ROBUST IDENTITY TOKENS FOR INTRUSION DETECTION IN SMART GRIDS

Kai Hendrik Wöhnert

Shashank Shekher Tripathi

Volker Skwarek

Forschungsprojekt DISEGO – Critical Components for Distributed and Secure Grid Operation
gefördert vom Bundesministerium für Wirtschaft und Energie

HAW HAMBURG

AGENDA

- Cyber-Bedrohungen auf das Stromnetz
- Bestehende Gegenmaßnahmen
- Vorschlag einer Zero-Trust Architektur mit robusten Identitätstokens für smart grid Kommunikation
- Evaluationsergebnisse

ANGRIFFE AUF SMART GRID

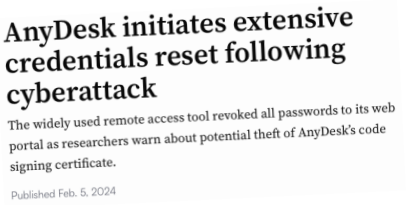
Das Stromnetz ist durch Hacking-Angriffe auf die IT-Infrastruktur der Netzbetreiber und unsichere Betriebsmittel in den Haushalten gefährdet

Zertifikatsbasierte Systeme sind zwar weit verbreitet, aber anfällig für Angriffe wie Zertifikatsdiebstahl, unsachgemäße Validierung der Vertrauenskette und Kompromittierung von Schlüsseln [1].

ANGRIFFE AUF SMART GRID

Das Stromnetz ist durch Hacking-Angriffe auf die IT-Infrastruktur der Netzbetreiber und unsichere Betriebsmittel in den Haushalten gefährdet

Zertifikatsbasierte Systeme sind zwar weit verbreitet, aber anfällig für Angriffe wie Zertifikatsdiebstahl, unsachgemäße Validierung der Vertrauenskette und Kompromittierung von Schlüsseln [1].


AnyDesk initiates extensive credentials reset following cyberattack

The widely used remote access tool revoked all passwords to its web portal as researchers warn about potential theft of AnyDesk's code signing certificate.

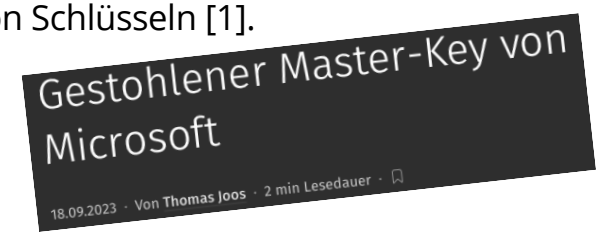
Published Feb. 5, 2024


Leaked stolen Nvidia key can sign Windows malware

70k staff email addresses and NTLM password hashes also dumped online

Gareth Corfield

Sat 5 Mar 2022 | 04:09 UTC

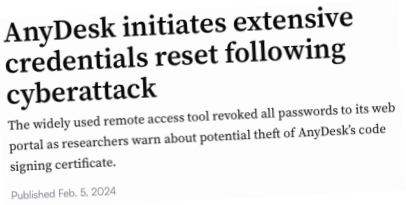

Gestohlener Master-Key von Microsoft

18.09.2023 · Von Thomas Joos · 2 min Lesedauer ·

ANGRIFFE AUF SMART GRID

Das Stromnetz ist durch Hacking-Angriffe auf die IT-Infrastruktur der Netzbetreiber und unsichere Betriebsmittel in den Haushalten gefährdet

Zertifikatsbasierte Systeme sind zwar weit verbreitet, aber anfällig für Angriffe wie Zertifikatsdiebstahl, unsachgemäße Validierung der Vertrauenskette und Kompromittierung von Schlüsseln [1].


AnyDesk initiates extensive credentials reset following cyberattack

The widely used remote access tool revoked all passwords to its web portal as researchers warn about potential theft of AnyDesk's code signing certificate.

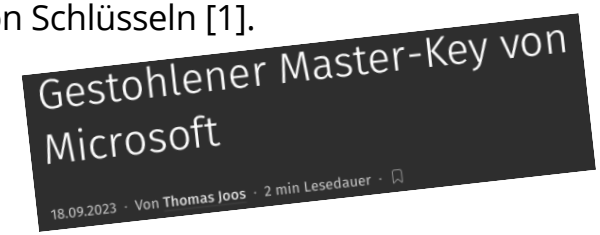
Published Feb. 5, 2024


Leaked stolen Nvidia key can sign Windows malware

70k staff email addresses and NTLM password hashes also dumped online

Gareth Corfield

Sat 5 Mar 2022 | 04:09 UTC


Gestohlener Master-Key von Microsoft

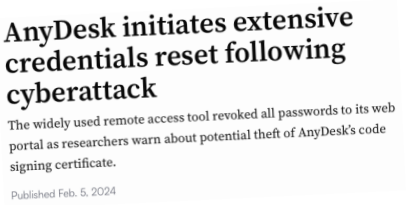
18.09.2023 · Von Thomas Joos · 2 min Lesedauer ·

Die von den 1.000 kommunalen Verteilernetzbetreibern eingesetzten Cyberabwehrmaßnahmen sind deutlich weniger umfassend.

