Einflüsse von NFC-Smartphones auf das RFID-Bibliothekssystem

Eine Analyse des Bedrohungspotentials durch NFC-Smartphones und Beschreibung von möglichen Gegenmaßnahmen

Sebastian Krautz

Dieses Kapitel soll einen Einstieg in die Problematik von NFC-Einflüssen auf Bibliothekssysteme geben. Dazu werden die Eigenschaften der beteiligten Systemkomponenten kurz erklärt. Anschließend werden zwei Hauptangriffsszenarien mit den Auswirkungen für eine Bibliothek beschrieben. Des Weiteren werden mögliche Wege aufgezeigt, wie solche Angriffe verhindert werden können und was bei Einsatz solcher Lösungen beachtet werden muss.

Einleitung

RFID wird in Bibliotheken mittlerweile seit vielen Jahren erfolgreich eingesetzt. Die Technologie wird dabei sowohl zur Unterstützung von Prozessen innerhalb der Bibliothek, wie etwa der Ausleihe eines Buches, als auch zur Diebstahlsicherung genutzt. In den letzten Jahren hat sich dieses System bewährt und ist aus einer modernen Bibliothek nicht mehr wegzudenken. Dieses System steht nun jedoch vor einer Herausforderung.

In Asien bereits sehr weit verbreitet, setzt sich auch bei uns eine neue Technologie, die sogenannte Near Field Communication (NFC), immer mehr durch. Diese Technologie wird vor allem in neuen Smartphones¹ eingesetzt. Sie basiert im Grunde auf RFID. Damit stellt NFC quasi einen kleinen RFID-Reader für jedermann zur Verfügung. Warum stellt dieser Fakt nun eine Herausforderung für das RFID-Bibliothekssystem dar!? Es ist deshalb eine Herausforderung, da nun »jeder« mit entsprechenden Mitteln relativ einfach beispielsweise die zur Diebstahlsicherung verwendeten Parameter mit seinem Smartphone verändern und somit außer Kraft setzen kann.

Aber auch weitere Angriffspunkte sind durch die Verwendung von NFC gegeben. Welche dies genau sind und welche Ansätze es gibt, um diesen zu begegnen wird im weiteren Verlauf noch genauer beleuchtet.

¹ Smartphone: nach Definition ein Mobiltelefon, welches einen leistungsstarken Prozessor besitzt und zusätzliche Geräte, wie Kameras, MP3-Player und Navigationssysteme enthält. [vgl. eteleon.de]

Ausgangssituation

Die Verbreitung von NFC-fähigen Smartphones sorgt bei vielen Bibliothekaren und Bibliotheksmitarbeitern für erhebliche Bedenken hinsichtlich der Einflüsse und Möglichkeiten der neuen Technologie im Bibliotheksumfeld. Daher wurde diese Thematik im Rahmen einer Masterarbeit näher untersucht. Die folgenden Abschnitte sollen kurz die nötigen Hintergrundinformationen zu Technologie, Standards und beteiligten Komponenten liefern.

NFC-Technologie

Die Technologie entstand bereits 2002. Sie basiert auf der Funktionsweise von induktiven RFID-Systemen. Die benutzte Frequenz liegt im, von den Bibliotheken häufig verwendeten, HF-Bereich bei 13,56MHz. Damit können Datenraten bis zu 424 kbit/s erreicht werden [vgl. 1]. Die Technologie basiert also ebenfalls auf der Erzeugung magnetischer Felder. Diese werden über eine Erzeugerspule aufgebaut. Eine solche Spule ist in der Regel in den entsprechenden NFC-Smartphones enthalten. Die Gegenstelle bildet auch hier ein Transponder. Das besondere bei NFC ist jedoch, dass die Gegenstelle kein normaler Transponder sein muss, sondern es kann ebenfalls ein weiteres NFC-Smartphone sein. Das wird durch einen besonderen Modus bei NFC ermöglicht, der bei herkömmlichen RFID-Systemen nicht zur Verfügung steht.

Für die Technologie gibt es zwei zentrale Standards. Den ersten bildet das Near Field Communication Interface and Protocol 1 (NFCIP-1). Hinter diesem steht der ISO Standard 18092. In diesem Standard werden die Übertragungsprotokolle von MIFARE und FeliCa kombiniert. Außerdem werden diese darin um zusätzliche Kommunikationsmöglichkeiten erweitert. Als letztes Merkmal wird ein neues Transportprotokoll ergänzt. Durch diesen Standard werden drei Übertragungsgeschwindigkeiten definiert, die auf den enthaltenen Protokollen basieren. So werden 106kbit/s auf Basis von MIFARE und 212kbit/s und 424kbit/s auf der Basis von FeliCa vorgeschrieben. [vgl. 1]

Der zweite Grundstandard für NFC ist NFCIP-2 mit dem zugehörigen ISO Standard 21481. In diesem werden die Funktionalitäten verschiedener Systeme zusammengeführt. Dazu zählen Proximity²- und Vicinity³-Systeme. Zu den Vertretern der Proximity zählen ISO 14443A und ISO 14443B. Zu den Vicinity gehört ISO 15693. Geräte die auf dem ISO 21481 Standard basieren, können also in diesen drei Bereichen operieren. Dazu wird definiert, wie dabei die Auswahl eines der drei möglichen Modi zu treffen ist. Wie NFCIP-1 und NFCIP-2 in die NFC-Landschaft einzuordnen sind, ist in der nächsten Abbildung dargestellt.

