Thomas Eisenbarth, Timo Kasper, Christof Paar

Sicherheit moderner Funktüröffnersysteme

Durch Automatisierung gelangt immer mehr Komfort in unseren Alltag. Ein System, das in den vergangenen Jahren rasante Verbreitung gefunden hat, sind Funktüröffner. Garagentor, Haustür und Auto entriegeln sich auf Knopfdruck aus mehreren Metern Entfernung. Wie sicher aber sind diese Verfahren? Die Autoren entwickelten einen erfolgreichen Seitenkanalangriff auf Funktüröffnersysteme.

Einleitung

Eine typische Krimiszene: Ein Einbrecher will das Zahlenschloss eines Tresors knacken. Er könnte nun zum unbefugten Öffnen des Schlosses unter erheblichem zeitlichen Aufwand alle möglichen Kombinationen des Zahlencodes ausprobieren. Stattdessen verwendet er ein Stethoskop, um die korrekte Stellung der Riegel aus dem von der Schließmechanik erzeugten Schall zu ermitteln. Der Einbrecher benutzt zur Öffnung des Tresors den Schall als *Seitenkanal*, um die geheime Kombination des Zahlencodes zu erhalten. Über diesen vom Hersteller nicht intendierten Kanal gibt der Tresor wertvolle Informationen preis, die einen Angriff erheblich erleichtern.

Analog zum Beispiel des Tresors verhält es sich in der Welt der Elektronik. Hier werden verschiedenste digitale Informationen in Chips durch Kryptografie gesichert. Das Gegenstück zur Zahlenkombination des Tresors ist ein digitaler Schlüssel, eine Folge von Nullen und Einsen, ohne den die Entschlüsselung eines mit einer Verschlüsselungsfunktion erzeugten Geheimtextes im Idealfall praktisch unmöglich ist. Sicherheitsrelevante Funktionen von Autos, Geldkarten, Handys, Reisepässen und vielen weiteren allgegenwärtigen Anwendungen könnten ohne Verschlüsselung nicht sicher realisiert werden.

Zum Schutz der geheimen Informationen werden als mathematisch sicher geltende Chiffren eingesetzt, eingebettet in elektrische Schaltkreise.

- **In diesen Schaltkreisen setzt die Seitenkanalanalyse an: Ein Angreifer kann die elektromagnetische Abstrahlung oder den Stromverbrauch des Computerchips als so genannten Seitenkanal nutzen. Die enthaltenen Informationen werden mit mathematischen Methoden ausgewertet und so schließlich der geheime Schlüssel oder zumindest Teile davon extrahiert.**

Ein Beispiel für die herausragende Bedrohung, die diese so genannten Seitenkanalangriffe für die Systemsicherheit darstellen, ist die im Folgenden vorgestellte Sicherheitsanalyse von auf dem „KeeLoq"-Verschlüsselungsalgorithmus basierenden Funktüröffnersystemen. Die Sicherheit des weit verbreiteten Zugangskontrollsystems, das z. B. für Garagen, Autos und Gebäude eingesetzt wird, kann unter Zuhilfenahme von Seitenkanalangriffen komplett ausgehebelt werden.

1 Funktüröffner, quo vadis?

Ein Funktüröffnersystem besteht typischerweise aus einem Empfänger, der z. B. im Inneren einer Garage mit einem Garagentorantrieb verbunden ist, und einem oder mehreren batteriebetriebenen Handsendern, die über eine Entfernung von bis zu 100 Metern die Fernbedienung des Tors ermöglichen.

