ITS Teststoff

ITS Lektion 2

2.4 Kontrollfragen

1. Skizzieren Sie im Bereich der IT-Sicherheit beispielhaft drei Verwendungsmöglichkeiten für kryptografische Verfahren.

1. Vertrauliche Kommunikation mit hilfe moderner Verschlüsselungsverfahren.
2. Sicherstellen der Datenintegrität durch Hashverfahren.
3. Sicherstellen der Verbindlichkeit durch Signaturverfahren.

2. Aus welchen Teilgebieten setzt sich die Kryptologie zusammen? Erläutern Sie diese!

Kryptographie: Methoden der Ver- und Entschlüsselung
Kryptoanalyse: Verfahren zur Entschlüsselung ohne Zugriff auf verwendete Schlüssel

3. Erklären Sie folgende Definition mit eigenen Worten: $D(E(M; K_E); K_D) = M$

Der Klartext M wird durch Anwenden eines Schlüssel K_E und einem Verschlüsselungsverfahren E verschlüssel. Auf das Ergebnis wird der Schlüssel K_D und das Entschlüsselungsverfahren D angewandt, wodurch man wieder den Klartext M erhält.

4. Was versteht man in der Kryptologie unter einem Alphabet?

endliche Zeichenmenge, welche für das Verfassen der Nachricht verfügbar ist

5. Erläutern Sie das Kerckhoffsche Prinzip!

Sicherheit des kryptographischen Systems soll nur von Geheimhaltung des Schlüssels und nicht von der Geheimhaltung der Verfahrens abhängen.

6. Was versteht man unter einem Substitutionsverfahren?

Ersetzen jedes Klartextelements durch ein Geheimtextelement, Reihenfolge der Elemente bleibt gleich.

7. Was ist der Unterschied zwischen Codierung und Chiffrierung?

Codierung: ersetzen von ganzen Wörtern
Chiffrierung: ersetzen einzelner Zeichen eines Alphabets

8. Was versteht man unter einem Transpositionsverfahren?

Zeichen des Klartextes bleiben erhalten, werden aber durcheinander gewürfelt.

9. Was versteht man unter dem Begriff Anagramm?

Ein Wort welches durch Permutation der Buchstaben ein neues Wort ergibt.

10. Erläutern Sie den Unterschied zwischen Transposition und Substitution.

Substitution: Klartextelement wird durch Geheimtextelement ersetzt, aber die Position in der Nachricht ändert sich nicht.
Transposition: Klartextelemente werden durcheinander gewürfelt, ändern somit Position in der Nachricht, es werden aber keine Klartextelemente durch Geheimtextelemente ersetzt.

11. Was ist der Unterschied zwischen mono- und polyalphabetischer Substitution?

monoalphabetisch: eine feste Zuordnungstabelle (= Geheimtextalphabet)
polyalphabetisch: mehrere Zuordnungstabellen im Wechsel

12. Cäsarverschiebung: Geben Sie die Entschlüsselungsvorschrift an, wenn die Verschlüsselungsvorschrift y=(x+ 13) mod 26 lautet! Was ist das besondere daran, bzw. unter welchem Namen wird diese Chiffre im Internet verwendet?

Entschlüsselungsvorschrift: y=(x+13) mod 26
Verschlüsselungs- und Entschlüsselungsvorschrift sind ident. ($K_E = K_D$)
Im Internet bekannt als ROT13

13. Was versteht man unter homophoner Substitution? Worin liegt die Schwäche dieses Verfahrens?

Es wird ein größeres Alphabet generiert (z.B.: mit 100 Geheimzeichen) und den Buchstaben werden nach der statistischen Wahrscheinlichkeit ihres Auftretens mehrere Geheimzeichen zugeordnet. (z.B.: E: 17 Geheimzeichen da in deutschsprachigen Texten eine Häufigkeit von 17%)
Durch die Analyse mit Hilfe der Häufigkeit von Bi- und Trigramme (en, ck, er, ch, sch) ist die Kryptoanalyse möglich.

14. Erläutern Sie das Prinzip der Vigenère-Verschlüsselung?

Ein Schlüsselwort wird Periodisch über den Klartext geschrieben. Jeder Buchstabe des Klartexts wird mit einer anderen Verschiebechiffre verschlüsselt, abhängig vom darüber liegenden Buchstaben des Schlüsselwortes.

Schlüsselwort: GELBGELBGELBGELBGEL
Klartext: EINHUNDUNDEINKORUND
Geheimtext: KMYIAROVTHPJTOZSARO

15. Erläutern Sie das Brechen einer Vigenère-Chiffre mit Hilfe des Kasiski-Tests.

Durch die begrenzte Länge des Schlüssels kommt es zu Wiederholungen.
z.B.: Man hat das Schlüsselwort “GELB” und ermittelt alle Möglichkeiten wie das Wort “UND” verschlüsselt werden kann (“UND” wird verwendet da es oft im Deutschen vorkommt). Nun werden die Möglichen Fragmente im Geheimtext gesucht. Der Abstand zwischen den Anfangsbuchstaben der selben Fragmente ist ein Vielfaches der Schlüssellänge. Durch die Analyse mehrere Abstände zwischen Fragmenten ist es möglich einen gemeinsamen Teiler zu finden, welcher der Schlüssellänge entspricht. Ist die Schlüssellänge bekannt, reduziert sich die Kryptoanalyse auf eine gewöhnliche Verschiebechiffre.

16. Erläutern Sie das Brechen einer Vigenère-Chiffre mit Hilfe des Autokorrelationstests.

Bestimmte Zeichenfolgen kommen häufiger vor und werden dadurch häufiger mit dem selben Buchstaben verschlüsselt. Verschiebt man den Geheimtext und vergleicht ihn mit dem ursprünglichen Geheimtext ist die Wahrscheinlichkeit für eine Übereinstimmung bei einer Verschiebung um ein Vielfaches der Schlüssellänge besonders hoch.

17. Was ist ein One-Time Pad und wann ist dieses Verfahren nachweislich perfekt?

polyalphabetische Substitution, Klartextlänge = Schlüssellänge
Schlüssel muss eine zufällige Zeichenfolge sein und darf nicht wiederverwendet werden.

18. Erläutern Sie Vor- und Nachteile des One-Time Pads?

Schlüssel ist so groß wie Klartext, dadurch doppeltes Datenvolumen.
Schlüsselaustausch ist problematisch.
Für jede Kommunikation ist ein eigener Schlüssel notwendig.

19. Was versteht man unter einer Vernam-Chiffre?

Sind dieselben Vorgaben wie bei einem One-Time Pad erfüllt und wird der Schlüssel bitweise mit dem Klartext addiert.

20. Erläutern Sie die beiden von Claude Shannon geforderten Eigenschaften an einen guten Verschlüsselungsalgorithmus!

Diffusion: statistische Struktur eines Klartextes soll über den Geheimtext zerstreut sein → Änderung am Klartext soll möglichst viel am Geheimtext ändern
Konfusion: Beziehung zwischen Schlüssel und Geheimtext soll möglichst komplex sein → ableiten des Schlüssels soll so schwer wie möglich sein

21. Was versteht man unter Diffusion? Durch welches Verfahren kann Diffusion erreicht werden?

Statistische Struktur eines Klartextes soll über den Geheimtext zerstreut sein → Änderung am Klartext soll möglichst viel am Geheimtext ändern.
Wird durch Transposition erreicht.

22. Was versteht man unter Konfusion? Durch welches Verfahren kann Konfusion erreicht werden?

Beziehung zwischen Schlüssel und Geheimtext soll möglichst komplex sein → ableiten des Schlüssels soll so schwer wie möglich sein.
Wird durch komplexe Substitutionsmechanismen erreicht.

23. Ist es besser, einen proprietären und somit geheimgehaltenen Algorithmus zu verwenden, oder sich auf die Sicherheit eines öffentlich bekannten Verfahrens zu verlassen? Begründen Sie Ihre Entscheidung!

Ein öffentlich bekanntes Verfahren ist besser, da es von vielen Kryptologen hin auf Schwachstellen überprüft wurde. Meist werden geheime Verfahren auch veröffentlicht und werden in den meisten Fällen gebrochen.

3.3 Kontrollfragen

1. Was versteht man unter einem symmetrischen Verschlüsselungsverfahren?

Es wird auf beiden Seiten der selbe Key zum ver- und entschlüsseln verwendet.

2. Erklären Sie folgende Definition mit eigenen Worten:

$$\forall M \in \mathcal{M} : D(E(M, K_{A,B}), K_{A,B}) = D(C, K_{A,B}) = M$$

Nachricht M wird mit dem selben Schlüssel ($K_{A,B}$) ver- und entschlüsselt.

3. Was ist eine Blockchiffre?

Die zu übertragende Nachricht wird in gleich große Blöcke unterteilt. (Blockgröße wird vom Algorithmus vorgegeben) Es wird immer Block für Block verschlüsselt.

4. Was ist eine Stromchiffre?

Aus geheimen Schlüssel wird pseudozufälliger Bitstrom erzeugt, mit welchem die Nachricht kontinuierlich per XOR verschlüsselt wird.

5. Zählen Sie wichtige Aufgaben einer S-Box auf.

Nichtlinearität: Kein Ausgangsbit ist linear von einem Eingangsbit abhängig.
Vollständigkeit: Jedes Ausgangsbit ist von jedem Eingangsbit abhängig.
Lawineneffekt: Die Änderung eines Eingangsbits bewirkt durchschnittlich die Änderung der Hälfte aller Ausgangsbits.

6. Feistel-Box: Erklären Sie folgende Definition mit eigenen Worten:

$$F_s(F_s(l,r)) = F_s(l \oplus S(r), r) = (l \oplus S(r) \oplus S(r), r) = (l, r)$$

Welches Problem wird dadurch elegant gelöst bzw. beseitigt?

In einer Feistelbox wird die Nachricht in linken und rechten Teil gespalten. Der rechte Teil wird mit einer nichtlinearen Funktion verschlüsselt, bleibt aber auch als Klartext erhalten und wird XOR mit dem linken Teil verknüpft.
Durch den unverschlüsselten rechten Teil ist es möglich durch verschlüsseln von diesem und XOR verknüpfen mit dem verschlüsselten linken Teil den linken Teil wieder als Klartext zu erhalten.

7. Was versteht man unter einem Rundenschlüssel?

Die Verschlüsselungsoperation wird mehrmals hintereinander ausgeführt um Konfusion und Diffusion auf den kompletten Klartext anzuwenden. Für jede dieser Runden wird ein Rundenschlüssel eingearbeitet welcher vom eigentlichen Schlüssel abgeleitet ist.

8. Was ist eine Produktchiffre?

Die Transformation eines Klartextblockes in einen Geheimtextblock ist das Produkt von mehreren Runden-Transformationen, die sich bis auf den verwendeten Rundenschlüssel gleichen.

9. Nennen Sie wesentliche Merkmale der in Feistel-Netzwerke integrierten Operationen.

Sie sind ausreichend komplex, nicht-linear aber umkehrbar.

10. Wozu dienen im Zusammenhang mit symmetrischen Blockchiffren die Betriebsarten?
Was wird dadurch verhindert?

Wenn jeder Klartextblock für sich verschlüsselt wird, sind auch die daraus verschlüsselten Blöcke alle gleich -> Kryptoanalyse
Die Betriebsarten legen fest wie eine Folge von Blöcken zu verschlüsseln ist.

11. Erläutern Sie die Betriebsarten ECB, CBC, CFB, CTR.

ECB (Electronic Codebook Mode): jeder Block wird einzeln verschlüsselt.
CBC (Cipher Block Chain Mode): Klartextblock wird mit vorhergehendem Block XOR verknüpft und verschlüsselt. Klartextblöcke resultieren somit nicht in gleich Cipherblöcke.
CFB (Cipher Feedback Mode): Ein 64-Bit Schieberegister wird verschlüsselt und das Byte welches am weitesten links ist wird XOR verknüpft mit dem Klartextbyte. Das verschlüsselte Byte wird verschickt und von rechts in das Schieberegister geschoben. Ermöglicht betrieb als Stromchiffre.
CTR (Counter Mode): Ein Initialisierungsvektor wird verschlüsselt und XOR mit dem Klartext verknüpft. Der Initialisierungsvektor wird für jeden Block hochgezählt. Dient um einfach auf einzelne Blöcke zugreifen zu können.

12. Erläutern Sie die Betriebsarten ECB und CBC. Was ist der Vorteil von CBC?

ECB verschlüsselt jeden Block einzeln, CBC verknüpft den Block XOR mit vorhergehenden Cipherblock, danach wird erst verschlüsselt. Analyse wird dadurch beim CBC erschwert, da der verschlüsselte Block vom vorhergehenden Block abhängig ist.

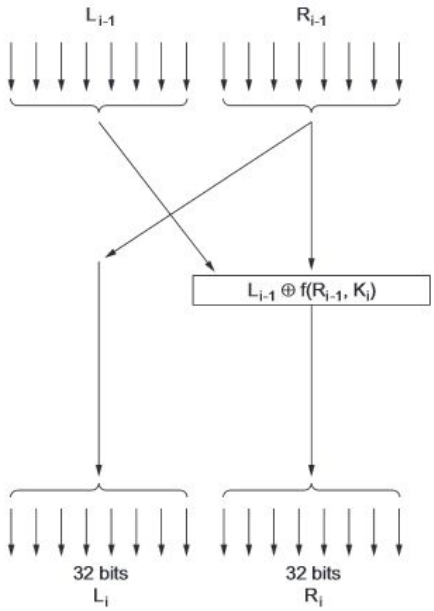
13. Welches Sicherheitsproblem gibt es im Zusammenhang mit der Betriebsart CBC?

Da bei der Veränderung eines Geheimtextblocks sind nur der aktuelle und der darauffolgende Geheimtextblock betroffen. Dadurch ist es möglich Cut-and-Paste Angriffe durchzuführen, bei welchem der Geheimtextblock durch einen anderen Geheimtextblock ersetzt wird, welcher mit dem selben Schlüssel verschlüsselt wurde.

14. Nennen Sie die Besonderheit des Galois Counter Mode.

Es wird ein zusätzlicher Authentication Tag eingesetzt welcher Integrität und Authentizität sicherstellt, zusätzlich kann über den Counter Mode auf einzelne Blöcke zugegriffen werden.

15. Gegeben sind zwei Blöcke (l,r) mit je 32 Bits Breite. Skizzieren Sie eine Runde eines
Feistel-Netzwerks (DES) unter Verwendung eines Rundenschlüssels.



16. Erläutern Sie Eigenschaften/Funktionsweise/Vor- und Nachteile von 3DES mit eigenen
Worten.

- Effektive Schlüssellänge steigt von 56 auf 112 Bit -> höhere Sicherheit
- 112 Bit Schlüssel wird in zwei 56 Bit Schlüssel (K1, K2) aufgeteilt
- drei DES Durchgänge
- Verschlüsselung DES mit K1, dann DES mit K2 und nochmals DES mit K1
- ermöglicht Kompatibilität mit DES durch wählen von K1=K2

17. Welche Schlüssellänge weist 3DES (bei Kaskadieren von DES im 56 Bit-Modus) auf.
Warum?

- 112 Bit
- ermöglicht Kompatibilität mit DES wenn zwei gleiche 56 Bit Keys aneinander gehängt werden.

18. Welche symmetrischen Blockchiffren kennen Sie neben DES bzw. 3DES? Erläutern Sie diese kurz!

AES (Advanced Encryption Standard):
- Unterstützte Blockgröße und Schlüssellänge: 128, 192, 256 Bit
- Blockgröße und Schlüssellänge müssen nicht gleich sein.
- gute Performance bei Hardwareimplementierung

IDEA (International Data Encryption Algorithm):
- 64 Bit Blöcke
- 128 Bit Schlüssellänge
- möglicher Nachfolger von DES

Blowfish:
- Feistel-Chiffre
- sehr gute Performance auf 32-Bit Prozessoren
- Schlüssellänge: 32 - 448 Bit
- Blockgröße 64 Bit

Twofish:
- Nachfolger von Blowfish
- Feistel-Chiffre
- Schlüssellänge: bis zu 256 Bit
- Blockgröße: 128 Bit
- Einsatz auch als Stromchiffre und Hashfunktion möglich

CAST:
- Schlüssellänge: 128 Bit
- Blockgröße 64 Bit
- Feistel-Chiffre
- wird in den neueren PGP-Versionen verwendet
- 256 Bit Version: CAST-256

19. Stromchiffren: Erklären Sie folgende Definition mit eigenen Worten:

$$C_1 \oplus C_2 = M_1 \oplus K_{Strom} \oplus M_2 \oplus K_{Strom} = M_1 \oplus M_2 \quad \text{, da} \quad x \oplus K_{Strom} \oplus K_{Strom} = x$$

Welches Problem ergibt sich daraus?

Zwei XOR verknüpfte Cipher-Texte ergeben die beiden XOR verknüpften Klartexte, wenn sie mit dem selben Schlüssel verschlüsselt wurden.

Problem:
Durch das Abhören der verschlüsselten Nachrichten ist es möglich auf den Schlüssel zurück zuschließen wenn die Klartextnachrichten bekannt sind (known plaintext, z.B.: Paketheader)

20. Erläutern Sie kurz die Eigenschaften der RC4 Stromchiffre.

- Schlüssellänge: bis 2048 Bit
- byte-weise Verschlüsselung
- Zufallsgenerator verwendet eine S-Box, die mit dem Geheimschlüssel initialisiert wird
- Dieser generiert im Betrieb die Zufallsfolgen

21. Welches Problem ergibt sich bei dem zu klein bemessenen Initialisierungsvektor im WEP-Standard? Was ist die Konsequenz?

- IV wiederholt sich ab ca. 5000 Paketen (~7MB)
- da sich Passwort nicht ändert hat der Angreifer zwei Geheimtexte die mit dem selben Schlüssel verschlüsselt sind
- $C_1 \oplus C_2$ ergibt $M_1 \oplus M_2$
- durch chosen plaintext Attacke oder known plaintext (Datei- bzw. Protokoll-Header) weiß der Angreifer den Klartext von M_1/M_2

ITS Lektion 3

4.6 Kontrollfragen

1. Was versteht man unter einem asymmetrischen Verschlüsselungsverfahren?

Asymmetrische Verschlüsselungsverfahren verwenden sich ergänzende Schlüsselpaar, wobei jeweils mit einem verschlüsselt wird und mit dem anderen entschlüsselt.

2. Erklären Sie folgende Definition mit eigenen Worten:

$$\mathcal{M} = \mathcal{C} \quad \text{und} \quad \forall M \in \mathcal{M} : E(D(M, K_D), K_E) = D(E(M, K_E), K_D) = M$$

Nachricht wird mit K_E (öffentlicher Schlüssel) verschlüsselt und mit K_D (privater Schlüssel) entschlüsselt. In umgekehrter Reihenfolge kann eine Nachricht signiert werden.

3. Stellen Sie symmetrische und asymmetrische Verschlüsselung gegenüber und finden Sie jeweils eine Stärke/Schwäche im Vergleich zum jeweils anderen Verfahren.

<u>symmetrisch:</u>
- performant
- nur ein Schlüssel
- Problem Schlüsselübergabe

<u>asymmetrisch:</u>
- schlechte Performance
- kein Problem mit Schlüsselübergabe, da ein öffentlicher und ein privater Schlüssel
- Problem Man-in-the-Middle-Angriffe
- verwendbar als digitale Signatur

4. Warum "mischt" man symmetrische und asymmetrische Verschlüsselung zu sog. hybriden Verfahren?

Mit asymmetrischen Verfahren werden die Schlüssel ausgetauscht, die symmetrischen Verfahren kümmern sich dann um das verschlüsseln der Daten. Löst das Problem des Schlüsselaustausch der symmetrischen Verfahren und das Performance Problem der asymmetrischen Verfahren.

5. Was versteht man unter einer Einweg-Funktion?

Ist eine Funktion die leicht berechenbar ist, aber schwer umzukehren.

6. Was versteht man unter einer Einweg-Funktion mit Falltür?

Sind Einweg-Funktionen die mit einer Zusatzinformation leicht umzukehren sind.

7. Nennen Sie drei mathematische Methoden, um Einwegfunktionen zu realisieren.

- Diskrete Exponentialfunktion
- Elliptische Kurven
- Primfaktorzerlegung

8. Warum ist die Umkehrfunktion der diskreten Logarithmusfunktion nur äußerst schwierig zu ermitteln?

Exponentialfunktion macht unvorhersehbare Sprünge, deshalb ist keine systematische Annäherung möglich.

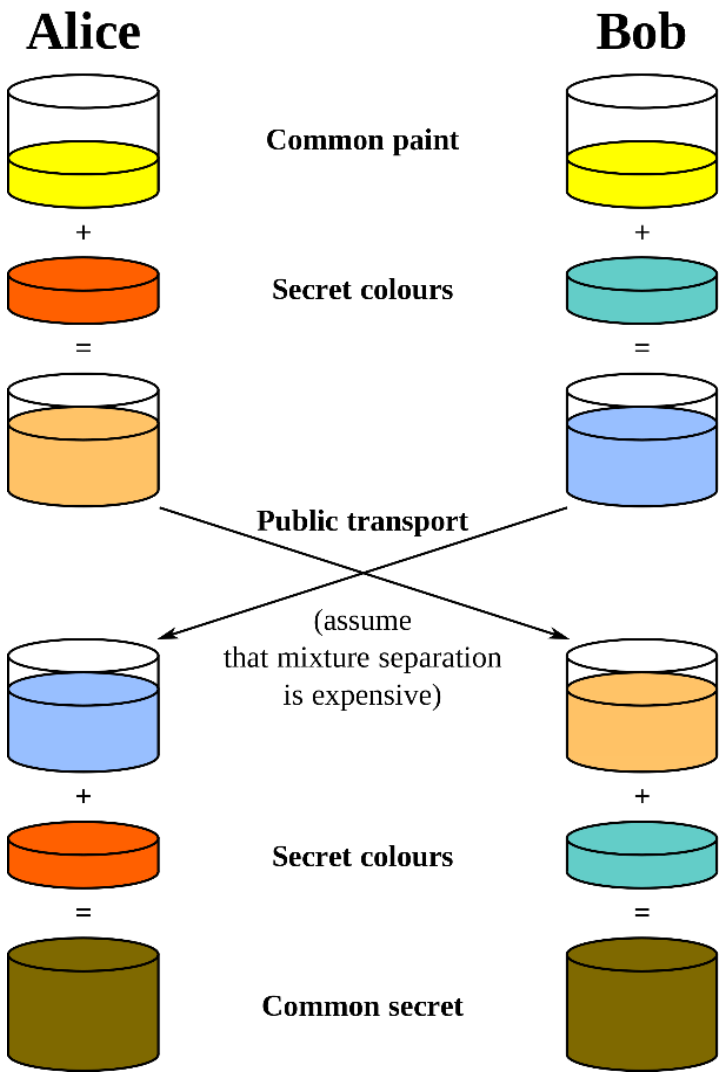
9. Nennen Sie die Vorteile des Diskreten Logarithmus Problem in elliptischen Kurven.

- kürzere Schlüssellänge
- höhere Geschwindigkeit
- geringere Speicheranforderungen

10. Was versteht man unter Primfaktorzerlegung?

Eine natürliche Zahl wird als Produkt zweier Primzahlen dargestellt. Derzeit gibt es kein effizientes Faktorisierungsverfahren.

11. Veranschaulichen Sie in einer Skizze, wie Simon Singh die Funktionsweise der Diffie-Hellman Schlüsselvereinbarung an Hand von Farbmischung beschreibt.



12. Nennen Sie Nachteile/Sicherheitsprobleme bei der Verwendung der Diffie-Hellman Schlüsselvereinbarung. Welches Schutzziel kann aus welchem Grund nicht gewährleistet werden.

- beide Kommunikationspartner müssen online sein
- kein Schutzziel Authentizität -> Man in the Middle Angriff

13. Was ist der Nachteil am ElGamal Verschlüsselungsverfahren? Welches Schutzziel kann aus welchem Grund nicht gewährleistet werden.

- Schlüssel kann nicht alleine generiert werden, es wird noch der geheime Parameter des anderen benötigt.
- somit kein Schutzziel Authentizität -> Man in the Middle Angriff (basiert auf Diffie-Hellman)

14. Erläutern Sie das Funktionsprinzip des RSA-Verfahrens mit eigenen Worten.

- man braucht zwei sehr große Primzahl p und q
- berechnet n = p . q
- m = (p-1) . (q-1)
- wählt e teilerfremd zu m
- $d = e^{-1} (\text{mod } m)$
- n, e bilden öffentlichen Schlüssel
- Nachricht x verschlüsseln: $y = x^e (\text{mod } n)$
- Nachricht y entschlüsseln: $x = y^d (\text{mod } n)$

15.Was bedeutet es, wenn zwei Zahlen a und b teilerfremd sind?