-
- 2 Proximity: bezeichnet Systeme mit einer Reichweite bis zu zehn Zentimeter. Ein Reader wird dabei als Proximity Coupling Device(PCD) und ein Transponder als Proximity Integrated Circuit Card (PICC) bezeichnet.
 - 3 Vicinity: bezeichnet Systeme mit einer Reichweite bis zu 50 oder auch 100 Zentimetern. Ein Reader wird dabei als Vicinity Coupling Device(VCD) und ein Transponder als Vicinity Integrated Circuit Card(VICC) bezeichnet.

Abb. 1: RFID- und NFC- Normen im Zusammenhang [1]

Komponenten

An einem Angriff sind in der Regel verschiedene Komponenten beteiligt. Bei einem Angriff durch NFC ist zunächst das entsprechende Smartphone zu nennen. Über ein solches Gerät wird mittels einer speziellen Anwendung der Angriff durchgeführt. Hierfür kann jedoch nicht jedes NFC-fähige Smartphone verwendet werden. Viele der heute am Markt verfügbaren Geräte unterstützen nur die Standards im Proximitybereich. Bibliotheken verwenden jedoch Transponder nach Standard ISO 15693, also Vicinity Systeme. Es wird also ein Gerät benötigt, welches es erlaubt auch mit diesem Standard zu kommunizieren. Bisher leisten dies nur wenige Mobiltelefone.

Ein Beispiel dafür ist das Google Nexus S, welches auch für das Testen der Angriffe verwendet wurde. Die bereits erwähnten Transponder sind die direkt angegriffene Komponente. Da der ISO Standard 15693 keine extra Sicherheitsmechanismen bietet, lassen sich Speicherinhalte der Transponder von jedem, mit den nötigen Geräten, verändern. Durch die veränderten Transponderwerte können dann auch weitere Teile des Bibliothekssystems »angegriffen« werden. Das Sicherungsgate kann beispielsweise ein unrechtmäßig verändertes AFI-Byte nicht von einem ordnungsgemäß verändertem unterscheiden. Auch der Selbstverbucher und das LMS können nicht erkennen, ob die Werte im Transponderspeicher verfälscht wurden oder nicht. Das heißt über die direkt angegriffenen Transponder können die weiteren Komponenten des RFID-Bibliothekssystems ebenfalls attackiert werden. Welche Möglichkeiten genau bestehen und wie sich diese auswirken wird in den nächsten Abschnitten noch genauer beschrieben werden.

Angriffsszenarien

Dieser Abschnitt beleuchtet nun zwei der Hauptangriffsvarianten genauer. Dabei wird zunächst beschrieben, wie die entsprechenden Angriffe durchgeführt werden können. Zur Vorgangsbeschreibung gibt es zu jeder Variante noch eine Einschätzung hinsichtlich des Bedrohungspotentials und des Schadens, der durch die jeweilige Attacke entstehen kann, gegeben.

AFI-Change

Dieser Vorgang zielt darauf ab den Diebstahlschutz für Medien außer Kraft zu setzen. Wie bereits beschrieben, ist der ISO 15693 Standard ein offener. Das bedeutet die Transponder sind nicht durch kryptographische Methoden gesichert. Daher kann ein Angreifer ohne weiteres den Transponderinhalt und damit auch das AFI-Byte umschreiben. Für diesen Vorgang kann ein NFC-Smartphone mit entsprechender Applikation genutzt werden. Um dem AFI-Byte einen anderen Wert zu geben muss lediglich die Anwendung gestartet werden und das Smartphone kurz an das Buch gehalten werden. Das Gerät handelt dabei dann als ein RFID-Reader. Ein solcher Angriff dauert in der Regel nur einen sehr kurzen Moment und ist damit auch sehr unauffällig durchführbar.

Mediennummernlotterie

Diese Variante zielt auf das System an sich. Da das Bibliothekssystem mit den sogenannten Mediennummern arbeitet, sind hier auch Angriffspunkte zu finden. Über die Mediennummer aus dem Transponder wird der Bezug zum eigentlich Medium hergestellt.

Ein Angreifer kann nun ebenfalls mit Hilfe eines NFC-Smartphones und einer Anwendung die Mediennummer im Transponder verändern. Auch hier übernimmt das NFC-Smartphone die Rolle des RFID-Readers und ändert die Werte im Transponderspeicher. Je nach Applikation können hier zufällige Nummernkombinationen, manuelle Eingaben oder auch stets die gleiche Nummer verwendet werden.

Bedrohungspotential

Das Bedrohungspotential dieser Angriffe ist unterschiedlich zu bewerten. Der AFI-Change stellt objektiv gesehen zunächst die größere Bedrohung dar. Das hat mehrere Gründe. Eine für diesen Angriff benötigte Anwendung gibt es zwar noch nicht im Internet, kann aber mit wenigen Mitteln selbst erstellt werden. Die Durchführung eines solchen Angriffs erfolgt zudem sehr schnell, da das Umschreiben insgesamt nur wenige Sekunden benötigt. Ein weiterer Punkt ist die Unauffälligkeit des Vorgangs. Ein solcher Angriff könnte rein theoretisch auch mit einem standardmäßigen RFID-Reader durchgeführt werden. Ein solcher ist jedoch relativ groß im Vergleich zu einem Smartphone und muss durch einen Computer gesteuert werden. Damit würde man doch sehr schnell auffallen, was abschreckend wirkt. Mit einem Mobiltelefon tritt dieser Fall nicht ein. Ein Mobiltelefon hat heute fast jeder ständig dabei. Deshalb ist es nicht ungewöhnlich, wenn ein Besucher der Bibliothek mit einem Smartphone in der Hand an den Regalen steht.

