Zertifikatsprogramm - Z308

Sicherheit mobiler Systeme

- Einführung
- Sicherheitsaspekte von Mobilfunknetzen
- Sicherheitsaspekte von Satellitentelefonen
- Sicherheitsaspekte von DECT
- Design mobiler Betriebssysteme

Prof. Dr. Thorsten Holz

Open C³S
Open Competence Center for Cyber Security

RUHR UNIVERSITÄT BOCHUM
RUB

Modul XXX

Sicherheit Mobiler Systeme [MobSec]

Studienbrief 1: Einführung

Studienbrief 2: Sicherheitsaspekte von Mobilfunknetzen

Studienbrief 3: Sicherheitsaspekte von Satellitentelefonen

Studienbrief 4: Sicherheitsaspekte von DECT

Studienbrief 5: Design mobiler Betriebssysteme

Studienbrief 6: Verzeichnisse

Autor:

Prof. Dr. Thorsten Holz

---

1. Auflage

Ruhr-Universität Bochum

© 2015 Ruhr-Universität Bochum
Bochum
Universitätsstr. 150
44801 Bochum

1. Auflage (11. Dezember 2015)

Didaktische und redaktionelle Bearbeitung:

Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der Verfasser unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung, und Forschung unter dem Förderkennzeichen 16OH12026 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen **5**
I. Abkürzungen der Randsymbole und Farbkodierungen 5
II. Zu den Autoren 6
III. Modullehrziele 7

Studienbrief 1 Einführung **9**

Studienbrief 2 Sicherheitsaspekte von Mobilfunknetzen **11**
2.1 Lernziele 11
2.2 Advanced Organizer 11
2.3 Einleitung 11
2.4 GSM 11
2.4.1 Systemdesign 12
2.4.2 Datenübertragung 14
2.4.3 Sicherheit 21
2.4.4 Angriffe 24
2.4.5 Kontrollaufgaben 28
2.5 UMTS 29
2.5.1 Systemdesign 29
2.5.2 Sicherheit 30
2.5.3 Kontrollaufgaben 37
2.6 Übungen 38

Studienbrief 3 Sicherheitsaspekte von Satellitentelefonen **39**
3.1 Lernziele 39
3.2 Advanced Organizer 39
3.3 Einleitung 39
3.4 Grundlagen 39
3.4.1 Netzwerkstruktur 40
3.4.2 Kanäle 41
3.4.3 Kodierung und Verschlüsselung 42
3.4.4 Architektur eines Satellitentelefons 44
3.4.5 Analyse existierender Protokolle 45
3.4.6 Kontrollaufgaben 45
3.5 GMR-1 Protokoll 46
3.5.1 Hardwarearchitektur 46
3.5.2 Struktur 46
3.5.3 Funktionsweise 47
3.5.4 Operationsmodi 48
3.5.5 Angriffe 50
3.5.6 Kontrollaufgaben 51
3.6 GMR-2 Protokoll 51
3.6.1 Hardwarearchitektur 51
3.6.2 Struktur 51
3.6.3 Funktionsweise 56
3.6.4 Operationsmodi 56
3.6.5 Exkurs: Angriff 57
3.6.6 Kontrollaufgaben 60
3.7 Übungen 60

Studienbrief 4 Sicherheitsaspekte von DECT **61**
4.1 Lernziele 61
4.2 Advanced Organizer 61

4.3 Einleitung 61
4.4 Grundlagen 61
4.5 Systemdesign 62
4.5.1 DECT-Referenzmodell 62
4.5.2 Kontrollaufgaben 66
4.6 Verbindungsverwaltung 67
4.6.1 Betriebszustände 67
4.6.2 Verbindung zwischen PP und FP 68
4.6.3 Handover 71
4.6.4 Kontrollaufgaben 71
4.7 Sicherheit in DECT 71
4.7.1 Architektur 72
4.7.2 Authentisierung 72
4.7.3 Verschlüsselung 74
4.7.4 Angriffe auf DECT 74
4.7.5 Kontrollaufgaben 79
4.8 Übungen 79

Studienbrief 5 Design mobiler Betriebssysteme 81
5.1 Systemdesign 81
5.2 Besonderheiten mobiler Systeme 81
5.3 Fallstudie: iOS 81
5.4 Fallstudie: Android 81
5.5 Fallstudie: Analyse von Android Apps 81

Studienbrief 6 Verzeichnisse 83

Liste der Lösungen zu den Kontrollaufgaben 85

Liste der Lösungen zu den Übungen 89
6.1 Literatur 93

Glossar 95

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

II. Zu den Autoren

Bild fehlt

Prof. Dr. Thorsten Holz leitet den Lehrstuhl für Systemsicherheit an der Ruhr-Universität Bochum seit dem Jahr 2012?. Bla bla bla...

III. Modullehrziele

TODO: lehrziele

Studienbrief 1 Einführung

Studienbrief 2 Sicherheitsaspekte von Mobilfunknetzen

2.1 Lernziele

Sie können Grundlagen der Mobilfunkkommunikation mittels der Protokolle GSM und UMTS aufzeigen und Unterschiede zwischen den beiden Protokollen benennen. Weiterhin können Sie die Sicherheitsarchitekturen der jeweiligen Protokollfamilien erläutern. Abschließend können Sie Schwachstellen und Angriffe auf die Sicherheitsfunktionen aufzeigen und skizzieren.

