Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Entwurf vom 19. Juni 2017

Masterarbeit

Exposé zur Masterarbeit - Pseudonymisierung von und Einsatz von Schwellwertschemata für Logeinträge

vorgelegt von

Tom Petersen

geb. am 13. Dezember 1990 in Hannover

Matrikelnummer 3659640

Studiengang Informatik

eingereicht am 19. Juni 2017

Betreuer: Dipl.-Inf. Ephraim Zimmer

Erstgutachter: -

Zweitgutachter: -

1 Einführung

Irgendein zufälliges [Lam81] Zitat. Und hier kommt auch noch ein Zitat hin: [Beu09]!

1.1 Motivation

- Insiderangriffe

- SIEM-Systeme in aktueller Form keine adäquate Lösung

- Datenschutzrecht Arbeitnehmer

- Spannungsfeld Aufdeckbarkeit und Datenschutz

1.2 Ziele der Arbeit

In dieser Arbeit soll es darum gehen prototypisch...

- OSSIM: wo ansetzen? Agent, Client, dazwischen (eigene Komponente) Performancemessungen

- Schlüsselmanagement (Clientseitig erzeugen, wie verteilen, etc.)

- Welche kryptographischen Schwellwertschemata? Performancemessungen

- Welche Funktionen? (Reine Verschlüsselung, Pseudonymisierung mit Mappingtabelle, ... -> erweiterbar)

2 Inhalte

2.1 SIEM-Systeme

- Was ist das?
- OSSIM als Open-Source-Vertreter

2.2 Pseudonymisierung

Pseudonymisierung als Möglichkeit der Verschleierung und Nicht-Verkettbarkeit.

2.3 Schwellwertschemata

- Shamir How to share a secret?
- Public Key Problematik
- Was ist das? (siehe auch Paper für Definition)
- Fünde (RSA, Paillier, ...) und Desmedt/Frankel evtl. hier schon Pedersen/...

Literatur

[Beu09] Albrecht Beutelspacher. *Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. 9. akt. Auflage. Wiesbaden: Vieweg + Teubner, 2009.

[Lam81] Leslie Lamport. *Password authentication with insecure communication*. In: *Communications of the ACM* 24.11 (1981), S. 770–772.