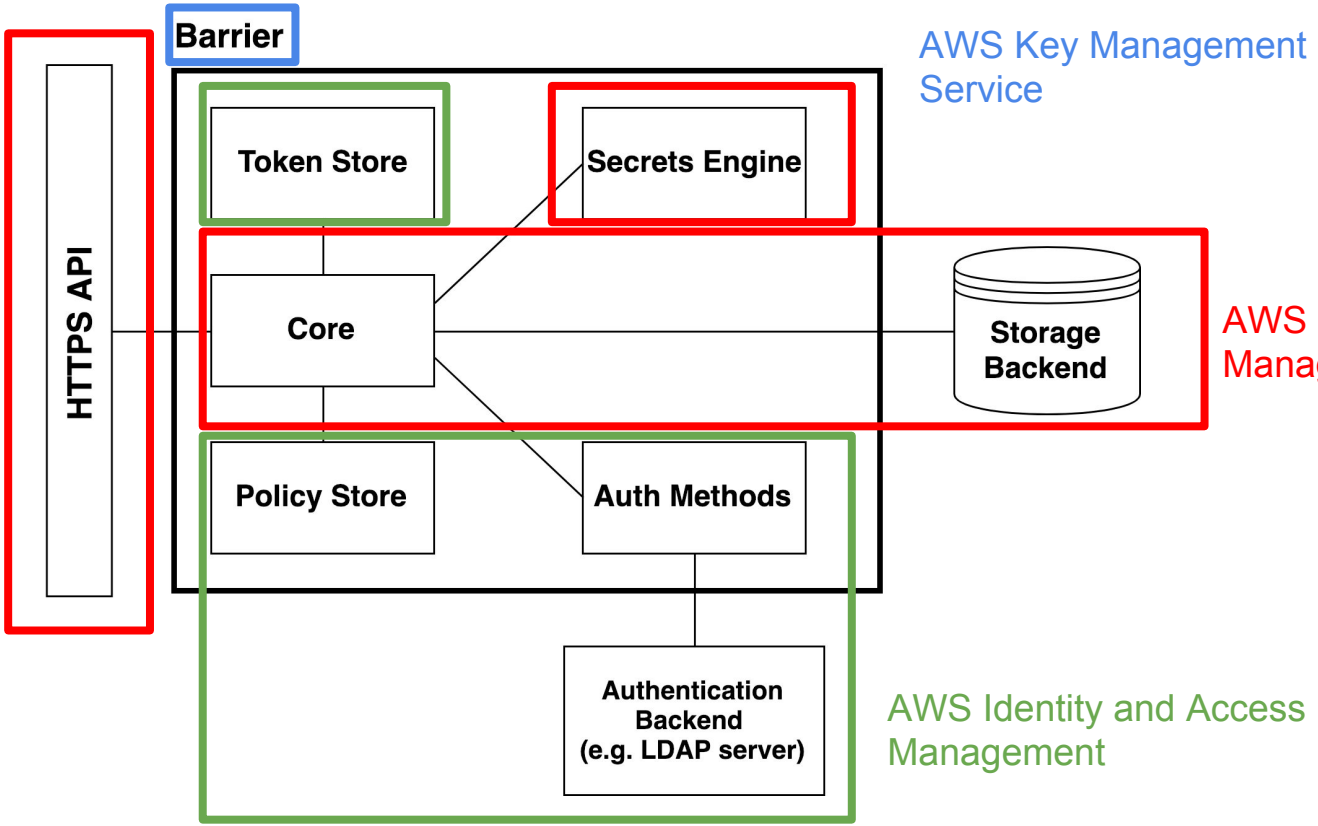
[13] How AWS Secrets Manager Uses AWS KMS

Secrets Management - Example - Vault



[14] Vault Architecture

Secrets Management - Mapping - Vault and AWS



[14] Vault Architecture

Secrets Management - Which solution?

- You need to answer …
  - What's your environment like?
  - What are your needs?
  - Does the system integrates into the environment you are using?
  - Security vs. Compliance?

- What are the first three things you need to do?
  - What are all our secrets and where are they?
  - Which application and who has access to what? (**Trust model**)
  - How can you enforce the trust model in a central place?