Ein weiterer Grund, neben der Einfachheit und Unauffälligkeit dieses Angriffes, für das hohe Bedrohungspotential ist der Schaden, der dabei angerichtet werden kann. Durch das Außerkraftsetzen des Diebstahlschutzes können die Medien ohne Alarm durch die Sicherungstore bewegt und damit aus der Bibliothek entwendet werden. Gerade bei sehr hochwertigen Medien können dabei schnell hohe Schadenssummen entstehen.

Durch den fehlenden Alarm am Gate hat die Bibliothek zudem keine Übersicht über die entwendeten Exemplare, weshalb diese als noch in der Bibliothek vorhanden geführt werden, jedoch nicht zur Verfügung stehen. Man könnte nun dagegen argumentieren, dass für einen solchen Angriff entsprechendes Hintergrundwissen nötig ist. Das ist natürlich in gewissem Maße richtig. Um das System auszuhebeln muss der Angreifer zunächst davon Kenntnis haben, dass ein solcher Angriff überhaupt möglich ist. Und er muss um das Prinzip des AFI-Bytes als Diebstahlschutz wissen. Das sind jedoch nur kleinere Hürden. Begründet ist dies dadurch, dass es bereits eine kommerzielle Applikation für die Ausleihe über ein NFC-Smartphone getestet wird. Das heißt, es ist damit gezeigt, dass es möglich ist. Das »Wie« kann dann sehr schnell über das Internet recherchiert werden. Es bleibt deshalb bei der Gefahreinschätzung hoch.

Das Bedrohungspotential der Mediennummernlotterie ist geringer einzustufen, als der AFI-Change. Das hat mehrere Gründe. Einer der Gründe ist der Anreiz, der von diesem Angriff ausgeht. Da dieser Angriff nicht darauf abzielt Medien zu entsichern und aus der Bibliothek zu entwenden, ist dieser Angriff wohl eher für eine kleinere Gruppe interessant. Die Erfahrung zeigt, dass zu dieser Gruppe die Personen gehören, die Angriffe auf Systeme durchführen, nur um ihre Fähigkeiten zu testen oder zu testen, was sich mit einem solchen Angriff anrichten lässt. Was einen solchen Angriff ebenfalls weniger interessant werden lässt, ist das zusätzliche Wissen, was dafür benötigt wird. Als erstes muss ein Angreifer das Prinzip der Mediennummern kennen. Das allein reicht jedoch nicht aus. Er benötigt ebenfalls die Stelle im Speicherbereich, in dem die Mediennummer hinterlegt ist. Diese beiden Informationen sind notwendig aber nicht geheim. Wenn ein Angreifer sich mit der Materie intensiv beschäftigt, kann er sich das Wissen selbst aneignen. Dann müsste für das ändern der Mediennummer eine entsprechende Anwendung programmiert werden. Aber auch hier entstehen einige Hürden mehr. Es müssen hier mehrere Werte verarbeitet werden. Für diesen Angriff müssen zuerst Werte gelesen werden und anschließend die Transponder in den ausgewählten Medien umgeschrieben werden. Die Anwendung gestaltet sich damit komplexer. Das wirkt sich natürlich auf die nötige Zeit für die Erstellung aus, welche damit länger wird. Dennoch steigt sie nicht übermäßig an. Die Auswirkung dieses Angriffes ist kein Diebstahl wie beim AFI-Change. Dieser Angriff zielt darauf ab das Bibliothekssystem an sich durch die gefälschten Mediennummern zu stören, sobald ein angegriffenes Medium automatisch ausgeliehen werden soll. Ist die Mediennummer eines Mediums verändert, kann das Bibliothekssystem das reale Exemplar nicht mehr mit dem richtigen Eintrag in der Datenbank in Verbindung bringen.

Das heißt, es wäre zwar noch möglich ein Buch auszuleihen aber in der Datenbank würde ein anderes vermerkt werden. Bei nur wenigen Exemplaren fällt dies eventuell nicht sofort auf. So könnten die falschen Einträge dazu führen, dass Bücher die noch in der Bibliothek stehen, nicht mehr über Suchfunktionen gefunden werden können, weil sie als ausgeliehen gelten.

Ist ein großer Teil der verfügbaren Medien von diesem Angriff betroffen, könnte eine automatische Ausleihe über RFID vermutlich zum Erliegen gebracht werden, da die Datenbank die Änderungen nicht kompensieren kann. Für das Bedrohungspotential bedeutet

das, dass es nicht als gering eingeschätzt werden kann. Die Voraussetzungen für diesen Angriff sind zwar höher als beispielsweise beim AFI-Change aber die Auswirkungen sind dennoch verheerend, wenn man den Ausfall des Systems in Betracht zieht. Das Bedrohungspotential wird deshalb mit mittel bis hoch bewertet.

