06.06.2019

Integrierte Sicherheit in vernetzten Medizintechnik-geräten

Dr. Esther Gelle
Adrian Helfenstein

CyOne SECURITY

Inhalt

CyOne SECURITY

Vernetzte Medizintechnikgeräte

Vernetzte Medizintechnikgeräte

SENSOREN

Temperatur, Glukose, Luft

Video-Objektive

Elektrokardiogramm (EKG)

Navigation

…

AKTOREN

Pumpen

Wärmetauscher

Servos, Motoren

…

Digitalanzeigen

Monitore

Drucker

…

MONITORE

Digitalisierung z.B. Aufzeichnungen in elektronischer Form

Remote Administration, Konfiguration, Kalibrierung, Überwachung, Wartung wie z.B. Backup und Update, Integration,

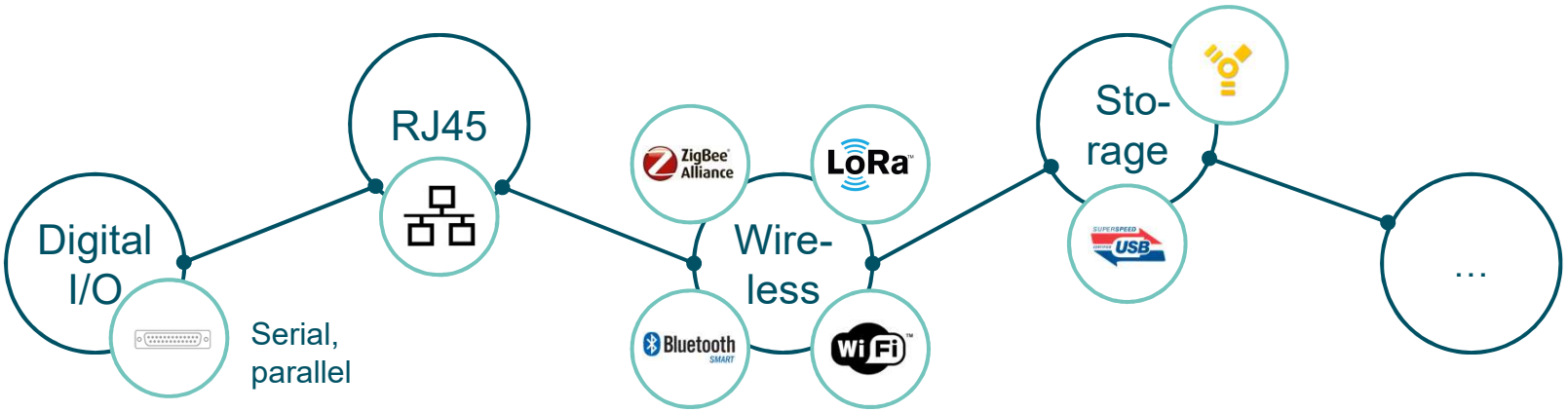
…

INDUSTRIE 4.0

Vernetzte Medizintechnikgeräte

Zunehmende Kommunikationsbedürfnisse …

… zunehmende Anzahl und verschiedenartige Schnittstellen …



… und noch viel mehr unterschiedliche Kommunikationsprotokolle!

Herausforderungen für Hersteller und Betreiber

CyOne SECURITY

Herausforderungen für Hersteller und Betreiber sind sich verändernde …

- … Prozesse, regulatorische (Sicherheits-)Anforderungen,
- … IT-Infrastrukturen und
- … Cyberbedrohungen

Hersteller berücksichtigen diese Indikatoren insbesondere bei …

- … Architekturwahl
- … Updatefähigkeit
- … Security by Design

Wesentliche Indikatoren:

Widerstands- und Anpassungsfähigkeit von Produkten und Lösungen

Betreiber berücksichtigen diese Indikatoren beim Design der Gesamtlösung, der Wahl der Produkte und der Hersteller

CyOne SECURITY

Zentrale Sicherheitsanforderungen

Zentrale Sicherheitsanforderungen

CyOne SECURITY

Persons who use open systems shall

Ensure the **authenticity**, **integrity**, and, as apporpriate, **confidentiality** of **electronic records** from the point of their creation to the point of their receipt

Electronic record

- Any combination of text, graphics, data, …,
- Information representation in digital form
- Created, modified, maintained, **archived**, retrieved, or distributed by a computer system
- Ensure integrity, authenticity, and when appropriate, the confidentiality of electronic records and to ensure that the signer **cannot readily repudiate** the signed record as not genuine

Aufbewahrungs-frist! Dauer?

