Grundlagen der Sicherheit

1. Was beinhaltet der Begriff der Sicherheit? Nennen Sie mindestens drei Aspekte.

- Verlässlichkeit der zu erbringenden Dienstleistungen in der gewünschten Qualität
- Schutz der Daten gegen Änderungen aus Versehen, mit Absicht oder aufgrund von Mängeln der Technik
- Zugang zu den Daten nur für berechtigte Personen auf berechtigte Art und Weise

2. Was wird unter Authentifizierung verstanden, was unter Autorisierung und was unter Identifizierung?

- Authentifikation: Prüfung der Identität des Subjekts
- Autorisierung: Zuordnung von Rechten an Subjekte in Bezug auf Objekte
- Identifizierung: Bestimmung der beteiligten Person (Identität der Subjekte)

3. Womit beschäftigt sich primär der Datenschutz? Datenschutz ergänzt Sicherheit noch durch:

- Beschränkungen für Personen mit erlaubten Zugang
- Beschränkungen der Datenerfassung, Abgleich und Weitergabe (jedoch nur für Daten mit Bezug auf Personen)

4. In welchen Schritten können Hacker systematisch von außen in ein Netzwerk eindringen? Skizzieren Sie eine sinnvolle Methodik.*

- Schritt 1: Auskundschaften (Suchmaschinen, Mitarbeiter, News,...)
- Schritt 2: Analyse des technischen Ziels (Scans, Analyse v. Servern/Bannergrabbing,...)
- Schritt 3: Angriffe (Ausnutzen v. Lücken, Denial of Service)
- Schritt 4: Übernahme des Systems (Backdoor, modifizieren v. Rechten, Rootkits, ...)

5. Welches ist das schwächste Glied in der Sicherheitskette?

- "2/3 aller ernsthaften Probleme entstehen durch die eigenen Mitarbeiter/innen."

6. Auf welchen Mängeln von Systemen beruht das Hacken von Computern in Netzen?

1. Qualitätsmängel in der Herstellung der Software
2. Beispiel: Bufferoverflow-Probleme
3. Qualitätsmängel bei der Konzeption
4. Bewusst in Kauf genommene Mängel durch das Management
5. Beispiele: Reduktion des Budgets, Terminverkürzungen
6. Konfigurationsmängel

7. Beispiele: Kein Einfahren von Aktualisierungen, Beibehalten von Standard-Passwörtern, Ausschalten von Sicherheitslösungen, z.B. Virenscanner

7. Was ist ein klassischer Virus? An welchen Stellen können in einem System Viren existieren?

- Programmstück, das sich an ein anderes Programm anfügt oder teilweise überschreibt und neben seiner Verbreitung eine Aktion durchführt
- Ein Virus kann z.b. den Read()-Syscall manipulieren, um so eigenen Code auszuführen

8. Was ist ein Trojaner, was ist eine Hintertür (backdoor)?

- Trojaner = Programm(teil), das neben einer offensichtlichen eine versteckte Funktion ausführt
- Back Doors = Server, die nach Außen Dienste anbieten und dies möglichst versteckt tun

9. Was sind Würmer (bei Netzwerken)?

- Würmer = Programme, die von Rechner zu Rechner - auch Plattformübergreifend – kopiert werden und auf jedem Rechner eine Aktion ähnlich den von Viren durchführen

10. Sind die heutigen Viren, die auf Visual Basic beruhen, wirklich Viren? Wie könnten Sie besser kategorisiert werden?

- Würmer, da sie sich verteilen

11. Was wird unter Malware verstanden? Und was unter Spyware? *Malware = Shadprogramme, Zusammenfassung von (Trojanern, Back Doors, Viren, Würmer, Spyware)* Spyware = Software, die Daten über die Benutzung des Rechners sammelt und an Dritte übermittelt oder durch Identifizierung diese Sammlung erst ermöglicht

12. Wie arbeiten Anti-Viren-Programme? Und woher kennen eigentlich die Hersteller von Anti-Viren-Programmen die Viren bzw. die Malware? Schreiben sie diese selbst?

- Erkennung: Mustererkennung (Signaturen) durch Virenscanner, Heuristiken (problematisch)
- Woher? : Honeypot, selbst geschrieben => unbewiesende Behauptung (eher unwahrscheinlich)

13. Was ist ein Hoax?

- Hoax: Scherzhafte oder böswillige Warnung vor einer fiktiven (Viren-)Gefahr

14. Mit welchen technischen Verfahren kann die Authentifizierung realisiert werden? Nennen Sie drei Beispiele unterschiedlicher Verfahren.

- Passwörter
- Standard, eingabe eines Passworts auf einer Website
- Chipkarten
- EC Karte
- Biometrie

- Fingerabdruck-Scanner

15. Bei der Biometrie werden typische Eigenschaften des Körpers einer bestimmten Person erfasst und zur Prüfung der Identität benutzt. Welche technischen Probleme haben heute biometrische Verfahren?

- Lassen sich teilweise einfach fälschen (siehe CCC Fingerabdruck)
- Abgeschnittener Daumen
- Unsicher, Ungenau, hohe Fehlerrate
- Nichterkennug von Lebendigkeit

16. Welches Problem aus der Sicht des Datenschutzes ist mit biometrischen Daten verbunden - außer dass sie personenbezogen sind? Skizzieren Sie eine (fiktive?) Missbrauchsmöglichkeit biometrischer Daten.

- Fingerabdruck lässt sich nicht ändern, falls ihn jemand klaut
- Nachweisprobleme, dass man es bei Missbrauch nicht selbst war
- Biometrie lässt sich "klauen" (Augen ausscharben) und "fälschen"

18. Was passiert beim Social Engineering? Durch welche Maßnahmen lässt sich die Wahrscheinlichkeit für Social Engineering in einem Unternehmen vermindern? Lässt sich Social Engineering grundsätzlich verhindern?

- Systematisches Auskundschaften des (sozialen) Umfelds der Organisation oder der Personen, die Zugang zum gewünschten System haben, sowie das Ausnutzen dieser Erkenntnisse [S. 32]
- Es lässt sich nicht grundsätzlich verhindern
- Mitarbeiter schulen (nie Passwörter rausgeben etc.), Administratoren gut bezahlen

19. Was machen Port Scanner und was Sniffer?

- Port Scanner scannen Ports von Computern und Servern mit Hilfe verschiedener Methoden (ICMP-Flags)
- Sniffer sammeln Netzwerkspackete und analysieren diese gegebenenfalls

20. Beim Surfen im Web sind aktive Inhalte problematisch. Nennen Sie mindestens zwei Beispiele mit ihren Gefahren.

- Aktive Inhalte = Programme als Teile von anderen Daten, die (unkontrolliert) nach dem Laden gestartet werden
- Javascript → XSS
- Cookies → Session-Hijacking
- Java, Flash → Sicherheitslücken (Buffer-Overflow)

21. Was ist ein Quarantäne-Rechner? Wären Netze aus Quarantäne Rechnern sinnvoll? Falls ja, für welche Zwecke?

- Rechner der nicht an das Netzwerk eines beispielsweise Unternehmens angeschlossen ist und für den test neuer Software eingesetzt wird (damit andere Rechner nicht

infiziert werden)

- Ja, da um Software zu testen, die eine Kommunikation über Netzwerke realisiert

22. Was ist (IP-)Spoofing?

- Paket mit falscher Source-IP Adresse

23. Was passiert beim Denial-of-Service-Angriff? Was bei der verteilten Version?

- Denial of Service-Angriff = DoS-Angriff = Eine Funktion oder ein ganzes System wird außer Kraft gesetzt oder so gestört, dass die Dienstleistung nicht erbracht werden kann (Große Anzahl von Paketen, fehlerhafte ICMP Packete, fehlerhafte Handshakes)
- Distributed = das gleiche auf mehreren Systemen (Brief-Bomben, Große Anzahl verteilter Pakete)

24. Welche Aufgaben hat eine Firewall?

- Pakete anhand festgelegter Regeln filtern und somit keine unerwünschten Pakete erhalten/senden

25. Was ist eine Demilitarisierte Zone (DMZ)? Was ist ein Grenznetz?

- Grenznetz deutsche Bezeichnung für DMZ
- enthält Bastionen, Server mit Schutzfunktionen und Server mit öffentlichem Zugang

26. Eine Firma betreibt einen eigenen Webserver. Wie würden Sie diesen Webserver mit Firewalls schützen?

- Server in DMZ, auf keinen Fall in gleichen Netzwerk wie Firmenrechner
- Ein Firewall vor und eine hinter den Webserver, hinter 2. Firewall kommt lokales Netz

Passwörter

1. Was ist eine Identität? Worin besteht beim Einloggen an Rechnern die Identifizierung und worin die Authentifizierung?

- Identifizierung: Bestimmung der beteiligten Personen (Identität der Subjekte)
- Authentifikation: Prüfung der Identität des Subjekts
- Identifizierung ist der Benutzername und Authentifizierung das Passwort

2. Was wird unter Autorisierung verstanden?

- Autorisierung: Zuordnung von Rechten an Subjekte in Bezug auf Objekte

3. Worin besteht der wesentliche Unterschied zwischen einem Passwort und einem Schlüssel?

- Passwort stellt die Identität des Benutzers fest
- Schlüssel beinhalten alle möglichen Bitkombinationen, während Passwörter nur

eingeschränkte Bitkombinationen (Zeichensatz) verwenden

- Schlüssel sind in der Regel länger als Passworte
- Schlüssel kann die Integrität von Daten durch eine Signatur sicherstellen

4. Was sind die Kriterien eines guten Passworts? Nennen Sie drei Kriterien, die maschinell geprüft werden können.

- Länge, Unterschiedliche Zeichen (Großbuchstaben, Kleinbuchstaben, Sonderzeichen), Kein Wort natürlicher Sprache

5. Skizzieren Sie ein Merkverfahren für einigermaßen gute Passwörter, die auch vergessliche Menschen behalten können (sollten).