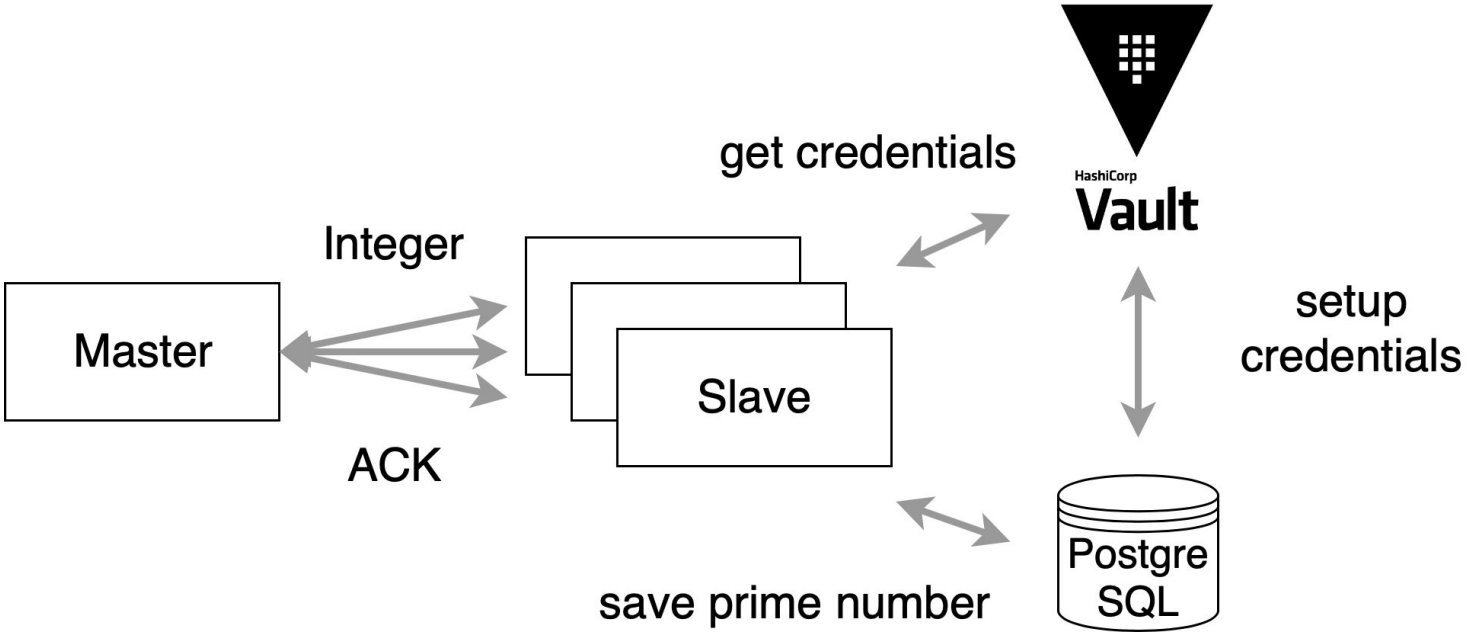
Secrets Management - Why Vault?

- It's been used by industry
- It's open source (Kerckhoffs's principle)
- It has a decent documentation, community, ...

- Is the orchestrator really the right place?
  - Solution which is designed to keep everything secret?
  - Kubernetes vulnerability, 12th Dec 2018, CVSS 9.8/10 **critical** [15]
- Security vs. Compliance?
  - Do you want/need to own the keys?

[15] CVE-2018-1002105

Example - Architecture



Example - Live Demo

[16] When I push a hotfix and it breaks production

Example - Attacks?

- **Single Point of Failure …**
- Example: Frequently changing secrets? Be careful!
  - Could have led to *DOS*
- What does *exploit-db.com* tell us?

Date	D	A	V	Title	Type	Platform	Author
2018-04-09	⬇		✕	CyberArk Password Vault Web Access < 9.9.5 / < 9.10 / 10.1 - Remote Code Execution	WebApps	JSON	RedTeam Pentesting
2018-04-09	⬇		✕	CyberArk Password Vault < 9.7 / < 10 - Memory Disclosure	DoS	Linux	RedTeam Pentesting

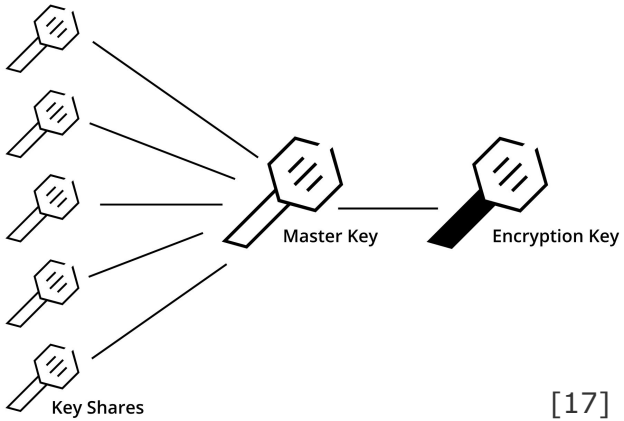
  - CyberArk: Commercial Secrets Management Solution

What comes next?

- What is our goal?
  - Technical comparison/evaluation of the current solutions
  - Best practice for sharing secrets in different scenarios

- Secret Sharing
  - Shamir's Secret Sharing!
  - Other approaches?

- Compare solutions
  - Ideas for criteria?
  - In what would you be interested?



[17]

[17] Vault Key Picture

We dedicate this presentations to our mothers Marianne and Sabine whose maiden names shall not be relevant because this is a security presentation

Thank you
for your attention!

Johannes Kroschewski and Nils Straßenburg

Secrets Management

Network Security In Practice - Midterm Presentation