FH MÜNSTER
University of Applied Sciences

Masterprojekte 2025

Prof. Dr. Sebastian Schinzel

E-Mail: schinzel@fh-muenster.de

Themen:

1. Preventing Transmission of Sensitive Data in Internet Scans
2. Large-Scale Log Parsing for Cyber Defense
3. FHIR Test Server Implementation

Preventing Transmission of Sensitive Data in Internet Scans

- Downloading sensitive data is „problematic“ legally and ethically, but hard to prevent while scanning the Internet

Research Question: Can we prevent the transmission of sensitive data at protocol (TCP) level while scanning?

Preventing Transmission of Sensitive Data in Internet Scans – **Project Goals/Tasks**

- For this project, you will …
  - … evaluate ways (TCP Receive Windows, TCP RST, …) to prevent further data transmission.
  - … evaluate ways to implement this (e.g., eBPF, Preload Library with Raw Sockets, Kernel Module).
  - … implement and benchmark the module/library.
  - … potentially write a paper with the ITS Lab about this ☺
- Betreuer: Dr. Fabian Ising, Prof. Schinzel.

Large-Scale Log Parsing for Cyber Defense

Datetime	Message
...	
2016-10-05T10:39:01	[CRON pid: 1807] pam_unix(cron:session): session closed for user root
2016-10-05T10:39:01	[CRON pid: 1807] pam_unix(cron:session): session opened for user root by (uid=0)
2016-10-05T10:39:26	[sshd pid: 1822] pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 ...
2016-10-05T10:39:27	[sshd pid: 1822] Failed password for root from 192.168.210.131 port 57190 ssh2
2016-10-05T10:39:33	[sshd pid: 1822] Connection closed by 192.168.210.131 [preauth]
2016-10-05T10:39:33	[sshd pid: 1822] Failed password for root from 192.168.210.131 port 57190 ssh2
2016-10-05T10:39:33	[sshd pid: 1822] PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ...
2016-10-05T10:42:33	[sshd pid: 1833] Received disconnect from 192.168.210.131: 11: Bye Bye [preauth]
2016-10-05T10:42:33	[sshd pid: 1836] pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 ...
...	
Other 397,839 lines of records	

Log Parsing is critical for Cyber Defense, Incident Response and Digital Forensics

State-of-the-art: Forensic Experts Write Your Parsers

Research Question: How to automate log parsing using machine learning?

Large-Scale Log Parsing for Cyber Defense – **Project Goals/Tasks**

- For this project, you will …
  - … evaluate ways (differential analysis & LLMs) to automate & **generalize** log parsing
  - … develop a corresponding methodology and implementation
  - … evaluate and benchmark the module/library
  - … potentially write a paper with the ITS Lab about this ☺
- Betreuer: Lukas Schmidt MSc., Prof. Schinzel.

FHIR Test Server Implementation

FHIR (Fast Healthcare Interoperability Resources) ist ein Standard für den **elektronischen Austausch von Gesundheitsdaten**.

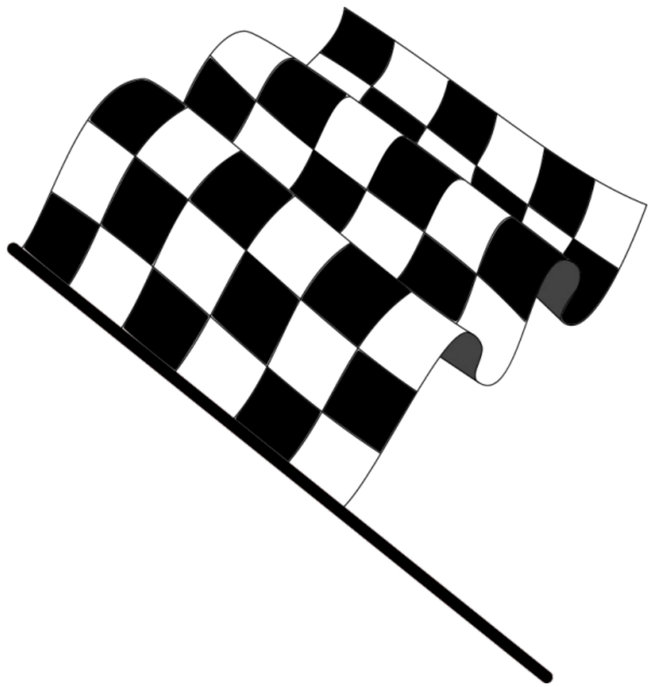
FHIR verwendet moderne Web-Technologien wie REST, JSON und XML, um eine einfache und flexible **Integration zwischen verschiedenen IT-Systemen im Gesundheitswesen** zu ermöglichen.

Ziel:

Installation und Konfiguration eines FHIR Servers und Implementierung von FHIR Skripten zu Forschungszwecken

FHIR Test Server Implementation
Projektziele & Aufgaben

- Installation und Grundkonfiguration von einem HAPI FHIR Server (inkl. der benötigen Komponenten wie z.B. eine Datenbank)
- Implementierung von Keycloak
- Implementierung von folgenden Authentifizierung Techniken für den HAPI FHIR Server:
  - Basic Authentication (Username/Password)
  - OAuth2 (auf basis von Keycloak)
  - SMART-on-FHIR (auf basis von Keycloak)
- Dokumentation (in Markdown) und weitgehende Automatisierung der Installation und Konfiguration von HAPI und Keycloak
- Entwicklung eines Clients (Script) zum Lesen und Schreiben von Patientendaten
- Betreuer: Nico Brüggemann MSc., Prof. Schinzel.



Interesse geweckt?

Melden Sie sich bei Prof. Dr. Sebastian Schinzel per Mattermost oder E-Mail: schinzel@fh-muenster.de