|  |
| --- |
|  |
| Übung für Grundlagen der IT-Sicherheit |
|  |

|  |
| --- |
| Yukun,Chen Cheng,Du Yixin,Peng Yajie,Qi  2018-10-29 |

1. **Grundlegende Begriffe**
2. **Benennen Sie den Unterschied zwischen Safety und Security. Geben Sie für beides jeweils zwei Beispiele aus dem IT-Bereich.**

（改）

A:Safety bezieht sich meist auf die Funktionssicherheit und Ausfallsicherheit von Systemen.

z.B.

1.periodisch erneuern die Datenbank gegen des Zusammenbruch von Daten

2.Windows/Linux-System update

Security ist Angriffssicherheit, also der Schutz vor beabsichtigten Angriffen.

Z.B. Schutzmassnahmen gegen Auslesen von Daten von Laptops.

Schutzmassnahmen gegen Überwachung von Laptops.

1. **Benennen Sie jeweils ein Gefährdungsbeispiel mit Begründung, das nicht unter den Begriff Security bzw. Safety fällt.**

A:Gefährdungsbeispiel fällt nicht unter den Security: Höhe Gewalt (z.B. Hochwasser, Blitzeinschlag, globaler Stromausfall).

Gründung: Höhe Gewalt ist zufällig und gehört nicht zu den angriffen.

Gefährdungsbeispiel fällt nicht unter den Safety: Fahrlässigkeit (z.B. Nichtbeachtung von Sicherheitsmassnahmen, ungeeigneter Umgang mit Passwörtern).

Gründung: Der größe Teil der Fahrlässigkeit ist auf Fehler von Menschen. Es ist kein Ausfall von Systemen.

1. **Erläutern Sie die Begriffe IT-Sicherheit und Informationssicherheit**

（改）

A: Informationssicherheit:

Informationssicherheit umfasst im Gegensatz zur IT Sicherheit auch nicht-technische Systeme.Die Informationssicherheit ist immer relativ zu einem bestimmten Schutzziel,z.B [Vertraulichkeit](https://de.wikipedia.org/wiki/Vertraulichkeit" \o "Vertraulichkeit), [Verfügbarkeit](https://de.wikipedia.org/wiki/Verf%C3%BCgbarkeit" \o "Verfügbarkeit) und [Integrität](https://de.wikipedia.org/wiki/Integrit%C3%A4t_(Informationssicherheit)" \o "Integrität (Informationssicherheit))zu verstehen , das man erreichen möchte.Informationssicherheit dient dem Schutz vor [Gefahren](https://de.wikipedia.org/wiki/Gefahr" \o "Gefahr) bzw. [Bedrohungen](https://de.wikipedia.org/wiki/Bedrohung" \o "Bedrohung), der Vermeidung von wirtschaftlichen [Schäden](https://de.wikipedia.org/wiki/Schaden" \o "Schaden) und der Minimierung von [Risiken](https://de.wikipedia.org/wiki/Risiko" \o "Risiko).

IT-Sicherheit:

Die IT-Sicherheit befasst sich andererseits mit dem Schutz der elektronischen IT-Sicherheit Informationen und bildet somit ein Teilgebiet der Informationssicherheit. Auch hier gilt, dass IT-Sicherheit stets relativ zu den relevanten Schutzzielen zu verstehen ist

1. **Grenzen Sie die Begriffe Schwachstelle, Bedrohung und Risiko voneinander ab. Erläutern Sie, was sich hinter den ersten fünf Sicherheitsaspekten aus der Vorlesung verbirgt. Worin unterscheiden sich insbesondere die Sicherheitsaspekte Integrität und Authentizität?**

A:Schwachstelle: Eine Systemeigenschaft, die Missbrauchsmöglichkeiten bietet.

Bedrohung: Jedes mögliche Vorkommen (böswillig oder anderweitig) mit ungewünschten Effekten auf die Werte (Assets) und Ressourcen eines Computersystems.

Risiko: Produkt aus Schadenshöhe und Eintrittswahrscheinlichkeit eines Ereignisses (aus Bedrohungszenario).

Fünf Sicherheitsaspekten:

Authentizität: Der Sender einer Nachricht ist derjenige der er vorgibt zu sein.

Integrität: Der Inhalt einer Nachricht ist derjenige, den der Emittent tatsächlich verschickt hat.

Vertraulichkeit: Der Inhalt einer Nachricht bleibt vor dritten verborgen, also nicht semantisch erkennbar.