GGT = 1 (multiplikatives Inverses kann gebildet werden)

16. Warum ist es beim RSA-Verfahren problematisch, wenn die gewählten Primfaktoren p und q zu knapp nebeneinander liegen?

Dann lassen sich diese durch die Methode von Fermat faktorisieren.

5.5 Kontrollfragen

1. Was versteht man unter einer Hashfunktion?

Ein nicht injektive Funktion, die ein Datum beliebiger Länge auf einen Hash-Wert fester Länge abbildet.

2. Wozu können Hashfunktionen verwendet werden?

- überprüfen der Integrität
- helfen bei der Erstellung von Signaturen (damit nicht die ganze Datei signiert werden muss sondern nur der Hash)
- speichern von Passwörtern

3. Was bedeutet der Ausdruck $H : A_1^* \longrightarrow A_2^k$ **?**

Ein Datum beliebiger Länge wird auf einen Hash-Wert fester Länge abbildet.

4. Warum sind Hashfunktionen nicht injektiv? Was bedeutet das?

Eine Hashfunktion bildet ein beliebig großes Datum auf einen Hash fixer Länge ab, ist damit nicht injektiv. Das bedeutet dass aus einem Hash nicht auf das Ausgangsdatum zurückgeschlossen werden kann.

5. Was versteht man unter dem "Lawineneffekt"?

Die Änderung eines Bits im Ausgangsdatum soll möglichst den gesamten Hash beeinflussen.

6. Was ist der Unterschied zwischen einer schwach kollisionsresistenten und einer stark kollisionsresistenten Hashfunktion?

schwach kollisionsresistent: soll praktisch unmöglich sein zu einem gegebenen Hash ein Datum zu finden das den selben Hash liefert

stark kollisionsresistent: soll praktisch unmöglich sein zwei unterschiedliche Datum zu finden die denselben Hash haben.

7. Das Geburtstagsparadoxon besagt, dass in einer Gruppe ab 23 Personen die Wahrscheinlichkeit, dass zwei Personen am gleichen Tag Geburtstag (Kollision) haben, höher als 50% ist. Bringen Sie diese Tatsache in Zusammenhang mit der Definition einer stark kollisionsresistenten Hashfunktion im Vergleich zur Definition einer schwach kollisionsresistenten Hashfunktion.

Es ist schwieriger zu einem gegebenen Geburtstag einer Person eine Person zu finden die am selben Tag Geburtstag hat (schwach kollisionsresistent) als zwei Personen die sich einen beliebigen Geburtstag teilen (stark kollisionsresistent).

8. Welche Implementierungen von Hashfunktionen kennen Sie?

- MD5 (Message Digest 5)
- Secure Hash Algorithm 1, 2, 3 (SHA-1, SHA-2, SHA-3)

9. Welche Empfehlungen würden Sie hinsichtlich der Verwendung des Hashalgorithmus MD5 für die in Abschnitt 5.3 (ab Seite 54) beschriebenen Einsatzbereiche geben?

Für digitale Signaturen sollte MD5 nicht mehr verwendet werden, da es seit 2004 möglich ist innerhalb kürzester Zeit Kollisionen zu finden. (Geburtstagsangriff, M und M' konstruieren, welche denselben Hash haben)

10. Was ist der Unterschied zwischen SHA-1 und SHA-2?

Funktionsweise ist weitestgehend gleich, SHA-1 verwendet eine feste Hashlänge von 160 Bit,
SHA-2 hat mehrere, längere Hashvarianten zwischen 224 und 512 Bit (SHA-224, SHA-256,SHA-384, SHA-512)

11. Wie kann eine symmetrische Blockchiffre als Hashfunktion eingesetzt werden? Warum?

M wird in Blöcke aufgeteilt und beim iterativen Prozess verschlüsselt und verknüpft. Der letzte Block ist von allen vorangegangen abhängig und ergibt den Hash.

6.5 Kontrollfragen

1. Was versteht man unter "Brute Force Attack"?

Durchprobieren aller möglichen Schlüssel.

2. Was versteht man unter "Dictionary Attack"?

Durchprobieren der Schlüssel einer zu diesem Zweck angefertigten Passwortsammlung.

3. Welche Klassen von kryptoanalytischen Angriffen kennen Sie?

Angriff mit bekanntem Geheimtext (ciphertext-only attack)
Angriff mit bekanntem Klartext (known-plaintext attack)
Angriff mit frei gewähltem Klartext (chosen-plaintext attack)
Angriff mit gewähltem Geheimtext (chosen-ciphertext attack)

4. Welche Arten der Kryptoanalyse kennen Sie?

- Analyse von monoalphabetischen Substitutionschiffren (Häufigkeitsverteilung einer natürlichen Sprache)
- Analyse von polyalphabetischen Substitutionschiffren (Mustersuche für ermitteln der Schlüssellänge)
- Differentielle Kryptoanalyse
- Lineare Kryptoanalyse

7.4 Kontrollfragen

1. Was ist ein Message Authentication Code (MAC)?

Dient zum Prüfen der Integrität und Authentizität einer Nachricht

2. Wie unterscheidet sich ein HMAC von einem MAC?

Sind MAC welche auf Hashfunktionen basieren.

3. Nach welchem Schema funktioniert der RSA-Signatur-Algorithmus?

- hinterlegen des öffentlichen Schlüssels in einer öffentlichen Datenbank
- bilden eines Hashes über die Nachricht
- signieren dieses Hashes mit dem privaten Schlüssel
- wird gemeinsam mit der Nachricht verschickt
- Empfänger bildet Hash über Nachricht
- entschlüsselt Signatur mit öffentlichem Schlüssel
- vergleicht die Hashes

4. Was ist der Unterschied zwischen Authentifikation und Autorisierung?

Authentifikation: feststellen der Identität anhand eines bestimmten Merkmals
Autorisierung: Zuweisung und überprüfung von Zugriffsrechten

5. Über welche Maßnahmen kann die Identitätsprüfung (Authentifizierung) für Benutzer
bzw. Prozesse erfolgen?

- spezifisches Wissen (Passwort)
- persönlicher Besitz (Smartcard)
- biometrische Merkmale (Fingerabdruck)

6. Erläutern Sie die Authentifizierung mit RSA.

- Sender verschlüsselt einen Cookie mit dem öffentlichen Schlüssel des Empfängers und bildet den Hash über den Cookie
- Empfänger entschlüsselt Cookie mit privaten Schlüssel und bildet den Hash über den Cookie
- Empfänger sendet Hash an Sender, welcher die Hashes vergleicht

8.4 Kontrollfragen

1. Was versteht man unter einem Zertifikat? Was kann damit sichergestellt werden?

Ein Zertifikat besteht aus den signierten Informationen der Person/Organisation (Name, Adresse, etc.) und dem signierten öffentlichen Schlüssel. Dadurch kann die Authentizität einer Person/Organisation Sichergestellt werden.

2. Wie erfolgt die Echtheitsgarantie eines Zertifikates?

Durch die CA (Certification Authority), welche wiederum vor der Ausstellung des Zertifikats die Identität prüft.

3. Wie erfolgt das Zurückziehen von Zertifikaten?

CRL (Certificat Revocation List)
OCSP (Online Certicate Status Protocol)

4. Was ist eine Certificate Revocation List? Welchen Nachteil birgt dieser Ansatz in sich?

Öffentliche Liste der zurückgezogenen Zertifikate.
Nachteile: Liste muss gepflegt werden (möglicherweise revoked Certificates nicht auf Liste eingetragen)

5. Was ist das OCSP (Online Certicate Status Protocol)?

Protokoll zur Überprüfung ob ein Zertifikat gesperrt wurde. Liefert Status gültig/good, zurückgezogen/revoked oder unbekannt/unknown zurück.

6. Erläutern Sie die beiden Abschnitte eines Zertifikates nach dem X.509 Standard. Was ist jeweils darin enthalten?

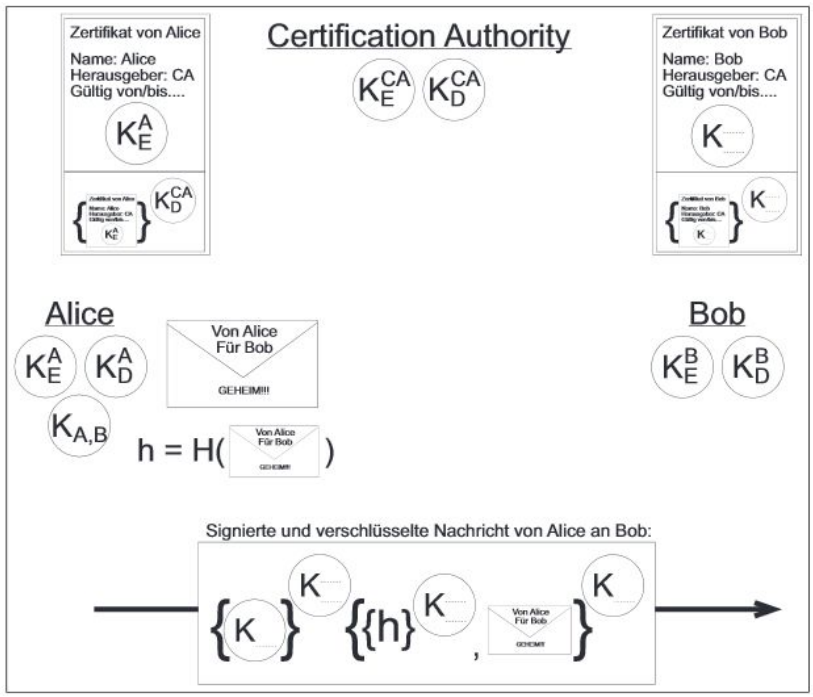
Datenabschnitt besteht aus den Informationen über die Person/Organisation (Name, Adresse, usw.), Details über das Zertifikat selbst (Seriennummer, Gültigkeit, usw.), über die ausstellende CA (Name der ausstellenden Instanz) und den Public Key der Person/Organisation

Signaturabschnitt besteht aus der Signatur der CA und der Information über den verwendeten Algorithmus.

7. Was versteht man unter einer hierarchischen Public Key Infrastructure (PKI)?

Es gibt eine root CA welche für eine oder mehrere sub-CAs die Zertifikate signiert und diese somit beglaubigt. Über diese sub-CAs können wiederum selbst Zertifikate ausgestellt werden.
Die daraus entstehende Kette an CAs bezeichnet man als Zertifizierungspfad (Chain of Trust).

8. Alice will an Bob eine Nachricht übermitteln. Gefordert sind die Schutzziele der Vertraulichkeit, Integrität sowie Authentizität. Die Zertifikate von Alice und Bob sind für den jeweils anderen verfügbar. Vervollständigen Sie die Grafik durch Einsetzen der jeweils anzuwendenden Schlüssel!



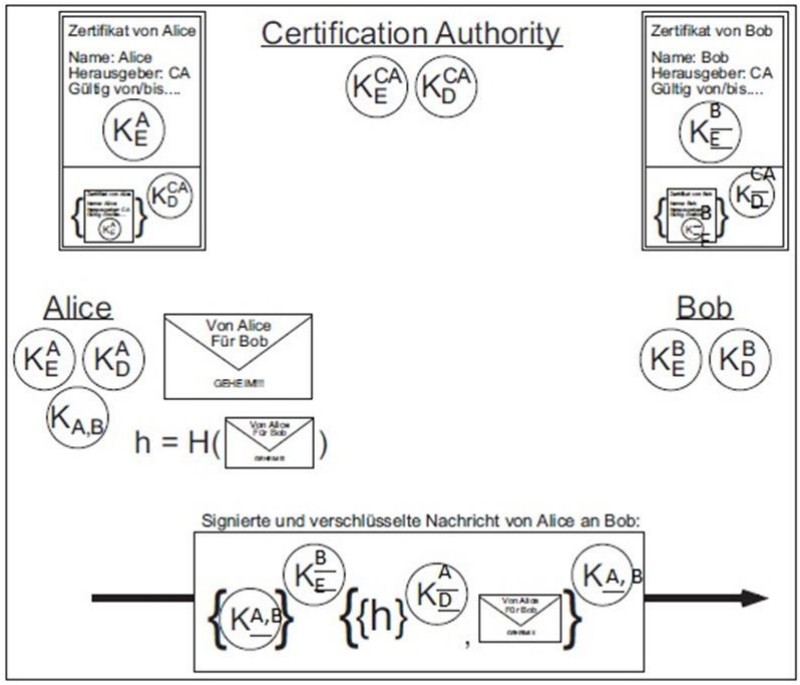


Abbildung 8.3: Einsetzaufgabe: Hybrides Verfahren

9. Wozu dienen die Public Key Cryptographic Standards?

Legen Standard für Format der Zertifikate fest, damit diese interoperable sind.

10. Welche Aufgabe(n) übernimmt eine Registration Authority?

Identifizieren einer natürlichen/juristischen Person und deren Registrierung.

11. Welche Aufgabe(n) übernimmt eine Certification Authority?

Ausstellen und widerrufen von Zertifikaten.

12. Aus welchen beiden Einrichtungen besteht das Trust Center?

Registration Authority + Certification Authority

13. Wie wird die Vertrauenswürdigkeit einer Stammzertifizierungsstelle gewährleistet?

root-Zertifikate werden mit Betriebssystemen und Browsern ausgeliefert und diesen wird standardmäßig vertraut.

14. Wozu dient eine “Certificate Policy”?

Verlässlichkeit der Zuordnung, Höhe der Sicherheitsanforderung bei Ausstellung

15. Welche Problematik ergibt sich aus isolierten PKI-Inseln?

Ein übergreifender Validierungspfad über Cross-Zertifikate muss zwischen den PKI-Inseln eingerichtet werden.

16. Was ist das Web of Trust? Erläutern Sie grob die Funktionsweise.

- dezentrale Alternative zur PKI
- Verteilung erfolgt über dezentrale Server oder durch selbständiges Verteilen (z.B.: E-Mail)
- Vertrauenswürdigkeit wird akkumuliert durch Signatur des eigenen öffentlichen Schlüssels durch andere User
- (Verwaltung der eigenen privaten Schlüssel im private Keyring, eigener öffentlicher Schlüssel und die anderer User werden im public Keyring gespeichert)

17. Was ist der Unterschied zwischen einer hierarchischen PKI und dem Web of Trust?

PKI: hierarchisch, zentral, Baumstruktur
Web of Trust: dezentral, basiert auf Vertrauensbeziehungen

18. Was versteht man beim Web of Trust unter einer transitiven Vertrauensbeziehung?

Signiert B den Schlüssel von C gilt dies als Vertrauensbeweis. Vertraut man selbst nun B so traut man auch automatisch C -> transitive Vertrauensbeziehung.

19. Nennen und beschreiben Sie unterschiedliche Arten von Schlüsseln bzw. Schlüsselhierarchien?

- Derived Unique Key Per Transaction (DUKPT): Master Key, Session Key
- WPA2: PSK -> Pairwise Master Key (PMK), davon abgeleitet Pairwise Transient Key (PTK)
- DNSec: Signierte Ressource Records, durch Zone Signing Key (ZSK), wegen Performance nur 1024 Bit, wird öfters gewechselt, ZSK durch Key Signing Key (KSK) signiert, KSK langlebiger -> 2048 Bit

18. Beschreiben Sie, wie ein Maskierungsangriff bei einem Schlüsselaustausch über ein hybrides Verfahren (Verschlüsseln des symmetrischen Sitzungsschlüssels über einen asymmetrischen Austauschschlüssel) vonstatten gehen könnten.

Bei einem Man-in-the-Middle Angriff (Maskierungsangriff) fängt eine dritte Person die Kommunikation zweier Partner ab und lässt beide mit der dritten Person einen Schlüsselaustausch durchführen. Dadurch ist es der dritten Person möglich den Datenverkehr mit zu lesen und zu manipulieren. Die dritte Person hat dann jeweils eine Session mit den beiden Partnern offen. Traffic zwischen den zwei Partnern wird über die dritte Person geroutet.

ITS Lektion 4

9.3 Kontrollfragen

1. Was versteht man unter Access Control?

Prozess, welcher den Zugang zu Systemressourcen gemäß einer Richtlinie steuert und nur Berechtigten Zugang gewährt.

2. Erläutern Sie den Unterschied zwischen einem Subjekt und einem Objekt.

Objekt: passive Komponente welche Information enthält (PC)
Subjekt: aktive Komponente welche Zugriff auf Objekt oder Information innerhalb des Objektes haben will (Benutzer)

3. Was ist der Unterschied zwischen Zutritt, Zugang und Zugriff?

Zutritt: zu Räumen, Gebäuden
Zugang: Gerät welches den Zugang ermöglicht
Zugriff: auf Daten/Informationen durch (Benutzer-)Rechte

4. Was ist der Unterschied zwischen physischem und logischem Schutz?

physisch: Schutz gegen Zutritt (absperren eines Raumes)
logisch: Regel auf Betriebssystem- bzw. Applikationsebene (Passwort)

5. Bringen Sie folgende Begriffe in einen chronologisch sinnvollen Zusammenhang und beschreiben Sie diese kurz: Autorisierung, Identifizierung, Authentifizierung.

Identifizierung: eindeutige Erkennung der Identität eines Subjekts, anhand eindeutigem Merkmal/Bezeichner
Authentifizierung: Überprüfung und Bestätigung der behaupteten Identität
Autorisierung: Zuweisung von Zugriffsrechten auf passive Komponenten (Objekte) nach Authentifizierung

6. Wozu dient die Identifizierung eines Subjekts?

Eindeutige Erkennung der Identität eines Subjekts, anhand eines eindeutigen Bezeichners (ID,...).

7. Wozu dient die Authentifizierung eines Subjekts?

Überprüfung und Bestätigung der behaupteten Identität. z.B.: Passwort

8. Welche drei Möglichkeiten der Authentifizierung gibt es? Geben Sie jeweils ein Beispiel an!

Wissen (Passwort)
Besitz (Chipkarte)
Biometrisches Merkmal (Fingerabdruck)

9. Was versteht man unter Autorisierung?

Zuweisung von Zugriffsrechten auf passive Komponenten (Objekte) nach Authentifizierung.

10. Welche formalen Modelle der Zugriffskontrolle kennen Sie?

Discretionary Access Control (DAC): Eigentümer der Ressource legt Zugriffsrechte fest
Mandatory Access Control (MAC): Zugriffsrechte werden vom System vorgegeben.
Role Based Access Control (RBAC): Zugriffsrechte werden über Rollen vergeben.

11. Erläutern Sie das Verfahren der Rule-Based Access Control.

Regelwerk nach “if-then-else”-Konzept (Router, Firewalls)

12. Erläutern Sie das Verfahren der Constrained User Interfaces.

Limitierung der Menüführung, Shells, Sichten in Datenbanken oder Bedienelementen (Tasten).

13. Erläutern Sie das Verfahren der Access Control Matrix.

Zweispaltige Tabelle über Subjekte und Objekte, welche jeweilige Rechte definiert.
Subjekt basiert (Capability Matrix): Bob darf auf File X lesen zugreifen.
Objekt basiert (Access Control List): Auf File X dürfen lesend zugreifen: Bob, Alice...

14. Was ist der Unterschied zwischen einer Access Control List und einer Capability Table?

Subjekt basiert (Capability Matrix): Bob darf auf File X lesen zugreifen.
Objekt basiert (Access Control List): Auf File X dürfen lesend zugreifen: Bob, Alice...

15. Erläutern Sie das Verfahren der Content-Dependent Access Control.

Zugriff hängt vom Inhalt des Objektes ab. (HTTP-Proxy: Filterung von Webseiten)

16. Erläutern Sie das Verfahren der Context-Dependent Access Control.

Zugriff hängt vom Kontext ab in welchem der Zugriff erfolgt. (Stateful Paket Filter welcher Pakete zu einer bestehenden TCP-Verbindung durch lässt.)

17. Nennen Sie ein Beispiel für zentralisierte Zugriffskontrolle.

RADIUS, wird in Unternehmen als zentrale Anmeldeinstanz verwendet

18. Nennen Sie Vor- und Nachteile der zentralisierten gegenüber der dezentralisierten Zugriffskontrolle.

dezentral: siedelt Kontrollmechanismen nahe an der Ressource an, schnell und unkompliziert eingerichtet, feine Granularität, jedoch Probleme bei Konsistenz

zentral: konsistent und verlässlich, Problem bei Skalierung

19. Was ist der Unterschied zwischen administrativen, physischen und technischen Kontrollmechanismen? Zählen Sie je ein Beispiel auf!

administrativ: nicht greifbar, im Bereich des Personals/Organisation und Verwaltung
Bsp.: Sicherheitsleitlinie

physisch: bauliche Schutzmaßnahmen, dedizierte Geräte (Kartenleser, Backup-Systeme)
Bsp.: Perimetersicherheit

technisch: logische Kontrollmechanismen, hauptsächlich durch Software umgesetzt
Bsp.: Systemzugang

20. Nennen Sie je ein Beispiel für einen Kontrollmechanismus mit präventiver, erkennender sowie korrigierender Funktionalität.

präventiv: Ausweiskarten
erkennend: Überwachungskameras
korrigierend: Antivirus Software

04-Kontrollfragen

1. **Wozu dient die Identifizierung eines Subjekts?**

Feststellung der Identität, Feststellung der von anderen Subjekten unterscheidenden Eigentümlichkeit.

2. **Was muss hinsichtlich der Erzeugung einer Benutzerkennung beachtet werden?**

- standardisiertes, durchdachtes, schlüssiges Namensschema
- im System eindeutig
- Position und Aufgabengebiet sollten sich nicht ableiten lassen
- soll dauerhaft zugeordnet sein

3. **Was ist der Unterschied zwischen einer „brute force" und einer „dictionary" Attacke?**

brute force: durchprobieren aller Möglichkeiten
dictionary: durchprobieren der erfolgversprechendsten, wahrscheinlichsten (gebräuchliche Schemata)

4. **Was versteht man im Zusammenhang mit der Qualität eines Passworts unter der Entropie?**

Die Entropie gibt an wie viele (vorhersagbare) Zustände eine Zeichenfolge (Passwort) annehmen kann. Desto höher die Entropie desto besser die Qualität des Passworts.

5. **Qualität von Passwörtern: Zur Bildung ist die Größe N des Alphabets sowie die maximale Länge L des jeweiligen Passwortes gegeben. Berechnen Sie daraus die Entropie bei zufälliger Wahl der Zeichen, wenn N=78 und L=10. Berechnen Sie weiters die Entropie, wenn ein Angreifer folgende Einschränkungen annehmen kann:**
    a. **[0-9]{2}: Ziffern von 0-9 an den ersten beiden Stellen.**
    b. **[a-z]{8}: Ein gebräuchliches 8-stelliges Wort, das sich in Wörterbüchern der Größenordnung 30.000 findet.**
    c. **[!§$%&/()[]{}~*#°]{1}: Ein (!) Buchstabe des Wortes aus (b) kann durch eines dieser Sonderzeichen ersetzt werden.**

log2(78^10) = 62.8540221886 keine Ahnung ob das so stimmt!!!

a. log2(10^2*78^8) = 56.9270739407
b. log2(30000)=14.8726748803
c. log2(16^1*26^7)=36.903078027

6. **Was versteht man unter einem CAPTCHA-Test?**

Completely Automated Public Turing test to tell Computers and Humans Apart
Test welcher von Mensch leicht aber maschinell schwer lösbar ist. Verhindert brute force Angriffe bei Login-Masken.

7. **Nennen Sie die Qualitätsparameter, aus denen sich die Entropie eines Passwortes bildet.**

- größe des Alphabets
- länge des Passworts
- Zufälligkeit der Zeichenfolge

8. **Nennen Sie die Regeln zur sicheren Passwortgestaltung und -verwendung.**

- möglichst hohe Entropie
- Passwort nur einmal verwenden
- regelmäßiges Ändern nicht immer sinnvoll (-> niedrigere Passwortqualität)
- Geheimfragen nicht verwenden, sind meist leicht zu erraten

9. **Was versteht man unter Social Engineering?**

Ausnutzen von menschlichen Schwächen um sensible Informationen zu erlangen.

10. **Was ist der Unterschied zwischen Human Based und Computer Based Social Engineering?**

human based: direktes Gespräch, internetgestützte Kommunikation (phishing)
computer based: betrügerische Webseite

11. **Erläutern Sie mindestens drei Methoden zur Beeinflussung (nach Caldini), auf die ein Social Engineer seinen Täuschungsangriff aufbauen könnte.**

- Regel der Sympathie: wenn sympathisch erfüllt man eher Wünsche
- Regel der Autorität: Autorität (auch scheinbarer) wird gerne gefolgt
- Regel der Gegenseitigkeit: wenn uns jemand einen Gefallen tut, erwidern wir dies gerne

12. **Was versteht man unter „Phishing“ und unter „Spear-Phishing“?**

phishing: gefälschte elektronisch Nachricht an eine vielzahl von Benutzern um sensible Daten zu erlangen
spear phishing: zielgerichtete Variante auf eine oder wenige Personen mit maßgeschneiderter Nachricht

13. Was versteht man unter „Zwei-Faktor-Authentifizierung“?

Zwei unterschiedliche Authentifizierungsmethoden werden kombiniert, z.B.: PIN und Bankomatkarte

14. Was ist die Eigenschaft eines Challenge-Response Verfahrens?

Methode wo das Passwort nicht übertragen wird, sondern nur der Beweis angetreten wird dass man das Passwort kennt. Lösen einer Aufgabe die nur mit Kenntnis des Passworts möglich ist.