ANGRIFFE AUF SMART GRID

Das Stromnetz ist durch Hacking-Angriffe auf die IT-Infrastruktur der Netzbetreiber und unsichere Betriebsmittel in den Haushalten gefährdet

Zertifikatsbasierte Systeme sind zwar weit verbreitet, aber anfällig für Angriffe wie Zertifikatsdiebstahl, unsachgemäße Validierung der Vertrauenskette und Kompromittierung von Schlüsseln [1].


AnyDesk initiates extensive credentials reset following cyberattack

The widely used remote access tool revoked all passwords to its web portal as researchers warn about potential theft of AnyDesk's code signing certificate.

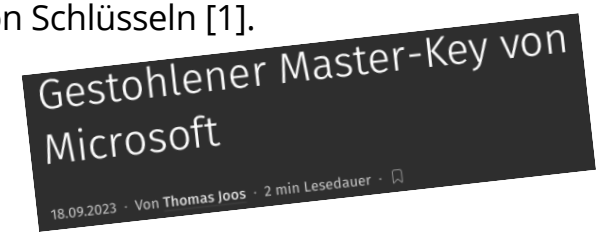
Published Feb. 5, 2024


Leaked stolen Nvidia key can sign Windows malware

70k staff email addresses and NTLM password hashes also dumped online

Gareth Corfield

Sat 5 Mar 2022 04:09 UTC


Gestohlener Master-Key von Microsoft

18.09.2023 · Von Thomas Joos · 2 min Lesedauer ·

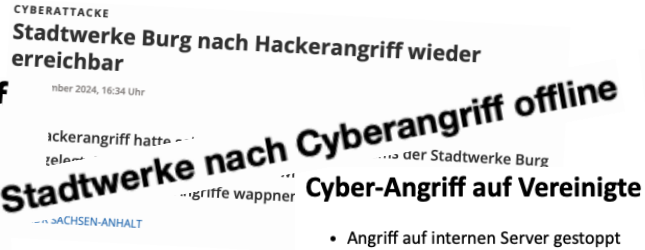
Die von den 1.000 kommunalen Verteilernetzbetreibern eingesetzten Cyberabwehrmaßnahmen sind deutlich weniger umfassend.


Digitale Bedrohung: Hackerangriff auf Stadtwerke

ZfK+ Kriminelle Attacke auf internes Netz der Stadtwerke Schwerte

Schwerte, eine mittlere Stadt au dem Kreis Unna in No ist Opfer eines Cyberangriffs geworden. Die Stadt hat Verbindung zum Versoger und zur Südwestfalen-IT gekappt.

08.03.2025


CYBERATTACKE

Stadtwerke Burg nach Hackerangriff wieder erreichbar

Detmold Stadtwerke nach Cyberangriff offline


Nach Hackerangriff

Meininger Stadtwerke haben Kontrolle wieder

Marko Hildebrand-Schönherr · 22.03.2024 - 12:04 Uhr

Cyber-Angriff auf Vereinigte Stadtwerke GmbH

- Angriff auf internen Server gestoppt
- Versorgungssysteme für Strom, Gas, Wasser, Wärme und Telekommunikation nicht betroffen
- Datenabfluss wird geprüft

ANGRIFFE AUF SMART GRID

Das Stromnetz ist durch Hacking-Angriffe auf die IT-Infrastruktur der Netzbetreiber und unsichere Betriebsmittel in den Haushalten gefährdet

MÖGLICHE ANGRIFFSABLÄUFE - PHYSISCHE LEITUNGSTRENNUNG

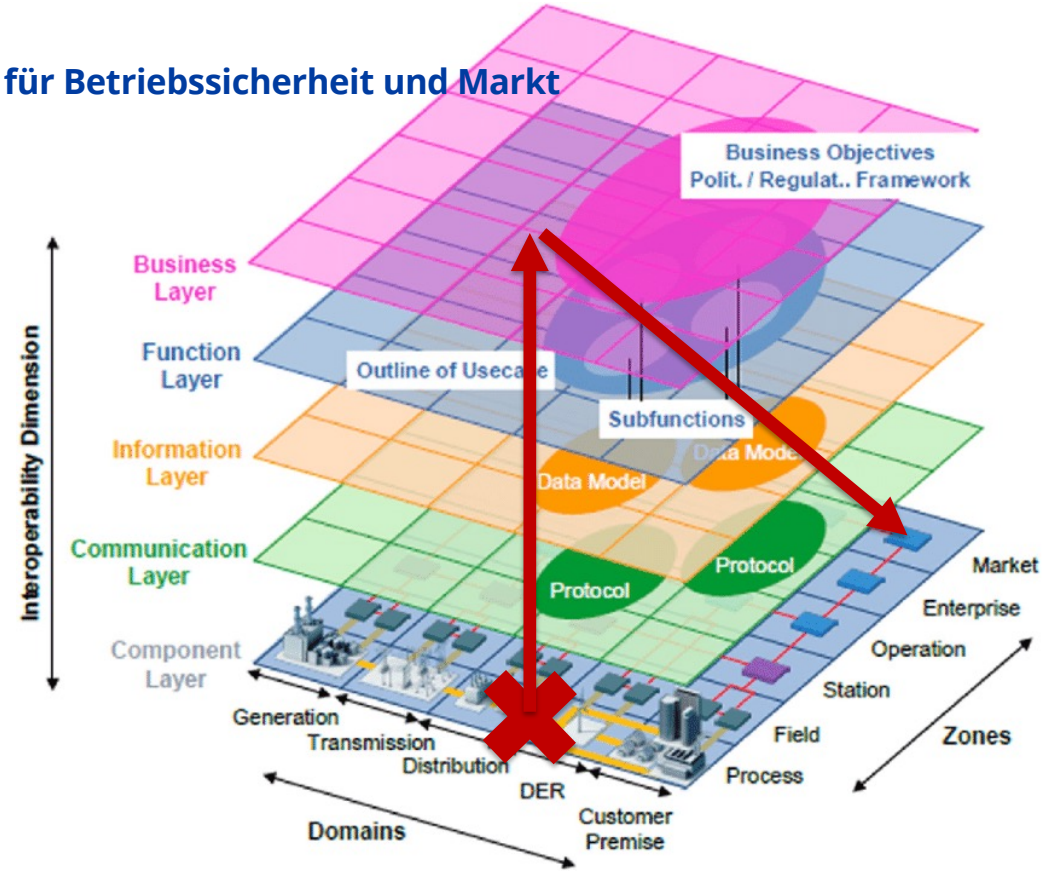
Fehlerfreie Kommunikation ist grundlegend für Betriebssicherheit und Markt

