Klausur
Einführung in die IT-Sicherheit

TECHNISCHE UNIVERSITÄT DARMSTADT

Sommersemester 2018 **30. Juli 2017**

Persönliche Daten (bitte vollständig in Druckbuchstaben ausfüllen)

Nachname: . . . . . Vorname: . . . . . .

Fachbereich: . . . . . Matrikelnummer: . . . . . .

Studiengang: . . . . . .

Hinweise zur Bearbeitung

- Die Bearbeitungszeit für diese Klausur beträgt *100 Minuten*.
- Es sind *keine Hilfsmittel* gestattet.
- Benutzen Sie weder *Bleistifte* noch *rot* oder *grün* schreibende Stifte.
- Schreiben Sie auf jedes Blatt rechts oben Ihren *Namen* und Ihre *Matrikelnummer*. Die Heftung darf *nicht* entfernt werden.
- Beantworten Sie die Fragen in den dafür vorgesehenen Feldern. Sollte der Platz nicht ausreichen, können Sie die Rückseiten verwenden.
- Verwenden Sie *kein eigenes Papier*. Wenn Sie zusätzliches Papier benötigen, können Sie es von der Klausuraufsicht erhalten.
- Sie dürfen Ihre Antworten auf *Deutsch* oder *Englisch* geben.
- Die Klausur besteht aus *8 Aufgaben* auf *22 Seiten*.
- Durch vollständiges Lösen aller Aufgaben können Sie maximal *48 Punkte* erhalten.

Punkteverteilung und Bewertung

Aufgabe	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	Σ	**B**	Σ	**Note**
Punkte												

1. Allgemeine Fragen

1.1. Fragenkatalog

1. Ordnen Sie den Beispielen die Begriffe Vulnerability (= Schwachstelle), Threat (= Bedrohung) und Attack (= Angriff) zu. Falls mehrere Begriffe passen wählen Sie bitten den Begriff der am besten das Beispiel klassifiziert. Beziehen Sie sich bitte nur auf die Beispiele und nicht auf Szenarien die durch die Beispiele entstehen können.

   a) Eine Anwendung benutzt veraltete Kryptographie.

   b) Hacker dringen in das Pentagon ein.

   c) In einer Anwendung lässt sich ein Buffer Overflow ausführen.

   d) Nordkoreanische Hacker sind in der Lage in Systeme einzubrechen.

2. Netzwerksicherheit

2.1. Fragenkatalog

Bitte kreuzen Sie für jede der folgenden Aussagen 'Wahr' *oder* 'Falsch' an.
Nur eine der beiden Auswahlmöglichkeiten ist richtig.
Jede korrekte Antwort gibt einen Punkt und erfordert keine weitere Begründung.

	Wahr	Falsch	
a)	☐	☐	Bei IPv6 bekommt jeder Client vom Router eine IPv6 Adresse zugewiesen
b)	☐	☐	Wenn Pakete größer als die Maximum Transmission Unit (MTU) sind müssen sie fragmentiert werden
c)	☐	☐	Beim finden von Routen im Internet wird immer der kürzeste Pfad gefunden
d)	☐	☐	Beim BGP TTL Hack wird die TTL auf 255 gesetzt, so dass ein BGP Speaker an der TTL sehen kann, ob das Paket von einem direkten Nachbarn stammt
e)	☐	☐	Ein Internet Router muss alle Layer des Internet Protocol Stack unterstützen um Pakete forwarden zu können
f)	☐	☐	IPv6 lässt sich mit jedem IPv4 Gerät ohne weiteres benutzen
g)	☐	☐	Der Internet Layer sorgt dafür, dass verlorene Pakete erneut gesendet werden
h)	☐	☐	Im Internet benutzen alle Router eines Autonomous System (AS) nur das Border Gateway Protocol für externe Verbinungen zu anderen Routern

2.2. BGP

1. BGP Angriffe können in 4 Klassen zusammen gefasst werden. Nennen Sie **zwei** und erklären diese **kurz**.

2. AS123 hat folgende Informationen von seinem benachbarten BGP Routern/AS:

Prefix	From Router	Path length
42.0.0.0/8	AS3	3
42.0.0.0/8	AS2	2
42.0.0.0/16	AS1	6
43.0.0.0/8	AS6	2
43.0.0.0/16	AS7	2
43.0.0.0/24	AS8	2
44.0.0.0/16	AS4	3
44.0.0.0/16	AS5	2