15. Beschreiben Sie die Funktionsweise von Challenge-Response Verfahren am Beispiel der HTTP-Digest Authentication.

Server erzeugt eine Zufallszahl und schickt diese an den Client. Client erzeugt den Hash über Passwort + Zufallszahl und überträgt dies an den Server. Server bildet ebenfalls Hash über das Passwort + Zufallszahl und vergleicht die Hashwerte.

16. Was ist der Unterschied zwischen dem TAN-, iTAN- und mTAN-Verfahren?

TAN: einmalig gültige Passwörter, können in beliebiger Reihenfolge verwendet werden
iTAN: TAN mit Index, es wird eine bestimmte TAN abgefragt
mTAN: TAN wird via SMS zugestellt

17. Erläutern Sie das Funktionsprinzip von RSA SecurID.

Auf Basis der Serialnummer des Tokens, einem symmetrischen Schlüssel und einer mit dem Server synchronisierten Uhr werden periodisch neue Tokencodes erzeugt. Dieser Tokencode muss bei der Authentifizierung eingegeben werden und wird vom Server überprüft.

18. **Beschreiben Sie die grundlegenden Funktionsprinzipien des S/KEY Verfahrens (Lamport's Hash) mit eigenen Worten.**

- Passwort wird weder über Netzwerk übertragen noch am Server gespeichert
- der Client hasht sein Passwort mehrmals (z.B.: 5 mal) und hinterlegt am Server das gehashte Passwort samt der Anzahl der Hash-Vorgänge
- Will der Client sich authentifizieren schickt der Server eine Indexzahl (z.B.: 4)
- der Client Antwortet mit dem der Indexzahl entsprechend gehashten Passwort (Passwort wird z.B.: 4 mal gehasht)
- Server kann nun das Passwort weiter hashen bis zu dem Hash den er selbst besitzt von dem Client und diesen vergleichen (in diesem Beispiel noch einmal hashen ergibt den Hash mit Index 5)
- Angreifer kann die Hashes nicht errechnen, da der Index immer weiter dekrementiert wird
- nur der Client kann vom Passwort ausgehend die Hashes berechnen

19. **Was macht ein Password Cracker?**

Software zur Wiederherstellung von Passwortinformationen, arbeitet mit selben Einwegfunktionen wie Authentifizierungsmechanismus.

20. **Was versteht man unter eine „Hashcracking-Tabelle"? Erläutern Sie das Funktionsprinzip und Gegenmaßnahmen.**

Vorberechnete Tabelle mit Hashwerten von Passwörtern bis zu einer bestimmten Länge. Ermöglicht einen "Time-Memory-Tradeoff". Ermöglicht Suche nach Hashwert und zugehörigem Passwort.

21. **Was versteht man im Zusammenhang mit Hashcracking unter einem „Salt-Wert"? Erläutern Sie das Funktionsprinzip.**

Ein beliebiger Werte welcher dem Passwort vor dem hashen hinzugefügt und neben dem Passwort-Hash gespeichert wird. Jedes Passwort hat einen eigenen Salt. Gegenmaßnahme gegen Hashcracking-Tabellen, da für jedes Passwort mit Salt eine eigene Tabelle notwendig ist.

22. **Was versteht man im Zusammenhang mit Hashcracking unter einem „Pepper-Wert"? Erläutern Sie das Funktionsprinzip.**

Beliebiger Wert welcher vor dem hashen zum Passwort hinzugefügt wird. Wird für alle Passwörter verwendet. Wird getrennt von Passwortdatei und möglicherweise verschlüsselt aufbewahrt. Schützt ebenfalls vor Hashcracking-Tabellen.

23. **Was sind die beiden Unterschiede zwischen einem „Salt-" und einem „Pepper-Wert"?**

Für jedes Passwort wird ein eigener Salt verwendet, der Pepper-Wert gilt für alle Passwörter. Salt wird neben dem Passworthash in der Passwortdatei gespeichert. Pepper-Wert wird separat von der Passwortdatei gespeichert, möglicherweise verschlüsselt.

24. Erläutern Sie die Idee hinter der „Password-Based Key Derivation Function 2“ (PBKDF2) im Zusammenhang mit Passwortsicherheit.

Eigentlich für Ableitung eines symetrischen Schlüssels von einem Passwort. Da aber sehr rechenintensiv sehr gut für das Speichern von Passwörtern. Angriff wird erschwert, da der Rechenaufwand extrem erhöht wird.

ITS Lektion 5

Buch [Sta14] 3.3:

1. **Erläutern Sie die Eigenschaft einer Memory Card.**

Können Daten speichern, aber nicht verarbeiten. z.B.: Kreditkarte mit Magnetstreifen, Karte mit elektrischem Speicher

2. **Erläutern Sie die Eigenschaft einer Smart Card.**

Enthält einen Mikroprozessor (CPU, RAM, ROM, EEPROM, I/O), welcher nicht nur Daten speichern, sondern auch verarbeiten kann, z.B.: kryptographische Operationen). Gibt es mit elektrischen Kontakten und Kontaktlos

3. **Klassifizieren und beschreiben Sie die drei Authentifikationsprotokolle, die bei Smart Cards in Verwendung sind.**

- statisch: Benutzer authentisiert sich gegenüber der Smart Card und die Smart Card authentisiert sich gegenüber dem Rechner.
- dynamischer Passwort generator: generiert periodisch Passwörter welche bei der Anmeldung eingegeben werden müssen. Rechner und Token müssen synchronisiert sein.
- challenge-response: Rechner generiert eine Challenge, sendet diese an den Token. Der Token generiert einen Response auf basis der Challenge. (z.B.: mit RSA)

4. **Nennen und beschreiben Sie die einzelnen Bauteile einer Smart Card (inklusive der Speichertypen).**

CPU, RAM, ROM, EEPROM, I/O

5. **Was versteht man unter einer eID Card (Electronic Identity Card)? Was sind die besonderen Eigenschaften?**

Nationaler elektronischer Ausweis, ähnlich einem Personalausweis. Ist eine Smart Card welche von Behörden ausgestellt wird und für die Authentifizierung verwendet werden kann, für staatliche und kommerzielle Services.

6. **Welche Daten sind an/auf/in einer eID Card gespeichert? Versuchen Sie diese nach Art der Verwertung/Auslesevorgang zu kategorisieren.**

aufgedruckt:
- persönliche Daten (Name, Adresse,...)
- Dokumentennummer (9 stellig alphanumerisch)
- Card access number (CAN, 6 stellig dezimal)
- Maschinenlesbar (machine readable zone, MRZ)

digital:
- digitale Repräsentation der Identität des Karteninhabers
- privater Schlüssel und Zertifikat

7. **Erläutern Sie die drei unterschiedlichen Funktionalitäten einer eID Card?**

- ePass: elektronischer Reisepass
- eID: Authentifizierung für berechtigte Dienste
- eSign: digitale Signatur

8. **Was versteht man unter "Password Authenticated Connection Establishment" (PACE)?**

Unerlaubtes auslesen der eID z.B.: via RFID wird durch eine PIN-Eingabe geschützt.

9. **Nennen Sie den Unterschied (im Anwendungsbereich) zwischen einer PIN (Personal Identification Number) und einer CAN (Card Access Number).**

PIN muss sich der Benutzer merken und ist für online Services gedacht. Die CAN wird für offline Services verwendet und ist auf der Karte aufgedruckt.

Studienbrief:

10. **Was versteht man unter einem „biometrischen Merkmal"?**

eindeutiges Merkmal einer Person, physiologisch (statisch, Fingerabdruck) oder verhaltenstechnisch (dynamisch, Tippverhalten)

11. **Nennen Sie die Anforderungen an ein biometrisches System.**

- universal: jede Person soll das Merkmal besitze
- einmalig: bei jeder Person unterschiedlich
- konstant: verändert sich nicht oder unwesentlich
- erfassbar: quantitativ messbar (als Wert mit Sensor erfassen)
- leistungsfähig: Erfassung ist hinreichend genau und performant
- akzeptiert: Verwendung wird von Benutzern akzeptiert
- überwindungs- und fälschungssicher

12. Was versteht man im Zusammenhang mit einem biometrischen System unter „Falschakzeptanzrate“?

Zulassungsrate Unberechtigter (unberechtigte Person wird Zugriff/Zutritt gewährt)

13. Was versteht man im Zusammenhang mit einem biometrischen System unter „Falschrückweisungsrate“?

Abweisungsrate Berechtigter (Berechtigter erhält keinen Zugriff/Zutritt)

14. Welchen Zusammenhang gibt es zwischen der Falschakzeptanz- und der Falschrückweisungsrate in einem biometrischen System?

Sind gegenläufige Kurven und je nach festgelegter Toleranz ist eine biometrische Authentifizierung komfortabler (weniger stritk) zu Bedienen oder sicherer (strikter).

15. Biometrische Systeme: Was versteht man unter der „Gleichfehlerrate“?

Wert bei welchem die Falschakzeptanz- und die Falschrückweisungsrate gleich sind.

16. Welchen Zusammenhang gibt es zwischen der Gleichfehlerrate und der Qualität eines biometrischen Systems?

Je niedriger dieser Wert ist, desto weniger Fehler produziert das System mit der eingestellten Toleranz, desto besser funktioniert es.

17. Nennen Sie mögliche Sicherheitsprobleme im Zusammenhang mit biometrischen Systemen.

- einschränkung des informationellen Selbstbestimmungsrechtes: erfasste Referenzdaten körperlicher Merkmale können anderweitig genutzt werden, z.B.: um Krankheit festzustellen
- Gewaltkriminalität: Körperteile werden zum Schlüssel
- unveränderlichkeit der Merkmale: kann nicht geändert werden wenn kompromittiert

18. Was versteht man unter „Single Sign On“?

Zugriff alle Dienste einer Umgebung über einen einzigen Authentifizierungsvorgang.

19. **Nennen Sie unterschiedliche Arten, wie Single Sign On Mechanismen realisiert werden können.**

- Portal: Authentifizierung für mehrere Dienste zusammengefasst, setzen eines Merkmals z.B.: Cookie, über Abfragen des Merkmals Zugriff auf Dienste
- Tickets: Kreis vertrauenswürdiger Dienste, Authentifizierung bei einem der Dienste welcher ein Ticket ausstellt, mittels des Tickets Zugriff auf andere Dienste
- lokale Stellverträterlösung: Authentifizierung bei lokaler Software welche das Anmelden bei den Diensten übernimmt z.B.: KWallet

Buch [Sta14] 3.5:

20. **Nennen Sie Gefährdungen, die sich bei entfernter Authentifizierung zusätzlich ergeben.**

Abhören des Passworts oder Replay-Attacken

21. **Challenge-Response Protocol bei passwortbasierter Authentifikation:**
    a. **Erläutern Sie den Protokollablauf.**
    b. **Nennen Sie die Vorteile dieses Schemas.**

a. Server schickt einen nonce an den Client und definiert eine Hashfunktion und eine weiter Funktion für das kombinieren des Passworthashes und der Nonce. Der Client bildet den Hash über Passwort und verknüpft den Passwort-Hash und die Nonce mit der zweiten Funktion. Das Ergebnis schickt dieser an den Server. Der Server hat auf seiner Seite den selben Vorgang durchgeführt und vergleicht die Ergebnisse.
b. Passwort wird nicht übertragen, sondern es wird nur anhand der gelösten Aufgabenstellung bewiesen dass man das Passwort kennt

22. **Challenge-Response Protocol: Erläutern Sie den Protokollablauf bei tokenbasierter Authentifikation.**

Der Server schickt eine Nonce und definiert eine Hashfunktion und eine weiter Funktion für das Verknüpfen von Nonce und Passwort. Der User gibt bei seinem Token das Passwort ein, wodurch dieser den Passcode oder das One Time Password für die Authentifizierung frei gibt. Passcode oder One Time Password werden mittels der Hashfunktion gehasht und mit der zweiten Funktion werden Nonce und Passwordhash verknüpft und an den Server geschickt. Der Server hasht ebenfalls den Passcode oder das OTP und verknüpft es mit der Nonce und kann durch vergleichen der Ergebnisse den User authentifizieren. Zu beachten ist dass bei einem One Time Password der Token mit dem Server synchronisiert sein muss.

11.3 Kontrollfragen

1. Was versteht man unter einem AAA-System?

System welches Benutzer für bestimmte Dienste authentifiziert und autorisiert. Weiters erfolgt ein accounting, also sammeln von Nutzungsdaten für z.B.: die Abrechnung.

2. Was ist Kerberos und welche zwei Aufgaben erfüllt es?

Kerberos ist ein Client/Server Authentifizierungsprotokoll in verteilten Umgebungen (SSO, Single-Sign On), basierend auf symmetrischer Kryptographie.
Aufgaben: Authentifizierung und vergabe symmetrischer Sitzungsschlüssel

3. Aus welchen Komponenten besteht das Key Distribution Center bei Kerberos und welche Aufgaben haben diese beiden Komponenten?

- Authentifizierungsserver (AS): speichert symmetrische Schlüssel, authentifiziert principals
- Ticket Granting Server (TGS): stellt Tickets für den Zugriff auf Ressourcen aus

4. Was versteht man bei Kerberos unter einem Ticket?

Ein Ticket wird vom Key Distribution Center (KDC) für einen Principal ausgestellt, welcher sich damit bei einem anderen Principal authentisieren kann.

5. Was versteht man bei Kerberos unter einem Ticket Granting Ticket?

Initiales Ticket welches während der Authentifizierung des principals verwendet wird. (enthält Angaben zum Benutzer, Gültigkeitsdauer, Sitzungsschlüssel)

6. Welche Aufgabe hat bei Kerberos ein Authentikator?

Wird vom principal zum KDC (Key Distribution Center) geschickt damit dieser die Authentizität des principals überprüfen kann. (besteht aus Kennung des principal, dessen IP und ein Timestamp, verschlüsselt mit dem Sitzungsschlüssel)

7. Nennen Sie zwei Sicherheitsprobleme im Zusammenhang mit Kerberos.

- schwache Passwörter ermöglichen Angreifer Angriff auf alle Systeme auf die der principal Zugriff hat.
- alle Schlüssel der principals sind mit einem Schlüssel am Server verschlüsselt, wird dieser kompromittiert müssen alle Passwörter geändert werden.
- Authentizität des Clients über IP-Adresse geprüft -> kann leicht gespoofed werden
- Single Point of Failure

8. Was ist RADIUS und wo wird es vorrangig eingesetzt?

- Remote Authentication Dial-In User Service
- Client/Server Protokoll
- AAA
- basiert auf UDP
- zentrale Authentifizierung von Einwahlverbindungen

9. Beschreiben Sie die Architektur von RADIUS mit eigenen Worten.

Clients authentisieren sich nicht direkt am RADIUS Server selbst, sondern auf einem RADIUS Client, welcher die Credentials als access request an den Server weiterleitet. Dort werden diese validiert und zurückgemeldet ob User accepted, rejected wurde oder bei challenge weiter Authentifizierungsinformationen notwendig sind. Gegebenenfalls werden noch netzwerkspezifische Konfigurationsparameter übermittelt.

10. Nennen Sie drei mögliche Server-Responses auf einen Access-Request eines RADIUS Clients.

access-accept:	User erhält Zugriff
access-reject:	User wird Zugriff verweigert
access-challenge	Server fordert weitere Authentifizierungsinformationen

11. Nennen Sie das Nachfolger-Protokoll von RADIUS.

Diameter

12. Wie unterscheiden sich Kerberos und RADIUS hinsichtlich ihres Funktionsumfanges?

Kerberos führt rein Authentifizierung durch, während RADIUS Authenfizierung, Authorisierung und Accounting übernimmt.

ITS Lektion 7

Buch [Sta14] 8.1-5 (IDS)

1. **Beschreiben Sie die Motive folgender Gruppen von Eindringlingen:**
    a. **Cyberkriminelle**
    b. **Aktivisten**
    c. **Staatsnahe bzw. von diesem gesponserte Organisationen**
    d. **Hacker aus Leidenschaft, Ehrgeiz, Reputation**

a. Individuen oder Mitglieder des organisierten Verbrechens, finanziell motiviert
b. oft Insider, oder Mitglied einer Gruppe von außenstehenden Angreifern, sozial oder politisch motiviert, auch hacktivists genannt
c. Gruppe von Hackern welche staatlich finanziert wird, deren alltägliche Arbeit
d. motiviert durch die technische Herausforderung oder Reputation in der Gruppe, erforschen von Systemen

2. **Erläutern Sie die einzelnen Schritte eines Einbruchs.**

- Ziel bestimmen und Informationen einholen (öffentliche Informationen - technisch od. nicht technisch, Scans,)
- Erster Zugriff (Ausnutzen einer Schwachstelle um Zugriff zu erlangen)
- Rechteausweitung (ausnutzen einer lokalen Schwachstelle um höhere Rechte zu erlangen)
- Informationen sammeln oder andere Systeme angreifen
- permanenten Zugriff einrichten (Backdoor)
- Spuren verwischen (Beweise vernichten, Logs manipulieren)

3. **Nennen und Beschreiben Sie die drei logischen Komponenten eines IDS.**

- Sensor: sammelt Daten (Netzwerkpakete, Logs, Syscalls), sendet diese an Analyzer
- Analyzer: stellt fest ob ein Angriff stattfindet/fand, sendet Alarme an das User Interface, enthält Informationen über den Angriff und möglicherweise Beweise, Sensordaten werden möglicherweise für weiter Analyse gespeichert
- User Interface: zeigt Alarme über Angriffe an, ermöglicht steuerung des IDS

4. **Unterscheiden Sie**
    a. **Host-based IDS (HIDS)**
    b. **Network-based IDS (NIDS)**
    c. **Distributed/hybrid IDS**

a. Monitort einzelnen Host durch Analyse von Process Identifiers, Systemcalls, Logs
b. Monitort Netzwerktraffic von Netzwerksegmenten, analysiert Netzwerk-, Transport- und Applikationsprotokolle
c. Kombiniert die Informationen verschiedener Sensoren, HIDS und NIDS, in zentralem Analyzer, für bessere Identifikation von Angriffen

5. **Nennen Sie drei Vorteile, die ein Einsatz eines IDS bringt.**

- wird ein Angriff schnell genug erkannt, kann dieser gestoppt werden bevor ein Schaden entsteht
- ein effektives IDS kann abschreckend wirken
- ermöglicht das Sammeln von Informationen über Angriffstechniken, wodurch präventive Maßnahmen gestärkt werden können

6. **Was ist der Unterschied zwischen "False Positive" und "False Negative"? Bei welchen Konfigurationen (restriktiv/locker) kommt es eher zum einen bzw. eher zum anderen?**

- false positive: autorisierte User werden als Angreifer identifiziert
- false negative: Angreifer wird nicht als Angreifer identifiziert
- bei einer lockeren, weit gefassten Konfiguration kommt es zu mehr "False Positives", da sich Angreiferverhalten und normales Verhalten teilweise überschneiden und Aktivitäten welche innerhalb dieser Überschneidung liegen als Angriff gewertet werden

7. **Was sind die Requirements für ein IDS?**

- kontinuierlicher Betrieb, ohne menschliche Überwachung
- Fehlertolerant, soll Betriebszustand selbst wiederherstellen können
- Unterwanderungsresistent (soll sich selbst monitoren)
- minimaler Overhead auf dem System auf dem es betrieben wird
- Konfiguration soll anpassbar sein auf zu monitorendes System
- soll sich über die Zeit Änderungen beim System und dem User-Verhalten anpassen
- Skalierbarkeit
- Ausfallsicherheit (fällt ein Teil des IDS aus, soll der Rest so wenig wie möglich betroffen sein)
- dynamische rekonfiguration (ohne neustart)

8. **Unterscheiden und bewerten Sie**
    a. **Anomalieerkennung**
    b. **Signaturerkennung**
    c. **Heuristische Erkennung**

a. Zuerst werden Daten über normales Verhalten über einen Zeitraum gesammelt. Für die Erkennung wird aktuell erfasstes Verhalten mit den gesammelten Daten verglichen um festzustellen ob es sich um normales Nutzerverhalten oder um einen Angreifer handelt
b. Für bekannte Angriffe wird eine Signatur erstellt anhand derer ein Angriff erkannt wird (kann nur bekannte Angriffe erkennen)
c. Definieren eines Regelwerks, anhand welchem entschieden wird ob es sich bei erfassten Verhalten um einen Angriff handelt (kann nur bekannte Angriffe erkennen)

9. **Statistische Anomalieerkennung: Unterscheiden Sie die univariate, multivariate sowie die Zeitreihenanalyse.**

Für die statistische Analyse werden statistische Profile von überwachten Metriken erzeugt.
univariate: jede erfasste Metrik wird unabhängig von anderen ausgewertet
multivariate: zwischen erfassten Metriken wird eine Korrelation hergestellt
Zeitreihenanalyse: Anordnung und Zeit zwischen den beobachteten Events werden verwendet um eine bessere Klassifizierung zu erreichen

10. **Anomalieerkennung: Was ist der Unterschied zwischen dem wissensbasierten Ansatz und maschinellem Lernen. Nennen Sie Vor- und Nachteile.**

- wissensbasiert: basiert auf Regeln welche während einer Trainingszeit erstellt werden. Vorteil: robust, flexibel; Nachteil: Regeln schwer zu erstellen, benötigt viel Zeit und menschliche Experten welche den Prozess unterstützen
- maschinelles Lernen: während der Trainingszeit werden automatisch Daten erfasst und automatisch ein Modell für die Klassifizierung erstellt.
  Vorteil: kein menschlicher Eingriff notwendig, relativ effizient; Nachteil: benötigt viel Zeit und Rechnerressourcen

11. **Host-based IDS: Nennen Sie gängige Datenquellen.**

- Überwachen von System Calls
- Logfiles
- Dateiintegrität (Checksummen)
- Überwachen der Registry

12. Network-based IDS: Welche beiden Inhalte werden im Netzwerk typischerweise analysiert?

- Muster im Netzwerkverkehr
- Analyse von Inhalt des Netzwerkverkehrs

13. Unterscheiden Sie Inline- und Passiv-Sensoren hinsichtlich Implementierung, Funktionalität bzw. Überwachungstätigkeit.

- inline: Netzwerkverkehr eines Netzwerksegments muss durch den Sensor fließen, kann Angriffe auch aktiv blockieren
  Vorteil: keine zusätzliche Hardware nötig, kann in Switch oder Firewall implementiert sein
  Nachteil: kann Durchsatz verringern, wenn Pakete erst nach Analyse freigegeben werden
- passiv: Sensor bekommt Kopie jedes Paketes (durch physical tap), Netzwerkverkehr fließt nicht durch Sensor
  Vorteil: Netzwerkverkehr wird nicht beeinflusst
  Nachteil: kann nicht aktiv Angriffe blockieren, benötigt zusätzliche Hardware

14. Dislokation des NIDS: Nennen Sie Vorteile folgender Einsatzorte:

a. Teil der externen Firewall
b. Außerhalb der externen Firewall (Richtung WAN)
c. Internes LAN-Segment (Serverbereich, Workstationbereich)

a.
i. erkennt Angriffe von Außerhalb
ii. zeigt Probleme mit der Firewall Policy oder Performanz
iii. erkennt Angriffe auf Web- und FTP-Server
iv. Angriff kann durch ausgehenden Traffic erkannt werden (wenn nicht durch eingehenden erkannt)

b.
i. dokumentiert Anzahl und Typ der Angriffe aus dem Internet, bevor sie von der Firewall gefiltert werden

c.
i. da nur ein Subset an Geräten geschützt werden muss, kann Performanz verbessert werden durch Einstellung auf bestimmte Protokolle und Attacken
ii. monitort trotzdem großteil des Netzwerkverkehrs
iii. Erkennt unerlaubte Aktivität der User
iv. Erkennt Attacken gegen kritische Systeme
v. ermöglicht Fokus auf Assets mit größter Bedeutung

15. **Nennen Sie Beispiele für Vorkommnisse im Netzwerk, die erkannt werden sollten durch**
    a. **Technologien der Signaturerkennung**
    b. **Technologien der Anomalieerkennung**

    Begründen Sie Ihre Beispiele.

a.
   i. Application/Transport/Network layer reconnaissance and attacks
   ii. Erkennung unerlaubter Services
   iii. Policy violations

Verstöße/Attacken sind bekannt und lassen sich dadurch in Signaturen fassen.

b.
   i. DoS Attacken
   ii. Scanning (Nmap)
   iii. Worms (Erkennung anormalen Netzwerktraffic)

Erzeugen anormalen Netzwerktraffic, welcher sich leicht von normalen Traffic unterscheiden lässt.