Leitungsdurchtrennung führt zu Kommunikationsausfall

Mögliche Auswirkung für Netzbetreiber:

- Loss of Control
- Loss of View
- Loss of availability
- Loss of Protection

Marktveränderungen durch Bilanzkreisfehler



MÖGLICHE ANGRIFFSABLÄUFE – MANIPULATION VON RUNDSTEUERSIGNALEN UND CLOUD-BEFEHLEN VON KLEINSTANLAGEN

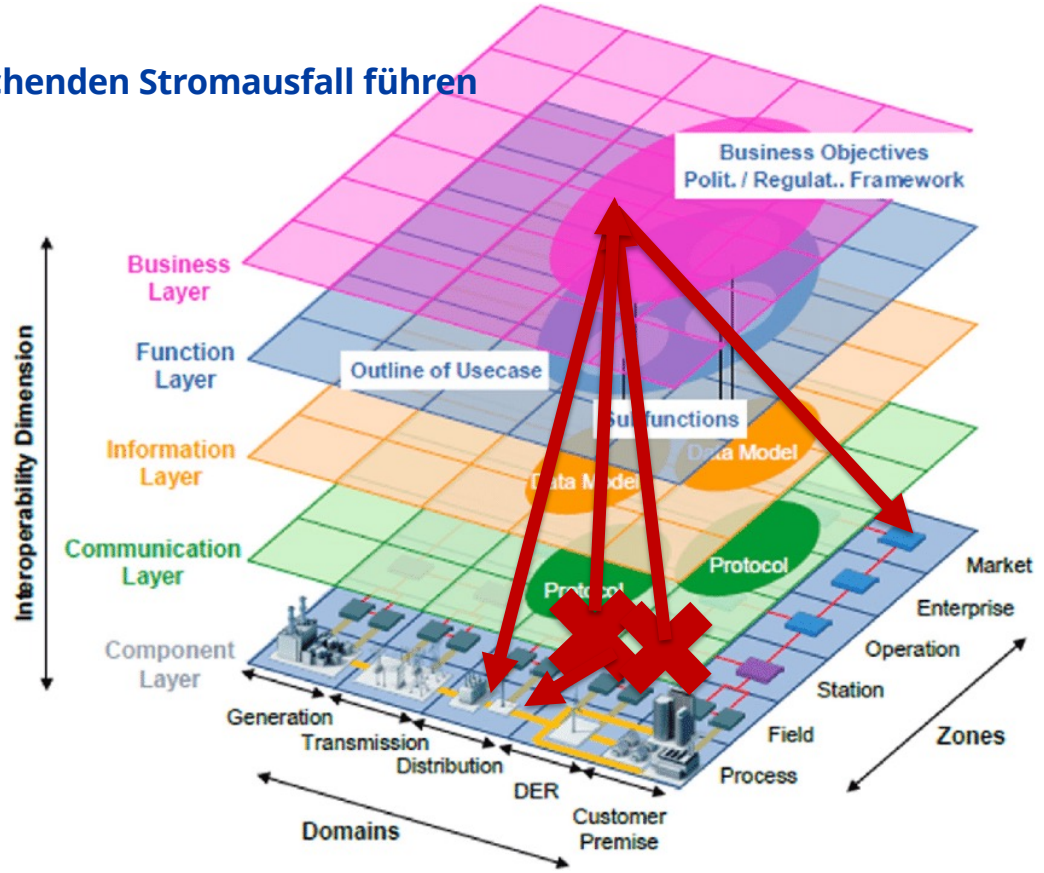
Unautorisierte Steuerung kann zum weitreichenden Stromausfall führen

Unautorisierte Steuerung von Anlagen kann zu Überlastungen des Stromnetzes führen

Prozesse werden gestört, Hardware kann zerstört werden

Mögliche Auswirkung für Netzbetreiber:

- Denial of Control
- Loss of Safety
- Damage to Property



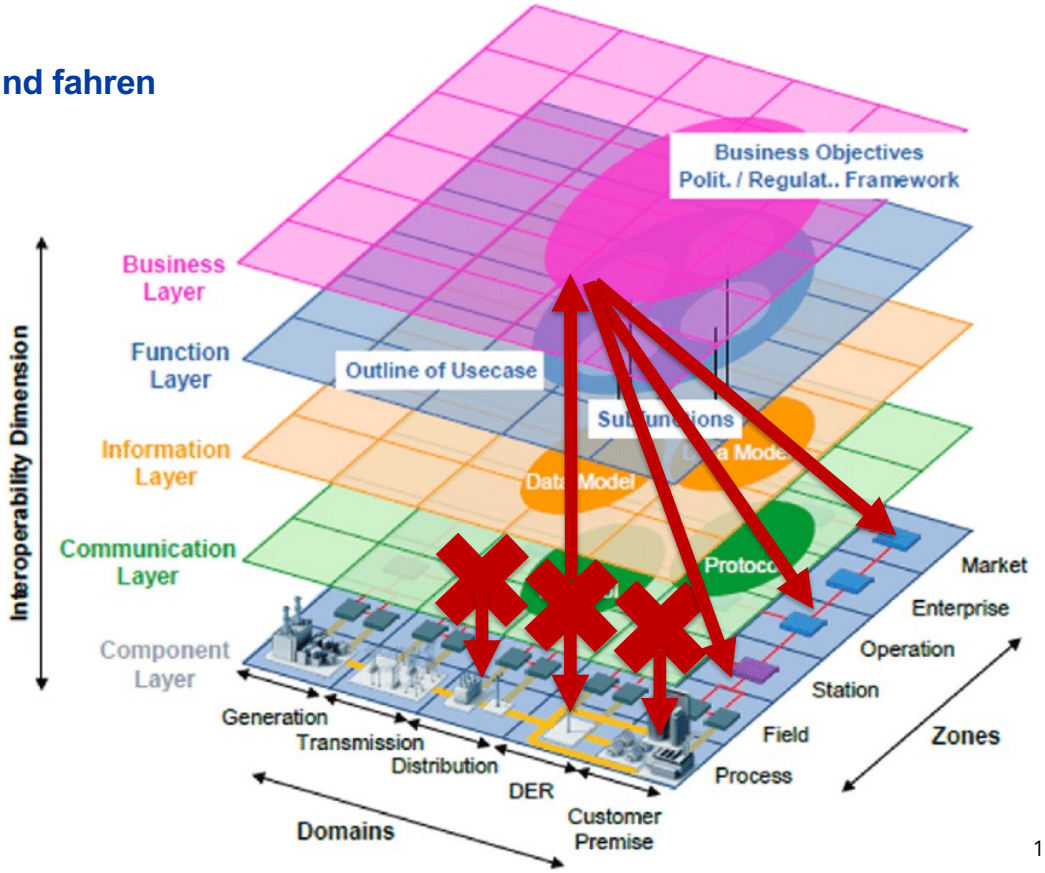
MÖGLICHE ANGRIFFSABLÄUFE – FALSE-DATA-INJECTION

Falsche Messdaten lassen die Netzbetreiber blind fahren

Falsche Messdaten führen zu falschen Zustandsschätzungen bis hin zur Beschädigung

Mögliche Auswirkung für Netzbetreiber:

- Loss of View
- Loss of Safety
- Damage to Property



GEGENMAßNAHMEN

Die schleppende Digitalisierung der Verteilnetze verhindert Stromausfälle durch Hacking-Angriffe

REGULARIEN

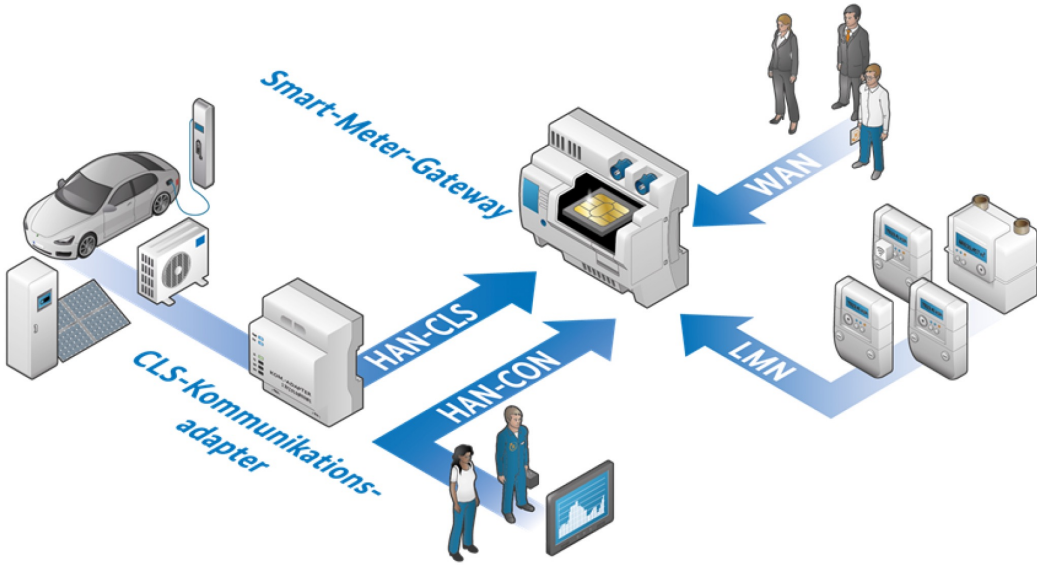
Zertifikatsverwaltete Smart-Meter-Gateways sind das Schlüsselement im Smart Grid