- Einen Satz (z.B. ein Zitat oder eine Zeile aus einem Gedicht) bei dem nur die Anfangsbuchstaben der Wörter genommen werden und diese inkl. Satzzeichen zu einem Passwort zusammengesetzt wird
- Leet-Speak

6. Welcher Vor- und welche Nachteile hat ein zwangsweises häufiges Ändern der Passwörter?

- Vorteile: ein Angreifer der Zugriff auf ein System hat kann nicht mehr zugreifen nachdem das Passwort geändert wurde (es sei denn er hat sich schon anders Zugriff beschafft)
- Nachteile: Passwörter können vergessen werden, vertleitet dazu besonders einfache Passwörter zu benutzen oder sich diese aufzuschreiben **7. Beschreiben Sie die prinzipiellen Vorgehensweisen bei der Passwortdefinition und Prüfung, wenn (a) DES oder (b) MD5 verwendet wird.**
- MD5: PW nehmen, verschlüsseln, Hashen, Hash wird abgelegt (PW wird also nicht im Klartext abgelegt)
- DES: im Prinzip das Selbe…

Angriffe

8. Wie arbeitet der Wörterbuchangriff? Gehört dieser zu den Brute Force Methoden?

- Alle Einträge eines Wörterbuchs (Worte, Silben, …) in die entsprechende Passwortform (MD5, DES, …) überführen und es mit dem vorhandenen Passwort abgleichen
- Nein, da eine übersichtliche Menge an Daten (nicht alle Kombinationen der definierten Zeichen) verwendet wird und diese nicht erst generiert werden wie bei Brute Force

9. Was ist bei der Verschlüsselung von Passwörtern das Salz? Wozu dient es? Muss es geschützt werden?

- Salz = Zufälliger, dem Angreifer (möglichst) unbekannter Wert, der in die Verschlüsselung eingeht
- Durch den zufälligen Anteil entstehen verschiedene Hashwerte aus Passwörtern
- Es muss geschützt werden, kann unter bestimmten Bedingungen aber auch bekannt

sein (siehe Linux Passwörter)

10. Welchen gravierenden Nachteil haben Key-Stores (verschlüsselte Dateien mit Passwörtern), die nach einer initialen Eingabe des Schlüssels eine ganze Sitzung lang benutzt werden können?

- Wenn Masterkey bekannt dann Zugriff auf alle Passwörter die gespeichert sind
- durch Schadsoftware auf dem System nach dem Öffnen auslesbar
- durch Kopierbarkeit Brute-Force/Wörterbuchangriff-anfälliger

11. Nennen Sie mindestens zwei Passwort-Crack-Werkzeuge.

- John the Ripper, Hashcat, Cain & Abel

12. Beschreiben Sie den typischen Infektionsweg von VBA-Viren.

- Word Dokumente (Makro)

13. Charakterisieren Sie die Idee, die hinter einem Bufferoverflow-Angriff liegt. Welcher Fehler ist die Ursache für solche Möglichkeiten?

- Bufferoverflow = Programmierfehler, der dazu führt, dass zu viele Daten in einen Puffer gelesen und dadurch Bereiche dahinter überschrieben werden
- Keine Überprüfung der Eingabelänge

14.Warum ist das Montieren von externen Datenträgern mit einem Filesystem bei jedem Betriebssystem kritisch? Worin besteht dabei das Problem?

- Auf dem Datenträger kann ein Betriebssystem sein welches beim Bootvorgang gestartet wird. Von diesem kann auf das Dateisystem des Rechners zugegriffen werden. Hier können nicht nur Daten kopiert sondern ggf. auch verändert werden (z.B. Installation eines Rootkits/Trojaners)
- Rechte des eigentlichen Dateisystems werden nicht beachtet, wenn auf dem externen Datenträger beispielsweise eine Linux-Live Distribution gestartet wird

15. Skizzieren Sie die Smurf-Attacke. Was wäre das Ziel dieser Attacke? Wie lässt sie sich verhindern?

Es handelt sich um einen DoS-Angriff, der mit Broadcast-Pings versucht ein bestimmtes System zu stören

Ablauf:

1. Zusammenbau eines Ping-Paketes
2. Zusammenbau eines IP-Paketes mit Absender-Adresse des Opfers (Spoofing)
3. (Mehrfaches) Absenden des Paketes mit Broadcast-Adresse

Folge:

- Die meisten Systeme schicken ein ECHO Reply an das Opfer, das mit einem Schlag eventuell hunderte von IP-Paketen bekommt

- Jetzt entscheidet die Implementierungsgüte des TCP/IP-Stacks über Leben und Tod
- Verhinderung: Broadcast durch Router nicht zulassen

16.Was wird unter OS-Fingerprinting verstanden? Was für ein Ziel wird bei derartigen Verfahren verfolgt? Durch dieses Verfahren werden anhand von Netzwerkreaktionen des Zielsystems Rückschlüsse auf das eingesetzt Betriebssystem gezogen. z.B. wie das System auf einen fehlerhafter Verbindungsaufbau zum Port 443 reagiert. Sobald man das Betriebssystem kennt, kann man versuchen, bestimmte Sicherheitslücken dieses Betriebssystems auszunutzen.

17.Was ist Banner Grabbing? Was für ein Ziel wird bei derartigen Verfahren verfolgt? Beim Zugriff auf FTP-Server, Webserver o.Ä. wird manchmal ein Banner (Einleitungstext) mit der Softwareversion und weiteren Informationen mitgesendet. Diese Informationen können teilweise sensible Daten (Version ,...) beinhalten und somit von Angreifern für spezialisierte Exploits ausgenutzt werden.

Rechtesystem von Unix

18. Wie werden Benutzer und wie Gruppen in Unix intern identifiziert? Wo werden diese definiert?

- /etc/group Datei (Zuordnung Benutzer: alle Gruppen-Id's)
- Durch Benutzer-Id uid und Gruppen-Id gid

19. Was waren die Gründe für die Einführung des Shadow-Systems? Was macht der Login-Prozess beim Shadow-System anders als beim alten hergebrachten System?

- Separierung der Informationen für Login und Benutzer
- Shadow-System dient dem Schutz der /etc/passwd-Datei, in der die Zugangspasswörter der Benutzer des UNIX-Systems abgelegt sind.
- Trennung von user id und (verschlüsselten) Passwörtern in zwei Dateien Zuordnung unterschiedlicher permissions

20. Für die Repräsentation der Rechte in UNIX reichen 9 bit. Welche Bedeutung haben diese?

- 3Bit User, 3Bit Group 3Bit Other
- Bit 1: Read, Bit 2: Write, Bit 3: Execute

21. Beschreiben Sie den Algorithmus zur Bestimmung der Rechte eines Prozesses, wenn dieser eine Datei eröffnet.

- Überprüfung in der Reihenfolge: User? Group? Other!
- syscall open -> Datei öffnen -> entspricht UID == Datei UID -> owner GID == GID -> Group...

22. Welche Wirkungen haben die Set-UID bzw. Set-GID-Bits?

- Leider benötigen einige harmlose Programme root-Rechte, z. B. mkdir oder rmdir.

- Daher werden pro Prozess zwei weitere 16-bit-Werte eingeführt: Effektive UID und effektive GID.
- Diese bestimmen die wirksamen Rechte. Die bisher vorgestellten IDs heißen reale UID und reale GID.
- Wird eine ausführbare Datei gestartet, so läuft folgendes Verfahren ab:
- Ist ein Set-UID-Bit der Datei zugeordnet, erhält der Prozess als effektive UID die UID des Datei-Owners.
- Ist ein Set-GID-Bit der Datei zugeordnet, erhält der Prozess als effektive GID die GID der Datei-Gruppe.
- Ist kein Set-Bit gesetzt, behält der Prozess seine alten UID/GIDWerte.
- Initial sind reale und effektive UID/GID gleich.

23. Warum wurden die Set-UID bzw. Set-GID-Bits eingeführt?

- Damit können für ein Programmlauf besondere Rechte ausgeliehen werden.

