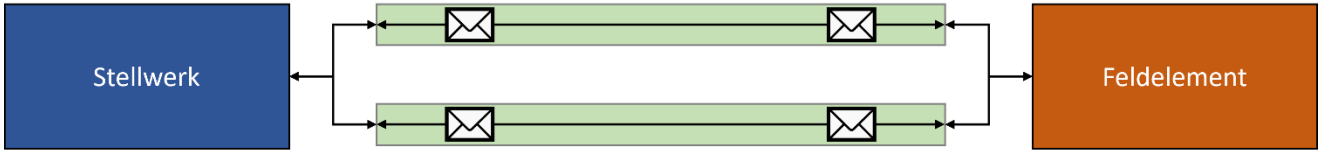
Intrusion Detection System für Object Controller

Christian Jäger-Waldau, Allan Jacob

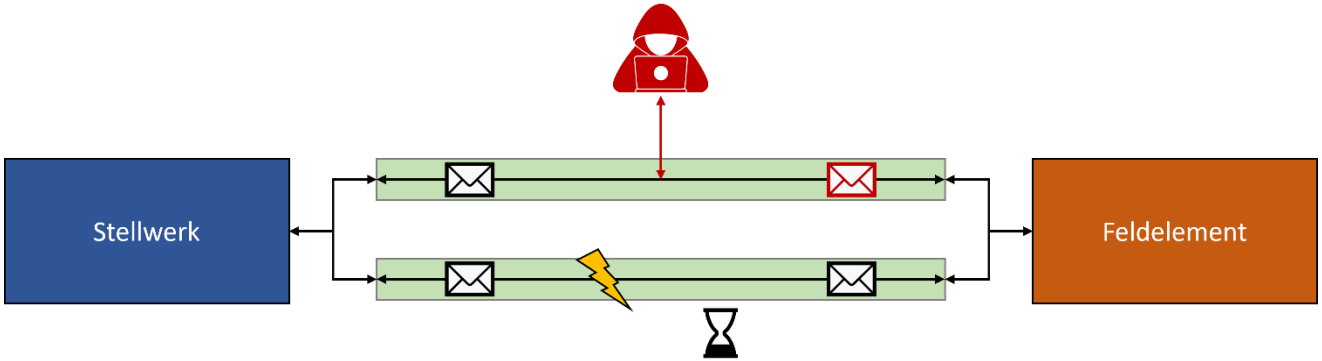
Problemstellung

- Bestehendes RaSTA-Protokoll wird für Kommunikation zwischen ESTW/DSTW und Feldelementen verwendet
  - Verwendung MAC-Verfahren basierend auf MD4-Hashfunktion zur Prüfsummenbildung
  - Modifikation von Nachrichteninhalten erfordert eine Neuberechnung des MAC
  - Übertragung der Nachricht über mehrere (physisch) getrennte Kanäle für Redundanz und Robustheit



Problemstellung

- Bestehendes RaSTA-Protokoll wird für Kommunikation zwischen ESTW/DSTW und Feldelementen verwendet
  - Verwendung MAC-Verfahren basierend auf MD4-Hashfunktion zur Prüfsummenbildung
  - Modifikation von Nachrichteninhalten erfordert eine Neuberechnung des MAC
  - Übertragung der Nachricht über mehrere (physisch) getrennte Kanäle für Redundanz und Robustheit
- Sicherheitsvulnerabilität wurde während vergangenen DRSS nachgewiesen
- Potenzielle schwerwiegende Konsequenzen für aktiven Eisenbahnverkehr
- Möglichkeit für Angreifer, Kontrolle über Feldelemente zu übernehmen und Aktivitäten vor Stellwerk zu verbergen



Zielstellung

- Entwicklung eines Intrusion Detection Systems (IDS) zur Erkennung von Angriffen
  - Detektion eines bereits im System befindlichen "Middleman"
- Unabhängig vom Eindringweg
- Verbesserung der Sicherheit in Kommunikation zwischen Stellwerk und Feldelementen
- Erhaltung bestehender Safety-Funktionen (Redundanzkanäle)
- Vermeidung von KI-Algorithmen