An welchen Router/AS werden folgende Pakete geschickt:

a) 42.0.0.1

b) 42.1.0.2

c) 43.0.0.3

d) 43.1.0.4

e) 44.0.0.5

3. Sie sind ein Angreifer und möchten den Datenverkehr der IP Adresse 44.4.4.4 zu sich leiten. Welches Routing Announcement schicken Sie hierfür an AS123 (siehe Tabelle):

   Prefix: _____, AS: 666, Path length: _____

2.3. IPSec

1. Nennen Sie die beiden Betriebsmodi von IPSec und erklaren Sie *kurz* deren Unterschied.

2.4. Transport Layer Security

1. Wozu dient die Session ID im Client/Server Hello und wo wird sie verwendet?

2. Erlautern Sie die Bestandteile der Ciphersuite
   `ECDHE-RSA-AES128-GCM-SHA256`.

3. Web Sicherheit

3.1. Fragenkatalog

Bitte kreuzen Sie für jede der folgenden Aussagen 'Wahr' *oder* 'Falsch' an.
Nur eine der beiden Auswahlmöglichkeiten ist richtig.
Jede korrekte Antwort gibt einen Punkt und erfordert keine weitere Begründung.

	Wahr	Falsch	
a)	☐	☐	Die Same-Origin-Policy wird vom Server umgesetzt.
b)	☐	☐	Der Angreifer kann via Cross Site Scripting (XSS) vertrauliche Daten von einem Opfer auslesen, ohne dass er Kontakt zum Opfer aufgenommen hat.
c)	☐	☐	Cookies mit HttpOnly Flag (HttpOnly: true) konnen via JavaScript (alert(document.cookie);) ausgegeben werden.
d)	☐	☐	Code injection funktioniert nur wenn SQL Datenbanken genutzt werden.

3.2. Gleiche-Herkunft-Richtlinie (Same-Origin-Policy)

Sie befinden sich auf der Seite `https://sit.tu-darmstadt.de` und wollen einige Skripte einbinden oder nachladen. Begründen Sie bei jedem nachfolgendem Punkt, ob die Same-Origin-Policy dies zulässt.

Hinweis: Eine kurze Antwort beginnend mit 'Ja' oder 'Nein' und einer kurzen Begründung ist ausreichend.

1. Ein JavaScript auf `https://sit.tu-darmstadt.de/insecure.php` versucht Inhalte von `https://abc:123@sit.tu-darmstadt.de` nachzuladen. Ist dies möglich?

2. Ein JavaScript auf `https://sit.tu-darmstadt.de/insecure.php` versucht Inhalte von `ftp://abc:123@sit.tu-darmstadt.de` nachzuladen. Ist dies möglich?

3. Ein JavaScript auf `https://sit.tu-darmstadt.de/secure.php` versucht Inhalte von `https://itsec.sit.tu-darmstadt.de` nachzuladen. Ist dies möglich?

4. Sie binden in einer HTML-Seite auf `https://sit.tu-darmstadt.de/index.html` ein externes Skript mit einem `<script>`-Tag der externen Quelle `https://www.nsa.gov/` ein. Wird das Skript geladen und ausgeführt?

3.3. Cookies

Die folgenden Cookies sind gegeben:

Name:	c1
Content:	John
Host:	www.tu-darmstadt.de
Path:	/
Expires:	end of session
Secure:	true

Name:	c2
Content:	True
Host:	www.sit.tu-darmstadt.de
Path:	/
Expires:	end of session
Secure:	true

Name:	c3
Content:	ijklmnop
Host:	tu-darmstadt.de
Path:	/
Expires:	Friday, June 29, 2018 04:00 PM
Secure:	true

Name:	c4
Content:	abcdefgh
Host:	sit.tu-darmstadt.de
Path:	/
Expires:	Tuesday, June 02, 2020 13:37 PM
Secure:	false

Geben Sie die Cookies an, die vom Browser bei der genannten Anfrage gesendet werden (Read Scope). Begründen Sie zusätzlich bitte kurz ihre Auswahl. Bitte überprüfen Sie außerdem das Ablaufdatum (Expires). Gehen Sie davon aus, dass heute der 09. Oktober 2017 ist.