Verbindlichkeit: Das versenden einer Nachricht oder die Durchführung einer Aktion kann nachgewiesen werden.

Verfügbarkeit: Erreichbarkeit und Nutzbarkeit von Informationssystemen.

Die Unterschiede zwischen Authentität und Integrität:

Authentität muss den Sender der Nachricht sichern.

Die Indentität des Senders und der Sender der Nachricht muss gleich sein.

Integrität muss den Inhalt der Nachricht nicht geändert sein.

Authentität sichert die Indentität

und Integrität sichert den Inhalt.

1. **Was besagt das Recht auf informationelle Selbstbestimmung und in welchem Kontext ist es relevant? Geben Sie dafür ein Beispiel. Worauf fußt das Bundesdatenschutzgesetz. Beschreiben Sie ganz kurz was damit geschützt werden soll?**

A:Informationelle Selbstbestimmung besagt dass der Einzelne die Möglichkeit haben soll, selbst zu bestimmen, wer bei welcher Gelegenheit welche Informationen über ihn erhält.

Rechtlicher Ausgangspunkt ist das Grundrecht auf informationelle Selbstbestimmung. Es ist relevant im Datenschutzgesetz.（Beispielsweise：Datenschutzgesetze der Bundesländer, Bundesdatenschutzgesetz, Teledienstedatenschutzgesetz, Telekommunikationsgesetz.）

Ein Beispiel für die Informationelle Selbstbestimmung:

Wenn ein man im Google Play Store ein APP herunterladet, wird er gefragt, welche Berechtigung verfügbar sind bzw. man bestimmt selbst, welche Informationen verfügbar sind.(?)

Grundpfeiler des Bundesdatenschutzgesetzes sind die Prinzipien:

Datenvermeidung und Datensparsamkeit

Bei der Datenverarbeitung dürfen nur so viele personenbezogene Daten gesammelt werden, wie für die jeweilige Anwendung unbedingt notwendig sind.

Das allgemeine Verbot der Verarbeitung personenbezogener Daten

Grundsätzlich dürfen personenbezogene Daten nur mit Einwilligung der Betroffenen oder aufgrund gesetzlicher Gestattung verarbeitet werden.

1. **Erläutern Sie mit eigenen Worten die Begriffe Authentifizierung, Verifikation, Identifikation und Autorisierung und erläutern Sie den Zusammenhang zwischen den Begriffen. (Alternativ: geben Sie Definitionen für die Begriffe.) Was ist der Unterschied zwischen einer Identifikation und einer Verifikation?**

A:Authentifizierung: Der Nachweis wird der behaupteten Identität durch ein Subjekt verstanden.

（改）Verifikation: ist der [Nachweis](https://de.wikipedia.org/wiki/Richtigkeit" \o "Richtigkeit), dass ein vermuteter oder behaupteter Sachverhalt [wahr](https://de.wikipedia.org/wiki/Wahrheit" \o "Wahrheit) ist.

Identifikation:Allgemeine und umfassende Bezeichnung für eine Phase des Wiedererkennens im Verlauf des Erinnerns.

Autorisierung: Die erfolgreiche Zuweisung solcher Rechte zu Identitäten bezeichnet man als Autorisierung.

Verifikation: ein Subjekt muss eine Identität entsprechen. einen 1:1-Vergleich.

(z.B. Passbild mit Person).

Identifikation: ein Subjekt kann im Bereich entsprechen. einen 1:n-Vergleich.( Person mit allen Bildern in einer DB)

（Alternativ：）Zusammenhang: Authentifizierung und Autorisierung. Zuerst macht man die Authentifizierung, um die Identität zu sichern. Dann macht man die Autorisierung, um die Rechte zu sichern.

1. **Identity Management**
2. **Was sind die Aufgaben des Identity Managements?**

A: Das Identity Management umfasst folgende Aufgaben:

1.die Repräsentation von Personen oder Objekten (allgemeiner: Entitäten) in einem System,

2.die Prüfung, ob eine Entität auch genau jene ist, für die sie sich ausgibt,

3.die Prüfung, welche Rechte mit dieser Person (Entität) verknüpft sind.

1. **Erklären Sie den allgemeinen Prozess der Benutzerauthentifizierung.**

Authentisiert sich am

Server

Benutzer

Authentifiziert den

（改）Zuerst muss der Benutzer dem Server den Antrag aufgeben,dann bekommt er die Antwort von Server,dazwischen wird die Indentität des Benutzers authentifiziert.

