FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Pentest und Forensik einer Schneider SPS

Dipl.-Ing. Stefan Nagel

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Aufgabenstellung

Untersuchung einer Schneider M258 SPS

- auf ihre IT-Sicherheit (Pentest)
- auf ihre forensische Möglichkeiten

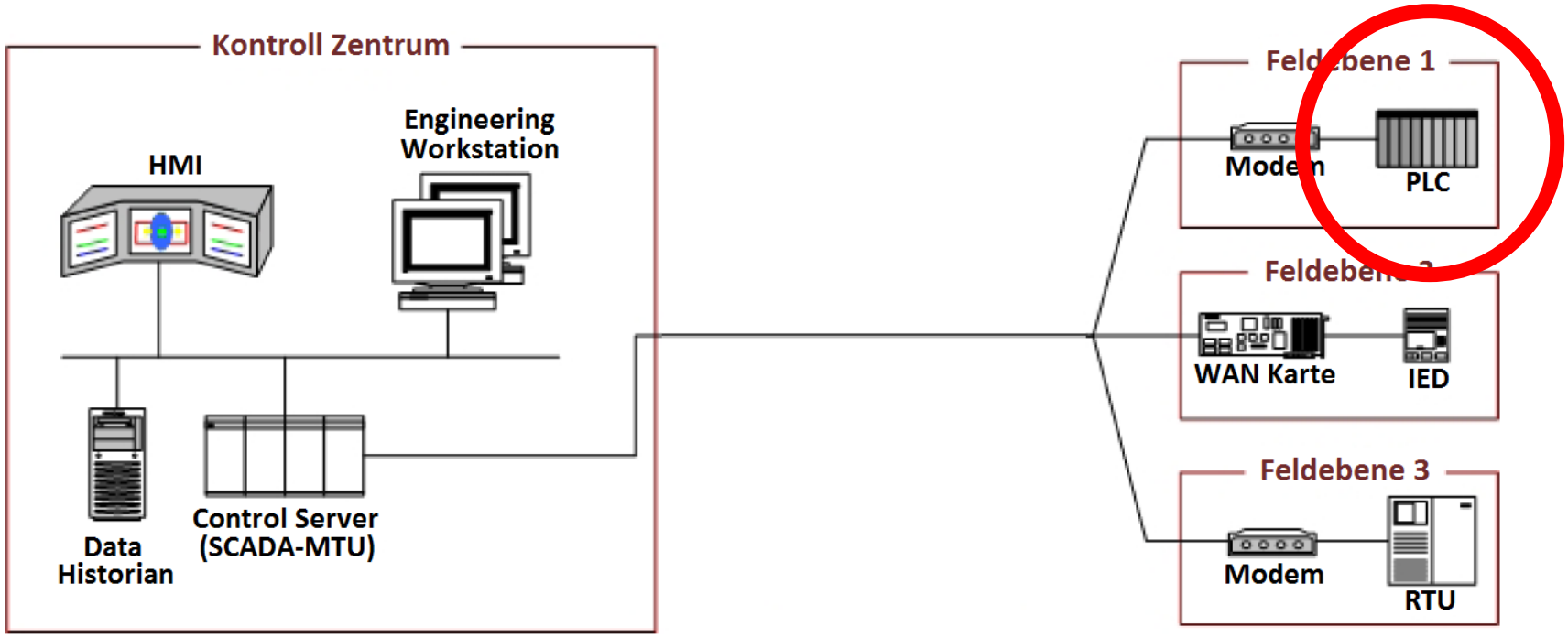
Agenda

- Einführung – Was ist SCADA ?
- Vorstellung Schneider M258 SPS
- Mögliche Angriffe
  - per Hardware
  - via Netzwerkprotokolle
  - via Webschnittstelle
- Fazit
- Kaffeepause