24. Welche Sonderregelungen betreffen Prozesse mit einer UID = 0?

- 0 gehört Root

Scanner

1. Was ist allgemein ein Scanner? Was ist dabei ein Netzwerk- und was ein System-Scanner?

- Scanner = Programm, das ein System systematisch auf Schwachstellen oder Probleme prüft und teilweise repariert
- System-Scanner = Scanner, der als Teil des zu analysierenden Systems arbeitet, z. B. von CDROM gestartet
- Netzwerk-Scanner = Scanner, der Systeme über Netze scannt
- Prüfen der Erreichbarkeit von Servern, z.B. Drucker
- Prüfung von Firewalls (offene Ports)

2. Nennen Sie mind. vier Schwachstellen, die ein guter System-Scanner aufdecken sollte.

- Fehlende Passwörter
- Zu leichte oder zu kurze Passwörter
- Laxe/fehlerhafte Dateirechte, z. B. suid root von Benutzerprogammen
- Laxe/fehlerhafte Konfigurationen, z. B. fehlerhafte .htaccess-, host.equiv-Dateien etc. oder freies Upload bei FTP-Servern
- Viren, Trojanische Pferde
- Modifikationen von Programmen

3. Nennen Sie ein Beispiel für einen System-Scanner - außer Viren und Spywarescannern.

- tiger, tara

4. Was ist ein Exploit und was ein Rootkit?

Exploit: systematische Möglichkeit, Schwachstellen auszunutzen, die bei der Entwicklung eines Programms nicht berücksichtigt wurden. Meist um sich Zugang zu Ressourcen zu verschaffen oder in Computersysteme einzudringen, bzw. diese zu beeinträchtigen.

Rootkit: Sammlung von Programmen, die Teile des Betriebssystems ersetzen, um einen leichten Zugang von außen zu realisieren

5. Exploits sind häufig frei im Internet verfügbar. Mit welcher Begründung werden diese Exploits von den Autoren veröffentlicht? Was spricht gegen die Veröffentlichung im Internet?

1. Dafür: Um den Druck für dessen Behebung aufzubauen
2. Dagegen: Ausnutzung des Exploits durch "jedermann"

6. Bei den Rootkits gibt es mehrere Gefährlichkeitsstufen - skizzieren Sie für drei Stufen die technische Verfahrensweise des Rootkits.

- Application-Rootkits = bestehen lediglich aus modifizierten Systemprogrammen.
- Kernel-Rootkits = ersetzen Teile des Kernels durch eigenen Code, um sich selbst zu tarnen und dem Angreifer zusätzliche Funktionen zur Verfügung zu stellen, die nur im Kontext des Kernels ausgeführt werden können.
- Userland-Rootkits = Sie stellen jeweils eine DLL bereit, die sich anhand verschiedener API-Methoden direkt in alle Prozesse einklinkt. Ist diese DLL einmal im System geladen, modifiziert sie ausgewählte API-Funktionen und leitet deren Ausführung auf sich selbst um („redirect"). Dadurch gelangt das Rootkit gezielt an Informationen, welche dann gefiltert oder manipuliert werden können.
- Speicher-Rootkits = existieren nur im Arbeitsspeicher des laufenden Systems. Nach dem Neustart des Systems sind diese Rootkits nicht mehr vorhanden.

7. Nennen Sie mindestens zwei Beispiele für Netzwerk-Scanner.

- nmap, strobe, ping, traceroute, Xprobe2, SuperScan

8. Was lässt sich alles mit nmap innerhalb des eigenen LANs herausfinden?

- offene Ports (TCP, UDP)
- Rechner (IPs) im Netz
- Fingerprint einer Anwendung (Banner-Grabbing) nach erfolgreichem 3-Wege-Handshake (TCP)
- OS-Detection

9. Wie lassen sich Ports von Systemen scannen, ohne dass das scannende System als solches in den Logfiles auftaucht? Skizzieren Sie eine Möglichkeit. Ist das auch ein praktikables Verfahren?

- Es wird eine unbelastete Maschine M gesucht
- Diese wird mit hping -r (Verwendung inkrementeller IP-IDs) beobachtet: Steigen die IP-IDs um 1, so ist M unbelastet
- Die Hacker-Maschine H überwacht mit ping M kontinuierlich und wertet die IP-ID-Differenzen aus
- Die Hacker-Maschine H testet parallel einen Port auf der Opfermaschine O mit der Absenderadresse von M
- Antwortet O an M (und arbeitet sonst niemand auf M), so ist IP-ID um 2 erhöht, was durch das ping durch H festgestellt wird
- Mit einem gewissen Risiko können die Ergebnisse als ein Portscan ausgewertet werden.

10. Wie arbeitet beim Portscannen ein Full-connect- und wie ein Halfconnect-Scann?

- Protokollablauf (H = Hackerhost, O = Opferhost)
- 1. H->O: SYN-Paket
- 1. O->H: SYN/ACK oder RST
- RST: Entweder zu diesem Zeitpunkt kein Verbindungsaufbau möglich oder "mit DIR rede ich nicht"
- Ist der Port geschlossen, gib es eine ICMP-Meldung oder gar nichts
- 1. H->O: ACK
- 1. O->H: Banner etc.
- 1. H->O: ACK und Abbau mit ordentlichen FIN
- bei Half-Connect wird bei Schritt 3 FIN mitgeschickt (Schritt 4 findet nicht statt) 5 wieder wie oben

11. Wie arbeitet der Xmas-Scan und wie der NUL-Scan?

- Xmas-Scan:
- Protokollablauf: Es wird ein FIN-Paket mit allen Flags gesetzt gesendet.
- Darauf muss bei geschlossenem Port mit einem RST geantwortet werden, ansonsten wie bei FIN-Scan.
- Null-Scan:
- Protokollablauf: Es wird ein FIN-Paket ohne ein einziges gesetztes Flag gesendet
- Darauf muss bei geschlossenem Port mit einem RSTgeantwortet werden, ansonsten wie bei FIN-Scan

12. Was macht der Scanner SATAN?

- Prüft Schwachstellen bei FTP, TFTP, NFS, Rsh, (R-Tools), Sendmail, X
- Ähnlich wie Nessus

13. Was prüft SAINT als Weiterentwicklung von SATAN über SATAN hinaus?

- CGI-Probleme

- DoS-Angriffe
- POP-Server-Probleme
- SSH-Probleme
- Pufferüberläufe

14. Nessus arbeitet mit vielen Plugins. Was wird in diesen definiert?

- Plugins erweitern Nessus um weitere Tests

15. Die Plugins sind eine der Ursachen für den Erfolg von Nessus. Wie entstehen diese Plugins? Wie werden sie realisiert?

- Die Plugins werden in NASL oder C geschrieben, davon ca. 99% in NASL (Nessus Scripting Language)
- Damit kann Nessus sehr leicht auf aktuelle Probleme bzw. Lücken angepasst werden
- Werden von der Community gemacht

16.Wie arbeitet Nessus? Skizzieren Sie dazu die globale Software-Architektur und erläutern Sie daran, was zu einem Scann alles gehört.

- Client: Über Browser gesteuert
- Server: Läuft als Dienst im Hintergrund und erledigt Scann
- Plugins: Erweiterung um Module zum Scanner bestimmter Schwachstellen

17.Gibt es für Scanner Tests, die für das zu scannende System gefährlich sein könnten? Falls ja, nennen Sie mindestens zwei Beispiele.

- Ping of Death: Senden eines fehlerhaften ICMP-Paketes (führt zu Bufferoverflow)
- Smurf-DoS-Attacke: Kurzeitig hohe Belastung des Netzes

Intrusion Detection Systeme (IDS)

1. Was wird unter einer Intrusion verstanden? Nennen Sie auch andere Erklärungen dieses Begriffs. Was spricht für den Begriff Incident? Was würde dieser bedeuten?

- Intrusion (Störung, Verletzung, Eindringen) = Erfolgreicher lesender oder schreibender, aber nicht erlaubter Zugriff auf Daten bzw. Ausführung von Programmen durch organisationsfremde Personen, also von Außen
- Misuse = Missbrauch = Erfolgreicher lesender oder schreibender, aber nicht erlaubter Zugriff auf Daten bzw. Ausführung von Programmen durch Personen der eigenen Organisation, also von Innen
- Incident = Zusammenfassender Oberbegriff von Intrusion und Misuse, Vorfall, bei dem etwas unerlaubtes geschah

2. Nennen Sie mindestens fünf Aufgaben, die ein gutes IDS realisieren sollte.

- Feststellen

- Erkennen aktuell laufender Angriffe
- Erkennen früher erfolgter Angriffe
- Feststellen von nicht erlaubten Modifikationen und Zugriffen
- Analyse der Probleme und deren Einschätzung
- Reagieren
- "Unterbrechen" betroffener Verbindungen, Abschotten
- Beenden betroffener Prozesse, z. B. Ausloggen und Sperren des betreffenden Logins
- Berichten bzw. Melden
- Zusammenfassung verschiedener Datenbestände
- Erstellung Berichte unterschiedlicher Detailliertheit
- Versenden von Alarm-Nachrichten, z.B. Mail, SMS

3. Wie kann ein IDS feststellen, warum eine Modifikation bestimmter Dateien während eines Angriffs erfolgte?

- Weil eine Kopie der Datei / einen Hash vorher erstellt wurde mit der das IDS die aktuelle Datei / den Hash in bestimmten Zeitabständen abgleicht
- Kann nur ein Mensch feststellen, warum eine Modifikation der Datei vorgenommen wurde

4. Was wird im Rahmen des Computer Forensics getan? Nennen Sie mindestens zwei typische Arbeiten.

- Erfassen von relevanten "Spuren"
- Beweis der Originalität der Spuren, d.h. dass Spuren nicht nachträglich verändert oder geschaffen wurden
- Nachweis der Herkunft der Spuren

5. Nennen Sie mindestens drei Beispiele für Anomalien, die Hinweise auf eine Intrusion liefern, und erläutern Sie für welche Ereignisse diese Anomalien Indizien sind.