2.2 Advanced Organizer

Wie sind GSM und UMTS aufgebaut, welche Sicherheitsmerkmale verwenden diese Protokolle und welche Angriffe sind auf die Protokollfamilien möglich? In diesem Studienbrief werden der Aufbau und die Sicherheitsarchitekturen von weit verbreiteten Mobilfunknetzwerken aufgezeigt und Schwachstellen erläutert.

2.3 Einleitung

In diesem Studienbrief werden die Grundlagen der Kommunikation von Mobilfunknetzen anhand der weit verbreiteten Protokolle GSM und UMTS erläutert. Dies umfasst insbesondere den Aufbau und die Funktionsweise der zugehörigen kryptographischen Verschlüsselungsfunktionen. Abschließend werden verschiedene Angriffe auf diese Verschlüsselungsfunktionen vorgestellt.

2.4 GSM

GSM steht für *Global System for Mobile Telecommunications* und ist ein international etablierter Standard zur Übertragung von Daten mittels Funktechnik für die kabellose zellulare Telefonie. GSM ist der erste Standard der sogenannten zweiten Mobilfunkgeneration (2G) und gilt als Nachfolger der analogen Mobilfunknetze. Die Entwicklung von GSM begann im Jahr 1983 durch das *European Telecommunications Standards Institute* (ETSI). Im Jahr 1991 wurde der Testbetrieb von mehreren GSM-Netzen in 5 Ländern aufgenommen [Lüd01]. Ab Sommer 1992 begann im Anschluss an die Testphase der kommerzielle Betrieb von 13 Mobilfunknetzen in 7 Ländern.

> Exkurs 2.1: Namensgebung GSM
>
> Die Abkürzung GSM stand ursprünglich für *Groupe Spéciale Mobile*, einer Arbeitsgruppe des *European Telecommunications Standards Institutes*. Erst mit der weltweiten Verbreitung wurde GSM als *Global System for Mobile Telecommunications* bekannt.

E

Das Design des GSM-Standards legt besonderen Fokus darauf, eine Vielzahl unterschiedlicher Telekommunikationsdienste zu unterstützen, sodass sowohl Sprach- (beispielsweise Anruf und Notruf) als auch Datenübertragungen ermöglicht werden. Weiterhin sollten mit Einführung des GSM-Standards unter anderem folgende Ziele erreicht werden [Fed99, Wal01a]:

- Hohe Mobilität (auch international)
- Hohe Erreichbarkeit unter einer international einheitlichen Rufnummer
- Hohe Teilnehmerkapazität

Studienbrief 3 Sicherheitsaspekte von Satellitentelefonen

3.1 Lernziele

Sie kennen die Grundlagen der Kommunikation über Satellitentelefone und können Unterschiede zwischen Protokollen von Satellitentelefonen und anderen Mobilfunkstandards wie GSM / UMTS benennen. Weiterhin können Sie die generellen Funktionsweisen von zwei Satellitentelefon-Protokollfamilien erläutern. Abschließend können Sie Angriffe auf die zwei Protokolle aufzeigen und skizzieren.

3.2 Advanced Organizer

Wie ist ein Satellitentelefonnetzwerk aufgebaut und welche Angriffe sind auf die verschiedenen Protokollfamilien möglich? In diesem Studienbrief werden der Aufbau und zwei der verwendeten Protokolle von Satellitentelefonnetzwerken aufgezeigt und Schwachstellen erläutert.

3.3 Einleitung

In diesem Studienbrief werden die Grundlagen der Kommunikation von Satellitentelefonen und ihre Einsatzgebiete erläutert. Weiterführend wird der Aufbau und die Funktionsweise von zwei verwendeten Protokollfamilien aufgezeigt. Dies umfasst insbesondere den Aufbau und die Funktionsweise der zugehörigen proprietären kryptographischen Verschlüsselungsfunktionen. Abschließend werden verschiedene Angriffe auf diese Verschlüsselungsfunktionen vorgestellt.

3.4 Grundlagen

Mobile Kommunikationssysteme haben die Art und Weise der heutigen Kommunikation revolutioniert. Statt für die Telefon- und Datenkommunikation wie vor einigen Jahren üblich statische Festnetzanschlüsse nutzen zu müssen, können heutzutage Daten mittels mobilen zellulären Systemen wie dem *Global System for Mobile Communications* (GSM) von beinahe jedem beliebigen Ort übertragen werden. Diese zellulären Systemen erfordern Funkzellen in denen Verbindungen innerhalb des mobilen Netzwerkes aufgebaut werden. Funkzellen werden durch den von der Sendeeinrichtung abgedeckten Bereich definiert, in der die Mobilfunksignale empfangen und fehlerfrei verarbeitet werden können. Eine Sendeeinrichtung besteht ihrerseits dafür aus Sendern / Empfängern, Antennen und digitalen Signalprozessoren zur Verarbeitung der Daten. Ein großer Nachteil dieser Sendeeinrichtungen besteht allerdings darin, dass die Reichweite limitiert ist und somit in abgelegeneren Orten ohne hinreichende Signalabdeckung keine Telefonie möglich ist. Dies trifft beispielsweise auf Ölplattformen oder Schiffe zu. Als Lösung wurden Satellitensysteme eingeführt, welche die Problematik der Signalabdeckung umgehen, indem die Sprach- und Nutzdaten direkt mit geostationären Telekommunikationssatelliten ausgetauscht werden.