Einführung – Was ist SCADA

Supervisory **C**ontrol **A**nd **D**ata **A**cquisition

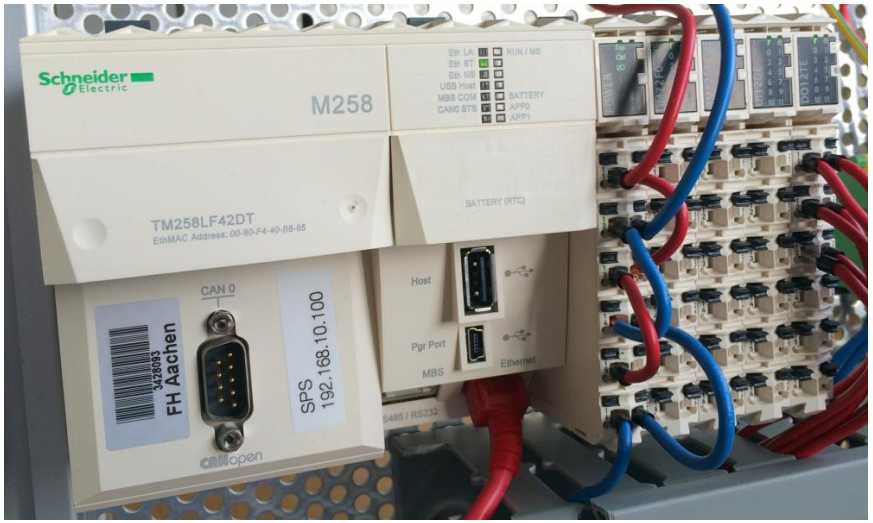
Netzaufbau:



Schneider M258 SPS

Schneider Modicon TM258LF42DT

- 64MB RAM (Anwendungsausführung)
- 128MB Flash (Programmdaten / Config)
- Linux OS
- Anschlüsse
  - Ethernet
  - RS232
  - USB-Programmierport
  - USB-Hostport
  - CAN-Port
  - Ein-/Ausgänge



Angriffe per Hardware

Firmwareupdate per USB-Stick (ZIP-Datei)

- Ausführen von /<version>/sys/Cmd/Script.cmd
- Mögliche Befehle:
  - Bootloader und Bootimage ersetzen
  - Dateien auf/von USB-Stick kopieren
  - Dateien löschen
  - SPS rebooten
  - Namen ändern
  - …

Angriffe via Netzwerk (1)

Verwendete Ports (Herstellerangaben):

