Bild: Fotolia/by-studio

Türstopper und freundliche Türaufhalter sollten das Sicherheitskonzept einer Zutrittskontrollanlage nicht aushebeln können.

Sicherheitslücken in Zutrittskontrollanlagen

Unerkannte Angriffe

Walter Wilke

Seit den Mifare-Classic- und Legic-Prime-Hacks wird die Sicherheit der Datenübertragung von Transpondersystemen diskutiert. Objekte, in denen ein gehackter Transpondertyp verwendet wird, sind potenziell gefährdet. Aber es gibt noch andere Sicherheitslücken in Zutrittskontrollanlagen.

So gibt es technische Angriffsmethoden, deren praktische Anwendung vor allem deshalb nicht bekannt ist, weil sie keine Spuren hinterlassen. Die Angriffsmethoden sind teilweise recht zeitaufwändig und erfordern außerdem technische Kenntnisse. Auch potenzielle Angreifer werden eine Kosten-Nutzen-Betrachtung anstellen. Die Kardinalfrage lautet: Was gibt es zu gewinnen, und geht es nicht einfacher? Ein Berechtigter hält höflich eine Tür auf. Türen werden unterkeilt und mangels Türoffenzeitüberwachung wird dies nicht bemerkt und abgestellt – das nur am Rande. Weiteres Thema ist die Sicherheit der Datenübertragung in Zutrittskontrollanlagen (ZKA) gegen Angriffe.

Datenfluss in ZKA

Die vereinfachende Prinzipdarstellung zeigt die Schnittstellen zwischen den wesentlichen Funktionselementen einer ZKA. Diese Schnittstellen sind gleichzeitig auch die möglichen Angriffspunkte. An erster Stelle steht die Luftschnittstelle. Die Kommunikation zwischen Ausweis und Ausweisleser findet hier statt. Die Mikroprozessoren (µ-Prozessoren) in Transponder und Ausweisleser und das dort laufende Programm und Protokoll sind spezifisch für den eingesetzten Transpondertyp, und werden beide im Regelfall durch den Hersteller des Transponders (wie Mifare, Legic, HID) hergestellt.

Der Ausweisleser wird durch einen Mikroprozessor des Herstellers der Zutrittskontrollanlage gesteuert. Dieser gibt über Schnittstelle a dem transponderspezifischen Mikroprozessor unter anderem vor, welches Segment des Ausweises gelesen werden soll, und erfährt über diese Schnittstelle, ob ein gültiger Ausweis erkannt wurde, sowie dessen Ausweisnummer. Der Ausweisleser kommuniziert über

Schnittstelle b mit der Zutrittskontrollzentrale (ZKZ) und übermittelt die gelesene Ausweisnummer an die ZKZ. In der ZKZ sind alle für diesen Zutrittspunkt berechtigten Ausweisnummern mit ihren Zutrittsprofilen (Raum- und Zeitzonen) gespeichert. Dort wird nach Prüfung der erforderlichen Zutrittsrechte der erkannten Ausweisnummer entschieden, ob die Tür freizugeben ist.

Die ZKZ wiederum ist über Schnittstelle c mit dem Server der ZKA (ÜZKZ, übergeordnete Zutrittskontrollzentrale) verbunden. In der ÜZKZ werden alle Nutzer der ZKA mit ihren Ausweisnummern und Zutrittsprofilen verwaltet. Ausweisnummern und zugehörige Zutrittsprofile werden in regelmäßigen Zeitabständen und nach Datenänderungen an die ZKZ übertragen. Dies ist, auf das Wesentliche reduziert, das Funktionsprinzip einer ZKA.

