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