Als Gegenargument könnte man anführen, dass Bibliotheken häufig mehrere Tausend oder sogar mehrere Hunderttausend Medien besitzen und diese nicht ohne weiteres alle umgeändert werden können. Dies ist wohl richtig, wenn man von einem einzelnen Angreifer ausgeht. Es würde sich bei einer Zeit von etwa zwei Sekunden, für den reinen Umschreibevorgang, eine Zeit von über 55 Stunden bei 100.000 Medien ergeben. Für einen Einzelnen ein sehr hoher Aufwand. Geht man aber davon aus, dass solch ein Angriff von einer Gruppe durchgeführt wird, wird der Aufwand für jeden Einzelnen wieder schnell kleiner. Deshalb führt der zeitliche Aufwand der Durchführung hier nicht zu einer Herabstufung des Gefährdungspotentials. Ein weiterer Aspekt dieses Angriffes ist die Behebung. Ausgangspunkt für die Betrachtung ist eine Verfälschung der Mediennummern, eines großen Teils des Bestandes. Wenn nun auffällt, dass eine Veränderung an den Nummern vorliegt, muss diese auch wieder behoben werden. Das kann einen enormen Aufwand für die Mitarbeiter der Bibliothek bedeuten. Als erstes müssen nun die betroffenen Medien identifiziert werden. Um zu gewährleisten, dass keine Falschausleihen mehr durchgeführt werden, müsste dazu der gesamte Bestand untersucht werden. Das ist deshalb nötig, da nicht zu erkennen ist welche Bücher genau betroffen sind. Anschließend müssten die korrekten Mediennummern gesucht und wieder in den Transponder geschrieben werden. Dies allein bedeutet einen Zeitaufwand über mehrere Manntage, wenn man wieder von 100.000 Exemplaren ausgeht. Hinzu kommt, dass Mitarbeiter in dieser Zeit nicht ihren normalen Tätigkeiten nachkommen können.

Gegenmaßnahmen

In diesem Abschnitt werden nun einige Möglichkeiten aufgezeigt, wie sich solche Angriffe verhindern lassen könnten. Es handelt sich dabei um Ansätze, die jeweils für eine Bibliothek bewertet werden müssen. Das ergibt sich daraus, dass bestimmte Szenarien nur für gewisse Typen von Bibliotheken geeignet sind.

Verbot von Smartphones

Die erste vorgestellte Variante ist das Verbot von Mobiltelefonen. Diese Option sieht vor, den Benutzern das Mitnehmen von Smartphones in den Bibliotheksbereich zu verbieten. In den meisten Bibliotheken gibt es bereits ein Verbot für Taschen. Diese müssen vor dem Betreten abgelegt werden. Dafür gibt es häufig gesonderte Bereiche mit abschließbaren Fächern, in denen die Rucksäcke und Taschen verstaut werden können. Ein solches Verbot würde Angriffe auf das Bibliothekssystem verhindern, da die Geräte zur Durchführung fehlen würden. In dieser Hinsicht wäre der Effekt natürlich optimal. Es ergeben sich aber hier durchaus auch negative Aspekte, beziehungsweise Schwierigkeiten, die bei einem Verbot bedacht werden müssen.

Zu bedenken ist, dass ein solches Verbot einen deutlichen Einschnitt in die Freiheiten des Bibliotheksbenutzers darstellt. Eine Tasche oder einen Rucksack abzugeben, ist für viele wohl eher ein kleines Übel. Ein Smartphone zu verbieten, könnte jedoch auf wesentlich weniger Verständnis stoßen. Das liegt zum einen an der vielseitigen Nutzung der neuen Telefone. Für viele ist es heute weit mehr als nur ein Telefon, was durch die Bezeichnung Smartphone klar wird. So wird mit solchen Geräten heute häufig das Internet genutzt, geschattet, Musik gehört oder auch navigiert. Da viele heute die eben beschriebenen Möglichkeiten nutzen, dürfte es schwierig werden, die Benutzer dahingehend zu sensibilisieren, auf ihr Smartphone für die Dauer des Bibliotheksaufenthaltes zu verzichten. Solch ein Verbot könnte sich also eher negativ auf die Benutzerzufriedenheit auswirken.

Ein anderer Gesichtspunkt sind die positiven Nutzungsmöglichkeiten von NFC innerhalb der Bibliothek. Wie bereits erwähnt, wurde bereits eine Applikation getestet, die es Nutzern ermöglicht, ein Buch ganz offiziell über ihr Smartphone auszuleihen. Diese Option wäre durch ein Verbot natürlich ebenfalls nicht möglich. Aber auch weitere Dienste wären ohne ein geeignetes Gerät nicht möglich. So könnten beispielsweise Tags mit Standortinformationen an den Regalen angebracht werden.

Diese könnten nicht nur helfen den Benutzer durch die Bibliothek zu navigieren, sondern auch Informationen zur im Regal enthaltenen Literatur zur Verfügung zu stellen.

