FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IDS für das Siemens Communication Protokoll

Dane Wullen

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

Gliederung

- Einführung in die Problematik
- Stand der Technik
- Bro NIDS
- Entwicklung der Protokoll-Analyzer
- Demo
- Stand der Entwicklung

Einführung in die Problematik

- Zunehmende Vernetzung von industriellen Kontrollsystemen führt zu Gefahren durch Angriffe
  - Dadurch gewinnt die IT-Sicherheit an Bedeutung
  - Erfolgreiche Angriffe tragen hohe finanzielle sowie sachliche Schäden mit sich
  - Beispiel: Stuxnet (2011), Stahlwerk in Deutschland (2014)
- Industrielle Kontrollsysteme stammen aus isolierter Feldbus-Ebene
  - Keine Anbindung an Netzwerke, keine Sicherheitsfunktionen etc.
  - Systeme und Protokolle demnach heute unsicher

Einführung in die Problematik

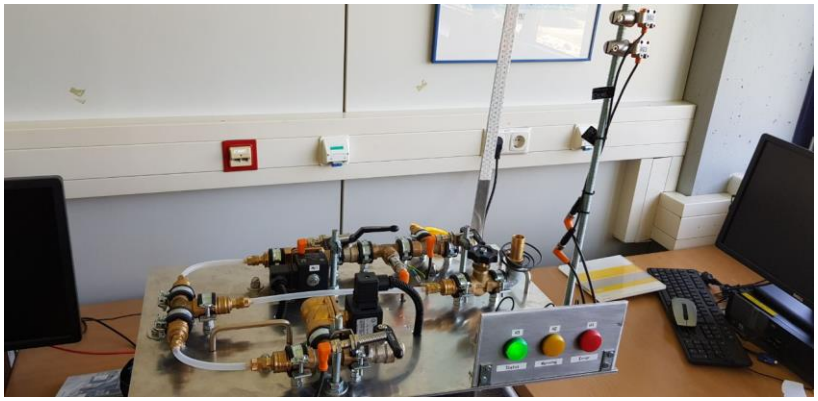
- Aktueller Bericht von Kaspersky (27.03.2018)
  - Analysiert ICS-Rechner verschiedener Branchen
  - Betroffen von min. einem Angriff:
    - ~39%: Energiebranche
    - ~35%: Maschinenbaubranche
    - ~31%: Baubranche
    - Andere: Versorgung, Telekommunikation, Gesundheitswesen, Bildungswesen etc.
  - Hauptquelle der Angriffe: Internet

https://www.kaspersky.de/about/press-releases/2018_cyberangriffe-gegen-industrie-rechner

Stand der Technik

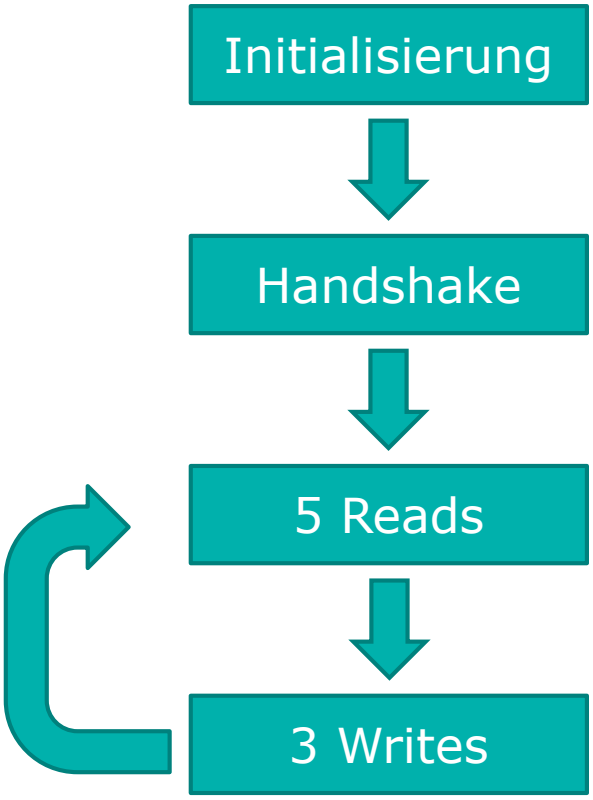
- Ziel der IT-Sicherheit: Angriffe erkennen, verstehen und verhindern
- Entwicklung einer Testanlage (J. Wollenweber, FH Aachen, 2018)
  - 2 Siemens SPS vom Typ S7-1200
  - Simuliert z. B. den Füllstand eines Tanks
  - „Opfersystem“ zur Durchführung / Erkennung von Angriffen