Die Luftschnittstelle

Die Sicherheit der Datenübertragung der Luftschnittstelle hängt direkt von der Integrität der Sicherheitsmechanismen des Transpondertyps ab. Sind diese überwunden, können Ausweise geklont und verfälscht werden. Dies ist jedoch nur dem möglich, dem die Sicherheitsmechanismen des gehackten Transpondertyps bekannt sind, und der Zugriff auf den gehackten Transpondertyp hat. Wird ein gehackter Transpondertyp verwendet, ist im Rahmen einer objektspezifischen Risikobetrachtung zu entscheiden, ob und welche Maßnahmen einzuleiten sind. Muss der Transpondertyp gewechselt werden, sollte unter Abwägung der bestehenden Risiken eine Migrationsstrategie zu einer sicheren Ausweistechnologie entwickelt und umgesetzt werden. Weitere Angriffsmöglichkeiten sind:

1. Der Relay-Angriff
Ausweisleser nach ISO 14443 haben eine Reichweite von fünf bis zehn Zentimetern. Durch Positionierung eines bidirektionalen Sender-Empfänger-Verstärkers mit höheren Feldstärken im Umfeld des Ausweislesers kann die Reichweite auf einige Meter vergrößert werden. So ist es denkbar, dass bei Nutzung eines solchen Geräts ein mit Abstand vorbeigehender Zutrittsberechtigter mit seinem Ausweis unfreiwillig eine Tür freischaltet, die dann geöffnet werden kann. Da Ausweis und Ausweisleser beide systemzugehörig sind, und tatsächlich über die größere Entfernung miteinander kommunizieren, wird dies nicht festgestellt. Gegen einen solchen Angriff helfen nur technische Maßnahmen im Ausweisleser, wie die Überwachung der Antwortzeiten, die bei größerer Entfernung länger sind.

2. Der Denial-of-Service-Angriff
Bei einem Denial-of-Service-Angriff (deutsch: Verweigerung der Funktion) wird durch einen aktiven Störsender das elektromagnetische Feld zwischen Ausweisleser und Ausweis so beeinflusst, dass die Kommunikation unterbunden wird. Dadurch wird zwar der Zutritt nicht erlangt, aber hier zeigen sich unter Umständen Mängel der Sicherheitsorganisation. Die denkbar schlechteste Lösung ist es, bei Störung eines Ausweislesers mit unbekannter Ursache die zugehörige Tür auf „dauerfrei“ zu schalten, damit hätte der Täter sein Ziel erreicht, unberechtigt Zutritt zu erlangen.

3. Schnittstelle a
Obwohl die Datenübertragung an Schnittstelle a zwischen den beiden Mikroprozessoren des Ausweislesers meist unverschlüsselt erfolgt, ist dies weniger kritisch. In einer aktiv genutzten, installierten ZKA ist diese Schnittstelle kaum zerstörungsfrei zugänglich und nutzbar. Häufig sind die Funktionen der beiden Mikroprozessoren des Ausweislesers auch in einem Chip vereint, und damit ebenfalls nicht zugänglich. Als Ziel eines Angriffs ist diese Schnittstelle nicht geeignet.

4. Schnittstelle b
Schnittstelle b als Verbindung des Ausweislesers mit der ZKZ ist außerhalb des Sicherheitsbereichs an den Anschlussklemmen des Ausweislesers zugänglich. Für Innentäter, gegebenenfalls auch durch Social Engineering „motivierbar“, ist sie entlang der gesamten Leitungsführung bis in die ZKZ, auch innerhalb des Sicherheitsbereichs, zugänglich. Insbesondere in älteren Anlagen wurde diese Schnittstelle als unverschlüsselte „Wiegand“- oder Clock-Data-Schnittstelle ausgeführt, die trotz ihrer Defizite nach wie vor angeboten wird. Unverschlüsselte Datenübertragung bedeutet, die übertragenen Daten können nicht nur ausgelesen, sondern auch „verstanden“ und damit nachgebildet oder verfälscht werden. In modernen Systemen erfolgt die Kommunikation dieser Schnittstelle im Regelfall über einen RS 485 BUS unter

Verwendung eines proprietären Protokolls des Herstellers der ZKA. Damit ist zwar eine verschlüsselte Datenübertragung prinzipiell möglich, aber längst nicht alle am Markt angebotene Systeme nutzen die Möglichkeit der Verschlüsselung.