Eine Navigation würde nicht nur in großen Bibliotheken einen Vorteil bringen. Auch in kleineren Bibliotheken könnten neue Benutzer so besser zu einem gesuchten Medium geleitet werden. Ebenso wäre eine Applikation denkbar, die beim Lesen eines Buchtransponders Verweise auf ähnliche Literatur oder Benutzerbewertungen gibt. Ein Verbot von Smartphones würde also alle eventuellen zusätzlichen NFC-Dienste ebenfalls unmöglich machen. Aber nicht nur die Behinderung von Zusatzdiensten und die Benutzerzufriedenheit stellen dabei negative Aspekte dar. Auch die logistischen Rahmenbedingungen sind nicht zu vernachlässigen. So müssten, um eine solche Maßnahme durchzusetzen, Mitarbeiter abgestellt werden, die dafür verantwortlich sind. Diese müssten die Besucher auffordern bei ihnen ihre Mobiltelefone abzugeben. Es wäre dabei dann nötig, die Telefone dem Besucher zuzuordnen und entsprechend gesichert zu verwahren. Dieser Umstand ist nicht zu unterschätzen, da dafür permanent Mitarbeiter eingesetzt werden müssen. Und nicht nur die Mitarbeiter sondern auch Lagerplatz für die Telefone ist einzurichten. Dieses System hat auch noch andere Schwachstellen. Für eine hundertprozentige Umsetzung müssten Besucher kontrolliert werden, ob sie ihr Gerät auch wirklich abgegeben haben. Aber eine Personenkontrolle durchzuführen ist rechtlich nicht einfach umzusetzen. Dieser Aufwand würde für eine einfache Bibliothek wohl nicht gerechtfertigt sein. Außerdem würde man damit die Zufriedenheit der Besucher wohl deutlich senken.

Einschätzung der Variante Verbot

Wie gesehen, erzeugt ein Verbot einige Schwierigkeiten. Für eine einfache öffentliche Bibliothek oder auch Hochschulbibliothek, wird diese Maßnahme als nicht geeignet

angesehen. Der Zusatzaufwand, der sich durch die Anforderungen an Mitarbeiter und Lagerraum stellt sowie die Einschränkung der Benutzer und Zusatzmöglichkeiten, steht wohl nicht im Gegensatz zu den eventuellen Schäden. Anders könnte sich dies für eine Bibliothek mit hochwertigen Medien darstellen. Bei Sicherung von wertvollen Medien könnte ein Verbot von Mobiltelefonen eher einsetzbar sein. Das begründet sich zum einen schon durch den höheren Wert der Medien, zum anderen sind die Besucherzahlen dort häufig nicht so hoch wie in anderen Bibliotheksformen. Dadurch ließe sich eine Abgabe von Geräten leichter realisieren als in Bibliotheken mit hohen Benutzerzahlen.

Es ist deshalb abzuwiegen, ob der Aufwand für die Durchsetzung eines Verbotes, vor allem dem wirtschaftlichen Nutzen angemessen gegenüber steht.

Verschlüsselung

Eine weitere Möglichkeit den AFI-Change und die Mediennummernlotterie deutlich zu erschweren, ist der Einsatz von Transpondern, die die Möglichkeit der Verschlüsselung bieten. Zunächst ist zu sagen, dass diese Variante nicht in bestehende Transponder nachgerüstet werden kann. Es ist nur möglich neue Transponder in die Medien einzubringen. Durch diese Transponder kann dann jeder Zugriff auf Daten des Chips unterbunden werden, sofern nicht der entsprechende Schlüssel im anfragenden Gerät vorliegt. Ein Umschreiben des AFI-Bytes oder auch das Ändern von Mediennummern wäre so nicht ohne weiteres möglich. Es gilt auch hier, dass eine Verschlüsselung wie jedes andere System keine hundertprozentige Sicherheit bietet. Die verwendeten Verschlüsselungsverfahren, wie beispielsweise Triple Data Encryption Standard (3DES), erfordern einen Aufwand zum Aufbrechen, der einen extremen Zeitaufwand und außerordentliche Rechenleistung benötigen würde.

Als einsetzbare Transponder kommen mehrere Varianten in Frage. Transponder mit Verschlüsselung gibt es heute größtenteils im Bereich von ISO 14443. Das sind solche Transponder, wie sie auch bei Benutzerausweisen oder ähnlichen datenschutzkritischen Karten verwendet werden. Der Einsatz dieser Transponder bringt zu den Vorteilen auch einige Nachteile mit sich. Um mit diesen Tags zu arbeiten, müsste ebenfalls die verwendete Hardware umgerüstet werden. Da ein Bibliothekssystem mit ISO 15693 Transpondern arbeitet, sind natürlich auch die entsprechend passenden RFID-Reader für diesen Standard in Selbstverbucher und Gate integriert. Für die Kommunikation müssen also ebenfalls neue Reader eingebaut werden. Für ein Gate ergibt sich eine zusätzliche Schwierigkeit. Da die ISO 14443 Transponder nur für sehr kurze Distanzen ausgelegt sind, ist es nicht möglich ein Gate zur Sicherung zu verwenden. Durch diesen Umstand sind solche Transponder nicht zum herkömmlichen Diebstahlschutz geeignet. Sie könnten dennoch für die Ausleihe verwendet werden.

Durch den offenen Standard im Bereich ISO 15693 waren die ISO 14443 Transponder im HF-Bereich lange Zeit die einzigen, die eine Verschlüsselung ermöglichten. Seit neuestem gibt es aber auch im Bereich ISO 15693 Möglichkeiten eine Verschlüsselung durchzuführen.

Dabei werden proprietäre Verfahren genutzt, um die Transponder zu verschlüsseln, da solche Verfahren nicht im ISO Standard vorgesehen sind.

