Sicherheitsaspekte eines Fernbedienungssystems für Intelligente Heime

Dr. Per Kaijser *Berater für IT-Sicherheit, Ismaning*

Ein System für ein intelligentes Heim kann mehrere Funktionen eines Hauses unterstützen, wovon einige für die Sicherheit zuständig sein können. In den meisten Fällen werden solche Funktionen im Hause ausgeführt, aber es ist auch möglich sie mit Fernbedienung, z.B. von einem Mobiltelefon via WAP-Technologie oder über Internet von einem PC, auszuführen. Wenn ein intelligentes Haus über diese Form von Fernbedienung gesteuert werden kann, muss man sich fragen ob Fremde auch diese Möglichkeiten bekommen können, um beispielsweise an einem kalten Wintertag die Heizung auszuschalten. Auch die Möglichkeit Informationen abzuhören oder zu lesen kann gefährlich sein, denn davon können potentielle Einbrecher profitieren und herausfinden, ob das Haus momentan leer oder bewohnt ist.

Risiken über Fernbedienungen können nicht nur durch Fremde entstehen. Auch der rechtmäßige Anwender kann der Verursacher für gefährliche Situationen sein. Dies ist besonders der Fall, wenn unerwünschte Befehle einfach durch falsche Bedienung oder Übertragungen gegeben werden. Wenn der Bewohner zu Hause ist, ist es im Gegensatz zur Fernbedienung einfach solche Fehler zu entdecken und zu korrigieren.

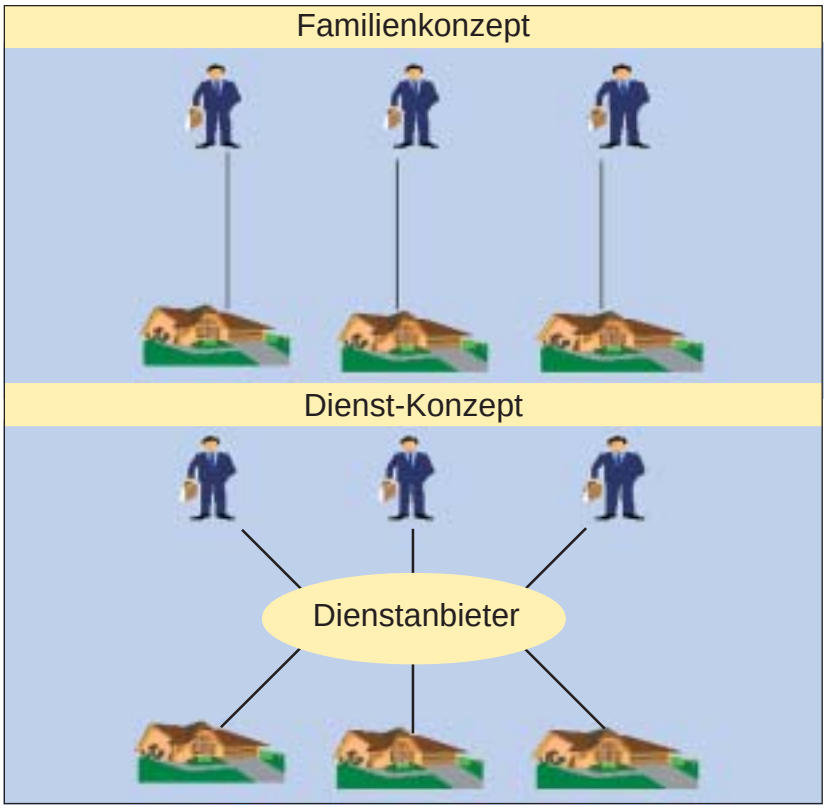
Sicherheitsprobleme durch Fernbedienung ist das Thema. Dazu werden zuerst die verschiedenen Sicherheitsaspekte eines Systems beschrieben. Die die für die Fernbedienung von Bedeutung sind werden dann in Zusammenhang mit Bedrohungen und Lösungen genauer behandelt.

Was ist Sicherheit ?

Es gibt viele Anforderungen um ein System eines intelligenten Hauses sicher zu machen. Die folgenden fünf komplementären Aspekte sind alle für ein sicheres und zuverlässiges System notwendig:

- Informationssicherheit (information security), die den Schutz von sowohl Informationen also auch das Informationssystem selbst betrifft, z.B. Korrektheit, Verfügbarkeit, und Vertraulichkeit der Information.