16. **Was versteht man unter "Stateful Protocol Analysis" (SPA)?**

Erkennung von Anomalien im Netzwerktraffic durch von Herstellern gelieferte universelle Profile.

Buch [Sta14] 9.1-5 (Firewalls)

17. **Nennen Sie die grundlegenden Aufgaben einer Firewall sowie die daraus resultierenden Anforderungen (Design Goals).**

- Der gesamte Traffic muss die Firewall passieren (erreicht durch blockieren von Traffic welcher nicht die Firewall passiert)
- Nur autorisierter Traffic darf passieren, definiert durch Security Policies
- Die Firewall muss immun gegen Angriffe sein (gehärtetes Betriebssystem, Trusted Computing bieten sich an)

18. **Welche Firewallklassen ("Types") kennen Sie?**

- Paketfilter (stateless/stateful)
- Application Level Proxy (Applikationsschicht)
- Circuit Level Proxy (Transportschicht)

19. Welche Firewallarchitekturen (“Basing”, “Location”, “Topology”) kennen Sie?

Single-Box Firewalls: (Firewall-Funktionalität in einer Box konzentriert bzw. befindet sich an/in einem Host)

- Personal Firewalls: auf Workstations zu finden, Untergruppe der Host-Base Firewalls
- Host-Based Firewalls: auf Host betriebene Filterkomponente
- Screening Router: Router mit Paketfilter (im SOHO Bereich)
- Dual-Homed Host (Single Bastion Inline): Bastion Host zwischen zwei Netzen, Routing deaktiviert -> Verkehr läuft über Application Level Proxy

Screened-Host:

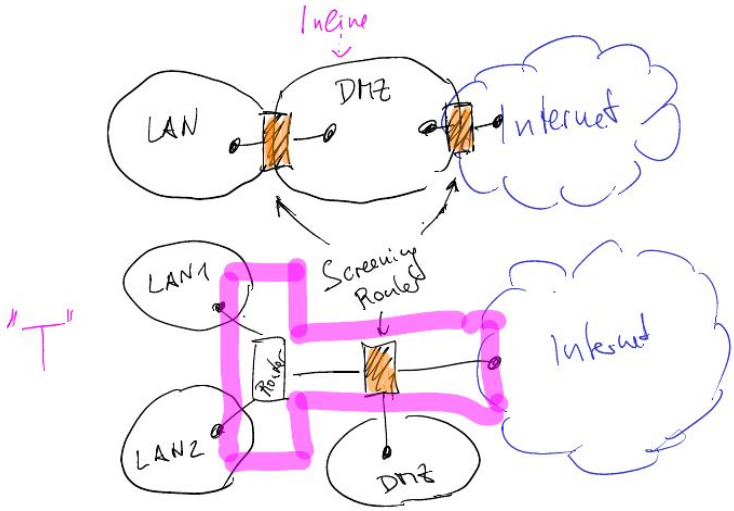
- Nur Bastion Host mit Application Level Proxy von extern erreichbar, durch Paketfilter (Screened Router) abgeschirmt. Hosts von extern nur über Bastion Host erreichbar.
- Mögliche Ausnahmen: unkritischer Verkehr kann direkt zu Hosts durchgelassen werden; Konfiguration möglich dass Clients nur über Bastion Host auf externes Netz zugreifen können

Screened-Subnet:
Double Bastion Inline:

- internes und externes Netz durch zusätzliches Netzsegment getrennt -> DMZ
- externer Screening-Router schützt DMZ und internes Netz vor Angriffen von extern
- interne Screening-Router schützt internes Netz vor Angriffen aus externem und der DMZ und schützt DMZ vor Angriffen aus internem Netz
- DMZ kann nach extern gerichtete Dienste beinhalten z.B.: Webserver

Single bastion T:

- vereinfachte Version von Double Bastion Inline
- interner und externer Router werden zu einem zusammengefasst, mit 3 Netzwerkschnittstellen



20. Was ist der Unterschied zwischen einer Firewallklasse und einer Firewallarchitektur?

Firewall-Klasse: Art der Filtermethode
Firewall-Architektur: Aufbau und Position im Netzwerk

21. "Packet Filtering Firewall":
   a. Was ist die Charakteristik eines Paketfilters?
   b. Was sind die Vorteile eines Paketfilters?
   c. Was sind die Schwächen eines Paketfilters?
   d. Nennen Sie mögliche Angriffe auf Paketfilter sowie Gegenmaßnahmen.

a. Filtert auf Basis der Verkehrsdaten, (Src/Dst IP/Port, Protokoll, Interface) ISO/OSI Schicht 2-4
b. einfach zu realisieren, performant, nicht anwendungsspezifisch
c. Filterung nur anhand der Informationen im Paket-Header -> leicht zu fälschen, grobgranular, keine Filterung in der Applikationsschicht
d.
   i. IP address spoofing: verwerfen von Paketen welche eine interne Src-IP haben, aber am externen Interface ankommen
   ii. Source routing attacks (Route wird vom Angreifer vorgegeben um Sicherheitsmaßnahmen zu umgehen): verwerfen aller Pakete die diese Option verwenden
   iii. Tiny fragment attacks (IP Pakete so stark fragmentieren, dass TCP Header in zusätzlichem Paket ist -> Firewall überprüft normalerweise nur erstes Paket): festlegen dass Verbindungen nur dann akzeptiert werden, wenn ein minimum des TCP Headers im ersten Paket enthalten ist

22. Was ist der Unterschied zwischen einem "stateless" und einem "stateful" Paketfilter?

- stateless: Weiterleitung hängt nur vom jeweiligen Paket ab, nicht vom Kontext
- stateful: Kontext der Verbindung wird beachtet, dynamische Filterregel welche bei erfolgreich aufgebauter Verbindung die Antwortpakete des Gegenübers automatisch zulässt

23. “Application Level Gateway”:

a. Was ist die Charakteristik eines Application Level Gateways?

b. Was sind die Vorteile eines Application Level Gateways?

c. Was sind die Nachteile eines Application Level Gateways?

a. fungiert als Stellvertreter in der Applikationsschicht, versteht das Protokoll der Applikation und kann somit feingranularer filter
b. genauere Filterung, genaueres logging und auditing
c. komplexer, höherer Rechenaufwand, möglicherweise aufbrechen von Ende-zu-Ende-Verschlüsselung

24. “Circuit Level Gateway”:

a. Was ist die Charakteristik eines Circuit-Level Gateways?

b. Erläutern Sie den Ablauf der Funktion eines Circuit-Level Gateways am Beispiel des SOCKS-Protokolls.

a. Arbeitet als Stellvertreter in der Transportschicht, hat die möglichkeit User zu authentifizieren, ist nicht anwendungsspezifisch
b. Es wird ein SOCKS-Server benötigt welcher als Mittelsmann fungiert. Die Anwendungen müssen so modifiziert/konfiguriert sein, dass sie Verbindungen über den SOCKS Server aufbauen. Der Client baut einen TCP-Verbindung zum SOCKS-Server auf, authentisiert sich und sendet einen relay request. Der Server verifiziert den relay request und baut gegebenenfalls die Verbindung auf. Für UDP werden die UDP Pakete über eine TCP-Verbindung übertragen.

25. Was ist ein “Bastion Host”? Nennen Sie die grundlegenden Designprinzipien.

Sicherheitskritischer Rechner, der meist einen application-level proxy betreibt

- speziell gesichertes/gehärtetes Betriebssystem
- nur benötigte Services installiert
- zusätzliche Authentifizierung für Proxy Service
- unterstützt nur ein Subset der Kommandos der Applikationen
- lässt nur Verbindungen von bestimmten Hosts zu
- detailliertes Auditlog
- kleines Proxy-Paket, ausgelegt auf sicherheit
- Proxies am Host sind unabhängig voneinander
- Partitionen mit Executesables und Konfigurationsdateien können read only sein -> erschwert installation eines Trojaners
- jeder unprivilegierte User läuft in eigenem privaten und gesichertem Verzeichnis

26. Erläutern Sie die Funktionsweise von "Host-Based" Firewalls und im Speziellen jene einer "Personal Firewall".

Softwaremodul direkt am Host, Filterung kann genau auf Host abgestimmt werden (anwendungsspezifische Filterung, Verzahnung mit Betriebssystem), unabhängig von restlicher Topologie, zusätzlicher Schutz zu Netzwerk-Firewalls

27. Was sind die wichtigsten Aufgaben einer "Personal Firewall"?

- schützt vor Zugriffen von außen
- überwachen des ausgehenden Datenverkehrs

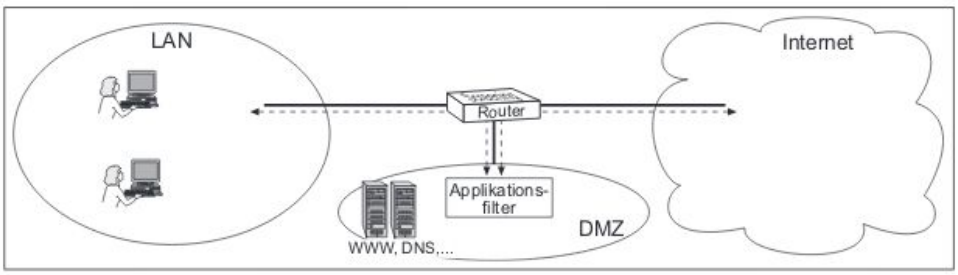
28. DMZ-Netzwerke:

a. Erläutern Sie mögliche Architekturen.
b. Welche Systeme/Dienste werden üblicherweise in einer DMZ betrieben?
c. Welche Aufgaben hat die externe Firewall?
d. Welche Aufgaben hat die interne Firewall?

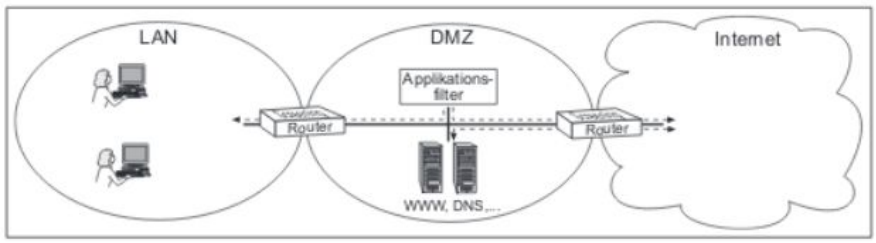
a.
   i. Single bastion T: Firewall zwischen intern, extern und DMZ
   ii. Double bastion inline: jeweils Firewall zwischen intern - DMZ und DMZ - extern
   iii. Double bastion T: DMZ befindet sich auf separatem Interface auf der Bastion Firewall
b. Mail, Web Server, FTP, DNS
c. Schützt die DMZ und das interne Netz vor Attacken aus dem externen Netz, ist weniger stringent eingerichtet
d. Schützt das interne Netz vor Attacken aus der DMZ und dem externen Netz, Schützt die DMZ vor Attacken aus dem internen Netz, ist stringenter eingerichtet als die externe

29. Skizzieren Sie folgende Architekturen: “Single Bastion T”, “Double Bastion T”, “Double Bastion Inline”.

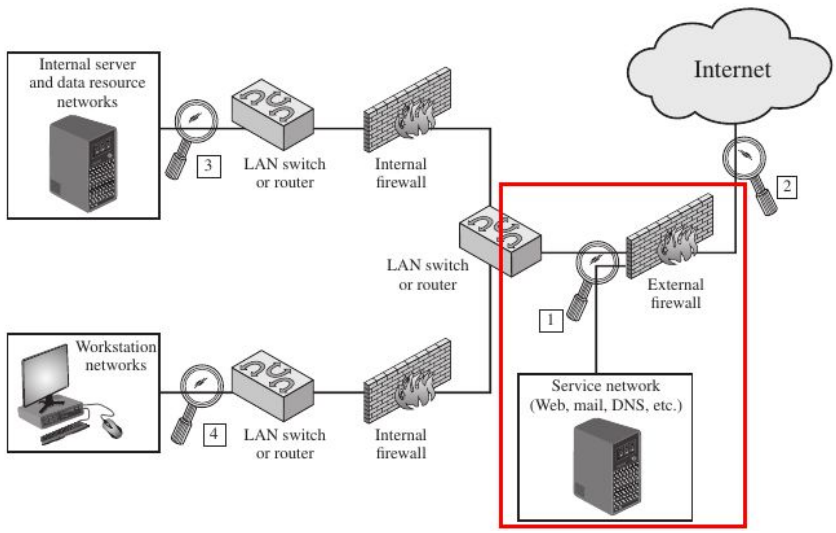
Single Bastion T:



Double Bastion Inline:



Double Bastion T:



Buch [Sta14] 9.6 (Intrusion Prevention Systems)

30. Was ist der Unterschied zwischen einem IDS und einem IPS?

Ein IDS erkennt Angriff und meldet diese, ein IPS blockiert darüber hinaus aktiv den Angriff.

31. **Nennen Sie Beispiele verdächtiger Systemaktionen (-verhalten), die ein hostbasiertes IPS (HIPS) analysieren/erkennen könnte.**

- modifikation von Systemressourcen (Rootkits, Trojaner)
- Privilege-escalation exploits
- Buffer-overflow exploits
- Zugriff auf Mail-Kontaktlisten
- Directory traversal

32. **Welche zusätzliche Funktionalität besitzt ein netzwerkbasiertes IPS (NIPS) im Vergleich zu einem NIDS?**

Die Autorität Netzwerkpakete zu verändern oder zu verwerfen und TCP Verbindungen zu unterbrechen

ITS Lektion 8

Buch [Sta14] 24.3 (IEEE 802.11 WLAN Overview)

1. **Erläutern Sie die Grundbegriffe**
    a. **Infrastruktur-Modus vs. Ad-hoc-Modus**
    b. **Independent Basic Service Set (IBSS) vs. Basic Service Set (BSS) vs. Extended Service Set (ESS)**
    c. **Distribution System (DS) sowie die Ausdrücke "distribution" vs. "integration"**

a. Infrastruktur-Modus: Wireless Network mit einem Access Point über welchen die Kommunikation läuft
   Ad-hoc-Modus: Peer-to-Peer Netzwerk zwischen zwei oder mehreren Rechnern, ohne Access Point
b. IBSS: ad hoc network, alle Stationen kommunizieren direkt
   BSS: Set von Stationen welche welche das selbe MAC (Medium Access Control) Protocol ausführen und sich dasselbe geteilte Wireless Medium teilen.
   ESS: besteht aus zwei oder mehreren BSS, verbunden durch ein DS
c. DS: verbindet die AP (Access Points) mehrerer BSS über z.B.: ein LAN, ein Switch oder ein anderes kabelloses Netzwerk.

2. **"Associated": Was bedeutet dieser Zustand zwischen STA (Station) und AP (Access Point)?**

Initiale Verbindung zwischen zwischen STA und AP. Bevor Datenübertragung erlaubt ist, muss die Identität und Adresse festgestellt werden.

Buch [Sta14] 24.1 (Wireless Security - Network Threats, Security Measures)

3. **Nennen Sie Schlüsselfaktoren, die den erhöhten Sicherheitsbedarf von Drahtlosnetzwerken im Vergleich zu verkabelten Netzwerken begründen.**

- Kanal: broadcast communication -> anfälliger auf abhören und stören (jamming)
- Mobilität: höheres Risiko durch höhere Portabilität
- Ressourcen: mobile Geräte haben meist limitierte Ressourcen -> anfällig auf DoS und Maleware
- Erreichbarkeit: Geräte sind teilweise unbeaufsichtigt zugänglich (z.B.: Sensoren)

4. **Zählen Sie jene Bedrohungen auf, die Kabellos-Netzwerken unterliegen.**

- Accidential assocation: unbeabsichtigtes verbinden mit einem anderen Netzwerk
- Malicious association: böswilliger AP um User-Passwörter abzugreifen
- Ad hoc networks: fehlende zentrale Kontrolle
- Identity theft (MAC spoofing): spoof der MAC-Adresse einer Station welche höhere Privilegien hat
- Man-in-the-middle attacks
- DoS: einfach, da shared medium
- Network injection: nicht gefilterte Routing-Protokolle

5. **Funkübertragung von Daten: Nennen Sie Bedrohungen und Gegenmaßnahmen.**

Bedrohung:
- Abhören
- verändern und injizieren von Messages

Gegenmaßnahmen:
- signal hiding: ssid broadcast deaktivieren, reduzieren der Signalstärke, APs im inneren des Gebäudes installieren, nicht bei Fenster und Türen
- encryption

6. **Gefährdungen im WLAN. Zählen Sie hinsichtlich der angeführten Schutzziele mögliche Gefährdungen/Szenarien auf:**
    a. **Vertraulichkeit**
    b. **Authentizität/Integrität**
    c. **Verfügbarkeit**

a. WLAN ohne Authentifizierung und Verschlüsselung
b. Man-in-the-middle Attacke (ändern und injizieren von Paketen)
c. DoS, Störsender

7. **Wireless Access Points: Wie kann man unautorisierten Zugriff verhindern?**

802.1X standard für port-based network access control, bietet Authentifizierungsmechanismen für kabellos und kabelgebundene Netzwerke

8. **Nennen Sie Gegenmaßnahmen, um den in Frage 4 zu erläuternden Bedrohungen gerecht zu werden.**

- Verschlüsselung
- Antivirus, Anti-Spyware
- SSID broadcast deaktivieren
- ändern des SSID Namen
- Default-Administratorpasswort ändern
- MAC Filterung

Buch [Sta14] 24.4 (IEEE 802.11i WLAN Security) bzw. [BSI-09]

9. **Erläutern Sie die Schwachstellen des WEP-Standards hinsichtlich der Schutzziele Authentizität, Integrität sowie Vertraulichkeit. (siehe [BSI-09], A.2.3)**

Authentizität: AP muss sich gegenüber Client nicht authentifizieren
Integrität: CRC-Checksumme unsicher -> Pakete können beliebig manipuliert werden
Vertraulichkeit: WEP-Schlüssel kann aus aufgezeichneten Paketen berechnet werden

10. **WPA - Wi-Fi Protected Access (siehe [BSI-09], A.2.5):**
    a. **Was sind die Hauptziele des WPA-Designs im Vergleich zu WEP?**
    b. **Was ist der Unterschied zwischen WPA2-Enterprise und WPA2-Personal?**

a. Beseitigung der Schwachstellen im WEP durch bessere Sicherung der Integrität, Authentizität und Vertraulichkeit
b. Enterprise: Authentisierung und Schlüsselverwaltung über RADIUS
   Personal: Authentifizierung über PSK (Pre-Shared Key)

11. **Was ist der Unterschied zwischen WPA2, Robust Security Network (RSN) und 802.11i?**

802.11i ist ein Standard welcher die Schwächen des 802.11 (WEP) ausbessern soll. Hersteller können WPA2 zertifiziert sein wenn sie den kompletten 802.11i Standard abdecken. Die finale Form des 802.11i wird RSN genannt.

12. **Was ist WPS (Wi-Fi Protected Setup) und wie funktioniert es? (siehe [BSI-09], A.2.6)**

Vereinfachte Setup-Methode für den privaten Bereich. AP erzeugt automatisch eine SSID und teilt diese dem Endgerät mit. Am AP wird anschließend ein Knopf gedrückt und dadurch wird vom AP das Schlüsselmaterial erzeugt und ausgetauscht (erfolgt mittels Diffie Hellmann). Man-in-the-middle kann während dieser Phase nicht ausgeschlossen werden

13. **Welche drei Dienste definiert die 802.11i Spezifikation?**

Authentication, Access control, Privacy with message integrity

14. 802.11i Spezifikation: Erläutern Sie die Aufgaben der Dienste

- **a. Authentifikation**
- **b. Netzzugang**
- **c. Vertraulichkeit und Integrität der Nachrichten**

a. Protokoll für Kommunikation zwischen User und AS (authentication server). Authentifizierung, erzeugung temporärer Schlüssel
b. forciert die Authentifizierung (-> sonst kein Zugriff), kümmert sich um richtiges routing der Pakete und erleichtert den Schlüsselaustausch
c. Verschlüsselung und dass die Daten nicht verändert wurden.

15. 802.11i Spezifikation: Nennen Sie die Protokolle der Dienste

- **a. Netzzugang**
- **b. Authentifikation und Schlüsselerzeugung**
- **c. Vertraulichkeit, Authentizität des Datenursprungs und Integrität der Nachrichten**

a. IEEE 802.1 Port-based Access Control
b. EAP (Extensible Authentication Protocol)
c. TKIP (Temporal Key Integrity Protocol), CCMP (Counter Mode with Cipher Block Chaining MAC Protocol)

16. 802.11i Spezifikation: Nennen Sie Algorithmen für die Dienste

- **a. Vertraulichkeit**
- **b. Integrität und Authentizität des Datenursprungs**

a. TKIP (RC4), CCM (Counter with CBC-MAC - AES-CTR), NIST Key Wrap
b. HMAC-SHA-1/MD5, TKIP, CCM (AES-CBC-MAC)

17. **Beschreiben Sie die fünf Phasen im Zyklus eines 802.11i Netzwerkes:**
    a. **Discovery (802.11i)**
    b. **Authentifikation (802.1X/EAP)**
    c. **Schlüsselmanagement (802.11i)**
    d. **Vertrauliche Datenübertragung (802.11i)**
    e. **Verbindungsabbau (802.11i)**

a. AP: Beacons und Probe Responses um IEEE 802.11i security policies anzubieten. STA verwendet diese um ein WLAN zu identifizieren und eine assocation aufzubauen -> entnimmt cipher suites und authentication Mechanismus aus Beacons und Probe Responses
b. STA und AS (authentication system) überprüfen gegenseitig die Identitäten, AP blockiert nicht authentifizierten Traffic, transportiert Authentifizierungs-Traffic zwischen STA und AS
c. Erzeugung der Schlüssel, installieren auf STA und AP
d. Verschlüsselte Datenübertragung zwischen STA und AP, aber nicht darüber hinaus
e. Verbindung wird zwischen STA und AP abgebaut

18. **Welche Sicherheitsparameter (Security Capabilities) werden im Zuge des Discovery ausverhandelt?**

- Protokolle für Vertraulichkeit und MPDU-Integrität (für Traffic zwischen STA und AP)
- Authentifizierungsmethode
- kryptographische Schlüsselverwaltung

19. **802.1X - Port Based Access Control: Setzen Sie das Konzept der Ports (logisch, kontrolliert, unkontrolliert) in einen Kontext mit den beiden Schnittstellen eines Access Point.**

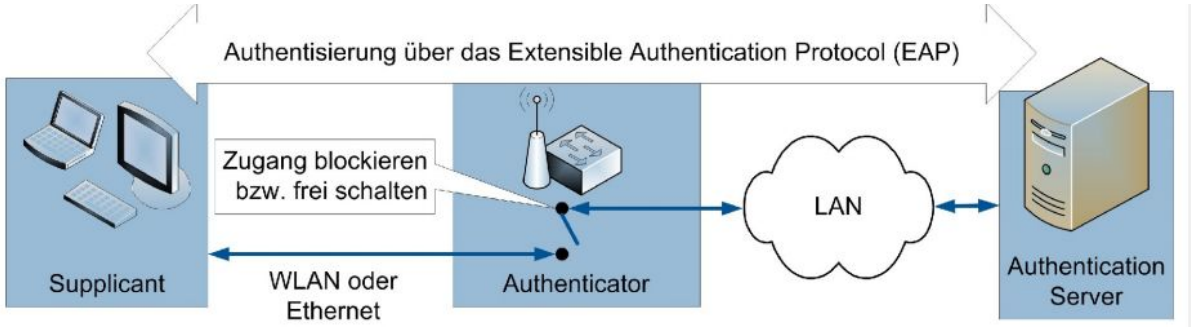
Sind logische Einheiten welche auf die physikalischen Netzwerkverbindungen (Richtung BSS und Richtung DS) des Authentikator (AP) referenzieren.

20. **Extensible Authentication Protocol (EAP): Erläutern Sie das Prinzip dieses Authentifizierungs-Frameworks nach [BSI-05], 7.1.1.**

Kein Authentifizierungsverfahren, sondern Gerüst in welchem Authentifizierungsverfahren (EAP-Typ, EAP-Methode) eingebettet sind. -> Modulares System
Macht Authentifizierungsverfahren auf Layer 2 verfügbar, damit Authentifizierung stattfindet bevor auf höheren Schichten kommuniziert wird.

21. **EAP im WLAN: Skizzieren Sie grob die Architektur/Rollenverteilung unter Einbeziehung von Supplicant, Authenticator und Authentication Service. Wo finden sich "Wireless Station" (STA) sowie der Access Point (AP) wieder? Betrachten Sie dazu die Grafik in der Slideshow im Lektionsblock (Semesterplan).**

Verbessern, eap nur bis ap!



