Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikations-
systeme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM
TEAM
Munich Network Management Team

Klausur zur Vorlesung IT-Sicherheit im WS20/21

16.03.2021

Aufgabenstellung

Aufgaben

- Aufgabe 1: Multiple Choice
- Aufgabe 2: Grundlagen
- Aufgabe 3: Social Engineering und Ransomware
- Aufgabe 4: Kryptographie
- Aufgabe 5: Asymmetrische Verschlüsselung mit RSA
- Aufgabe 6: Buffer Overflows
- Aufgabe 7: Needham-Schroeder und Kerberos
- Aufgabe 8: ISO/IEC 27000

Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikations-
systeme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM
TEAM
Munich Network Management Team

Aufgabe 1:
Multiple Choice

Hinweise zu den Multiple-Choice Aufgaben

- Pro Multiple-Choice-Frage ist ***mindestens*** eine Antwort richtig.
- Pro Multiple-Choice-Frage kann also ***mehr als eine*** Antwort richtig sein.
- Kreuzen Sie ***genau alle*** richtigen Antworten an!
- Für jede ***vollständig richtig*** beantwortete Frage erhalten Sie 1 Punkt.
- Für ***nicht vollständig*** richtig, ***nicht*** oder ***falsch*** beantwortete Fragen erhalten Sie jeweils 0 Punkte.
- Es gibt ***keinen Punktabzug*** für falsch beantwortete Fragen.

Teilaufgabe 1.1 (1)

MD5 ist eine bekannte kryptographische Hashfunktion.
Welche der folgenden Aussagen dazu sind korrekt?

A	Die Länge des resultierenden Hashwertes ist im Gegensatz zu SHA-3 variabel.
B	Zu MD5 sind derzeit keine Angriffe bekannt, daher gilt es als die sicherste Hashfunktion und sollte verwendet werden.
C	Die zu hashende Nachricht wird in 512-Bit lange Eingabeblöcke aufgeteilt.
D	Es wird häufig beim Download größerer Dateien, z.B. ISO-Images eingesetzt, um prüfen zu können, ob das heruntergeladene File korrekt ist.

Teilaufgabe 1.2 (1)

Welche der folgenden Aussagen trifft auf das von Microsoft entwickelte *MS-CHAPv2* zu?

A	Das Protokoll ist im Vergleich zu Version 1 vereinfacht worden.
B	Alle in Version 1 vorhandenen Probleme wurden vollständig gelöst.
C	MS-CHAPv2 hängt weiterhin von der Wahl eines guten Benutzerpasswortes ab.
D	Ein Angreifer hat eine Möglichkeit einen Version-Fallback auf MS-CHAPv1 zu initiieren.

Teilaufgabe 1.3 (1)

Schadcode hat charakteristische Eigenschaften.
Wie unterscheidet sich ein Virus von einem Wurm?

A	Viren können sich durch Selbstverschlüsselung tarnen, Würmer nicht.
B	Ein Wurm ist zwingend auf ein Wirtssystem bzw. Interaktion mit dem Nutzer angewiesen.
C	Ein Rechner kann mit mehreren Viren infiziert sein, aber maximal mit einem Wurm.
D	Ein Wurm ist selbständig lauffähig.

Teilaufgabe 1.4 (1)

Mit welchen der folgenden Sicherheitsmaßnahmen versuchen Unternehmen, erfolgreiche Brute-Force-Angriffe auf ihre System- und Applikationszugänge zu verhindern?

A	Beschränkung der maximalen Loginversuche je Nutzer je Zeiteinheit.
B	Intrusion Detection Systeme.
C	Multi-Faktor-Systeme, z.B. RSA Token, Yubikeys, ...
D	Mandatory Access Control Lists.

Teilaufgabe 1.5 (1)

Der Schutz personenbezogener Daten und damit die Einhaltung der geltenden Rechtsvorschriften ist für Organisationen wichtig.
Die Datenschutzgrundverordnung (DSGVO) folgt hierbei gewissen Grundprinzipien.

