|  |  |
| --- | --- |
| **Grundlagen** | |
| **Kryptographie** | |
| Kryptographie | Kryptographie ist die Wissenschaft und Technik der Erstellung von Geheimschriften (Chiffre, Cypher). Grundsätzlich wird eine Nachricht mit Hilfe eines Schlüssels so umgewandelt, dass die entstehende Chiffre nur von dem gelesenen werden kann, der den Schlüssel kennt.  Umwandlung einer Nachricht (**Klartext**) mit Hilfe eines Verfahrens (**Krypto-Algorithmus**) und eines Geheimnisses (**Schlüssel**) in eine scheinbar sinnlose Zeichenfolge (**Geheimtext**), die mit Hilfe des Schlüssels und des Umkehrverfahrens wieder in den Klartext umwandelbar ist.  Ziele der Kryptographie ist die Sicherstellung der **Vertraulichkeit** (Zugriffsschutz), **Integrität** (Änderungsschutz)**, Verbindlichkeit** (Nichtabstreitbarkeit) und **Authentizität** (Fälschungsschutz). |
| Kryptoanalyse | Die Kryptoanalyse befasst sich mit der Ableitung eines Schlüssels oder eines Klartextes aus einer Chiffre ohne Schlüsselkenntnis.   * Vollständiges Brechen (Finden des Schlüssels) * Universelles Brechen (Finden eines äquivalenten Verfahrens) |
| Steganographie | Die Steganographie befasst sich mit dem Verstecken von geheimen Daten in anderen, in der Regel unbedeutenden Daten. |
| 3 Pfeiler der Netzwerk – Sicherheit | Netzwerksicherheit umfasst drei wesentliche Merkmale. Das eine ist die **Integrität**. Dazu zählen Mechanismen und Verfahren, die die Echtheit von Daten prüfen und sicherstellen können und somit auch vor Manipulation schützen. Das zweite ist die **Vertraulichkeit** der Kommunikation. Hier geht es darum dafür zu sorgen, dass niemand Einblick in die Daten und Kommunikation erhält. Hier stehen die **Authentifizierung** der Kommunikationspartner und die Verschlüsselung der Kommunikation im Vordergrund. Das dritte ist die Authentizität der Kommunikationspartner. Hier geht es darum festzustellen, ob der Kommunikationspartner auch tatsächlich der ist, für den er sich ausgibt. |
| Authentifizierung, Autorisierung und Authentisierung | Authentifizierung ist der Vorgang, bei dem eine Person oder Maschine auf ihre Identität geprüft wird. Autorisierung ist der Vorgang, bei dem ermittelt wird, was die Person oder Maschine machen darf (Berechtigung). Authentisierung bedeutet, dass eine Person oder Maschine sich gegenüber eines Kommunikationspartners identifizieren muss. |
| Authentifizierung | Die Authentifizierung erfolgt zum Beispiel mit Benutzername und Passwort. Knackpunkt bei jeder Authentifizierung ist die Übertragung von Benutzername und Passwort. Erfolgt die Übertragung unverschlüsselt, dann kann ein Angreifer die Zugangsdaten abhören und für seine Angriffsversuche missbrauchen.   * Pre – Shared – Key * Zertifikate |
| Pre – Shared – Key | Ein Pre – Shared – Key ist ein symmetrischer Schlüssel (Passwort, PIN), das vor einer Verbindungsaufnahme ausgetauscht werden muss. Es handelt sich dabei um einen unsignierten Schlüssel, der frei wählbar ist. Wer den Schlüssel kennt, bekommt Zugang zu einem Netzwerk. |
| **Angriffstypen** | |
| Brute Force Methode | Bedeutet das simple Ausprobieren verschiedener Passwortmöglichkeiten. Klassisches Anwendungsbeispiel für Brute Force Attacken ist das Knacken von verschlüsselten Passwortlisten, welche in der Regel aus Hash – Werten bestehen, bei welchen die Verschlüsselung nicht mehr rückgängig gemacht werden kann. Die einzige Möglichkeit der Gefahr entgegenzuwirken ist eine ständige Vergrösserung der Schlüssel. Derzeit ist eine Schlüssellänge von 1024 Bit gängig. |
| Wörterbuchangriff | Alle Schlüssel aus speziell zu diesem Zweck angefertigten Passwortsammlungen werden nacheinander durchprobiert. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativen einfachen Passwort ausgegangen werden kann. |
