R

Repudiation

2. Ein Angreifer kann den Inhalt von Logdaten beeinflussen, einen Log Reader (Programm oder Nutzer) darüber angreifen und es ist nicht dokumentiert, ob und wie verschiedene Logdaten validiert werden.

3. Ein unprivilegierter Nutzer oder Angreifer hat lesend Zugang zu interessanten Sicherheitsinformationen in den Logs.

4. Ein Angreifer kann digitale Signaturen manipulieren, weil Sie einen MAC Algorithmus statt eines Signier-verfahrens nutzen, oder weil das Signierverfahren unsicher ist.

5. Ein Angreifer kann Lognachrichten verändern, die übers Netz übertragen werden, weil kein starker Mechanismus zur Gewährleistung der Integrität implementiert ist.

6. Ein Angreifer kann einen Logeintrag ohne Zeitstem-pel erzeugen (oder die Logs haben generell keine Zeitstempel).

7. Ein Angreifer kann das Log zum Überlaufen bringen, so dass alte Logdaten überschrieben werden und somit verloren sind (wrap- around).

Fortsetzung umseitig

Repudiation

R

Repudiation cont.

8. Ein Angreifer kann das Logging so austricksen, dass sicherheitsrelevante Logdaten nicht geschrieben werden oder durcheinander geraten.

9. Ein Angreifer kann einen Shared Key nutzen, um sich als jemand anders auszugeben, so dass seine Aktionen ebenfalls unter dieser Identität mitgeloggt werden.

10. Ein Angreifer kann beliebige Logdaten in ein Logsystem einschleusen, weil die Logquellen nicht oder nur schwach authentisiert werden.

J. Ein Angreifer kann unbemerkt Logs editieren, löschen oder deren Übermittlung unterbinden.

Q. Ein Angreifer kann abstreiten, etwas getan zu haben und es gibt keine brauchbaren Daten, um das Gegenteil zu beweisen.

K. Das System hat keine Logs.

A. Sie haben einen neuen Repudiation Angrif erfunden.