Prüfungsprotokoll 1866 und 1672

Datum: 08.02.2007
Prüfer: Prof. Dr. Keller
Beisitzer: war nett, Namen konnten ich mir trotzdem nicht merken
Note: 1.0

Ich durfte mir aussuchen, was zuerst geprüft werden sollte, da es mir egal war, hat Prof. Dr. Keller halt mit 1866 angefangen.

1866

Was sind die 4 Schutzziele:
Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität

Wie kann man Vertraulichkeit gewährleisten?
Über Verschlüsselung
(habe dann noch symmetrische und asymmetrische V. erklärt (ohne die mathematischen Hintergründe))

Wie kann man die Integrität gewährleisten?
Hashverfahren

Wie kann ich es verhindern, dass der Angreifer den Hashwert der Nachricht und die Nachricht selber verändert?
digitale Signatur
(Verschlüsselung des Hashwerts mit sym. oder asym. Schlüssel)

Wie kann man die Person wirklich authentifizieren?
Zertifikate

Was steht in einem Zertifikat?
Name, Version, Name des Ausstellers, öffentlicher Schlüssel des Ausstellers, Fingerprint

Wovon ist der Fingerprint?
vom öffentlichen Schlüssel des Aussteller

Wie kann ich sicher sein, dass es wirklich das Zertifikat ist, ich könnte es mir ja auch in einer Textdatei selber zusammenschreiben?
das Zertifikat ist ja mit dem privaten Schlüssel der CA signiert

Verfügbarkeit von Webservern. Wie kriege ich das hin?
richtige Konfiguration
(Patches, Updates, HA ... das wollte er aber gar nicht hören, er wollte in den Bereich der Firewall)

Wie trenne ich den internen Bereich, den Webserver und das Internet?
FW-Strategie inkl. Paketfilter und ALG (Proxy)

Wie kann ich DoS-Angriffe auf den Webserver verhindern?
Stateful-Inspection
(Hier hatte ich keine Ahnung, wo er hin wollte, habe was von Proxy-Systemen erzählt oder von Kernelpatches oder von Konfigurationsänderungen für Syn-Floods oder die Anzahl der halboffenen Verbindung, ihm ging es aber darum, dass sich die FW merkt, dass es viele Pakete gibt, die zusammengehören, aber nie ganz komplett sind und sie daher nie den Webserver erreichen. Ich bin bei der Frage die ganze Zeit davon ausgegangen, dass die FW SPI macht, irgendwie war das für mich klar...)

1672:

ACID-Paradigma erklären!
Atomicity, Consistency, Isolation, Durability
(Hier habe ich auch noch erklärt, was die einzelnen Sachen so machen, bzw. wofür die stehen)

Synchronistationsverfahren erklären!
optimistische und pessimistische Verfahren
(die einzelnen Verfahren dann noch erklärt)

Sperrprotokolle erklären, nicht die Sperrmodi!
2-Phasen-Sperrprotokoll, strikte 2-Phasigkeit, Preclaiming
(erklärt, wann LOCKs und UNLOCKs gesetzt werden können)

Was passiert, wenn irgendwer dem DBMS den Strom klaut, um zu Staub zu saugen? Was brauche ich dann?
Recovery
(dabei noch physisches und logisches Logging erwähnt)

2 Strategien des Recovery?
UNDO / REDO
(Rückgängigmachen und Wiederholen)

Wie funktionieren sie?
durchlaufen der Logs in entsprechender Reihenfolge

Datenschutz der DB. Wie kann ich es einrichten, dass User nur den Bereich bearbeiten können, den sie sollen?
Über Zugriffskontrolle oder über Sichten.

Was tun gegen Plattenklau und dem damit verbundenen Maßnahmen zur Sicherung der Daten?
Kryptographische Methode wie symmetrische Verschlüsselung.

Dann war es vorbei, ging recht schnell, und bis auf das SPI bin ich auch sauber durchgekommen.
Raus ... warten ... wieder rein ... etwas Smalltalk ... happy nach Hause gefahren ;-)

Prof. Dr. Keller ist absolut zu empfehlen. Nett, ruhig und bei Schwierigkeiten hilfsbereit. So nimmt er einem ein bisschen die Nervosität. Wünsche allen noch viel Spass bei ihren FPs.

Prüfung für das erste Wahlfach im Rahmen der Bachelor-Abschlussprüfung

Kurse: 1866 Sicherheit im Internet
1672 Datenbanken II
Prüfer: Prof. Keller
Datum: 21.09.2004
Dauer: 20 Minuten (jeder Kurs ziemlich exakt die Hälfte)

Sicherheit im Internet

- Wie lauten die Schutzziele?
- Verfügbarkeit sticht dabei heraus. Warum ist sie ein Schutzziel?
  (Erwähnung wirtschaftlichen Schadens war wohl wichtig.)
- Die anderen Ziele können durch Verschlüsselung geschützt werden. Symmetrische Verschlüsselung ist klar. Wie kann man Vertraulichkeit sonst noch erreichen?
  (Hier habe ich dann die Asymmetrische Verschlüsselung erklärt.)
- Wie kann man Integrität schützen?
  (Digitale Signatur und Hashing)
- Wieso vertraue ich einem Public Key?
  (Zertifikate, Hierarchie, RegTP, Erwähnung von Veröffentlichung des Fingerprints in anderen Medien, z.B. Print, wohl wichtig.)

Datenbanken II

- Synchronisation
  (Was ist das? Wer sorgt dafür? Und wie wird sie gewährleistet?)
- Was ist Serialisierbarkeit?
- Wie wird diese gewährleistet?
  (Optimistische und pessimistische Verfahren)
- Sperrverfahren. Worauf muss man achten?
- Deadlock. Was ist das? Wie erkennt man einen und wie löst man ihn auf?
  (Habe zyklischen Neustart direkt mit erwähnt.)
- Was ist erforderlich wenn der Rechner abstürzt oder ausgeschaltet wird?
  (Recovery)
- Log-Dateien
  (Physisch und logisch mit Inhalten und wie benutze ich sie im Fehlerfall. UNDO und REDO angesprochen)
-

Ich habe den Prüfungsverlauf aus dem Gedächtnis heraus aufgeschrieben, kann also weder für Vollständigkeit noch Korrektheit garantieren. Ich glaube aber, den Verlauf ganz gut getroffen zu haben.

Prof. Keller schafft es eine recht angenehme Prüfungsatmosphäre zu schaffen, indem er vorneweg erst ein wenig plaudert und dann auf die Prüfung umschwenkt. Gerade am Anfang der einzelnen Themen holt er etwas weiter aus. Der Redeanteil gleicht sich im Laufe der Prüfung aber wieder aus.
Fragestellungen und Benotung waren extrem fair. Kurskombination und Prüfer kann ich uneingeschränkt empfehlen.

Viel Glück!