1. **Auf welche Arten von Referenzdaten kann eine Authentifizierung basieren? Nennen Sie jeweils Beispiele für jede dieser Arten.**

A:

Passwort.

Beispiel: UNIX/Linux: /etc/passwd und /etc/shadow.

Wissen.

Beispiel: Authentifikation eines Subjekts gegenüber einer Instanz.

Besitz:

Beispiel:Smartcard

1. **Zu welcher Authentifizierungsart gehört die Unterschrift bei einer EC-Karte.**

A: Die Unterschrift bei einer EC-Karte gehört zu Authentifikation durch Merkmal.

1. **Geben Sie ein Beispiel mit Begründung für eine statische und eine dynamische Modalität.**

A: Statische Modalität: Fingerabdruck. Fingerabdruck wird im Übergang der Authentifizierung nicht geändert.

（改） Dynamische Modalität: Unterschrift. Die Unterschrift kann nicht immer gleich, weil die Handschrift wegen des verschiedenen Kugelscheiber oder Kraft von Scheiben geändert wird .

1. **Erläutern Sie an Hand eines Beispiels warum die Eigenschaften second preiamge resistance und collsion resistance für Password Hashing von Bedeutung sind.**

（待补充）

1. **Ist folgendes Bildungsgesetz eine gute Wahl für die Bildung von Passwörtern: 7 Zeichen aus [A-Z1-7!]. Begründen Sie Ihre Antwort mathematisch.**

A: 34^7≈2^36 Die Entropie ist 36. Beim einem Brute-Force-Angriff ist die äußere Average-Case Komplexität 2^35. Mit diesem Cracker sind ca. 2^44 Bitoperationen in der Sekunde möglich. 2^-9 Sekunden kann ein Cracker korrekte Passwort bekommen.

1. **Wie würden Sie ein Bildungsgesetz für Passwörter formulieren? Welche Maßnahmen würden Sie serverseitig ergreifen?**

(改)

Der Passwort/Schlüsselraumes muss größ sein. Je länger das Passwort, desto besser die Sicherheit.Es wäre besser,dass man die Passwörter mit mindesten 10 Zeichen von [A-Za-z0-9],weil die Entropie jetzt 54 ist,d.h der Hacker braucht am Mindestens 2048 Stunden,nämlich 85 Tage,die Passwörter zu bekommen.

Serverseitig benutze ich die Hash Funktion,um Passwort zu verschlüsselung. Beim Speicher vergröße ich die Dauer der Vorberechnung und Speicherbedarf von Time-Memory-Offs.

1. **Kerberos**
2. **Erläutern Sie den Begriff Single-Sign-On.**

(改)

A: Benutzer wird sich nur einmal (zentral) authentifiziert ,statt er die Authentifikation bei einzelnen Dienstnutzungen(Server) verlangt zu werden.

1. **Was ist der Unterschied zwischen symmetrischer und asymmetrischer Verschlüsselung? Worauf basiert Kerberos?**

A:

In der symmetrischen Verschlüsselung benutzen Sender und Empfänger beiden denselben Schlüssel.

In der asymmetrischen Verschlüsselung besteht Schlüssel aus einem privaten und einem öffentlichen Teil.

Kerberos basiert auf symmetrische Verschlüsselung.

1. **Wie erhält ein Benutzer das gemeinsame Geheimnis?**

A: Benutzer loggt sich mit Passwort auf lokalem Rechner ein. Dann fragt am AS(Authentifikation Server). AS extrahiert Benutzer-Master-Key aus seiner Datenbank.（待补充）

1. **Welche Folgen hat es für die Verfügbarkeit einer IT-Infrastruktur, wenn in einer KerberosUmgebung:**

**i. Der Authentication Server ausfällt  
ii. Der Ticket-Granting Server ausfällt  
iii. Ein Server eines Dienstes ausfällt  
Hinweis: Überlegen Sie zunächst welche Prozesse von den jeweiligen Ausfällen betroffen sind und welche nicht.**

A: i. Man kann kein Ticket für den Ticket Granting Service bekommen.(忘了，但好像不是这样写的)

(改) ii. Man kann kein neues Ticket für den Server bekommen, aber er kann das authentifizierte Server besuchen,

iii.Man kann Ticket von den Ticket Granting Service bekommen.nur kann man das ausfallende Server nicht mehr besuchen.