SEMINAR

Sicherheit von Funk- und RFID-Systemen

Titel des Seminars:

Sicherheit von Funk- und RFID-Systemen

Untertitel des Seminars:

Technische Grundlagen, Bedrohungen und Gegenmaßnahmen

Seminarbeschreibung:

Die Verwendung von RFID-Systemen oder Funktechnologie im Allgemeinen ist heute aus dem Alltag und Logistik-Anwendungen im speziellen nicht mehr wegzudenken. Mit der Verwendung von kontaktlosen Schnittstellen sowie eingebetteten Chips und Prozessoren entstehen neue Sicherheitsrisiken, über deren Ausmaß oft Unklarheit besteht. In diesem Seminar werden dazu zunächst einige Grundlagen der IT-Sicherheit und von RFID sowie verwandten Systemen aufgearbeitet. Anhand von Fallstudien werden anschließend in der Realität aufgetretene Schwachstellen demonstriert, eingeordnet und diskutiert. In einem (optionalen) Teil des Seminars wird den Teilnehmern der Umgang mit Tools für Sicherheitsanalysen (RFID-Emulator ChameleonMini, Software Defined Radio) nahegebracht. Abschließend werden Maßnahmen zur besseren Absicherung der betrachteten Systeme erarbeitet.

Dauer des Seminars:

Individuell auslegbar

Institute for Supply Chain Security GmbH Hauert 20, 44227 Dortmund
Mail: seminare@supply-chain-security.org Web: www.supply-chain-security.org
Telefon: +49 (0) 231 / 33 00 99 79

Seminarinhalte:

0. Motivation: Zielstellung des Seminars und Ausgangssituation

1. Grundlagen von RFID und Funksystemen
    a. Begriff RFID
    b. Passive Transponder (insbesondere ISO14443 und ISO15693 bei 13,56 MHz)
    c. Aktive Transponder (z.B. Logistik)
    d. Vergleichbare Funksysteme (z.B. Autoschlüssel, Türöffner, …)

2. Grundlagen der IT-Sicherheit
    a. Verschlüsselung
    b. Authentifizierung
    c. Gängige Algorithmen und aktuelle Empfehlungen
    d. Protokolle für Funksystemen (Fix code, Rolling code, Challenge-response)
    e. Klassische Angriffe
    f. Neuartige Angriffsmethoden: Seitenkanal-Analyse, Implementierungsangriffe
    g. Abschätzung zukünftiger Entwicklungen

3. Fallstudie 1: Aktive RFID-Tags in der Logistik
    a. Standards und Technologien
    b. Erforderliche Ausrüstung (Software Defined Radio)
    c. Erkennung und Abhören
    d. Denial-of-service, Senden gefälschter Daten
    e. Bewertung / Diskussion

4. Fallstudie 2: Kontaktlose Türöffner und KeeLoq
    a. Anwendungsbereiche
    b. Vertiefung: Systeme mit Rolling code
    c. Praktische Anwendung von Seitenkanal-Analyse
    d. Betrachtung der Auswirkungen auf das Gesamtsystem (Schlüsselverteilung)
    e. Bewertung / Diskussion

5. Fallstudie 3: (Un-)Sicherheit alltäglicher RFID-Anwendungen
    a. Zusammenfassung: Angriffe der letzten Jahre (Mifare Classic, Legic Prime, …)
    b. Tools: RFID-Emulator ChameleonMini, selbstentwickelter RFID-Reader
    c. Vorstellung verschiedener (einfach angreifbarer) Systeme: Bezahlkarten, Verleih-Karten, Türschlösser, …
    d. Bewertung / Diskussion

6. Fallstudie 4: Mifare DESFire MF3ICD40 – Angriffe auf „sichere“ Verschlüsselung
    a. Funktionen von Mifare DESFire
    b. Vertiefung: Seitenkanal-Analyse (im Kontext von RFID)
    c. Durchführung und Aufwand der Angriffe
    d. Praktische Auswirkungen: Analyse einer echten Anwendung
    e. Bewertung / Diskussion

7. *Optional*: Praktischer Teil (am PC)
    a. Einführung
    b. Übungen zu
        i. Nutzung von RFID-Reader an PC / auf Smartphone
        ii. ChameleonMini: Emulation von RFID-Tags (13,56 MHz)
        iii. Software Defined Radio: Tools zum Abfangen/Interpretieren von Funksignalen (z.B. 433 MHz, 868 MHz, …)
    c. Diskussion

8. Gegenmaßnahmen und Zusammenfassung
    a. Rückblick
    b. Abschätzung zukünftiger Entwicklungen
    c. Mögliche Gegen- und Schutzmaßnahmen
        i. Kryptographie
        ii. Geschützte Hardware
        iii. Systemebene
    d. Abschließende Frage- und Diskussionsrunde

Teilnehmer / Zielgruppen:

Entwickler, Projektleiter, Sicherheitsverantwortliche

Teilnahmebedingungen / -voraussetzungen:

Grundlegende Kenntnisse im Bereich von IT-Systemen.

Teilnehmernutzen:

Die Teilnehmer gewinnen einen Überblick über die Entwicklung und aktuelle Lage der IT-Sicherheit in RFID- und Funkanwendungen, insbesondere aus Sicht eines potentiellen Angreifers. Damit unterstützt das Seminar bei der Einschätzung von potentiellen Sicherheitsproblemen und der Ergreifung geeigneter Gegenmaßnahmen. Im optionalen, praktischen Teil wird der Umgang mit modernen Analysewerkzeugen geübt.

Lehrmethoden / Didaktik:

Vortrag, unterbrochen durch Diskussions- und Fragerunden

Ggf. praktische Arbeit mit Tools (ChameleonMini, Software Defined Radio) am PC

Seminarsprachen:

Deutsch, Englisch

Teilnehmerzahl:

Minimal: 5 Maximal: 40

Seminarorte:

Offene Seminare

Inhouse-Seminare

Angaben zu den Referenten:

Dr.-Ing. Timo Kasper

Timo Kasper ist ein Experte für Sicherheitsanalysen eingebetteter kryptografischer Systeme, insbesondere RFID- und Funkanwendungen. Er studierte Elektro- und Informationstechnik an der Ruhr-Universität Bochum und an der University of Sheffield (Großbritannien). Seit Oktober 2006 ist Timo Kasper wissenschaftlicher Mitarbeiter am Lehrstuhl für Embedded Security. Seine Forschung umfasst Implementierungs- und Protokoll-Angriffe, Sicherheitsbetrachtungen auf Systemebene und die Entwicklung entsprechender Gegenmaßnahmen. Seine Dissertation wurde mit dem 1. Platz des Promotionspreises für IT-Sicherheit 2012 prämiert. Herr Kasper hat mehrjährige Erfahrung als Vortragender auf internationalen wissenschaftlichen Konferenzen, bei industriellen Veranstaltungen und in der universitären Lehre.

Dr.-Ing. David Oswald

David Oswald studierte Sicherheit in der Informationstechnik an der Ruhr-Universität Bochum und ist seit 2009 wissenschaftlicher Mitarbeiter am Lehrstuhl für Embedded Security. Sein Forschungsgebiet ist die Sicherheitsanalyse von praktisch eingesetzten, kommerziell verfügbaren Systemen, z.B. von kontaktlosen (RFID) und kontaktbehafteten Smartcards.

Timo Kasper

David Oswald