GSS-Übungsblatt 5 zum 18.06.2014

A. Struck, S. Haase, E. Böhmecke

18. Juni 2014

Aufgabe 1

1)

Bei einem symmetrischen Kryptosystem besitzen beide Kommunikationspartner den gleichen Schluessel. D.h., es wird der gleiche Schluessel zum ent- und verschluesseln verwendet.
Im asymmetrischen Kryptosystem hingegen besitzen beide Kommunikationspartner jeweils ein eigenes Schluesselpaar aus Public Key und Private Key. So kann jeder mit dem oeffentlich zugaenglichen Public Key Dokumente verschluesseln, die nur dem Besitzer des Private Key zugaenglich sind. Andersherum kann der Besitzer des Private Keys Dokumente signieren, wobei jeder mit Hilfe des Public Keys die Authentizitaet der Signatur ueberpruefen kann.

2)

a)

Falls Alice Bob eine grosze Menge an Daten senden moechte, waere es effiezenter, ein hybrides Kryptosystem einzusetzen.

b)

Dabei wird ein symmetrischer Schluessel generiert, welche die gesamten Nutzdaten verschluesselt. Der symmetrische Schluessel selbst wird mit Alices asymmetrischen Schluessel verschluesselt und ebenfalls uebertragen.

c)

Den Nutzdaten der Nachricht geht der mit Bobs Public Key verschluesselte symmetrische Schluessel voraus, mit dem die anschliszenden Nutzdaten verschluesselt wurden.

Aufgabe 2

2)

Es scheint moeglich zu sein, sich die verguenstigungen auf jedes Ticket "aufzustempeln", da diese nicht in eine größere Checksumme aufgenommen werden. Es handelt sich um einfache Zahlen, die an den eigentlich Code prependiert werden.
Angreifermodell:

- Rolle: Benutzer
- Verbreitung: Systemfehler des Parkhauses (systemweit)
- Verhalten: aktiv (Druck eigener/Veränderung von vorhandenen Tickets)
- Rechenkapazität: Keine herkömmliche (vielleicht Drucker). Ansonsten so lange, wie der Angreifer braucht das Muster zu finden

3)

Alle Daten muessen Teil einer groszen Checksumme werden, welche dann mit einem dem System bekannten Schluessel verschluesselt wird. Das Resultat davon wird als Barcode auf die Karte gedruckt.

Aufgabe 3

3.1.:

Passiver Angriff (abhören der Kommunikation von c): Anmeldung (je nach E_k) dauerhaft oder einmalig durch Angreifer möglich, Daten abfragen möglich.
(lokales abhören von c): Anmeldung (je nach E_k) dauerhaft oder einmalig durch Angreifer möglich, Daten abfragen möglich.
Aktiver Angriff (Zugang, wie beim passivem Angriff): Ändert Daten auf dem Server.
MiM-Angriff: Tut so, als ob der Angreifer der Server wäre. Kann durch Angriff auf den User k erlangen und somit durch c möglicherweise E_k reverse Engineeren.

3.2.:

Das reverse Engineering von E_k wird erschwert. So lange r nicht serverseitig generiert UND sicher übertragen wird, ändert sich an den Angriffen nichts.

3.3.:

Durch Mitschneiden der gesamten Kommunikation ist ein MiM immer noch möglich, das direkte Einloggen alleine durch Kenntnis von c, ist allerdings verhindert.

Aufgabe 5

2)

$$\Phi(n) = (p-1)(q-1) \tag{1}$$
$$\Phi(n) = (281-1)(389-1) \tag{2}$$
$$\Phi(n) = 108640 \tag{3}$$

Modulare inverse von 67 mod 108640 = d = 3243

Der entschlüsselte Text lautet:
Fuer die GSS-Klausur sind folgende Themen wichtig: Schutzziele, Angreifermodelle, Rainbow Tables, die (Un-)Sicherheit von Passwoertern und dazugehoerige Angriffe, Zugangs- und Zugriffskontrolle, Biometrische Verfahren, Timing-Attack und Power-Analysis, Grundlagen der KryptographieQ2 Authentifikationsprotokolle, das RSA-Verfahren und natuerlich alle anderen Inhalte, die wir in der Uebung und der Vorlesung behandelt haben :-)