(FDA, CFR 21, part 11)

Zentrale Anforderungen

Audit trails

- **Secure**, computer-generated, time-stamped
- To record operator entries and actions that create, modify, or delete electronic records
- Record changes shall not obscure previously recorded information.
- **Shall be retained** (at least as long as that required for the subject electronic records)
- Available for review

(FDA, CFR 21, part 11, sec. 11.10)

Weitere Gesetze und Verordnungen

Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

(DSG, Art.7, Abs. 1)

- Personendaten bearbeiten, Kommunikationsnetz zur Verfügung stellen
- **Vertraulichkeit, Verfügbarkeit** und **Integrität** der Daten
- Gegenwärtiger Stand der Technik
- Massnahmen periodisch überprüfen

(VDSG, Art. 8)

Geforderte Sicherheitsziele

CyOne SECURITY

Vertraulichkeit

Informationen sind nur autorisierten Personen, Entitäten, Prozesse, etc. zugänglich und bekannt

Integrität

Die Richtigkeit, Komplettheit und Unveränderbarkeit von Daten über ihren ganzen Lebenszyklus hinweg sicherstellen; nicht autorisiertes Verändern von Daten wird verhindert oder festgestellt

Authentizität
(Daten und Entitäten)

Beweis der Rechtmässigkeit von Identitätsansprüchen oder des Ursprungs von Daten

Non-Repudiation

Aktionen/Ereignisse eindeutig mit einer Person, Entität, Prozess, etc. assoziieren; nur mit vernachlässigbarer Wahrscheinlichkeit bestreitbar und «öffentlich» verifizierbar

Zuordnung dieser Sicherheitsziele auf gesetzliche Anforderungen

CyOne SECURITY

	Vertraulichkeit	Integrität	Authentizität	Non-Repudiation
Security Protocols	x	x	x	
Electronic Records	(x)	x	x	
Digital Signatures		x	x	x
Audit Trails		x	x	x
Access Control System		x	x	
Passwords	x	x		
Soft- und Firmware		x	x	x

Gute Neuigkeiten: Es gibt Lösungen zur Erreichung dieser Sicherheitsziele!

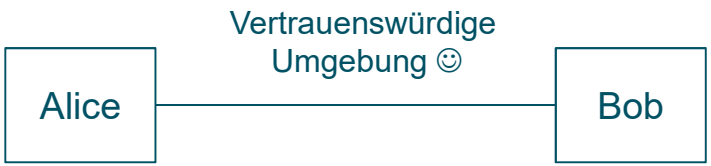
CyOne SECURITY

Lösungskonzepte und Mechanismen

Sicherheitsprotokolle

Protokoll

Ein Protokoll ist eine Abfolge von Schritten durchgeführt von zwei oder mehr Parteien.

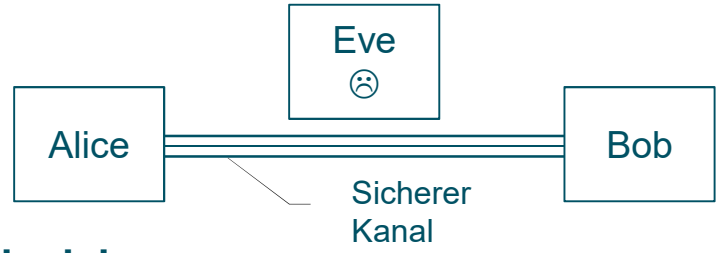


Beispiele

- Ethernet, IP, TCP, HTTP, SMB, …
- Feldbus-Protokolle
- Protokolle über serielle Schnittstellen, z.B. RS-232, RS-485

Sicherheitsprotokoll

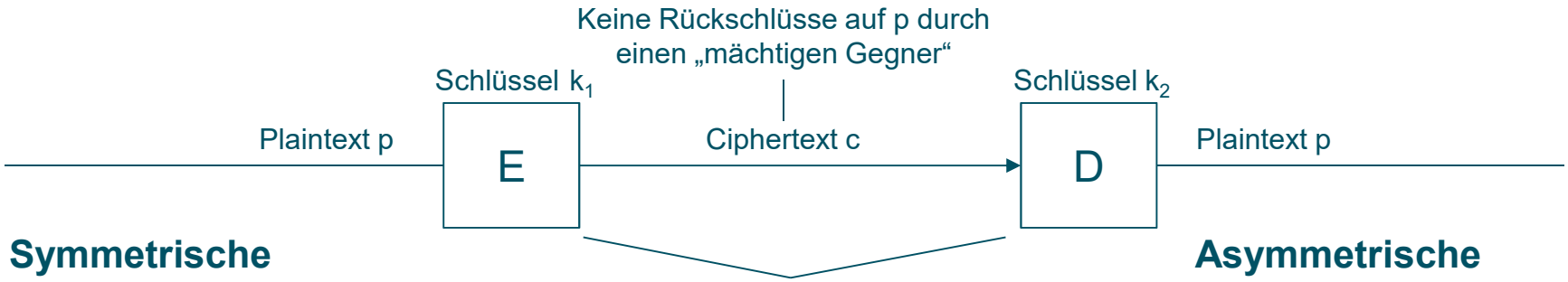
Ein Sicherheitsprotokoll ist ein Protokoll welches in einer nicht vertrauenswürdigen Umgebung ablaufen kann und dabei Sicherheitsziele erreicht.