| Man in the middle | Die Man in the middle Attacke ist eine Angriffsart, bei der der Angreifer zwei oder mehrere kommunizierenden Computern den jeweils anderen Partner vorspielt. Der Angreifer kann dadurch Daten und Informationen nach Belieben einsehen und sogar manipulieren. Diese Angriffe können durch Einsatz kryptographischer Verfahren zur Verschlüsselung und Authentifikation wirksam vermieden werden.  Problem: Gehört der Public Key demjenigen, der ihn vorzeigt?  Lösung: Beglaubigung des Public Key durch „Trusted Third Pary“ |
| Geheitextangriff | Dem Angreifer steht ein grösseres Stück Geheimtext zur Verfügung. An diese Information kann der Angreifer etwa durch Sniffing oder durch eine Man-in-the-Middle Attacke gelangen. Der bekannte Geheimtext kann nun auf bestimmte Muster durchsucht werden. |
| Klartextangriff | Zusätzlich zum Geheimtext ist nun auch ein Teil der Klartextes bekannt. Daraus versucht der Kryptoanalytiker den Schlüssel zu finden, um den restlichen Klartext zu entschlüsseln. |
| Angriff mit ausgewählten Klartext | Der Angriff mit ausgewähltem Klartext ist ebenfalls ein Klartextangriff, mit dem Unterschied, dass der Angreifer selbst den Klartext vorgibt, diesen verschlüsseln lässt und den daraus entstehenden Geheimtext analysiert. Durch geeignete Wahl der zur verschlüsselnden Nachricht können eventuell sehr leicht Rückschlüsse auf das verwendetet Verschlüsselungsverfahren oder den Schlüssel gezogen werden. |
| **Symmetrische Verfahren** | |
| Symmetrisches Verschlüsselung | Hierbei wird derselbe Schlüssel zum Ver- und Entschlüsseln verwendet. Darin liegt auch der Nachteil dieses Verfahrens. Kennt ein Angreifer den Schlüssel, kann er Nachrichten entschlüsseln und eigene falsche Nachrichten verschlüsseln, ohne dass dies erkannt wird. Deswegen wird, wie bei SSL, meist vor der eigentlichen Datenübertragung der Schlüssel über ein asymmetrisches Verfahren ausgetauscht. |
| DES – Data Encyption Standard | DES ist immer noch eines der verbreiteten Verschlüsselungsverfahren, ein von der NSA entwickelter Algorithmus zur digitalen Signatur. Heute wird DES aufgrund der verwendeten Schlüssellänge von nur 64 Bit (jedoch 8 Bit als Prüfsumme) für viele Anwendungen als nicht ausreichend sicher erachtet. |
| 3DES | Die Schlüssellänge kann durch Mehrfachanwendung des DES auf einfache Weise vergörssert werden, dies wird als Tripple – DES bezeichnet. Blockgrösse 168 Bit davon 112 Bits Schlüssellänge. 3DES wurde durch AES als Standard abgelöst. |
| IDEA – International Data Encryption Standard | IDEA ist ein symmetrischer Algorithmus und gehört zu den Blockchiffren (mit einer Blocklänge von 64 Bit). Der Algorithmus wurde als Ersatz für DES in Erwägung gezogen. Schlüssellänge von 128 Bit 🡪 Softwarefreundlich |
| AES – Advanced Encryption Standard (Rijndael) | AES ist ein symmetrisches Kryptosystem, das als Nachfolger für DES und 3DES als Standard bekanntgegeben wurde. AES schränkt die Blocklänge auf 128 Bit und die Wahl der Schlüssellänge auf 128, 192 oder 256 Bits ein. Die Bezeichnung der drei AES – Varianten AES-128, AES-192 und AES-256 beziehen sich jeweils auf die gewählte Schlüssellänge. AES ist in den USA für staatliche Dokumenten mit höchster Geheimhaltungsstufe zugelassen. |
| **Asymmetrische Verfahren** | |
| Asymmetrische Verschlüsselung | Ist ein Verfahren mit unterschiedlichen Schlüsseln für die Ver- und Entschlüsselung. Der Schlüssel für die Verschlüsselung wird dabei veröffentlicht. Derart verschlüsselte Nachrichten können nur vom Besitzer des zugehörigen geheimen Schlüssels entschlüsselt werden. Problem Man-in-the-Middle Attacke: Ist das wirklich Bobs öffentlicher Schlüssel? 🡪 Zertifikate bestätigen die Zugehörigkeit von öffentlichen Schlüssel zu Individuen. |