- [Anomalie = außergewöhnliches Verhalten (von Software) Anormal ist ein Verhalten, das sich vom "Durchschnitt" wesentlich unterscheide]
- Ein verreister Mitarbeiter loggt sicht ein -> nicht der Mitarbeiter sondern Hacker
- Eine langschläfrige Mitarbeiterin loggt sich um 7:00Uhr früh ein -> nicht der Mitarbeiter sondern Hacker
- Zugriff auf Daten aus Backups -> Daten werden geklaut

6. Worin unterscheiden sich die NIDS von den HIDS? Scannen die NIDS ein Netzwerk?

- Host-basierte IDS = HIDS = IDS zur Überwachung eines Systems, wobei das IDS auf diesem System auch arbeitet
- Netzwerk-basierte IDS = NIDS = IDS zur Überwachung von Netzwerkverbindungen
- vor einer Firewall ("draußen")
- hinter einer Firewall in der DMZ

- in Netzsegmenten des Innenbereichs
- Nein, die NIDS scannen kein Netzwerk

7. Eine Firma hat ein lokales Netzwerk und über eine Firewall einen Anschluss ans Internet. Wo könnten die HIDS und wo die NIDS sinnvollerweise positioniert werden?

- HIDS:
- alle Server und Endgeräte wo Kommunikation von außen stattfindet
- Firewalls
- NIDS:
- hinter der Firewall

8. Was ist ein Honeypot? Durch welche Maßnahmen bzw. welche Art von Software wird ein Honeypot typischerweise realisiert?

- Honeypot = Spezielles System, das absichtlich Angriffe zulässt, um die Art und Technik der Angriffe studieren zu können
- Rechner mit "gewollten" Sicherheitslücken
- Software mit Monitor-Funktion
- Virtuelle Machine

9. Eine Firma hat ein lokales Netzwerk und über eine Firewall einen Anschluss ans Internet. Wo sollten sinnvollerweise die Honeypots positioniert werden?

- Honeypot = Spezielles System, das absichtlich Angriffe zulässt, um die Art und Technik der Angriffe studieren zu können
- vor der Firewall
- hinter einer Firewall in der DMZ

10. Wie kann ein IDS zu einem DoS-Angriff mißbraucht werden? Ist das zu verhindern?

- Absichtlich produzierte Fehlalarme
- Einschränkung bei der Überwachung von Ports, Fehlermeldungen, etc.

11. Was ist eine Policy? Welche Aufgabe wird mit der expliziten Formulierung von Policies gelöst?

- Policy = Politik = Sicherheitsrichtlinie oder Regelsystem, das den Umgang mit der EDV aus dem Blickwinkel der Sicherheit festlegt
- was ein Angriff ist,
- wie der Schutz vor Angriffen gestaltet werden soll,
- wer was tun darf bzw. muss (Rechte/Pflichten)
- Dies betrifft häufig Rollen innerhalb von Organisationen.
- Organisatorische Aspekte der Sicherheit, z.B. Aufgaben des Sicherheitsbeauftragten

12. Die Software tripwire gehört zu der Gruppe der HIDS. Wie arbeitet tripwire?

1. Policy für die Überwachung definieren (twpol.txt, twpol)
2. Datenbank der zu überwachenden Dateien erstellen ()
3. tripwire starten und Logdateien regelmäßig überprüfen

13. Wie können IDS, wie z.B. tripwire oder aide, selbst angegriffen werden? Durch welche Maßnahmen können Sie diese Gefährdung abwenden (nennen Sie zwei Möglichkeiten)?

- Angriff: provozierte Fehlalarme, Sicherheitslücken in der Software, Änderung der Policy-Datei
- Gegenmaßnahmen: Hashen der Policy Datei und speichern des Schlüssels auf einem USB-Stick

14. Die Software snort ist ein NIDS. Kann snort Portscanns erkennen? Wie arbeitet snort?

- Snort kann Portscanns erkennen, wenn die ICMP-Pakete vom selben Host an verschiedene Ports des Systems in kurzen Zeitabständen kommen

15. Kann snort Zugänge bei Feststellung eines Angriffs sperren?

- Snort kann keine Zugänge sperren, sondern nur Netzwerkverkehr analysieren und auswerten

Firewalls

1. Was wird allgemein unter einer Firewall verstanden?

- Firewall = Gerät, Betriebssystemkomponente oder Programm, das oder die eine Zugriffskontrolle mit Hilfe eines Filters realisiert

2. Worin besteht der Unterschied zwischen einer Proxy-Firewall und einem Packet-Filter?

- Packet-Filter = Firewall, die Pakete der Ebenen 3 und/oder 4 ohne Betrachtung der Dateninhalte prüft
- Proxy-Firewall = Firewall, die Pakete der Ebenen 3, 4 bis 7 einschließlich der Daten prüft
- Typische Aufgaben der Proxies in Firewalls sind:
- Prüfung auf aktive Inhalte bei HTTP
- Prüfung auf "ungesunde" Kommandos bei SMTP oder FTP
- Prüfung auf zulässige Web Services, z. B. über SOAP

3. Skizzieren Sie einen Angriff auf eine Firewall, der mit fragmentierten Paketen arbeitet.

- Tear-Drop:
- Kopf vom ersten Fragment in Ordnung, erlaubte Ports werden angesprochen und Paket

durchgelassen

- zweites Fragment kann bspw Portnummern des ersten Fragments überschreiben, wird aber auch durchgelassen, da 1. Fragment okay war

4. Skizzieren Sie Situationen, in denen das Verbieten von Fragmentierung bzw. das Unterdrücken von korrespondierenden zu Problemen führt.

- kein Standards für die maximale Packetgröße von IP-Paketen (MTU)
- verschiedene Hardware nutzt unterschiedliche Packetgrößen
- da der beste Durchsatz durch die Nutzung der maximalen Paketgröße erreicht wird, handelt die Software die Paketgröße mit den einzelnen Endgeräten aus
- deshalb ist der Verbot von IP-Fragmentierung und korrespondierenden Paketen nicht sinnvoll

5. Wie sähe eine allgemeine Architektur von Firewalls aus? Was wäre dabei der minimale und was der maximale Ausbau?

- Architektur: Das WAN wird über eine Firewall getrennt mit einem DMZ oder Intranet verbunden.
- Minimal: Komponente auf einem Host, dessen Netzschnittstellen mit Filtern versehen sind, und auf dem die zu schützenden Applikationen laufen
- Maximal: Aufteilung in äußeren und inneren Bereich

6. Was ist eine Personal Firewall? Kann diese mit Proxies arbeiten? Wo würden dann diese laufen?

- Personal Firewalls = Firewalls auf den Endsystemen.
- Diese Firewalls sind bei Ende-zu-Ende-Verschlüsselung notwendig.
- Leider müssen sie von den Benutzern administriert werden.
- Auch kommen häufig Benutzer mit den Meldungen der Firewalls nicht zurecht
- Ja, sie kann mit Proxies arbeiten, wobei die Firwall dann auf dem Proxy-Server eingerichtet wird und die Clients vor Angriffen/unsicheren Paketen schützt

7. Unter welchen Umständen kann auf Personal Firewalls nicht verzichtet werden? Wann würde daher eine zentrale Firewall beim Übergang in das betreffende Netz nicht ausreichen?

- Bei Ende-zu-Ende Verschlüsselung

8. Was wird unter einem Dual Homed Host verstanden?

- Dual-homed host: haben zwei Netzschnittstellen mit jeweils zwei Filtern

9. Worin besteht der Unterschied zwischen einem zustandslosen und einem zustandsbehafteten Packet-Filter?

- Zustandslose Firewall = stateless firewall = statische Firewall =
- Firewall, bei der jedes Paket isoliert von allen anderen untersucht wird
- Manchmal auch: stateless filtering genannt

- Kontextsensitive Firewall = statefull firewall = dynamische Firewall =
- Firewall, bei der mehrere im Zusammenhang stehende Pakete zur Grundlage der Entscheidung über das Filtern gemacht werden
- Manchmal auch: statefull filtering genannt

10. Welche Vor- und welche Nachteile hat ein statisches Packet-Filter? Und welche ein dynamisches?

Zustandslos

Vorteile

- Schnell – Einfache Regeln, überschaubar

Nachteile

- Leicht zu überwinden, z. B. mit Fragmentieren

Zustandbehaftet

Vorteile:

- Fängt sehr viel ab

Nachteile:

- Langsam
- Schwer zu implementieren
- Hohe Qualität schwer zu erreichen
- Für DoS-Angriffe gefährdet, da Tabellen überlaufen können (Was passiert in diesem Fall? Sperren? "Rückfall" in den zustandslosen Betrieb?

