Gedächtnisprotokoll zur Bachelorprüfung 1866/1867 Sicherheit im Internet I+II

Prüferin: Frau Dr. Kern-Isberner
Datum: 14.06.2004
Dauer: 25 min
Note: 1,7

Prüfungsvorbereitung:

Die **Kursskripte / EAs**, **eigene Zusammenfassung**, die **Zusammenfassung von Thomas Schwarze** (http://www.stud.fernuni-hagen.de/q5045983/SicherheitSkript.ps) und die folgenden Bücher:

- Klaus Schmeh "**Kryptographie und public key Infrastrukturen**", Dpunkt 2001, ISBN: 3932588908
- Krzysztof Janowicz "**Sicherheit im Internet**", O'Reilly 2002, ISBN: 3897212730
- Andrew S. Tanenbaum, "**Computernetzwerke**", Addison-Wesley 2003, 4. Aufl., ISBN: 3827370469
- Jörg Roth "**Mobile Computing**", Dpunkt 2002, ISBN: 3898641651

Prüfungsablauf:

Was sind die Schutzziele?
Vertraulichkeit, Authentizität, Integrität, Verfügbarkeit erklärt

Was sind konkrete Bedrohungen im Internet und welche Auswirkungen können Sie haben?
Viren, Würmer (Beispiel W32.Blaster), Trojaner, Rootkits

Wie sichert man einen privaten Rechner?
Nicht als Admin arbeiten/Rechte vergeben, OS-Updates (evtl. mittels Microsoft SUS-Server), Virenscanner mit Realtime Protection (H+B EDV AntiVir) und Personal Firewall (Kerio, ZoneAlarm) installieren

Woher bekommt man aktuelle Informationen zur IT-Sicherheit
http://www.BSI-fuer-Buerger.de / http://www.Heisec.de / http://enterprisesecurity.Symantec.de / http://de.mcafee.com/virusInfo

Wie kann man sicher Kommunizieren/Daten übertragen
PGP und SSL erklärt

Symmetrische/private key-Verfahren
Prinzip, Funktion und Vor-/Nachteile erklärt, DES

Worauf basieren sie?
Feistelschema (1866, Abb. 2.4) gezeichnet und erklärt

Asymmetrische/public key-Verfahren
Prinzip, Funktion und Vor-/Nachteile erklärt, RSA

Kann man aus dem public key den private key berechnen?
Nein.

Wie lässt sich der RSA-Algorithmus mathematisch herleiten?
(1866, Kap 2.4.2)

Angriffe auf Verschlüsselung
Brute force (cipher text only), Lineare (known plain text) und Differentielle (chosen plain text) Kryptoanalyse

Wieso und wie kann man den RSA brechen?
Versucht "Quadratic Sieve"-Algorithmus (1867 Kap. 1.8.5) zu erklären, Beispiel dazu aufgeschrieben

Wie kann ich Zugriff auf einen entfernter Rechner erhalten
SSH, rlogin, telnet, VNC, Microsoft Remote Desktop

Was sind VPN und wie funktionieren Sie?
Prinzip von VPNs, Varianten genannt und erklärt, IPsec und Tunneling-Prinzip erklärt

Was sind IDS, welche Arten werden Unterschieden und wie funktionieren sie?
network based (snort) und host based IDS (TCPdump, IPcop) erklärt und Beispiele genannt

Warum ist eine Remote-Verbindung mit telnet gefährlich?
User-Login und Password werden unverschlüsselt übertragen

Was macht man, wenn man eine Attacke feststellt?
Prozess: „containment -> erradiction -> recovery -> lessons learned“ erklärt

Was sind Firewalls und welche Arten gibt es?
Packet Filtering Router, Stateful Inspection Filter, Application Level Gateway (Proxy), Screened Subnet, DMZ erklärt

Detaillierter Architektur einer E-Commerce Anwendung
Versucht Drei-Schichten-Modell mit Firewall, IDS und Sensoren aufzuzeichnen und erklärt (1867, Abb. 4.2)

Fazit:

Frau Dr. Kern-Isberner ist eine sehr ruhige, freundliche und gerechte Prüferin. Sie fragt die verschiedenen Aspekte der Kurse sehr ausgeglichen ab. Können Fragen nicht beantwortet werden, so leitet sie die Lösungen während bzw. nach der Prüfung verständlich und ausführlich her (Quadratic Sieve).

