technische universität
dortmund

Einrichtung /
Fakultät

Sicherheit: Fragen und Lösungsansätze Übung 2

Thomas Ruhroth | Dortmund
13.Nov 2012

Übung 2

- Hinweise
- Gruppenübung
- ~~Besprechung der Abgaben~~

- Ziele:
  - Verschiedene Wissensblöcke in Prüfungen
  - Wissen für den Block 1
  - Vertiefen der Grundbegriffe

Nächste Woche gibt es eine zusätzliche Übung.

Hinweise zu Abgaben

- Aufgaben sollen vollständig beantwortet werden
- Stellen Sie die Lösung präzise und kurz dar
- Keine Email-Abgabe
- Nicht nur die Gesetze hinschreiben
- Schreiben Sie nicht mehr Infos als nötig in die Lösungen
- Seien Sie eindeutig

Wissensblöcke in Prüfungen

„Über dem Strich“

„Unterm dem Strich“

Übertragen auf andere Probleme

Anwenden und Durchführen

Basis-Wissen: Grundbegriffe, Definitionen und Techniken

Aus dem Modulhandbuch: Kompetenzen

Die Studierenden sollen die Fragen zur Sicherheit umfassend verstehen und gängige Lösungsansätze mitsamt der Nachweise ihrer Wirksamkeit kennen und anwenden können.
Darüber hinaus sollen sie weitergehende Lösungsvorschläge im Hinblick auf die Sicherheitseigenschaften eigenständig untersuchen und bewerten können.

Basis-Wissen: Grundbegriffe, Definitionen und Techniken

Anwenden und Durchführen

Übertragen auf andere Probleme
Hier:
Analyse und Bewertung

Basis-Wissen: Grundbegriffe, Definitionen und Techniken

- Sie sollten alle Basis-Begriffe definieren und einordnen können.
  - Meist finden sich 80% der Begriffe in den ersten 20% der Vorlesung
- Sie sollten die Algorithmen und Techniken die in der Vorlesung vorgestellt werden kennen und beschreiben können.
  - Anwenden ist eine Aufgabe der Stufe 2 :-)

- Antworten Sie knackig.
- Nur Übersetzen reicht nicht (wird keine Punkte geben)!
- Finden Sie den wesentlichen Punkt.

Beispiel

- Cryptography:
  - Verschleiern des Inhaltes eines Geheimnisses durch Codierung in eine Form, so dass der Angreifer nur unter unverhältnismäßig großen Aufwand das Geheimnis erfahren kann aber durch ein Zusatzwissen (z.B. Schlüssel) schnell wieder hergestellt werden kann.
- Schlechte Beispiele:
  - Verschlüsselung (0 Punkte, nur Übersetzung)
  - Verstecken eines Geheimnisses (0 Punkte, da nicht charakteristisch für Verschlüsselung – Steganographie)

Test!

Bitte legen Sie alle inhaltlichen Materialien weg!

Drehen Sie den Zettel erst um wenn ich Sie auffordere.

Wenn die Zeit abgelaufen ist, hören Sie sofort mit dem Schreiben auf und halten den Zettel nach oben.

Die Zeit läuft

Auswertung

- Geben Sie Ihren Test ihren Nachbarn
- Prüfen Sie:
  - Ist die Schrift gut lesbar?
  - Verstehen Sie die Antwort?
  - Enthält die Antwort eine Charakterisierung?
  - Ist die Charakterisierung richtig und vollständig?
  - Ist die Einordnung eindeutig gekennzeichnet?
  - Ist die Einordnung richtig?
- Wie viele Punkte würde Sie geben?

Basis-Wissen: Grundbegriffe, Definitionen und Techniken

Wenn Sie Probleme bei der Aufgabe hatten:

- Lernen und Üben! Jetzt!
- Erstellen Sie ein(e) Glossar/Liste/Karteikartensammlung/...
- Üben Sie in Paaren oder Gruppen
  - Verstehen die die Antworten des Anderen ohne weitere Erklärungen?

Caesar-Verschlüsselung

```
Klar:    a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheim:  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

$$encrypt_{K(P)} = (P + K) \bmod 26$$

$$decrypt_{K(P)} = (P - K) \bmod 26$$

- Vergleich mit Randomzeichenfolgen....
- Hat der Angreifer eine bessere Chance als raten?