GSS Aufgabe 01

Carolin Konietzny, Paul Bienkowski, Julian Tobergte, Oliver Sengpiel, Lars Thoms

15. April 2015

2.1 (Abgrenzung I)

a) **Anonymität, Pseudonymität, Unbeobachtbarkeit**
In allen drei Bereichen geht es um die Verschleierung der Identität und/oder der Handlungen von Sender/Empfänger. Anonymität ist hierbei die stärkste Ausprägung, da hier noch nicht einmal der Kommunikationspartner weiß, um wen es sich bei seinem Gegenüber handelt. Dies ist jedoch nur dann möglich, wenn die Aktionen nicht von der Identität der Personen abhängen, wie es zum Beispiel bei einem Handel der Fall wäre. Pseudonymität bietet eine abgeschwächtere Stufe der Identitätsverschleierung. Hier hat der Kommunikationspartner die Möglichkeit die Identität des Gegenübers über ein Pseudonym zu verifizieren (Beispiel Accountname). Die letzte Form wäre die Unbeobachtbarkeit. Hier sind die Identitäten für die beiden Sender/Empfänger jeweils bekannt, aber die Aktionen zwischen den beiden werden nach außen hin versteckt, so dass kein Dritter diese abhören kann.

b) **Vertraulichkeit, Verdecktheit**
Bei diesen Begriffen geht es um die Inhalte der Daten, die versandt/weitergegeben werden. Bei beiden geht es darum die Inhalte vor Dritten zu verstecken. Vertraulichkeit kann zum Beispiel durch Verschlüsselung erreicht werden. Verdecktheit hingegen erreicht man nur, indem man den Informationsaustausch an sich versteckt. Dies nennt sich Steganographie.

3.1 (Angreifermodell)

Angreifermodelle werden dazu benutzt, um die „Stärke" zu bestimmen/festzulegen, die ein Angreifer höchstens haben darf, damit die Sicherheitsvorkehrungen ihn gerade noch davon abhalten in die Integrität oder Vertraulichkeit des Systems eingreifen zu können.

Ein Angreifer wird dabei durch folgende Begriffe charakterisiert: Rolle, Verbreitung, Verhalten und Rechenkapazität.

Die Rolle kann zum Beispiel „Außenstehender" oder „Wartungsmitarbeiter", aber auch „Benutzer" oder „Produzent" sein. Die Verbreitung gibt an, an welchen Stellen im System der Angreifer agieren kann. Das Verhalten kann entweder „aktiv" oder „passiv" sein. Nur ein aktiver Angreifer kann verändernd auf ein System wirken. Die Rechenkapazität wird zwischen „unbeschränkt" und „beschränkt" unterschieden.