11. Welche Arten von Absenderadressen können bei einer Personal Firewall mit einem Übergang zum Internet von Außen in jedem Fall herausgefiltert werden? Nennen Sie drei Beispiele.

- (einzelne) Absenderadresse
- Adressbereich
- Absendernetz (Subnetz)

12. Welche Arten von Absenderadressen können bei einer Dual-Homed-Firewall, mit einem Übergang zum Internet, von Außen in jedem Fall herausgefiltert werden? Nennen Sie drei Beispiele.

- gleiche wie bei 11. ?

13. Welche Arten von ICMP-Paketen sollten als kritisch eingestuft und ihre Herausfilterung in Betracht gezogen werden bzw. welche ICMP-Pakete sind relativ ungefährlich?

- Ping ist von Fall zu Fall zu entscheiden

- Gefährlich
- Port (unreachable)
- alles was mit Routerkommunikation zu tun hat (es sein denn es gibt tatsächlich mehrere Router in dem Netzwerk)
- Ungefährlich
- Domain Name Request, Reply
- Timestamp, Reply
- Parameterfehler
- TTL

14. Was ist bei iptables eine Chain (Kette)? Skizzieren Sie den allgemeinen Algorithmus bei der Bearbeitung dieser Ketten.

- Eine Regelkette wird solange durchlaufen bis das Ende erreicht wird oder die erste Bedingung zutrifft (hierbei gibt es Ausnahmen).
- Eine Ausnahme sind Logging-Aktionen, nach denen weiter gelaufen wird.
- Bei einem Zutreffen der Bedingung wird eine Aktion durchgeführt.
- Ist das Ende einer Tabelle erreicht, wird eine allgemeine Regel angewandt: die Policy

15. Das Filtermodul von iptables arbeitet mit 3 Regelketten. Welche sind dies und welche Bedeutung haben diese?

Dirk

- Input: Alle Pakete die als Destination der eigenen IP-Adresse entsprechen
- Forward: Alle Packete die als Destination oder als Source nicht der eigenen IP-Adresse entsprechen
- Output: Alle Packete die als Source der eigenen IP-Adresse entsprechen

Messer

- Input-Chain: Filter für eingehende Pakete an Prozesse
- Output-Chain: Filter für ausgehende Pakete von Prozessen
- Forward-Chain: Filter für Pakete, die durchgeleitet werden

16. Was macht ganz allgemein das Kommando iptables?

- iptables setzt, ändert, löscht Regelen und Policies für die einzelnen Chains Input, Output und Forward

17. Worin besteht der Unterschied zwischen den iptables-Aktionen REJECT und DROP?

- Reject: Verwerfen und mit ICMP-Fehlermeldung ablehnen
- Drop: Verwerfen

18. Wodurch wird entschieden, ob ein empfangenes Paket durch die INPUT- oder durch die FORWARD-Chain „läuft“?

- Alle Pakete die als Destination der eigenen IP-Adresse entsprechen gehen in die Input-Chain und alle Pakete mit eine anderen Destination-Adresse gehen in die Forward Chain

Verschlüsselung und Zertifikate

1. Lassen sich allein mit symmetrischen Verschlüsselungsverfahren Dokumente signieren? Was ist das Charakteristische dieser Verfahren?

- Nein, da die Signatur nur bei der asymmetrischen Verschlüsselung funktioniert
- die Signatur wird für die zur Überprüfung der Integrität genutzt
- dazu wird ein privater Schlüssel benötigt, der einer Person zugeordent sein muss
- bei der symmetrischen Verschlüsselung kennen beide Personen den Schlüssel und bestitzen keinen privaten
- Symmetrische Verschlüsselung = Verschlüsselung mit einem Schlüssel zum Ver- und Entschlüsseln (SSL, DES, AES)
- Asymmetrische Verschlüsselung = Verschlüsselung mit einem öffentlichen Schlüssel und Entschlüsselung mit einem privaten Schlüssel

2. Wie arbeiten asymmetrische Verschlüsselungsverfahren?

- Bei der asymmetrischen Verschlüsselung wird ein Schlüsselpaar verwendet, das folgende Eigenschaften hat:
- Es ist zufällig gewählt.
- Aus dem einen Schlüssel kann nicht der andere rekonstruiert werden.
- Wenn ein Text mit dem einen Schlüssel verschlüsselt wurde, kann er nur von dem anderen entschlüsselt werden
- Einer der beiden Schlüssel wird öffentlich gemacht, der andere bleibt geheim:
- Public Key = Schlüssel einer Identität, der bekannt gegeben werden kann
- Secret Key = Geheimer Teil des Schlüsselpaares, der immer gegenüber allen anderen Identitäten geheim gehalten werden muss

3. Worin besteht der wesentliche Unterschied zwischen der symmetrischen und der asymmetrischen Verschlüsselung?

Bei der symmetrischen Verschlüsselung wird derselbe Schlüssel für die Ver- und Entschlüsselung verwendet. Diese murr beiden Teilnehmern bekannt sein. Bei der asymetrischen Verschlüsselung verfügen die Teilnehmer über ein Schlüsselpaar (Public- / Privatkey). Die Verschlüsselung erfolgt jeweils mit dem Public-Key des anderen Teilnehmers und die Entschlüsselung mit dem eignen Privat-Key.

4. Wie läuft das elektronische Unterschreiben eines Dokuments ab? Beschreiben Sie die einzelnen Schritte.

- Bilden eines Hash-Werts der zu verschickenden Nachricht

- Verschlüsselung mit Private-Key
- Versand der Signatur und der verschlüsselten Nachricht

5. Wie läuft die Prüfung einer elektronischen Unterschrift eines Dokuments ab? Beschreiben Sie die einzelnen Schritte.

- Empfangende Signatur des Hash-Wertes wird mit dem öffentlichen Schlüssel des Absenders entschlüsselt
- Ist Verifizierung erfolgreich, dann ist die Nachricht vom Absender

6. Was ist ein Schlüssel, was eine Signatur und was ein Zertifikat?

- Schlüssel
- Bitkette, deren Werte statistisch gleich verteilt und lang genug ist, um nicht unter definierten Bedingungen durch Ausprobieren bestimmt werden zu können
- Signatur
- Wird nun ein Fingerabdruck mit dem geheimen Schlüssel verschlüsselt, so wird das Resultat digitale Unterschrift oder Signatur genannt
- Eine Signatur ist deshalb eindeutig, da nur derjenige, der im Besitz des geheimen Schlüssels ist, in der Lage ist, sie zu erstellen.
- Zertifikat
- besteht aus Identität, öffentlichem Schlüssel der Identität und Signatur der CA

7. Welche Aufgaben hat eine CA? Wofür steht das Kürzel CA? Und was ist ein Trustcenter?

- Eine Certification Authority (CA) - oder Trustcenter genannt - hat ein Verzeichnis von öffentlichen Schlüsseln samt Identitätsbeschreibungen und beglaubigt die Verbindung zwischen Identität und öffentlichen Schlüssel durch ein Zertifikat.

8. Werden beim Erstellen einer Signatur die Nutzdaten verschlüsselt?

- Nur signieren: Nein

9. Lassen sich Zertifikate fälschen? Skizzieren Sie dazu ein Verfahren.

- Variante 1: in eine CA einbrechen und sich selbst eins ausstellen
- Variante 2: geheimen Schlüssel zum öffentlichen finden

10. Wie erhält eine Person das Zertifikat eines Schlüssels einer fremden Person? Nennen Sie mindestens zwei Möglichkeiten, die möglichst legal sind.

1. Server, der Cert hat übergibt es beim Handshake an den Client (falls Client ein Cert hat, kann er es auch gleich übergeben)
2. Zertifikats- und FTP-Server, wo Zertifikate runtergeladen werden können (da öffentliche Dokumente)

11. Unter welchen Umständen müssen Zertifikate noch innerhalb ihres Gültigkeitszeitraums zurückgenommen werden? Nennen Sie dazu zwei Beispiele.

- Geheimer Schlüssel der Identität ist aufgedeckt
- Identität wird von CA nicht länger akzeptiert
- Geheimer Schlüssel der CA ist aufgedeckt

12. Wie wird das Zurücknehmen ausgegebener Zertifikate realisiert? Was bedeutet das für den Prozess des Prüfens eines Zertifikats?

- Ein Rückruf muss bei der CA vorgenommen werden und wird in eine entsprechende Liste eingetragen
- Bei der Überprüfung des Zertifikats wird geprüft, ob es einen Rückruf zum Zertifikat gab

13. Was muss alles getan werden, um die Korrektheit eines Zertifikats prüfen?

- Wie kann sich Person A von der Glaubwürdigkeit des Zertifikats überzeugen? Indem A mit dem öffentlichen Schlüssel vom Trustcenter dessen Unterschrift prüft (mit demselben Verfahren, wie jede Unterschrift geprüft wird).
- Dadurch entsteht eine Kette von Zertifikaten, die sich jeweils – bis auf das erste – bestätigen. Das erste muss geglaubt werden

14. Warum sind im X.509-Zertifikat Angaben zu den verwendeten kryptographischen Verfahren enthalten?

- das Verfahren soll austauschbar bleiben, falls ein verfahren sich als angreifbar heraustellt soll einfach ein anderes benutzt werden können

15. In einem X.509-Zertifikat sind u.a. persönliche Daten, wie z.B. die EMail-Adresse enthalten. Ist das nicht Futter für die Spammer, die nun geprüfte Mailadressen erhalten?

