UNIVERSITÄT PASSAU

Angriff auf RaSTA

Projekt Hackathon - DRSS 2022

Marion Christl, Sven Gebauer, Maximilian Seitz

14. Juni 2022

Kontext

UNIVERSITÄT PASSAU

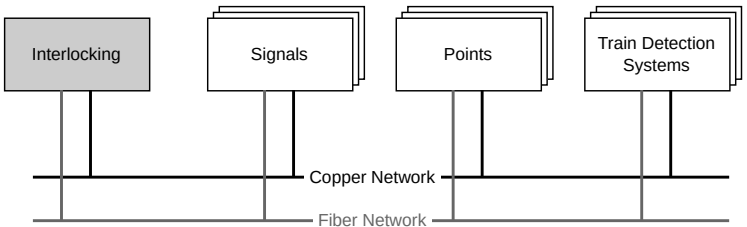
UNIVERSITÄT PASSAU

- IP-Basierte Kommunikation zwischen Stellwerken und Feldelementen
  - Gleiche Übertragungstechnik wie im Internet

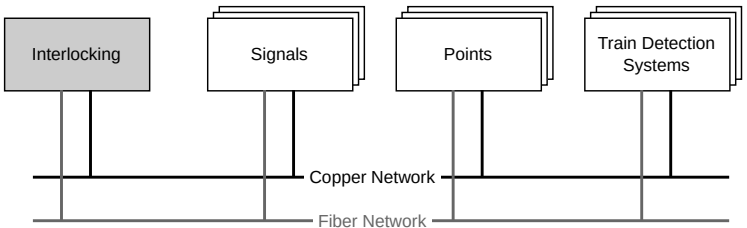
UNIVERSITÄT PASSAU

- IP-Basierte Kommunikation zwischen Stellwerken und Feldelementen
  - Gleiche Übertragungstechnik wie im Internet
- Problem: TCP/IP liefert nicht die nötige Zuverlässigkeit. Lösung:

- IP-Basierte Kommunikation zwischen Stellwerken und Feldelementen
  - Gleiche Übertragungstechnik wie im Internet
- Problem: TCP/IP liefert nicht die nötige Zuverlässigkeit. Lösung:
  - Redundante Verkabelung von Feldelementen



- IP-Basierte Kommunikation zwischen Stellwerken und Feldelementen
  - Gleiche Übertragungstechnik wie im Internet
- Problem: TCP/IP liefert nicht die nötige Zuverlässigkeit. Lösung:
  - Redundante Verkabelung von Feldelementen
  - Zuverlässiges Transportprotokoll

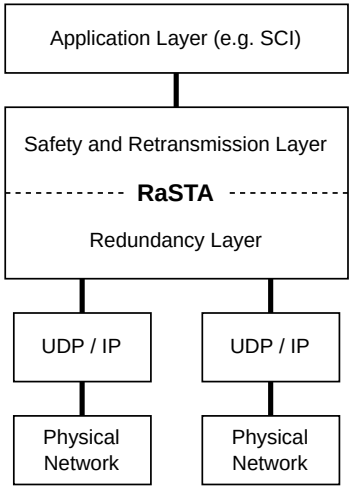


Rail Safe Transport Application (RaSTA)

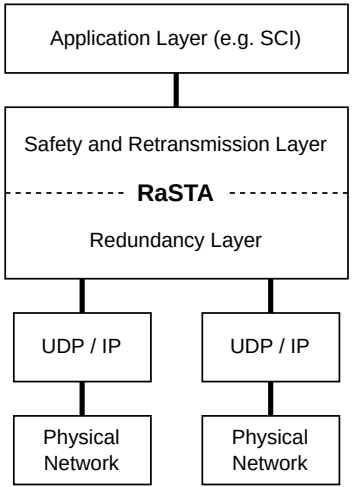
UNIVERSITÄT PASSAU

- Ermöglicht zuverlässige Kommunikation über IP-Netze:
  - Integrität und Authentizität
  - Korrekte Reihenfolge von Paketen
  - Erkennung von Übertragungsverzögerungen

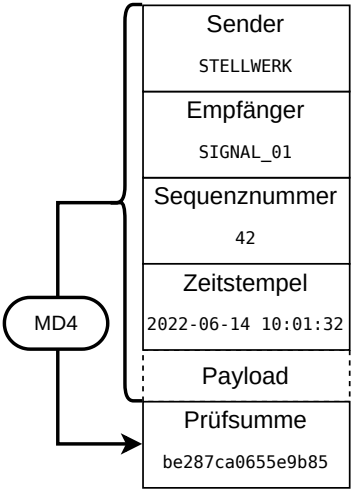
- Ermöglicht zuverlässige Kommunikation über IP-Netze:
  - Integrität und Authentizität
  - Korrekte Reihenfolge von Paketen
  - Erkennung von Übertragungsverzögerungen
- Kombiniert mehrere physische Netzwerkverbindungen