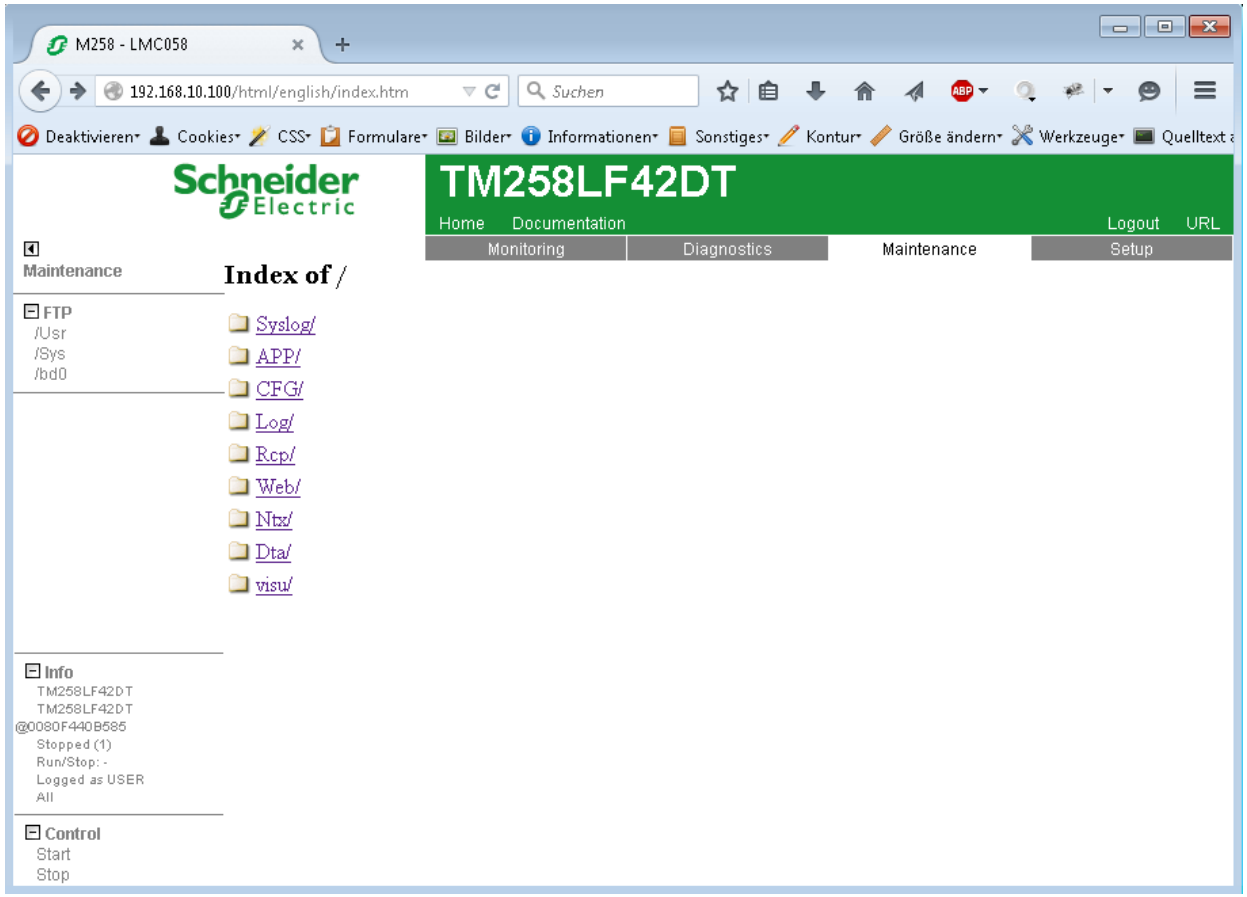
Protokoll	Zielportnummern
SoMachine	UDP 1740, 1741, 1742, 1743 TCP 1105
FTP	TCP 21, 20
HTTP	TCP 80
Modbus	TCP 502
Discovery	UDP 27126, 27127
SNMP	UDP 161, 162
NVL	UDP-Standardwert: 1202
Ethernet/IP	UDP 2222 TCP 44818

Angriffe via Netzwerk (2)

- Standard-Angriffe
  - DoS-Attacke
  - Brute-Force Attacke auf Passwort
    - Webinterface (hier nur Passwort)
    - FTP (User: „USER“)
- Angriffe auf Dienste
  - tcp/502 – Modbus
  - tcp/80 – Webserver
  - tcp/21 – FTP-Server
  - …
- Man-In-The-Middle

Angriffe via Webschnittstelle (1)

