Team 4 Innovation

4Security Protokollbeschreibung

Mathematisch nachvollziehbare Protokollbeschreibung der Kommunikation zwischen Zentralsystem und Fingerprintscanner

Grundsätzliches:

Es wird hier das Kommunikationsprotokoll zwischen einem Zentralsystem (ZS) und einem Fingerprintscanner (FP) beschrieben.
Hierbei werden Anforderungsstrings x0 Fingerprintdaten x1 und Antwortdaten x2 übertragen.
Der Fingerprint selbst in seiner Ursprungsform wird als X1 bezeichnet, der mittels Kompressionsverfahren bzw. durch weitere Abstraktion auf x1 reduziert und konvertiert wird.
Die Verschlüsselung wird mit einem Stern gekennzeichnet, also x1 verschlüsselt mit $A_1^{'}$ wird geschrieben als $x1 * A_1^{'}$.
Die einzelnen Schlüssel werden in folgender Weise benannt:

X_n für einen orginären Entschlüsselungskey

$X_n^{'}$ für den zu X_n gehörenden Verschlüsselungskey, aber auch der zu $X_n^{''}$ gehörende Entschlüsselungskey.

$X_n^{''}$ ist folglich der Verschlüsselungskey für $X_n^{'}$

Zusammengefasst also:

Entschlüsselung	Verschlüsselung
X_n	$X_n^{'}$
$X_n^{'}$	$X_n^{''}$

Aber X_n hat keinen direkten Bezug zu $X_n^{''}$

N steht bei den Keys für die jeweilige Kommunikationsnummer, So gilt für die Kommunikation Nummer 1, dass die vorhergehenden Keys n=1-1 also n=0 tragen, die aktuellen Keys n=1 und die Keys für die folgnede Kommunikation n=2 tragen.
Die Keys $X_n^{'}$ und $X_n^{''}$ sind Ableitungen aus dem jeweilig vorhergehenden Key also $X_n^{'}$ ist eine Ableitung von X_n; $X_n^{''}$ ist eine Ableitung von $X_n^{'}$. Insofern kann diese Nomenklatur als sinnvoll – auch für die Beschreibung mehrerer Transaktionen bezeichnet werden.

Folgende Keyklassen gibt es:

Keyklasse A für Basiskeys, die im Zentralsystem (ZS) erstellt werden,

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

Keyklasse B für Scannerkeys, die im Fingerprintscanner (FP) erstellt werden,
Keyklasse C für im FP erstellte Kombikeys und
Keyklasse D für im ZS erstellte Kombikeys.

Nun die einzelnen primären Keys und ihre Lokationen in der Übersicht:

Key	Ersteller	Lokation
A_n	ZS	ZS
$A_n^{'}$	ZS	FP
$A_n^{''}$	ZS	ZS
B_n	FP	FP
$B_n^{'}$	FP	ZS
$B_n^{''}$	FP	FP

Hinzu kommen noch die Metakeys, die aus mehreren Keys zusammengesetzt werden:

Key	Ersteller	Bestehend aus	Korrespondenzkey	Lokation
C_n	FP	$A_n^{'} \times B_n$	$D_n^{''}$	FP
$C_n^{''}$	FP	$A_n^{'} \times B_n^{''}$	D_n	FP
D_n	ZS	$A_n \times B_n^{'}$	$C_n^{''}$	ZS
$D_n^{''}$	ZS	$A_n^{''} \times B_n^{'}$	C_n	ZS

Wir betrachten in der Kommunikation zwischen dem Zentralsystem exemplarisch den Zeitpunkt 1; also gilt für Keys, die in der vorhergehenden Kommunikation erstellt wurden n=0, für die aktuellen Keys n=1;

Nun also zum eigentlichen Ablauf:

1. FP fordert bei ZS einen Key an:

   FP erstellt den Anforderungsstring x0 und verschlüsselt diesen mit $C_0^{''}$, also $x0 * C_0^{''}$.
   Dieser String wird in ZS über D_0 entschlüsselt.
   Falls die Anforderung verstanden werden kann (sie mit dem richtigen Schlüssel verschlüsselt ist und der String x0 korrekt ist,

2. erzeugt ZS folgende Schlüssel:

   A_1 ; $A_1^{'}$; $A_1^{''}$

   A_1 und $A_1^{''}$ verbleiben im ZS, während $A_1^{'}$ an FP übertragen werden muß. Dies geschieht

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com

über $A_1^{'} * D_0^{''}$, das heißt $A_1^{'}$ wird mit dem vorhergehenden Kombikey verschlüsselt und an FP übertragen.
FP entschlüsselt $A_1^{'} * D_0^{''}$ mit C_0. Falls dort ein gültiger $A_1^{'}$ dabei herauskommt (Schlüssellänge, bestimmte Formvorschriften, etc.)

3. erstellt FP folgende Schlüssel:

   B_1 ; $B_1^{'}$; $B_1^{''}$

   B_1 und $B_1^{''}$ verbleiben im FP, während $B_1^{'}$ an ZS übertragen wird. Dies geschieht über $B_1^{'} * A_1^{'}$; das heißt $B_1^{'}$ wir mit dem zuvor übertragenen Zentralschlüssel $A_1^{'}$ verschlüsselt und an ZS übertragen.
   Im ZS wird $B_1^{'} * A_1^{'}$ mit Hilfe von A_1 entschlüsselt und auf Gültigkeit geprüft.

4. Kombinationskeyerstellung:

   In FP werden aus
   $A_1^{'} \times B_1$ → C_1 und aus
   $A_1^{'} \times B_1^{''}$ → $C_1^{''}$ erstellt

   Im ZS werden aus

   $A_1 \times B_1^{'}$ → D_1 und aus
   $A_1^{''} \times B_1^{'}$ → $D_1^{''}$ erstellt.

5. Übertragung des Fingerprints:

   Der im FP aufgenommene Fingerprint X1 wird in x1 überführt X1 → x1. Die Fingerprintdaten x1 werden mit $C_1^{''}$ verschlüsselt, also $x1 * C_1^{''}$ und von FP an ZS versandt.
   In ZS wird $x1 * C_1^{''}$ mit Hilfe von D_1 entschlüsselt.

6. Übertragung von Rückmeldungen:

   Nachdem die entschlüsselten Fingerprintdaten in ZS abgeglichen wurden wird eine Antwort x2 mit $D_1^{''}$ verschlüsselt und an FP versandt, also $x2 * D_1^{''}$.
   In FP wird $x2 * D_1^{''}$ mit C_1 entschlüsselt.

Team 4 Innovation GBR
Herbststr. 27
85737 Ismaning

Phone: +49 89 962 073 - 54
Fax: +49 89 962 073 - 55
Web: www.Team4Innovation.com
e-mail: info@team4innovation.com