5. Der Spoofing- und der Replay-Angriff
Bei unverschlüsselter Datenübertragung ist es möglich, ohne Beteiligung des Ausweislesers ein Datenpaket mit einer zutrittsberechtigten Ausweisnummer zum Beispiel auf einem Notebook zu generieren, und über die Anschlussleitung des Ausweislesers einzuspielen. Bei einem Replay-Angriff wird eine zuvor abgehörte und aufgezeichnete Datenübertragung zu einem späteren Zeitpunkt wieder eingespielt. Wird dabei eine Ausweisnummer mit Zutrittsberechtigung verwendet, erkennt die ZKZ keine Unregelmäßigkeit und wird die Tür freigeben. Hiervor schützt auch nicht jede Art von Verschlüsselung. Keinen Schutz gegen Replay-Angriffe bietet eine statische Verschlüsselung, bei der für alle Übertragungen derselbe Schlüssel verwendet wird. Das Datenpaket selbst ist zwar unverständlich, aber konstant für jeden einzelnen Ausweis. Es ist zwar nicht verfälschbar, jedoch erfolgreich wiederholbar. Schutz vor Replay-Angriffen bietet nur eine starke Verschlüsselung, für die vor jeder Datenübertragungssitzung zwischen Ausweisleser und ZKZ der zu verwendende Schlüssel neu ausgehandelt wird. Wiederholungen einer aufgezeichneten Übertragung werden dadurch von der ZKZ erkannt und nicht akzeptiert.

Denial-of-Service – Teil 2

Bei den meisten Systemen sind mehrere Ausweisleser „in Reihe“ auf den RS 485 BUS geschaltet. Dies trifft auch für die meisten Systeme zu, bei denen für jeden Ausweisleser eigene Anschlussklemmen in der ZKZ vorgesehen sind, die BUS-Topologie wird hier innerhalb der ZKZ gebildet. Bei einem Denial-of-Service-Angriff wird ein ständiger, beliebiger Datenstrom an beliebiger Stelle in den BUS eingespielt, wodurch für alle BUS-Teilnehmer, das heißt alle auf diesem BUS angeschlossenen Ausweisleser, keine Kommunikation mehr möglich ist. Aus „unerklärlichen“ Gründen funktioniert die Zutrittskontrolle nicht, und wie bereits oben gesagt, ist die Dauerfreischaltung der betroffenen Türen als Reaktion auf die Störung eine schlechte Lösung.

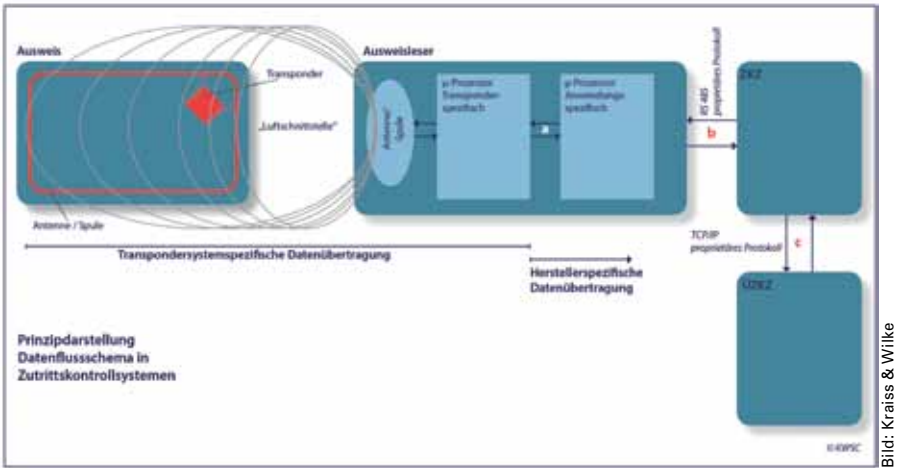

Bild: Kraiss & Wilke

Prinzipdarstellung des Datenflussschemas in Zutrittskontrollanlagen.