Dr. Per Kaijser ist selbständiger Berater für IT-Sicherheit in Ismaning bei München



- Sicherheit (safety), die Bedrohungen für Personen und die Umgebung verhindern sollen, z.B. Sicherstellen dass das Gerät keine gefährliche Strahlungen aussendet, oder dass kein elektrischer Schlag oder Feuer entstehen kann.
- Verlässlichkeit (reliability) ist ein Qualitätsmerkmal, das eine Aussage über die Stabilität des Systems, z.B. das es ausfallsicher ist, macht.
- Vertrauenswürdigkeit (assurance) ist ein anderes Qualitätsmerkmal, das über die Glaubwürdigkeit des Systems Aussagen macht, die hauptsächlich die Implementierung der verschiedenen Funktionen betrifft.
- Bedienbarkeit, die durch Minimierung möglicher Fehlbedienung die Fernbedienung sicher machen sollen.

Für die Fernbedienung sind nur der erste und letzte Punkt von Bedeutung, d.h. Informationssicherheit und Bedienbarkeit. Dies bedeutet nicht das die anderen weniger wichtig sind, nur das sie eigentlich mehr das System selbst betreffen und deswegen genau so wichtig sind, wenn das System lokal verwendet wird. Da die Bedrohungen und Lösungen für die beiden Punkte vollständig unabhängig sind, können sie auch unabhängig behandelt werden.

Bedienbarkeit

Es gibt zwei Klassen von Sicherheitsaspekten womit Fehlbedienungen minimiert werden können: (a) eine gute Bedienoberfläche (Man-Machine-Interface (MMI)), und (b) eine Konfiguration des Systems so dass nur unempfindliche Befehle über die Fernbedienung ausgeführt werden können.

Die Bedeutung eines wohl durchdachten MMI kann nicht genug geschätzt werden. Ein gutes MMI muss einfach für Laien zu verstehen und bedienen sein. Ist es zu kompliziert können Fehler schnell gemachen und wenn es zu einfach ist, kann man nicht genug Steuerfunktionen einbauen. Es ist fast mehr eine Kunst als eine Ingenieuraufgabe ein perfektes MMI zu entwickeln.

Ein Beispiel soll die Gefahr einer schlechten Konfiguration illustrieren. Es macht Sinn über die Fernbedienung – die Möglichkeit den Ofen auszuschalten anzubieten– aber es gibt gute Gründe, die

Möglichkeit den Ofen einzuschalten, zu verbieten. Nicht nur Befehle sondern auch Befehlswerte können durch eine Konfiguration begrenzt werden.
Als Ergebnis stellen wir fest, dass es zwei Lösungsansätze gibt, die Handhabung von Fernbedienungssystemen, sicherer zu machen durch

- die Bedienoberfläche (Man-Machine-Interface (MMI) und
- die Konfiguration erlaubter Fernbedienungsbefehle und Befehlswerte.

Informationssicherheit

Bedrohungen, Schutzmaßnahmen und Lösungskonzepte

Informationssicherheit hat laut Definition vier Eigenschaften:

- Vertraulichkeit, d.h. Schutz vor unbefugter Preisgabe von Informationen,
- Integrität, d.h. Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Programmen,
- Verfügbarkeit, d.h. Schutz vor unbefugter Vorenthaltung von Informationen oder Betriebsmitteln,
- Verbindlichkeit, d.h. eindeutige und nachweisbare Zuordnung von Aktionen zu den Personen, die sie ausgeführt haben.

Die wichtigsten Dienste der Informationssicherheit sind:

- Zugriffskontrolle (access control), d.h. ein Dienst der sicherstellt dass nur autorisierte Anwender den richtigen Zugriff auf Daten und Systeme haben, z.B. lesen, schreiben, vernichten oder verändern von Daten,
- Vertraulichkeitsschutz, d.h. ein Dienst der sicherstellt, dass nur autorisierte Anwender die geschützten Daten lesen können, z.B. durch Verschlüsselung von Daten,
- Integritätsschutz, d.h. ein Dienst der sicherstellt, dass Daten oder Programme nicht verändert werden, z.B. ist es möglich sicherzustellen, dass ein Empfänger nur Daten erhält die mit den abgesandte Daten identisch sind,
- Verbindlichkeit (audit), ein Dienst der sicherheitsrelevante Aktionen dokumentiert, u.a. wann und von wem sie ausgeführt wurden.

Um diese Dienste zu ermöglichen braucht man zusätzlich sowohl

- Authentifizierung, d.h. die Nachprüfung einer Identität, als auch
- die Verwendung von kryptographischen Verfahren.

