Master Praktische Informatik: Modulprüfung **Sicherheit - Safety & Security 01867 & 21811**
Gedächtnisprotokoll aus 2017

Prüfer: Prof. Dr. Keller
Dauer: ca. 25 Minuten
Note: 1.0

Allgemein
Herr Prof. Dr. Keller gestaltet die Prüfung eher wie ein Gespräch. D. h. die Fragen bauen aufeinander auf, was insgesamt sehr angenehm ist, da man so nie lange überlegen muss, auf was Herr Prof. Keller hinaus möchte. Prof. Keller bezieht sich während der Prüfung auch immer wieder auf Beispiele aus dem Kurs, was ebenfalls sehr angenehm ist. Teilweise bin ich bei den Antworten etwas vom Skript abgewichen (bspw.: „Wie könnten Sie an mein Passwort kommen?“ => Social Engineering), was nach meinem Empfinden gut ankam, aber sich zumindest nicht negativ auf die Note ausgewirkt hat. Ich hatte allerdings manchmal Probleme im Gesicht von Herrn Prof. Keller zu lesen, ob er mit meiner Antwort (bereits) zufrieden ist, oder ob er noch mehr erwartet. Insgesamt ist es wichtig die Materie und alle Zusammenhänge verstanden zu haben, und diese auch auf reale Situationen übertragen zu können. Begonnen hat die Prüfung mit dem Kurs 1867. Die Fragen sind sicherlich nicht vollständig.

Fragen 1867
Wie können Passwörter mit Brutforce geknackt werden?
In einer Welt, in der jeder zufällige Passwörter verwendet, und es nur absolut sichere Algorithmen/Systeme gibt, ist Brutforce unschlagbar. Leider leben wir nicht in einer solchen Welt.
Wie würden Sie vorgehen, wenn Sie mein Passwort herausfinden wollen würden?
Wenn Sie das Passwort von einem Nutzer für einen relativ unwichtigen Dienst haben, nutzt Ihnen das etwas, um auch auf weitere Dienste des Nutzers zuzugreifen?
Warum verwenden Nutzer für viele Dienste ähnliche/identische Passwörter?
So, nun haben Sie mein Passwort und melden sich damit an. Woher könnte ein IDS trotzdem erkennen, dass es sich bei Ihnen nicht um mich handelt?
Das IDS hat nun erkannt, dass es sich um einen Angreifer handeln könnte. Was sollte als nächstes geschehen?
Der Angriff konnte somit erfolgreich abgebrochen werden. Aber wie könnte man nun feststellen, ob etwas am PC/der Konfiguration geändert wurde, bevor der Angriff abgebrochen werden konnte?
Was hindert den Angreifer daran, das Host-Based IDS auf dem angegriffenen System zu manipulieren?

Fragen 21811
Wie ist denn die stationäre Unverfügbarkeit definiert?
Um die Verfügbarkeit zu veranschaulichen gibt es verschiedene Blockdiagramme. Welche sind das?
Wie kann ein serielles System mit einem logischen Ausdruck dargestellt werden?
Und warum genau nimmt man dafür die Oder- und nicht die Und-Schreibweise?
Wie können Sie denn nun so einen Fehler entdecken? Nehmen wir an, dass Sie einen Bitfehler in einem Codewort erkennen möchten.
Welche Fehlerarten können Sie mit Paritäten denn erkennen?

So, nun übertragen Sie größere Datensätze, die meinetwegen mit CRC auf Korrektheit geprüft werden. Der Empfänger schickt Ihnen entsprechend ein ACK oder ein NACK. Was machen Sie aber, wenn weder NACK noch ACK bei Ihnen ankommt?
Woher wissen Sie, wie lange Sie warten sollten, bis eine Nachricht erneut übertragen werden sollte? Wie können Sie Schwankungen in der Übertragungsgeschwindigkeit messen, so dass Sie einen Wert für das Timeout berechnen können, der die aktuelle Netzlast berücksichtigt?

Prüfungsprotokoll (Modulprüfung MSc Informatik)

Kurse: *01867 –Sicherheit im Internet II*
21811 – Fehlertoleranz in Computersystemen und Netzwerken

Datum: 07.11.2012
Prüfer: Prof. Dr. Jörg Keller
Beisitzer: Hr. Cichowski
Dauer: ca. 25 Minuten
Note: 1,0