- Ja
- Aber Attributzertifikate können helfen (Firmenintern)

16.Nennen Sie zwei symmetrische Verschlüsselungsverfahren, die weite Verbreitung gefunden haben.

- Diffie-Hellman-Verfahren
- RSA-Verfahren

17. Wenn zwei Personen über weite Entfernungen ihre Kommunikation mit einem symmetrischen Verfahren verschlüssel wollen: welches schwerwiegendes Problem muss dazu gelöst werden?

Sichere Übermittlung des Schlüssels.

18.Wie können zwei sich nicht persönlich kennende Personen ein Geheimnis, z.B. einen Schlüssel oder ein Passwort, austauschen, ohne dass Fremde das Geheimnis erfahren?

Mit dem Diffie-Hellman Verfahren (A und B einigen sich auf einem Prim- und natürliche Zahl welche öffentlich sind)

19. Skizzieren Sie das Prinzip des Man-in-the-Middle-Angriffs.

Der Kommunikationskanal zweier Teilnehmer wird durch einen dritten abgehört. Hierbei können die Nachrichten durch diesen auch manipuliert werden.

20. Beschreiben Sie ein möglichst sicheres Verfahren, mit dem Sie feststellen können, mit wem Sie kommunizieren.

Signierung mit asynchroner Verschlüsselung (Privatkey-Signierung eines Hashes).

21. Wie werden die Organisationen bzw. Firmen genannt, die Zertifikate heraus geben? Auf welche Weise prüfen diese Organisationen, ob die im Zertifikat angegebenen Personen tatsächlich die richtigen sind? Machen Sie dazu einen Vorschlag.

- CA - certificate authority
- Persönliche Identifikation gegenüber der CA (z.B. Personaldokumente z.B. Personalausweis)

22. Was wird unter einem Zertifizierungpfad verstanden?

- Die Echtheit und Unversehrtheit eines Zertifikates, also des mitgesendeten öffentlichen Schlüssels, wird über die Signatur des Herausgebers geprüft: Jedes persönliche Zertifikat ist von einem Trustcenter (CA) signiert. Ist diese Signatur gültig, wurde auch das Zertifikat nicht geändert. Natürlich kann auch die Echtheit des Herausgeberzertifikats geprüft werden, das oft wieder von einer anderen Instanz herausgegeben wurde.
- Ermöglicht die Rückverfolgung zum Ersteller / Aussteller.

23. Jemand möchte elektronisch sein Testament machen. Welche technischen Probleme müssen dabei überwunden werden? Machen Sie einen Vorschlag zur Lösung.

- Es muss sichergestellt werden, dass der öffentliche Schlüssel einer Person wirklich dieser gehört
- Über den Eintrag in eine CA kann sichergestellt werden, dass die Identität der Person und des öffenltichen Schlüssels übereinstimmen
- (Wenn der CA vertraut wird!!!!)
- Uhrzeit muss vor Tod sein

Symmetrische Verschlüsselung

1. Worin besteht ein Ciphertext-Only-Angriff bzw. worin ein KnownPlaintext-Angriff?

- Ciphertext-Only-Attack (Geheimtextanalyse): Der Angreifer kennt nur den Chiffretext.
- Dies ist der häufigste und schwierigste Angriff.
- Es wird u.a. ausgenutzt, dass bestimmte Eigenschaften des Klartextes bei der Verschlüsselung erhalten bleiben.
- Ziel: möglichst viele Klartextanteile oder den Schlüssel bestimmen

- Known-Plaintext-Attack: Der Angreifer kennt zu einem Chiffretext den Klartext bzw. einen Teil davon.
- Öfter vorkommenden Passagen, wie z.B. Anreden, Grüße
- Response-Challenge-Verfahren
- Bekannt sind Paare von Chiffre-/Klartexten mit demselben Schlüssel

2. Schildern Sie eine Situation bzw. ein Verfahren, bei dem Sie als Angreifer mindestens ein Paar(Cipher-Text,Plain-Text) zu einem bestimmten Schlüssel (leicht) erhalten, das Sie zum Brechen der Verschlüsselung benutzen können.

- Challenge and Response verfahren

3. Beschreiben Sie das Verfahren der Verschlüsselung bei One-TimePads? Sind diese sicher?

- Ja, da einmalig verwendet (keine Analyse über mehrere verschlüsselte Texte möglich → Übereinstimmungen)
- Es wird eine Tabelle (Pad) mit wirklich zufälligen Zeichen der Länge L erstellt.
- Der Klartext hat dieselbe Länge L.
- Verschlüsselung:
- Jedes Zeichen des Klartextes wird mit dem korrespondierenden Zeichen der Tabelle verknüpft, z. B. per XOR.
- Entschlüsselung:
- Jedes Zeichen des Chiffretextes wird mit dem korrespondierenden Zeichen der Tabelle mit einer inversen Funktion verknüpft, z. B. auch per XOR

4. Worin liegen die wesentlichen Probleme bei der Benutzung von OneTime-Pads? Nennen Sie zwei.

- beide Seiten müssen den Schlüssel besitzen (Tabelle)
- nur einmalig verwendbar
- Schlüssel wächt proportional zum zu verschlüssselnden Text

5. Was ist eine Blockchiffre und was eine Stromchiffre?

- Blockchiffre = Unabhängige Verschlüsselung von Blöcken gleicher Länge, meist 64 bit
- Jeder Block wird für sich getrennt von anderen behandelt.
- Die kryptographischen Nachteile werden durch Blockmodi beseitigt.
- Stromchiffre = Kontinuierliche Verschlüsselung unterschiedlich langer Blöcke, von 1 bit bis viele Bytes auch variierend

6. Bei welchen Anwendungen sollten am besten Block- und bei welchen eher Stromchiffren eingesetzt werden?

Stromchiffre

- es muss sich keine bestimmte Datenmenge angesammelt haben, damit die

Verschlüsselung erfolgen kann

- es kann bereits nach den ersten Bits starten
- Bsp.: Echtzeitübertragung Mobilfunk
- Blockchiffre:
- Bei großen Datenbeständen (Dateien)

7. Erläutern Sie die typischen Bitoperationen bei symmetrischen Verschlüsselungsverfahren.

- XOR-Verknüpfung
- Permutation (Änderung der Bitreihenfolge)
- Substitution (Ersetzen der Bitfolge)

8. Charakterisieren Sie das DES-Verfahren anhand der Schlüssellänge, Blocklänge und Sicherheit.

- 56 Bit Schlüssellänge
- 64 Bit Blocklänge
- nicht mehr sicher genug (Ablösung furch AES)

9. Worin liegt das größte Problem beim DES?

- Schlüssellänge zu gering

10. Wodurch unterscheidet sich das DES-Verfahren bei der Ver- und Entschlüsselung?

- Teilschlüssel werden in umgekehrter Reihenfolge angewandt

11. Wenn Sie einen Datenblock mit zwei Schlüsseln zwei Mal hintereinander mithilfe des DES-Verfahrens verschlüsseln, verdoppelt sich damit die effektive Schlüssellänge?

- Nein, da Meet-in-the-middle-Angriff (durch Probieren aufgrund des bekannten und unverschlüsselten Textes)

12. Was wird unter effektiver Schlüssellänge gemeint?

- Reduktion des Schlüssels (2x DES ist 57, statt normaler 2x56 = 112)

13.Wie groß ist etwa die effektive Schlüssellänge von 2DES (zwei-fachmit zwei unterschiedlichen Schlüsseln) und wie die von 3DES (dreifachmit zwei Schlüsseln)?

- 2xDES: 57 Bit Schlüssellänge
- 3xDES: 112 Bit Schlüssellänge

14.Worin besteht die Idee des Meet-in-the-Middle-Angriffs? Skizzieren Sie das Verfahren anhand eines fiktiven Beispiels.

