Kurs 1868 Sicherheit im Internet 1 – Ergänzungen

Hauptklausur 04. Februar 2012

Lösungsvorschläge

Prof. Dr. J. Keller , LG Parallelität & VLSI

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.

siehe Kurstext Seite 26

Aufgabe 2: **(13 Punkte)**

Welche der folgenden Aussagen treffen zu?

Trifft zu	Trifft nicht zu	
☒	☐	Ein Angreifer muss alle Mixe einer Mix-Kaskade übernehmen, um eine Verbindung nachverfolgen zu können.
☐	☒	Ein digital signiertes ActiveX-Control enthält wegen der Signierung garantiert keine Schadfunktionen.
☐	☒	Ein Beziehungspseudonym wird von einer Person immer dann benutzt, wenn die Person sich in einer bestimmten Rolle befindet. Dabei ist es egal, wer der Kommunikationspartner ist.
☐	☒	Java-Applets dürfen Dateien des lokalen Dateisystems lesen.
☐	☒	Beim Konzept des Dummy Traffic verschickt der Benutzer seine Nachrichten verschlüsselt, jedoch keine überflüssigen Nachrichten.
☒	☐	Ein Broadcast anonymisiert den Empfänger der Nachricht, der Nachrichteninhalt ist aber nicht geschützt.
☒	☐	Ein Rewebber entfernt aus einem http-Request alle Informationen, die auf den Absender schließen lassen.
☒	☐	Ein http-Proxy, der das Intranet einer Firma mit dem Internet verbindet, verschleiert einem Angreifer, welcher Mitarbeiter eine bestimmte Anfrage stellt.

Aufgabe 3: **(8 Punkte)**

Wie viele sogenannte Ringe bieten typische Intel-CPUs? Welcher Ring entspricht dabei dem System-Modus (Betriebssystem)? Wozu dienen die beiden mittleren Ringe?

4 Ringe

Ring 0 = BS
Ring 1 = Treiber
Ring 2 = Dienste

Aufgabe 4: **(13 Punkte)**

Welche der folgenden Aussagen treffen zu?

Trifft zu	Trifft nicht zu	
☐	☒	Beim Konzept der Access-Control-Listen wird die Zugriffskontroll-matrix (pro Benutzer eine Zeile, pro Ressource eine Spalte) zeilenweise bei den Benutzern gespeichert.
☐	☒	Die False Rejection Rate eines biometrischen Verfahrens ist niemals höher als die Equal Error Rate.
☒	☐	Die False Rejection Rate sagt aus, wie oft ein legitimer Benutzer fälschlicherweise nicht vom System akzeptiert wird.
☐	☒	Im Bell-LaPadula-Modell der Informationsflusskontrolle muss die Sicherheitsklasse von Objekten niemals heruntergestuft werden.
☒	☐	Beim Konzept der Paravirtualisierung weiß das Gast-Betriebssystem, dass es in einer virtuellen Maschine läuft und nicht direkt auf der Hardware.
☒	☐	Ein Treiber, der im Betriebssystem-Modus läuft, kann Schadcode zum Auslesen von Speicherbereichen anderer laufender Programme enthalten.
☒	☐	Der Zugriffsschutz in Datenbanken ergänzt die Zugriffsschutz-Funktionen des Betriebssystems.
☐	☒	Die Passkontrolle ist ein Beispiel für ein One-to-Many-Matching.

Aufgabe 5:

Schildern Sie als Beispiel einer Challenge-Response-Authentisierung die Nutzung von TANs beim Web-Banking. Geben Sie hierzu genau an, was die Challenge und was die Response ist, und worin das Geheimnis des Benutzers besteht.

Lösung: siehe Kurstext Seite 77 ff.

Aufgabe 6: **(12 Punkte)**

Das WEP-Verfahren in WLANs benutzt RC4 als Stromchiffre mit einem 24-Bit Initialisierungsvektor und einem 40-Bit Schlüssel. Wir machen folgende Annahmen: dem Angreifer sind 16 Bit des Initialisierungsvektors bekannt. Der Klartext eines übertragenen und abgehörten Pakets ist dem Angreifer ebenfalls bekannt. Der Angreifer kann pro Sekunde den Klartext 2^{23} mal verschlüsseln und mit dem verschlüsselten abgehörten Paket vergleichen. Im Mittel muss der Angreifer die Hälfte aller Schlüssel ausprobieren, bis er den richtigen findet.

Wieviele Tage (Zweierpotenz) braucht der Angreifer im Mittel, um den richtigen Schlüssel zu finden? Begründen Sie Ihre Antwort. Wie ändert sich die benötigte Zeit, wenn dem Angreifer alle Bits des Initalisierungsvektors bekannt sind?
Hinweis: Gehen Sie davon aus, dass ein Tag 2^{16} Sekunden hat.