Veraltete Systeme, die einen fixen Code senden, ermöglichen eine einfache *Replay-Attacke*, zu deren Durchführung der Angreifer zunächst einen Code einmalig über die Funkschnittstelle abfängt, um ihn anschließend beliebig oft zum unbefugten Öffnen einer Tür zu senden. Um diese Art von Angriffen abzuwehren, wurden so genannte Rolling Code oder *Hopping Code Systeme* entwickelt, bei denen der Handsender einen Zählerstand verschlüsselt an den Empfänger übermittelt. Mit jedem Druck auf den Knopf des Senders erhöht sich dieser Zähler, dessen aktueller Wert bei jedem erfolgreichen Öffnungs- oder Schließvorgang in den Empfänger übernommen wird. Spielt nun ein Dieb einen zuvor abgefangenen Code ab, so wird der dechiffrierte Zählerstand vom Empfänger als veraltet erkannt, wenn zwischenzeitlich ein gültiges Kommando mit einem aktuelleren Wert empfangen wurde.

Dipl.-Ing. Thomas Eisenbarth

Wiss. Mitarbeiter am Lehrstuhl für Embedded Security, Ruhr-Universität Bochum
E-Mail: eisenbarth@crypto.rub.de

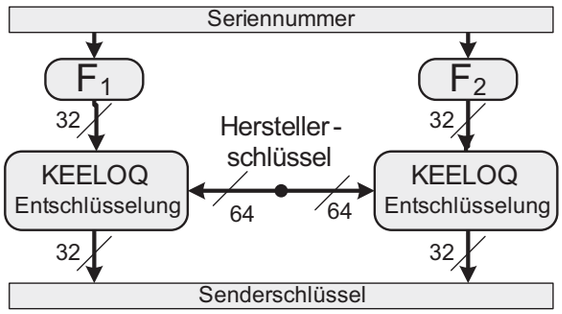
Dipl.-Ing. Timo Kasper

Wiss. Mitarbeiter am Lehrstuhl für Embedded Security, Ruhr-Universität Bochum
E-Mail: tkasper@crypto.rub.de

Prof. Dr.-Ing. Christof Paar

Inhaber des Lehrstuhls für Embedded Security, Ruhr-Universität Bochum
E-Mail: cpaar@crypto.rub.de

Abbildung 1 | Ableitung des Senderschlüssels aus der Seriennummer und dem Herstellerschlüssel



Der in zahlreichen Systemen zum Verschlüsseln des Zählers eingesetzte KeeLoq-Algorithmus soll durch seine mathematischen Eigenschaften sicher stellen, dass weder auf den Wert des Zählers noch auf den nächsten gültigen Code geschlossen werden kann. Nur ein Angreifer, der den geheimen Schlüssel kennt, ist in der Lage, den aktuellen Zählerstand zu extrahieren und gültige Nachrichten, die Hopping Codes, zu senden [HCS01].

2 Schlüsselableitung

Im Normalfall erhält jeder Handsender eines KeeLoq-Türöffnersystems während der Herstellung eine Seriennummer und einen einmaligen, geheimen Schlüssel, den so genannten Senderschlüssel, der wie oben beschrieben zum Erzeugen der Hopping Codes verwendet wird. Die Seriennummer ist Bestandteil jedes Hopping Codes und wird im Klartext über die Funkschnittstelle gesendet.

Damit ein neuer Handsender mit einem Empfänger zusammenarbeitet, muss der Handsender zunächst am Empfänger angelernt werden. Hierzu berechnet der Empfänger aus der Seriennummer des Handsenders den geheimen Senderschlüssel des Handsenders. Während dieser Berechnung kommt ein im Empfänger gespeicherter und gegen unbefugtes Auslesen geschützter Herstellerschlüssel ins Spiel: Der Empfänger entschlüsselt die Seriennummer des Handsenders unter Verwendung des Herstellerschlüssels. Der so erhaltene Geheimtext entspricht dem Senderschlüssel des angelernten Handsenders und wird empfängerseitig zum zukünftigen Entschlüsseln der Hopping Codes gespeichert. Denn nur wenn beide Seiten den Senderschlüssel kennen, können sie später vertraulich kommunizieren.