Eingesetzt werden solche Chips momentan eher im Bereich von Kartentranspondern. Es wäre aber auch möglich diese Chips in einfache Papierlabel zu integrieren. Obwohl diese Label sich am ISO 15693 Standard orientieren, ist es nötig Anpassungen an der bestehenden RFID-Hardware vorzunehmen. Die Reader können die Transponder zwar erkennen aber durch die Verschlüsselung nicht auf diese zugreifen. Daher muss, wenn möglich, der Algorithmus mit zugehörigem Schlüssel im Reader des Selbstverbuchers nachgerüstet werden. Ist eine Nachrüstung nicht möglich, müssen zu den Transpondern auch die entsprechenden Reader angeschafft und implementiert werden.

Den Vorteil den diese Transponder zu denen im Bereich von ISO 14443 besitzen, ist die Tatsache, dass die Reichweite hier größer ist. Diese wird auch nicht durch die Verschlüsselung eingeschränkt. Daher kann ein solcher Transponder ganz normal auch für den Diebstahlschutz eingesetzt werden, da auch die Funktionalität des AFI implementiert ist. Für die reine Diebstahlsicherung würden dabei am Gate keine Änderungen vorgenommen werden müssen. Sollen aber auch zusätzliche Informationen, wie die Mediennummer, bei gesicherten Transpondern ausgelesen werden, müsste auch hier nachgebessert werden. Es müssten dann die gleichen Veränderungen durchgeführt werden, wie bei den Selbstverbuchern.

Sonst könnten die Reader in den Sicherungsgates nicht auf die Daten der verschlüsselten Transponder zugreifen.

Einschätzung der Variante Verschlüsselung

Eine Verschlüsselung zu benutzen, ist zunächst als sehr positiv zu bewerten. Das Schutzniveau, welches dadurch erreicht wird, ist deutlich höher als eines bei unverschlüsselten Transpondern. Dadurch könnten also für einen längerfristigen Zeitraum Angriffe über NFC vermieden werden.

Zu beachten ist jedoch bei der Variante mit den ISO 14443 Transpondern die eingeschränkte Nutzungsmöglichkeit. Durch die Tatsache, dass die Transponder nicht wie gewohnt über ein Gate zur Sicherung eingesetzt werden können, würde ein erheblicher Einschnitt entstehen. Der Einsatz dieser Transponder ist also, wenn überhaupt, nur in speziellen Fällen empfehlenswert. Vom Funktionsumfang und damit der Einsatzfähigkeit her betrachtet stellen die neuen ISO 15693 Transponder, mit proprietärer Verschlüsselung eine wesentlich bessere Alternative dar. Diese Transponder wären, durch die Konformität zum ISO Standard, gut für den Einsatz in allen Arten von Bibliotheken geeignet. Der Schutz der dadurch erzielt werden könnte, würde Angriffe wie AFI-Change und die Mediennummernlotterie wirksam verhindern können. Damit ist der Einsatz von verschlüsselten Transpondern dieser Art zunächst durchaus positiv zu bewerten.

Diese Variante hat jedoch auch negative Aspekte, die ebenfalls betrachtet werden müssen. Solche Transponder sind durch die Komplexität entsprechend teurer, als

herkömmliche Transponder. Teilweise sind die Preise für solche Transponder um das Drei- oder Vierfache höher. In Bibliotheken, in denen ein RFID-System eingesetzt werden soll, muss also zunächst analysiert werden, ob der höhere Anschaffungswert überhaupt aufzubringen ist und dem Nutzen angemessen gegenüber steht. Ein weiterer Punkt der nicht unerheblich ist, ist die Tatsache, dass sich die Verschlüsselung nicht nachträglich in die Transponder integrieren lässt. Dieser Umstand bringt für Bibliotheken, die bereits RFID eingeführt haben einen großen Nachteil mit sich. Würde man die neuen Transponder einsetzen wollen, müsste man zunächst noch einmal Investieren um die Tags zu beschaffen. Dabei können, wie eben gesehen, schnell sehr hohe Summen anfallen. Das zweite Problem ist, dass diese Transponder in die Medien eingebracht werden müssen. Für die Bibliotheksmitarbeiter bedeutet dieser Umstand, dass der gesamte Bestand wieder die Konvertierung durchlaufen muss.

Hier entsteht ein nicht zu unterschätzender Personalaufwand. Durch die Bindung der Mitarbeiter in der Konvertierung entstehen natürlich auch zusätzliche Personalkosten. Ein Beispiel hierfür bildet die folgende Rechnung. Ausgegangen wird dabei von einer Bibliothek mit einem Bestand von 200.000 einfachen Printmedien. Ein Team aus zwei Mitarbeitern benötigt die für die Konvertierung die folgenden Arbeitskraftstunden (AKh):

200.000 / 3.500 Bücher pro Tag, zwei Personen und 8AKh 912AKh

Für weitere Einflussgrößen wie Fehlen, Rüstzeiten oder Marge des Anbieters muss ein zusätzlicher Faktor eingerechnet werden. Dieser wird mit 1,3 angesetzt.

Daraus ergibt sich: $912AKh * 1,3 = 1.185AKh$

Die Arbeitszeit allein, die für eine Konvertierung aufgewendet werden muss, ist bereits beträchtlich. Nimmt man nun einen Satz von 24€/h Vollkosten an, bedeutet dass, eine Summe 28.440€ für die berechneten AKhs. [vgl. 2] Auch hier entstehen also deutliche Kosten. Diese bereits einmal durch die Einführung von RFID in den Bibliotheken entstanden. Sollte nun das System auf verschlüsselte Transponder umgerüstet werden, würden diese Zeiten und Kosten abermals anfallen.