Verzeichnis-Index unter http://<ip>/ftp_usr/

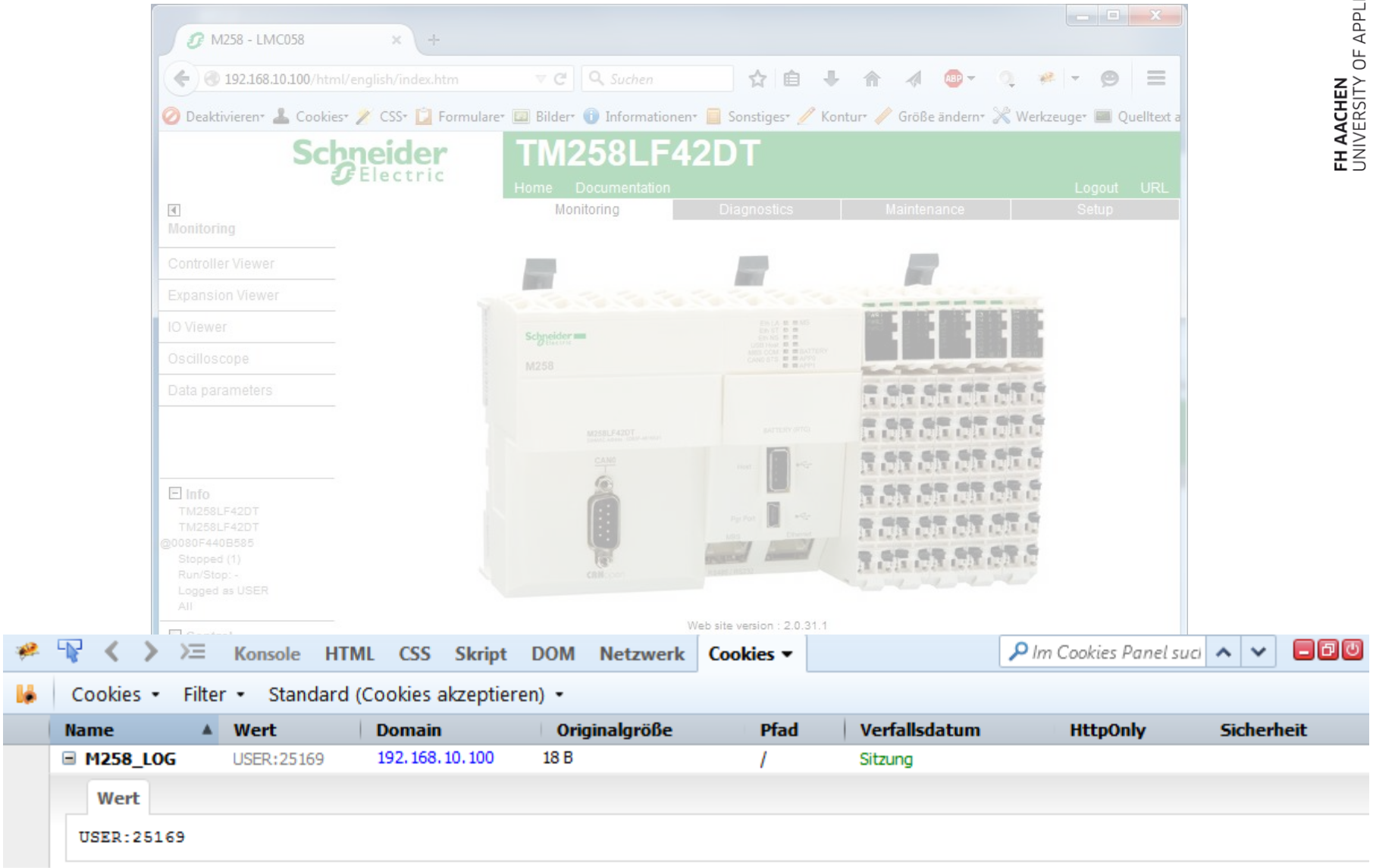


Angriffe via Webschnittstelle (2)

Authentifizierung an der Webseite

- Passwort-Login (Formularfeld)
- Setzt Cookie
- Cookie hat festen Wert
  - Benutzername
  - Authentifizierungslevel
  - Unabhängig von Zeit oder aktuellem Passwort

Angriffe via Webschnittstelle (3)



Weitere Angriffsmöglichkeiten

Noch zu untersuchen:

- CAN-Bus ?
- Serielle Schnittstelle (RS232) ?
- USB-Programmierport ?
  - Debug Modus ?
- Buffer-Overflows

Fazit

- Schneider SPS wie andere Hersteller auch leichtes Angriffsziel
- Betriebssystem Linux-basiert, deutlich sicherer als Embedded-Windows-Varianten
- Webschnittstelle mit gravierenden Sicherheitslücken
- Netzwerk- und physikalischen Zugriff vermeiden

Fragen

Hier könnte Ihre Frage stehen…

Applaus !

Vielen Dank für Ihre Aufmerksamkeit.

Kontakt: s.nagel@fh-aachen.de