Für die Satellitenkommunikation werden heutzutage hauptsächlich die folgenden zwei Protokollfamilien verwendet, die beide vom *European Telecommunications Standards Institute* (ETSI) entwickelt und standardisiert wurden.

- Das *Geostationary Earth Orbit (GEO) Mobile Radio Interface* (besser bekannt als GMR-1) ist ein ETSI-Standard, der vom terrestrischen zellulären GSM-Standard abgeleitet wurde. Die Spezifikationen von GMR bilden eine Erweiterung zum GSM-Standard, wobei einige Eigenschaften der Spezifikationen speziell für die Satellitenkommunikation abgeändert wurden. Die GMR-1-Familie wird von verschiedenen Anbietern wie Thuraya, SkyTerra und

Studienbrief 4 Sicherheitsaspekte von DECT

4.1 Lernziele

Sie kennen den Aufbau des DECT-Standards und können sowohl Vor- als auch Nachteile von DECT benennen. Weiterhin können Sie Unterschiede zwischen DECT und anderen Mobilfunkstandards wie GSM / UMTS erläutern. Abschließend können Sie die Sicherheitsarchitektur von den DECT-Standard skizzieren.

4.2 Advanced Organizer

Wie wird der DECT-Standard im Mobilfunk eingesetzt und welche Sicherheitsmerkmale werden angewandt? In diesem Studienbrief werden der Aufbau und die verwendeten kryptographischen Protokolle des DECT-Standards aufgezeigt und Schwachstellen erläutert.

4.3 Einleitung

In diesem Studienbrief wird der DECT-Standard vorgestellt, welcher im Mobilfunkbereich für die Sprach- als auch Datenübertragung eingesetzt wird. Dazu werden in einer Einführung die Grundlagen und Ziele von DECT benannt. Weiterführend wird der Aufbau und die Funktionsweise von DECT erläutert. Dies umfasst insbesondere den Aufbau einer Datenübertragung und die Anwendung von Sicherheitsmaßnahmen. Abschließend werden die verschiedene Sicherheitsmerkmale von DECT-Standard vorgestellt.

4.4 Grundlagen

DECT steht für *Digital Enhanced Cordless Telecommunications* und ist ein international etablierter Standard zur Übertragung von Daten mittels Funktechnik, primär für die kabellose picozellulare Telefonie. DECT wurde vom *European Telecommunications Standards Institute* (ETSI) entwickelt und löste im Jahr 1992 den analogen Standard CT1 (Cordless Telephone generation 1) sowie den digitalen Standard CT2 (Cordless Telephone generation 2) ab.

> Exkurs 4.1: Namensgebung DECT
>
> Die Abkürzung DECT stand ursprünglich für *Digital European Cordless Telephone* und wurde vom *European Telecommunications Standards Institute* als einheitlicher Standard für kabellose Telefonsysteme eingeführt. DECT erlangte über die Zeit allerdings auch außerhalb Europas immer höhere Verbreitung. Weiterhin wurden neben der Telefonie weitere Anwendungsgebiete erschlossen, sodass der Standard in *Digital Enhanced Cordless Telecommunications* umbenannt wurde.

E

Das Design des DECT-Standards legt besonderen Fokus darauf, eine Vielzahl unterschiedlicher Telekommunikationsdienste und Anwendungen zu unterstützen. Speziell für die Zusammenarbeit mit bereits bestehenden Netzen wie dem analogen Telefonnetz oder ISDN wurden Zugriffsprotokolle und Anwendungsprofile definiert. Die Minimalanforderungen für diese Anwendungsprofile wurden im *Generic Access Profil* (GAP) zusammengefasst, welches ab dem Jahr 1997 von allen Anbietern von DECT-Infrastruktur wie Basisstationen und mobilen Endgeräten unterstützt werden muss. Die Einführung von GAP ermöglicht beispielsweise die Kombination von Basisstationen und mobilen Geräten verschiedener Hersteller.

obwohl einige Eigenschaften DSC deutlich stärker machen würden als den A5/1 Algorithmus (vgl. Tabelle 4.1).

Die Sicherheit von DSC könnte deutlich verbessert werden, indem beispielsweise die Anzahl der Initialisierungsrunden vergrößert werden und weiterhin eine Neu-Initialisierung des Schlüssels von Zeit zu Zeit stattfinden würde. Ähnlich zum DSAA wäre allerdings eine bessere Strategie, ein von Experten begutachtetes kryptographisches Protokoll für die Verschlüsselung in der nächsten Version vom DECT-Standard zu nutzen.

4.7.5 Kontrollaufgaben

In diesem Abschnitt befinden sich verschiedene Kontrollaufgabe, die die Inhalt der vorherigen Abschnitte auffassen und daher zur Vertiefung des Stoffs beitragen sollen.

K

Kontrollaufgabe 4.5: Kryptographische Algorithmen

Benennen Sie die kryptographischen Algorithmen in DECT, deren Funktionen und ob deren Einsatz DECT kryptographisch sicher macht.