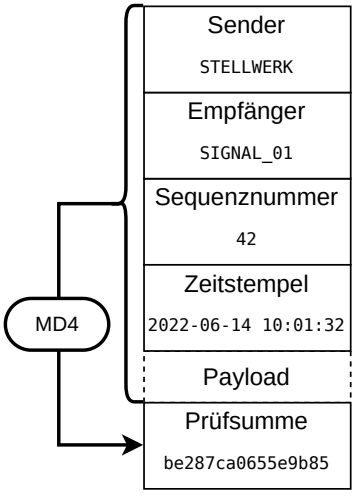
- Ermöglicht zuverlässige Kommunikation über IP-Netze:
  - Integrität und Authentizität
  - Korrekte Reihenfolge von Paketen
  - Erkennung von Übertragungsverzögerungen
- Kombiniert mehrere physische Netzwerkverbindungen
- Arbeitet zwischen Transport- und Anwendungsschicht (ähnlich zu SSL/TLS)



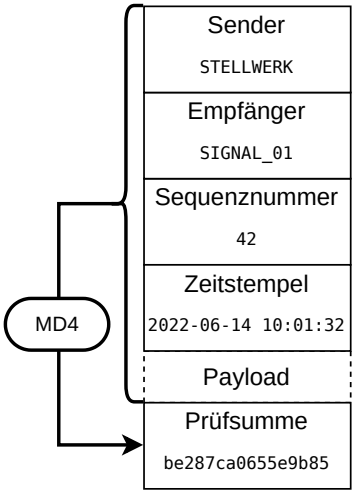
RaSTA-Datenpakete



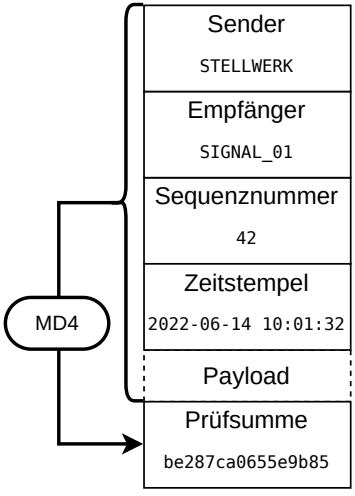
- Sequenznummern für korrekte Paket-Reihenfolge



- Sequenznummern für korrekte Paket-Reihenfolge
- Zeitstempel zur Erkennung von Verzögerungen

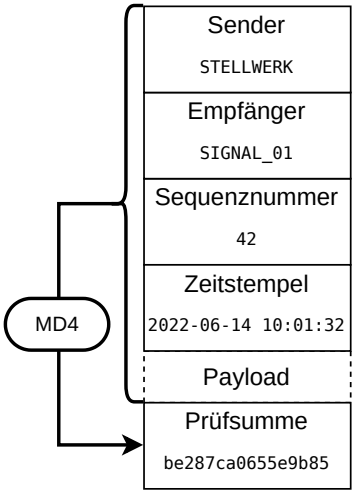


- Sequenznummern für korrekte Paket-Reihenfolge
- Zeitstempel zur Erkennung von Verzögerungen
- MD4-Prüfsumme zur Erkennung von Übertragungsfehlern und -manipulation



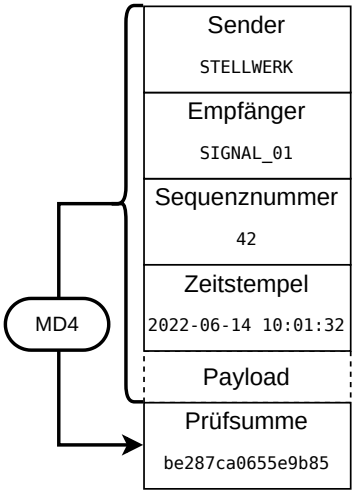
- Sequenznummern für korrekte Paket-Reihenfolge
- Zeitstempel zur Erkennung von Verzögerungen
- MD4-Prüfsumme zur Erkennung von Übertragungsfehlern und -manipulation

- MD4 ist eine *Hashfunktion*
  - Input: Datenpaket, beliebige Länge
  - Output: Prüfsumme (*Hash*), konstante Länge

