Prüfungsprotokoll Systemsicherheit / Netzwerksicherheit

Diplom Informatik, Fach Betriebssysteme

24. März 2009

Sven Pfaller

Nach ein, zwei Minuten „Small-Talk“ ging die Prüfung auch schon los. Insgesamt war ich anfangs nervös, doch durch die lockere Art der Prüfung legte sich das schnell. Ich durfte mir aussuchen mit welchen Themengebiet (NetSec oder SysSec) ich beginnen wollte, und habe NetSec gewählt.

Netzwerksicherheit

(Herr Dressler)

1) Angefangen hat es mit der Frage ob ich meinen Personalausweis vorzeigen soll. Das wurde erstmal als Diskussionsgrundlage genommen: Ist der Personalausweis wirklich zur Authentifizierung geeignet?

   Authentifizierung durch Besitz und TTP: A besitzt den Perso und B vertraut der Bundesregierung (TTP). Integrität ist gegeben durch verschiedene Mechanismen zur Verhinderung einer Fälschung.

2) Wie kann man sich im Netzwerk authentifizieren?

   Zum Beispiel Needham-Schroeder, Otway-Rees oder Authentifizierungsmechanismen von IPSec, SSL, SSH, usw.

3) Beschreibe prinzipiell wie man sich direkt authentifizieren kann.

   A und B mit Verbindung gezeichnet. A und B kennen ein Shared Secret KAB. A schickt an B eine Zufallszahl verschlüsselt mit KAB, B antwortet mit Zufallszahl + 1, wieder verschlüsselt mit KAB.

4) Beschreibe ein Verfahren mit dem man sich über eine TTP authentifizieren kann.

   Needham-Schroeder beschrieben.

5) Wie kann man Vertraulichkeit und Integrität sicherstellen?

   Verschlüsselung und MDC.

6) Bewerte die folgenden drei Reihenfolgen von Verschlüsselung und MDC auf Sicherheit und Integrität.
   - E(M) || H(M)
   - E(M || H(M))
   - E(M) || H(E(M))

   Die ersten beiden sind okay. Beim letzten ist die Integrität nicht wirklich geschützt, da man ein E(M) erfinden und dazu den gültigen MDC H(E(M)) berechnen kann.

7) Wie kann man Replay-Attacken verhindern?
   - Authentifizierung: Mit Zufallszahlen / Timestamps
   - Verlässliches Protokoll (z.B. TCP): Sequenznummern
   - Unverlässliches Protokoll (z.B. UDP): Replayfenster (wie bei IPSec)

Nach ca. 20 Minuten übernahm Herr Kleinöder das Ruder.

Systemsicherheit
(Herr Kleinöder)

1) Was für Sicherheitsziele hat man für ein lokales System?

   Authentifizierung, Vertraulichkeit, Integrität, Stabilität (Anti-DoS)

2) Beschreibe die Umsetzung von einem der Ziele.

   Vertraulichkeit: Verschlüsselung für Dateien / Partitionen.

3) Welche Probleme gibt es bei Verschlüsselung?

   - Daten sind evtl. unverschlüsselt im Speicher / im Swap / in temporärer Datei
   - Passwörter meist zu unsicher
   - Was passiert wenn man das Passwort vergisst? Key-Recovery?

4) Wie funktioniert Key-Recovery?

   Erstmal Windows EFS erklärt. Der Administrator kann die Datei immer entschlüsseln und die Passwörter der Benutzer ändern, er übernimmt die Key-Recovery.

5) Welche Probleme gibt es bei der Key-Recovery?

   - Wo ist der Private Key des Administrators gespeichert?
   - Was wenn jemand Administratorrechte erlangt?

Der Übergang zum Kryptographieteil war ziemlich fließend...

Kryptographie
(Herr Kleinöder)

1) Woher kommt der FEK bei EFS?

   Wird zufällig erstellt. Pseudo Random Number Generator allgemein und RSA-PRNG grob erklärt. Eignung eines PRNG kann mit Next-Bit-Test überprüft werden.

2) Die Datei wird ja dann mit dem FEK symmetrisch verschlüsselt. Wie funktioniert das?

   Die Datei wird Blockweise verschlüsselt. Ein Block wird mit dem Feistelnetzwerk verarbeitet, die einzelnen Blöcke werden dann mit ECB, CBC, CFB oder OFB zusammengefügt.

3) Wo liegt der Unterschied zwischen den vier Blockverfahren?

   ECB und CBC grob erklärt. CFB und OFB sind Stream-Ciphers.

Dann war die Prüfung auch schon vorbei. Die Fragen waren nicht so scharf getrennt wie hier dargestellt, sondern haben sich immer durch das Gespräch ergeben. Auch die Antworten haben sich meistens „entwickelt“. Etwas ins Straucheln gekommen bin ich bei den ersten drei NetSec Fragen (wegen der Aufregung) und bei NetSec Frage 6 hat es lange gedauert bis ich auf die Antwort gekommen bin. Trotzdem ist die Prüfung insgesamt „sehr gut“ ausgefallen :) .