Prüfungsprotokoll der mündlichen Prüfung Sicherheit im Internet I 1866 und Sicherheit im Internet - Ergänzungen 1868 (Bachelor Informatik)

Prüfer: Prof. Dr. Keller
Semester der Prüfung: WS 10/11
Datum der Prüfung: 31.05.2011
Dauer: ca. 25 min
Note: 1.0

Hier sind sicherlich nicht alle Fragen, jedoch ein großer Teil. Die Fragen habe ich umformuliert und die Antworten waren ausführlicher.

Schutzziele ?
-> Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit
Welche Arten von Verschlüsselung gibt es ?
-> symmetrisch und asymetrisch (beides kurz erläutert)
Geben Sie ein Beispiel zu jeder Art ?
-> DES (symmetrisch) und RSA (asymmetrisch)
Auf welchem mathematischen Problem basiert RSA ?
-> Zerlegung großer Zahlen in ihre Primfaktoren
Welchen Schlüssel nehme ich, wenn ich eine Nachricht an Sie verschlüsseln möchte (RSA) ?
-> Meinen öffentlichen Schlüssel
Und wenn ich meinen privaten Schlüssel nehme ?
-> Digitale Signatur
Wie kann ich sicher sein, daß die Person wirklich die ist, die sie vorgibt zu sein ?
-> Mit Zertifikaten. Erklärt. CA beschrieben usw... Die Person muss Nachricht, Digitale Signatur und ein Zertifikat senden. Inhalt eines Zertifikats genannt.

Was macht eine Packetfilter Firewall genau ?
-> Überprüft die Daten im Header eines IP-Packets und filtert anhand dieser.
Wie geht das ?
-> Anhand einer Regeltabelle. Verfahren erklärt. Alles was nicht explizit erlaubt ist, ist verboten und umkekehrt.

Welche Modi besitzt CPU (Ringe) ?
-> 4 Modi: Anwendungen, Dienste, Treiber und Betriebssystem. Es werden aber nur 2 benutzt.
Warum gibt es diese Modi ?
-> Kritische Systemaufrufe nur über Betriebssystem usw... .

Authentisierung mit Kerberos (ohne Ticket Granting Server)?
-> Aufgezeichnet und erklärt.

Ist WEP sicher ?
-> Nein
Warum nicht ?
-> Kurzer IV und es wird immer mit dem gleichen geheimen Schlüssel verschlüsselt. Kann man knacken.
Warum denn überhaupt das WLAN sichern ?
-> Nachbar hört vertrauliche Nachrichen ab, klaut Bandbreite, kann im Internet mit meiner IP Schaden illegale Aktivitäten ausführen und kann sich ev. mit meinem PC verbinden und Schwächen ausnutzen.

Warum ist WPA/WPA2 besser ?
-> Benutzt Session Key, einen einen doppelt so langen IV

Zur Prüfung allg.:
Prof. Dr. Keller ist ein sehr netter Prüfer. Er nimmt einem die Aufregung und erzählt viel von sich aus. Ich kann Prof. Dr. Keller als Prüfer nur weiterempfehlen.

19.01. 2011 mündliche Prüfung bei Prof. Keller
Internet Security I+II (1866/1867 Versionen WS09/SS10)
Note 1,7
Dauer 20 Minuten

Welche Schutzziele gibt es?
Alle vier genannt und auch kurz mit 2-3 Sätzen erklärt, was es damit auf sich hat

Verschlüsselung – welche zwei Arten kennen sie?
Symmetrische und Asymmetrische

Beispiele für beides?
Die alten (Cäsar-Chiffre etc.) waren nicht gefragt, Feistel, DES, AES und RSA, El-Gamal und Diffie-Hellmann

Welchen Schlüssel benutze ich bei der asymmetrischen Verschlüsselung, wenn ich ihnen eine Nachricht verschlüsselt zukommen lassen möchte?
Meinen öffentlichen Schlüssel

Was wäre es, wenn ich die Nachricht mit meinem privaten Schlüssel verschlüsselt hätte?
Digitale Signatur

Zertifikat – was steht denn so alles in einem Zertifikat?
Name, öffentlicher Schlüssel. Mehr wusste ich nicht mehr, im Nachgespräch wurde das als ein Kritikpunkt aufgeführt

Wofür überhaupt Zertifikat? Wie kann man sicher sein, dass sich da nicht einer selbst ein Zertifikat gebastelt hat?
Erklärt, dass mein Zertifikat mit dem privaten Schlüssel der CA zertifiziert ist, also digital signiert. Vertrauensfrage wird weitergereicht, man muss nicht mehr dem Absender vertrauen, sondern der CA. Problem der Verkettung von CA erklärt.

Host-based IDS – wie arbeitet das System? Was wird protokolliert? Man macht ja kein Abbild der gesamten Festplatte…
Hash-Werte von Dateien. Wollte noch Meta-Daten wissen, auf die ich nicht gekommen bin

Eigener Webserver soll von außen abgeschottet sein, aber auch nicht im internen Netz sein. Jetzt habe ich also ein Problem…
Lösung: DMZ, Aufbau und Funktion erklärt

Firewalls: Wie arbeitet so eine Firewall im einfachsten Fall?
Paketfilter erklärt.

Wonach filtern die?
IP-Adresse Empfänger und Absender, Ports

Eine DoS Attacke kann man damit aber nicht abwehren…
Nein, Besser Stateful Inspection Filter

Biometrie – welche Probleme ergeben sich z.B. bei Fingerabdrücken?
Merkmale werden digitalisiert und komprimiert gespeichert. Fehler sind da nicht auszuschließen. Auf diese beiden Punkte bin ich leider nicht gekommen. Habe noch FAR/FRR/EER erklärt und einige weitere Merkmale sowie Anforderungen aufgeführt.

