Kapitel 8

Sicherheit Grundlagen

Übersicht

In eingebetteten und mobilen Systemen sowie im Allgemeinen in der Informationstechnik ist Sicherheit ein komplexes und umfangreiches Thema. Neben einer Darstellung der aktuellen Situation vermittelt dieses Kapitel die erforderlichen Grundlagen und Begriffe, um tiefer in diese Thematik einzusteigen.

Lernziele
Nach Abschluss des Kapitels

- ist Ihnen die Notwendigkeit von Sicherheitslösungen bewusst,
- sind Ihnen die grundlegenden Begriffe bekannt,
- sind Sie mit dem Konzept Trusted Computing vertraut.

8.1 Einleitung

Sicherheitsanalysen verdeutlichen häufig große Sicherheitsprobleme von heute im Einsatz befindlichen eingebetteten Systemen. Da die Hauptursachen für diese Probleme in den meisten Fällen auf Unkenntnis oder Unachtsamkeit zurückzuführen sind, müssen die erforderlichen Grundlagen vermittelt und ein Sicherheitsbewusstsein geschaffen werden. So lassen sich konzeptionelle Mängel, Implementierungsfehler, Fehler bei der Systemadministration und Benutzungsfehler vermeiden.

8.2 Sicherheitsbedarf

In unserer modernen Gesellschaft nimmt die Menge an Systemen in der Informationstechnik (IT) und deren Vernetzung stetig zu. Denkt man hier in erster Linie an Personal Computer (PCs) so wird deren Anzahl schon lange durch die große Zahl an Eingebetteten Systemen übertroffen. Mehr als 95 % der weltweit produzierten Mikroprozessoren werden mittlerweile in diesen Systemen verbaut, die in allen Bereichen der Technik vertreten sind. Sowohl im privaten als auch im industriellen Umfeld übernehmen diese Systeme immer mehr Aufgaben, was sie nahezu unverzichtbar macht. Eingebettete Systeme sind für die Steuerung von großen Fertigungs- und Industrieanlagen genauso verantwortlich, wie für den Betrieb von Consumer Produkten und Haushaltsgeräten. Auch aus dem Automobilbereich sind sie nicht mehr wegzudenken. So sind in einem modernen PKW mehr als 80 eingebettete Steuergeräte für die unterschiedlichsten Funktion vorhanden.

Durch ihre hohe Verbreitung rücken solche Systeme immer weiter in den Fokus von gezielten Angriffen. Mit der Zahl und der Häufigkeit der Angriffe steigen auch die durch sie entstandenen Schäden.

Von großer Bedeutung ist dies vor allem im industriellen Umfeld, da hier überwiegend Eingebettete Systeme zum Einsatz kommen. Waren diese Systeme früher noch durch eine sogenannte "Airgap" geschützt, weil sie nicht mit dem restlichen Netzwerk verbunden waren, so stellen sie heutzutage durch die zunehmende Vernetzung und ihre schlechte Umsetzung eine große Anzahl an Angriffszielen für Hacker dar. Um den laufenden Prozess nicht zu gefährden ist es in der Industrie nur selten möglich, notwendige Sicherheitsupdates durchzuführen, wie man sie aus der klassischen IT kennt. Im Gegensatz zu herkömmlichen IT-Systemen, in denen Geräte selten Laufzeiten über 5 Jahre haben, sind in Industrieanlagen Laufzeiten bei denen ein System 20 Jahre oft ununterbrochen im Einsatz ist keine Seltenheit. Durch die existierenden Schwachstellen und dem oft fehlenden Bewusstsein dafür, sind nicht nur professionelle Angriffe wie z.B. durch Stuxnet (2010), Duqu (2011) oder Flame (2012), sondern auch Angriffe mit einfachen Methoden wie z.B. vorgefertigte Skript-Angriffe oder Denial of Service (DoS) Attacken erfolgreich.