A	Personenbezogene Daten dürfen ausschließlich dann erhoben werden, wenn der Nutzer seine Zustimmung dazu erteilt hat.
B	Der behördliche Datenschutzbeauftragte besitzt ein Veto-Recht, d.h. dieser darf die Verarbeitung personenbezogener Daten untersagen.
C	Die Daten dürfen nur zu bestimmten Zwecken verarbeitet werden.
D	Organisationen dürfen alle Netz- und Nutzeraktivitäten aufzeichnen und diese Protokolle beliebig lange aufbewahren und auswerten.

Teilaufgabe 1.6 (1)

Die Displaysperre mobiler Geräte, wie z.B. bei Smartphones kann mithilfe eines Fingerabdrucks sehr einfach aufgehoben werden. Häufig kommen dabei optische Sensoren zum Einsatz, weil ...

A	... sich diese nicht mit einem Gummi-Finger überlisten lassen.
B	... deren Akzeptanzrate bei 100% liegt.
C	... sie günstiger sind als kapazitative oder Ultraschallsensoren.
D	... sie unterhalb des Displays verbaut werden können.

Teilaufgabe 1.7 (1)

Welche der folgenden Aussagen über Fuzzing und dessen Anwendung ist korrekt?

A	Wird in WEP verwendet, um den verschlüsselten Bitstrom zu berechnen.
B	Es bezeichnet keinen speziellen Angriffstyp, der auf den Diebstahl von Zugangsdaten abzielt.
C	Ist ein bekanntes Verfahren, um die Passwortsicherheit zu erhöhen.
D	Automatisiertes Eingeben von Zufallswerten, z.B. zum Auffinden von Buffer Overflows

Teilaufgabe 1.8 (1)

Bei der Absicherung von WLANs galt einige Zeit das *Wired Equivalent Privacy* (WEP) als sicher.

Welche der folgenden Aussagen treffen auf dieses Verfahren **nicht** zu?

A	Der Initialisierungsvektor ist immer 64 Bits lang.
B	Nachricht M konkateniert mit CRC(M) wird mit dem Bitstrom XOR-verknüpft.
C	Zur Erzeugung des Bitstroms kommt alternativ DES oder AES zum Einsatz.
D	Bei dem zur Integritätssicherung eingesetzten Cyclic Redundancy Check (CRC) handelt es sich nicht um ein kryptographisches Hashverfahren.

Teilaufgabe 1.9 (1)

Welche der folgenden Ziele der Informationssicherheit können Sie erreichen, wenn Sie kryptographische Verfahren anwenden?

A	Vertraulichkeit
B	Authentizität
C	Verfügbarkeit
D	Integrität

Teilaufgabe 1.10 (1)

Welche Aussagen über das Common Vulnerability Scoring System 3 (CVSSv3) sind korrekt?

A	Man unterscheidet Base, Temporal und Environmental Metrics.
B	Der Base Score wird unabhängig von der Komplexität zur Ausnutzung einer Sicherheitslücke errechnet.
C	Die Auswirkung einer erfolgreichen Ausnutzung einer Sicherheitslücke bezieht sich immer nur auf die Verfügbarkeit eines IT-Systems.
D	Mithilfe der Temporal Metrics kann abgeschätzt werden, ob die Lücke nur theoretisch oder schlimmstenfalls bereits durch einen funktionsfähigen Exploit ausgenutzt wird.

Teilaufgabe 1.11 (1)

Was sind charakteristische Eigenschaften des SYN-Flooding-Angriffs?