Irgendwie kamen wir noch auf Application Level Gateway, das habe ich dann ebenfalls erklärt.

Bei der Prüfung kamen keine mathematischen Fragen vor oder wie Verschlüsselung / Verbindungsaufbau denn nun genau funktioniert, obwohl ich z.B. Diffie-Hellmann, Feistel, RSA, PGP, SSH, SSL etc. auswendig gelernt hatte.
Die Atmosphäre war gleich zu Beginn sehr freundlich und ich hatte nie das Gefühl, in die Ecke getrieben worden zu sein. Alles in allem eine gelungene Prüfung!

Prüfungsprotokoll

Bachelor-Modulprüfung Sicherheit im Internet (01866 / 01868)

Datum:	19.01.2011
Prüfer:	Prof. Dr. Keller
Beisitzer:	Dr. Bernhard Fechner
Dauer:	20 Minuten
Note:	1,0

<u>Sicherheit im Internet I</u>

- *Wie lauten die Schutzziele die wir kennen gelernt haben?*
  → Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit

- *Vertraulichkeit wird ja mit Verschlüsselung erreicht. Da gibt es zwei Arten, welche sind das?*
  → symmetrisch (private key) und asymmetrisch (public key)

- *Wenn ich jetzt eine Nachricht verschlüsselt an den Herrn Fechner schicken möchte, was muss ich dazu tun?*
  → Mit dem öffentlichen Schlüssel von Herrn Fechner verschlüsseln und dieser kann es mit seinem privaten Schlüssel entschlüsseln

- *Nun möchte ich die Nachricht digital signieren. Was muss ich dann tun?*
  → Mit dem eigenen privaten Schlüssel verschlüsseln und Herr Fechner kann es mit dem öffentlichen Schlüssel von Ihnen entschlüsseln und somit prüfen ob die Nachricht wirklich von Ihnen stammt.

- *Jetzt verschlüsselt man bei der digitalen Signatur ja nicht die komplette Nachricht, sondern was?*
  → einen Hash-Wert der Nachricht

- *Genau! Jetzt überlege ich mir selbst mal eine Hash-Funktion. Nehmen wir an, meine Nachricht besteht aus Zeichen von einem 256 Zeichen großen Alphabet. Ich nehme nun die Nachricht und addiere einfach die Werte aller Zeichen, dann forme ich das ganze noch ein wenig um, so dass ich auf einen 256 Bit Hash-Wert komme.*
  Ist diese Hash-Funktion kollisionsresistent?
  → Hier kam ich ein wenig ins Schleudern und habe erst etwas davon erzählt, dass die Nachricht mit wenigen Zeichen einfach zu knacken wäre, aber dafür hat er ja ein großes Alphabet benutzt.
  Nach ein wenig Hilfe kam ich dann aber doch noch darauf, dass durch die Kommutativität der Addition die Zeichen beliebig vertauscht werden können und trotzdem der selbe Hashwert herauskommt. Dadurch ist diese Hash-Funktion natürlich nicht kollisionsresistent.

- *Nun haben wir ja gelernt, dass es ein System benötigt, dass das interne "gute" Netz vom "bösen" externen Netz abschirmt. Das ist ja eine Firewall. Da gibt es ja dann verschiedene Arten und im einfachsten Fall ist das ein Paketfilter. Wie kann man sich*

denn gegen einen SYN-Flooding Angriff wehren?
→ Dazu benötigt man eine Stateful Inspection Firewall

- *Jetzt habe ich da meinen Webserver, der ja von außen und innen zugänglich sein soll, ich kann den aber nicht einfach vor oder hinter die Firewall stellen. Was macht man da?*
  → Dafür gibt es ein extra Netz, nämlich das Screened Subnet bzw. die DMZ

- *Jetzt habe ich aber ein Problem, wenn ich zum Beispiel Emails nach außen verschicken möchte, da ich ja nichts direkt von innen nach außen schicken kann. Wie löst man dieses Problem?*
  → Dafür benötigt man dann Proxies, die man in die DMZ stellt.

<u>Sicherheit im Internet I - Ergänzungen</u>

- *Es gibt ja ein Protokoll das es einem erspart sich ständig neu anzumelden an verschiedenen Systemen. Das ist Kerberos. Wie funktioniert das denn?*
  → Hier habe ich den genauen Ablauf inklusive Ticket-Granting-Server aufgezeichnet und erklärt.

- *Gehen wir mal zum Thema WLAN. Welche Verschlüsselungsarten gibt es denn da?*
  → WEP und WPA/WPA2

- *Warum sollte man denn WEP nicht mehr benutzen*
  → Ist mittlerweile leicht zu knacken und WPA hat eine verbesserte Verschlüsselung und eine erweiterte Authentifizierung

- *Wenn ich jetzt zu Hause nur mein kleines Heimnetzwerk habe und Online Banking nur verschlüsselt mache, warum sollte ich denn dann mein WLAN noch verschlüsseln?*
  → Ich meinte dann, dass jeder der das möchte sich dann kostenlos über das private Netz ins Internet verbinden kann und außerdem auch nicht verschlüsselte Pakete mithören kann.
  Prof. Dr. Keller hat dann noch ergänzt, dass derjenige ja auch meine Bandbreite klaut.

- *Warum ist denn das Fernuni-WLAN nicht verschlüsselt?*
  → Weil man sich noch über LDAP an einem Gateway authentifizieren und danach einen verschlüsselten VPN-Tunnel aufbauen muss. Es ist also hinreichend geschützt.