22. **Welchen Zusammenhang gibt es zwischen 802.1X, EAP und EAPOL (EAP over LAN)?**

802.1X ist der Standard, hat kein eigenes Authentifizierungsprotokoll definiert und empfiehlt deshalb EAP/EAPOL für die Authentifizierung.

23. **WPA/WPA2-Enterprise: Erläutern Sie die drei Phasen der Authentifikation, wie vom IEEE 802.11 Standard vorgegeben. Über welche beiden Protokolle (STA <-> AP <-> AS) wird der damit abgebildete EAP-Exchange typischerweise transportiert?**

- STA baut association mit AP auf und startet Authentifizierung via EAP gegenüber Authentikator (AP)
- AP stellt RADIUS Request an AS (Authentication Server)
- AS stellt an die STA Challenge Request über AP, welchen STA beantwortet

STA <-> AP -> EAPoL
AP <-> AS -> RADIUS

24. Betrachten und unterscheiden Sie die unterschiedlichen EAP-Methoden (EAP-MD5, EAP-TLS, EAP-TTLS, PEAP) in der Slideshow im Lektionsblock (Semesterplan) sowie unter [BSI-09], A2.4.3 und [BSI-05], 7.2.

EAP Selection Quick Reference for common Types

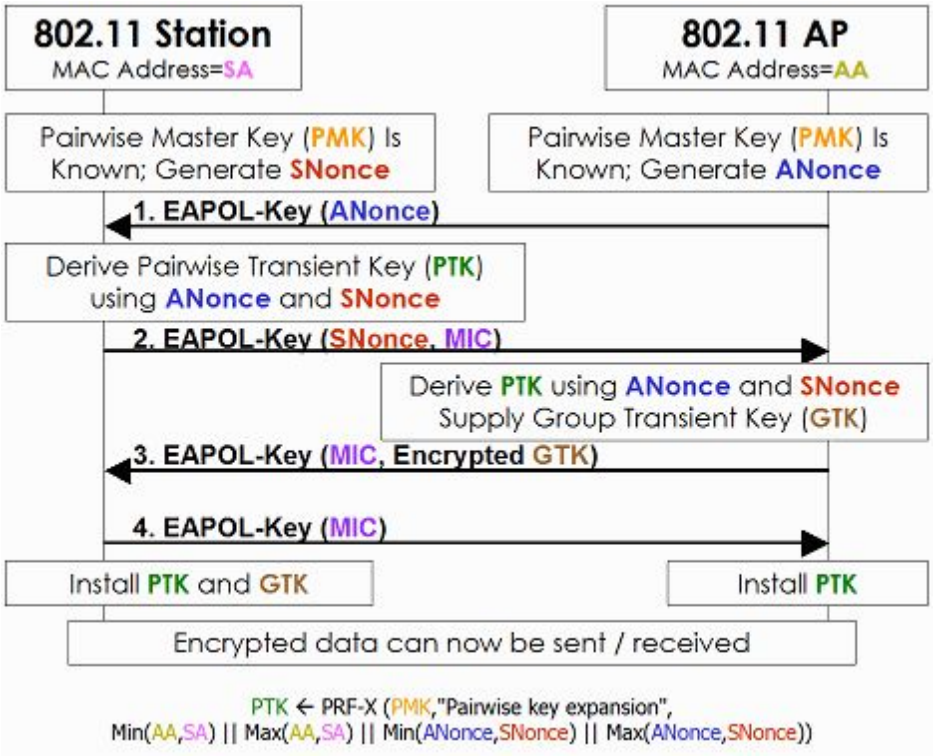
	EAP-MD5	LEAP	EAP-TLS	EAP-TTLS	PEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificates required	No	No	Client/Server	Server only	Server only
Dynamic Key Generation	No	Yes	Yes	Yes	Yes
Costs and Management overhead	Low	Low	High	Low/ Medium	Low/ Medium
Industry Support	Low	High	Medium	High	High

Die Methoden unterscheiden sich durch die Verbreitung, die Möglichkeit neben Client auch den AP zu authentifizieren, der dynamischen erzeugung von Schlüsseln und der mutual authentication.

25. Erläutern Sie das “pairwise” Schlüsselmanagement unter 802.11i unter Verwendung folgender Begriffe: “Master Session Key” (MSK), “Pairwise Master Key” (PMK), “Pairwise Transient Key” (PTK).

Ausgehend von einem PSK oder einem MSK (bei Enterprise) wird eine PMK abgeleitet. Wiederum vom PMK wird der PTK abgeleitet, welcher für die Verschlüsselung der Kommunikation genutzt wird.

26. WPA/WPA2-Personal: Betrachten Sie die untenstehende Abbildung (802.11i 4-way Handshake) und erläutern Sie, aus welchem Grund die Entropie der Passphrase zur Bildung des PSK (=PMK !) eine entscheidende Bedeutung hat:



PSK wird in Kombination mit der SSID als PMK verwendet und PTK wird vom PMK abgeleitet.
Weiters ist der PSK für alle Teilnehmer gleich und wird somit der PSK gecrackt ist die Kommunikation aller Teilnehmer kompromittiert.

27. TKIP (Temporal Key Integrity Protocol): Was sind die Ziele dieses Protokolls und wie werden sie umgesetzt?

Vertraulichkeit und Integrität
Vertraulichkeit wird durch die Verschlüsselung mittels RC4 sichergestellt und die Integrität durch einen MIC (Message Integrity Code) welche mittels dem Michael Algorithmus erstellt wird.

28. Was versteht man unter AES-CCMP? Betrachten Sie die Grafik in der Slideshow im Lektionsblock (Semesterplan) sowie die Beschreibung unter [BSI-09], A2.4.2 und erläutern Sie die Funktionsweise.

Counter-Mode/CBC-MAC Protocol
Verschlüsselung erfolgt durch den AES Counter Mode (Counter wird verschlüsselt und XOR mit Datenblock verknüpft, dadurch kann direkt auf einen einzelnen Block zugegriffen werden)
Integrität durch CBC-MAC gesichert.

29. **CCM (Counter with CBC-MAC) im Vergleich zur Betriebsart GCM (Galois Counter Mode). Nennen Sie Gemeinsamkeit sowie Unterschied.**

Beide verwenden den Counter Mode.

CCM: MAC then encrypt
GCM: encrypt then MAC

-> GCM state of the art

Buch [Sta14] 24.2 (Mobile Device Security)

30. **Erläutern Sie Bedrohungen, die sich im Zusammenhang mit mobilen Endgeräten (Mobile Devices) besonders ergeben.**

- fehlen physischer Sicherheitskontrollen (Gerät wird vom User mitgenommen)
- Benutzung nicht vertrauenswürdiger Geräte (User nimmt eigenes Gerät mit)
- Benutzung nicht vertrauenswürdiger Netze (MitM wenn in fremden Netz)
- Benutzung nicht vertrauenswürdiger Applikationen (User darf selbst Apps installieren)
- Interaktion mit anderen Systemen (Synchronisierung von Daten)
- Benutzung der Ortungsfunktion (Angreifer kann User/Gerät orten)

31. **Was versteht man unter "BYOD"? Welche Probleme ergeben sich für ein Unternehmen dadurch?**

Benutzer bringt sein eigenes Gerät (Handy, Notebook) und verwendet dies für Arbeitszwecke. Da der Benutzer verantwortlich ist für die Sicherheit und Wartung des Geräts, hat die IT des Unternehmens wenig Einfluss und es kann leicht zur Kompromittierung des Firmennetzes durch das Gerät des Benutzers kommen.

ITS Lektion 9

17.4 Kontrollfragen

1. **Listen Sie die Schichten des ISO/OSI Schichtenmodells auf und beschreiben Sie deren Funktionen.**

- **Physical Layer**: Bitübertragungsschicht (Übertragung der Bitströme)
- **Data Link Layer**: Sicherungsschicht, Übertragung im Subnetz (auf Basis der MAC Adresse, switching), Prüfsumme
- **Network Layer:** Übertragung über Subnetzgrenzen hinweg (IP basierend, routing)
- **Transport Layer:** TCP, UDP, End-to-End Verbindung, kümmert sich um Paketreihenfolge
- **Session Layer:** logische Verbindung zwischen Endpunkten
- **Präsentation Layer:** Verschlüsselung, Kompression,....
- **Application Layer:** eigentliche Applikation

2. **Welche Klassen an Sicherheitsdiensten nach der ISO/OSI Sicherheitsarchitektur kennen Sie?**

   1. Authentifikation
   2. Zugriffskontrolle
   3. Vertraulichkeit
   4. Integrität
   5. Verbindlichkeit

3. **Wie werden Authentikationsdienste nach der OSI Sicherheitsarchitektur unterschieden?**

- einseitige und die wechselseitige Authentifikation von Kommunikationsendpunkten
- Authentifikation des Datenursprungs

4. **Wie werden Vertraulichkeitsdienste nach der OSI Sicherheitsarchitektur unterschieden?**

Vertraulichkeit:
- verbindungsorientierter/verbindungsloser Kommunikation,
- ausgewählter Datenfelder und
- der Verkehrsdaten

5. **Wie werden Integritätsdienste nach der OSI Sicherheitsarchitektur unterschieden?**

Integrität:
- verbindungsorientierter Kommunikation mit/ohne Recovery,
- verbindungsloser Kommunikation und
- ausgewählter Datenfelder

6. **Wie werden Verbindlichkeitsdienste nach der OSI Sicherheitsarchitektur unterschieden?**

Nachweisbarkeit:
- des Ursprungs
- der Zustellung

7. **Welche spezifischen Sicherheitsmechanismen nach der ISO/OSI Sicherheitsarchitektur kennen Sie?**

    1. Verschlüsselungsverfahren
    2. Digitale Signaturen
    3. Zugriffskontrollmechanismen
    4. Datenintegritätsmechanismen
    5. Austausch von Authentizitätsinformationen
    6. Anonymisierung, Verschleierung von Verkehrsdaten
    7. Mechanismen zur Kontrolle der Wegewahl
    8. Notariatsmechanismen

8. **Welche durchgängigen Sicherheitsmechanismen nach der ISO/OSI Sicherheitsarchitektur kennen Sie?**

    1. Vertrauenswürdige Funktionalität
    2. Zuordnung von Klassifikationen
    3. Ereignisverwaltung
    4. Auditing
    5. Recovery

9. **Auf welcher Schicht gem ISO/OSI Modell sollten Authentifikationsdienste angesiedelt sein?**

Anwendungsschicht (Transportschicht wenn anwendungsspezifische Informationen dort vorhanden)

10. **Auf welcher Schicht gem ISO/OSI Modell sollten Dienste der Zugriffskontrolle angesiedelt sein?**

Ab Layer 2 (z.B.: Firewalls)

11. Auf welcher Schicht gem ISO/OSI Modell sollten Vertraulichkeits- und Integritätsdienste angesiedelt sein?

Ab Layer 4 (da aber hier End-to-End Verbindung)

12. Auf welcher Schicht gem ISO/OSI Modell sollten Verbindlichkeitsdienste angesiedelt sein?

Layer 7 (stark Anwendungsabhängig)

13. Was ist der Unterschied zwischen Verbindungsverschlüsselung und Ende-zu-Ende- Verschlüsselung?

<u>Verbindungsverschlüsselung:</u>
- alles oder nichts Verschlüsselung
- uneingeschränkt Filtern möglich
- Verkehrsdaten verschlüsselt
- nur Authentifikation von Systemen
- PPTP (Point-to-Point-Tunneling Protocol, L2TP (Layer 2 Tunneling Protocol)

<u>End-zu-End Verschlüsselung:</u>
- Selektives Verschlüsseln möglich
- Filterung eingeschränkt
- Verkehrsdaten liegen offen
- System-, Prozess-, Benutzerauthentifikation
- IPSec, SSL/TLS

14. Sicherheitsprotokolle auf der Netzwerk- und/oder Transportschicht: Finden und erläutern Sie charakteristische Unterschiede.

Erst ab Transportschicht Ende-zu-Ende Kommunikation.
- Netzwirkschicht: Verschlüsselung immer nur zwischen Netzwerkknoten
- Transportschicht: Verschlüsselung durchgehend zwischen den Endpunkten

15. Was versteht man unter Tunneling?

Protokoll B verbindet zwei Netzwerkknoten (datalink) und darin wird Protokoll A gekapselt transportiert. Protokoll B muss Protokoll A nicht unterstützen.

16. Was versteht man unter einem VPN?

Logischer Tunnel um über ein öffentliches Netz zwei Netze zu verbinden.

17. **Was versteht man unter One-Pass-Processing?**

Alle Verschlüsselungsinformationen (Verfahren, Schlüssel, Zertifikat, ...) wird in die Nachricht gepackt, sodass das Gegenüber zu einem späteren Zeitpunkt die komplette Nachricht auf einmal verarbeiten kann.

18. **Was ist der Unterschied zwischen einem sicheren Kommunikationsprotokoll und Sicherheitsmechanismen, die in die Anwendung integriert sind? Nennen Sie Vor- und Nachteile und zählen Sie Beispiele auf!**

- Kommunikationsprotokoll: aufbau eines sicheren Kanals zwischen den Hosts, wobei zuerst der Kanal aufgebaut wird (Authentifzierung, Vereinbarung Kryptoverfahren und Parameter) und dann über diesen Kanal die Daten übertragen werden
- Sicherheitsmechanismus: Daten werden direkt von der Anwendung verschlüsselt und zusammen mit den Sicherheitsparametern übertragen. Authentifizierung und Ver-/Entschlüsselung erfolgen in einem Schritt durch die Anwendung (One-Pass).

Buch [Sta14] 22.5 (IPsec):

1. **Welche Sicherheitsdienste bietet IPsec?**

Authentizität und Vertraulichkeit
Schlüsselverwaltung durch IKE (erst IKEv2 teil von IPsec)

2. **Zählen Sie Anwendungsgebiete für den Einsatz von IPsec auf.**

- Verbindung von Außenstellen über das Internet
- Remote Access über das Internet
- extranet und intranet Verbindungen mit Partnern
- Erhöhte Sicherheit für Anwendungen

3. **Nennen Sie Vorteile, die der Einsatz von IPsec bietet.**

- Sicherheit durch Verschlüsselung des gesamten Verkehrs außerhalb der Perimeters
- Kann nicht umgangen werden wenn über die Firewall eingerichtet (FW ist einziger Punkt über den der Traffic nach außen läuft)
- Kann unabhängig von der Software eingesetzt werden (da auf Transport Layer)
- Transparent für Enduser.
- Sicherheit für den einzelnen User (Remote Access)

4. **Was versteht man bei IPsec unter einer Security Association (SA)?**

Unidirektionale Beziehung zwischen Sender und Empfänger welche die Sicherheitsdienste anbietet für den übertragenen Traffic.

5. **Wodurch wird bei IPsec eine Security Association (SA) eindeutig identifiziert?**

- Security parameter index (SPI): wird im ESP Header übertragen um die anzuwendende SA zu identifizieren.
- IP destination address: IP des Zieles
- Protocol identifier: ob AH oder ESP

6. **Welche Informationen enthält bei IPsec eine Security Association (SA)?**

- Sequence number counter
- Sequence counter overflow
- Antireplay window
- AH information
- ESP information
- Lifetime of this SA
- IPsec protocol mode (tunnel, transport)
- Path MTU

7. **Was versteht man bei IPsec unter einem Security Parameter Index (SPI)?**

Ermöglicht dem Empfänger die richtige SA auszuwählen um das empfangene Paket zu verarbeiten.

8. **Im Bedarfsfall wird nach Maßgabe einer Security Policy bei beiden Teilnehmern die Security Association (SA) gebildet. Wie kann die hierfür notwendige Ausverhandlung/-Verteilung der benötigten Parameter (Geheimnisse) erfolgen?**

- manuell
- IKE (v1/v2) Protokoll

9. **Was versteht man bei IPsec unter einer Security Association Database (SAD)?**

- enthält alle aktuell aktiven SAs
- in den Paketen wird der Index (SPI) der SA mitgeschickt, welcher auf den Eintrag in der SAD verweist

10. Welche Sicherheitsdienste bietet das ESP-Protokoll?

- Authentizität
- Integrität
- Vertraulichkeit

11. Was versteht man bei IPsec unter "Transportmodus"?

Payload eines IP Paketes wird geschützt, somit Schutz für Protokolle höherer Schichten. Wird bei der Kommunikation zwischen Hosts eingesetzt.

12. Was versteht man bei IPsec unter "Tunnelmodus"?

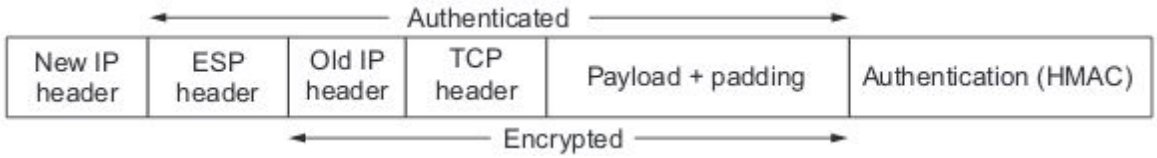
Das komplette IP Paket wird gekapselt und geschützt. Der Tunnelmodus wird verwendet um Netzwerke zu verbinden.

13. Beschreiben Sie die Unterschiede zwischen Transport- und Tunnelmodus bei IPSec.

Transport: Schutz der Payload
Tunnel: Kapseln des komplette IP Pakets und Schutz dessen

14. Skizzieren Sie die Struktur des ESP-Protokolls (Transportmodus) im Kontext eines IP-Datagramms.

15. Skizzieren Sie die Struktur des ESP-Protokolls (Tunnelmodus) im Kontext eines IP-Datagramms.



Buch [Sta14] 22.3,4 (TLS):

16. Beschreiben Sie die Funktionsweise von TLS, welche Sicherheitsdienste können mit TLS verwirklicht werden?

Basiert auf TCP und ist für die Ende-zu-Ende Verschlüsselung ausgelegt. Aufbau: Handshake Layer baut Verbindung auf und sichert die Authentizität. Record Layer ist für die Datenübertragung zuständig und sicher Vertraulichkeit und Integrität.
Sicherheitsdienste: Authentizität, Integrität, Vertraulichkeit

17. Ordnen Sie TLS in das ISO/OSI Schichtenmodell ein.

Sitzungs- u. Präsentationsschicht

18. Was ist der Unterschied zwischen IPsec und TLS? Zählen Sie jeweils Vor- und Nachteile auf.

IPsec: Arbeitet auf der Netzwerkschicht, Aushandlung der Sicherheitsparameter und Authentifizierung ausgelagert

- Vorteil: Transparent
- Nachteil: kann nicht für einzelne Anwendung eingerichtet werden

TLS: Arbeitet auf Sitzungs- u. Präsentationsschicht, Aushandlung der Sicherheitsparameter und Authentifizierung integriert

- Vorteil: Applikationsorientiert (Kommunikation von Applikation kann unabhängig gesichert werden)
- Nachteil: nicht transparent, Schützt nicht Traffic eines gesamten Systems

19. Was sind die Aufgaben/Designziele von TLS?

- kryptographische Sicherheit
- Interoperabilität
- Erweiterbarkeit
- Effizienz

20. Was ist bei TLS der Unterschied zwischen einer Verbindung und einer Sitzung?

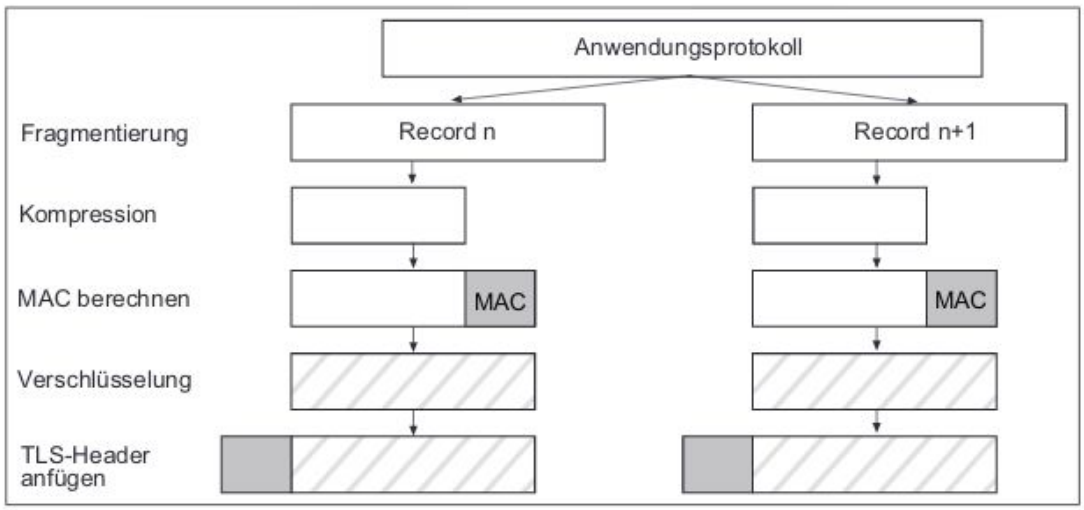
Eine Sitzung wird durch den Handshake Layer aufgebaut (aushandeln der Sicherheitsparameter) und über diese Sitzung können mehrere Verbindungen abgehandelt werden (damit nicht jedes mal die Sicherheitsparameter neu ausgehandelt werden müssen).

21. Nennen Sie die beiden Sicherheitsdienste des TLS Record Protokolls.

Vertraulichkeit, Integrität

22. Beschreiben Sie den Protokollablauf des TLS Record Protokolls.

Daten werden von Anwendung übernommen, in Records fragmentiert, komprimiert, der MAC (Integrität) berechnet und angefügt, verschlüsselt, der TLS Header vorne angefügt und versendet.



23. Welche Aufgabe hat das Change Cipher Spec Protokoll bei TLS?

Dient zum Auslösen einer Zustandsänderung. Besteht nur aus einer Message welche signalisiert dass die darauffolgende Kommunikation mit den vorhergehend vereinbarten Parametern erfolgt.

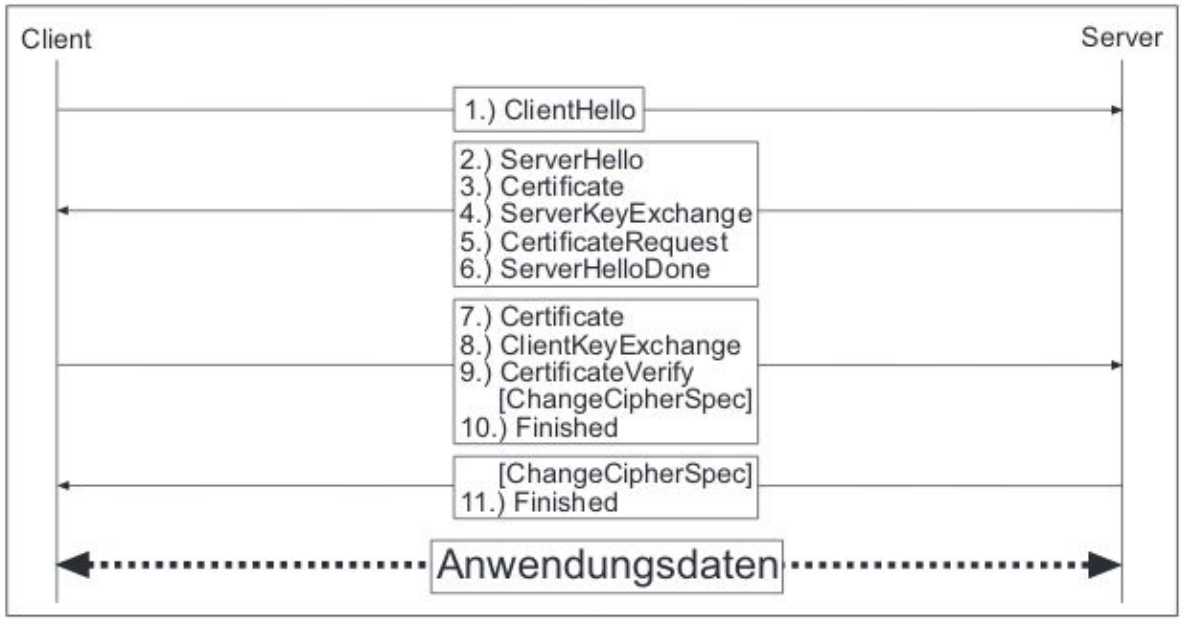
24. Welche Aufgabe hat das Alert Protokoll bei TLS?

Zum versenden von Alarmmeldungen. Enthält Schweregrad (warning bis fatal) und Beschreibung. Bei “fatal” wird die Verbindung abgebrochen und weiter Verbindungsversuche unterbunden.

25. Welche Aufgabe hat bei TLS der Handshake Layer?

Authentifikation und ausverhandeln der Sicherheitsparameter für den Aufbau einer Sitzung über welche die Verbindungen abgehandelt werden.