Ich kann Frau Dr. Kern-Isberner und diese Kurse von Herrn Wohlfeil uneingeschränkt empfehlen.

Während und nach der Durcharbeitung der Skripte wurden mir viele Probleme zum Thema IT-Sicherheit erst richtig bewusst. Die Tipps, wie man (seine) Rechnersysteme/Netzwerke sichert und überwacht sollte sich jeder zu Herzen nehmen und beachten. Es schadet bestimmt nicht!

ACHTUNG:
Es handelt sich hier nur um ein Gedächtnisprotokoll. Die Antworten spiegeln nur meine Sicht bzw. meinen Wissensstand wieder. Sie können natürlich auch Fehler enthalten. Bitte verlasst euch also nicht nur darauf! Mit den Literaturhinweisen solltet ihr euch aber gut vorbereiten können. Dank auch an Thomas Schwarze ;-)

Viel Glück und Erfolg!

Bernhard Traurig
mailto:Bernhard.Traurig@Fernuni-Hagen.de

Kombinationsprüfung 1831/1866
"Neuronale Netze" und "Sicherheit im Internet"
Mai 2003
Prüfer: Prof. Helbig und Dr. Kern-Isberner
Dauer jeweils 15 min
Gesamtnote 1,7

Neuronale Netze (1831) - Prof. Helbig

Wie lassen sich neuronale Netze charkterisieren?
- Netztopologie (FF-/FB-Netze genannt und erklärt)
- Lernverfahren (Selbstorganisation und überwachtes Lernen genannt und erklärt)
- matematische Beschreibung einzelner Neuronen (ab hier ging es in die Tiefe)

Mathematische Beschreibung eines Neurons
- zeichnen (habe ich mir etwas schwer getan)
- mathematische Formeln aufschreiben (Eingabe-/Ausgabevektor, Gewichtsmatrix, Propagations-/Aktivierungs-/Ausgabefunktion)

Welche Aktivierungsfunktionen gibt es?
- lineare (Bsp. Kohonennetz genannt. War der Aufhänger um später darauf zurück zu kommen)
- Schwellwertfunktion (erklärt)
- Sigmoide Funktionen (Fermi -Funktion als Beispiel genannt. Bedingung der Differenzierbarkeit für BP-Algorithmus genannt. Damit ging es in die nächste Vertiefung)

Wie sieht die Fermi-Funktion denn aus?
(Er wollte Zeichnung. Ausser S-förmig fiel mir nichts ein, daher ging es in eine zähe Herleitung. Die Formel habe ich irgendwie noch aus dem Gedächtnis gegraben und dann ging es daran, Werte einzusetzen und die Funktion zu zeichnen.)

Warum muss sie differenzierbar sein?
(Erst habe ich ihm den gesamten Backpropagation Algorithmus detailliert erklärt, hat ihn nicht zufrieden gestellt. Dann habe ich ihm die erweiterte Delta-Regel und den Gradientenabstieg erklärt. Hat ihn auch nicht zufrieden gestellt. Er wollte die Fehlerfunktion des Backpropagation Algorithmus haben und dass diese zu minimieren ist. Irgendwie habe ich das aber nicht hinbekommen. Er hat die Formel dann selbst hingeschrieben und dann war auch mir alles sonnenklar.)