- Gestaltung als zusätzliche Netzwerkschicht ohne Interferenz mit RaSTA
- Betrachtung der gesendeten Nachrichten als "Black Box" ohne Datenausschnitte für IDS

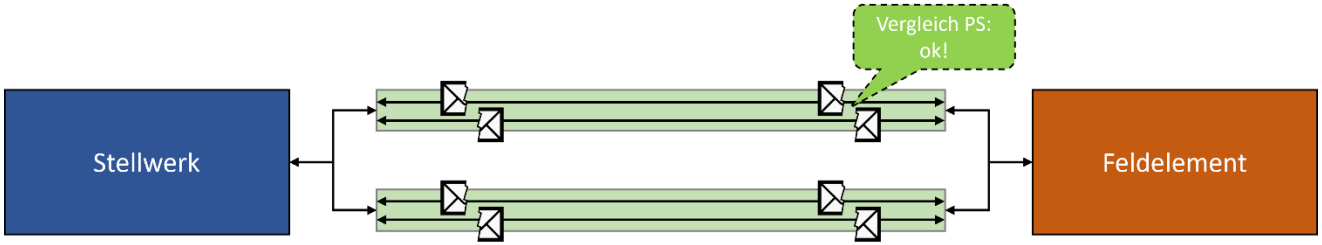
- Implementierung in Testumgebung zur Fehlererkennung

Vorgehensweise

- **Datenflussübersicht:**
  - Diagrammatische Darstellung des Datenflusses zwischen Stellwerk und Feldelementen
  - Zwei Datenflüsse: Vom Stellwerk zum Feldelement und vom Feldelement zum Stellwerk
- **Schwerpunkt auf Feldelement zum Stellwerk:**
  - Dieser Datenfluss schützenswerter
  - Angriff kann erkannt werden, wenn dieser Fluss nicht manipuliert wird
  - Jedoch Bevorzugung eines symmetrischen Systems
- **Entwicklung IDS-System**
- **Implementierung in Testumgebung**
  - Schrittweises Hinzufügen von Funktionen
- **RAMS-Analyse**

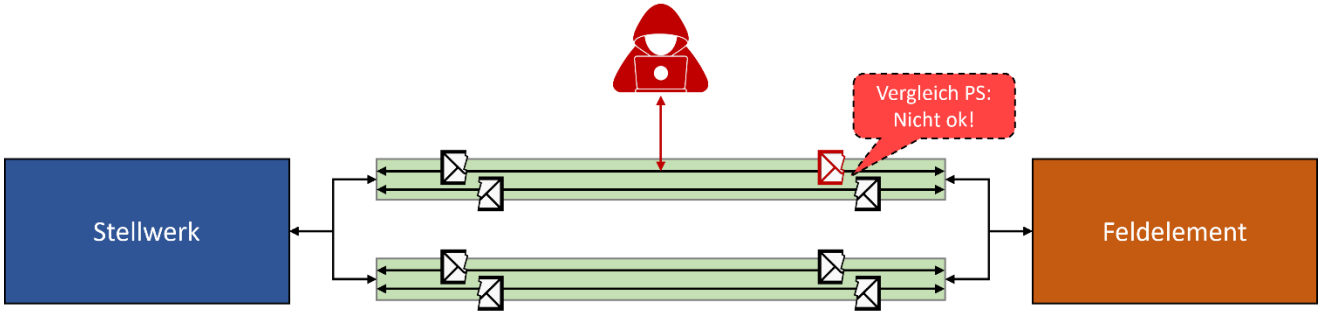
IDS Konzept

- **Physische und Logische Kanäle:**
  - Aufteilung der Nutzdaten in kleinere Einheiten, z. B. DataX1 und DataX2
  - Übertragung aufgeteilt über verschiedene logische Kanäle
    - Analyse verschiedener Ansätze zur Nachrichtenteilung
  - Reduzierung des Manipulationsrisikos durch Aufteilung der Daten
  - Prüfsummenvergleich zur Aufdeckung von Datenmanipulation
  - Für Middleman erhöhter Aufwand für vollen Datenzugriff (aber nicht unmöglich)