26. Erläutern Sie die vier Phasen des TLS Handshakes.



1. Aufbauen der Verbindung, übermitteln der unterstützten Algorithmen
2. Antwort mit gewählter Cipher Suite, Zertifikat oder temporärer RSA Schlüssel, falls erforderlich Anfrage wegen Client Zertifikat zur Authentifizierung
3. Client überprüft Server Zertifikat, sendet falls notwendig eigenes Zertifikat, übermitteln des ClientKeys für die Verschlüsselung des Pre-master Secrets. Aktivierung der neuen Parameter.
4. Server prüft gegebenenfalls Client Zertifikat, aktiviert neue Parameter.

27. Welche Eigenschaften/Inhalte des Serverzertifikats werden durch den Client im Zuge des TLS Handshakes überprüft?

- zeitlich gültig
- nicht gesperrt
- CA vertrauenswürdig
- öffentlicher Schlüssel der CA noch gültig
- stimmt FQDN des Servers mit Angaben im Zertifikat überein
- entspricht Signaturalgorithmus kryptographischen Anforderungen
- ist die Signatur gültig

28. Gruppieren Sie bekannte Angriffe gegen TLS.

- Angriffe auf das Handshake Protokoll
- Angriffe auf Record oder Application Data Protokoll
- Angriffe auf die PKI
- Andere Angriffe
-

ITS Lektion 10

22.5 Kontrollfragen

1. Handelt es sich bei SSH um eine Applikation oder um ein Netzwerkprotokoll? Begründen Sie Ihre Antwort.

Beides
Anwendung: Remote Shell auf entfernten Rechner
Protokoll: SCP, SFTP,...

2. Erläutern Sie die Funktionsweise von SSH.

Client-Server Protokoll auf Basis von TCP, stellt vertrauliche, authentifizierte und integere Verbindung zur Verfügung.

3. Zählen Sie Beispiele des Funktionsumfanges von SSH auf.

- Secure Shell auf einem entfernten Rechner.
- Tunneln bzw. Port Forwarding, als Alternative zum eigenständigen VPN.
- SCP, Files sicher kopieren von einem Rechner auf einen entfernten Rechner
- SFTP, als sichere Alternative zu FTP
- SSHFS (Secure SHell FileSystem), um entfernte Filesysteme in das lokale Filesystem einzuhängen.
- dynamisches Port Forwarding -> Proxy Server

4. Beschreiben Sie die Protokollarchitektur (drei Schichten) von SSH.

- Transport Layer (Parametervereinbarung und sichere Verbindung)
- Authentication Layer
- Connection Layer (vereint mehrere logische Kanäle zu einer SSH Verbindung)

5. Welche Aufgaben hat der SSH Transport Layer?

Kompression, Parametervereinbarung, sichere Verbindung, Serverauthentifizierung
- Vereinbarung der Algorithmen
- Serverauthentifizierung
- Vereinbarung der Sitzungsschlüssel
- Optionale Kompression des Klartextes
- Verschlüsselung des Klartextes
- Sicherstellen der Integrität über HMAC

6. Welche Aufgaben hat der SSH User Authentication Layer?

Benutzerauthentifizierung (password, public key, keyboar-interactive)

7. Welche Aufgaben hat der SSH Connection Layer?

Kommunikation der SSH Dienste (und auch zusammenfassen dieser)

8. Beschreiben Sie grob die vier Schritte des Authentifikationsvorganges bei SSH.

- Verbindungsaufbau
- Aushandeln der Algorithmen/Parameter
- Serverauthentifizierung
- Clientauthentifizierung

9. Welches Problem ergibt sich beim erstmaligen Verbinden mit einem SSH-Server (ohne Zertifikat)? Wie kann dies sicher gelöst werden?

leap of faith, Server kann nicht authentifiziert werden, muss manuell über Fingerabdruck des public keys erfolgen

10. Was ist bei SSH der Unterschied zwischen interaktivem und nicht-interaktivem Modus?

interaktiv: user hat shell auf remot rechner
nicht-interaktiv: User setzt Befehl über SSH ab und bekommt Ergebnis auf der lokalen Shell angezeigt

11. Welche Arten der Portweiterleitungen bei SSH kennen Sie?

- lokale
- entfernte
- dynamische
- umleiten von X11 (Desktop) des entfernten Rechners

Buch [Sta14] 22.1 (S/MIME):

1. **Was versteht man unter "MIME"?**

Multipurpose Internet Mail Extension

- MIME spezifiziert Message Header, den Inhaltstyp und Kodierung
- wurde spezifiziert um Binärdaten über Protokolle versenden zu können die nur 7-Bit ASCII unterstützen (SMTP)

2. **Was versteht man unter "S/MIME". Welchen Sinn & Zweck hat dieser Standard?**

Standard um kryptografische Nachrichtenelemente als spezifischen MIME-Typ in Nachrichten einzubetten. Erweitert herkömmliche MIME-Nachrichten um Sicherheitsdienste Vertraulichkeit, Integrität und Authentizität.

3. **Nennen und beschreiben Sie die vier relevanten Funktionalitäten, die über die S/MIME Content-Types gewährleistet werden.**

Enveloped data: verschlüsselter Content und Schlüssel für einen oder mehrere Empfänger
Signed data: Signatur über den Content (Hash und verschlüsseln dessen mit privaten Schlüssel)
Clear-signed data: Signatur über den Content, nur Signatur wird base64 kodiert -> Empfänger ohne S/MIME können Nachricht lesen
Signed and enveloped data: Enveloped data und Signed data nested -> verschlüsseln und signieren des Content

4. **Wie ist eine S/MIME Nachricht aufgebaut?**

- kombination aus MIME bodies und CMS content type (Cryptographic Message Syntax)
- MIME body enthält Content
- CMS -> Signatur, Zertifikate, Algorithmen, wrapped in MIME

5. **Was ist der Unterschied zwischen "Signed Data" und "Clear-signed Data"?**

Signed Data: Signatur und Content base64 kodiert
Clear-signed Data: nur Signatur base64 kodiert, somit kann Empfänger ohne S/MIME die Nachricht lesen

6. **Erläutern Sie den typischen Ablauf, wie über S/MIME aus einer Klartextnachricht eine verschlüsselte sowie signierte Nachricht erzeugt wird.**

Die abzusichernden Nachrichtenelemente werden durch den Absender signiert und/oder verschlüsselt und die Signatur resp. der verschlüsselte Block als CMS-Objekt angefügt.

7. **Was versteht man unter dem Radix-64 (Base-64) Format? Wozu dient diese Codierung?**

- Binärdaten in ASCII darstellen
- abbilden von 3x8-Bit auf 4x6-Bit Blöcke
- Zeichen: {A-Z,a-z.0-9,+,/}

24.4 Kontrollfragen

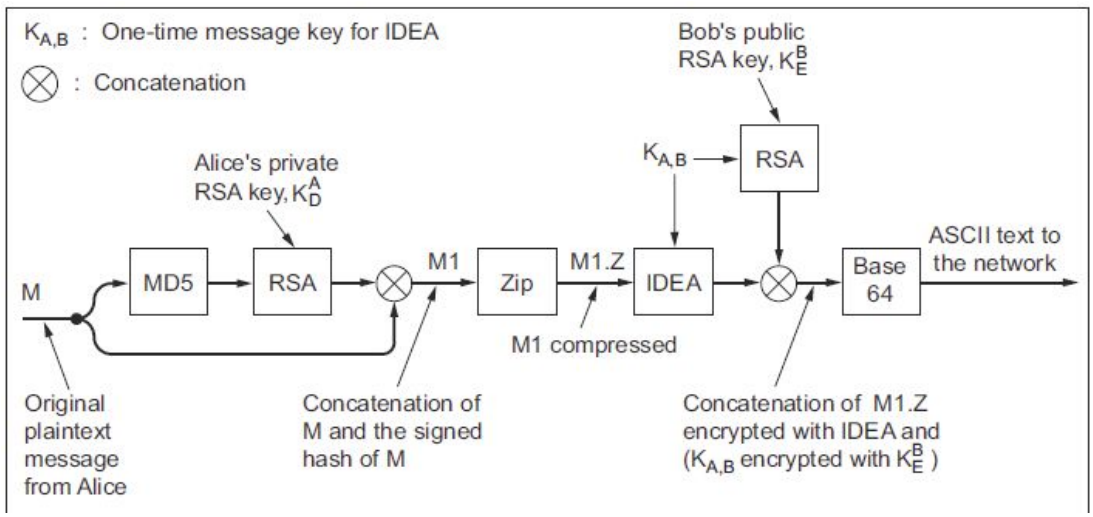
1. Was ist PGP?

Pretty Good Privacy
Stellt Authentizität, Vertraulichkeit und Integrität für Texte und Dateien zur Verfügung auf Basis von symmetrischer und asymmetrischer Verschlüsselungsverfahren

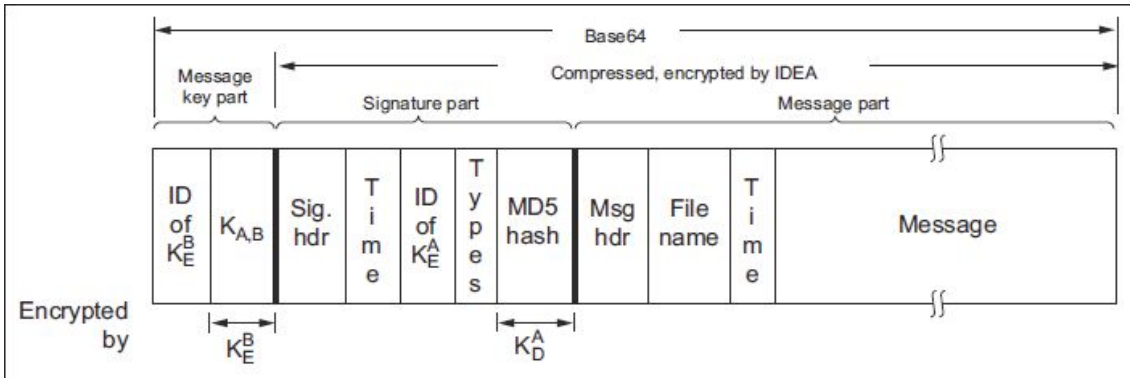
2. Welche Sicherheitsdienste werden durch PGP gewährleistet?

- RSA/Diffie-Hellman
- symmetrische Verfahren (IDEA, 3DES,...)
- Integrität, Authentizität (MD5, SHA1)
- Signatur (RSA, DSS)

3. Beschreiben Sie den genauen Ablauf, wie PGP aus einer Klartextnachricht eine signierte und verschlüsselte Nachricht erzeugt.



4. Beschreiben Sie das Nachrichtenformat einer PGP-Nachricht.



5. Aus welchen drei Komponenten besteht eine PGP-Nachricht? Erläutern Sie diese.

- Verschlüsselungskomponente
  - ID des öffentlichen Schlüssel des Empfängers
  - verschlüsselter Verbindungsschlüssel
- Signaturkomponente
  - Zeitstempel
  - ID des öffentlichen Schlüssels des Absenders
  - signierter Hashwert
- Nachrichtenkomponente
  - Dateiname
  - Zeitstempel
  - Nachricht

6. Welche drei Schlüsselklassen finden bei PGP Anwendung? Erläutern Sie diese.

symmetrischer Nachrichtenschlüssel, asymmetrisches Schlüsselpaar, symmetrischer Schlüssel zum speichern des private keys

7. Was wird im Private-Key-Ring abgespeichert?

privater Schlüssel

8. Was wird im Public-Key-Ring abgespeichert?

öffentliche Schlüssel der Kommunikationspartner

9. Beschreiben Sie die Funktionsweise des Web of Trust. Gehen Sie dabei auf die Begriffe Owner Trust, Signatory Trust und Direct Trust ein.

Durch von anderen Teilnehmern stammende Beglaubigungen (Signaturen) entstehen Vertrauenspfade, öffentliche Schlüssel akkumulieren Vertrauensgrade.
Owner Trust: Benutzer ordnet öffentlichen Schlüssel im Public-Key-Ring Vertrauensgrade zu
Signatory Trust: Signatur des öffentlichen Schlüssel durch andere
Direct Trust: persönliche Prüfung der Authentizität

10. Was versteht man beim Web of Trust unter Owner Trust?

Benutzer ordnet öffentlichen Schlüssel im Public-Key-Ring Vertrauensgrade zu

11. Was versteht man beim Web of Trust unter Signatory Trust?

Signatur des öffentlichen Schlüssel durch andere

12. Was versteht man beim Web of Trust unter Direct Trust?

persönliche Prüfung der Authentizität

13. Was ist der Unterschied zwischen Owner Trust und Signatory Trust?

Owner Trust: Vertrauensgrad wird durch Benutzer zugewiesen
Signatory Trust: Vertrauen wird durch signieren des öffentlichen Schlüssels durch andere akkumuliert

14. Wie werden öffentliche Schlüssel und deren Signaturen global zugänglich gemacht?

Schlüsselserver

15. GnuPG: Welche Vertrauensgrade in öffentliche Schlüssel kennen Sie? Was bedeuten sie jeweils?

- unknown: Besitzer hat keine weiteren Informationen
- untrusted: wird nicht vertraut, Signaturen von diesem Schlüssel werden ignoriert
- marginal: teilweises Vertrauen
- complete: volles Vertrauen
- ultimate: zu diesem Schlüssel besitzt man selbst den geheimen Schlüssel

16. Wie kann ein Benutzer seinen Schlüssel für ungültig erklären - daher zurückrufen?

Generieren eines Key Revocation Zertifikates mit dem privaten Schlüssel und upload des Zertifikats auf den Schlüsselserver.

17. Wann ist - nach den Regeln von GnuPG - ein öffentlicher Schlüssel einer dritten Person gültig bzw. vertrauenswürdig?

Wenn eine transiente Beziehung besteht (jemand dem man vertraut spricht dem dritten gegenüber sein vertrauen aus und dadurch entsteht transientes Vertrauen)

ITS Lektion 12

Domain Name Security (DNSsec); [ARIMIT07], [WIS10]:

1. **Wie funktioniert das Domain Name System (DNS)? Gehen Sie dabei auf folgende Begriffe ein:**
    a. **Reverse-Zone**
    b. **Forward-Zone**
    c. **Zonentransfer**
    d. **Iterative vs. rekursive Auflösung**
    e. **Root Server**

DNS ist ein Protokoll welches über UDP arbeitet und bietet den Service DNS-Namen auf IP-Adressen aufzulösen (Forward-Zone) und IP-Adressen auf DNS-Namen aufzulösen (Reverse-Zone).
Ein Zonentransfer dient der Synchronisierung mehrer DNS-Server, in dem die komplette Datenbank mit DNS-Einträgen von einem Server mittels Zonentransfer auf einen anderen übertragen wird.
Iterative Auflösung: kann der Server die Auflösung nicht durchführen verweist er auf den zuständigen DNS-Server
Rekursive Auflösung: kann der Server die Auflösung nicht durchführen, fragt dieser bei anderen, zuständigen, DNS-Server nach und holt sich von diesen die notwendige Information.
Root Server: Wurzel des DNS-Systems, speichern die IPs aller DNS-Server welche für Top Level Domains zuständig sind.

2. **Erläutern Sie Sicherheitsprobleme des DNS hinsichtlich der Schutzziele Integrität, Authentizität und Verfügbarkeit.**

DNS basiert auf UDP und sieht keine Verschlüsselung bzw. Authentifizierung da. Dadurch ist es einem Angreifer möglich durch eine MitM-Attacke DNS-Packete zu verändert (Integrität) oder einfach anstatt der eigentlichen Antwort eine komplett gefälschte zu senden (Authentizität). Durch eine DDoS-Attacke ist es möglich die Auflösung von TLDs (Top Level Domains) zu verhindern und somit die komplette Namensauflösung zu stören (Verfügbarkeit)

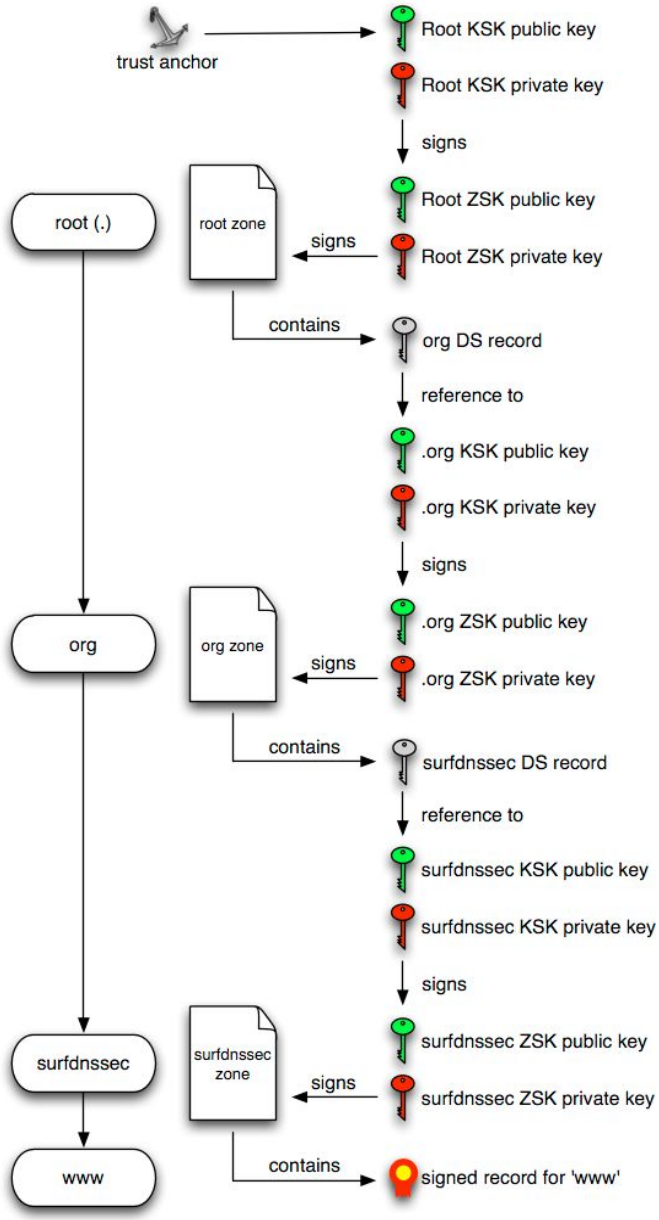
3. **Was ist der Unterschied zwischen DNS-Spoofing und DNS-Cache-Poisoning?**

Fälschen der Antwort eines DNS-Servers um den Datenverkehr eines Hosts umzuleiten.
Bei DNS-Spoofing geht es um die Abänderung von DNS-Records im DNS-Packet.
DNS-Cache-Poisoning versucht DNS-Records im DNS-Cache des Ziels zu manipulieren.

4. **Erläutern Sie die Funktionsweise von DNSsec.**

Die Resource Records (RR) werden signiert, wodurch die Authentizität sichergestellt wird. Hierfür wird eine Chain of Trust verwendet, bei welcher die Schlüssel mit welchem eine Domain signiert wird mit dem Schlüssel der übergeordneten DNS-Zone signiert wird.

5. **Skizzieren/Beschreiben Sie die DNSsec-Vertrauenskette (Chain of Trust) bei DNSsec anhand der Grafik in der Slideshow im Lektionsblock (Semesterplan).**



- KSK signiert ZSK.
- ZSK signiert Einträge der Zone
  -> dadurch Chain of Trust, Einträge enthalten auch Keys der darunter liegenden Zonen und Domains

6. **Welche beiden Schlüsselpaare verwendet DNSsec pro Domäne? Wozu dienen diese?**

KSK (Key Signing Key): wird verwendet um den ZSK (Zone Signing Key) zu signieren und ist meist mindestens 2048 Bit lang
ZSK (Zone Signing Key): wird benutzt um die DNS-Records zu signieren. Aus Performancegründen ist der ZSK kleiner (z.B.: 512 Bit), wird aber auch öfters gewechselt. Damit dies leichter möglich ist, wird der ZSK mit dem KSK signiert.

7. **Mit welchem Schlüssel wird bei DNSsec die Echtheit der Zoneneinträge geprüft? Wie kommt der lokale DNS-Resolver zu diesem Schlüssel?**

Mit dem öffentlichen Schlüssel des ZSK. Der Schlüssel wird über den DNSKEY Record via DNS verfügbar gemacht.

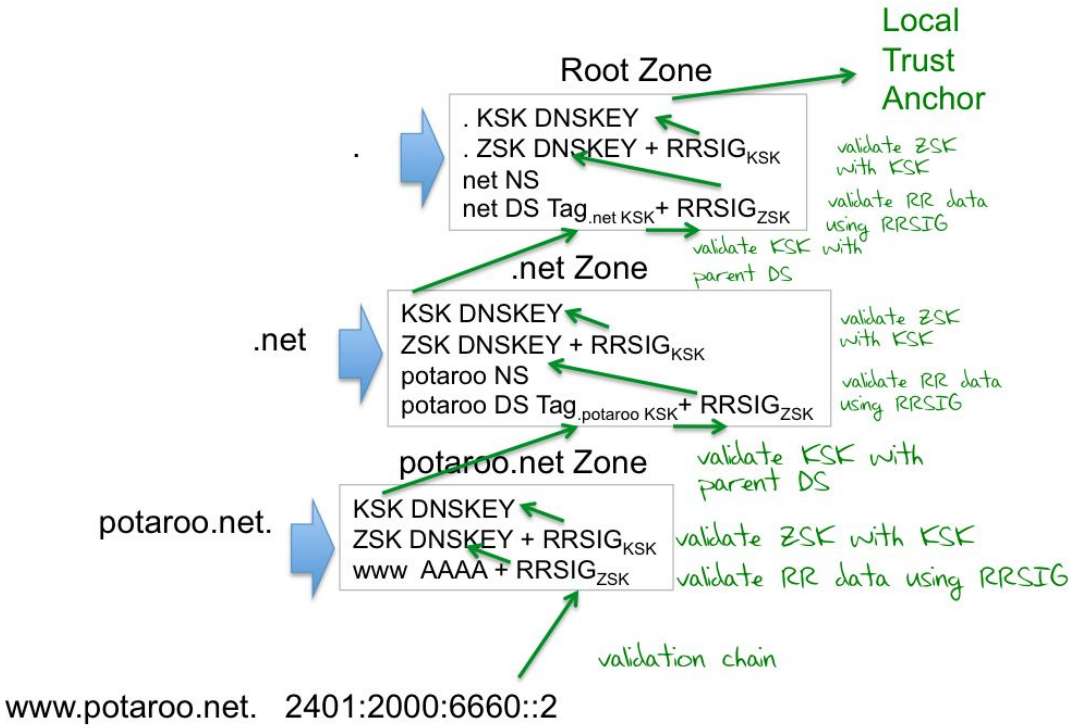
8. **DNS-Datentypen: Erläutern sie die Inhalte von**
    a. **RRSIG**
    b. **DNSKEY**
    c. **DS**

a. enthält Signatur eines anderen Resource Record
b. enthält öffentlichen Schlüssel des ZSK oder KSK
c. dient zur Verkettung von DNSSEC Zonen zu einer Chain of Trust

9. **Zeichnen Sie die Hierarchie der Schlüsselinfrastruktur bei DNSsec anhand der Domänen .at sowie .tw.at.**

root KSK - sign -> root ZSK
root ZSK - sign -> .at KSK
.at KSK - sign -> .at ZSK
.at ZSK - sign -> .tw.at KSK
.tw.at - sign -> .tw.at ZSK

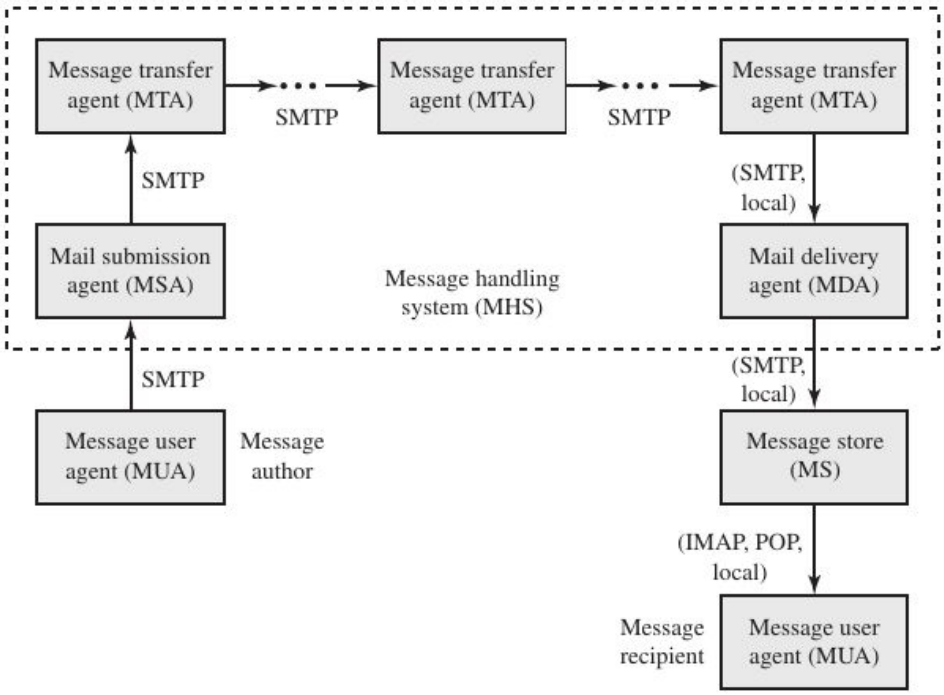
10. Erläutern Sie die Schritte der Authentizitätsprüfung von DNS-Antwortdaten entlang der DNSsec-Vertrauenskette anhand der Grafik in der Slideshow im Lektionsblock (Semesterplan).