Wie sieht die Aktivierungsfunktion im Kohonennetz aus?
- Netto input

Werden alle Neuronen aktiviert?
- Nein nur das Neuron dessen Gewichtsvektor dem Eingabevektor am ähnlichsten ist (Zuerst habe ich die Nachbarn als mitaktivierte Neuronen beschrieben, den Fehler aber selbst gemerkt und bei der Gelegenheit noch die Lernregel und das Mitlernen der Nachbarneuronen erklärt.)

Professor Helbig ist ein ruhiger und freundlicher Prüfer. Wenn er einen Schwachpunkt entdeckt hat, lässt er allerdings nicht locker, bis er das Thema mit dem Prüfling "erarbeitet" hat. Darauf sollte man sich einstellen und sich nicht so nervös machen lassen, wie ich es dadurch geworden bin. Ein Hänger spiegelt sich weniger in der Note wieder, als die Art, wie man mit dem Hänger umgeht. Er hat mir als Tip mitgegeben, als zentralen Ausgangspunkt für den BP-Algorithmus die Fehlerfunktion und das damit verbundene Optimierungsproblem zu nehmen. Dann ist die Differenzierbarkeitsforderung an die Fermifunktion auch einfach motiviert. Die erweiterte Deltaregel hätte er dann schon

nicht mehr wissen wollen, weil die komplizierter ist. Ich habe es mir mit meiner Konzentration auf den Algorithmus und die Lernregel also selbst unnötig schwer gemacht. Dieser Teil der Prüfung wäre alleinstehend mit einer 2 benotet worden. Für meine starken Hänger im mathematischen Bereich fand ich das sehr fair.

Sicherheit im Internet (1866) - Dr. Kern-Isberner

Was sind die Schutzziele?
Was sind konkrete Bedrohungen im Internet?
Welche Netztopologien gibt es und welchen Einfluss auf die Sicherheit haben sie?

Welche grundsätzlichen Verschlüsselungsverfahren gibt es?
- symmetrische private key - Verfahren (Prinzip und Vor-/Nachteile erklärt)
- asymmetrische public key - Verfahren (Prinzip und Vor-/Nachteile erklärt)

Kann ich nicht aus dem public key den private key berechnen?
- Nein. RSA und Idee der Primfaktorzerlegung erklärt

Wie lässt sich der RSA - Algorithmus mathematisch herleiten? (Auf dieser Detaillierungsebene musste ich passen)

Wie sieht denn im allgemeinen das Feistelschema aus?
(Zeichnung und grundsätzliches Prinzip haben gereicht)

Wie funktioniert denn die Authentifizierung mit public key verfahren?
- Digitale Signatur
- Fingerprint (Hashwert der Nachricht) und Nachrichtenaustausch erklärt

Sie sind Sicherheitsbeauftragte in einem Unternehmen. Wie gehen Sie Ihre Aufgabe an?
- Sicherheitsprozess erklärt

Was macht eine Firewall?
Worauf muss ich bei der Konfiguration einer Firewall achten? (Habe erklärt, dass ich Zugriffe auf Paket- und Portebene, evtl. auch Anwendungsebene filtern muss. Auch, dass man entweder alles erlaubt, was nicht verboten ist, oder umgekehrt. War die letzte Frage und ich bin nicht sicher, ob sie das wirklich hören wollte.)

Frau Dr. Kern-Isberner ist eine ruhige und faire Prüferin. Sie bohrt nicht lange in einer Schwachstelle, sondern wechselt dann das Thema. Sie versucht möglichst viele Bereiche des Kurses zu prüfen. Es war meine dritte Prüfung bei ihr, und diese Erfahrung habe ich in allen Prüfungen gemacht. Man sollte sich darauf einstellen, einen sehr guten Gesamtüberblick bis zur letzten Seite des Kurses zu haben. Formelwissen ist für eine glatte 1 bei ihr auch notwendig. Dieser Teil der Prüfung wäre allein stehend mit einer 1,3 bewertet worden.