§ 14a EnWG: Neue Regelung für steuerbare Verbrauchseinrichtungen (Wärmepumpen, Ladeeinrichtungen, Stromspeicher) in Verbindung mit Smart Meter Gateways und Steuerboxen

BSI TR-03109 – Hauptrichtlinie für intelligente Messsysteme

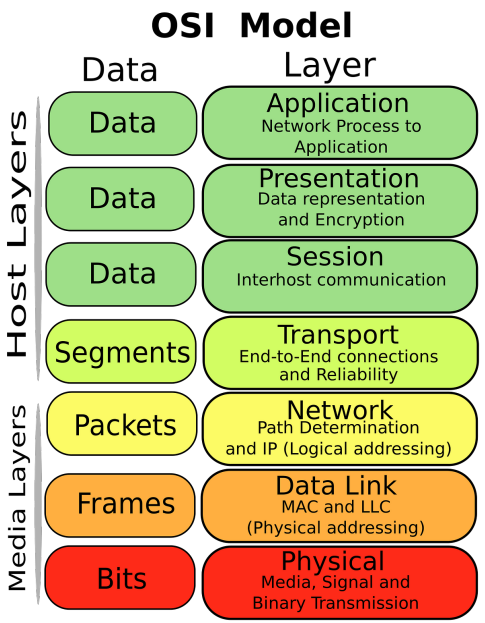
- Aufgeteilt in 6 Subrichtlinien
- Letztes Update im Dezember 2025

- ➢ Verschlüsselte Kommunikation von Steuerbefehlen und Messdaten
- ➢ Zertifikatsbasiertes Identitätsmanagement mit Smart Meter Gateway als Mittelpunkt und zentralem Gateway-Administrator

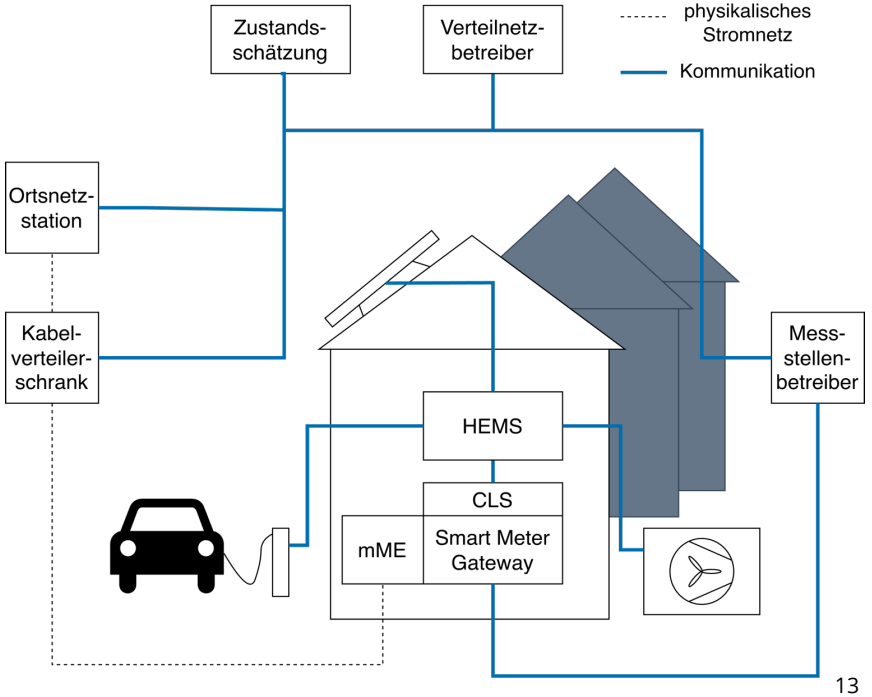


TOPOLOGIE DER STAND DER TECHNIK

Abschottung und Applikationsbezogene Anomalieerkennung schützt vor False-Data-Injection nicht