K

Kontrollaufgabe 4.6: DSC Algorithmus

Wozu dient der LFSR R_4 im DSC Algorithmus?

4.8 Übungen

Ü

Übung 4.1: DECT vs. CT1/CT2

Finden Sie heraus, aus welchen Gründen CT1 bzw. CT2 Ende 2008 verboten wurden?

Ü

Übung 4.2: Unterschiede zwischen DECT und GSM

Erläutern Sie einige Unterschiede zwischen DECT und GSM.

Ü

Übung 4.3: Verschlüsselungsverfahren

Warum ist es nicht sinnvoll, wenn Verschlüsselungsverfahren wie bei DECT auf geheimen Algorithmen basieren?

Ü

Übung 4.4: DSAA

Nennen Sie ein kryptographisches Verfahren, welches die unsichere `cassable` Blockchiffre ersetzen könnte.

Studienbrief 5 Design mobiler Betriebssysteme

5.1 Systemdesign

5.2 Besonderheiten mobiler Systeme

5.3 Fallstudie: iOS

5.4 Fallstudie: Android

5.5 Fallstudie: Analyse von Android Apps

Liste der Lösungen zu den Kontrollaufgaben

Lösung zu Kontrollaufgabe 2.1 auf Seite 28

Das GSM-System besteht aus:

- Mobilstation[1]
- Base Transceiver Station[1]
- Base Station Controller[1]
- (Gateway) Mobile Switching Center
- Operation and Maintenance System
- Home Location Register
- Visitor Location Register
- Authentication Center
- Equipment Identification Register

Die mit [1] gekennzeichneten Komponenten bilden das Funk-Teilsystem.

Lösung zu Kontrollaufgabe 2.2 auf Seite 29

Ein Angreifer könnte folgendermaßen vorgehen:

- Passiv: Er lauscht alle Funk-Verbindungen mit und wartet, bis sich eine Mobilstation erstmalig mittels IMSI in das GSM-Netz einbucht. Dies ist möglich, da beim erstmaligen Einbuchen die IMSI im Klartext an das GSM-Netz übertragen wird, um den teilnehmerspezifische Schlüssel zu bestimmen. In dieser Phase ist dementsprechend keine Verschlüsselung aktiv.
- Aktiv: Der Angreifer gibt sich als Basisstation aus und zwingt eine Mobilstation statt der TMSI die IMSI zu übertragen. Dies ist möglich, da sich die Basisstation gegenüber der Mobilstation nicht authentisieren muss.

Lösung zu Kontrollaufgabe 2.3 auf Seite 29

Ein Angreifer könnte folgendermaßen vorgehen:

- Er nutzt Schwachstellen in den Verschlüsselungsroutinen aus.
- Er gibt sich als Basisstation aus und unterdrückt wie in Abbildung 2.8 dargestellt die Verschlüsselung zwischen Mobil- und Basisstation.

Lösung zu Kontrollaufgabe 2.4 auf Seite 37

Das UMTS-System besteht aus:

- (Gateway) Mobile Switching Center
- Operation and Maintenance System
- Home Location Register
- Visitor Location Register
- Authentication Center
- Equipment Identification Register

Weiterhin wurden zur Unterscheidung zwischen GSM und UMTS neue Komponenten eingeführt bzw. bestehende Komponenten umbenannt.

- *UE*: Das *User Equipment* besteht aus dem mobilen Endgerät und dem *UMTS Subscriber Identity Modul* (USIM).
- *Node B*: Der *Node B* entspricht im wesentlichen der GSM-Basisstation und übernimmt die funktechnische Versorgung.
- *RNC*: Der *Radio Network Controller* übernimmt die Aufgaben der BSCs in GSM und verwaltet mehrere Node B-Komponenten.

Lösung zu Kontrollaufgabe 2.5 auf Seite 37

Die Basisstation sendet die Parameter $RAND$ und $AUTN = (SQN \oplus AK, AMF, MAC)$.

- $RAND$: Zufallszahl
- SQN: Sequenznummer - Schutz vor Replayangriffen (Freshness)
- AK: Anonymity-Key
- AMF: Authentication and Key Management Field
- MAC: Message Authentication Code - Authentizität des GSM-Netzes

Nach Erhalt des Tuples $(RAND, AUTN)$ berechnet die USIM zuerst den Anonymity-Key $AK = f5(K_i, RAND)$ und die Sequenznummer $SQN = (SQN \oplus AK) \oplus AK$. Im Anschluss wird die MAC $XMAC = f1(K_i, SQN, RAND, AMF)$ berechnet und mit der in $AUTN$ erhaltenen MAC des UMTS-Netzes verglichen. Bei Gleichheit verifiziert die USIM, ob die erhaltene Sequenznummer SEQ mit Hilfe der gespeicherten SQN_{MS} in einem gültigen Wertebereich liegt. Zuletzt berechnet die USIM $RES = f2(K_i, RAND)$, sendet diesen Wert zurück an die Basisstation und berechnet den Cipher-Key $CK = f3(K_i, RAND)$ und den Integrity-Key $IK = f4(K_i, RAND)$.

Lösung zu Kontrollaufgabe 2.6 auf Seite 37

Die $f8$-Funktion ist eine symmetrische Stromchiffre, welche den Schlüsselstrom für die Verschlüsselung der Daten in UMTS generiert. Die $f9$-Funktion bildet einen Message Authentication Code, welcher als Integritätsschutz einer Nachricht dient.