- *Jetzt nehmen wir mal an ich möchte zu Hause wirklich keine Verschlüsselung und ich trage einfach die drei Rechner, die ich zu Hause habe mit ihrer MAC-Adresse in den Filter des Access Points ein. Das ist doch dann ausreichend, oder?*
  → Schöne Idee, aber mittlerweile kann man die MAC-Adresse durch Mitlesen von Paketen leicht herausfinden und diese kann auch bei einem anderen PC eingetragen werden. Dieser kann dann auch wieder ohne Probleme ins Netzwerk.

<u>Fazit:</u>
Prof. Dr. Keller erzählt viel von sich heraus und gibt einem auch Hilfestellungen, wenn man einmal nicht weiter weiß. Meinen Hänger wegen seiner Hash-Funktion hat er nicht mit bewertet, was ich sehr fair finde. Er meinte, dass ich sonst alles gut erklärt habe und besonders die Kerberos-Erklärung hat ihm gefallen.
Ich kann Herrn Prof. Dr. Keller als Prüfer nur weiterempfehlen.

Mündliche Prüfung: Sicherheit im Internet I / II (1866 / 1867)
Prof. Keller
Am 02.02.2010

Auch ich werde heute meiner Pflicht nachkommen und ein Prüfungsprotokoll schreiben. Allerdings möchte ich an dieser Stelle nur die neuen noch nicht bekannten Prüfungsfragen niederschreiben. Die meisten Fragen aus meiner Prüfung kamen in den anderen Protokollen bereits alle vor.

Hier die neuen:

- Beispiel für asym. und sym. Verschlüsselungsalgorithmus?
    - Hier habe ich RSA und DES genannt
- Warum ist DES heute nicht mehr sicher?
    - Wurde geknackt; zu kleiner Schlüssel
- Jetzt habe ich aber die ganze Hardware für DES was könnte ich dann machen?
    - 3DES einsetzten
- VPN was ist das?
    - Habe ich nur allgemein erklärt. Sichere Übertragung über unsicheres Netz. Kostengünstig usw.
- Wofür setzt man VPN ein?
    - Site-to-site; end-to-site … Beispiele
- Wenn ich eine Firma habe und eine zweite dazu kaufe und beide Firmen nutzen unterschiedliche VPN um ihre Außendienstmitarbeiter an das Firmennetz anzubinden, was kann man kurzfristig machen damit ein Außendienst Mitarbeiter der Firma A auch auf das Netz der Firma B zugreifen kann?
    - VPN als site-to-site zwischen Firma A und B als kurzfristige Lösung

Ansonsten kann ich zur Prüfung sagen, dass sie relativ stressfrei abläuft. Herr Keller ist ein netter sympathischer Mensch, von dem ich mich jederzeit wieder prüfen lassen würde. Trotz ein paar „Schlenkern“ (wortlaut Herr Keller) in meiner Prüfung habe ich noch eine 1,3 bekommen, was super fair ist!

Viel Erfolg beim Studium und viele Grüße
Bastian Probst

Prüfungsprotokoll

Diplomprüfung
Kurse 01866 „Sicherheit im Internet I“
01867 „Sicherheit im Internet II“

Datum: April 2009
Prüfer: Prof. Dr. Jörg Keller
Dauer: ca. 20 Minuten
Note: 1,3

Prof. Keller sprach zwei Sätze zur Einleitung und legte dann direkt los mit seiner Standardfrage:

- *Welche Schutzziele werden im Kurs genannt?*
  Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit.
- *Nun kann man die Vertraulichkeit mit Verschlüsselung erreichen. Welche zwei großen Prinzipien der Verschlüsselung gibt es?*
  Symmetrische und asymmetrische Verschlüsselung.
- *Bei den asymmetrischen Verfahren haben wir das RSA-Verfahren kennen gelernt. Worauf basiert denn dieses Verfahren?*
  Primfaktorzerlegung
- *Genau. Und wie funktioniert das jetzt genau?*
  Hier waren die mathematischen Grundlagen gefragt! Da musste ich leider passen.
- *Wenn ich Ihnen eine asymmetrisch verschlüsselte Nachricht schicken will, welchen von den 4 Schlüsseln, die da im Spiel sind, also meine 2 und Ihre 2, nehme ich denn dann?*
  Meinen öffentlichen Schlüssel. Hatte erst irrtümlich seinen privaten Schlüssel genannt, konnte mich aber dann korrigieren.
- *Was wäre es denn, wenn ich die Nachricht mit meinem privaten Schlüssel verschlüsselt hätte?*
  Eine digitale Signatur.
- *Richtig, aber dabei verschlüsselt man ja in der Regel nicht die ganze Nachricht, sondern nur einen Hash-Wert. Welche Anforderungen stellt man denn an eine Hash-Funktion?*
  Einwegfunktion, muss gut streuen, schwache und starke Kollisionsresistenz. Die Stichworte genügten ihm.
- *Jetzt habe ich ein Gerät, mit dem ich mein Netzwerk gegen die böse Außenwelt schützen will. Wie nennt man so etwas?*
  Firewall.
- *Im einfachsten Fall ist das ja nun ein einfacher Filter. Nach welchen Kriterien filtert der denn?*
  IP-Adressen von Sender und Empfänger, Portnummern.
- *Und wenn ich nun die allerbeste Firewall habe, die man auf dem Markt kriegen kann, und Sie stehen vor dem Vorstand und sollen ihm ein IDS verkaufen, was würden Sie sagen?*
  Die Bedrohung kann auch von Innen kommen, ob vorsätzlich (Manipulation) oder nicht (Viren im Mail-Anhang geöffnet).