Bei Namensauflösung wird RRSIG des ZSK und KSK der Domain geladen und mit dem öffentlichen Schlüssel der darüber liegenden Zone validiert. Dies wird fortgeführt bis zu der Root Zone.

Domainkeys Identified Mail (DKIM); Buch [Sta14] 22.2:

11. **Schlüsselkomponenten der E-Mail Architektur: Skizzieren Sie die Zusammenhänge zwischen Message User Agent (MUA), Mail Submission Agent (MSA), Mail Transfer Agent (MTA), Mail Delivery Agent (MDA) sowie Mail Store.**



MUA: Mailclient des Users
MSA: Nimmt Nachrichten entgegen welche vom MUA submitted werden (via SMTP), kann Teil des MUA sein
MTA: zuständig für den Transport der Nachrichten zwischen MSA und MDA, kann über mehrere MTA verlaufen
MDA: Nimmt Nachrichten entgegen und speichert diese im MS
MS: MUA holt sich von hier via IMAP, POP die Nachrichten

12. **Was regelt die DKIM-Spezifikation bzw. wofür dient diese? Nennen Sie weiters Besonderheiten.**

Stellt die Authentizität von Nachrichten sicher, dass diese von einer bestimmten Domain versandt wurde, transparent für den Benutzer. Public Key wird im DNS abgelegt.

13. **Nennen Sie Gemeinsamkeiten sowie Unterschiede zwischen DKIM und S/MIME hinsichtlich**
    a. **gewährleistete Schutzziele,**
    b. **Authentizität des Absenders/der Inhalte,**
    c. **Integration resp. Interaktion durch Endanwender.**

a. DKIM: stellt nur die Authentizität und Integrität sicher -> Signatur
   S-MIME: stellt Authentizität, Integrität und Vertraulichkeit sicher -> Verschlüsselung und Signatur
b. DKIM: Signatur der gesamten Nachricht durch privaten Schlüssel der administrativen Domain -> Authentizität der Domain sichergestellt
   S-MIME: Signatur über Teile der Nachricht mittels Zertifikat welches von einer vertrauenswürdigen Stelle ausgestellt wurde -> Authentizität des Benutzers sichergestellt
c. DKIM: wird am Server implementiert -> transparent für den Benutzer
   S-MIME: wird im Mailclient implementiert -> Benutzer kümmert sich um Verschlüsselung & Signatur, Schlüsselmanagement durch den User

14. **Beschreiben Sie anhand der Skizze aus Frage 11 den typischen Ablauf, wie der über DKIM spezifizierte Sicherheitsmechanismus auf E-Mails angewandt wird.**

Der MSA signiert die Nachricht und stellt somit die Authentizität dieser sicher. Will nun der Empfänger (MDA) die Signatur prüfen, fragte dieser via DNS den public key dieser Domain an und überprüft mit diesem die Signatur.

Webapplication Security; [OWASP] sowie Buch [Sta14], S404-408:

15. **Was bedeutet es, dass HTTP zustandslos ist. Wie kann dennoch zwischen einzelnen Transaktionen ein Kontext hergestellt werden?**

Jede HTTP Anfrage erfolgt unabhängig von den vorhergehenden. Ist eine Authentizierung notwendig muss dies für jede Anfrage erfolgen -> Basic Authentizierung
Durch Sessions (Session-IDs) ist es möglich einen Kontext herzustellen.

16. **Was versteht man unter der „Same Origin Policy“ (vgl. Grafik in der Slideshow im Lektionsblock)? Was soll dadurch verhindert werden?**

Verhindert den Zugriff (durch JavaScript, ActionScript, CSS) auf Objekte die von einer anderen Website stammen. Verhindert den Zugriff auf den Kontext einer anderen geladenen Website im Browser (auslesen, manipulation.

17. **Was versteht man unter einem Drive-by-Download Angriff?**

Das unbewusste, unbeabsichtigte herunterladen von Software ohne zutun des Users.
Z.B.: Zugriff auf eine präparierte Website welche eine Schwachstelle im Browser ausnutzt um Software auf den Client herunter zu laden.

18. OWASP Top-Ten: Injection:

- **a. Command-Injection: Was versteht man unter dieser Schwachstelle? Wie/Wo wird sie ausgenützt?**
- **b. SQL-Injection: Was versteht man unter dieser Schwachstelle? Wie/Wo wird sie ausgenützt?**
- **c. Code-Injection: Was versteht man unter dieser Schwachstelle? Wie/Wo wird sie ausgenützt?**
- **d. Unterscheiden Sie Local File Inclusion (LFI) und Remote File Inclusion (RFI).**
- **e. Injection allgemein: Welche Gegenmaßnahmen empfehlen Sie einem Webentwickler?**

a. Ausführen von beliebigen Befehlen auf dem Betriebssystem des Hosts durch eine fehlerhafte Applikation.
Wird eine Benutzereingabe für die konstruktion eines Befehls genutzt.

b. Usereingaben werden nicht ausreichend überprüft wodurch sich SQL-Befehle einschleusen lassen, welche von der Datenbank ausgeführt werden. Diese Schwachstelle ist oft bei Websites zu finden.

c. Injizieren von ausführbarem Code über eine Schwachstelle in einer Applikation.
Z.B.: Pfad für die include()-Funktion wird über Variable eines GET-Request manipuliert.
Meist bei Skriptsprachen (z.B.: PHP)

d. LFI: einbinden einer Datei welche Code enthält vom lokalen Dateisystem
RFI: einbinden einer Datei welche Code enthält von einem entfernten System (PHP-Code wird auf Webserver gehostet und eingebunden)

e. Keinen Userinput unüberprüft übernehmen.

19. OWASP Top-Ten: Broken Authentication and Session Management:

- **a. Was versteht man darunter?**
- **b. Nennen Sie client- und serverseitige Verwundbarkeiten.**
- **c. Nennen Sie beispielhaft Angriffsszenarien.**

a. Broken Authentication: Fehler bei den Passwortverwaltungsfunktionen einer Webapplikation
Session Management: Fehler bei der Implementierung welche es einem Angreifer ermöglichen eine Session zu hijacken.
b. Broken Authentication: Ausnutzen der Passwort zurücksetzen-Funktion
Session Management: Vorhersagbare Session-ID
c. Broken Authentication: Sicherheitsfragen welche durch Soziale Netzwerke leicht zu ermitteln sind
Session Management: Auslesen der Session-ID über eine manipulierte Website

20. OWASP Top-Ten: Cross Site Scripting (XSS):

- **a. Was versteht man unter dieser Schwachstelle?**
- **b. Unterscheiden Sie reflektiertes, persistentes und DOM-basiertes XSS.**
- **c. Wie/Wo wird XSS ausgenützt?**
- **d. Welche Gegenmaßnahmen empfehlen Sie einem Webentwickler sowie einem User?**

a. Injizieren von Skriptcode in vertrauenswürdige Websites. Der Skriptcode wird durch den Browser des Clients ausgeführt.
b. reflektiert: Skriptcode wird in einen Link eingebettet welcher vom Opfer angeklickt wird und wird in der Ausgabe der Website reflektiert
persistent: Skriptcode wird in die betroffene Website eingebettet, z.B.: über Kommentarfunktion
DOM-basiert: manipulieren der DOM Umgebung im Browser des Opfers, sodass das Client Side Script auf eine schadhafte Weise arbeitet
c. Bei Websites um Clients zu attackieren
d. Überprüfen von Benutzereingaben um Client Side Scripts heraus zu filtern, bzw. unschädlich zu machen

21. OWASP Top-Ten: Was versteht man unter „Insecure Direct Object Reference“?

Direkter Zugriff auf ein Objekt durch manipulation eines Parameters, wobei Zugriffsrechte nicht überprüft werden. z.B.: Zugriff auf User-Profil über ID, Zugriffsrecht wird nicht überprüft.

22. OWASP Top-Ten: Cross Site Request Forgery (CSRF):

- **a. Was versteht man unter dieser Schwachstelle?**
- **b. Wie/Wo wird diese Schwachstelle ausgenützt?**
- **c. Welche Gegenmaßnahmen empfehlen Sie einem Webentwickler?**

a. Über ein Client Side Script wird auf einer Website wo der User angemeldet ist eine Aktion ausgeführt, welche dieser nicht möchte
b. Im Browser des Opfers welcher das Script ausführt
c. Durch CSRF-Token kann das Ausführen solcher Aktionen verhindert werden

Cloud Security; Buch [Sta14] 5.8-11:

23. **Cloud Computing, Definition gem. NIST: Nennen und erläutern Sie die fünf essentiellen, charakteristischen Eigenschaften.**

Pool an Ressourcen welche von mehreren genutzt werden, können schnell und einfach konfiguriert und verfügbar gemacht werden. Verfügbarkeit steht im Vordergrund.
Broad network access: über Netzwerk und über standard Mechanismen erreichbar
Rapid elasticity: schnelles expandieren und reduzieren
Measured service: Überwachung um automatisch zu optimieren
On-demand self-service: Kunde kann ohne zutun des Providers Ressourcen hinzufügen
Resource pooling: Pool an Ressourcen welcher unter den Kunden geteilt wird und dynamisch zugewiesen werden kann

24. **Cloud Computing, Definition gem. NIST: Nennen und erläutern Sie die drei (Service)-Modelle.**

Software as a service (SaaS): Software wird Kunden zur Verfügung gestellt, wird alles vom Provider verwaltet (z.B.: Gmail)
Platform as a service (PaaS): Platform wird Kunden zur Verfügung gestellt, Software muss vom Kunden selbst gestellt werden. (z.B.: Website Hosting)
Infrastructure as a service (SaaS): Stellt Kunden Infrastruktur zur Verfügung aus welcher eigene Betriebssysteme und Software betrieben werden kann. Kann über Interface gesteuert werden. (z.B.: Amazon AWS, Windows Azure)

25. **Cloud Computing, Definition gem. NIST: Nennen und erläutern Sie die vier vorgestellten Einsatzszenarien/Betriebsmodelle.**

Public Cloud: Öffentlich verfügbar, wird als Cloud Service in der Öffentlichkeit verkauft
Private Cloud: Cloud Infrastruktur wird von Firma betrieben (kann auch durch dritten zur Verfügung gestellt werden) und ist nur für diese zugänglich
Cummunity Cloud: Wird von mehreren Organisationen geteilt, welche ähnliche Bedürfnisse hat (z.B.: Security). Wird durch die Organisationen oder einen dritten gemanaged
Hybrid Cloud: Setzt sich aus zwei oder mehr der anderen Formen zusammen.

26. **Nennen Sie Beispielanwendungen für das SaaS-Modell.**

Webmail-Provider wie z.B.: gmail

27. **Was versteht man unter dem PaaS-Modell? Wann ist dieses Modell vorteilhaft?**

Plattform wird durch Cloud Provider zur Verfügung gestellt, wie z.B.: ein Webserver und der Kunde kann die Software selbst stellen, z.B.: Website
Dann Sinnvoll wenn man sich um die Infrastruktur nicht kümmern will und nur die Software unter eigenen Kontrolle haben will

28. Beschreiben Sie das IaaS-Modell und nennen Sie Beispielanwendungen.

Infrastruktur wird durch Cloud Provider gestellt. Hat den Vorteil dass schnell skaliert werden kann und der Kunde sich nicht um die Hardware kümmern muss

29. Was ist das prinzipielle Dilemma (Buch: "essential concept"), dem Unternehmen ausgesetzt sind, die Cloud-Dienste verwenden?

Verlust der Kontrolle über Ressourcen und Services, hat aber Verantwortung über Sicherheit und die Privatsphäre -> kann diese nicht mehr vollständig garantieren.

30. Nennen und erläutern Sie fünf Sicherheitsbedrohungen, wie sie gerade für das Cloud-Computing spezifisch sind.

Ausnutzen von Cloud Services: für z.B.: Spamming, DDoS
Unsichere Interfaces und APIs: durch welche die Sicherheit des Cloud Services nicht sichergestellt werden kann.
Bösartiger Insider: beim Cloud Provider, welcher Zugriff auf die Infrastruktur des Kunden hat
Geteile Infrastruktur: Cloud Service für mehrere Kunden wird auf einer Infrastruktur betrieben -> kann nicht 100% voneinander isoliert werden
Verlust von Daten oder leakage: da Daten beim Cloud Provider liegen und der Kunde nicht die volle Kontrolle darüber hat
Account/Service hijacking: Angreifer erlangt dadurch Zugriff auf die Cloud Infrastruktur des Kunden

31. Erläutern Sie jene spezifischen Eigenschaften von Cloud-Computing, die hinsichtlich der Datensicherheit von Relevanz sind.

Infrastruktur wird zwischen Kunden geteilt.
Daher ist bei Datenbanken ein multi-instance oder ein multi-tenant model (Daten werden mit einer Kunden-ID getagged) notwendig. Im Idealfall werden alle Daten verschlüsselt gespeichert und sollten erst auf den Rechnern des Kunden entschlüsselt werden.

32. Was versteht man unter Security as a Service (SecaaS) der Cloud Security Alliance? Welche Dienste/Funktionalitäten werden typischerweise bereitgestellt?

Security Services welche durch den Provider zur Verfügunge gestellt werden und die Verantwortlichkeit zum Provider verlagert.

Dienste/Funktionalitäten:

- Identity and access management
- Data loss prevention
- Web security
- E-Mail security
- Security assessments
- Intrusion management
- Security information and event management (SIEM)
- Encryption
- Business continuity and disaster recovery
- Network security

33. Nennen und erläutern Sie fünf Service-Kategorien, die SecaaS bereitstellt.

- Data loss prevention: Überwachen, schützen und überprüfen von Daten um zu verhindern dass Daten unberechtigt das Unternehmen verlassen
- Web Security: echtzeit Schutz gegen Angriffe (Malware, Hacking) für eine Website
- Security Assessment: Audit um z.B.: Sicherheitsschwachstellen festzustellen
- Encryption: Verschlüsselung von Daten, z.B.: VPN um Daten bei der Übertragung zu sichern
- Network security: Monitoring und sichern der Netzwerkinfrastruktur gegen z.B.: DDoS-Attacken

ITS Lektion 14

Software Security Issues; Buch [Sta14] 11.1:

1. **In welche drei Kategorien werden die Fehler der CWE/SANS "Top 25 Most Dangerous Software Error List" gruppiert?**

- Insecure Interaction Between Components
- Risky Resource Management
- Porous Defense

2. **CWE/SANS Top 25 Most Dangerous Software Errors: Nennen Sie jeweils min. drei Beispiele für den Bereich**
    a. **Insecure Interaction between Components**
    b. **Risky Resource Management**
    c. **Porous Defenses**

a. SQL Injection, OS Command Injection, XSS
b. Buffer Overflow, Path Traversal, Download of Code Without Integrity Check
c. Missing Authentication for Critical Function, Missing Authorization, Use of Hard-coded Credentials

3. **CWE/SANS Top 25 Most Dangerous Software Errors: Überlegen Sie sich eine sinngleiche Übersetzung der drei Kategorien ins Deutsche. Beschreiben bzw. erläutern Sie weiters die einzelnen Kategorien mit eigenen Worten resp. anhand Ihrer Beispiele aus Antwort 2:**
    a. **Insecure Interaction between Components**
    b. **Risky Resource Management**
    c. **Porous Defenses**

a. Unsichere Interaktion zwischen Komponenten: Ausgabe des Frontends zum Backend wird nicht überprüft (z.B.: SQL Injection)
b. Riskantes Ressourcenmanagement: Eingaben werden nicht Überprüft und ermöglichen das Ausnutzen einer Schwachstelle (z.B.: Buffer Overflow, Path Traversal)
c. Schlechte Verteidigung: Authentifizierung und Autorisierung wird nicht oder nicht sicher durchgeführt (z.B.: Hard-coded Credentials, fehlende Authentifizierung)

4. **Software quality/reliability vs. Software security: Nennen Sie die wesentlichen Unterschiede hinsichtlich der jeweils erforderlichen Qualitätssicherungs-Maßnahmen.**

Bei normaler Qualitätssicherung werden wahrscheinliche Eingaben getestet um dadurch hervorgerufene Fehler zu finden. In Security hinsicht werden willkürliche Eingaben verwendet um einen ausnutzbaren Fehler zu provozieren.

5. **Nennen und erläutern Sie die Definition von "Defensive or Secure Programming". Was ist die Schlüsselregel?**

Programmieren von Software welche selbst unter Angriff noch funktioniert. Erkennen von fehlerhaften Verhalten -> weitere sichere Ausführung oder fail gracefully. Schlüsselregel: es darf nie etwas angenommen werden, aber es muss alles überprüft und auf jeden möglichen Fehler reagiert werden können.

6. **Beschreiben Sie das "Wesen und Wirken" eines Computerprogramms[1] unter Verwendung folgender Begriffe: Algorithmus, System Calls, Datenverarbeitung, Umgebung, Eingaben, Ausgaben, Betriebssystem.**

Ein Computerprogramm setzt einen oder mehrere Algorithmen für die Datenverarbeitung um, welche durch die Eingabe gespeist und als Ergebnis eine Ausgabe produzieren. Ein Programm wird unter einem Betriebssystem ausgeführt, welches die Umgebung für die Ausführung zur Verfügung stellt. Die Interaktion mit dem Betriebssystem erfolgt über sogenannte Systemcalls.

7. **Was ist das Software Assurance Forum for Excellence in Code (SAFECode)?**

Besteht aus großen Unternehmen der IT Industrie, entwickelt Best Practice Richtlinien für die Softwareentwicklung und Software-Sicherheit

Handling Program Input; Buch [Sta14] 11.2:

8. **Definieren Sie "Program Input". Was bzw. welche Quellen fallen Ihnen diesbezüglich ein?**

Jegliche Daten welche von außerhalb des Programms kommen und dessen Inhalt zur Zeit der Programmerstellung nicht bekannt sind.

[1] Als "Programm" bezeichnet man den niedergeschriebenen, ausführbaren Code bzw. eine ausführbare Datei als passives Objekt. Die aktive Instanz, d.h. das laufende Programm, ist eigentlich ein Prozess (oder Task).

9. **Welche beiden Kenngrößen sind bei möglichen Eingabewerten von Belang? Begründen Sie das.**

Größe der Eingabe: es muss ausreichend Speicher reserviert sein
Bedeutung und Interpretation: es muss z.B.: das Encoding bekannt sein um die Daten richtig dekodieren und Interpretieren zu können

10. **Was ist ein dynamischer Puffer?**

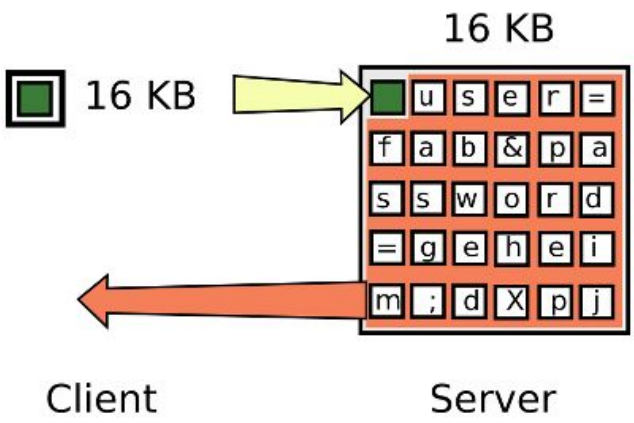
Der Speicher für den Puffer wird dynamisch reserviert, je nachdem wie groß die Eingabe ist.

11. **Was ist der Unterschied, wenn Eingabedaten binär oder textuell (characters) interpretiert werden? Nennen Sie je ein Beispiel.**

Bei binären Daten muss bekannt sein ob es sich z.B.: um einen Integer oder eine komplexere Struktur handelt.
Bei textuellen Daten muss das Encoding bekannt sein, z.B.: ASCII oder UTF8 um die Zeichen korrekt darstellen zu können. ASCII z.b.: kennt nicht alle UTF8 Zeichen und kann diese somit nicht darstellen.

12. **Lesen Sie sich auf heise.de den Artikel "So funktioniert der Heartbleed-Exploit" durch, und fassen Sie diesen kurz zusammen.**

Client schickt ein Heartbeat-Paket und gibt als Größe mehr an als er schickt. Der Server reserviert Speicher für die angegebene Größe, schreibt aber nur so viel wie er vom Client empfängt. Als Antwort sendet der Server die selbe Payload die er vom Client erhalten hat. Da dieser aber weniger geschickt hat als reserviert wurde, sendet der Server Inhalt aus dem Speicher mit, welcher mitunter sensibel Daten enthalten kann (private Key des Zertifikats)



13. **Webapplication-Security: Wiederholen Sie von Kapitel 12 (OWASP Top-Ten) die Punkte “Injection bzw. File Inclusion” sowie Cross Site Scripting (XSS). Formulieren Sie hinsichtlich des Themas “Handling Program Input” das gemeinsame Kernproblem.**

Injection bzw. File Inclusion: Code wird direkt oder indirekt in über die Eingabe der Webanwendung in diese eingebracht und zur Ausführung gebracht
XSS: es wird Code in die Webanwendung über die Eingabe eingebracht, welcher auf der Client-Seite ausgeführt wird.

In beiden Fällen wird die Eingabe nicht richtig überprüft und es ist einem Angreifer möglich Code auf Seiten des Servers (Injection, File Inclusion) zur Ausführung zu bringen, oder die Webanwendung auszunutzen und Code auf Seiten des Clients auszuführen.

14. **Validierung des Inputs: Unterscheiden Sie Whitelisting und Blacklisting.**

Whitelisting: es sind bestimmte, sichere Eingaben erlaubt
Blacklisting: bekannte gefährliche Eingaben werden blockiert

15. **Was ist ein “regulärer Ausdruck”? Bringen Sie ein Beispiel.**

Muster welches aus einer Sequenz aus Zeichen besteht, welche erlaubte Eingaben beschreiben.

Bsp.: [hc]at lässt hat und cat zu

16. **“Multiple Encodings”:**
    a. **Was versteht man unter dem Unicode-Standard und weiters in diesem Zusammenhang unter dem Unicode Transformation Format (UTF)[2]?**
    b. **Welche Sicherheitsprobleme ergeben sich durch die Verwendung unterschiedlicher Encodings? Nennen Sie ein Beispiel.**
    c. **Was versteht man unter “Kanonisierung”? Welches Problem wird dadurch gelöst?**

a. Erweiterung gegenüber Standard ASCII um z.B.: japanische und chinesische Zeichen darzustellen. UTF ist das entsprechende Encoding welches verwendet wird z.B.: UTF-8 -> 8 bit Encoding
b. Das Encoding muss dem Gegenüber bekannt sein oder bekannt gemacht werden. Ansonst muss das Gegenüber das Encoding annehmen.
   Erschwert das Filtern und kann zu fehlinterpretationen führen.
   z.B.: UTF-8 kennt mehrere Encodings für “/”, dadurch wird es schwieriger dies zu filtern.
c. Ersetzen von alternativen, äquivalenten Encodings durch ein standardmäßiges Encoding

17. **“Fuzzing”: Erläutern Sie diese Test-Methode und nennen Sie Vor- und Nachteile.**

Testtechnik welche zufällig generierten Input für eine Anwendung generiert um Fehler zu entdecken. Ermöglicht es relativ einfach ausnutzbare Fehler zu finden. Fehler welche durch z.B.: Komplexe Sequenzen hervorgerufen werden, werden wahrscheinlich nicht gefunden.

Writing Safe Program Code; Buch [Sta14] 11.3:

18. **Warum war es in frühen Versionen des Netscape Browsers möglich, bei SSL-Verbindungen den Session Key zu erraten?**

Schlecht implementierter Zufallszahlengenerator, welcher es möglich gemacht hat die Zufallszahlen vorher zu sagen.

19. **Aus welchem Grund ist dezidierter Test- resp. Debugging-Code nicht nur nützlich?**

Wird der Code mit der produktiven Anwendung ausgeliefert, ist es möglich dass dieser von einem Angreifer ausgenutzt wird (z.B.: sendmail, DEBUG-Command durch welches sendmail remote gesteuert werden konnte)

[2] Der Blogeintrag “The Absolute Minimum Every Software Developer Absolutely, Positively Must Know About Unicode and Character Sets" des CEO von stackexchange.com fasst die Problematik auf kurzweilige Art und Weise zusammen.