Beide Funktionen nutzen die Kasumi-Chiffre.

Lösung zu Kontrollaufgabe 3.1 auf Seite 45

Der $A3$-Algorithmus führt die Challenge-Response Berechnungen während der Authentisierungsphase durch, wohingegen der $A8$-Algorithmus den Sessionkey K_c generiert.

Lösung zu Kontrollaufgabe 3.2 auf Seite 45

Satellitentelefone bestehen häufig aus einem Standard-Mikroprozessor, einem dedizierten digitalen Signalprozessor, Speicher und weiterer Peripherie.

Lösung zu Kontrollaufgabe 3.3 auf Seite 51

Der R_4 LFSR spielt bei der Bestimmung der Taktungen für die LFSRs R_1, R_2 und R_3 eine Rolle, fließt aber nicht direkt mit in die Majority-Funktionen ein.

Lösung zu Kontrollaufgabe 3.4 auf Seite 51

Der Initialisierungsvektor wird aus der Frame-Nummer und dem Sessionkey K_c berechnet und hat die Aufgabe, die LFSRs vor der Generierung des Schlüsselstroms in einen initialen Zustand zu überführen.

Würde jeder Teilnehmer einen eigenen Initialisierungsvektor verwenden (ohne diesen mit dem Netzwerk zu teilen), könnte der Satellitenbetreiber die von einem Teilnehmer verschlüsselten Nachrichten nicht entschlüsseln. Ebenso könnte auch der Teilnehmer die Nachrichten vom Satellitenbetreiber nicht entschlüsseln, da der A5-GMR-1-Algorithmus auf jeder Seite einen anderen Schlüsselstrom erzeugen würde.

Lösung zu Kontrollaufgabe 3.5 auf Seite 60

Lookup-Tabellen spezifizieren in Rechenoperationen häufig genutzte statische Werte, um deren Berechnungen während der Laufzeit einzusparen.

Lösung zu Kontrollaufgabe 3.6 auf Seite 60

Der Schlüsselstrom fließt direkt in die Berechnungen der $\mathscr{F}$-Funktion ein und wird weiterhin in das Statusregister an Position S_0 getaktet.

Lösung zu Kontrollaufgabe 4.1 auf Seite 66

Die TDMA-Struktur erlaubt bis zu 12 simultanen Duplex-Sprachverbindungen pro Trägerfrequenz und damit einhergehend insgesamt 120 gleichzeitigen Sprachverbindungen im DECT-Standard.

Lösung zu Kontrollaufgabe 4.2 auf Seite 66

Das DECT-Referenzmodell entspricht den drei Schichten *Physical*, *Data Link* und *Network* des ISO/OSI-Modells.

Lösung zu Kontrollaufgabe 4.3 auf Seite 71

Der Dummy-Bearer enthält System- und Synchronisationsinformationen für die mobilen Endgeräte, sodass diese sich mit dem Takt der Basisstation synchronisieren können.

Lösung zu Kontrollaufgabe 4.4 auf Seite 71

Bei einem externen Handover wird der Fixed Part des mobilen Endgerätes gewechselt. Bei dem Übergang von altem zum neuen FP müssen Prozesse wie beispielsweise Verschlüsselung gestoppt und neu synchronisiert werden, sodass ein *Seamingless-Handover* nicht garantiert werden kann.

Lösung zu Kontrollaufgabe 4.5 auf Seite 79

DECT verwendet den *DECT Standard Authentication Algorithm* für die Authentisierung und die *DECT Standard Cipher* für die Generierung des Schlüsselstromes. Bei

beiden Algorithmen konnten die Funktionsweisen mittels Reverse-Engineering ermittelt und analysiert werden. Weiterhin wurden in beiden Algorithmen massive Schwachstellen und Sicherheitslücken entdeckt, sodass sowohl Authentisierung als auch Verschlüsselung in DECT nicht kryptographisch sicher sind.

Lösung zu Kontrollaufgabe 4.6 auf Seite 79

Der LFSR R_4 spielt lediglich bei der Bestimmung der Taktungen für die LFSRs R_1, R_2 und R_3 eine Rolle und fließt nicht direkt mit in die Kombinierfunktion ein.

Liste der Lösungen zu den Übungen

Übungsaufgaben zu Studienbrief 2

Lösung zu Übung 2.1 auf Seite 38

- Der Angreifer gibt sich gegenüber der Mobilstation als Basisstation und gegenüber dem Netz als Mobilstation des Opfers aus.
- Das GSM-Netz sendet die Authentisierungsanfrage *RAND* an den Angreifer.
- Der Angreifer leitet *RAND* an die Mobilstation.
- Die Mobilstation berechnet die Response *SRES* und sendet diese dem Angreifer.
- Der Angreifer leitet *SRES* an das GSM-Netz weiter und ist authentisiert.
- Das GSM-Netz initiiert eine A5/1 bzw. A5/3-Verschlüsselung mit dem Angreifer, wobei der Angreifer zu diesem Zeitpunkt K_c noch nicht kennt.
- Der Angreifer initiiert eine A5/2-Verschlüsselung mit der Mobilstation.
- Mittels Ausnutzung des Angriffes auf A5/2 berechnet der Angreifer innerhalb weniger Sekunden den Schlüssel K_c.
- Der Angreifer kommuniziert im folgenden mittels A5/1 bzw. A5/3 mit dem GSM-Netz und mittels A5/2 mit der Mobilstation.