A	Der Angreifer scannt mit gespoofter Quell-IP-Adresse nach Servern, die bei ihrer Antwort zu viele SYN-Flags im IP-Header setzen.
B	Der Angreifer verändert den Hashwert von SYN-Cookies und schickt diese wiederholt zum Zielsystem.
C	Der Angreifer baut X-SYN-Header in HTTP-Anfragen ein, um falsch konfigurierte Webserver zu überlasten.
D	Der Angreifer baut so viele sog. halb-offene Verbindungen zum Zielsystem auf, bis dessen Ressourcen erschöpft sind.

Teilaufgabe 1.12 (1)

Angriffe auf IT-Systeme lassen sich auf unterschiedliche Art und Weise kategorisieren. Welche der folgenden Aussagen sind korrekt?

A	Neben aktiven Angriffen gibt es auch passive.
B	Angriffe lassen sich mithilfe eines Angreifermodells, wie z.B. dem MOM-Prinzips (Motivation - Opportunity - Means) beschreiben.
C	Bei Angriffen sollten sich Unternehmen allein auf die externen beschränken. Interne Angriffe gibt es nicht.
D	Angriffe zielen immer nur auf die Ziele Vertraulichkeit und Verfügbarkeit ab.

Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

Aufgabe 2: Grundlagen

Teilaufgabe 2.1 (3)

Offene DNS-Resolver sind IT-Serversysteme, die für so genannte *Amplification Attacks* anfällig sind.

Erläutern Sie kurz und in Stichpunkten **drei** Grundprinzipien dieses Angriffstyps!

Teilaufgabe 2.2 (2)

Geben Sie, bezogen auf den DNS-Amplification-Angriff aus Teilaufgabe 2.1, **zwei Möglichkeiten** an, wie Unternehmen ihre Server effektiv vor solchen Angriffen schützen bzw. diese abwehren können.

Teilaufgabe 2.3 (4)

Sicherheitsmaßnahmen lassen sich in unterschiedliche Kategorien einordnen, z.B. werden einerseits *technische* und *organisatorische* Maßnahmen unterschieden, andererseits *präventive, detektierende* und *reaktive* Maßnahmen.

Ordnen Sie die folgenden Maßnahmen in diese Kategorien, z.B. Maßnahme M-*X* gehört zur Kategorie *organisatorisch-präventiv*.

- M-*A* Firewall oder Access Control Listen
- M-*B* Verfahren zur Handhabung von Sicherheitsvorfällen
- M-*C* Datensicherung (Backup)
- M-*D* Logging-Richtlinie

Teilaufgabe 2.4 (2)

Cross-Site-Scripting (XSS) nutzen Angreifer z.B. um einzelne Nachrichten oder ganze Webseiten zu verändern (Defacement).

Worauf könnte ein Angreifer noch abzielen?

Nennen Sie zwei Beispiele.

Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikations-
systeme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM
TEAM
MUNICH NETWORK MANAGEMENT TEAM

Aufgabe 3:
Social Engineering und Ransomware

Teilaufgabe 3.1 (2)

Nennen Sie zwei Beispiele für menschliche Eigenschaften, die ein Social Engineer im Rahmen eines *human-based Social Engineering* Angriffs ausnutzen könnte!

Teilaufgabe 3.2 (3)

Erläutern Sie den Unterschied zwischen *human-based* und *computer-based Social Engineering*?

Nennen Sie jeweils zwei Beispiele.

Teilaufgabe 3.3 (2)

Beschreiben Sie *Reverse Social Engineering.*

Geben Sie hierfür ein Beispielszenario an.

Teilaufgabe 3.4 (2)

Sie möchten per Phishing-E-Mail eine möglichst erfolgreiche Ransomware-Attacke auf ein Unternehmen starten.

Welche Art von Phishing-Angriff verwenden Sie dafür und **warum**?

Teilaufgabe 3.5 (3)

Angenommen ihre Attacke aus Teilaufgabe 3.4 verlief tatsächlich an einer Stelle erfolgreich.

Beschreiben Sie, wie sich aktuelle Ransomware in einem Unternehmen weiter verbreitet.

Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

Aufgabe 4:
Kryptographie

Teilaufgabe 4.1 (2)

Einfache, kryptographische Verfahren nutzen auch einfache Operationen.

Nennen Sie zwei Eigenschaften wodurch sich eine *Permutation* von einer *Substitution* unterscheidet.

Teilaufgabe 4.2 (3)

Steganographie ist eine einfache Möglichkeit zur Übertragung geheimer Nachrichten an einen Empfänger.

Erläutern Sie knapp, wie *Steganographie* funktioniert.

Nennen Sie mindestens eine Voraussetzung, die Sie für einen erfolgreichen Angriff benötigen und **beschreiben Sie wie** ein solcher Angriff aussehen könnte?

Teilaufgabe 4.3 (4)

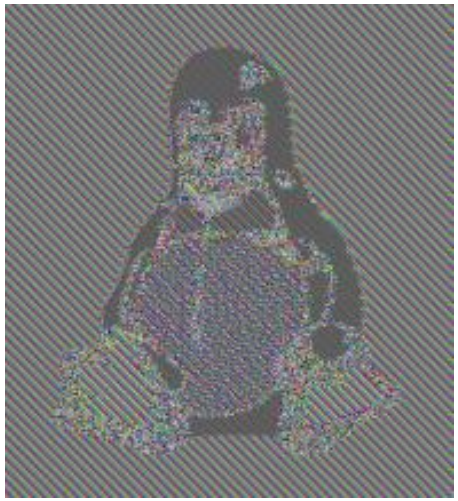
Bei Blockchiffren haben Sie in der Vorlesung zwei Betriebsmodi kennengelernt.

Mit welchem Modus wurde das **Bild auf der folgenden Seite** verschlüsselt?

Geben Sie kurz die Unterschiede beider Modi an und **beschreiben Sie**, wie das Bild aussehen würde, wenn es mit dem anderem Modus verschlüsselt worden wäre.

Teilaufgabe 4.3

Original: 

Verschlüsselt: 

Teilaufgabe 4.4 (2)

Bei dem Verschlüsselungsverfahren *DES* existieren **4 schwache** und **6 semi-schwache** Schlüssel.

Skizzieren Sie, was passiert, wenn man einen **schwachen** Schlüssel benutzt?

Teilaufgabe 4.5 (2)

Der Algorithmus *AES* gilt als Nachfolger für den inzwischen als unzureichend sicher angesehenen DES-Algorithmus.

Handelt es sich bei AES, ebenso wie bei DES, um eine so genannte **Feistel-Chiffre**?

Begründen Sie ihre Antwort.

Teilaufgabe 4.6 (2)

In der Verschlüsselung mit *AES* wird auf jeden Block der so genannte *SpaltenMix* (*MixColumns*) angewendet.

Welche mathematische Operation wird hierfür verwendet?

Wie sieht diese Operation bei der Entschlüsselung eines Chiffreblocks aus?

Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikations-
systeme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM
TEAM
Munich Network Management Team

Aufgabe 5:
Asymmetrische Verschlüsselung mit RSA

Teilaufgabe 5.1 (2)

Nennen Sie einen Vorteil und **einen Nachteil**, den ein asymmetrisches Verschlüsselungsverfahren gegenüber einem symmetrischen Verfahren hat.

Teilaufgabe 5.2 (2)

Gegeben sind die Primzahlen $p = 11$ und $q = 3$, sowie die ganzzahlige Klartextnachricht $m = 4$.

Verschlüsseln Sie die Nachricht m mit dem RSA-Verfahren.
Benutzen Sie hierzu den *Verschlüsselungsexponenten* $e = 3$.

Geben Sie den Wert der chiffrierten Nachricht an.

(*Hinweis: Achten Sie darauf, dass ihr Rechenweg nachvollziehbar ist.*)

Teilaufgabe 5.3 (4)

Berechnen Sie nun den zu Teilaufgabe 5.2 gehörenden Entschlüsselungsexponenten *d*.