- Für den Meet-In-the-Middle-Angriff wird der ein Paar des unverschlüsselten und verschlüsselten Textes benötigt
- Ausgehend von einer 2xDES-Verschlüsselung werden alle 256 Varianten für den

unverschlüsselten Text durchprobiert und in einer Datenbank gespeichert

- Anschließend werden auch alle 256 Varianten für den verschlüsslten Text probiert und in einer weiteren Datenbank gespeichert, da es mehrere mögliche Kandidaten gibt
- Mit einem weiteren Paar aus unverschlüsselten und verschlüsslten Text kann die Liste der möglichen Kandidaten eingeschränkt werden

15. Wie arbeitet das üblich Triple-DES (3DES)? Welche effektive Schlüssellänge wird dabei benutzt?

- 3xDES mit 2 Schlüsseln: 112Bit Schlüssellänge
- 1. A = Verschlüsselung des Klartextes mit einem 56Bit Schlüssel K1
- 1. B = Entschlüsselung des verschlüsselten Text A mit mit K2
- 1. C = Verschlüsselung des verschlüsselten Text B mit K3
- K1 = K3

16. Welchen Vorteil und welchen Nachteil hat das 3DES-Verfahren?

- Vorteil: auch nach heutigem Standard sichere Verschlüsselung
- Nachteil: wegen der dreifachen verschlüsselung auch dreimal zeitaufwändiger als DES

17. Was beschreibt eine Betriebsart?

- Betriebsart = Verfahren, das beschreibt, wie mit einer Blockchiffre Nachrichten verschlüsselt werden

18. Worin besteht der Grund zur Benutzung von Betriebsarten bei der Verschlüsselung?

- Erst die Kombination von Blockchiffre und Betriebsmodus erlaubt es, Nachrichten zu verschlüsseln, die länger sind als die Blocklänge

19.Was charakterisiert die Betriebsart Electronic Codebook (ECB)? Welches Problem hat diese Betriebsart?

Probleme

- Angriff durch Häufigkeitsanalyse
- Gleiche Blöcke werden gleich verschlüsselt

20. Beschreiben Sie das Verfahren der Betriebsart Output-FeedbackMode (OFD).

1. Verschlüsselung eines Intalivektors I (128Bit) = I1
2. XOR Verknüpfung von I1 mit Klartextblock K1 = E2 (erster verschlüsselter Block)
3. Verschlüsselung des verschlüsselten Initialsverkors I1 = I2
4. XOR Verknüpfung von I2 mit Klartextblock K2 = E3 (zweiter verschlüsselter Block)
5. siehe 3. mit I2 und 4. mit I3 und K3

21. Was macht die Betriebsart Output-Feedback-Mode (OFD) so performant? Hat der

Electronic Codebook (ECB) denselben Performanzvorteil?

- Die Verschlüsselungsketten können im Voraus/parallel berechnet werden, so dass hohe Parallelität erreicht werden kann.
- Klartexte können mit ECB auch parallel verschlüsselt werden, da die Nachricht in 128Bit-Blöcke aufgeteilt wird und jeder Block mit dem gleichen Schlüssel verschlüsselt wird

22. Beschreiben Sie das prinzipielle Ablaufschema für die Verschlüsseling bei Stromchiffren.

- sofortige Verarbeitung des Klartextes ohne auf eine bestimmte Blocklänge zu warten
- Stromchiffren = Verschlüsselungsalgorithmen, die keine Einheiten mit festgelegter Größe (Blöcke) benötigen und bei denen die Einheiten ähnlich den Blockmodi verknüpft sind.

23. Nennen Sie ein Beispiel für ein Stromchiffre-Verfahren.

- RC4

24. In welchem Zusammenhang stehen Stromchiffre-Verfahren und Pseudozufallsgeneratoren?

- Forschaltfuntion erzeugt ähnlich wie ein Pseudozufallsgenerator aus einem übergebenen Startwert zufällige Werte (mit denen Ver-/Entschlüsselt wird)
- Forschaltfunktion muss beiden Parteien bekannt sein

Asymmetrische Verschlüsselung

1. Worin besteht der wesentliche Unterschied zwischen asymmetrischen und symmetrischen Verschlüsselungsalgorithmen, wenn die Implementierungen des Verfahrens betrachtet werden?

- Die symmetrischen Verschlüsselungsverfahren basieren auf logischen Bit-Operationen
- Die asymmetrischen Verschlüsselungsverfahren basieren darauf, dass Blöcke von Informationen als lange INTEGER-Werte aufgefasst werden, die arithmetisch nach der Modulo-Arithmetik behandelt werden.

2. Erläutern Sie die typischen Rechenoperationen bei asymmetrischen Verschlüsselungsverfahren. Orientieren Sie sich hierbei an dem RSA-Verfahren.

- Modulo, Eulersche Funktion, GGT, erweiterter euklidischer Algorithmus [S. Folie 36]

3. Was wird bei der Modulo-Arithmetik (manchmal) als Modul bezeichnet?

- der Modulowert zB 5 mod 7 --> 7 = Modul

4. Was wird bei algebraischen Strukturen als neutrales und was als inverses Element bezeichnet? Nennen Sie jeweils ein Beispiel für die Addition und Multiplikation.

- a ° e = a ← e neutrale Element
- 0 neutrales Element bei Addition
- a ° -a = e ← -a inverses Element

5. Sie wollen entsprechend der Modulo-Arithmetik zwei Zahlen dividieren. Unter welcher Bedingung ist dies möglich?

- Die Zahlen müssen Ganzzahlen sein und ungleich 0

6. Was lässt sich durch den einfachen Euklid'schen Algorithmus berechnen?

- der GGT (Größter gemeinsamer Teiler)

7. Was bedeutet teilerfremd (relativ prim)? Was bestimmt die Euler'sche Φ-Funktion?

- zwei Zahllen sind teilerfremd sobald sie keinen gemeinsamen Teiler außer 1 besitzen
- Φ: Anzahl der positiven ganzen Zahlen, die kleiner als n und zu n teilerfremd sind.

8. Für welche Werte ist der Wert der Φ-Funktion sehr leicht zu berechnen?

- für Primzahlen

9. Wie können Sie testen, ob zwei positive ungleiche Zahlen teilerfremd sind?

[Siehe S. 26]

- Es gilt: a^Φ(m) ≡ 1 (mod m), mit a>0 und ggT(a,m)=1

10. Skizzieren Sie die Idee der schnellen Exponentiation. In welchen kryptographischen Verfahren wird dieses Potenzieren z.B. benötigt?

- Exponent wird als Binärzahl dargestellt.
- Für jede 1 wird ein Summand als entsprechende 2er-Potenz berechnet.
- Dann werden alle Summanden addiert
- RSA – Kryptosystem (zur beschleunigten Berechnung)

11. Was für ein Ziel hat das Verfahren von Diffie-Hellman?

- Verfahren zum Schlüsselaustausch ohne Algorithmus (Public-Key-Verfahren)

12. Lassen sich mit dem Verfahren von Diffie-Hellman Daten verschlüsseln?

- Nein, weil es nur ein Verfahren zum Schlüsselaustausch ist

13. Ist das Verfahren von Diffie-Hellman robust gegen den Man-in-theMiddle-Angriff?

- Nein (Zusätliche Authentifizierung wäre notwendig)

14. Auf welchem rechnerisch sehr aufwendigen Verfahren beruht die Sicherheit des Diffie-Hellman-Verfahrens?

- Diskreter Logarithmus (siehe Seite 18)

15. Beschreiben Sie den Algorithmus des Diffie-Hellman-Verfahrens in einer Freistil-Notation jeweils aus der Sicht der Kommunikationspartner.

16. Erläutern Sie das Diffie-Hellman-Verfahren anhand eines kleinen Zahlenbeispiels.

17. Kann irgendein Schlüssel des RSA-Schlüsselpaares zum öffentlichen und der andere zum privaten gemacht werden? Bitte begründen Sie die Antwort.

- Nein, der geheime Schlüssel wird gebildet mit einem geheimen Anteil. Würde man den geheimen Schlüssel zum öffentlichen machen, würde man diesen geheimen Anteil preisgeben

18. Benutzt das RSA-Verfahren eine feste Schlüssellänge sowie z.B. das DES-Verfahren?

Nein

19. Nennen Sie für das RSA-Verfahren eine „vernünftige“ Schlüssellänge in bit.

- mindestens 1024 Bit empfohlen

20. Wie läuft prinzipiell die Wahl der Schlüsselpaare beim RSA-Verfahren ab. Skizzieren Sie dazu einen Algorithmus in Freistilnotation.

(1) Wähle 2 zufällige Primzahlen p, q (100 bis 200 Dezimalstellen) (2) Berechne n= q*p und Φ(n)=(p-1)*(q-1) (3) Wähle ein e und berechne c, d und GGT(e, Φ(n)), so dass e*d + Φ(n)*c=GGT(e,Φ(n)) ist Erweiterter Euklid'scher Algorithmus,Falls GGT(e,Φ(n))<>1 wähle ein neues e (4) Öffentlicher Schlüssel ist {e,n} (5) Geheimer Schlüssel ist {d,n}

21. Beschreiben Sie das Ver- und das Entschlüsseln nach dem RSA-Verfahren, indem Sie einen Algorithmus in Freistilnotation definieren.

(1) p und q sind ungleiche, positive große Primzahlen: n= p *q (2) e und d sind Î Z und so gewählt, dass d* e º 1 mod F(n) (3) P ist Î Z+ und repräsentiert den Klartext (4) Verschlüsseln: C = Pe MOD n (5) Entschlüsseln: P' = Cd MOD n mit P' = P

- Öffentlicher Schlüssel: {e, n}
- Geheimer Schlüssel: {d, n}

22. Erläutern Sie das Ver- und das Entschlüsseln nach dem RSA-Verfahren anhand kleiner Zahlen.

- Siehe Seite 37 (und vorherige)

23. Wie verläuft die Faktorisierungsattacke auf das RSA-Verfahren? Skizzieren Sie dessen Idee.

- Zerlegung von n in p und q (RSA → n = p*q)

- p und q sind die beiden Primzahlen in die anhand von n faktorisiert werden soll

24. Für das RSA-Verfahren werden zwei große zufällig gewählte Primzahlen benötigt. Sie haben eine Zufallszahl erhalten. Können Sie definitiv feststellen, ob es eine Primzahl ist? Welches Problem müssen Sie dabei lösen?