Bei symmetrischen Verschlüsselungsverfahren ist ein eindeutiger Herstellerschlüssel für das Anlernen von zusätzlichen elektronischen Schlüsseln notwendig. Ihn geheim zu halten ist von höchster Relevanz für die Sicherheit des gesamten Systems, da seine Kenntnis einem Angreifer ermöglicht, aus der unverschlüsselt übertragenen Seriennummer den Senderschlüssel zu berechnen. Mit weitreichenden Konsequenzen:

- **Wer im Besitz des Herstellerschlüssels ist, kann beliebig viele neue Handsender mit gültigen Senderschlüsseln erzeugen, die nicht von originalen zu unterscheiden sind. Des Weiteren kann durch Abfangen von mindestens einer Nachricht eines Handsenders eine Kopie des Handsenders erzeugt werden, ohne physikalischen Zugriff auf einen Handsender oder den Empfänger des Opfers. Dieser „Lauschangriff" ermöglicht ein unbefugtes Umgehen des Türöffnungsmechanismus, ohne dass Spuren hinterlassen werden – ein bedeutsamer Umstand im Falle ungeklärter Versicherungsfälle.**

Für die oben beschriebene Schlüsselableitung aus der Seriennummer findet im Fall von KeeLoq ein handelsüblicher PC den geheimen Senderschlüssel des Handsenders aus der abgehörten Nachricht im Bruchteil einer Sekunde und ermöglicht damit umgehend ein Klonen des originalen Handsenders. In der Praxis reicht zum Abspielen der Hopping Codes schon ein Laptop, das über den Parallelport einen Sender ansteuern und so jeden beliebigen Handsender imitieren kann.

Aus Sicht eines Herstellers von Türöffnersystemen ist auch das Erzeugen von kompatiblen Handsendern mit unangenehmen Folgen verbunden, da mit den im Zubehörhandel vertriebenen Ersatz-Handsendern ein nicht unwesentlicher Anteil des Gewinns erzielt wird. Ein Monopol auf die Handsenderproduktion hat er aber nur, so lange der Herstellerschlüssel geheim bleibt.

3 Seitenkanalanalyse

Konnte der geheime Schlüssel bisher, wenn überhaupt, nur mit großem finanziellen Aufwand z. B. durch „Social Engineering" beschafft werden, demonstrieren wir, wie sich die Sicherheit von eingebetteten Systemen mit dem mächtigen Werkzeug der Seitenkanalattacke völlig ändert.

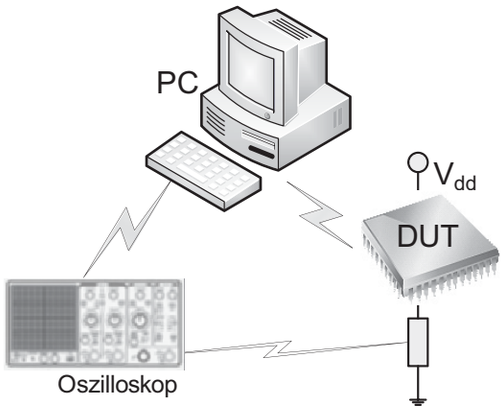
Wie in der Einleitung beschrieben wird dazu die Stromaufnahme des Halbleiters durch einen mit dem Messobjekt in Reihe geschalteten Widerstand gemessen und die erhaltenen Stromkurven mit einem Digitaloszilloskop aufgezeichnet. Alternativ werden Messungen des elektromagnetischen Feldes mit einer direkt über dem Schaltkreis positionierten Nahfeldsonde durchgeführt, mit dem Vorteil, die Schaltung zur Messung der Seitenkanalinformationen nicht modifizieren zu müssen. Nach der Identifikation des relevanten Zeitbereichs werden die Messdaten zur weiteren Auswertung durch eine so genannte Stromprofilanalyse (häufig DPA – *Differential Power Analysis* genannt [KJJ99]) an einen PC übergeben. Dort werden die Daten mit digitalen Filtern nachbearbeitet und die Datenmenge reduziert. Mit speziellen Algorithmen gelingt es dann, die im Energieverbrauch der Implementierung enthaltenen Informationen über den geheimen Schlüssel zu extrahieren und so den Schlüssel zu rekonstruieren [EKM08].