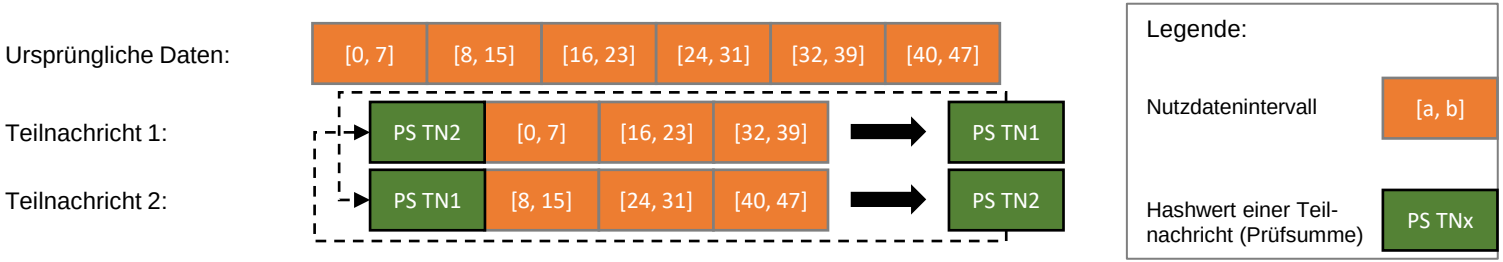
IDS Konzept

- **Physische und Logische Kanäle:**
  - Aufteilung der Nutzdaten in kleinere Einheiten, z. B. DataX1 und DataX2
  - Übertragung aufgeteilt über verschiedene logische Kanäle
    - Analyse verschiedener Ansätze zur Nachrichtenteilung
  - Reduzierung des Manipulationsrisikos durch Aufteilung der Daten
  - Prüfsummenvergleich zur Aufdeckung von Datenmanipulation
  - Für Middleman erhöhter Aufwand für vollen Datenzugriff (aber nicht unmöglich)



Zerstückelung & Intrusion Detection System

- Aufteilung der Daten in zwei Teilnachrichten
  - Zerstückelung nach vorher definiertem Trennungsintervall (8 Bytes)



- IDS zur Aufdeckung und Meldung möglicher Datenmanipulation
  - Erstellung von SHA256-Hashes als Prüfsumme der Nachrichtenteile
  - Mitsenden der Prüfsummen mit jeweils anderem Nachrichtenteil
  - Bei Nachrichtenzusammensetzung Erstellung neuer Hashes und Abgleich mit gesendeten Hashwerten

DRSS
Digital Rail
Summer School

TECHNISCHE UNIVERSITÄT
CHEMNITZ

Technische
Hochschule
Wildau
Technical University
of Applied Sciences
WILDAU

Vielen Dank für Ihre Aufmerksamkeit!

RAMS Analyse

Zuverlässigkeit (Reliability):

- SHA-256-Hashfunktionen zur Datenintegritätsprüfung
- Fehlerbehandlungen beim Teilen und Zusammenführen der Teilnachrichten
- Verwendung von Sequenznummern zur Nachrichtenreihenfolgenüberwachung

Verfügbarkeit (Availability):

- Verwendung einer Endlosschleife zum Empfangen/Senden
- Timeout-Behandlung beim Empfang von Daten von Netzwerk-Sockets sorgt für Aufrechterhaltung der Kommunikation

Wartbarkeit (Maintainability):

- Modulare Code-Struktur für Änderungen und Erweiterungen
- Sinnvolle Variablennamen und Funktionsnamen zur Verbesserung der Lesbarkeit

Sicherheit (Safety):

- Erhaltung der Redundanz durch Beibehaltung der physischen Kanäle
- Fehlerbehandlungen beim Teilen und Zusammenführen der Teilnachrichten
- Timeout-Behandlung beim Empfang von Daten von Netzwerk-Sockets sorgt für Aufrechterhaltung der Kommunikation

Flussdiagram