Es wird deutlich, dass die bisher eingesetzten Maßnahmen zum Schutz von Eingebetteten Systemen oft unzureichend oder für bestehende Anwendungen ungeeignet sind. In vielen Fällen werden, wie in beschrieben, Eingebettete Systeme sogar ohne jeglichen Schutz mit dem Internet verbunden.

8.3 Sicherheit - Security vs. Safety

Für den deutschen Begriff "Sicherheit" existieren im Englischen zwei Übersetzungen.

Diese beiden Wörter bezeichnen, anders als im Deutschen, zwei unterschiedliche Verständnisweisen von Sicherheit. Bedingt durch diese Ungenauigkeit der deutschen Sprache, ist eine exakte Definition des Begriffes notwendig.

Spricht man von **"Safety"** so ist damit die

eines Systems gemeint. Diese gewährleistet ein Betriebsverhalten innerhalb definierter Parameter, sowie den Schutz der mit dem System interagierenden Umgebung. Die Absicherung eines stromführenden Leiters gegen menschlichen Zugriff ist ein mögliches Beispiel für diese Art von Sicherheit. (vgl. VDI/VDE 2182)

Bei **"Security"** spricht man von

Durch sie wird eine Manipulation des Systems, sowie der Zugriff auf geschützte Daten verhindert. Das System wird also vor der Umgebung geschützt. Die Abfrage eines Passwortes bei der Anmeldung an einem PC ist ein klassisches Beispiel für Security. (vgl. VDI/VDE 2182)

8.4 Schutzziele

Informationen bzw. Daten sind zu schützende Güter (Assets) von informations- bzw. datensicheren Systemen. Um ausgewählte Assets zu schützen, werden Schutzziele definiert.

Unter der Authentizität versteht man die Echtheit und Glaubwürdigkeit eines Objekts bzw. Subjekts. Sie ist anhand einer eindeutigen Identität und charakteristischen Eigenschaften überprüfbar.

Ein System gewährleistet die Datenintegrität, wenn es Subjekten nicht möglich ist, die zu schützenden Daten unautorisiert und unbemerkt zu manipulieren.

Ein System gewährleistet die Informationsvertraulichkeit, wenn es keine unautorisierte Informationsgewinnung ermöglicht.

Ein System gewährleistet Verfügbarkeit, wenn authentifizierte und autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.

Man sagt, dass ein System die Verbindlichkeit bzw. Zuordenbarkeit von Aktionen gewährleistet, wenn es nicht möglich ist, dass ein Subjekt im Nachhinein die Durchführung einer solchen Aktion abstreiten kann.

In bestimmten Fällen können auch Anonymisierung und Pseudonymisierung Schutzziele sein (z.B. Kommunikation über Internet).

8.5 Bedrohungen

Grundsätzlich kann man die Bedrohungen denen ein IT-System ausgesetzt sein kann in zwei Klassen unterteilen:

Diese Art von Bedrohungen ist dem Aspekt der Safety zuzuordnen. Beispiele hier zu sind höhere Gewalt (Blitzschlag, Feuer, Erdbeben, ...), technisches Versagen und Fehlfunktionen, sowie Fahrlässigkeit (Irrtum, Fehlbedienung). Maßnahmen, die man gegen solche Bedrohungen ergreifen kann, umfassen Methoden des Software Engineering und die Schaffung von Hardware und Software Redundanzen.

Ein IT-System kann unterschiedliche Schwachstellen besitzen. Wird eine dieser Schwachstellen ausgenutzt, so kann es zu Beeinträchtigungen der Datenintegrität, Informationsvertraulichkeit oder auch Verfügbarkeit kommen. Diese Art von Angriffe fallen unter den Aspekt Security.

8.6 Trusted Computing

Der Begriff Trusted Computing (TC) oder auch Trustworthy Computing wird erstmals im Standard Trusted Computer System Evaluation Criteria des Verteidigungsministeriums der USA (Department of Defense) im Jahr 1983 definiert. Dieses auch unter dem Namen Orange Book bekannte Dokument bildet die Grundlage für den international anerkannten Standard zur Zertifizierung von IT-Systemen *Common Criteria For Information Technology Security Evaluation*.