- *Nun gibt es ja spezielle host-based IDS, wie arbeiten denn die?*
  Protokolliert Prozesse und Dateizugriffe, vergleicht Daten auf dem PC mit „Sicherungskopien“.
- *Und wenn der Angreifer sehr schlau ist und die Sicherungskopien gleich mit verändert?*
  Sicherungskopie sollte auf schreibgeschütztem Medium erfolgen.
- *Genau, der klassische Fall ist ja, dass man es einfach auf eine CD brennt. Jetzt nehmen wir mal an, ein Hacker hat sich meine Zugangsdaten besorgt und sich beim Fernuni-Server mit meinen gültigen Zugangsdaten eingewählt. Wie kann ein IDS erkennen, dass da vielleicht was nicht in Ordnung ist?*
  Hier war ich nicht ganz sicher, was er hören wollte. Ich habe erwähnt, dass man vielleicht schauen könne, ob sich der Nutzer ungewöhnlich verhalte, oder ob sich jemand auf dem Account einloggt, obwohl der Nutzer im Urlaub ist. Prof. Keller ergänzte dann noch, dass man auch schauen könne, ob es von einer ungewöhnlichen IP-Adresse stamme oder zu Zeiten, zu denen der Nutzer normalerweise nicht eingeloggt ist (z. B. nachts). Das alles seien aber nur Hinweise und keine sicheren Anzeichen für einen Angriff.
- *Jetzt machen wir uns die ganze Mühe mit der Authentizitätsprüfung, obwohl wir doch eigentlich alle unverkennbare Merkmale am Körper haben, mit denen man uns identifizieren könnte. Welche Merkmale sind denn das so und wie geht das?*
  Fingerabdruck, Irisscan, Stimm- und Gesichtserkennung. Habe dann noch ein bisschen über die Fehleranfälligkeit dieser Systeme erzählt (FAR, FRR, ERR) und dass man ja z. B. Zwillinge kaum auseinanderhalten könne, bis Prof. Keller das Thema wechselte.
- *Wenn ein Angreifer mich auf eine von ihm gefälschte Seite locken will, wie kann er das machen?*
  Phishing-Mails mit gefälschten Links, URL hacking.
- *Nun springen wir mal zum Schluss des Skripts. Dort geht es ja um die Anbieter von Telekommunikationsdienstleistungen und welchen Gesetzen und Verordnungen sie unterliegen. Welche Arten von Anbieter unterscheidet man denn da?*
  Zugangs-, Inhalte- und Diensteanbieter. Habe noch Beispiele gegeben.
- *Für diese Firmen gelten ja auch einige Regeln im Zusammenhang mit Datenschutz. Darüber gab es doch in letzter Zeit ziemlich viel in den Nachrichten zu lesen …*
  Stichwort Vorratsdatenspeicherung.
- *Genau. Dass sich da Politik und Datenschützer drüber aufregen, ist ja klar, aber warum denn auch die Telekommunikationsanbieter?*
  Weil es viel Geld kostet, die Daten zu speichern und auch die Infrastruktur bereitzuhalten, mit der Strafverfolgungsbehörden darauf zugreifen können.

Fazit: Die Prüfung bei Prof. Keller war sehr entspannt. Er schafft ziemlich schnell eine lockere Prüfungsatmosphäre. Vor und nach der Prüfung war Zeit für ein bisschen Smalltalk rund ums Studium. Während der Prüfung erzählt er sehr viel von sich aus und nennt auch viele Stichwörter selber, so dass man (meist) schnell weiß, worauf er hinaus will. Beim RSA-Algorithmus musste ich passen, was zu minimalem Punktabzug führte, ansonsten führt er einen schon in die richtige Richtung, wenn man mal nicht weiter weiß. Meine Antworten waren teilweise etwas ausführlicher als hier angegeben, aber es tauchte doch auch die eine oder andere Frage auf, die mir bisher aus den Protokollen noch nicht so geläufig war. Und wahrscheinlich habe ich auch die eine oder andere Frage vergessen. Drum gilt wie immer: Protokolle sind hilfreich zur Vorbereitung, aber lernen muss man schon selber! ;-) Prof. Keller kann ich aber uneingeschränkt für Prüfungen weiterempfehlen! Viel Erfolg euch allen und bitte immer fleißig Protokolle schreiben!

Prüfungsmitschrift Sicherheit im Internet I und II

Prüfer: Prof. Keller
Beisitz: Dipl. Inf. Udo Hönig

Prüfling: Mag. Gunther Hebein

1. Wir hatten da Schutzziele bei der Sicherheit definiert, wie lauten die denn?
Die Antworten kamen wie aus der Pistole geschossen, kein Wunder, beginnt doch jede Prüfung mit dieser Frage.

2.Welche grossen Arten von Verschlüsselung kennen Sie denn?
Symmetrisch und asymmetrisch.

3. Bei den symmetischen Arten haben wir den RSA kennengelernt, auf was basiert denn der?
Auf der Primfaktorzerlegung.

4. Ist denn der RSA-Algorithmus sicher?
Derweilen schon noch, aber wenn es eine Möglichkeit gibt, schnell eine Primfaktorzerlegung eines public-Keys zu erledigen, ist RSA gefallen.

5. Sie schicken nun eine blanke Message an jemanden, wie könne Sie Authentizität herstellen
Durch HASH-Berechnung (MD5 oder SHA1) und anschliessende Verschlüsselung des HASH-Wertes mit dem eigenen privaten Key.

6. Nun gibt es Zertifikate. In einem Zertifikat steht ja allerhand drinnen, aber erzeugen könnte das ja ein jeder. Wodurch ist das ganze vertrauenswürdig?
Eine Zertifizierungsbehörde unterzeichnet mein Zertifikat als authentisch. Ich muss halt dann der Zertifizierungsinstanz trauen.