$2^8 \cdot 2^{40} / (2^{23} \cdot 2^{16} \cdot 2) = 2^8$ Tage

Wenn alle: 1 Tag

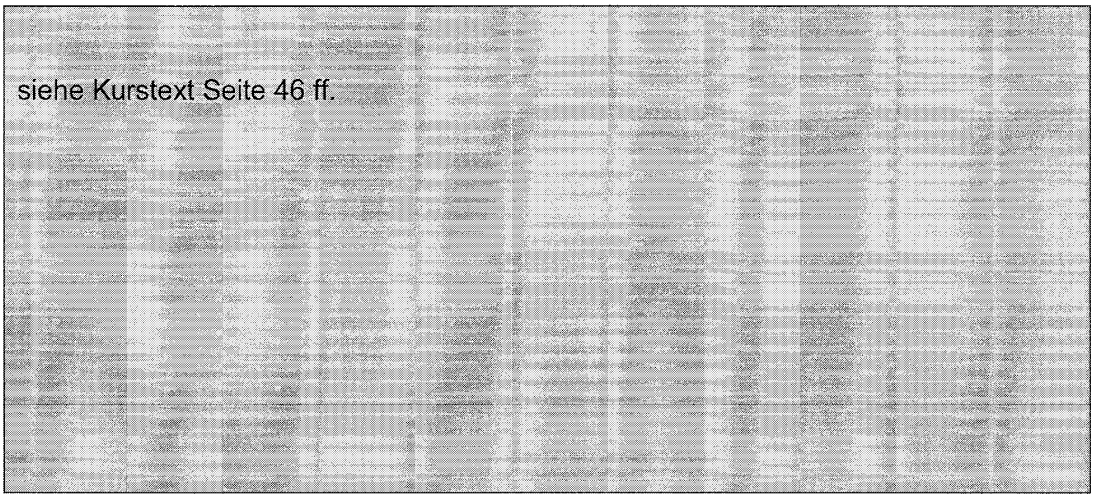
Aufgabe 7: **(11 Punkte)**

Welche der folgenden Aussagen treffen zu?

Trifft zu	Trifft nicht zu	
☒	☐	Beim War-Driving fährt man mit einem Laptop durch eine Stadt und sucht unverschlüsselte WLANs.
☐	☒	Das Verschlüsselungsverfahren WPA/TKIP ist ein Blockverschlüsselungsverfahren.
☐	☒	Ein WLAN-Access-Point kann durch eine Zugriffskontrolle auf Basis von MAC-Adressen zuverlässig vor unberechtigter Nutzung geschützt werden.
☒	☐	Bei VoIP gibt es zur Signalisierung (Verbindungsaufbau) das Session-Initiation-Protocol (SIP) der IETF und den H.323-Standard der ITU.
☐	☒	Es ist unmöglich, VoIP-Telefone aus dem normalen Telefonnetz anzurufen.
☒	☐	Um bei einem VoIP-Anruf die Sprachdaten mit SRTP zu verschlüsseln, muss ein Session Key zwischen Anrufer und Angerufenem ausgetauscht werden.

Aufgabe 8: **(8 Punkte)**

Wofür stehen die Zeilen und Spalten einer Zugriffskontrollmatrix?
Geben Sie weiterhin an, wie eine Zugriffskontrollmatrix jeweils bei Access-Control-Lists und Capabilities gespeichert wird.



Aufgabe 9: **(16 Punkte)**

Gegeben sei ein Kerberos-System mit N Servern (plus einem Authentication-Server) und M Clients. Geben Sie an, wieviele Schlüssel, die zur Ticket-Erstellung benötigt werden (keine Session Keys), jeweils der Authentication-Server, jeder Server und jeder Client kennen muss. Wie ändern sich diese Werte, wenn auf Kerberos verzichtet wird, und stattdessen für jedes Paar aus einem Client und einem Server ein pre-Shared Key benutzt wird?
Es seien N=10 Server und M=1000 Clients vorhanden. Der Schutz eines Rechners, der nur 1 Schlüssel kennt, koste 10 Euro/Jahr. Der Schutz eines Rechners, der mehr als 1 Schlüssel kennt, koste 1000 Euro/Jahr. Bestimmen Sie für beide Situationen (Kerberos und pre-Shared Keys) die jährlichen Kosten.

Anth Server	N+M
Server	1
Client	1

$1 \cdot 1000 + 1010 \cdot 10 = 11100$

Client	: N
Server	: M

$1010 \cdot 1000 = 1.010.000$