Was ebenfalls noch negativ ins Gewicht fallen kann, ist die Tatsache, dass es bisher nur wenige Anbieter solcher Transponder gibt und sich eine Bibliothek unter Umständen in Sachen Transponder von einem Hersteller abhängig machen könnte.

Zusatzdatenbank

Dieser letzte Lösungsansatz arbeitet nicht wie die vorher gezeigten Varianten mit der Sicherung von Transpondern. Es wird hier eine zusätzliche Datenbank genutzt, die auf einer Änderung der Arbeitsweise des Bibliothekssystems basiert. Bisher arbeitet der Großteil der Bibliothekssysteme mit den Mediennummern, die im Transponder hinterlegt sind. Diese werden zur Zuordnung der Transponder zu den Einträgen im LMS genutzt. Weiterhin wird das AFI-Byte verwendet um Medien mit Hilfe eines Gates vor Diebstählen zu sichern. Durch diese Arbeitsweise werden jedoch auch die vorgestellten Angriffe erst ermöglicht. Um nun einen solchen Angriff zu verhindern, ist es, wie gezeigt, möglich die

Transponder selbst zu sichern. Es gibt jedoch auch die Möglichkeit das System an sich anzupassen. Der erste Schritt dabei ist, von den Daten des Transponders nur die UID zu verwenden. Dadurch lassen sich die oben gezeigten Angriffe, die auf das AFI-Byte oder auch die Mediennummer abzielen, wirksam verhindern. Da die UID nicht veränderbar ist, kann diese auch nicht über ein NFC-fähiges Smartphone angegriffen werden.

Damit ist ein zunächst sehr einfacher Mechanismus zur Sicherung gefunden. Um diese Art des Schutzes nutzen zu können, müssen jedoch noch weitere Umstellungen vorgenommen werden. Auch das LMS muss an die neue Situation angepasst werden. Dazu muss sofern dies möglich ist, anstatt einer Mediennummer die UID des Transponders in der Datenbank gespeichert werden. Beziehungsweise ist es auch möglich, weiterhin eine Mediennummer zu benutzen. Diese wird dann nur innerhalb des LMS verwendet und mit der zugehörigen Seriennummer des Tags abgeglichen. So können an einem Selbstverbucher die UIDs der Medientransponder ausgelesen und an das LMS gesendet werden. Im LMS werden, wie sonst auch, die Daten abgeglichen und die Informationen zu den Medien zurück an den Selbstverbucher gesendet. Damit ist die Funktion der Selbstausleihe gewährleistet. Um die Sicherung der Medien zu gewährleisten wird eine entsprechende Datenbank verwendet. Für eine solche Datenbank gibt es unterschiedliche Möglichkeiten.

Als eine Variante könnte die Datenbank sämtliche UIDs der Medien der Bibliothek enthalten. Zu diesen wird dann der entsprechende Status gespeichert, also ob ein Medium gesichert oder entliehen ist. Wird nun am Selbstverbucher eine Ausleihe getätigt, wird nicht nur das LMS angesprochen, sondern auch die Datenbank, die nur den Status enthält. Dieser wird entsprechend gesetzt. Wird nun das Medium durch ein Sicherungsgate getragen, wird vom Transponder nicht das AFI-Byte, sondern die Seriennummer gelesen. Diese wird dann an die Datenbank gesendet und verglichen.

Ist das Medium nicht ordnungsgemäß entliehen, wird ein Alarm aktiviert. Da Transponder die zu anderen Anwendungen gehören nicht in der Datenbank sind, wird bei diesen auch kein Fehlalarm ausgelöst. Für die Umsetzung dieser Funktionalität müssen selbstverständlich Änderungen an den Komponenten vorgenommen werden.

Die Datenbank muss zunächst erstellt und eingerichtet werden. Da eine solche Datenbank relativ wenige Daten verarbeiten muss, sind auch die Anforderungen an die benötigte Hardware nicht außerordentlich. Für die Sicherung über ein Gate muss eine Verbindung zwischen der neuen Datenbank und dem Gate selbst bestehen. Wichtig ist, dass die Verbindung zwischen Gate und Datenbank sehr schnelle Antwortzeiten ermöglicht. Das ist notwendig, um auch zum richtigen Zeitpunkt einen Alarm auszulösen und diesen nicht verzögert anzuregen, zum Beispiel wenn sich das betreffende Medium bereits nicht mehr im Gate befindet.

Es muss zusätzlich eine weitere Verbindung vom Selbstverbucher zur Datenbank eingerichtet werden, um den Status für ein entliehenes Medium oder ein zurückgebuchtes Medium zu aktualisieren. Dadurch, dass das Gate nun nicht mehr allein für die Sicherung zuständig ist, sind auch hier die neuen Abläufe zu implementieren. Im günstigsten

Fall lassen sich diese ohne Probleme mit der bestehenden Firmware umsetzen. Ist dies nicht möglich, ist es nötig eine für diesen Anwendungsfall passende Firmware zu entwickeln.

