Leistungsnachweis-Klausur

Kurs 01868 Sicherheit im Internet I – Ergänzungen

05.02.2010

Lösungshinweise

Aufgabe 1: **(8 Punkte)**

Geben Sie vier Systeminformationen an, die zum Systemzustand im Sinne der Computerforensik gehören. Ein Beispiel einer solchen Systeminformation ist der Inhalt des Hauptspeichers.

S. Kurstext Seite 26

Aufgabe 2: **(9 Punkte)**

Welche der folgenden Aussagen treffen zu?

☒ Ein Angreifer muss alle Mixe einer Mix-Kaskade übernehmen, um eine Verbindung nachverfolgen zu können.

☐ Von einem digital signierten ActiveX-Control ist bekannt, dass es keine Schadfunktionen enthalten kann.

☒ Ein Rollenpseudonym wird von einer Person immer dann benutzt, wenn die Person sich in der zugehörigen Rolle befindet. Dabei ist es egal, wer die Kommunikationspartner sind.

☒ Java-Applets dürfen keine Dateien des lokalen Dateisystems lesen.

☐ Beim Konzept des Dummy Traffic verschickt der Benutzer seine Nachrichten verschlüsselt, jedoch keine überflüssigen Nachrichten.

☐ Ein Rewebber leitet einen http-Request eines Client unverändert an den Web-Server weiter.

Aufgabe 3: **(6 Punkte)**

Wie viele Ringe bieten typische Intel-CPUs. Welche Ringe entsprechen dabei dem Benutzer-Modus (Anwendungsprogramme) und dem System-Modus (Betriebssytem)?

4 Ringe, Anwendung=Ring 3, System=Ring 0

Aufgabe 4: **(9 Punkte)**

Welche der folgenden Aussagen treffen zu?

☐ Beim Konzept der Access-Control-Listen wird die Zugriffskontrollmatrix (pro Benutzer eine Zeile, pro Ressource eine Spalte) zeilenweise bei den Benutzern gespeichert.

☒ Beim Konzept der Access-Control-Listen wird die Zugriffskontrollmatrix (pro Benutzer eine Zeile, pro Ressource eine Spalte) spaltenweise bei den Ressourcen gespeichert.

☐ Die False Acceptance Rate sagt aus, wie oft ein legitimer Benutzer fälschlicherweise nicht vom System akzeptiert wird.

☒ Im Bell-LaPadula-Modell der Informationsflusskontrolle benötigt man besonders vertrauenswürdige Personen, die die Sicherheitsklasse von Objekten auch wieder herunterstufen dürfen. (Denn sonst hätten irgendwann alle Objekte die höchste Sicherheitsstufe, was nicht sinnvoll ist.)

☐ Das Modell der Informationsflusskontrolle von Kenneth Biba versucht, die Vertraulichkeit von Daten sicherzustellen.

☒ Beim Konzept der Paravirtualisierung weiß das Gast-Betriebssystem, dass es nicht direkt auf der Hardware läuft, sondern in einer virtuellen Maschine.

Aufgabe 5: **(6 Punkte)**

Auf welche Weise ist ein Betrug (gefälschtes Dokument) möglich, wenn ein Client bei einer Challenge-Response-Authentisierung die Challenge unverändert signiert?

s. Lösung zur Einsendeaufgabe 2.2

Aufgabe 6: **(8 Punkte)**

Das WEP-Verfahren in WLANs benutzt RC4 als Stromchiffre mit einem 24-Bit Initialisierungsvektor und einem 40-Bit Schlüssel.

Wir machen folgende Annahmen: der Initialisierungsvektor wird im Klartext übertragen und abgehört. Der Klartext eines übertragenen und abgehörten Pakets ist bekannt. Ein Angreifer kann pro Sekunde den Klartext 2^{17} mal verschlüsseln und mit dem verschlüsselten abgehörten Paket vergleichen. Im Mittel muss der Angreifer die Hälfte aller Schlüssel ausprobieren, bis er den richtigen findet.

Wie viele Tage (Zweierpotenz) braucht der Angreifer im Mittel, um den richtigen Schlüssel zu finden?
Gehen Sie davon aus, dass ein Tag 2^{16} Sekunden hat.

Da der Initialisierungsvektor bekannt ist, muss der Angreifer im Mittel 2^{39} Schlüssel ausprobieren, indem der den Klartext des Pakets verschlüsselt und mit dem abgehörten Paket vergleicht. Dies dauert, da pro Sekunde 2^{17} Klartexte verschlüsselt werden können:
$2^{39-17}=2^{22}$ Sekunden~$2^{22-16}=2^{6}$ Tage.

Aufgabe 7: **(4 Punkte)**

Welche der folgenden Aussagen treffen zu?

☐ WEP Verschlüsselung ist sicher, wenn der Access Point die SSID im Beacon Frame leer lässt (sog. Hide SSID) und zusätzlich eine Filterung anhand der MAC-Adresse vornimmt.

☐ Das Verschlüsselungsverfahren WPA/TKIP ist ein Blockverschlüsselungsverfahren.

☒ Bei der WPA Enterprise Mode Authentisierung mit EAP-TLS müssen der Access Point und alle Clients, die sich mit ihm verbinden wollen, ein X.509-Zertifikat besitzen.

☒ Über einen RADIUS-Server kann eine Authentisierung mit Hilfe von individuellen Benutzer-Passwörtern realisiert werden.

Hinweis: sollte bei EAP-TLS statt Access Point besser heißen:
der zum Access Point gehörende Authentication Server