Grundlagen der Systemsoftware

Modul: InfB-GSS

Veranstaltung: 64-091

Mittwoch, 10-12

Utz Pöhlmann
4poehlma@informatik.uni-hamburg.de
6663579

Louis Kobras
4kobras@informatik.uni-hamburg.de
6658699

Hans Wurst
hwurst@sausage.de
6654232

Nobody Nose
nobody@nose.de
6543216

Steve
steve@steve.de
6666666

18. April 2016

Punkte für den Pflichtteil:

1.1	1.2	1.3	Σ

Zettel Nr. 1 (Ausgabe: 11. April 2016, Abgabe: 20. April 2016)

Übungsaufgabe 2.1: Schutzziele - Abrenzung I

[| 5]

a)
- **Anonymität:** die eigenen Identität wird niemandem offenbart
- **Pseudonymität:** anderen wird eine falsche Identität (Pseudonym) offenbart
- **Unbeobachtbarkeit:** die eigene Anwesenheit bzw. Existenz wird geheim gehalten

Abgrenzung. Der Unterschied zwischen Anonymität, Pseudonymität und Unbeobachtbarkeit ist, dass der Gesprächspartner im ersten Fall zwar weiß, dass jemand da ist, aber nicht, wer. Im zweiten Fall glaubt der Gesprächspartner, zu wissen, wer da ist, irrt sich aber. Im dritten Fall ist er sich nicht einmal über die Anwesenheit einer weiteren Entität im Klaren.

b)
- **Vertraulichkeit:** jemand ist sich der Übertragung bewusst, kann sie aber nicht auslesen
- **Verdecktheit:** die Übertragung bleibt unentdeckt

Abgrenzung. Während eine dritte Partei sich im ersten Fall dessen bewusst ist, dass es eine Übertragung gibt, deren Inhalt allerdings nicht erlangen kann, ist sich die dritte Partei dem Vorhandensein einer Übertragung im zweiten Fall nicht bewusst.

Übungsaufgabe 2.2: Schutzziele - Abgrenzung II

[| 4]

a)
- **Integrität:** Änderung der Inhalte können durch den Empfänger festgestellt werden
- **Zurechenbarkeit:** es ist nachweisbar, wer die Daten gesendet und wer sie empfangen hat

Abgrenzung. Der Unterschied zwischen Integrität und Zurechenbarkeit ist, dass im ersten Fall zwar festgestellt werden kann, ob die Daten verändert wurden, aber nicht eingesehen werden kann, wer die Daten verändert hat. Im zweiten Fall geht es darum, dass man definitiv weiß, wenn eine dritte Partei in den Datenstrom eingegriffen hat.

b)
- **Verfügbarkeit:** Ressourcen sind vorhanden, wenn jemand darauf zugreifen will
- **Erreichbarkeit:** Ressourcen sind abrufbar, wenn jemand sie benötigt

Abgrenzung. Der Unterschied zwischen Verfügbarkeit und Erreichbarkeit ist, dass im ersten Fall die Ressource nur vorhanden sind, aber nichts darüber gesagt wird, ob sie auch abrufbar sind. Im zweiten Fall geht es darum dass verfügbare Ressourcen auch abrufbar sind.

Übungsaufgabe 2.3: Schutzziele - Techniken

[| 4]

Schutzziel	**Technik**
Anonymität	VPN
Pseudonymität	VPN
Unbeobachtbarkeit	VPN
Vertraulichkeit	RSA
Verdecktheit	F5
Integrität	Prüfsummen
Zurechenbarkeit	Signatur (PGP)
Verfügbarkeit	Diversität der Daten
Erreichbarkeit	Redundanz der Daten

Übungsaufgabe 3.2: Angreifermodell - Praxisbeispiel

[| 10]

- **Rolle:**
  - Außenstehender
- **Verbreitung:**
  - Pin erahnen bis errechnen
  - Magnetstreifen auslesen
- **Verhalten:**
  - passiv
  - beobachtend
- **Rechenkapazität:**
  - beschränkt

Übungsaufgabe 5.3: Passwortsicherheit - Brute-Force-Angriff

[| 3]

Das gegebene Tool berechnet (1.000.000 Passwörter pro Sekunde $*60$ Sekunden $*60$ Minuten $*24$ Stunden $*$ 365 Tage) $= 3.1516x10^{12}$ Passwörter pro Jahr.

- 62 alphanumerisch Zeichen
  - 8 Zeichen lang
  - $\Rightarrow 62^8 \approx 2.18x10^{13}$ Möglichkeiten
  - $\Longrightarrow 62^8$ Möglichkeiten $/3.1516x10^{13}$ Passwörter pro Jahr ≈ 6.92 Jahre ≈ 2527 Tage dauert es im worst-case, ein solches Passwort zu knacken
- 10 Ziffern
  - 1-16 Zeichen lang
  - $\Rightarrow \Sigma_{i=1}^{16}(10^i) \approx 1.11x10^{16}$ Möglichkeiten (eine mehr, wenn als Passwort "kein Passwort" zugelassen ist, d.h. ein Passwort der Länge 0)
  - $\Longrightarrow \Sigma_{i=1 \text{ xor } i=1}^{16}(10^i)$ Möglichkeiten $/3.1516x10^{12}$ Passwörter pro Jahr ≈ 352.33 Jahre ≈ 128.600 Tage.

Am Exponenten der Basis kann bereits erkannt werden, dass der erste Fall mit dem Passwort statischer Länge, aber mit größerer Wertemenge, einfacher zu lösen ist. Um alle Möglichkeiten mit variabler Länge durchzurechnen, wird ein deutlich größerer Zeitaufwand gefordert.