Karlsruher Institut für Technologie

Vorhandene sichere IT-Infrastrukturen für IoT nutzen

Institut für Neutronenphysik und Reaktortechnik (INR)

Umfeld

- Karlsruher Institut für Technologie
- Institut für Neutronenphysik und Reaktortechnik
- Gruppe für Messtechnik und experimentelle Methodik
- Versuchsanlagen mit wechselnder Payload

Motivation

- Datenerfassung im wissenschaftlichen Umfeld
- Viel Legacy-Technik
- Wandel ist absehbar
- IoT anwenden oder gar selbst bauen?

Ziele

- Anpassung an wechselnde Payload
- Langfristige Nutzbarkeit
- Pflegeleicht

Rahmen

- Professionele metrologische IT
- Vorhandene Infrastrukturen nutzen
- Fehlende Infrastrukturen erkennen und anstoßen

Karlsruher Institut für Technologie

Stabilität

vs.

Wandel

Bisheriger Stabilitätsbegriff

- Unveränderte Systemfunktion über die Betriebszeit
- Verstärkte Legacy-Probleme

Instabil, weil unflexibel

- Kein Betriebssystemsupport
- Erzwungener Umstieg IoT-Hardware
- Eigene Installation zu aufwändig

- Somit Legacy
- Umstieg auf neue Plattform, obwohl Hardware sehr gut ist

Stabilität

DURCH

Wandel!

Moderne Stabilität

- Dauerhafte Funktion im Wandel
- Längere System-Zyklen
- Legacy-Probleme reduziert

- Beispiel:
- PC-Industrie Anfang der 2000er
- Virendurchsetzt, ganze Netze down

IT-Stabilität durch Veränderung

- Automatisierte Installation
- Systematische Updates
- Funktions-Überwachung

- Ebenso Linux und Pi: stabil

Wandel der Anforderungen

- Rechtliche Situation: Umweltmessungen gerichtsfest?
- Konservative Medien ziehen die Messungen in Zweifel
- Es wird mehr Messstellen geben
- IoT als Dienstleistung

Metrologische Informationstechnik

- Physikalisch-Technische Bundesanstalt
- Fachbereich 8.5

- “Sollte es nicht möglich sein, Schlüsselmaterial auf einem Gerät ausreichend zu sichern, kann versucht werden, im Zentralsystem Routinen vorzusehen, die es ermöglichen, kompromittierte Geräte zu detektieren und auszuschließen“

- “In diesem Kontext sind Methoden relevant, die darauf abzielen, kompromittiertes bzw. anomales Verhalten von Geräten mithilfe von maschinellen Lernverfahren zu detektieren“

- Quelle: https://oar.ptb.de/resources/show/10.7795/310.20160499 „Metrologische IT, Teil I“

- “Informationssicherheit lässt sich generell nie vollumfänglich lösen. Anstatt dessen versucht man, den Aufwand für Angreifer auf realistisch prohibitive Niveaus zu heben.“

Sicherheit: Schutzziele

- Vertraulichkeit
- Integrität
- Authentizität
- Nichtabstreitbarkeit
- Zurechenbarkeit
- Privatsphäre
- Verfügbarkeit

- Quelle: http://www.kryptowissen.de/schutzziele.php
- Quelle: Buchmann 2013, Dullien 2018

Metrologische Informationstechnik

- Variante:
- Stromsparende Microcontroller
- Solar autark
- Code gut bis sehr gut geschützt

- Erfordert Low-Power Netzwerke
- Keine automatisierten Updates
- Funktionsupdates schwierig
- Keine Überwachung

Metrologische Informationstechnik

- Variante:
- Kleincomputer mit Betriebssystem
- Überwachung möglich
- Sicheres Deployment machbar

- Stromzufuhr nötig
- Betriebssystem und Medium „in the Wild“
- Betrieb wie im Rechenzentrum

Deployment

- Medium beschreiben, ID hinterlegen
- Booten
- Netzwerk autokonfiguriert (IPv6)
- Software- und Schlüsselverteilung mit Ansible

Sicherheit

- Zugriff auf Systeme ausschließlich per Key
- Nur durch Deployment-Automatismen
- Notfall-Account und Key bereitstellen und sichern
- Alle Datenübertragungen verschlüsselt

Authentizität / Nichtabstreitbarkeit

- Datenablage nur mit Schlüssel / Account
- Daten signieren, am besten ab Sensor
- Softwarestände dokumentieren
- Zeitverlauf des Schlüsselinventars speichern

Public Key Infrastructure PKI

- Sehr aufwändig
- Als Service verfügbar
- Anbindung an Netz-Infrastrukturen schwierig
- Buchmann 2013 „Introduction to Public Key Infrastructures“

Public Key Infrastructure PKI

- Schlüsselerzeugung per API
- Automatisches Deployment auf Systeme
- Überwachung und Deaktivierung der Schlüssel nötig

Alternative: LDAP

- Anbindung an Netzwerke einfacher
- APIs verfügbar
- Netzwerkabsicherung gleichwertig

Vertraulichkeit

- Betriebsystem und Nutzlast können getrennt werden
- Container oder Virtualisierung möglich
- Mandatenfähigkeit
- VPN

Sicherheit

- Accounts etc müssen pro Gerät einzigartig sein
- Netze müssen strikt getrennt sein (Wifi2VLAN)
- Gateways müssen sicher sein
- Edge-Computing: Sicher?

Softwareentwicklung

- Alle Programmiersprachen werden verfügbar
- Netzwerkstacks werden durchs Betriebssystem bereitgestellt
- Hardware-Spezialisten schreiben die Datenerfassung

- CI / CD möglich
- Code-Signierung
- Versions-Monitoring

Probleme

- PKI ist ein Biest
- Medium derzeit nicht zu schützen
- Kultur der metrologischen Informationstechnik

Mängel im System

- PKI
- Keine zuverlässige Laufwerksverschlüsselung
- Deployment des Grund-Betriebssystems nicht automatisiert

Neue Möglichkeiten

- IoT-Infrastruktur als Service
- Mehrere Kunden sicher getrennt auf einer Infrastruktur
- Edge-Computing sicher und als Service

Fazit

- Betriebssysteme sind an neue Bedarfe anpassbar
- Schnelle Entwicklungszyklen
- Sehr gute Sicherheitskonfiguration machbar
- Investition in Know-How notwendig