Netzsicherheit I, WS 2011
Übung 1

Prof. Dr. Jörg Schwenk

Betreuer: Florian Feldmann, Florian Giesen

Abgabe: Montag, 23. Oktober 2011, 11:00h

In der Übung, am Kasten vor ID 2/467, oder per Mail an Florian.Giesen AT rub.de
Gruppenarbeit bis max. 3 Studenten pro Gruppe ist erlaubt und erwünscht.

1 Das GSM-Protokoll

In der Vorlesung haben Sie gelernt, wie sich die Mobile Station (MS) gegenüber dem Home Enviroment (HE) mit Hilfe des Home Location Registers (HLR) authentifiziert.

a) Erklären Sie den Unterschied zwischen IMSI und IMEI. Für welchen Zweck werden diese verwendet?

b) Aus welchem Grund wird anstatt der IMSI oft eine TMSI übertragen? Welche Partei erzeugt diese TMSI?

2 IMSI-Catcher

IMSI-Catcher werden in der Praxis dazu eingesetzt, die Kommunikation von Mobile Stations abzuhören. Dabei gibt sich der IMSI-Catcher gegenüber der Mobile Station als Basisstation aus. Um die Kommunikation abhören zu können, verleitet der IMSI-Catcher die Mobile Station dazu, keine Verschlüsselung (A5) für die Kommunikation zu verwenden
Hinweis: Damit in Ausnahmesituationen wie z.B. Resourcenüberlastung die Kommunikation weiterhin funktioniert, unterstützen die Mobile Stations einen Fallback auf Null-Verschlüsselung. (Stichwort: availability)

a) Wird die Kommunikationsfähigkeit der Mobile Station durch den Einsatz eines IMSI-Catchers beeinträchtigt? (Kann sich der IMSI-Catcher mit der IMSI der Mobile Station gegenüber der Base Station authentifizieren?)

b) Wie kann der Besitzer eines abgehörten GSM-Handy herausfinden, dass er abgehört wird?

c) Kann ein Benutzer verhindern, dass sein GSM-Handy abgehört wird? Falls ja, wie?

3 UMTS

Warum funktioniert ein IMSI-Catcher nicht mit dem UMTS-Protokoll? Geben Sie an, welche Schritte im UMTS-Protokoll entfernt werden müsten, damit der Angriff möglich ist.
Hinweis: Skizzieren Sie das UMTS-Protokoll und verdeutlichen Sie die Bedeutung der Parameter.

4 Sicherheit von Challenge-and-Response-Verfahren

Betrachten Sie die folgenden Challenge-Response Varianten:

1. Alice schickt RAND und die aktuelle Uhrzeit an Bob, Bob antwortet mit der Verschlüsselung dieser Nachricht.
2. Alice schickt Bob die Verschlüsselung von RAND und der aktuellen Uhrzeit, Bob antwortet mit RAND.

a) Welche Variante bietet eine höhere Sicherheit, wenn RAND von einem schwachen Zufallszahlengenerator erzeugt wird? Begründen Sie Ihre Antwort und sagen Sie, wie Bruce Schneier[1] die schwache Variante kaputt macht.

b) Welche Variante hat einen Nachteil, wenn RAND echt zufällig gewählt wird? Begründen Sie Ihre Antwort.

5 Angriff auf das TMN-Protokoll (Klausur)

Nachfolgend (Abbildung 1) ist eine Variante des TMN Protokolls dargestellt. Das Protokoll verwendet statt dem XOR von r_A und r_B die Addition modulo n.

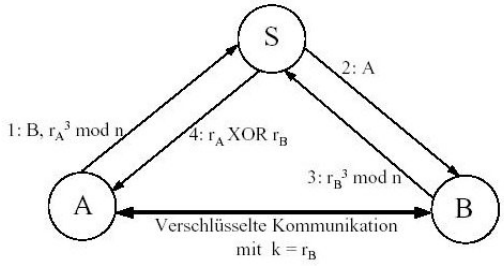

Abbildung 1: Das TMN-Protokoll

a) Führen Sie den Angriff von Simmons auf das oben dargestellte Protokoll durch. Gehen Sie wie folgt vor.
   1. Stellen Sie den Angriff graphisch dar. Verwenden Sie dabei die Notation aus obiger Grafik, und nummerieren Sie die einzelnen Schritte aufsteigend in der richtigen Reihenfolge.
   2. Führen Sie für jeden einzelnen Schritt die jeweils notwendigen Berechnungen durch. Verwenden Sie folgende Werte: $n = 667$, $r_A^3 = 167$, $r_B^3 = 507$ und wählen Sie die Zufallswerte $r' = 150$ und $r_C = 200$. Geben Sie am Ende den Schlüssel $k = r_B$ aus. *Hinweis*: Es gilt $637^3 = 347 \; mod \; n$.

[1] Bruce Schneier ist ein Synonym für einen sehr fähigen Kryptologen: www.schneierfacts.com