3.1 Klonen eines Handsenders

In einem Handsender wird der KeeLoq-Algorithmus typischerweise in einem ASIC (Anwender-Spezifische Integrierte Schaltung) vollständig in Hardware durchgeführt. Das Ergebnis der Seitenkanalanalyse ist erstaunlich: Sowohl aus den Messungen mittels eingelötetem Widerstand als auch aus den nicht-invasiven Messungen mit der Nahfeldsonde kann der 64-Bit Schlüssel des KeeLoq-Algorithmus mit nur fünf bis 30 Strommessungen ermittelt werden. Die Auswertung mit einem Standard PC dauert nur Minuten.

Für diesen Angriff ist ein physikalischer Zugriff auf den Handsender erforderlich,

Abbildung 2 | Typischer Seitenkanalmessplatz: Der PC steuert das Oszil-loskop und den Testchip (DUT). Das Oszilloskop misst die Leistungsaufnahme des Testchips über der Zeit. Die gesammelten Daten werden dann am PC ausgewertet.



wenigstens lange genug, um die Stromkurven aufnehmen zu können. Dies ist beispielsweise in einem „Leihwagenszenario" denkbar: Der Angreifer könnte während der Mietdauer den geheimen Senderschlüssel im Handsender ermitteln, eine Kopie des Schlüssels anfertigen und sich zu einem späteren Zeitpunkt Zugang zum Fahrzeug verschaffen. Der zu betreibende Aufwand ist relativ hoch, da für jedes Objekt eine eigene Seitenkanalanalyse durchgeführt werden muss, so dass sich der Angriff nur für sehr hochwertige Produkte lohnt.

3.2 Rückgewinnung des Herstellerschlüssels

Verheerendere Folgen hat die Rückgewinnung des Herstellerschlüssels, der in jedem Empfänger gespeichert ist und, wie oben beschrieben, nur während der Schlüsselableitung zum Einsatz kommt. Bei den Empfängern wird der KeeLoq-Algorithmus üblicherweise in Software auf einem Mikrocontroller ausgeführt. Dementsprechend wird der Empfänger wiederholt in den Lern-Modus versetzt, und es werden ihm immer neue virtuelle Handsender vorgegaukelt, die er anzulernen versucht.

- **Mit ca. 1.000 Messungen gelingt es auch hier, den Herstellerschlüssel aus dem Stromprofil des Mikrocontrollers zu extrahieren. Die große Gefahr dieses Angriffs besteht darin, dass seine einmalige erfolgreiche Ausführung die Sicherheit aller Geräte des Herstellers gefährdet.**

Zur Durchführung der Schlüsselextraktion beschafft sich der Angreifer z. B. im Baumarkt einen Empfänger des anzugreifenden Herstellers und führt eine Seitenkanalattacke durch.

4 Konsequenzen

Natürlich genügt der Herstellerschlüssel allein noch nicht, um sich Zugang zu beliebigen Objekten zu verschaffen, die mit Systemen des jeweiligen Herstellers gesichert sind. Hierzu wird immer noch die im Empfänger registrierte Seriennummer eines angelernten Handsenders benötigt. Im Folgenden werden zwei signifikante Angriffe zur Umgehung des KeeLoq-Schließsystems und ihre Auswirkungen erläutert. Zu ihrer Ausführung bedarf es keiner speziellen Fachkenntnisse, da die einmalig notwendige Extraktion des Herstellerschlüssels an kriminelle Kryptografen ausgelagert werden kann.

