Embedded Security

Die wichtigsten Gegenstände unserer persönlichen Identität sind unser Ausweis, Kreditkarten, Handy, Passwörter zu Accounts und unser Haustürschlüssel. Wie sehr unterscheiden sich diese Sachen zu den Geheimnissen und Identität auf einem Embedded Device? Was sind die Folgen, wenn Sie in falsche Hände geraten?

Embedded Geräte sind in sehr unterschiedlichsten Bereichen im Einsatz und die Verfügbarkeit von wichtigen Diensten in unserem Leben hängen davon ab. Die Vernetzung der Geräte untereinander und mit Servern / Clouds nimmt immer weiter zu. Meist stehen die Funktionen eines Gerätes im Vordergrund und nicht dessen Absicherung vor ungewollten und gewollten Missbrauch.
Dieser Vortrag gibt einen Einblick, welche Schnittstellen und Komponenten bei Embedded Devices wie gefährdet sind. Ein wichtiger Schwerpunkt sind auch die notwendigen technischen und organisatorischen Möglichkeiten zur Absicherung eines Embedded Devices.

Die Frage ist leider nicht, wie hoch die Wahrscheinlichkeit ist, dass Ihre Geräte angegriffen werden, sondern eher wann es geschehen wird und wie gut Sie darauf vorbereitet sind.
Ihr Gerät ist dabei nicht unbedingt das Hauptziel, sondern es kann auch die Tür in ein Server-System oder Industrieanlage sein.

Dipl. Ing. (FH) Maik Otto, Security-Ingenieur bei PHYTEC