Geben Sie abschließend die Entschlüsselungsvorschrift an, die Sie nun auf den in Teilaufgabe 5.2 berechneten Chiffretext anwenden müssten, um diesen zu entschlüsseln.

(*Hinweis: Ausrechnen der Entschlüsselungsvorschrift nicht notwendig!*)

Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

Aufgabe 6: Buffer Overflows

Teilaufgabe 6.1 (2)

Erläutern Sie knapp, wie ein Pufferüberlauf generell zustande kommt und **welches Ziel** ein Angreifer bei einem Stack-Smashing-Buffer-Overflow-Angriff verfolgt.

Teilaufgabe 6.2 (3)

Sie möchten einen Buffer Overflow Exploit schreiben.

Leider verwendet die CPU des Opfers das *NX-Bit* und auch im installierten Betriebssystem ist diese Funktion aktiviert.

Erläutern Sie kurz, **was** dadurch verhindert wird.

Nennen und erläutern Sie einen Angriff bzw. eine Methode, wie Sie das NX-Bit umgehen können.

Teilaufgabe 6.3 (3)

Sie haben sich aus einer Exploit-Datenbank einen Exploit-Code heruntergeladen. Darin befinden sich folgende Instruktionen:

```
...
NOP
NOP
NOP
NOP
NOP
NOP
MOV AH, 1 int 21
...
```

Erläutern Sie, warum ein Angreifer diese NOP-Instruktionen verwenden sollte und **was** die CPU ausführen wird?

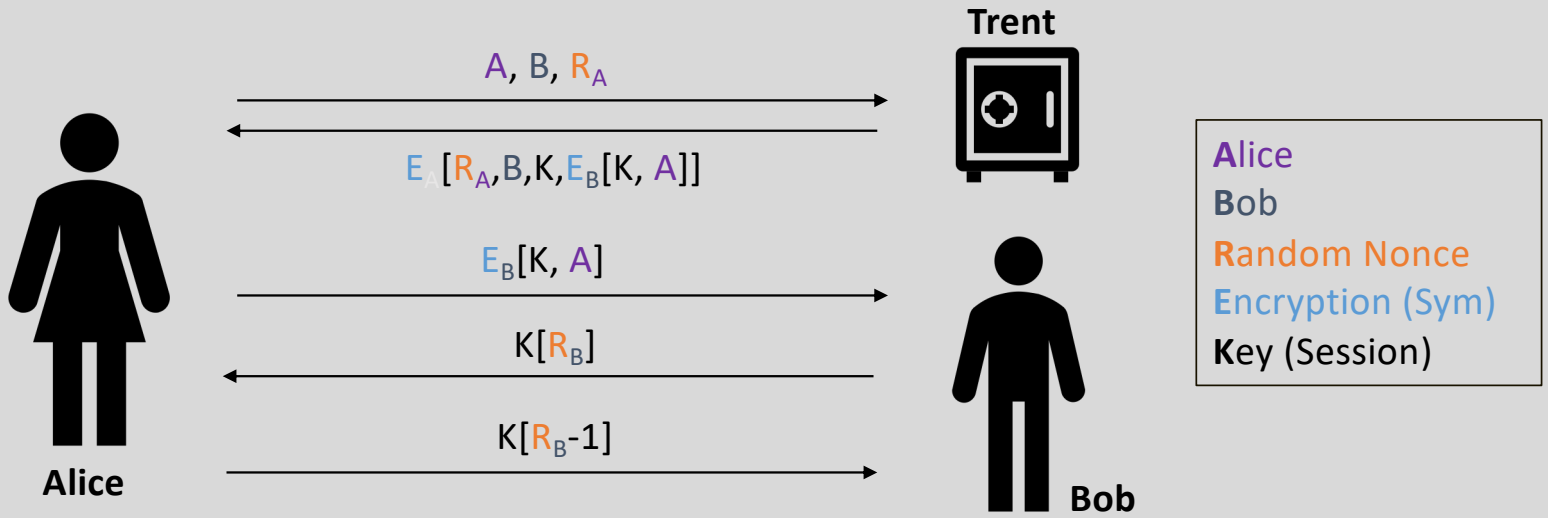
Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikations-
systeme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM
TEAM
Munich Network Management Team