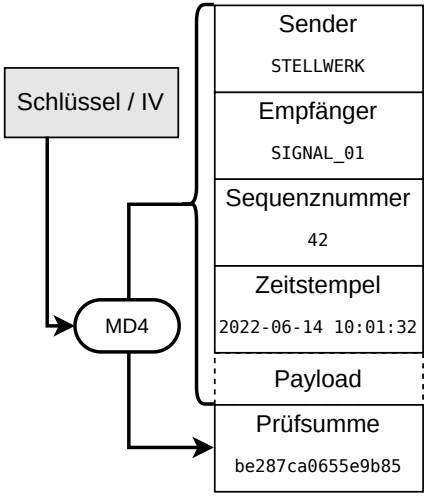


- Sequenznummern für korrekte Paket-Reihenfolge
- Zeitstempel zur Erkennung von Verzögerungen
- MD4-Prüfsumme zur Erkennung von Übertragungsfehlern und -manipulation

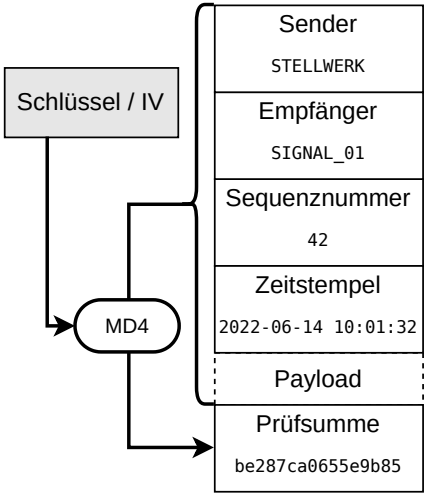
- MD4 ist eine *Hashfunktion*
  - Input: Datenpaket, beliebige Länge
  - Output: Prüfsumme (*Hash*), konstante Länge
- Berechnung von einfachem MD4 erfordert keinen Schlüssel → Angreifer könnte Pakete manipulieren



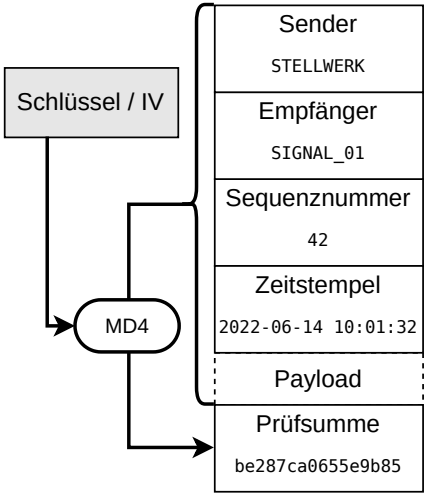
- RaSTA benutzt modifiziertes MD4 mit geheimem *Initialisierungsvektor (IV)*
  - Maximal 128 bit ($\approx$ 16-stelliges Passwort)
  - Anderer IV $\rightarrow$ Andere Prüfsumme



- RaSTA benutzt modifiziertes MD4 mit geheimem *Initialisierungsvektor (IV)*
  - Maximal 128 bit ($\approx$ 16-stelliges Passwort)
  - Anderer IV $\rightarrow$ Andere Prüfsumme
- IV wird benötigt um gültige Prüfsummen zu berechnen / überprüfen



- RaSTA benutzt modifiziertes MD4 mit geheimem *Initialisierungsvektor (IV)*
  - Maximal 128 bit ($\approx$ 16-stelliges Passwort)
  - Anderer IV $\rightarrow$ Andere Prüfsumme
- IV wird benötigt um gültige Prüfsummen zu berechnen / überprüfen
- ... und muss also allen Geräten im Netzwerk bekannt sein



Wir nehmen an auf folgendes Zugriff zu haben:

Wir nehmen an auf folgendes Zugriff zu haben:

- Den MD4-IV

Wir nehmen an auf folgendes Zugriff zu haben:

- Den MD4-IV
- Die Möglichkeit alle redundanten Verbindungen zu einem Feldelement zu kompromittieren

Wir nehmen an auf folgendes Zugriff zu haben:

- Den MD4-IV
- Die Möglichkeit alle redundanten Verbindungen zu einem Feldelement zu kompromittieren
  - Alle Nachrichten **an** das Feldelement können gelesen und ersetzt werden (wie auch die direkten Antworten darauf)

Folgendes wird von unserem Angriff erwartet:

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden
  - Auf Nachrichten welche das Feldelement sendet wird kein Zuriff benötigt

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden
  - Auf Nachrichten welche das Feldelement sendet wird kein Zuriff benötigt
  - Direkte Antworten auf Nachrichten nutzen den selben Kanal, wodurch auch auf diese Antworten Zugriff gewährt ist