Im für einen Angreifer besten Fall findet er den Herstellerschlüssel in einem Forum im Internet – ein mittelfristig durchaus denkbares Szenario – und benötigt damit zur Durchführung der im Folgenden beschriebenen Angriffe oder zur Erstellung von zum System kompatiblen Handsendern höchstens die Kenntnisse eines „Elektrobastlers".

4.1 Der Lauschangriff

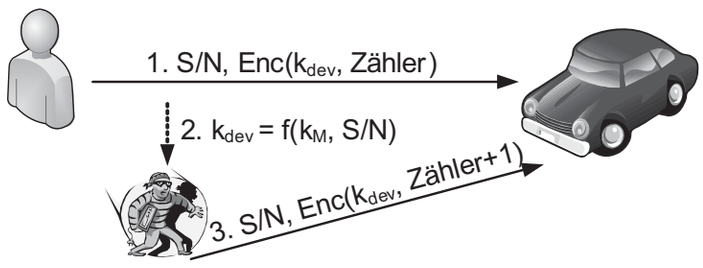
Begibt sich der Angreifer nun in die Nähe des durch einen Funktüröffner geschützten Objekts, um eine vom Handsender des Opfers gesendete Nachricht abzufangen, erhält er – wie in Abbildung 3 visualisiert – die im Klartext versandte registrierte Seriennummer (S/N). Mittels des Herstellerschlüssels (k_M) führt er die Schlüsselableitung aus und erhält den Senderschlüssel (k_{dev}). Die empfangene Nachricht kann nun entschlüsselt und aus ihr der aktuelle Zählerstand im originalen Handsender ermittelt werden. Der Angreifer besitzt nun alle Informationen, um unverzüglich eine gültige Nachricht zu erzeugen und senden zu können – der Empfänger öffnet den Schließmechanismus.

4.2 Verweigerung der ordnungsgemäßen Funktion

Ist ein Angreifer einmal im Besitz des Herstellerschlüssels, lässt sich außer dem Klonen von Handsendern ein weiterer folgenschwerer Angriff inszenieren, und zwar eine klassische Denial-Of-Service Attacke: Zur Verhinderung von „Replay"-Attacken muss der übertragene Zählerwert bei jeder Nachricht erhöht werden. Wird eine alte Nachricht erneut gesendet, erkennt der Empfänger, dass der Zählerstand des Senders zu niedrig ist, und entriegelt das geschützte System nicht.

Handsender können den Zähler üblicherweise bei jedem Knopfdruck nur um eins erhöhen. Ein Angreifer kann jedoch mit dem PC beliebige gültige Nachrichten

Abbildung 3 | Der Lauschangriff. Ein unbefugter Dritter fängt die Nachricht des Funktüröffners ab. Kennt er den Herstellerschüssel (kM), so kann er wie in Abschnitt 2 beschrieben den Senderschlüssel (kdev) berechnen und sich Zugang zum gesicherten Objekt verschaffen.



generieren, wenn er den Senderschlüssel (zum Beispiel wie in Abschnitt 3.2 beschrieben) kennt. Erhöht er den Zähler jetzt um eine große Zahl, so muss der rechtmäßige Besitzer seinen Handsender unter Umständen einige tausend Mal betätigen, bevor sich die Tür erneut öffnen wird – besonders im Kontext von Kraftfahrzeugen ein Grund, von einem Defekt auszugehen und beim Hersteller eine Beschwerde einzulegen.