Sicherheit im Internet II

- ***Wie funktioniert ein Wörterbuchangriff?***
  → Ausprobieren von Wörtern und Kombinationen mit Zahlen / Zeichen
  → Hash-Wert bilden und mit tatsächlichem Hash-Wert vergleichen
  → tatsächlichen Hash-Wert bekommt man aus Registry oder Passwortdateien
  → Alternative: Passwort im Netzwerk mitlesen
- ***Wie kann man mit einem Host-based IDS erkennen, dass ein Trojaner installiert wurde?***
  → Host-based IDS erstellt zu Beginn Snapshot mit Hash-Werten der Dateien + Meta-Daten
  → Wenn Trojaner installiert wurde, wird der Hash verändert, so kann man das erkennen.
- ***Wie kann man verhindern, dass der Hacker auch den Hashwert / Snapshot mit verändert?***
  → Sicherheitskopie auf CD oder extern gelagerter Festplatte etc.
- ***Nun hat ein Hacker es geschafft, meinen Benutzernamen und zugehöriges Passwort herauszufinden. Jetzt loggt er sich damit per SSH auf einem unserer Server ein und tut dort etwas Böses. Wie kann ein dort installiertes Host-based IDS erkennen, dass das nicht ich bin?***
  → Ungewöhnliches Verhalten
  → ungewöhnliche Uhrzeit
  → Nur Hinweise, aber mit mehreren Hinweisen kann das System Alarm schlagen
- ***Nun ist ja bald Weihnachten und da bekommen Sie dann ein IDS-System mit 6 Sensoren geschenkt. Jetzt gehen wir mal davon aus, Sie haben ein Netzwerk zu Hause mit Paketfilter, DMZ, Web-Servern und internem Netz. Wo platzieren Sie nun diese Sensoren?***
  → ein network-based IDS vor dem ersten Paketfilter
  → ein host-based IDS auf dem ersten Paketfilter
  → ein network-based IDS in der DMZ
  → ein host-based IDS auf dem Web-Server
  → ein network-based und ein host-based IDS im internen Netz
  → siehe Abbildung 3.13 auf Seite 115 im Kurs
- ***Wofür benötigt man Primzahlen?***
  → Für kryptographische Verfahren, z.B. RSA
- ***Wie erzeugt man eine Primzahl?***
  → ungerade Zufallszahl generieren
  → Prüfen mit probabilistischen Primzahltest

- ***Wie lange dauert es denn, bis so ein Verfahren zum Generieren von Primzahlen auch eine gefunden hat?***
  → ln(n)
- ***Was gibt es denn für Fehler bei den Primzahltests?***
  → Es gibt Zahlen, die die Tests bestehen, aber gar keine Primzahlen sind: starke Pseudoprimzahlen
- ***Wie kann man die Fehlerwahrscheinlichkeit verringern?***
  → Mehrere verschiedene Tests und oft hintereinander ausführen
- ***Wie funktioniert das, wenn man nur den Miller-Rabin-Test hat?***
  → Der benötigt eine Zufallszahl a. Hier kann man den Test mit verschiedenen a's durchführen.

Fehlertoleranz in Computersystemen und Netzwerken

- ***Es gibt ja zur Fehlererkennung Paritäten. Wie funktioniert das?***
  → zusätzliches Bit
  → gerade Parität: wenn Anzahl an Bits mit Wert 1 ungerade ist: 1, sonst: 0
  → ungerade Parität: umgekehrt
- ***Kann man damit Fehler erkennen? Wenn ja: Welche?***
  → Nur ungerade Bit-Fehler können erkannt werden
- ***Was kann man mit der 2-dimensionalen Parität erkennen bzw. korrigieren?***
  → 1-bit-Fehler kann sie erkennen und korrigieren
  → 2-bit-Fehler können nur erkannt, aber nicht korrigiert werden (z.B. gleiche Zeile)
  → 4-bit-Fehler können gar nicht mehr erkannt werden, wenn sie z.B. im Viereck auftreten
- ***Systeme kann man ja in Diagrammen darstellen. Was gibt es da für zwei Typen?***
  → parallel: UND
  → seriell: ODER
- ***Wie ist die stationäre Unverfügbarkeit definiert?***
  → U = 1 – V = MTTR / MTBF
- ***Wenn nun bei der Übertragung ein Fehler auftritt und der Empfänger kann das erkennen, wie bekommt das dann der Sender mit?***
  → Indem der Empfänger ihm ein NACK sendet
- ***Was passiert denn wenn weder ACK noch NACK ankommt?***
  → Sender wartet Timer ab und sendet das Paket dann erneut
- ***Und wenn das ACK dann verspätet ankommt? Woher weiß denn der Sender dann für welches Paket das bestimmt war?***
  → Das kann man über Sequenznummern regeln

Fazit:

Herr Prof. Keller ist als Prüfer sehr zu empfehlen.
Er nimmt einem die Nervosität durch Smalltalk zu Beginn und eine lockere Prüfungsatmosphäre, die eher einem Fachgespräch ähnelt.
Auch nach der Prüfung nimmt er sich noch Zeit für einen und redet über die Zukunft im Studium, z.B. noch anstehende Prüfungen und Master-Arbeit.
Ich denke er legt eher Wert auf das Verständnis der Zusammenhänge, als auf Formeln.
Ich hatte zum Beispiel die Zeitspanne für das Generieren von Primzahlen etwas falsch genannt, was mir aber nicht von der Note abgezogen wurde.
Die oben genannten Fragen waren evtl. nicht alle, die gefragt wurden, aber mehr fällt mir nicht mehr ein. Außerdem wurden sie nicht immer genauso gefragt, wie sie hier stehen.