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden
  - Auf Nachrichten welche das Feldelement sendet wird kein Zuriff benötigt
  - Direkte Antworten auf Nachrichten nutzen den selben Kanal, wodurch auch auf diese Antworten Zugriff gewährt ist
- Eingriff in das System muss konsequenzlos beendet werden können

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden
  - Auf Nachrichten welche das Feldelement sendet wird kein Zuriff benötigt
  - Direkte Antworten auf Nachrichten nutzen den selben Kanal, wodurch auch auf diese Antworten Zugriff gewährt ist
- Eingriff in das System muss konsequenzlos beendet werden können
  - Sequenznummern, Zietstempel, etc. von Nachrichten müssen konsistent bleiben

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden
  - Auf Nachrichten welche das Feldelement sendet wird kein Zuriff benötigt
  - Direkte Antworten auf Nachrichten nutzen den selben Kanal, wodurch auch auf diese Antworten Zugriff gewährt ist
- Eingriff in das System muss konsequenzlos beendet werden können
  - Sequenznummern, Zietstempel, etc. von Nachrichten müssen konsistent bleiben
- Angriff darf nicht direkt erkennbar sein

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden
  - Auf Nachrichten welche das Feldelement sendet wird kein Zuriff benötigt
  - Direkte Antworten auf Nachrichten nutzen den selben Kanal, wodurch auch auf diese Antworten Zugriff gewährt ist
- Eingriff in das System muss konsequenzlos beendet werden können
  - Sequenznummern, Zietstempel, etc. von Nachrichten müssen konsistent bleiben
- Angriff darf nicht direkt erkennbar sein
  - Keine fehlenden Heartbeat Nachrichten

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden
  - Auf Nachrichten welche das Feldelement sendet wird kein Zuriff benötigt
  - Direkte Antworten auf Nachrichten nutzen den selben Kanal, wodurch auch auf diese Antworten Zugriff gewährt ist
- Eingriff in das System muss konsequenzlos beendet werden können
  - Sequenznummern, Zietstempel, etc. von Nachrichten müssen konsistent bleiben
- Angriff darf nicht direkt erkennbar sein
  - Keine fehlenden Heartbeat Nachrichten
  - Keine falschen Sequenznummern

Folgendes wird von unserem Angriff erwartet:

- Nur die Verbindung zu einem ausgewählten Feldelement muss kompromittiert werden
  - Auf Nachrichten welche das Feldelement sendet wird kein Zuriff benötigt
  - Direkte Antworten auf Nachrichten nutzen den selben Kanal, wodurch auch auf diese Antworten Zugriff gewährt ist
- Eingriff in das System muss konsequenzlos beendet werden können
  - Sequenznummern, Zietstempel, etc. von Nachrichten müssen konsistent bleiben
- Angriff darf nicht direkt erkennbar sein
  - Keine fehlenden Heartbeat Nachrichten
  - Keine falschen Sequenznummern
  - Muss nach Beendigung des Angriffs weiterhin unerkannt bleiben

In einem System mit einer Stellwerk und einem Signal soll eine Situation ausgelöst werden, in der die Stellwerk glaubt das Signal zeige ein Halte-Symbol, während das Signal tatsächlich eine Durchfahrt erlaubt.

In einem System mit einer Stellwerk und einem Signal soll eine Situation ausgelöst werden, in der die Stellwerk glaubt das Signal zeige ein Halte-Symbol, während das Signal tatsächlich eine Durchfahrt erlaubt.

Verhalten vor Angriff

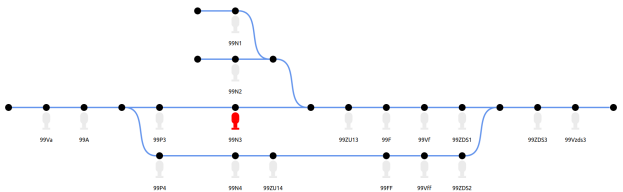


Figure: Daten bei Stellwerk

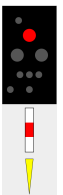


Figure: Angezeigtes Signal

In einem System mit einer Stellwerk und einem Signal soll eine Situation ausgelöst werden, in der die Stellwerk glaubt das Signal zeige ein Halte-Symbol, während das Signal tatsächlich eine Durchfahrt erlaubt.

