Ostbayerische Technische Hochschule (OTH) Amberg-Weiden

Fakultät Elektrotechnik, Medien und Informatik

Informationssicherheit – Prof. Dr. A. Aßmuth und Prof. Dr. U. Schäfer

Wintersemester 2016/17

Name:				Vorname:				
Matrikelnummer:				Studiengang: ◯ AI-MI ◯ SW				
A 1	A 2	A 3	A 4	A 5	A 6	A 7	**Gesamt**	**Note**
/ 10	/ 15	/ 10	/ 4	/ 8	/ 6	/ 7	/ 60	
Erstprüfer: ..... Aßmuth				Zweitprüfer: ..... Schäfer				

Die vorliegende Prüfung enthält insgesamt 5 Seiten mit Angaben (Deckblatt, Angaben zur Prüfung sowie Aufgabenstellungen) und insgesamt 7 Aufgaben. Die maximal erreichbare Punktzahl beträgt **60**.
Für die Bearbeitung der Aufgaben liegt beim Durchführenden der Prüfung Zusatzpapier bereit. Alle Blätter (diese Angabe sowie Zusatzpapier) sind vor Abgabe der Prüfung mit Namen und Matrikelnummer zu beschriften. Während der Prüfung sind außer einem Lineal oder Geometriedreieck und einem nicht programmierbaren Taschenrechner keine Hilfsmittel zugelassen.
Sämtliches vernetzbares technisches Equipment ist während der Prüfung nicht zugelassen und führt im Falle der Zuwiderhandlung zum Nichtbestehen der Prüfung. Mobiltelefone sind während der Prüfung auszuschalten.

Viel Erfolg!

Aufgabe 1: Aktuelle Bedrohungen (10 Punkte)
Die folgenden Teilaufgaben stehen in keinem Zusammenhang und können daher unabhängig voneinander bearbeitet werden.

(a) Sweet32 (CVE-2016-2183, CVE-2016-6329) ist ein Angriff gegen TLS oder OpenVPN, wenn in diesen Protokollen eine Blockchiffre mit 64 Bit Blocklänge verwendet wird. Ausgenutzt wird dabei die Tatsache, dass jede Blockchiffre bei der Verschlüsselung sehr großer Mengen von teilweise bekanntem Klartext mit nur einem Schlüssel unsicher wird, wobei eine Abhängigkeit von der jeweiligen Blocklänge und dem verwendeten Betriebsmodus besteht. Sweet32 nutzt diese Unsicherheit bei Blockchiffren mit 64 Bit Blocklänge im CBC-Modus in einem Man-in-the-Browser-Szenario aus. Das Opfer ruft eine vom Angreifer kontrollierte Webseite auf und diese bringt den Computer des Opfers dazu, immer wieder die gleiche Nachricht über den TLS-Kanal zu übermitteln. Mit ca. 232 Geheimtextblöcken kann der Angreifer das Session Cookie entschlüsseln.
Beschreiben Sie kurz ein geeignetes Vorgehen, wie sich Benutzer gegen diesen Angriff schützen können. *(3 Punkte)*

(b) Zur Authentifizierung wird auch heute noch oft die Kombination von Benutzername (oft Emailadresse) und Passwort verwendet. Erklären Sie kurz, wie ein Angreifer Benutzeraccounts kompromittieren kann, bei denen (i) ein gängiges Wort als Passwort

bzw. (ii) ein zu kurzes Passwort (beispielsweise kürzer als sechs Zeichen) verwendet wird. *(4 Punkte)*

(c) Im September 2016 verzeichnete der französische Webhoster OHV einen DDoS-Angriff mit Rekord-Werten von bis zu 1,1 Terabit pro Sekunde. Es wird vermutet, dass ein Botnetz bestehend aus mehr als einer Million Geräte aus dem Internet der Dinge (IoT) die Kapazitäten für den Angriff zur Verfügung gestellt hat.
Erläutern Sie kurz, was man unter einem DDoS-Angriff versteht und gegen welches Schutzziel sich diese Klasse von Angriffen richtet. *(3 Punkte)*

