Aufbau und Analyse von Netzwerken in der industriellen Produktion

Themen für Praktika

1. **Entwicklung von Wireshark-Plugins mit C (Karg)**
   - Werkzeuge zur Entwicklung von Wireshark Plugins
   - Vorgehen zur Entwicklung eines Wireshark Plugins
   - Bibliotheken
   - Plugin-Beispiele
   - Performance Vergleich LUA vs. C
2. **Analyse des Netzwerks der Fabrik im Industrie 4.0 Labor (Karg)**
   - Netzwerkanalyse mit NMap
   - Erstellung eines Graphen mit den Knoten im Netzwerk
   - Zuordnung Netzwerkknoten zu Fertigungsstationen
   - Datenflussanalyse
   - Zuordnung Datenfluss zu Produktionsschritten
3. **Analyse von Netzwerkdaten (Karg)**
   - Wie durchsucht man in Wireshark usw. die gesammelten Daten?
   - Syntax von Suchanfragen
   - Beispiele für Wireshark, TCP-Dump, etc.
   - Extraktion von Daten (Bilder, Webseiten, Dateien) aus den Netzwerkpaketen
4. **Hacking mit Scapy (Karg)** (mehrere Gruppen möglich)
   - Skripten von Angriffen mit Scapy
   - Man-In-The-Middle Attacken
   - Replay-Attacken
   - Demonstration anhand von mehreren Beispielen
5. **Datenanalyzer (Zimmermann)**
   - Setzt auf bestehenden Adam-MicroIDS auf (mit 4" TFT)
   - Analyse Gerät für die Darstellung von Protokoll-Typen - Zahl Pakete - Zahl/sec - Länge Durchschnitt - Abweichungen/sec
   - XMOS Programmierung mit TFT Grafik Ausgabe basierend auf funktionsfähigem Demo Programm
   - Ethernet Paket Analyse

6. **Paketdatenbank für Offline Analyse (Zimmermann)**

   - Datensensor (basierend auf MicroIDS) programmieren: Pakete aufsammeln und senden an Host - Typen: alle, TCP, Profinet, UDP
   - Hostprogramm: Aufsammeln der Pakete und speichern in Datenbank, Datenbank Tags mit Beschreibung des Anlagenzustands
   - XMOS Programmierung und Kommunikation XMOS-Host per UDP
   - PC Programmierung mit Datenbank (Spreadsheet oder SQL)

7. **Anomalien erkennen in Online Daten (Zimmermann)**

   - Merkmale aus Paketdaten extrahieren: Länge pro Typ, Abweichungen (wie Projekt 5)
   - Trainingsphase für bestimmte Anlagenzustände
   - Erkennung von Anlagezuständen basierend auf Merkmalen und Ähnlichkeiten
   - Erkennung von Ausreißern
   - XMOS Programmierung auf MicroIDS-200 (neuer Prozessor mit mehr Speicher und 2 Kernen/1000MIPS)