F.T. Breuer, O. Kramer, M. Stolpe Dortmund, 12. Januar 2009

Übungen zur Vorlesung

Betriebssysteme, Rechnernetze und verteilte Systeme II

Wintersemester 2008/2009

Blatt 11

Aufgabe 10.3 von Blatt 10 erscheint als Aufgabe 11.1 auf diesem Blatt noch einmal, da Firewalls erst am 12.01.2009 besprochen werden. Abgaben zur Aufgabe 10.3 werden gewertet, sofern für Aufgabe 11.1 keine erneute Abgabe vorliegt.

Aufgabe 11.1 (2 Pkte.) Sie beraten ein Unternehmen in Sicherheitsfragen. Das Unternehmen plant den Kauf einer Firewall.

(a) Erläutern Sie, warum der Einsatz einer Firewall unter Umstanden das Risiko eines Angriffs erhöhen kann.

(b) Welche Lösung scheint in ihren Augen die bessere zu sein: das Abschalten nicht benötigter Dienste oder eine Zugriffsbeschränkung auf nicht benötigten Diensten mit Hilfe einer Firewall? Diskutieren Sie Vor- und Nachteile der Varianten in Hinblick auf Sicherheitsrisiken und Administrationsaufwand.

Aufgabe 11.2 (4 Pkte.) Um das Abhören der Kommunikation durch Dritte zu verhindern, wird in WLAN-Netzen Verschlüsselung eingesetzt.

(a) Welcher Typ von Verschlüsselung wird bei der Kommunikation zwischen Clients und Access Points in WLAN-Netzen verwendet?

(b) Erläutern Sie stichpunktartig die Arbeitsweise von WEP. Warum gilt WEP als unsicher?

(c) Nennen Sie ein in der Vorlesung vorgestelltes Protokoll, das ebenfalls eingesetzt werden könnte, um den gesamten IP-Verkehr in einem WLAN-Netz zu verschlüsseln. Auf welcher Schicht arbeitet ein solches Protokoll?

Aufgabe 11.3 (2 Pkte.) Digitale Signaturen können bestätigen, dass ein Text von einer bestimmten Person hergestellt worden ist und seitdem nicht verändert wurde.

(a) Nennen Sie Vor- und Nachteile digitaler Signaturen im Vergleich zu herkömmlichen Unterschriften.

(b) Wie vertrauenswürdig erscheint ihnen eine digitale Signatur, welche i) auf dem kryptographischen Hash-Verfahren MD5 und ii) auf SHA-1 basiert?

Aufgabe 11.4 (4 Pkte.) Verschaffen Sie sich auf den Webseiten

- `http://www.heise.de/security/` und
- `http://www.securityfocus.com/vulnerabilities`

einen Eindruck von den Sicherheitslücken, die in der Vergangenheit bei den Betriebssystemen Windows und Linux sowie den Browsern Internet-Explorer und Mozilla Firefox aufgetreten sind.

Versetzen Sie sich in die Lage eines Hackers, der den mit einem als kryptographisch sicher geltenden Verfahren verschlüsselten Datenverkehr zwischen Tante Erna und ihrer Bank abhören und verändern möchte. Beurteilen Sie die folgenden Angriffe, indem Sie für jeden Angriff die Erfolgswahrscheinlichkeit (hoch/mittel/niedrig) und den Aufwand (hoch/mittel/niedrig) abschätzen. Begründen Sie ihre Schätzung jeweils stichpunktartig.

1. Abfangen der Kommunkation auf einem Router und Entschlüsselung mittels Brute-Force-Angriff.
2. Ausnutzen einer Schwachstelle bei der Bank (Server, Skripte, etc.) und Installation eines Trojaners auf dem Server der Bank.
3. Ausnutzen einer Schwachstelle bei Tante Erna (Betriebssystem, JavaScript oder ActiveX im Browser, sonstige Software) und Installation eines Trojaners auf dem Client-Rechner.
4. Anruf bei Tante Erna als vermeintlicher Mitarbeiter der Bank mit Bitte um PIN und nächster TAN-Nummer. Vorgabe, diese seien bei einem Absturz der Bankrechner leider abhanden gekommen und die Freischaltung des vorgeblich gesperrten Kontos sei nur möglich mit den geforderten Angaben.