In GSM wird die Identität des GSM-Netzes nicht validiert. Weiterhin wird für die Verschlüsselungsalgorithmen A5/1, A5/2 und A5/3 der gleiche Schlüssel K_c verwendet.

Lösung zu Übung 2.2 auf Seite 38

Im GSM-Standard wird die Integrität von Nachrichten nicht verifiziert, sodass ein Angreifer Nachrichten modifizieren kann. Im Gegensatz dazu nutzt UMTS die Integritätsfunktion $f9$, sodass der Empfänger mittels eines MAC erkennen kann, ob Änderungen an einer verschickten Nachricht durchgeführt wurden.

Lösung zu Übung 2.3 auf Seite 38

Besteht eine Chiffre auf einem Feistelnetzwerk, so ist die Chiffre in jedem Fall umkehrbar, d.h., der Ciphertext ist in jedem Fall wieder in den Klartext rückführbar.

Ein Feistelnetzwerk besteht aus mehreren Runden, wobei pro Runde nur eine Hälfte der Eingabe unter Zuhilfenahme eines Rundenschlüssels in die Berechnungen einfließt.

Übungsaufgaben zu Studienbrief 3

Lösung zu Übung 3.1 auf Seite 60

Ein LFSR hat die Aufgabe, streng deterministischen Pseudozufallszahlenfolgen zu generieren. Das Feedback-Polynom bestimmt die Abfolge der Pseudozufallszahlen und definiert damit die maximale Länge des LFSRs.

Lösung zu Übung 3.2 auf Seite 60

Stromchiffren eignen sich durch ihre Struktur besonders bei Echtzeitanwendungen wie der Telefonie, da jedes Bit/Byte der Nutzdaten direkt mit einem Bit/Byte des Schlüsselstroms verknüpft werden kann. Eine Blockchiffre benötigt eine bestimmte Anzahl an Nutzdaten und verarbeitet diese Daten erst, wenn ein Datenblock komplett gefüllt und damit für die Verschlüsselung bereit ist. Dies kann zu Verzögerungen während der Laufzeit führen.

Übungsaufgaben zu Studienbrief 4

Lösung zu Übung 4.1 auf Seite 79

Die Frequenzbereiche für CT1 und CT2 sind seit 2009 für die anderweitige Nutzung vorgesehen (öffentlichen Mobilfunk und Funkanwendungen kleinerer Reichweiten), sodass seit Ende des Jahres 2008 die Nutzung dieser Frequenzbereiche für CT1 bzw. CT2 nicht mehr gestattet ist.

Lösung zu Übung 4.2 auf Seite 79

Weiterhin sind die Frequenzträger in GSM in Upload und Download unterteilt, wobei bei DECT jeder Frequenzträger Up- als auch Downloadkanäle überträgt.

Lösung zu Übung 4.3 auf Seite 79

Nach Kerckhoffs' Prinzip sollte die Sicherheit eines Verschlüsselungsverfahrens nicht auf der Geheimhaltung des Verschlüsselungsverfahrens sondern auf der Geheimhaltung des Schlüssels basieren. Mittels Reverse Engineering und ähnlichen Techniken können Algorithmen rekonstruiert werden.

Lösung zu Übung 4.4 auf Seite 80

Generell können Verfahren wie Wi-Fi Protected Access 2 (WPA2) angewandt werden, die sich in ähnlichen Bereichen bereits bewährt haben. Der Einsatz von Public-Key Verfahren wäre ebenfalls denkbar.

Tabelle 6.1: Unterschiede zwischen DECT und GSM aus [Lüd01].

	DECT	GSM
Frequenzband	meist lizenzfrei	lizenziert
Mobilitätsbereich	begrenzt (Heimbereich / Büro)	international
Trägerabstand	1728 kHz	200 kHz
Duplexverfahren	TDD	FDD
Rahmenlänge	10 ms	4,6 ms
Zeitschlitze pro Rahmen	24	8
Kontrollkanäle	kombinierte Kanäle	gesonderte Kanäle
Kanalwahl durch	PP	FP
Handover durch	PP	FP

6.1 Literatur

[BBK08a] Elad Barkan, Eli Biham, and Nathan Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. *Journal of Cryptology*, 21(3):392–429, 2008.

[BBK08b] Elad Barkan, Eli Biham, and Nathan Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. *Journal of Cryptology*, 21, March 2008.

[Ben13] Benedikt Driessen. *PPractical Cryptanalysis of Real-World Systems: a Engineer's Approach*. Dissertation, Ruhr-Universität Bochum, 2013.

[BER07] Andrey Bogdanov, Thomas Eisenbarth, and Andy Rupp. A Hardware-Assisted Realtime Attack on A5/2 Without Precomputations. In *Cryptographic Hardware and Embedded Systems (CHES)*, 2007.

[Bou10] Noureddine Boudriga. *Security of Mobile Communications*. Taylor & Francis, 2010.