Im Jahr 1999 wird die Trusted Computing Platform Alliance (TCPA) von den Mitgliedern Compaq, Hewlett-Packard, IBM, Intel und Microsoft gegründet um industrielle Standards für vertrauenswürdige Computersysteme zu spezifizieren. Aufgrund eines ineffektiven Entscheidungsprozesses, bei dem sämtliche Beschlüsse einstimmig sein mussten, und zunehmender öffentlicher Kritik, wird dieses Konsortium 2003 von der neu gegründeten Trusted Computing Group (TCG) ersetzt. Die TCG übernahm die bis dahin entstandenen Spezifikationen. Viele Mitglieder der TCPA werden auch Mitglied in der TCG.

Der Begriff „Trusted Computing“ wird im Jahr 2004 von der TCG wie folgt definiert:

Die zur Umsetzung des TC-Ansatzes notwendigen Anpassungen der Hardware werden von der TCG als Trusted Computing Platform TCP definiert. Dies beinhaltet sowohl zusätzliche Bauteile wie z.B. Sicherheitschips als auch Veränderungen an der verwendeten Firmware.

Das Konzept eines Vertrauensankers (Root of Trust) mit einer darauf aufbauenden Vertrauenskette (Chain of Trust) ist ein Kernelement einer TCP. Die Vertrauenswürdigkeit dieses Ankers wird durch externe Zertifikate sichergestellt. Wie in Abb. 8.1 dargestellt, definiert die TCG drei Vertrauensanker, die zusammen den Trusted Building Block TBB bilden.

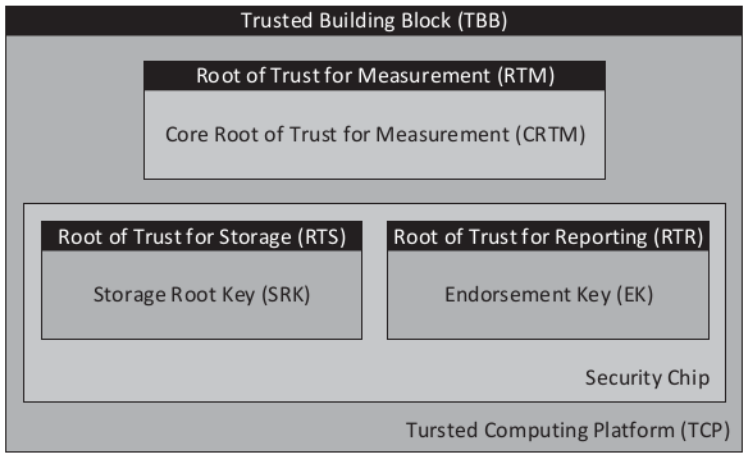

Abbildung 8.1: TBB der TCG (vgl. Müller 08)

- Der RTM ist die Grundkomponente für Integritätsmessungen die sicherstellen, dass das System in einem vertrauenswürdigen Zustand startet. Die dafür erforderlichen Messwerte werden von der Core Root of Trust for Measurement (CRTM) erzeugt, die nach dem Einschalten als erste Komponente auf dem System ausgeführt wird.

- Der RTR ist für den Aufbau einer Plattform-Identität und für die sichere Übertragung des aktuellen Zustands des Systems verantwortlich. Grundlage dafür ist ein RSA-Schlüsselpaar, der sog. Endorsement Key EK. Durch den EK und dessen Zertifikat werden Attestation Identity Keys AIKs erzeugt, mit denen der aktuelle Zustand gegenüber einer dritten Partei attestiert werden kann.

- Der RTS ist für den Schutz von sensiblen Daten verantwortlich. Darunter fallen Messwerte, die den aktuellen Zustand des Systems darstellen, ebenso wie kryptographische Schlüssel. Für diese Aufgabe besitzt der RTS ebenfalls ein RSA-Schlüsselpaar, den sog. Storage Root Key (SRK), mit dem andere Schlüssel oder Daten verschlüsselt werden.