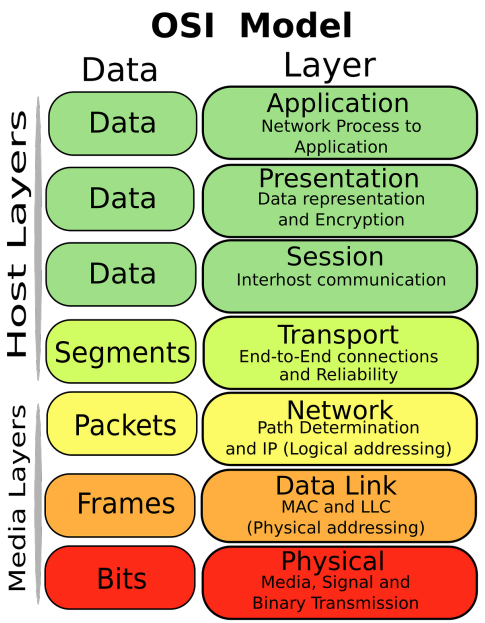


Anomalieerkennung

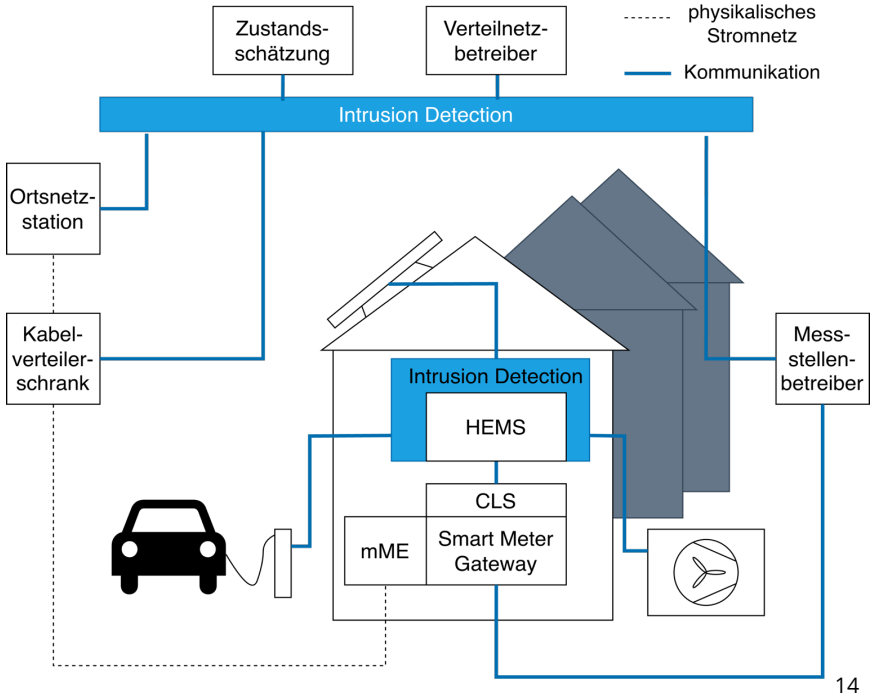


VORSCHLAG EINER SICHEREN ARCHITEKTUR

Umfassende Identität als Vertrauensanker und Zero-Trust erhöhen die Sicherheit des Systems

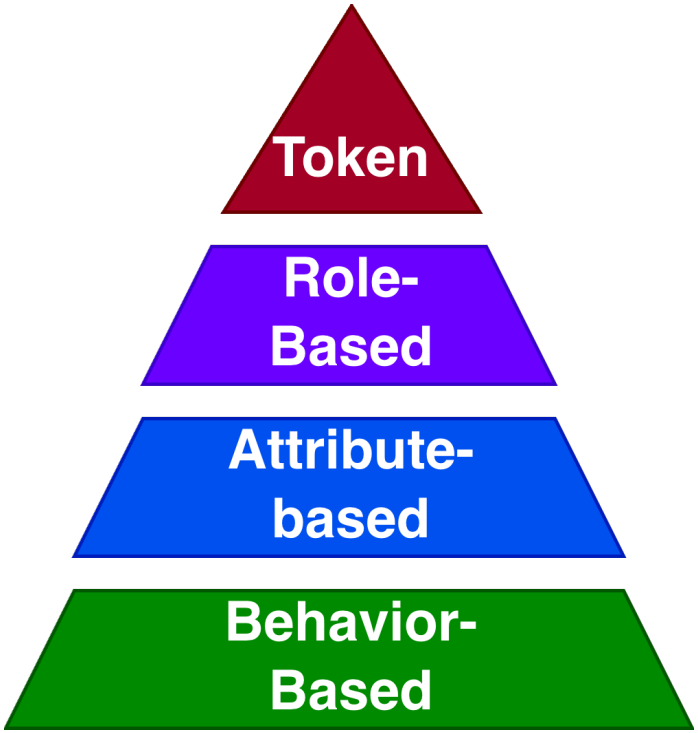


Authentifizierung und Autorisierung basierend auf Eigenschaften, Kontext und Verhalten