Eine zweite Variante für eine Speicherung des Status von Medien wäre die Vorhaltung der Informationen direkt im Reader des Sicherungsgates. Dabei wird, im Gegensatz zum vorhergehenden Fall, keine zusätzliche Hardware benötigt. In der Regel besitzen RFID-Reader in Sicherungsgates einen sogenannten Pufferspeicher. In diesem können Transpondernummern abgespeichert werden. Diese Möglichkeit erlaubt es nun die Diebstahlsicherung zu gewährleisten. Dazu wird eine zusätzliche Verbindung vom Selbstverbucher zum Gate eingerichtet. Diese dient dazu die UUIDs von ausgeliehen Medien in den Pufferspeicher des Reader zu sichern und umgedreht, bei Rückbuchungen, diese zu entfernen. Wird nun ein Medientag im Gate erkannt, welcher nicht im Pufferspeicher hinterlegt ist, gibt das Gate einen Alarm. Es kann dafür nötig sein, einen größeren Speicher nachzurüsten oder Reader mit größeren Speichern anzuschaffen. Da der Speicher jedoch im Reader integriert ist sollten an dieser Stelle keine Zeitprobleme beim Überprüfen des Status auftreten.

Die Umstellung der Arbeitsweise ist hier etwas schwieriger. Die Transponder können zwar bei einer Ausleihe oder Rückbuchung entsprechend ausgelesen und dann einen Eintrag in der Datenbank erhalten, dies setzt aber voraus, dass die Daten noch nicht verfälscht wurden.

Das Gate müsste für die Zeit der Umstellung dann entweder zusätzlich noch über AFI sichern oder bei jedem Transponder der nicht in der Datenbank ist einen Alarm geben. Dadurch würde gewährleistet, dass bisher noch nicht erfasste Transponder gesichert sind. Andernfalls wäre es nötig, den gesamten Bestand zu erfassen. Liegen die Zuordnungen zwischen Medium und UUID bereits in irgendeiner Weise vor, kann dies jedoch auch schnell und einfach implementiert werden.

Einschätzung der Variante Zusatzdatenbank

Zunächst ist zu sagen, dass der Schutz, der durch die Änderung der Arbeitsweise erreicht werden kann, sehr hoch ist. Für Angreifer ist es nicht möglich, mittels NFC die UUID von Transpondern zu verändern. Und da weder AFI-Byte noch Mediennummer auf dem Tag verwendet werden, lassen sich auch darüber keine Angriffe mehr durchführen. Damit liegt der Schutz noch höher als bei den Varianten, die mit Verschlüsselung, Passwort oder anderen Sicherheitsmerkmalen arbeiten. Ein weiterer Vorteil ist, dass keine neuen Transponder angeschafft werden müssen. Somit müssen für diese keine Mittel für Beschaffung und Nachlabeln aufgewendet werden, was gegenüber Verschlüsselung eine erhebliche Einsparung darstellt. Die zusätzlich benötigte Hardware für Datenbank und Verbindungen ist in diesem Fall unwesentlich klein. Wie angesprochen, müssen hier auch Änderungen am LMS vorgenommen werden. Da aber wie bisher die Datensätze weiter verwendet werden können, muss nur eine zusätzliche Verknüpfung zwischen Mediennummer und UUID eingeführt werden.

Die beiden genannten Varianten besitzen beide Vor- und Nachteile. Bei der ersten Option können keine fremden Transponder Fehlalarme auslösen, da alle UIDs in der Datenbank hinterlegt sind. Allerdings können hier bei langsamer Verbindung oder Verarbeitung ungewollte Verzögerungen entstehen. Die zweite Option bietet schnellen Zugriff auf die gespeicherten Transponder. Da sich hier jedoch nur die ausgeliehenen Transponder im Speicher befinden, werden auch Alarme ausgelöst, wenn anwendungsfremde Tags durch das Gate gebracht werden. Nach heutiger Technik sollte die Verbindung zwischen Gate und Datenbank jedoch so aufzubauen sein, dass die benötigten Vorgaben erfüllt werden, weshalb diese Variante zu empfehlen ist. Auch wenn die Implementierung einige Risiken bergen kann, ist der erreichte Schutz ausgezeichnet. Bei Bibliotheken die ein System neu einführen, würde dieser Schritt bei der Konvertierung der Medien, mit angepasster Konvertierungssoftware, mit durchgeführt werden können.

Fazit

NFC findet mittlerweile immer stärkere Verbreitung in verschiedenen Anwendungsgebieten. Durch die Integration in neue Generationen von Smartphones gibt es nun quasi den RFID-Reader für jedermann. Auch wenn bisher noch andere Probleme in Bibliotheken überwiegen, wird es in Zukunft wichtig sein sich auch mit diesem Thema auseinander zu setzen. Die hier beschriebenen Angriffe zeigen welche Folgen NFC für eine Bibliothek mit RFID-System haben kann. Es ist deshalb wichtig sich schon frühzeitig um eine ausreichende Sicherung zu bemühen. Die hier gezeigten Maßnahmen stellen nur die ersten Ansätze dar und müssen von Bibliothek zu Bibliothek nach den entsprechenden Vorgaben auf Umsetzbarkeit untersucht werden.

Literatur und Internetquellen

- [1] Roland, Michael/Langer, Joseph (2010). Anwendungen und Technik von Near Field Communication (NFC), Springer-Verlag Berlin, Heidelberg
- [2] Kern, Christian (2011). RFID für Bibliotheken, Springer-Verlag, Berlin, Heidelberg