- es ist möglich, jedoch sehr aufwändig

25. Nehmen wir an, dass Sie aus Versehen eine nicht-Primzahl für das RSA-Verfahren gewählt haben. Was hat das für Konsequenzen?

- nicht primzahl -> schlechte Verschlüsselung
- mehrere Kombinationen könenn zum gleichen Ergebnis führen
- somit für Angreifer leichter

26. Auf welchem rechnerisch sehr aufwendigen Verfahren beruht die Sicherheit des RSA-Verfahrens?

- Die Sicherheit des RSA-Verfahrens beruht daraus, dass es rechnerisch sehr aufwändig ist, die Zahl n wieder in ihre beiden Faktoren zu zerlegen.
- siehe http://www.mathematik.uni-muenchen.de/~gerkmann/probestudium/probe1.pdf (http://www.mathematik.uni-muenchen.de/~gerkmann/probestudium/probe1.pdf) S.37

27. Gehört das RSA-Verfahren zu den Blockchiffren? Sie wollen eine Datenbank mit RSA verschlüsseln, wie gehen Sie algorithmisch dabei vor?

- Nein
- Für jede Tabelle einen Schlüssel
- Zeilenweise verschlüsseln

Hash-Verfahren

1. Was ist eine Authentifizierung von Nachrichten? Wird dabei auch die Integrität des Inhalts geprüft?

- Prüfung, ob eine Nachricht in der vorliegenden Form von einer bestimmten Identität stammt, d.h. Inhalt und Herkunft werden geprüft.
- mit MAC (Message Authentication Code = MAC) wird auch integrität geprüft

2. Wenn Sie eine Nachricht erfolgreich authentifiziert haben. Was wissen Sie dann unter welchen Bedingungen sicher?

- Die Nachricht wurde nicht verändert und stammt vom Versender
- Bedingungen: wenn das Verfahren nicht kompromittiert und der Schlüssel nicht veröffentlicht wurde

3. Wie sehen drei Variationen zur Benutzung von Hash-Funktionen zur Feststellung der

Authentizität einer Nachricht bzw. eines Dokuments aus?

1. Es wird ein gemeinsames Geheimnis (key) auf beiden Seiten zur Verschlüsselung des Hashwertes benutzt.
2. Dies ist der symmetrischen Verschlüsselung sehr ähnlich.
3. Es wird das Prinzip der elektronischen Unterschrift (Signatur) angewandt. (Asymetrisch, Public-Private Key)
4. Es wird an die Nachricht ein Geheimnis, das beide Seiten kennen müssen, angehängt und den Hash über beide Teile gebildet.

4. Was ist allgemein eine Hash-Funktion? Welchen weiter gehenden Bedingungen muss eine kryptographische gegenüber einer „normalen“ Hash-Funktion genügen?

- Hash-Funktion = Funktion h(x), für die folgendes gilt:
- Kompression: Abbildung eines beliebigen Bitstrings auf einen Ausgabewert mit einer festen in der Regel kurzen Länge. Dieser ist der Hash-Wert.
- Effizienz: Für jeden Eingabewert x lasst sich die Funktion h(x) mit geringem Aufwand berechnen. Das muss nicht umgekehrt gelten.
- Kryptographische Hash-Funktion = Hash-Funktion h(x), für die zusätzlich noch folgendes gilt:
- Unbestimmbarkeit von Urbildern: Nur mit erheblichen Aufwand ist das x für ein gegebenes y bei y=h(x) zu bestimmen.
- Unbestimmbarkeit eines weiteren Urbildes: Nur mit erheblichen Aufwand ist für ein gegebenes x ein weiteres x' zu bestimmen, wobei h(x)=h(x') gilt.
- Kollisionsfreiheit (Collision Resistance): Nur mit erheblichen Aufwand sind zwei beliebige x und x' zu bestimmen, wobei h(x)=h(x') gilt.

5. Was ist bei Hash-Funktionen eine Kollision?

- Wenn die Hash-Funktion ausgeführt auf verschiedene Eingaben die selben Ergebnisse liefert
- Kollision = Eine Kollision liegt vor, wenn derselbe Hash-Wert anhand verschiedener Urbilder erzeugt werden kann.

6. Sind bei einer kryptographischen Hash-Funktion Kollisionen ausgeschlossen? Falls nicht, was für einen Sinn haben dann diese? Oder anders gefragt: worauf beruht die Sicherheit von kryptographischen Hash-Funktionen?

- kollisionen sind theoretisch nicht ausgeschlossen
- Praktisch haben Kollisionen nur in wenigen Fällen Relevanz, da menschlich lesbare Texte, z. B. Verträge, nur eine sehr kleine Teilmenge aller Bitkombinationen benutzen
- Nur mit erheblichen Aufwand sind zwei beliebige x und x' zu bestimmen, wobei h(x)=h(x') gilt.

7. Unter welchen Voraussetzungen gelingt ein Angriff mittels RainbowTabellen oder

allgemeiner: vorgefertigter Tabellen?

- bei ungesalzenen Hashes

8. Wie verläuft ein Geburtstagsangriff? Skizzieren Sie dessen Idee.

- Es gibt zwei Nachrichten m1 und m2, wobei m1 für den Angreifer schlecht und m2 gut ist.
- Der Angreifer variiert m1 und m2 - z. B. Einfügen von Blanks oder Zeichen, die mit einem nachfolgenden Backspace unsichtbar gemacht werden o.ä. - und bestimmt die Hash-Werte.
- Nach durchschnittlich 2r/2 Versuchen, wobei r die Länge des Hash-Wertes ist, hat der Angreifer zwei Variationen m1' und m2', gefunden, die denselben Hash-Wert besitzen.
- Nun lässt der Angreifer m1' unterschreiben.
- Der Angreifer tauscht den unterschriebenen Text m1' mit dem anderen Text m2' aus...
- Um das zu verhindern, sollte man Hashverfahren nutzen, die möglichst lange Hashes erstellen (z.B. 256 Bit statt 160 Bit) -> hier ist die Wahrscheinlichkeit geringer, dass man zwei Dokumente findet, die denselben Hash haben

9. Wenn Sie das HMAC-Verfahren anwenden: was können Sie dabei erreichen?

- Unveränderter Gebrauch verfügbarer Hash-Funktionen
- Ersetzbarkeit durch andere Hash-Funktionen
- Einfache Verwendung von Schlüsseln

Zufall und Zeit

1. Wodurch unterscheidet sich ein Zufallsbitgenerator von einem Pseudozufallsbitgenerator?

- Zufallsbitgenerator = Random Bit Generator = Gerät oder Verfahren, das eine Sequenz statistisch unabhängiger und gleich verteilter Bitfolgen erzeugt.
- Pseudozufallsbitgenerator = PZBG = Pseudo Random Number Generator = Gerät oder Verfahren, das einen deterministischen Algorithmus realisiert, als Eingabe eine zufällige Bitfolge der Länge k (Seed) erhält und eine Bitfolge der Länge l produziert, die den Eindruck der Zufälligkeit erweckt.

2. Wie lassen sich „echte“ Zufallszahlen auf einem PC erzeugen? Warum geht das so schwer?

- ein PC ist eine deteministische Maschine die keinen Zufall kennt
- einbinden von externen physikalischen Werten (z.B. Spannungsunterschiede benachbarter Halbleitern, Zugriffszeiten auf Festplatten,...)

3. Nennen Sie ein paar Quellen für Zufall, die auf (fast) jedem PC benutzt werden können, also ohne Spezialhardware.

- Analyse der Tastatureingaben
- Analyse von Mausbewegungen
- Uhrzeit auf ms genau
- Positionierungszeiten der Platte
- Analyse von Transfers auf dem LAN

4. Was ist ein Seed (bei Pseudozufallsbitgeneratoren)?

- Seed = möglichst zufälliger Startwert eines PZBG

5. Beschreiben Sie ein einfaches Zeitstempelverfahren mit einer dritten neutralen Partei.

1. A erzeugt einen Hash-Wert des Dokuments .
2. A übermittelt TTP den Hash-Wert.
3. TTP fügt Datum und Uhrzeit an den Hash-Wert.
4. TTP unterschreibt das Ganze.
5. TTP übermittelt A unterschriebenen Hash-Wert mit Zeitstempel

6. Mit dem Diffie-Helmann-Verfahren vereinbaren Sie eine Zahl, die aber als Schlüssel zu klein ist. Wie könnten Sie z.B. einen Schlüssel mit der richtigen Länge erzeugen?

- Bilden eines Hashcodes, das jedes Mal erneut bis die Länge erreichtist
- Schlüssel als Startwert für Zufallsgenerator verwenden