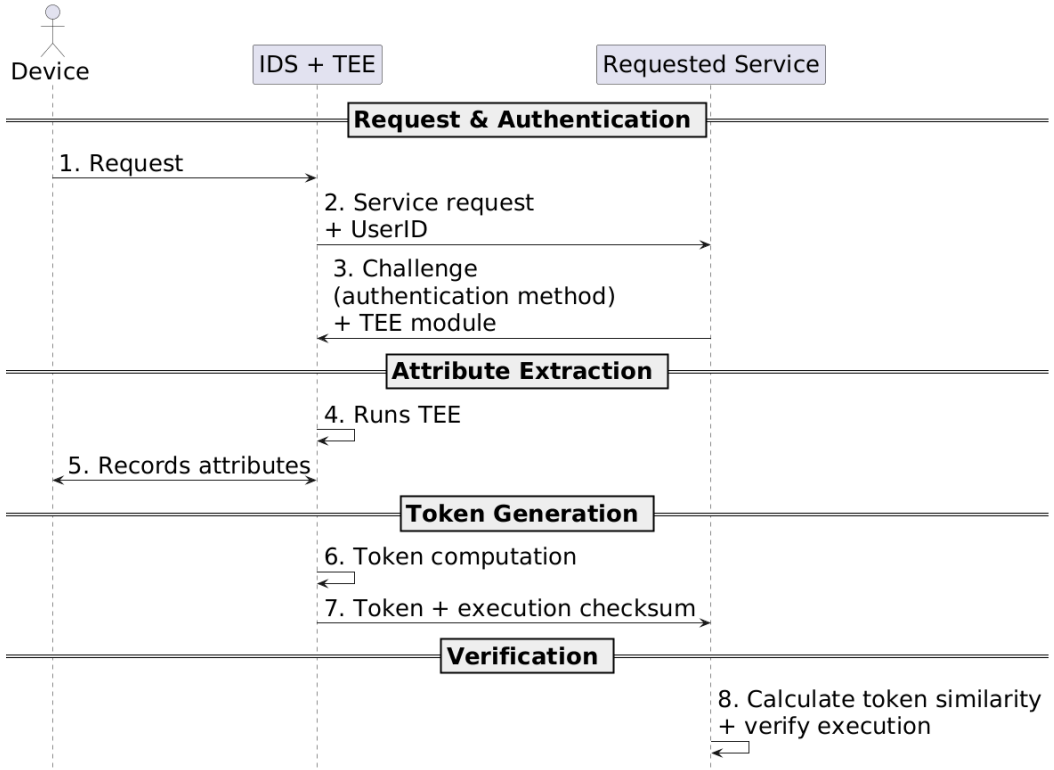
ZUGANGSKONTROLLMODELLE

Behavior-Based Access Control deckt einen umfassenden Ausschnitt der Identität ab



AUTHENTIFIZIERUNG

Die Authentifizierung wird dem Dienst abgenommen



IDENTITÄTSTOKEN

Der Identitätstoken ist robust gegenüber benignen Veränderungen

Natürliche Veränderungen der Attribute müssen vom Token berücksichtigt werden

- Statisch: Unveränderliche Eigenschaften

$$A = \{a_1, a_2, \ldots, a_n\} \quad (1)$$

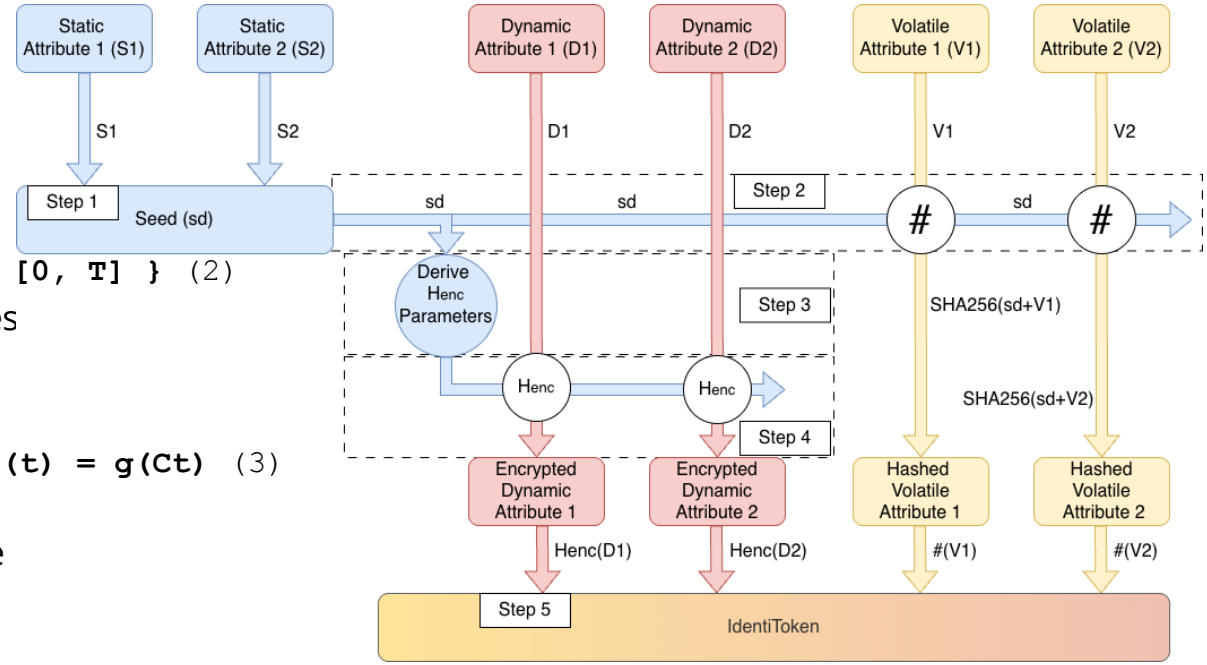
$$S = \{ a_i \in A \mid da_i/dt = 0 \ \forall t \in [0, T] \} \quad (2)$$

- Dynamisch: Eigenschaft, die aufgrund des normalen Nutzungskontexts schwanken, jedoch innerhalb eines bestimmten, deterministischen Leistungsbereichs begrenzt bleiben.

$$D(t) = g(Ct) \quad (3)$$

- Volatil: Transiente Zustandsvariablen, die die unmittelbare Benutzerkonfiguration oder Umgebung widerspiegeln. Diese Werte sind sehr instabil und haben einen undefinierten oder unendlichen potenziellen Bereich.