Sicherheit gegen äußere Angriffe schafft die Verwendung von geteilten Ausweislesern, bei denen nur die Antenne außerhalb, die Elektronik und die Anschlussklemmen des Lesers innerhalb des Sicherheitsbereichs angeordnet sind. Eine vollständige Sabotageüberwachung der Ausweisleser, Verteiler in der Leitungsführung und der ZKZ durch Deckel- und Abreißkontakte kann nur dann Erfolg zeigen, wenn die entsprechenden Meldungen bemerkt, angezeigt und unmittelbar, zum Beispiel durch Intervention, bearbeitet werden. Auch hier sei auf die Erfordernis einer funktionierenden Sicherheitsorganisation verwiesen, durch die Angriffe auf sicherheitstechnische Einrichtungen rechtzeitig bemerkt und abgewehrt werden können.

Schnittstelle c

Die Vernetzung der ZKZ mit der ÜZKZ erfolgt in heutigen Systemen über Ethernet unter Verwendung des Netzwerkprotokolls TCP/IP. Daten werden mittels herstellerspezifischer, proprietärer Protokolle übertragen. Es würde zu weit führen, im Rahmen dieses Beitrags auf grundsätzliche Fragen der Sicherheit von IP-Netzen einzugehen. Sicherheitsrelevante Anwendungen, so auch die Zutrittskontrolle, sollten immer über abgeschottete Netzwerksegmente kommunizieren, die als physikalisch getrenntes Netz oder „logisch" getrennt als Subnetz ausgeführt werden.

Prinzipiell können hier alle modernen und starken Verschlüsselungsverfahren eingesetzt werden. Die Vernetzung älterer Systeme erfolgt über RS 485 BUS, ähnlich wie unter Schnittstelle b beschrieben, jedoch ist das zu übertragende Datenvolumen deutlich größer als auf Schnittstelle b. Da Ver- und Entschlüsselung sowohl Rechenkapazität wie Zeit erfordern und das zu übertragende Datenvolumen erhöhen, erfolgt hier nicht bei allen Systemen eine verschlüsselte Übertragung. Unabhängig von der BUS-/Netztopologie sollte der physische Zugang zu den Knoten beschränkt und überwacht sein, um Denial-of-Service-Angriffe auszuschließen oder zumindest rechtzeitig zu erkennen. Erfolgt die Übertragung der Nutzdaten unverschlüsselt, ist dies umso wichtiger. Jeder, der Zugang zu dem Netz erlangt und das unverschlüsselte proprietäre Protokoll ausspäht, kann Daten auf der ZKZ verändern und sich selbst Zutrittsrechte zuweisen, die vom Sicherheitsverantwortlichen nicht vorgesehen sind. Einer Veränderung der Daten der ÜZKZ über das Netz stehen zusätzlich noch die Sicherheitsmechanismen der verwendeten Datenbank entgegen, sofern diese entsprechend eingerichtet sind.

Risikobetrachtung

Die beschriebenen Angriffsmethoden auf die Datenintegrität einer ZKA erfordern Vorbereitung, technische Kenntnisse und Zugangsmöglichkeit zu den einzelnen Funktionseinheiten. Ob zu erwarten ist, dass potenzielle Täter diesen Aufwand auf sich nehmen, sollte in einer Risikobetrachtung in einer frühen Projektphase bewertet werden. Entsprechend ist das Gesamtkonzept der Anlage einschließlich der begleitenden Sicherheitsorganisation zu entwickeln. Ob und welche Sicherheitsmaßnahmen in einer ZKA implementiert sind, ist bei deren Herstellern zu erfahren. Abschließend noch eine Anmerkung zur Sicherheit der Luftschnittstelle: Auch wenn die aktuellen Transpondersysteme der führenden Hersteller zurzeit sicher sind, ist es nur eine Frage der Zeit, bis auch diese überwunden werden.

Walter Wilke, Sicherheitsberater, Kraiss & Wilke Security Consult GmbH, www.kraiss-consult.de