Kryptographie ist notwendig für Vertraulichkeits- und Integritätsdienste für Kommunikationen. Für sowohl Zugriffskontrolle um die richtige Zuordnung Zugriffsrechte zu erteilen, als auch für die Verbindlichkeit um der Identität der ausführenden Person zu bestätigen ist Authentifizierung notwendig.
Zugriffskontrolle ist mit Abstand der wichtigste Dienst. Er stellt sicher, dass nur autorisierte Anwender Zugriff auf das Heim haben. Ohne Zugriffskontrolle können beliebige Anwender das intelligente Heim beeinflussen. Zum ersten Schritt in einem Zugriffskontrollsystem gehört die Bestätigung der Identität der Anwender durch einen Authentifizierungsmechanismus. Es gibt mehrere solche Technologien, einfache passwortbasierte Lösungen bis hochtechnische Lösungen basierend auf Smart Cards oder biometrischen Verfahren. Die beste und sicherste Lösung ist die, die zwei Komponenten enthält, (a) bei der der Anwender ein Geheimnis wissen muss, z.B. Passwort oder PIN, und (b) bei der der Anwender ein Gerät besitzen soll, z.B. ein Smart Card, oder eine biometrische Eigenschaft zeigen kann, z.B. die Stimme oder der Fingerabdruck.
Nach einer Bestätigung, dass der Zugriffsantrag von einem rechtmäßigen Benutzer kommt, kann der Zugriffsprozess weitergehen. Abhängig von der gewünschten Anwendung und der zugeordneten Zugriffsrechte des Anwenders wird das System über den Zugriff entscheiden. Das Zugriffskontrollsystem sollte so konfiguriert sein, dass es kontrollieren kann, welche Daten gelesen werden dürfen und welche Befehle und entsprechende Befehlswerte erlaubt sind. Es ist sinnvoll und sollte auch möglich sein, einem Anwender, der über Fernbedienung das Haus steuern möchte, weniger Zugriffsrechte zu vergeben als wenn er zu Hause ist.
Auch wichtig ist die Möglichkeit die Integrität der übertragenen Daten zu überprüfen. Eine Änderung der Daten kann entweder mit Absicht von einem Fremden oder unabsichtlich durch Störungen während der Kommunikation entstehen. Es gibt zwei Varianten von Schutzmaßnahmen. Für Störungen genügt eine error-correcting-code, aber mit diesem Mechanismus erhält man keinen Schutz gegen absichtliche Veränderungen. Dazu braucht man eine kryptographische Lösung. Deswegen ist ein solcher Integritätsdienst erforderlich, um die Kommunikation zwischen dem Anwender und dem Haus zu schützen.
Zwei weitere Dienste sind stark empfehlenswert. Einer davon ist die Kommunikation zu verschlüsseln um Vertrauensschutz zu gewährleisten. Der andere ist, einen Auditdienst (Verbindlichkeit) einzubauen um das System überwachen zu können, insbesondere ob jemand versucht hat einzudringen und vielleicht Daten unerlaubt geändert hat. Dies ist besonders wichtig wenn das System mit der Außenwelt verknüpft ist, denn wenn es z.B. einem Fremden gelingt sich im System als berechtigter Anwender zu registrieren, und dadurch die Integrität des Zugriffssystem zu zerstören, ist das Heim für ihn jederzeit offen.
Aufgrund möglicher Bedrohungen, der Ernsthaftigkeit und der Wahrscheinlichkeit ihres Auftretens, wird vorgeschlagen folgende Gewichtungen für Informationssicherheitslösungen für entfernt zugängliche intelligente Haussysteme zu wählen:

- Authentifizierungsmechanismus = unverzichtbar
- Zugriffskontrolle = unverzichtbar
- Integritätsdienst = fast unverzichtbar
- Vertraulichkeitsschutz = besonders zu empfehlen
- Verbindlichkeitsdienst (Audit) = besonders zu empfehlen

Es gibt mehrere technische Lösungen, die einige oder all diese Funktionen unterstützen. Zwei vollständig unterschiedliche Sicherheitsarchitekturen für den Schutzes sollen hier beschrieben werden. Das erste, das „Familienkonzept“ *(oberes Bild)* deutet darauf, dass der Inhaber des Hauses alles unter „seiner/ihrer“ Kontrolle hat. Das bedeutet, dass die Bewohner ihr Haus ansteuern. Das andere, das „Dienst-Konzept“ *(unteres Bild)* basiert auf einem Dienstanbieter, der Dienste für mehrere Bewohner anbietet, einschließlich der Sicherheitsdienstleistungen. In diesem Fall haben Bewohner unterschiedlicher Haushalte Zugang zum Dienstanbieter, der zuerst die Identität der Benutzer überprüft und den Zugriffskontrolldienst anbietet und dann erst nach Erfolg die Kommunikation zwischen den autorisierten Benutzern für das entsprechende Haus liefert.

Ein Dienstanbieter kann prinzipiell mehrere Dienstleistungen anbieten. Er kann routinemäßig die Korrektheit der Konfiguration und dass kein unautorisierter Benutzer Zugang zum System gehabt hat überprüfen. Beide Konzepte haben ihre Vorteile und Nachteile. Beide haben unterschiedliche Sicherheitsrisiken und haben demzufolge unterschiedliche Sicherheitsanforderungen.