[DHW+12] Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz. Don't Trust Satellite Phones: A Security Analysis of Two Satphone Standards. In *Proceedings of the 2012 IEEE Symposium on Security and Privacy*, SP '12, pages 128–142, Washington, DC, USA, 2012. IEEE Computer Society.

[DHW+13] Benedikt Driessen, Ralf Hund, Carsten Willems, Christof Paar, and Thorsten Holz. An Experimental Security Analysis of Two Satphone Standards. *ACM Trans. Inf. Syst. Secur.*, 16(3):10:1–10:30, December 2013.

[DKS10] Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the kasumi cryptosystem used in gsm and 3g telephony. In *Proceedings of the 30th Annual Conference on Advances in Cryptology*, CRYPTO'10, pages 393–410, Berlin, Heidelberg, 2010. Springer-Verlag.

[Dri12] Benedikt Driessen. Eavesdropping on Satellite Telecommunication Systems. Cryptology ePrint Archive, Report 2012/051, 2012. `http://eprint.iacr.org/2012/051`.

[ETS99] ETSI. ETSI TS 133 102 V3.6.0 (2000-10); Universal Mobile Telecommunications System (UMTS); 3G Security; Security Architecture (3GPP TS 33.102 version 3.6.0 Release 1999), 1999.

[ETS01] ETSI. ETSI TS 135 201 V4.1.0 (2001-12); Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications (3GPP TS 35.201 version 4.1.0 Release 4), 2001.

[ETS02] ETSI. ETSI TS 101 376-5-3 V1.2.1 (2002-04); GEO-Mobile Radio Interface Specifications; Part 5: Radio interface physical layer specifications; Sub-part 3: Channel Coding; GMR-1 05.003, 2002.

[ETS07] ETSI. ETSI TS 135 201 V4.1.0 (2001-12); Universal Mobile Telecommunications System (UMTS); Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification (3GPP TS 35.202 version 7.0.0 Release 7), 2007.

[ETS11] ETSI. Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security features, 2011.

[Fed99] Hannes Federrath. *Sicherheit mobiler Kommunikation: Schutz in GSM-Netzen, Mobilitätsmanagement und mehrseitige Sicherheit*. DuD-Fachbeiträge. Vieweg+Teubner Verlag, 1999.

[For97] DECT Forum. DECT - the standard explained. Website, 1997. Online verfügbar auf `http://www.dectweb.com/DECTForum/publicdocs/TechnicalDocument.PDF`; besucht am 28.10.2014.

[LST+09] Stefan Lucks, Andreas Schuler, Erik Tews, Ralf-Philipp Weinmann, and Matthias Wenzel. Attacks on the DECT Authentication Mechanisms. In Marc Fischlin, editor, *CT-RSA*, volume 5473 of *Lecture Notes in Computer Science*, pages 48–65. Springer, 2009.

[Lüd01] Christian Lüders. *Mobilfunksysteme: Grundlagen, Funktionsweise, Planungsaspekte*. Kamprath-Reihe. Vogel, 2001.

[NTW10] Karsten Nohl, Erik Tews, and Ralf-Philipp Weinmann. Cryptanalysis of the DECT Standard Cipher. In *Proceedings of the 17th International Conference on Fast Software Encryption*, FSE'10, pages 1–18, Berlin, Heidelberg, 2010. Springer-Verlag.

[PFS00] Slobodan Petrovic and Amparo Fuster-Sabater. Cryptanalysis of the A5/2 Algorithm. Technical report, 2000. `http://eprint.iacr.org/2000/052`.

[Wal01a] Bernhard Walke. *Mobilfunknetze und ihre Protokolle 1*. Mobilfunknetze und ihre Protokolle. Teubner, 2001.

[Wal01b] Bernhard Walke. *Mobilfunknetze und ihre Protokolle 2*. Mobilfunknetze und ihre Protokolle. Teubner, 2001.

Glossar

Begriff	Erklärung
(G)MSC	(Gateway) Mobile Switching Center
3GPP	3rd Generation Partnership Project
AUC	Authentication Center
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CC	Call Control
CCCH	Common Control Channel
CCFP	Central Control Fixed Part
CCH	Control Channel
CHVI	Card Holder Verification Information
CN	Core Network
DECT	Digital Enhanced Cordless Telecommunications
DLC	Data Link Control
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DSP	Digitaler Signalprozessor
EIR	Equipment Identification Register
ETSI	European Telecommunications Standards Institute
FCCH	Frequency Correction Channel
FDD	Frequency Division Duplexing
FDM	Frequency Division Multiplex
FP	Fixed Part
GAP	Generic Access Profil
GEO	Geostationary Earth Orbit
GGSN	Gateway GPRS Support Node
GIP	DECT/GSM Interworking Profil
GMR	Geostationary Earth Orbit Mobile Radio Interface
GP	Guard Period
GPRS	General Packet Radio Service
GSM	Global System for Mobile Telecommunications
GSN	GPRS Support Node
HLR	Home Location Register
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity

IWU	Interworking Unit
LAI	Location Area Identifier
LFSR	Linear rückgekoppeltes Schieberegister
MAC	Medium Access Control
MC	Multi Carrier
MM	Mobility Management
MS	Mobilstation
OMC	Operation and Maintenance System
PCU	Packet Control Unit
PLMN	Public Land Mobile Network
PP	Portable Part
RFP	Radio Fixed Part
RFPI	Radio Fixed Part Identifier
RNC	Radio Network Controller
SGSN	Support GPRS Support Node
SIM	Subscriber Identity Modul
TCH	Traffic Channel
TCH3	Traffic Channel-3
TDD	Time Division Duplexing
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access
VLR	Visitor Location Register

Open C³S
Open Competence Center for Cyber Security

Fort- und Weiterbildung

Neue Bedrohungszenarien stellen Sicherheitsexperten und IT-Verantwortliche in Unternehmen und einschlägigen Behörden vor immer größere Herausforderungen. Neue Technologien und Anwendungen erfordern zusätzliches Know-how und personelle Ressourcen.