1. Anfrage: `https://www.tu-darmstadt.de`
   Gesendete Cookies und Begründung:

2. Anfrage: `http://sit.tu-darmstadt.de`
   Gesendete Cookies und Begründung:

3. Anfrage: `https://www.sit.tu-darmstadt.de/`
   Gesendete Cookies und Begründung:

4. Anfrage: `http://secure.tu-darmstadt.de`
   Gesendete Cookies und Begründung:

3.4. PHP Script Analyse

In Listing 1 finden Sie eine Sicherheitslücke. Bitte nennen Sie den Angriff und formulieren Sie eine beispielhafte URL, wie er ausgeführt werden könnte. Erläutern Sie zusätzlich kurz wie er funktioniert. Geben Sie eine Möglichkeit an, wie dieser verhindert werden kann. Die Website wird zum Beispiel via `show_messages.php?tuid=ab12cdef` aufgerufen. Das gewünschte Verhalten der Website ist also, einen User anhand einer beliebigen ID zu löschen.

```
1 <?php
2 include 'guestbook.inc.php'; // guestbook_* Funktionen
3
4 $conn = mysqli_connect($servername, $username, $password);
5 mysqli_select_db($conn, 'exam');
6
7 guestbook_print_header();
8
9 // load custom css style
10 if (isset($_COOKIE['my_tuid'])) {
11   echo file_get_contents('./css/' . $_COOKIE['my_tuid']);
12 }
13
14 if (isset($_GET['tuid'])) {
15     $tuid = strtolower($_GET['tuid']); // lowercase
16     $cmd = "SELECT * FROM messages WHERE tuid='".$tuid."'";
17     mysqli_multi_query($conn, $cmd);
18     $res = mysqli_store_result($conn);
19
20     // display messages
21     while ($row = $result->fetch_row()) {
22       guestbook_print_message($row);
23     }
24 } else {
25   echo "Nutzer mit ID " . $_GET['id'] . " existiert nicht!";
26 }
27
28 guestbook_print_footer();
29 ?>
```

Listing 1: Angreifbarer PHP Code.

1. Name des Angriffs: _____

   Ausführung:

   Erläuterung und Gegenmaßnahme:

2. Name des Angriffs: _____

   Ausführung:

Erläuterung und Gegenmaßnahme:

3. Name des Angriffs: _____

   Ausführung:

   Erläuterung und Gegenmaßnahme:

4. Wireless Security & IoT

1. Nennen Sie **zwei** Angriffe die bei drahtlosen Netzwerken einfacher durchzuführen sind als bei drahtgebundenen Netzwerken und erläutern **kurz** Sie warum.

2. In der Vorlesung wurden verschiedene Typen von Jammern vorgestellt. Nennen Sie **zwei** und Beschreiben Sie diese jeweils in einem Satz.

3. Warum verwenden IoT Geräte wie z.B. Smart Lights nicht TLS?

5. Security Engineering

5.1. Fehlercode

In Listing 2 finden Sie C Programmcode. Dieser enthält mehrere kritische Fehler. Bitte nennen Sie zwei dieser Fehler (inklusive Zeilenangabe) und erläutern Sie kurz, was durch den Fehler passieren kann und wie man es beheben kann.

```
1 int main(int argc, char *argv[]) {
2   char code[10];
3
4   if (argc != 2) return 1;
5   printf(argv[1]);
6
7   strcpy(code, ”9999999999”);
8   for (int i = 0; i < 10; ++i) {
9     code[i] -= argv[1][i] % 10;
10  }
11
12  printf(”, %s\n”, code);
13
14  return 0;
15 }
```

Listing 2: C Programmcode.