5 Kryptoanalyse der Chiffre

Die KeeLoq-Chiffre, die auch in Form von passiven RFID-Transpondern (Radio Frequenz Identifikation), z. B. für Wegfahrsperren in Kraftfahrzeugen eingesetzt wird, wurde in den 80er Jahren entwickelt und nie von den Entwicklern offengelegt. Nach der Patentierung des KeeLoq-RKE-Verfahrens Mitte der 90er Jahre verbreiteten sich Geräte weit, die auf dem vom Hersteller als hochsicher beworbenen Algorithmus [SEL98] basieren. In den USA und in Europa findet er besonders häufig in Wechselcode-Systemen zum Öffnen von Garagen Verwendung. Nachdem die Chiffre 2006 im Internet (Wikipedia) auftauchte, dauerte es nur ca. ein Jahr, bis Mathematiker sich erfolgreich mit der Kryptoanalyse der Chiffre beschäftigten. Die erste erfolgreiche Attacke von Bogdanov im Februar 2007 [BOG07] wurde im Sommer 2007 von Indesteege et al. derart erweitert, dass schon ca. 65.000 Klar- und Geheimtextpaare nach ca. einer Woche Rechenarbeit von 50 Pentiums den geheimen Schlüssel offenbaren [IKD08].

Bei Funktüröffnern handelt es sich prinzipiell um Einweg-Systeme, d. h. es werden nur Chiffretexte verschickt (s. o.), während der dazugehörige Klartext für den Angreifer unsichtbar im Handsender verbleibt. Daher ist die Durchführung dieser mathematischen Attacken praktisch unmöglich – im Gegensatz zu der hier vorgestellten Seitenkanalanalyse, die ein Auffinden des Schlüssels schon nach ca. zehn Betätigungen des Handsenders (und gleichzeitiger Messung des Stromverbrauchs) nach einer Rechenzeit von weniger als einer Stunde mit einem Standard PC ermöglichen.

Fazit

Erneut zeigt sich, dass das Prinzip *Security by Obscurity*, also das Erzeugen von „Sicherheit“ durch Geheimhaltung der verwendeten Verfahren, langfristig versagt. Obwohl längst sichere, patentfreie Chiffren und verschiedenste Arten von Gegenmaßnahmen – auch solche gegen Seitenkanalattacken – existieren, setzen Hersteller von kommerziellen Systemen weiterhin oft überholte oder schlicht unsichere proprietäre Kryptografie ein.

- **Unsere Angriffe zeigen, dass Seitenkanalattacken eine reale Bedrohung für ungeschützte Implementierungen darstellen. Entwickler neuer Systeme sollten diese Gefahr entsprechend berücksichtigen und geeignete Gegenmaßnahmen implementieren.**

Im Fall von KeeLoq hätte neben dem Einsatz einer sicheren Chiffre (z.B. AES) schon eine verbesserte Schlüsselverwaltung einen Großteil der Verwundbarkeit des Verfahrens verhindert.

Besonders in der RFID-Welt und bei vergleichbaren Funksystemen werden Sicherheit und Gegenmaßnahmen aus Kostengründen oft vernachlässigt oder ganz weggelassen. Infolgedessen sind zukünftig weitere neue, erfolgreiche Angriffe auf ähnliche Systeme zu erwarten.

Literatur

[BOG07] A. Bogdanov. Attacks on the KeeLoq Block Cipher and Authentication Systems. 3rd Conference on RFID Security 2007.

[EKM08] T. Eisenbarth, T. Kasper., A. Moradi, C. Paar, M. Salmasizadeh, M. Shalmani. *On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme.* Erscheint in Proceedings of CRYPTO 2008.

[HGI] Horst Görtz Institut für IT-Sicherheit http://www.hgi.rub.de

[IKD08] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel. *A Practical Attack on KeeLoq*. Advances in Cryptology – EUROCRYPT 2008.

[KJJ99] P. C. Kocher, J. Jaffe, and B. Jun. *Differential Power Analysis*. Proceedings of CRYPTO '99.

[EMSEC] Lehrstuhl Embedded Security: http://www.crypto.ruhr-uni-bochum.de

[HCS01] Microchip. *HCS410, KeeLoq Code Hopping Encoder and Transponder.* http://ww1.microchip.com/downloads/en/DeviceDoc/40158e.pdf

[SEL98] E. Sells. *Lexus RX 300 Uses Keeloq Code-Hopping Technology for Highly Secure RKE System.* http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=2018&mcparam=en013328