Zur Erhöhung des Fachkräftepools und um neues Forschungswissen schnell in die Praxis zu integrieren, haben sich die im Bereich lehrenden und forschenden Verbundpartner zum Ziel gesetzt, ein hochschuloffenes transdisziplinäres Weiterbildungsprogramm im Sektor Cyber Security zu entwickeln. Auf der Grundlage kooperativer Strukturen werden wissenschaftliche Weiterbildungsmodule im Verbund zu hochschulübergreifenden Modulpaketen und abschlussorientierten Ausbildungslinien konzipiert und im laufenden Studienbetrieb empirisch getestet.

Die Initiative soll High Potentials mit und ohne formale Hochschulzugangsberechtigung über innovative Weiterbildungsangebote (vom Zertifikat bis zum Masterprogramm) zu Sicherheitsexperten aus- und fortbilden. Hierzu werden innovative sektorale Lösungen zur Optimierung der Durchlässigkeit von berulicher und hoch- schulischer Bildung entwickelt und für eine erfolgreiche Implementierung vorbereitet. Unter prominenter Beteiligung einschlägiger Verbände, der Industrie sowie Sicherheits und Ermittlungsbehörden verfolgt die Initiative das Ziel, im deutschsprachigen Raum eine Generation von Fachkräften wissenschaftlich aus- und weiterzubilden, die unser Internet schützen kann.

Open Competence Center for Cyber Security

Open C³S ist aus dem Verbundvorhabens Open Competence Center for Cyber Security entstanden. Das Gesamtziel des Programms war die Entwicklung eines hochschuloffenen transdisziplinären Programms wissenschaftlicher Weiterbildung im Sektor Cyber Security. Das Bundesministerium für Bildung und Forschung (BMBF) fördert das Großprojekt im Rahmen des Wettbewerbs „Aufstieg durch Bildung: offene Hochschulen“, der aus BMBF-Mitteln und dem Europäischen Sozialfonds finanziert wird.

Neun in Forschung und Lehre renommierte Hochschulen und Universitäten aus dem gesamten Bundesgebiet haben sich zum Ziel gesetzt, Online-Studiengänge auf dem Gebiet der Cybersicherheit zu entwickeln. Dieses Konzept soll den Studierenden ermöglichen, sich berufsbegleitend auf hohem Niveau wissenschaftliche Qualifikationen anzueignen und akademische Abschlüsse zu erlangen. Beruflich erworbene Kompetenzen können eingebracht werden. Die Bezeichnung „Open“ steht auch für die Öffnung des Zugangs zu akademischer Bildung ohne klassischen Hochschulzugang.

Mission der Initiative ist es, dringend benötigte Sicherheitsexperten aus- und fortzubilden, um mit einer sicheren IT-Infrastruktur die Informationsgesellschaft in Deutschland und darüber hinaus zu stärken.

Umsetzungsnahes Wissen ist ein wesentlicher Schlüssel um der wachsenden digitalen Bedrohung zu begegnen. Solange wir nicht in der Lage sind, Systeme hinreichend zu härten, Netzwerke sicher zu designen und Software sicher zu entwickeln, bleiben wir anfällig für kriminelle Aktivitäten. Unser Ziel ist es, die Mitarbeiter von heute zu Sicherheitsexperten und Führungskräften von morgen auszubilden und dafür zu sorgen, dass sich die Zahl und die Fertigkeiten dieser Experten nachhaltig erhöht.

Weitere Informationen zu Open C³S: https://open-c3s.de

Z308 Sicherheit mobiler Systeme

Im Modul „Sicherheit mobiler Systeme“ werden verschiedene Sicherheitsaspekte von mobilen Systemen vorgestellt. Anhand von konkreten Beispielen wird erläutert, wie verschiedene Arten von mobilen Systemen aufgebaut sind und welche Sicherheitsrisiken diese besitzen.

Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Sicherheitsaspekten von mobilen Endgeräten vertraut, welche auf andere Arten von Systemen übertragen werden können.

Sie verfügen über detaillierte Kenntnisse der Sicherheit von mobilen Endgeräten. Die Studierenden haben die Fähigkeit, sich eine Meinung über die Sicherheit von mobilen Endgeräten zu bilden. Darüber hinaus besitzen sie die Kompetenz, eigenständig neue Angriffe und Bedrohungen aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren.

Zertifikatsprogramm

Die Zertifikatsmodule auf wissenschaftlichem Niveau und mit hohem Praxisbezug bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung. Damit können einzelne Module nebenberuflich studiert werden. Durch die Vergabe von ECTS-Punkten können sie auf ein Studium angerechnet werden.

https://zertifikatsprogramm.de