20. **Welche Probleme können aus Unterschieden zwischen dem im Quellcode implementierten Algorithmus und dem resultierenden Maschinencode entstehen?**

Durch Kompileroptimierungen ist es möglich das Sicherheitsvorkehrungen ausgehebelt werden und dadurch der Algorithmus im eigentlichen Sourcecode nicht angreifbar ist, aber durch die Optimierungen der Maschinencode angreibar ist.

21. **Starke vs. schwache Typisierung:**
    a. **Erläutern Sie, was man darunter versteht.**
    b. **Stellen Sie Vor- und Nachteile gegenüber.**
    c. **Nennen Sie beispielhaft Programmiersprachen.**

a. Bei starker Typisierung werden die möglichen Operationen eingeschränkt auf die welche für den Typ zulässig sind. (z.B.: C ist schwach typisiert, da Datentypen einfach anders interpretiert werden können, z.B.: ein Integer als Pointer)
b. Stark typisiert: vermeidung von Fehlern durch einschränkung der Operationen
   Schwach typisiert: mehr freiheit beim programmieren durch einfacheres Ändern der Interpretierung eines Datentyps.
c. Schwach typisiert: C, PHP
   Stark typisiert: C++, Object Pascal

22. **Was versteht man unter “Memory Leak”?**

Anwendung verabsäumt die Freigabe von Speicher, wodurch sukzessive der vorhandene Heap-Speicher belegt wird und dadurch die Anwendung bei vollem Heap möglicherweise abstürzt.

Interacting with the OS and Other Programs; Buch [Sta14] 11.4:

23. **Zählen Sie Quellen auf, aus denen ein Prozess vom ausführenden Betriebssystem Information bezieht.**

Umgebungsvariablen, Kommandozeilen-Argumente

24. **Mehrfachzugriff von unterschiedlichen Subjekten auf gemeinsam verfügbare Objekte im Betriebssystem: Zählen Sie Relationen (Subjekt -> Objekt) auf, die sicherheitstechnisch relevant sind.**

- Datei wird von zwei Benutzern gleichzeitig editiert
- USB-Stick soll ausgeworfen werden während noch darauf geschrieben wird

25. **Welche Möglichkeiten bieten sich für einen Angreifer bei der Manipulation von Umgebungsvariablen? Nennen Sie ein Beispiel.**

Möglichkeit nicht validierten Input in das Programm zu bringen.
z.B.: PATH-Variable: kann durch Angreifer manipuliert werden, sodass beim Aufruf eines Programmes zuerst das vom Angreifer kontrollierte Verzeichnis durchsucht wird -> Angreifer platziert Schadprogramm mit Namen des aufgerufenen Programms.

26. **Welche möglichen Schwachstellen ergeben sich im Zusammenhang mit der Umgebungsvariablen `LD_LIBRARY_PATH` ?**

Ermöglicht es einem Angreifer ein Verzeichnis in LD_LIBRARY_PATH zu schreiben, welches als erstes durchsucht wird und hinterlegt in diesem Verzeichnis eine Dynamic Loadable Library welche anstatt der eigentlichen geladen wird und Schadcode ausführt.

27. **Privileges and Access Rights:**
    a. **Mit welchen Rechten werden Prozesse idR bei Ihrem Start ausgestattet?**
    b. **Was versteht man unter "Privilege Escalation"?**
    c. **Erläutern Sie das setuid-Dateirecht bei Unix.**
    d. **Nennen Sie Situationen, in denen ein Prozess - wenn auch nur kurzfristig - Superuser-Rechte (root, administrator) benötigt.**

a. Mit den Rechten des aufrufenden Benutzers.
b. Rechteausweitung, im Idealfall um das komplette System kontrollieren zu können.
c. Durch das setuid-Dateirecht wird die Datei als der Benutzer ausgeführt, welcher als Owner (Besitzer) eingetragen ist. (setuid auf Datei welche root gehört -> Datei läuft bei Ausführung als root)
d. Verwendung von lowlevel Port (<1024) z.B.: SSH, ändern des Benutzerpassworts, Benutzer-Login

28. **Erläutern Sie mögliche Verwundbarkeiten, wenn ein Webserverprozess (httpd) hinsichtlich seiner Schreibrechte nicht nach dem "Least Privilege"-Prinzip konfiguriert ist.**

Defacement -> Angreifer ersetzt die Dateien der Website

29. **Welchen Vorteil bietet die modulare Aufteilung komplexer Programme?**

Höhere Privilegien nur einem Teil und nur solange wie nötig. Höhere Isolation zwischen den Komponenten. Einfacheres Testen.

30. **Isolation von Prozessen:**
    a. **Erläutern Sie die Grundsätze des Sandbox-Mechanismus und nennen Sie ein konkretes Beispiel.**
    b. **Was ist ein “chroot-jail”?**

a. Isolation und stärkere Kontrolle des ausgeführten Programms
b. Isoliert die Sicht eines Programms auf das Dateisystem auf einen bestimmten, konfigurierten Teil. Dadurch kann bei kompromittierung des Programms nur dieser Teil des Dateisystems manipuliert werden.

31. **Welche Probleme ergeben sich bei Solid-State Disks beim Verändern von Dateien? Verallgemeinern Sie aus dieser Tatsache das prinzipielle Problem, das sich an der Schnittstelle (OS, Treiber) -> (Device, Controller) ergibt.**

Bei einer SSD versucht der Controller die Schreibzugriffe auf einen Block so gering wie möglich zu halten und verwendet deswegen möglicherweise einen anderen Block.
Durch die vielen Schichten kann nicht eine einfache Annahme getroffen werden, dass Code welcher Daten überschreiben soll diese auch wirklich auf Blockebene am Speicher überschreibt.

32. **Synchronisationsmechanismen auf Filesystemebene:**
    a. **Erläutern Sie die Lösung über Lockfiles.**
    b. **Welche Probleme ergeben sich bei der Verwendung von Lockfiles?**
    c. **Was versteht man unter einer “atomaren Operation”?**

a. Programm erstellt ein Lockfile bei Zugriff auf eine geteilte Ressource. Ein Programm muss vorher prüfen ob ein Lockfile vorhanden ist bevor es auf die geteilte Ressource zugreift und gegebenenfalls warten.
b. Ist abhängig von der Implementierung im Programm, kann auch einfach ignoriert werden.
c. Für den Check eines Lockfiles sollte nicht zuerst eine Leseoperation und dann gegebenenfalls eine Schreiboperation folgen, da zwischen den beiden Operationen ein anderes Programm ein Lockfile erstellen könnte.
   Ein Programm soll direkt das Lockfile erstellen und kann anhand einer auftretenden Fehlermeldung feststellen ob ein Lockfile existiert.

33. **Stellen Sie die Problemstellung hinsichtlich Shared Files jenen hinsichtlich temporärer Dateien gegenüber. Wieso beschreibt Stallings das als “konträres Problem”?**

Temporäre Dateien sollen nicht zwischen Prozessen geteilt werden und das Ziel ist es die Berechtigungen so zu setzen, dass nur das erstellende Programm drauf Zugriff hat.
Dafür muss ein einzigartiger Dateiname verwendet werden.
konträres Problem: bei geteilten Ressourcen soll der Zugriff durch mehrere Programme geregelt werden.

34. Erläutern Sie die Verwundbarkeit CVE-2001-0774 (“Tripwire vulnerable to arbitrary file overwriting via symlink redirection of temporary file”).

Name der temporären Datei konnte erraten werden und durch setzen eines Symlinks auf das passwd-File mit Namen der temporären Datei war es möglich Tripwire dazu zu bringen das passwd-File über den Symlink zu überschreiben, da Tripwire mit root-Privilegien ausgeführt wird. Das überschreiben der passwd führt zu einem DoS da alle Login-Daten der User zerstört wurden.

35. Nennen, gruppieren und erläutern Sie Methoden zur Interprozesskommunikation[3].

Datentransfer:

Pipes, FIFOs, Stream Sockets	Bytestream zwischen Prozessen
SysV MQ, POSIX MQ	Austausch von messages zwischen Prozessen

shared memory:

SysV shmem, POSIX shmem, memory mapping	Prozesse teilen sich dieselben memory pages

Handling Program Output; Buch [Sta14] 11.5:

36. Der Output eines Programmes sollte deterministisch und authentisch sein. Überlegen Sie bzw. diskutieren Sie die resultierenden Sicherheitsimplikationen, wenn dies nicht zutrifft.

Wird der Output als Input für eine andere Anwendung verwendet kann dies zu z.B.: Command execution führen, wie z.B.: bei VT100 Textterminals wenn Steuerzeichen enthalten sind. Weiters können auch Daten manipuliert oder abgegriffen werden wie z.B.: bei XSS Angriffen, wo das Script des Angreifers über den Webserver ausgeliefert und am Client ausgeführt wird. Dies ermöglicht es z.B.: Cookies zu stehlen.

[3] Eine gute Übersicht zu IPC bietet die Vortragsunterlage “An Introduction to Linux-IPC” (PDF) von Michael Kerrisk, Autor des Buches “The Linux Programming Interface” (Oktober 2010, No Starch Press, ISBN 978-1-59327-220-3).

ITS Lektion 15

1. **Versuchen Sie, für den Begriff “Malware” eine vollständige Definition zu finden.**

Malware ist ein Schadprogramm welches über verschiedene Verteilungsmechanismen verteilt wird und eine Payload mit sich trägt welche die schädliche Funktion ausführt. Weiters handelt die Malware autonom oder kann auch ferngesteuert werden. Meist wird für die Verbreitung und möglicherweise auch für die Payload eine oder mehrere Schwachstellen im System ausgenutzt.

Types of malicious software, Advanced Persistent Threat (APT); Buch [Sta14] 6.1,2:

2. **Nach welchen Gesichtspunkten kann man die unterschiedlichen Arten von Malware klassifizieren?**

- Art der Verteilung
- Art der Payload

3. **Nennen Sie Möglichkeiten, wie sich Malware verbreiten kann (Propagation Mechanisms).**

- Selbständiges verbreiten durch Ausnutzen einer Schwachstelle im System
- Verteilung durch mithilfe des Users (z.B.: Versand per Mail)
- Getarnt in einer legitimen ausführbaren Datei (Trojaner)
- drive-by-download

4. **Malware: Treffen Sie eine Unterscheidung hinsichtlich der Autarkie (Selbstständigkeit) sowie der Replikationsfähigkeit und nennen Sie Beispiele.**

Infektion von Applikationen -> keine selbständige Verbreitung, wird durch Hilfe des Users verbreitet (Virus)
Eigenständige Applikation -> nutzt Schwachstelle im System aus und verbreitet sich so von System zu System (Wurm)

5. **Payload Actions: Ein Sammelbegriff lautet “bösartige, ärgerliche und irreführende Software”. Nennen Sie jeweils Malware-Funktionalitäten, die diesen Eigenschaften zuzuordnen sind.**

bösartig: löschen von Dateien, Remote Zugriff für angreifer
ärgerlich: Malwaretising -> Popups
irreführend: Verschleierung (versteckt sich, z.B.: durch ähnlichen Namen im system32 Ordner)

6. **Was versteht man unter "Crimeware". Erläutern Sie als prominentes Beispiel die Funktionalität des "ZeuS Crimeware Toolkit"[4].**

Toolkits welche das generieren von Malware mit verschiedenen Propagation-Mechanismen und Payloads ermöglicht.

Botnet welches via Phishing verteilt wird und Credentials (vorallem eBanking-Daten) abgreift.

7. **Nennen Sie unterschiedliche Institutionen/Organisationen, die Malware für ihre Zwecke einsetzen.**

politisch motiviert, Kriminelle, organisiertes Verbrechen, Nationen

8. **Advanced Persistent Threat (APT). Erläutern Sie die namensstiftenden Charakteristika:**
    a. **Advanced**
    b. **Persistent**
    c. **Threats**

a. anwenden verschiedener Techniken zum eindringen, genau auf Einsatz zugeschnitten
b. Angriff über einen längeren Zeitraum, mit unterschiedlichen Methoden, um Erfolgschancen zu maximieren
c. Gefahr für Ziel durch organisierte, fähige und gut finanzierte Angreifer

[4] Vgl. "Zeus: King of the Bots" von Symantec (2009).

Propagation: Virus vs. Wurm vs. Trojaner; Buch [Sta14] 6.3-5:

9. **Virus vs. Wurm vs. Trojaner:**
    a. **Was versteht man unter einem Virus. Was ist für diese Art von Software charakteristisch und inwiefern unterscheidet sich ein Virus von einem Wurm und einem Trojaner? Nennen Sie weiters ein konkretes Beispiel für einen Virus.**
    b. **Was versteht man unter einem Wurm. Was ist für diese Art von Software charakteristisch und inwiefern unterscheidet sich ein Wurm von einem Virus und einem Trojaner? Nennen Sie weiters ein konkretes Beispiel für einen Wurm.**
    c. **Was versteht man unter einem Trojaner. Was ist für diese Art von Software charakteristisch und inwiefern unterscheidet sich ein Trojaner von einem Wurm und einem Virus? Nennen Sie weiters ein konkretes Beispiel für einen Trojaner.**

a. “Infizieren” andere Programme, fügen sich selbst einem Programm hinzu und ändern den Programmfluss so, dass auch der Virus ausgeführt wird wenn das Programm ausgeführt wird. Benötigt menschliche Hilfe zur Verbreitung -> Programm muss ausgeführt werden.
   Bsp.: Brain Virus
b. Nutzt Schwachstelle im System aus um sich selbst zu verbreiten, sucht effektiv nach Maschinen welche infiziert werden können.
   Bsp.: Conficker
c. Versteckt sich in einem legitimen Programm und wird bei der ausführung dessen aktiv und führt die Schädliche funktion aus. Im gegensatz zum Virus werden keine anderen Programme infiziert. Bietet oft dem Angreifer eine Hintertür zum System.
   Bps.: Hydraq

10. Viren:

- **a. Aus welchem Grund war diese Art von Schadsoftware anfänglich so erfolgreich?**
- **b. Aus welchen drei funktionalen Komponenten besteht ein Virus bzw. Malware im generellen? Erläutern Sie die Komponenten.**
- **c. Klassifizieren/Unterscheiden Sie unterschiedliche Arten von Viren anhand**
  - **i. des Infektionsziels,**
  - **ii. der eingesetzten Verschleierungstaktik.**
- **d. Was versteht man unter einem Makrovirus? Was macht Makroviren besonders gefährlich?**

a. fehlende Authentifizierung und Zugriffskontrolle
b. Infektionsmechanismus, Auslöser, Payload
c. .
   i. Boot sector infector, File infector, macro virus, multipart virus (verschiedene Methoden um verschiedene Dateien zu infizieren)
   ii. Verschlüsselung, Stealth (mutation, komprimierung, rootkit-Technik), polymorph (veränderung der Codestruktur), metamorph (schreibt sich selbst neu durch verschiedene Transformationstechniken, auch mögliche Verhaltensänderung)
d. eingebettet in z.B.: Excel-Datei, ausführbarer Makrocode, Plattformunabhängig, infiziert Dokumente, Zugriffskontrolle nicht zielführend da davon ausgegangen wird dass die Datei geändert wird durch User

11. **Würmer:**
    a. **Zählen Sie Möglichkeiten auf, wie sich Würmer über Netzwerke erfolgreich verbreiten können.**
    b. **Aus welchen beiden Teilaufgaben besteht die Fortpflanzungs-/Verbreitungsphase eines Wurms? Erläutern Sie diese.**
    c. **Interpretieren Sie die Abbildung 6.3. im Buch hinsichtlich der epidemischen Dynamik, mit der sich Würmer verbreiten und nennen Sie die drei Phasen.**
    d. **Nennen und beschreiben Sie mindestens drei bekannte Würmer der letzten Jahre.**
    e. **Zählen Sie die herausragenden Eigenschaften/Funktionen eines "state of the art" Wurms auf.**

a. Mail, file sharing, remote execution capability, remot file access/transfer, remote login capability
b. Suchen eines Zieles (host table, Adressbuch, Buddy List, Scan v. IP Range) und dorthin Propagieren (ausnutzen einer Schwachstelle)
c. Zu beginn sind wenig Maschinen infiziert, deshalb verbreitet sich der Wurm nur langsam, dann steigt die Geschwindigkeit exponential und nimmt gegen Ende wieder ab, da hier oft versucht wird bereits infizierte Maschinen erneut zu infizieren
d. Warezov: erzeugt mehrer ausführbar Dateien im System-Verzeichnis und startet diese automatisch beim Systemstart, propagiert via Email
   Conficker: propagiert über Windows Buffer Overflow und USB Sticks
   Stuxnet: gezielter Angriff auf Uran Zentrifugen, verteilt via USB Sticks
e. Multiplatform, Multi-exploit, Ultrafast spreading, Polymorphic, Metamorphic, Transport vehicels (liefern Schadcode aus), ausnutzen von Zero-day exoploits

12. **Nennen und erläutern Sie die vier Phasen im Lebenszyklus eines Virus oder eines Wurms.**

Dormant phase: wartet auf aktivierung
Propagation phase: Verteilung, Angriff des Ziels
Triggering phase: aktivierung der Payload
Execution phase: ausführen der Payload

13. **Was versteht man unter einem "Zero-Day Exploit"?**

Unbekannte Schwachstelle, welche noch nicht öffentlich gemacht wurde und wahrscheinlich nur dem Entdecker bekannt ist. -> Noch kein Patch verfügbar.

14. **Mobile Code:**
    a. **Was versteht man unter dem Begriff "mobile Code"?**
    b. **Wie unterscheidet sich das Ausführungsmodell von mobilem Code vom Client-Server Modell?**
    c. **Nennen Sie Beispiele für mobilen Code.**

a. Skript, Makro, etc. welches ohne Änderung auf verschiedenen Plattformen mit identen Ergebnis ausgeführt werden kann.
b. Wird am Client ausgeführt, benötigt Server nur für Auslieferung
c. JavaScript, VBScript, Java Applets

15. **Erläutern sie folgende Begriffe. Welche Verwundbarkeiten werden hier (und wo) ausgenützt?**
    a. **Drive-by Download**
    b. **Watering-hole Attack**
    c. **Malvertising**
    d. **Clickjacking**

a. Web Seite unter kontrolle des Angreifers welche ein Browser Exploit ausnutz um bei ansurfen der Seite Malware downloaded und installiert
b. gezielte Version des drive-by downloads, sucht gezielt Schwachstelle in Website welche vom Opfer genutzt wird und verwendet malware welche möglicherweise auch nur am System des Opfers ausgeführt wird
c. Platzieren von Werbung auf einer Website und aufrufen dieser Werbung über infizierte Opfer um Geld durch die Clicks zu lukrieren
d. Platzieren eines unsichtbaren Frames über der eigentlichen Website. Dadurch können Clicks auf der Website für andere Aktionen missbraucht werden.

Payload; Buch [Sta14] 6.6-9:

16. **Nennen Sie mögliche Schäden an Systemen, die durch Malware verursacht werden können.**

Datenverlust, Zerstörung von Hardware

17. **Was versteht man unter Ransomware?**

Verschlüsselt Daten des Opfers und fordert Lösegeld für die Herausgabe des Schlüssels

18. **Zählen Sie mindestens drei Einsatzmöglichkeiten für einzelne Robots (Bots) bzw. ganze Botnets auf.**

DDoS, Spamming, Keylogging, verteilen neuer Malware, Traffic Sniffing

19. **Welches Merkmal unterscheidet einen Bot von einem Wurm?**

Bot wird zentral gesteuert (C&C)

20. **Command-and-Control (C&C) Funktionalität. Zählen Sie mögliche Umsetzungen auf.**

IRC, P2P, HTTP

21. **Was versteht man unter "Phishing"? Was ist dabei der Unterschied zu "Spear-Phishing"?**

Versenden einer gefälschten Mail, z.B.: von einer Bank, welche auf eine gefälschte Website verweist. Auf dieser Website werden z.B.: Zugangsdaten abgegriffen.
Spear-Phishing ist die Zielgerichtet Variante. Mail ist maßgeschneidert auf Ziel (bekannter Service welchen dieser nutzt) und wird auch nur diesem zugestellt.

22. **Welche Parallele erkennen Sie zwischen Spear-Phishing und einem Watering-hole-Angriff?**

Zielgerichteter Angriff welcher möglichst unentdeckt bleiben soll

23. **Was versteht man unter einer "Backdoor"? Welchem Zweck diente dies ursprünglich?**

Zugriff über eine Funktion welche die Authentifizierung und Zugriffskontrolle umgeht. Sollte ursprünglich bei Entwicklung beim Debugging helfen.

24. **Rootkit:**
    a. **Welchen beiden Zwecken dient ein Rootkit?**
    b. **Wie funktioniert ein "User-Mode Rootkit"?**
    c. **Wie funktioniert ein "Kernel-Mode Rootkit"?**
    d. **Wodurch charakterisiert sich ein auf Virtualisierung basierendes Rootkit bzw. ein Rootkit im External Mode? Welche Gegenmaßnahmen fallen Ihnen diesbezüglich ein (Tipp: Lektion 6)?**

a. halten der Administrator/root-Privilegien, Entdeckung vermeiden
b. intercepted API-Calls und manipuliert Ausgabe (z.B.: verhindert Ausgabe bei Auflistung eines Verzeichnisses)
c. intercepted API-Calls auf Kernel-Ebene, kann sich dadurch von der Liste der aktiven Prozesse löschen
d. befinden sich ausserhalb des Betriebssystems, kann durch Trusted Platform Module verhindert werden (Signatur der Boot Stages)

Countermeasures; Buch [Sta14] 6.10:

25. **Anti-Malware Präventivmaßnahmen: Nennen Sie die vier erwähnten Hauptkategorien und finden Sie je ein konkretes Beispiel.**

- policy (Zugriffskontrolle)
- awareness (Training des Users)
- vulnerability mitigation (Patchmanagement)
- threat mitigation (Verschlüsselung)

26. **Anti-Malware Akutmaßnahmen:**
    a. **Nennen Sie die chronologisch ablaufenden (drei) Schritte.**
    b. **Nennen und erläutern Sie die Anforderungen an die Gegenmaßnahmen.**
    c. **Tiefgestaffelte Verteidigungsmaßnahmen: Wo bzw. an welchen Schnittstellen können Anti-Malware-Mechanismen eingesetzt werden?**

a. Erkennung, Identifikation, Entfernung
b. Generell: abhandeln von verschiedensten Attacken
   Zeitkritisch: schnelle Reaktion, möglichst wenig Infektionen
   Widerstandsfähig: gegen Evasion-Techniken des Angreifers
   Geringe Ausfallszeit
   Transparent: sollte keine Modifikation notwendig sein
   globale/lokale Abdeckung: Verteidigung gegen interne und externe Bedrohungen

27. **Nennen Sie Vor- und Nachteile von hostbasierter Antivirus (AV) Software.**

Vorteil: Zugriff auf alle Systemressourcen (kompletter Traffic, alle Dateien am System)
Nachteil: kann erst eingreifen wenn die Malware das System erreicht hat

28. **Beschreiben Sie die Entwicklung von AV-Software über die im Buch geschilderten vier Generationen und erwähnen Sie dabei die jeweils charakteristische Funktionalität.**

- einfache Scanner: Signatur basierend
- heuristische Scanner: heuristisches Regelwerk für die Suche nach Viren
- memory-resident: Erkennung von bestimmten Aktionen
- full-featured protection: Kombination verschiedener Techniken

29. **Was versteht man im Zusammenhang mit AV-Software unter "Generic Decryption"?**

Erkennen von Polymorphen Viren durch Simulation. Während der Simulation der Ausführung wird nach Viren Signaturen gescannt.

30. Nennen Sie verdächtige Aktionen im/am OS, die für ein hostbasiertes IPS alarmierend sind.

- öffnen, anzeigen, löschen, modifizieren von Dateien
- löschen der Festplatte
- modifikation von ausführbaren Dateien
- ändern von kritischen Systemeinstellungen
- gescripteter versand von ausführbaren Dateien
- aufbauen einer Netzwerkverbindung

31. Stellen Sie die beiden Richtungen (Ingress/Egress) gegenüber, entlang denen ein Network-based IDS (vgl. Lektion 7) Malware erkennen soll.

- eingehend: Anomalie oder Signaturerkennung, z.B.: Zugriffe auf nicht benutzte IPs
- ausgehend: Anomalieerkennung, z.B.: erkennen von Scan einer IP-Range durch einen Wurm

32. Beschreiben Sie die grundlegende Architektur/Funktionsweise eines verteilten IPS, wie sie zur Erkennung/Blockierung von Malware zum Einsatz kommt.

Sammeln von Informationen von verschiedenen Stellen (host-based und perimeter Sensoren) und sammelt diese an einer zentralen Stelle wo diese korreliert und analysiert werden. Auf basis der gewonnen Informationen können dann auf wiederum Signaturen und Verhaltensmuster für die Erkennung erstellt werden.