Das „Familienkonzept“ hat den Vorteil, das alles eigener Steuerung unterliegt und der Hausherr braucht so keinem Außenseiter vertrauen. Andererseits erfordert es hohes technisches Kompetenz- und Sicherheitsbewusstsein. Es kann extrem schwierig sein, die Sicherheit des Systems aktuell zu halten, dass alle Konfigurationen korrekt sind und dass keine Fehler bei irgendwelchen Sicherheitsdienstleistungen gemacht werden. Eine Ausweichlösung könnte auch notwendig sein, wenn etwas Unerwartetes auftritt.

Das „Dienst-Konzept“ stellt hohe Anforderungen an den Dienstanbieter. Der Dienstanbieter muss in der Lage sein, die verschiedenen Benutzer zu unterscheiden, damit andere autorisierte Benutzer von einem intelligenten Haus nicht in der Lage ist, Informationen irgendeines anderen Kunden dieses Dienste zu erlangen. Kompetenz und ein hoher Grad an Integrität des Diensteanbieters und seiner Mitarbeiter sind dazu erforderlich. Der Dienstanbieter sollte 24 Stunden pro Tag zugänglich sein. Ein vertrauenswürdiger Dienstanbieter kann eine Menge Dienste für den Bewohner anbieten und ihn vor vielen unliebsamen Überraschungen schützen. Das Verhältnis zwischen Kunden und dem Dienstanbieter wird durch einen Vertrag geregelt, der die Verantwortlichkeits- und Verischerungsfragen umfassen muss, um beide Partner zu schützen. Ein vertrauenswürdiges „Dienst-Konzept“ hat viele Vorteile in Bezug auf Sicherheit. Die Tatsache, dass der Dienstanbieter ein hohes Maß an Kompetenz besitzt, beinhaltet auch dass über neue Bedrohungen informiert wird und jederzeit der letzte und beste Lösungen anbietet.

Das größte Problem des Dienstanbieters ist die Zuverlässigkeit, hauptsächlich der Integrität und Kompetenz der Personen und folglich der Gefahr, Außenstehenden die Kontrolle über das Haus zu geben.

Zusammenfassung

Ein System für ein intelligentes Heim hat Bedürfnisse für mehrere sicherheitsrelevante Schutzmaßnahmen. Dieser Beitrag hat eine Übersicht über verschiedene Aspekte zu berücksichtigen um ein System sicher und vertrauenswürdig zu machen. Wenn es darum geht den Einfluss von Außen zu analysieren, sind die Drohungen, Anforderungen und Lösungen auf Fernbedienung begrenzt.

Drei Klassen von Bedrohungen wurden identifiziert. Die Erste und gefährlichste wäre die Möglichkeit das Fremde von Außen das intelligente Heim beeinflussen. Die zweite Möglichkeit wäre, das fremde Informationen über das Heim finden, entweder durch Lesezugriff in das System oder durch das Abhören von Kommunikationen. Die Dritte ist die Möglichkeit für berechtigte Anwender versehentlich falsche oder unerwünschte Funktionen einzuschalten.

Von den drei genannten Klassen gehören die beiden ersten zu Informationssicherheit. Wir haben hier eine Übersicht über Informationssicherheit gemacht und welche Bedrohungen entstehen können wenn keine Schutzmaßnahmen vorhanden sind. Gegen diese Bedrohungen können Sicherheitsmaßnahmen wie z.B. Zugriffskontrolle und verschlüsselte Kommunikationen installiert werden. Eine Prioritätenliste von Schutzmechanismen für die Fernbedienung eines Systems wurde ausgearbeitet. Die Dritte und letzte Klasse ist von einem anderen Typ. Hier braucht man eine Gute Benutzerschnittstelle (Man-Machine-Interface (MMI)) und eine gut ausgedachte Konfiguration, die die möglichen Steuerungsfunktionen und –werte für Fernbedienung begrenzt, um Einschalten von falschen und unerwünschten Funktionen zu vermeiden.

Zwei vollständig unterschiedliche Sicherheitskonzepte für die Sicherheitslösungen wurde präsentiert. In der Einen kontrolliert der Anwender selbst alles, und in der Anderen verlässt er sich auf einen Dienstanbieter. Beide Konzepte sind für unterschiedliche Bedrohungen gedacht und haben deswegen unterschiedliche Anforderungen. Beide besitzen Vorteile und Nachteile. Es gibt sicherlich ein Markt für beide Lösungen aber es ist zu erwarten, dass die Dienstanbieterlösung für die Masse der intelligente Heimbesitzern besser geeignet ist.