Aufgabe 7: Needham-Schroeder und Kerberos

Needham-Schroeder Protokoll

Needham-Schroeder ist ein einfaches Authentifizierungsprotokoll, das sowohl symmetrisch als auch asymmetrisch implementiert werden kann. Unten sehen sie die symmetrische Version aus der Vorlesung, mit Alice, Bob und der vertrauenswürdigen Instanz Trent. → **Aufgabe nä. Seite.**



Teilaufgabe 7.1 (3)

Das Needham-Schroeder-Protokoll beginnt also mit einer Kommunikation zwischen Alice und Trent.

Mallory versucht nun an dieser Stelle einen Replay-Angriff mit kompromittiertem *Session key M* durchzuführen.

Skizzieren Sie den Aufbau eines solchen Angriffs.

Ist dieser, wie in der Abbildung (*Seite vorher!*) dargestellt, erfolgreich? **Begründen Sie**, warum oder warum nicht?

Teilaufgabe 7.2 (3)

In der asymmetrischen Variante von Needham-Schroeder wird die Antwort von Trent jeweils verschlüsselt verschickt.

Geben Sie an, wer diese Nachricht entschlüsseln kann **und ob der Verlust der Vertraulichkeit** dieser Nachricht ein Sicherheitsproblem darstellt?

Teilaufgabe 7.3 (2)

Bei Kerberos wird zwischen *Ticket* und *Authenticator* unterschieden. Das Ticket ist mit einem symmetrischen Schlüssel verschlüsselt und beweist damit, dass es wirklich vom Server stammt.

Geben Sie an, welche Entität den *Authenticator* erstellt und **was** der *Authenticator* verhindert.

Teilaufgabe 7.4 (2)

Erläutern Sie, wie der *Authenticator* im Kerberos-Protokoll verwendet wird.

Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikations-
systeme und Systemprogrammierung
Prof. Dr. Helmut Reiser

MNM
TEAM
MUNICH NETWORK MANAGEMENT TEAM

Aufgabe 8: ISO/IEC 27000

Teilaufgabe 8.1 (4)

Zentraler Prozess innerhalb von ISO/IEC 27000 ist das *Informationssicherheitsrisikomanagement*.

Beschreiben Sie kurz den grundsätzlichen Ablauf der *Risikobeurteilung* und gehen dabei insbesondere auf die Schritte *Risikoanalyse* und *Risikobewertung* ein.

Teilaufgabe 8.2 (3)

In der Nomenklatur der ISO/IEC 27000 ist die zweite Phase des Risikomanagementprozesses die *Risikobehandlung*.

Nennen und erläutern Sie mindestens drei sinnvolle Behandlungsoptionen.

Teilaufgabe 8.3 (1)

In welchem für ISO/IEC 27000 zentralen **Dokument** werden diese Behandlungsoptionen beschrieben?

Teilaufgabe 8.4 (2)

Erläutern Sie den Begriff *Restrisiko*.

Welche Aufgabe hat der *Risikoeigentümer* bezüglich dieser Restrisiken?

Teilaufgabe 8.5 (4)

Ein ISO/IEC 27000 zugrunde liegendes Konzept ist das der *kontinuierlichen Verbesserung*.

Dazu fordert der Standard, dass Organisationen die *Leistung* bzw. die *Wirksamkeit des ISMS* messen müssen.

Nennen und erläutern Sie zwei Möglichkeiten, wie das in der Praxis umgesetzt werden kann.

Ende der Aufgabenstellung