Beispiele

IPSec, TLS, HTTPS, …

Verschlüsselung für Vertraulichkeit



Symmetrische Verschlüsselung

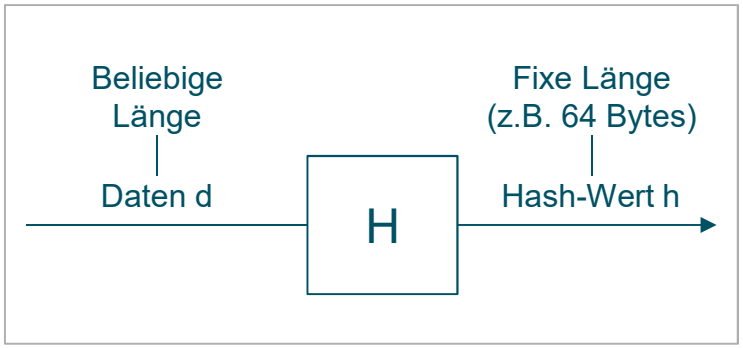
- $k_1 = k_2$
- k_1 und k_2 geheim

- $D_{k2}(E_{k1}(p)) = p$
- und mathematisch definierte Sicherheitseigenschaften!

Asymmetrische Verschlüsselung

- $k_1 \neq k_2$
- k_2 geheim

Kryptographische Hash-Funktionen für Integrität



Eigenschaften von kryptographischen Hash-Funktionen

- Einwegfunktion, deterministisch
- Gegeben h, schwer eine Nachricht d zu finden, so dass H(d) = h
- Gegeben Nachricht d1, schwer ein d2 zu finden, so dass H(d1) = H(d2)
- Schwer d1, d2 (d1≠d2) zu finden, so dass H(d1) = H(d2)

Typische Representanten

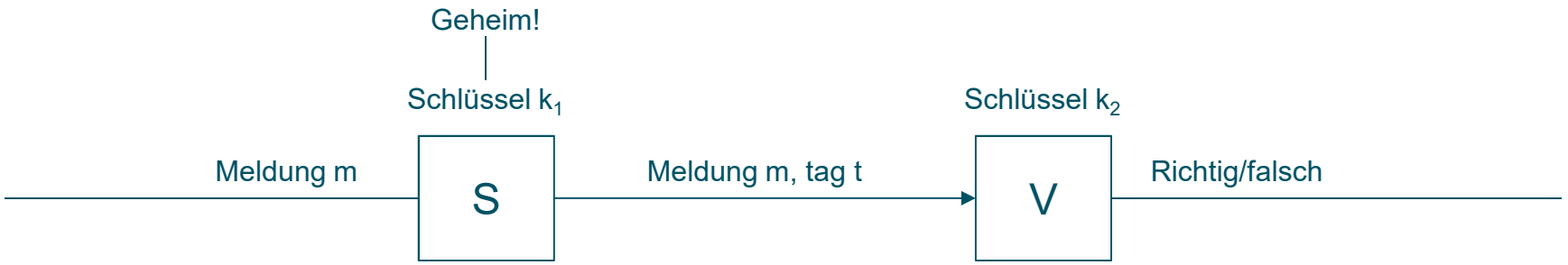
- SHA, RIPEMD, …

Integritätsprüfung für Daten d

- Ausgabe von H(d) mit dem bereits bekannten Hash-Wert h von d vergleichen

Cyclic Redundancy Checks (CRCs) sind **KEINE** kryptographischen Hash-Funktionen!

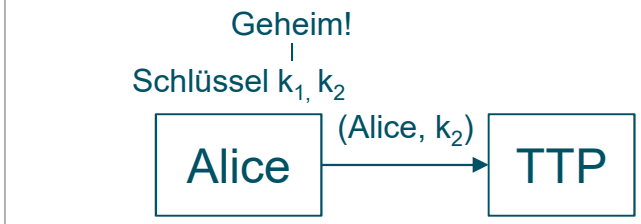
Message Authentication Codes für Integrität und Authentizität



Generiere Tag
$S(k_1, m) \rightarrow t$

Verifiziere Tag
$V(k_2, m, t) =? \text{ richtig}$

Authentication und Trusted Third Party für Non-Repudiation



1

Trusted Third Party (TTP)

- Identifiziert Alice
- Verifiziert Alice's Besitz von k_1
- Assoziiert k_2 mit Alice

Signiere d
$S(k_1, d) \rightarrow s$

Verifiziere
$V(k_2, d, s) =? \text{ true}$
$TTP(k_2, Alice) =? \text{ true}$

2

Beweise
$V(k_2, d, s) =? \text{ true}$
$TTP(k_2, Alice) =? \text{ true}$

3

CyOne SECURITY

Fazit

Fazit

CyOne SECURITY

- Medizintechnikgeräte werden immer mehr vernetzt
- Dadurch entstehen zusätzliche Sicherheits-Anforderungen
- Diese betreffen die Entwicklung sowie den Betrieb von Medizintechnikgeräten und darüber hinaus die Aufbewahrung von Daten
- Konzepte, Mechanismen und Lösungen für integrierte Sicherheit sind verfügbar

Security by Design !

Sichere Schweiz.
Bit für Bit.

CyOne SECURITY

Adrian Helfenstein
adrian.helfenstein@cyone.ch
Telefon +41 41 748 85 00

Esther Gelle
esther.gelle@cyone.ch
Telefon +41 41 748 85 00

cyone.ch