Aufgabe 2: Netzwerksicherheit (15 Punkte)

(a) In immer mehr Restaurants, Hotels, Kaufhäusern etc. wird den Kunden ein kostenloses und meist unverschlüsseltes WLAN zur Verfügung gestellt. Smartphones, die einmal mit einem solchen Netz verbunden waren, speichern die SSID (Abk. f. Service Set Identifier), um sich automatisch wieder verbinden zu können, wenn sich das Gerät wieder in der Funkreichweite des entsprechenden Netzes befindet.
Erläutern Sie kurz, wie dies durch einen Angreifer ausgenutzt werden kann. Benennen Sie das Ziel dieses Angreifers sowie eine Gegenmaßnahme, mit der sich Smartphone-Nutzer schützen können. *(5 Punkte)*

(b) Stellen Sie das Angriffsszenario "TCP-Session-Hijacking" dar. Klassifizieren Sie diesen Angriff und benennen Sie etwaige Voraussetzungen. *(5 Punkte)*

(c) Entwerfen Sie für einen Anwendungsdienst ein Protokoll zur beidseitigen Authentifizierung (Client und Server). Gehen Sie dabei davon aus, dass beide Kommunikationspartner ein Geheimnis besitzen, welches zur Identifizierung des jeweiligen Kommunikationspartners genutzt werden kann. *(5 Punkte)*

Aufgabe 3: Wahr oder falsch? (10 Punkte)
Entscheiden Sie, ob die nachstehenden Aussagen wahr oder falsch sind. Kreuzen Sie Ihre Antworten entsprechend an, Sie brauchen Ihre Antworten nicht zu begründen.
Hinweis: Sei r die Anzahl der richtigen und sei f die Anzahl der falschen Antworten. Sie erhalten für diese Aufgabe insgesamt $\max\{0, r - f\}$ *Punkte, nicht beantwortete Fragen gehen nicht in die Bewertung ein.*

(a) Um Benutzereingaben HTML-Formularen auszuwerten, sollte man aus Gründen der Sicherheit die JavaScript-Funktion `eval` verwenden.

☐ wahr ☐ falsch

(b) Jedes Unternehmen braucht einen Datenschutzbeauftragten.

☐ wahr ☐ falsch

(c) Beim Fluhrer-Mantin-Shamir-Angriff gegen die WEP-Verschlüsselung in WLANs nach IEEE 802.11 b handelt es sich um eine sog. "Known-Plaintext Attack".

☐ wahr ☐ falsch

(d) Wenn ein(e) Benutzer/-in urheberrechtlich geschützte Inhalte bei Facebook nur mit den jeweiligen Freunden teilt, ist das erlaubt.

☐ wahr ☐ falsch

(e) Um Passworte in einer Benutzer-Datenbank auf dem Server zu speichern, sollte man nur gehashte Passworte in der Datenbank ablegen.

☐ wahr ☐ falsch

(f) Diese Hashwerte sollten als primary key für die Benutzer-Tabelle der Datenbank verwendet werden.

☐ wahr ☐ falsch

(g) Wenn vom Smartphone sämtliche Kontakte eines WhatsApp-Benutzers zu WhatsApp übertragen werden, dürfen diese uneingeschränkt von WhatsApp genutzt werden.

☐ wahr ☐ falsch

(h) Die private Adresse einer Person ist laut dem BDSG und der EU-Datenschutz-Grundverordnung eine besondere Art einer personenbezogenen Information.

☐ wahr ☐ falsch

(i) Eine Paketfilter-Firewall arbeitet auf der Netzzugangsschicht des TCP/IP-Referenzmodells.

☐ wahr ☐ falsch

(j) Soll eine Nachricht signiert und verschlüsselt werden, wird sie in der Praxis zunächst signiert und anschließend verschlüsselt.