7. Was könne Sie mir generell über die HASH-Funktion sagen?
Ich habe die Grundanforderungen an eine HASH-Funktion erwähnt: Nicht umkehrbar, schnell und einfach zu berechnen, schön gestreut. Schwache und Starke Kollisionsresistenz. Da habe ich mich verhaspelt, weil ich nicht wusste wo denn jetzt der praktische Unterschied ist. Ich habe halt die Definitionen der beiden Resistenzen erklärt und erwähnt, dass die schwache Kollisionsresistenz sicherlich in der Praxis relevanter ist, da ein Diebstahl einer Passwortdatei mit HASH-Werten leicht ausgenützt werden kann um ein anderes PW zu finden was den gleichen HASH-Wert hat.
Er wollte aber auf das Geburtstagsparadoxon hinaus...

8. Firewalls - was ist das?
Die Typen erörtert und was da so welche Komponente macht.
Packetfilter oder besser SPI, Application Level Gateway, Circuit Level Gateway, jeweils screened host oder screened subnet.

9. Wie können Sie eine DoS-Attacke abwimmeln?
Durch das SPI-Firewall. Nicht durch Packetfilter!

10. Sie haben jetzt eine tolle Firewall, bewiesenermassen uneinnehmbar, Ihr Administrator will aber zusätzlich 20000 Euro für Sicherungsmassnahmen. Was sagen Sie?

Ich habe gesagt, dass er mir dann mal erklären soll wo da noch Gefahren zu sehen sind und dass ich mir zuerst mal ausrechne was denn die Kosten von einem Eindringling wären. Wenn der dann nur einen Schaden von 10 Euro anrichtet, dann überlege ich mir das.
Prof. Keller wollte aber auf interne Fieslinge hinaus und das Stickwort IDS hören. Ich hab an alles andere gedacht nur nicht an IDS.

11. Sie haben jetzt einen PC nagelneu geliefert bekommen, was machen Sie jetzt?
Ich habe gesagt, dass ich alle Dienste die ich nicht brauche sperre. Dann Benutzer anlegen, Standardbenutzer weg. Rechtevergabe, möglichst rigoros niedrige Rechte. Web-Server das Hopping aus usw.
Nicht erwähnt habe ich tägliches Backup und Directory Listing bei apache.

12. Und jetzt wollen Sie einen e-shop eröffnen, welche Bezahlungsarten bieten Sie an.
Ich habe alle Arten aus dem Skript aufgezählt. Auch die Nachnahme. Da ich selber einen Shop betreibe, weiß ich, dass Nachnahme am sichersten für beide Seiten ist.
Prof. Keller wollte allerdings auch Sammelrechnung hören (denn da fällt das Disaggio am moderatesten aus), aber auf die kam ich erst nach langem Nachfragen, denn wer wartet denn schon 3 Monate freiwillig auf sein Geld?

Alles in allem ist Prof. Keller weiter zu empfehlen, manchmal weiss man bei Ihm halt nicht worauf er hinaus will, aber er leitet einen dann schon dort hin.

Meine Literatur:
Wikipedia
Bishop, Matt: Computer Security: Art and Science, Addison Wesley 2004 (Anm.: Zu detailliert!)
Stallings, Williams: Network Security Essentials, Prentice Hall, 2. Auflage (Optimal als Ergänzung zum Skriptum)

Diplomprüfung Sicherheit im Internet I+II 1866/67
Prüfer. Prof. Dr. Keller
07.04.2004
Note 1.0

Themengebiete:

Schutzziele - Besonderheit der Verfügbarkeit wurde tiefer hinterfragt

Verschlüsselung – symmetrisch – asymmetrische Verfahren

- ich habe hier auch die mathematischen Hintergründe gelernt, die nicht erforderlich waren.

Zertifikate – Trust-Center – Woher kommt die Sicherheit über die Identität eines Zertifikates

Hashfunktionen – Anforderungen

Firewalls – Architekturen, Funktionsweise

IDS – welche Techniken, wie wird wa erkannt

Wie kann ein Hacker ermittelt werden?

Insgesamt gab es keine Überraschungen, alle abgefragten Themengebiete kommen in den Protokollen bereits vor. Die nichttechnischen Aspekte des Zahlungsverkehrs wurden überhaupt nicht angesprochen.

Prof. Keller ist als Prüfer ohne Einschränkungen zu empfehlen.

Fach: 1866/1867 Sicherheit im Internet I/II (Versionen SS04 / WS03)
Prüfung: Bachelor Fachprüfung Wahlfach
Prüfer: Prof. Dr. Keller
Beisitzer: Herr Hönig
Datum: 26. Okt. 2004
Note: 1.0

Welche Schutzziele gibt es?
Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität

Warum sticht Verfügbarkeit heraus?
Hier hab ich viel Zeugs geredet, was wohl nicht falsch war, aber nicht gemeint. So wie "Wenn ich einen Shop habe und der fällt aus, dann kostet mich das Geld". Gemeint war aber wohl, dass ich bei der Verfügbarkeit aktiv sein muss, damit etwas nicht passiert, im Gegensatz zu den anderen Schutzzielen (Aktiv sein, damit etwas passiert: Verschlüsselung)

Es gibt symmetrische Verschlüsselung, welche kennen Sie noch?
Grundprinzip der Asymmetrischen/Public-Key-Verfahren erläutert. Abgrenzung zum Secret Key.

Was ist nötig, damit RSA funktioniert?
Hier habe ich ein bisschen was über die Funktion erzählt, was aber wieder nicht gemeint war. Ziel war: Die Menge aus Plaintext und Ciphertext muss gleich groß sein.

Woher weiß ich, dass der öffentliche Schlüssel wirklich von dem stammt, von dem ich es annehme?
Zertifikat oder Web of Trust.

Wer stellt Zertifikate aus?
Certifikation Authority und das Problem der Verkettung von Zertifizierungen genannt, dass im Prinzip nur über Fingerprints in Printmedien zu lösen ist.