5.2. Buffer Overflow

```
1 // Adresse dieser Funktion ist 0xf800f101
2 char *copy_something(char *src)
3 {
4   char dst[] = "This is just a placeholder.";
5   //kopiere von 'src' zu 'dst' 'len(src)' bytes
6   memcpy(dst,src,len(src));
7
8   return dst;
9 }
10
11 // Adresse dieser Funktion ist 0xf800f202
12 void hidden_function()
13 {
14   system("/bin/sh");
15 }
16
17 // Adresse dieser Funktion ist 0xf800f303
18 int main(int argc, char *argv[])
19 {
20   char *data = copy_something(argv[1]);
21   printf("You input: %s\n", data);
22 }
```

Listing 3: C Pseudocode.

1. Betrachten Sie den C Pseudocode in Listing 3. Er wird nach erfolgreicher Kompilierung auf einem 32bit System (x86 little-endian Architektur) ausgeführt. Wie muss das erste über die Kommandozeile übergebene Argument, also `argv[1]`, aussehen, damit die Funktion `hidden_function` durch einen Bufferoverflow aufgerufen wird. Bitte begründen Sie ihre Antwort.

2. Nennen Sie eine Gegenmaßnahme für Buffer Overflows und nennen Sie eine Methode die heute statt Buffer Overflows verwendet wird.

5.3. Secure Coding Guidelines

1. Ordnen Sie die Schritte den einzelnen Phasen im Microsoft Security Development Lifecycle zu.
   Die Phasen sind:
   1. Requirements 2. Design 3. Implementation 4. Verfication 5. Release

- Certify Release and Archive: _____
- Deprecate Unsafe Functions: _____
- Establish Design Requirements: _____
- Establish Security Requirements: _____
- Perform Dynamic Analysis: _____
- Perform Security and Privacy Risk Assessments: _____
- Perform Static Analysis: _____
- Use Approved Tools: _____

6. Security Management

6.1. Metriken für Sicherheitsmanagementsysteme

1. Erklären Sie kurz drei Anforderungen an “gute” Metriken in Sicherheitsmanagementsystemen.

2. Welchen Nutzen haben Standards zur Informationssicherheit? Sie haben drei kennengelernt. Nennen Sie zwei Nutzen und *jeweils* ein Beispiel dazu.

3. Sie haben eine 2 Faktor Authentifizierung eingeführt. Nun möchte die Geschäftsführung eine Bewertung, wie diese von den Mitarbeitern angenommen wird. Sie wollen folgende Metrik nutzen: *Zufriedenheit der Mitarbeiter mit dem 2 Faktor Authentifizierung*
   Ist die Metrik eine gute Metrik? Begründen Sie Ihre Antwort.

7. Identity, Access, Privacy und Blockchain

7.1. Fragenkatalog

Bitte kreuzen Sie für jede der folgenden Aussagen 'Wahr' *oder* 'Falsch' an.
Nur eine der beiden Auswahlmöglichkeiten ist richtig.
Jede korrekte Antwort gibt einen Punkt und erfordert keine weitere Begründung.

	Wahr	Falsch	
a)	☐	☐	Eine nicht-leere, k-anonyme Tabelle muss mindestens k voneinandern nicht unterscheidbare Datensätze enthalten.
b)	☐	☐	Eine Umwandlung einer Access Control Matrix (ACM) in Access Control Lists (ACL) ist nicht möglich.
c)	☐	☐	Blockchains lassen sich nur als Hash-Bäume (Merkle Trees) implementieren.
d)	☐	☐	Eine Blockchain kann gleichzeitig richtlinienlos (permissionless) und privat sein.

1. Weissen Sie am gegebenen Beispiel Klausureinsieht den Schritten die Begriffe Autorisierung, Identifizieren und Authentifizierung zu.

   a) "Hallo mein Name ist Klara Musterfrau"

   b) Die Studentin gibt der Aufsicht Studierendenausweis und Personalausweis, welche die Aufsicht überprüft.

   c) Die Aufsicht gibt der Studentin Ihre Klausur.

2. Wie funktioniert der *Hashcash*-Algorithmus? Wozu war er ursprünglich gedacht? Wozu wird er bei der Bitcoin-Blockchain benutzt?

8. Post-Quantum Kryptographie

1. Was ist Shor's Algorithmus und was kann damit gebrochen werden?

2. Welche Gegenmaßnahme ist bei symmetrischer Kryptographie empfohlen um PQ Angriffe zu erschweren?

3. Es gibt postquantensichere Kryptographie. Nennen Sie **vier** Ansätze.