☐ wahr ☐ falsch

Aufgabe 4: Forensische Sprachtechnologie (4 Punkte)
Im Vortrag von Prof. Weir bzw. in der Vorlesung wurde ein Verfahren vorgestellt, das die Autorenschaft eines Textes einer Person aus einer Auswahl von Autoren, von denen weitere Texte zugänglich sind, zuordnet. Beschreiben Sie das Verfahren. Worauf ist bezüglich der eingesetzten Textmengen bei der Zuordnung zu den Autoren zu achten? *(4 Punkte)*

Aufgabe 5: Web-Sicherheit I (8 Punkte)

(a) Wie funktioniert ein SQL-Injection-Angriff und welcher Schaden kann damit angerichtet werden? *(2 Punkte)*

(b) Nennen Sie drei Möglichkeiten für JavaScript- bzw. PHP-Entwickler, SQL-Injection-Schwachstellen bei der Webentwicklung zu vermeiden, und erläutern Sie diese kurz, ggf. mit Beispiel. *(3 Punkte)*

(c) Beschreiben Sie das wesentliche Funktionsprinzip von Cross-Site-Scripting-Angriffen. *(3 Punkte)*

Aufgabe 6: Web-Sicherheit II (6 Punkte)
Bitte lesen Sie folgenden Artikel und beantworten Sie die beiden Fragen dazu am Ende.

"**Konzerthaus leakt Tickets fremder Nutzer**
Nach langer Verzögerung und deutlich gestiegenen Kosten soll die Hamburger Elbphilharmonie morgen endlich eröffnen - zuvor wurde aber noch ein Datenschutzproblem im Ticketsystem entdeckt. Angreifer hätten die Tickets anderer Besucher herunterladen können.
Das Ticketsystem des neuen Hamburger Konzerthauses Elbphilharmonie hatte in den vergangenen Monaten offenbar ein Datenschutzproblem. Wie Heise.de meldet, konnten Nutzer, die im Shop eingeloggt waren, auf fremde Tickets im PDF-Format zugreifen. Das Problem wurde seitens der Elbphilharmonie mittlerweile behoben. Die Tickets für das neue Konzerthaus sind begehrt und werden teils zu hohen Preisen auf dem Schwarzmarkt gehandelt. Für das morgige Eröffnungskonzert sollen zum Teil mehr als 1.000 Euro für ein Ticket gefordert worden sein. In der Vergangenheit war es mehrfach zu Überlastungen des Ticket-Shops gekommen, ein effektives Load-Balancing oder ein DDoS-Schutz scheinen also nicht vorhanden zu sein.
Tickets durch URL-Manipulationen
Das Datenschutzproblem ließ sich nach Angaben von Heise ausnutzen, wenn ein Nutzer sich mit einem gültigen Zugang im System eingeloggt hatte. Durch Manipulation der URLs im Shop konnten dann bereits bezahlte, gültige Tickets im PDF-Format abgerufen werden. Bei Vorverkaufsdienstleistern bestellte Papiertickets sind nicht betroffen. Die Elbphilharmonie prüft derzeit nach eigenen Angaben, ob die Schwachstelle aktiv ausgenutzt wurde und Tickets heruntergeladen wurden. [...]" *Quelle: golem.de 10.1.2017*

(a) Wie konnte das (technisch) passieren? Diskutieren Sie zwei verschiedene Möglichkeiten. *(4 Punkte)*

(b) Es ist im Artikel von einem "Datenschutzproblem" die Rede. Bewerten Sie die Verwendung des Begriffs "Datenschutz" in diesem Kontext. *(2 Punkte)*

Aufgabe 7: Android-Sicherheit (7 Punkte)

(a) Skizzieren Sie, wie in Android (ab Version 4) der grundlegende Schutz vor Buffer-overflow-Exploits funktioniert. *(3 Punkte)*

(b) Warum können bei Android auf der DVM (Dalvik Virtual Machine) basierende Schutzmechanismen nicht für jede App wirken? *(2 Punkte)*

(c) Welche Angriffswege für z. B. unautorisierten Datenzugriff oder Schadcode-Ausführung sind bei Smartphones denkbar? Bitte nennen und skizzieren Sie vier Angriffswege in Stichworten. *(2 Punkte)*