Universität Hamburg
Fachbereich Informatik

Hinweise für das Erscheinungsbild von Seminar-, Studien- und Bachelor-, Master- und Diplomarbeiten

am Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

Prof. Dr. Hannes Federrath

28. November 2014

(Muster für das Deckblatt: siehe letzte Seite dieser Hinweise)

Zusammenfassung

Für den eiligen Leser sollen auf etwa einer halben, maximal einer Seite die wichtigsten Inhalte, Erkenntnisse, Neuerungen bzw. Ergebnisse der Arbeit beschrieben werden.

Durch eine solche Zusammenfassung (im engl. auch Abstract genannt) am Anfang der Arbeit wird die Arbeit deutlich aufgewertet. Hier sollte vermittelt werden, warum der Leser die Arbeit lesen sollte.

Inhaltsverzeichnis

1 Verschlüsselungsschema

Nachdem eine Nachricht aus dem Message Space - wie im vorherigen Kapitel beschrieben - durch eine DTE auf den Seed Space abgebildet wurde, folgt die Verschlüsselung des Ergebnisses. Hierfür schlägt [[**?**]] zwei verschiedene Vorgehensweisen vor. Die unter Verwendung dieser Vorgehensweisen entstehenden Honey Encryption-Schemata werden im Folgenden dargestellt.

1.1 Hashbasierte Verschlüsselung

Im ersten Schritt ...

$\text{HEnc}_{\text{Hash}}(M, K)$
- $S \xleftarrow{<r>} \text{DTE}(M)$
- $K_D = \text{PBKDF}(K)$
- $R \xleftarrow{<r>} 0,1^n$
- $H = \text{HF}(K_D, R)$
- $C = H \oplus S$
- Return (C, R)

Abbildung 1: Hashbasierte Verschlüsselung

$\text{HDec}_{\text{Hash}}((C, R), K)$
- $K_D = \text{PBKDF}(K)$
- $H = \text{HF}(K_D, R)$
- $S = H \oplus C$
- $M = \text{DTE}^{-1}(S)$
- Return M

Abbildung 2: Hashbasierte Entschlüsselung

1.2 Auf Blockchiffren basierte Verschlüsselung

$\text{HEnc}_{\text{Block}}(M, K)$

$S \xleftarrow{<r>} \text{DTE}(M)$

$R \xleftarrow{<r>} 0,1^k$

$K' = \text{HF}(K, R)$

$P = \epsilon$

For $i = 1$ to $\left\lceil \frac{|S|}{n} \right\rceil$

$P = P \parallel \text{Enc}(K', i)$

$C = P[1..|S|] \oplus S$

Return (C, R)

Abbildung 3: Verschlüsselung mit Blockchiffre (CTR-Modus)

$\text{HDec}_{\text{Block}}((C, R), K)$

$K' = \text{HF}(K, R)$

$P = \epsilon$

For $i = 1$ to $\left\lceil \frac{|S|}{n} \right\rceil$

$P = P \parallel \text{Enc}(K', i)$

$S = P[1..|S|] \oplus M$

$M = \text{DTE}^{-1}(S)$

Return M

Abbildung 4: Entschlüsselung mit Blockchiffre (CTR-Modus)