Welche Anforderungen sollte eine Hashfunktion erfüllen?
Aus der Hashsumme sollte nicht die Ursprungsmenge berechnet werden können sowie schwache und starke Kollisionsresistenz.

Wie kann ich denn nun vertrauliche Daten abhören?
Sniffing/Spoofing

Und wenn ich keinen Zugang zu einem DNS-Server habe?
URL-Hacking

Wie erkenne ich einen Angriff?
Intrusion Detection System

Welche Typen von IDSs gibt es?
Host und Network Based und die Prinzipien sowie Produkte genannt.

Wie kann ich meinen privaten PC schützen?
Virenscanner, Personal Firewall und korrekte Konfiguration

Was macht die Personal Firewall?
Blockt grundsätzlich erst einmal die einkommenden privilegierten Ports und lässt zunächst auch keine Anwendung Verbindungen nach draußen herstellen.
Arbeitet regelbasiert und merkt sich, wenn ein Programm bspsw. der Browser eine Verbindung auf Port 80 machen darf.

Wie schütze ich denn Anonymität im Internet?
Rewebber und Anonyme E-Maildienste.

Welche Gesetze sind für Nutzer und Anbieter im Internet relevant?
Die drei Bereiche aus dem Kurs genannt: allgemeiner, für ISPs und für Dienstanbieter. Zu jedem Bereich ein paar Gesetze genannt, die mir zum Teil noch eingefallen sind.

Was sind Replay-Angriffe und wie kann ich sie verhindern?
Kryptographie ist deterministisch, sodass im ECB-Modus beispielsweise die Nachricht morgen die gleiche ist, wie heute. Abhilfe schafft der CBC-Modus, bei dem ein Teil der vorherigen Nachricht, bzw. ein Initialwert in die Verschlüsselung einfließt um Wiederholung des Ciphertextes bei gleichem Plaintext zu vermeiden.

Und neben CBC wie noch?
Hier musste ich rückfragen, da ich keine Ahnung hatte, was gemeint war.

Stellen Sie sich vor, ich wäre eine Bank… Ah, dann nutze ich PIN und TANs, die mir die einzelne Transaktion bestätigen. Wobei die TAN nur für eine Transaktion gültig ist.

Dies ist nur eine Zusammenfassung! Die Fragen waren nicht immer so eindeutig und konkret gestellt, wie ich versuche sie thematisch hier darzustellen.
Meist ergaben sie sich aus dem Gespräch. Die Antworten vielen natürlich auch ausführlicher aus.

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!

Diplomprüfung: 1866/1867 „Sicherheit im Internet I und II“

Prüfer	: Prof. Dr. Keller
Datum	: 27. Januar 2004
Dauer	: 20 Minuten
Note	: 1,0

Vorbereitung

Zur Prüfungsvorbereitung habe ich mir erst eine (sehr persönliche) Zusammenfassung der Skripte erstellt. Diese basiert u.a. auf einem vorhandenen Prüfungsprotokoll über den Kurs 1866 sowie ein Gespräch über die Schwerpunkte der Prüfung, das ich mit Prof. Keller einige Wochen vorher geführt habe. Da der Kurs 1867 zum Zeitpunkt der Prüfung das erste Mal angeboten wurde, existierte darüber bis dahin noch kein Prüfungsprotokoll.

Prüfungsverlauf

Bei der Begrüßung legte ich gleich meinen Studierenden- und Personalausweis vor. Aufgrund des etwas älteren Fotos, welches nur noch eine leichte Ähnlichkeit mit mir aufweist, meinte Prof. Keller, dass wir auf den Personalausweis noch im späteren Verlauf der Prüfung kommen würden, was den Beisitzer, dessen Namen ich mir leider nicht gemerkt habe, erstaunte.

Ohne weitere Einleitung kam Prof. Keller danach gleich zur ersten Frage. Der Verlauf der Prüfung hat sich ungefähr wie folgt abgespielt:

Welche Angriffsziele / Schutzziele im Internet gibt es?

- Vertraulichkeit
- Integrität
- Authentizität
- Verfügbarkeit

Ich erwähnte zusätzlich noch die *Anonymität*, worüber wir im Anschluss an die Prüfung noch diskutiert haben.

Die ersten drei betreffen die Dateninhalte, das letzte bezieht sich mehr auf die Technik. Sprechen wir erst über die ersten drei Schutzziele. Wie kann man Vertraulichkeit erreichen?
Durch Verschlüsselung.

Warum muss denn überhaupt verschlüsselt werden? Das ist doch eigentlich für den Nachrichtenaustausch gar nicht notwendig.
Ich gab einen kurzen Überblick über das Internet als offenes Netz, bei dem prinzipiell jeder alles mitlesen kann.

Welche Art von Verschlüsselung gibt es?

- Symmetrische bzw. private key Verfahren und

- asymmetrische bzw. public key Verfahren

Nun haben wir irgendwo gehört, dass symmetrische Verschlüsselung schneller geht. Was ist dabei zu beachten, wenn ich Ihnen symmetrisch verschlüsselt eine Nachricht zusenden möchte?
Die Schlüssel müssen vorher ausgetauscht werden, wobei derselbe Schlüssel sowohl für die Ver- als auch die Entschlüsselung dient. Die Vertraulichkeit ist dann und nur dann gewährleistet, wenn ausschließlich der Sender und der Empfänger der Nachricht den Schlüssel haben.

Kommen wir nun zum nächsten Schutzziel, der Integrität. Wie können wir die gewährleisten?
Auch durch Verschlüsselung. Wenn ich einen Text wieder entschlüsseln und lesen kann, dann weiß ich, dass die Nachricht vollständig und nicht verändert wurde.