Verhalten vor Angriff

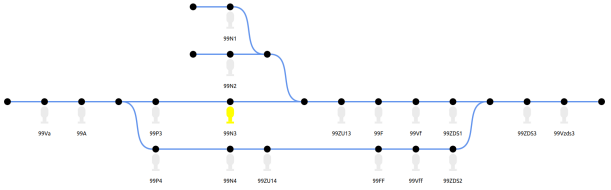


Figure: Daten bei Stellwerk

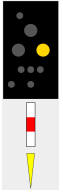


Figure: Angezeigtes Signal

In einem System mit einer Stellwerk und einem Signal soll eine Situation ausgelöst werden, in der die Stellwerk glaubt das Signal zeige ein Halte-Symbol, während das Signal tatsächlich eine Durchfahrt erlaubt.

Verhalten vor Angriff

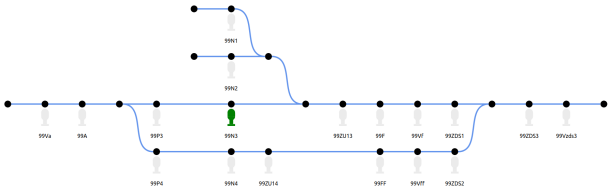


Figure: Daten bei Stellwerk

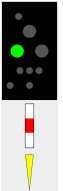


Figure: Angezeigtes Signal

In einem System mit einer Stellwerk und einem Signal soll eine Situation ausgelöst werden, in der die Stellwerk glaubt das Signal zeige ein Halte-Symbol, während das Signal tatsächlich eine Durchfahrt erlaubt.

Verhalten nach Angriff

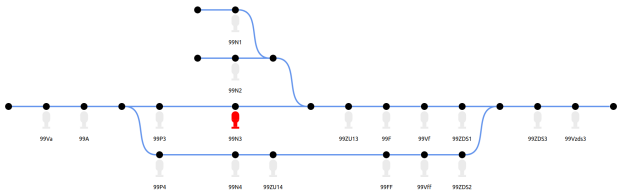


Figure: Daten bei Stellwerk

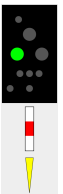


Figure: Angezeigtes Signal

In einem System mit einer Stellwerk und einem Signal soll eine Situation ausgelöst werden, in der die Stellwerk glaubt das Signal zeige ein Halte-Symbol, während das Signal tatsächlich eine Durchfahrt erlaubt.

Verhalten nach Angriff

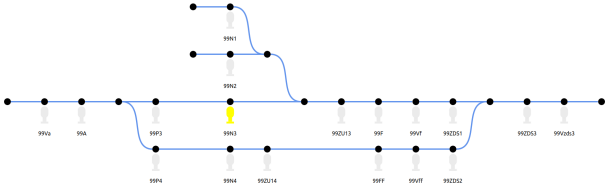


Figure: Daten bei Stellwerk

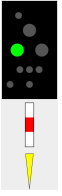


Figure: Angezeigtes Signal

In einem System mit einer Stellwerk und einem Signal soll eine Situation ausgelöst werden, in der die Stellwerk glaubt das Signal zeige ein Halte-Symbol, während das Signal tatsächlich eine Durchfahrt erlaubt.

Verhalten nach Angriff

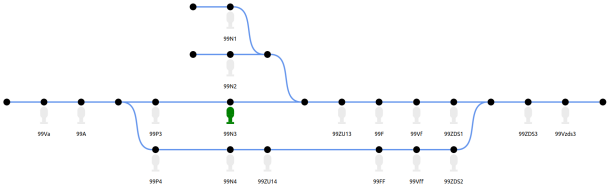


Figure: Daten bei Stellwerk

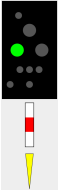


Figure: Angezeigtes Signal

- Um mit der Kommunikation des Systems konsistent zu bleiben, werden Nachrichten nur ersetzt (niemals eingefügt oder verworfen)

UNIVERSITÄT PASSAU

- Um mit der Kommunikation des Systems konsistent zu bleiben, werden Nachrichten nur ersetzt (niemals eingefügt oder verworfen)
  - Inhalt von Nachrichten vom Stellwerk an das Signal wird ausgetauscht ("Zeige Rot an" $\rightarrow$ "Zeige Grün an")

UNIVERSITÄT PASSAU

- Um mit der Kommunikation des Systems konsistent zu bleiben, werden Nachrichten nur ersetzt (niemals eingefügt oder verworfen)
  - Inhalt von Nachrichten vom Stellwerk an das Signal wird ausgetauscht ("Zeige Rot an" $\rightarrow$ "Zeige Grün an")

- Um mit der Kommunikation des Systems konsistent zu bleiben, werden Nachrichten nur ersetzt (niemals eingefügt oder verworfen)
  - Inhalt von Nachrichten vom Stellwerk an das Signal wird ausgetauscht ("Zeige Rot an" $\rightarrow$ "Zeige Grün an")
  - MD4-Prüfsumme muss neu berechnet werden