$$V(t) \sim A(Entropy \rightarrow \infty) \quad (4)$$



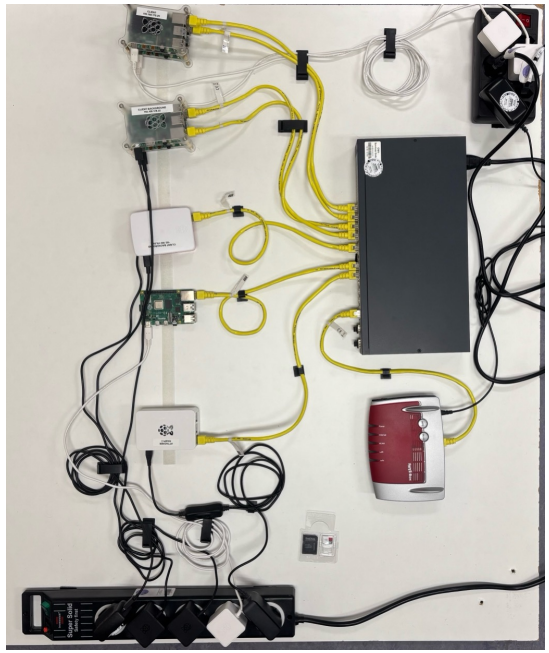
EVALUATION

Laboruntersuchungen zeigen Machbarkeit

- Testumgebung mit einem Router, einem Switch, fünf Raspberry Pi 4B und zwei Raspberry Pi 3B+

- 50 % Angriff: Zertifikatsdiebstahl und Man-in-the-Middle,
- 50 % harmloser Datenverkehr

- Merkmalsextraktion: tshark
- Merkmalsauswahl: cicflowmeter und seine 10 wichtigsten Merkmale unter Verwendung von Random Forest
- Es wurden 605.400 Identitäts-Token mit unterschiedlichen Parametern erstellt
- Bei einem Schwellenwert von 80 % Hamming-Ähnlichkeit werden



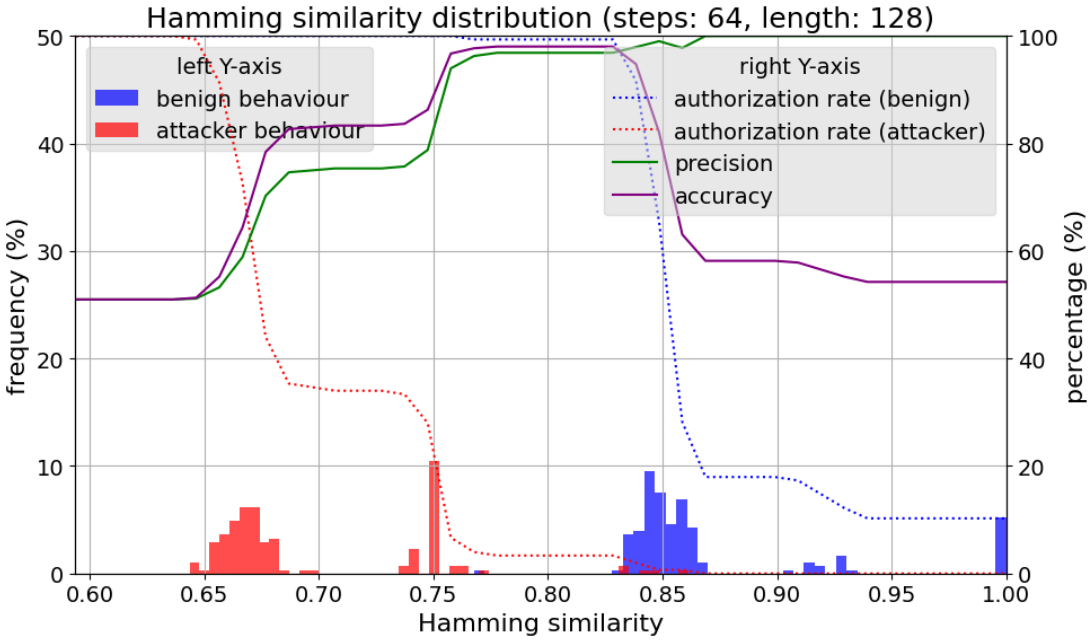
EVALUATION

Laboruntersuchungen zeigen Machbarkeit

- Testumgebung mit einem Router, einem Switch, fünf Raspberry Pi 4B und zwei Raspberry Pi 3B+

- 50 % Angriff: Zertifikatsdiebstahl und Man-in-the-Middle; 50 % harmloser Datenverkehr
- Merkmalsextraktion: tshark
- Merkmalsauswahl: cicflowmeter und seine 10 wichtigsten Merkmale unter Verwendung von Random Forest
- Es wurden 605.400 Identitäts-Token mit unterschiedlichen Parametern erstellt

- Bei einem Schwellenwert von 80 % Hamming-Ähnlichkeit werden Tokens zu 98% richtig klassifiziert



ERGEBNIS

- ✓ Zero-Trust Prinzipien im Netzwerk
- ✓ Zusätzlich zu dem Zertifikatssystem ist das System mit einem weiteren Authentifizierungsfaktor abgesichert
- ✓ Absicherung befindet sowohl behind-the-meter und im Verteilnetz und geht bis auf untere Protokollschichten
- ➢ Laboruntersuchungen werden ins Feld getragen
- ➢ Intensivierung von Maschinellem Lernen gestützter Generierung von Netzwerkverkehr und Erkennung von Angriffen
- ➢ Rollout und Regulierungsnovellen, die die Architektur neudenken

LET‘S DISCUSS!

HAW
HAMBURG

REFERENCES

[1] V Venkateswara Rao, R Marshal, and K Gobinath. “The IoT supply chain attack trends-vulnerabilities and preventive measures”. In: 2021 4th International Conference on Security and Privacy (ISEA-ISAP). IEEE. 2021, pp. 1–4.