Und wenn ich Ihnen eine Binärdatei zuschicke, die Sie nach der Entschlüsselung nicht lesen können? Dann könnte ein Angreifer etwas verändert haben, ohne dass Sie etwas merken.
Richtig, dann wird die Nachricht von Ihnen erst mit einem vernünftigen Hash-Algorithmus verarbeitet und dann verschlüsselt. Mit dem Hash-Wert, den ich ebenso erzeugen und mit Ihrem ursprünglichen vergleichen kann, kann ich die Integrität der entschlüsselten Nachricht prüfen.

Hash ist gut. Kommen wir zur Authentizität. Wie können wir bei unserer Email sicherstellen, dass eine Email an mich wirklich von Ihnen kommt?
Durch ein Zertifikat von mir.

Wie wird ein Zertifikat erstellt? Was ist das denn überhaupt?
Ein Zertifikat wird von einer Zertifizierungsstelle oder auch Trust Center auf meinen Antrag für mich ausgegeben. Es handelt sich dabei um meinen öffentlichen Schlüssel, der von der Zertifizierungsstelle mit deren privatem Schlüssel verschlüsselt wurde. Die höchste Zertifizierungsstelle in Deutschland ist die RegTP.

Wenn Sie meine Email bekommen, können Sie mit dem öffentlichen Schlüssel der Zertifizierungsstelle mein Zertifikat entschlüsseln. Damit verifizieren Sie meine Authentizität und erhalten damit meinen öffentlichen Schlüssel, um meine Email zu entschlüsseln.

Wie erhalten Sie denn so ein Zertifikat?
Es existieren verschiedene Sicherheitsstufen. Eine davon erfordert z.B., dass ich mich mit meinem Ausweis persönlich bei der Zertifizierungsstelle oder entsprechender Behörde vorstelle („da war der Personalausweis“ war der Hinweis von Prof. Keller an den Beisitzer).

Woher wissen Sie denn, dass das Zertifikat der Zertifizierungsstelle korrekt ist? Man kann zwar die eine Zertifizierungsstelle mit einer anderen Zertifizierungsstelle zertifizieren, aber ist das ausreichend?
Nein, zumindest von der obersten Zertifizierungsstelle, in Deutschland der RegTP, muss der Fingerprint des Zertifikats z.B. in der Zeitung, dem Bundesanzeiger o.ä., also außerhalb der „Computerwelt“ veröffentlicht werden. Der Fingerprint deshalb, weil der Mensch das eigentliche Zertifikat (den öffentlichen, mathematischen Schlüssel) nicht vernünftig überprüfen kann. Danach können sich weltweit alle (oberen) Zertifizierungsstellen gegenseitig zertifizieren. Wichtig ist, dass ich von einer den echten Nachweis der Echtheit habe.

Kommen wir nun zum vierten Schutzziel, der Verfügbarkeit. Warum ist sie überhaupt ein Schutzziel?
Weil Dummköpfe und Scriptkiddies sich einen Spaß daraus machen, Rechner zum Absturz zu bringen bzw. vom Netz zu trennen. Ein Großteil des eCommerce lebt aber davon, online zu sein. Die heutige Wirtschaft, und nicht nur die, ist extrem auf die Verfügbarkeit von Computersystemen angewiesen. (Prof. Keller brachte dazu das Argument, wenn Amazon einen Tag offline sei, hätten diese einen immensen Schaden).

Wenn sich jetzt ein Privatmann einen PC und ein Modem kauft und ins Internet möchte. Was würden Sie ihm raten?
Von allen Programmen und Betriebssystemteilen sollten die neuesten Versionen eingesetzt bzw. alle verfügbaren Patches eingespielt werden.

Darüber hinaus sollte eine Firewall eingesetzt werden. Am Besten ist diese auf einem eigenständigen PC einzurichten. Bei einer Privatperson, die keine hohen Ansprüche an die Geheimhaltung stellt, reicht aber auch eine PersonalFirewall auf dem Benutzer-PC.

Und was ist, wenn ich auch Email empfangen möchte, deren Inhalte ich nicht kenne? Wie sieht es mit Schadensprogrammen aus?
Ja, natürlich, das hatte ich vergessen. Ein Antiviren-Programm, selbstverständlich auch in der aktuellsten Version, muss ebenfalls installiert werden.

Kommen wird jetzt zu einer Firma, die ihr Netzwerk an das Internet anschließen möchte. Eindringlinge werden ja nicht von selbst erkannt. Was muss denn gemacht werden, damit Angriffe so früh wie möglich erkannt werden?
Es müssen unterschiedliche Intrusion Detection Systeme (IDS) installiert werden, je nachdem, wie das anzuschließende Netz aussieht und welche Angriffe ich erkennen möchte.

Zur Netzüberwachung werden Netzscanner (network based IDS) eingesetzt. Zur Überwachung einzelner Computer werden host based IDS eingesetzt.

Welches von beiden ist denn besser geeignet, wenn ein Angriff stattgefunden hat, um ein Evidence anzulegen? Was ist für den forensischen Nachweis in einem späteren Schadensersatzprozess besser?
Das kommt darauf an, was für ein Angriff vorlag. Grundsätzlich sind beide Verfahren geeignet. Viel wichtiger für ein späteres Gerichtsverfahren ist die Genauigkeit, Vollständigkeit und Nachvollziehbarkeit der Aufzeichnungen.

Geht es z.B. darum, nach einem Portscan einen der Ports für einen Angriff oder eine vorhandene Sicherheitslücke im IIS von Microsoft ausgenutzt zu haben, mittels Buffer overflow den IIS oder andere Prozesse zum Absturz zu bringen, und wird dadurch eine Administratorshell für den Angreifer eröffnet, kann dieses sich gut mittels mitgeschnittener Datenpakete eines network based IDS nachweisen lassen, da bei einem abgestürzten Prozess oft keine veränderten Dateien auf der Festplatte zu finden sind.