Stand der Technik



Stand der Technik

- Anlage hat festen Zyklus

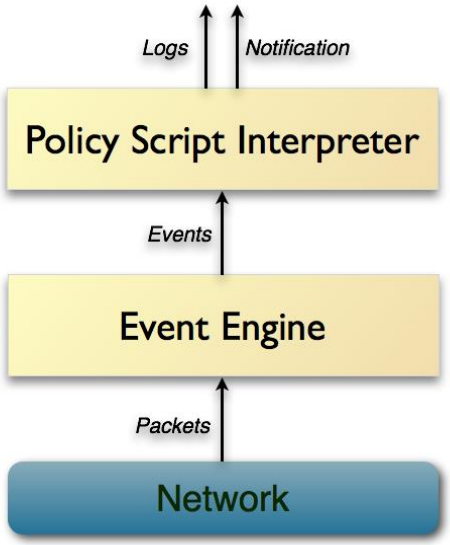


- 1. Read: Status der Sensoren
- 2. Read: Druck des Kompressors
- 3. Read: Status der Anlage
- 4. Read: Informationen über Regulation
- 5. Read: Fehlermeldungen

- 1. Write: Aktiviere Akteure
- 2. Write: Standardwerte setzen
- 3. Write: E-Stop (Notaus)

Bro NIDS

- Open Source Projekt, 1999
- Geschrieben in C++, Quellcode offen
- Network Security Monitor / Intrusion Detection System
- Passiv, greift nicht in Datenverkehr ein
- Event-basiert, Policy-Skripte mit eigener Skript-Sprache
- Umfangreich an Protokoll-Analyzern, u. a. DNP3 und ModbusTCP
- Erweiterbar durch Plugins



https://www.bro.org/sphinx/_images/architecture.png

Entwicklung der Protokoll-Analyzer

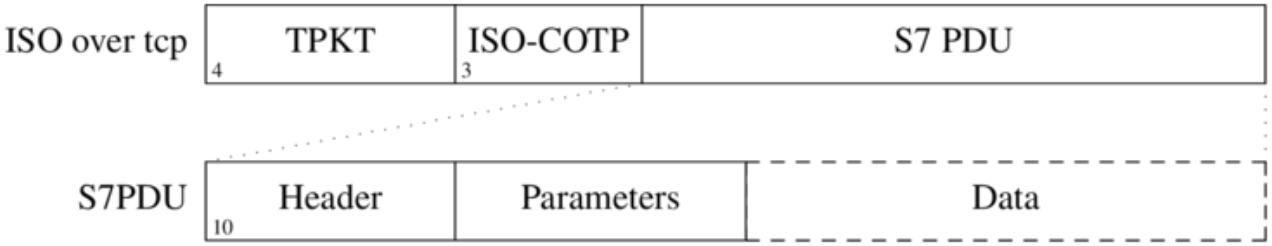
Wie kommunizieren Siemens-SPSen?

- S7Comm und S7CommPlus
  - Proprietäre Protokolle
  - Verwenden Port 102 (TCP)
  - Gekapselt in ISO Over TCP
  - S7Comm: 0x32, S7CommPlus: 0x72
  - Datenaustausch, Up/Download von Programmen, Schreiben/Lesen von Variablen, Start/Stop der SPS etc.
  - Beide Protokolle sehr komplex und stark verschachtelt aufgebaut

Entwicklung der Protokoll-Analyzer

Wie Protokoll-Analyzer entwickeln?

- Protokoll-Struktur modellieren
  - Hier: schwierig, da proprietär. Basis für Analyzer: Wireshark Dissector von T. Wiens, welcher das Protokoll „dekodiert“ hat



  - Struktur des Pakets stark von Inhalt der Header & Parameter abhängig, hohe Permutation
  - S7Comm vollständig, S7CommPlus noch recht unbekannt

http://gmiru.com/images/s7proto/s7packet.png

Entwicklung der Protokoll-Analyzer

- BinPAC
  - Parser-Generator, automatisiert Prozess
  - Einfache Bedienung, übersichtliche Sprache, „Baukastenprinzip“
  - Für S7Comm & S7CommPlus nicht geeignet, da das Protokoll zu komplex ist
- C++
  - Kernsprache für Bro, hohe Flexibilität und Kontrolle, fehleranfälliger
  - „API“ vorhanden, wichtige Funktionen und Klassen werden vererbt, erleichtert die Entwicklung
  - Für S7Comm & S7CommPlus eher geeignet

Entwicklung der Protokoll-Analyzer

Demo

Stand der Entwicklung

- S7Comm Analyzer fertig und funktionsbereit
  - Getestet an mehreren PCAPS, u. a. PCAPS der Testanlage
  - Skripte zur Erkennung von Datenpaketen, Auswertung von Variablen etc.
- S7CommPlus Analyzer Grundstruktur
  - Schwer zu entwickeln, da grundsätzlich weniger Informationen verfügbar sind
  - Protokoll noch komplexer, sehr verschachtelt, große Anzahl an Datentypen

Stand der Entwicklung

Fragen?

Stand der Entwicklung

Danke für Ihre Aufmerksamkeit!