Wurde hingegen ein Angriff mit einem sogenannten *rootkit* gestartet (als Prof. Keller mich fragend ansah, erklärte ich ihm, dass die meisten Server im Internet unter Unix laufen und es daher auch für Dummies diverse „Spielzeuge“ (root-Kits) gibt, welche einem durch verschiedene Tricks root-Rechte einräumen, wenn man diese Kits auch ohne root zu sein auf dem Computer installiert bekommt), dann wird man diese i.d.R. nur durch ein host based IDS erkennen und nachweisen können. Network based IDS würden z.B. in dem Fall versagen, wenn diese rootkits

von einem Benutzer von innen heraus auf dem Computer installiert wurde.

Fazit

Das Protokoll stellt natürlich keine wortgenaue Wiedergabe dar. Bei den meisten Antworten habe ich noch etwas ausführlicher geantwortet. Die Fragen sind aber meinem Gedächnis zufolge alle vorhanden. Durch die Darstellung des Prüfungsprotokolls als quasi Wortprotokoll wollte ich versuchen, etwas die entspannte Atmosphäre wiederzugeben.

Die Prüfung verlief eigentlich mehr in einer Art Fachgespräch. Lediglich die erste Frage war eine „typische“ Prüfungsfrage. Die anderen Fragen waren eher von der Art, als wenn ein interessierter Kunde einem EDV-Verkäufer Informationsfragen stellt. Dadurch kam zu keinem Zeitpunkt der Prüfung irgendeine Nervosität auf, da Prof. Keller mir immer das echte Gefühl gab, wirklich an den Antworten bzw. den gegebenen Informationen interessiert zu sein. Bei Nachfragen kam nicht das Gefühl auf, etwas vergessen zu haben und jetzt vorgeführt zu werden. Eher war es so, dass er da noch weitere Sachen gehört habe und darüber auch noch gerne Infos hätte (siehe z.B. bei der „Beratung des Privatmanns“, bei dem ich zuerst die Antiviren-Software vergessen hatte).

Ich kann Prof. Keller und diesen Kurs für eine Prüfung uneingeschränkt empfehlen und allen, die sich auch nur etwas für diese sehr einprägsame Materie interessieren, als Vertiefungsfach ans Herz legen.

Ich wünsche allen viel Erfolg bei den Prüfungen.

Thomas Schwarze

19.01. 2011 mündliche Prüfung bei Prof. Keller
Internet Security I+II (1866/1867 Versionen WS09/SS10)
Note 1,7
Dauer 20 Minuten

Welche Schutzziele gibt es?
Alle vier genannt und auch kurz mit 2-3 Sätzen erklärt, was es damit auf sich hat

Verschlüsselung – welche zwei Arten kennen sie?
Symmetrische und Asymmetrische

Beispiele für beides?
Die alten (Cäsar-Chiffre etc.) waren nicht gefragt, Feistel, DES, AES und RSA, El-Gamal und Diffie-Hellmann

Welchen Schlüssel benutze ich bei der asymmetrischen Verschlüsselung, wenn ich ihnen eine Nachricht verschlüsselt zukommen lassen möchte?
Meinen öffentlichen Schlüssel

Was wäre es, wenn ich die Nachricht mit meinem privaten Schlüssel verschlüsselt hätte?
Digitale Signatur

Zertifikat – was steht denn so alles in einem Zertifikat?
Name, öffentlicher Schlüssel. Mehr wusste ich nicht mehr, im Nachgespräch wurde das als ein Kritikpunkt aufgeführt

Wofür überhaupt Zertifikat? Wie kann man sicher sein, dass sich da nicht einer selbst ein Zertifikat gebastelt hat?
Erklärt, dass mein Zertifikat mit dem privaten Schlüssel der CA zertifiziert ist, also digital signiert. Vertrauensfrage wird weitergereicht, man muss nicht mehr dem Absender vertrauen, sondern der CA. Problem der Verkettung von CA erklärt.

Host-based IDS – wie arbeitet das System? Was wird protokolliert? Man macht ja kein Abbild der gesamten Festplatte…
Hash-Werte von Dateien. Wollte noch Meta-Daten wissen, auf die ich nicht gekommen bin

Eigener Webserver soll von außen abgeschottet sein, aber auch nicht im internen Netz sein. Jetzt habe ich also ein Problem…
Lösung: DMZ, Aufbau und Funktion erklärt

Firewalls: Wie arbeitet so eine Firewall im einfachsten Fall?
Paketfilter erklärt.

Wonach filtern die?
IP-Adresse Empfänger und Absender, Ports

Eine DoS Attacke kann man damit aber nicht abwehren…
Nein, Besser Stateful Inspection Filter

Biometrie – welche Probleme ergeben sich z.B. bei Fingerabdrücken?
Merkmale werden digitalisiert und komprimiert gespeichert. Fehler sind da nicht auszuschließen. Auf diese beiden Punkte bin ich leider nicht gekommen. Habe noch FAR/FRR/EER erklärt und einige weitere Merkmale sowie Anforderungen aufgeführt.

Irgendwie kamen wir noch auf Application Level Gateway, das habe ich dann ebenfalls erklärt.

Bei der Prüfung kamen keine mathematischen Fragen vor oder wie Verschlüsselung / Verbindungsaufbau denn nun genau funktioniert, obwohl ich z.B. Diffie-Hellmann, Feistel, RSA, PGP, SSH, SSL etc. auswendig gelernt hatte.
Die Atmosphäre war gleich zu Beginn sehr freundlich und ich hatte nie das Gefühl, in die Ecke getrieben worden zu sein. Alles in allem eine gelungene Prüfung!