| Vorteile und Nachteile | Gute Eignung für digitale Signaturen, Geringer Aufwand für die Schlüsselverwaltung und nach bisherigen Erkenntnisse extrem Unangreifbar.  Im Vergleich zum symmetrischen Verfahren werden grosse Schlüssellängen benutzt, Geringere Datendurchsatz bei der Ver- und Entschlüsselung. |
| RSA – Rivest Shamir Adlerman | Bekannteste und am meisten eingesetzten Algorithmus des asymmetrischen Verschlüsselungsverfahren. Basiert auf der Idee, dass die Faktorisierung einer Zahl eine sehr aufwändige Angelegenheit ist, während das Erzeugen der Zahl durch Multiplikation zweier Primzahlen trivial ist. Die RSA – Verschlüsselung mit 1024 Bit Schlüssellänge benutzt die Modulo – Funktion. |
| Diffie – Hellman – Merkle | Dieses asymmetrischen Verfahren verwendet man für den Schlüsselaustausch. Des besondere ist, dass nicht der geheime Sitzungsschlüssel, sondern nur das Ergebnis einer Rechenoperation übertragen wird. |
| **Hybride Verschlüsselung** | |
| Hybride Verschlüsselung | 1. Zuerst wird ein zufälliger Sitzungsschlüssel für die symmetrische Verschlüsselung generiert 2. Dann verschlüsselt der Sender diesen Sitzungsschlüssel mit dem Public Key des Empfängers (Asymmetrisches Verfahren) 3. Der Sender schickt dann den asymmetrisch Verschlüsselten Sitzungsschlüssel an den Empfänger. 4. Mit seinem privaten Schlüssel kann der Empfänger den Sitzungsschlüssel entschlüsseln 5. Danach werden die Daten mit Hilfe des Sitzungsschlüssels verschlüsselt übertragen |
| Einwegfunktion | Eine Funktion f(x) lässt sich leicht berechnen. Die Umkehrfunktion f^-1(x) lässt sich nur sehr schwer berechnen. Potenzieren mit zufällig gewählten Exponenten. Oft auch als Falltürfunktion bezeichnet. Beispiel Telefonbuch 🡪 Suche nach Namen einfach da alphabetisch, such nach Telefonnummer sehr schwierig. |
| **Hashfunktion** | |
| Hash Funktion | Die Hashfunktion ist eine eindeutige Prüfsumme (Fingerabdruck) aus einer beliebig grossen Datenmenge. Der Hashwert kann zum Auffinden von Daten in einer Datenbank oder zum digitalen Signieren eines Dokumentes verwendet werden.   * Eindeutigkeit: Eine identische Zeichenfolge muss zum selben Hash – Wert führen * Reversibilität: Der Hash – Wert darf nicht in die ursprüngliche Zeichenfolge zurückberechnet werden können * Kollisionsresistenz: Zwei unterschiedliche Zeichenfolgen dürfen nicht den gleichen Hash – Wert ergeben |
| MAC – Message Authentication Code | Ein MAC dient dazu, Gewissheit über den Ursprung von Daten oder Nachrichten zu erhalten und ihre Integrität zu überprüfen. MAC – Algorithmen erfordern zwei Eingabeparameter, erstens die zu schützende Daten und zweitens einen geheimen Schlüssel. Diese beiden Parameter berechnen die Prüfsumme. |
| MD5, MD2, MD4 – Message Digest | MD5 ist eine der bekannteste Einweg – Hashfunktion. Sie wurden ebenfalls, wie die beiden Vorgänger MD2 und MD4, von Ronald L. Rivest entwickelt. Sie arbeiten mit einer Blockgrösse von 512 Bit und einem 128 Bit langen Hashwert. MD5 gilt inzwischen nicht mehr als sicher, da es mit überschaubarem Aufwand möglich ist, unterschiedliche Nachrichten zu erzeugen, die den gleichen MD5 – Hashwert aufweisen. |
| **Zertifikate** | |
| Zertifikate  Gehört der Public Key demjenigen, der ihn vorzeigt? | Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Die Ausstellung des Zertifikates erfolgt durch eine offizielle Zertifizierungsstelle, die Certification Authority (CA) oder Trusted Third Party / Trusted Center. |
| Einsatzgebiete | |  |  |  | | --- | --- | --- | | Zweck | Bedeutung | Mittel | | Server – Authentifizierung | Ist das der echte Server? | SSL / TLS | | Client – Authentifizierung | Ist das der berechtigte User? | SSL / TLS, SSH | | Vertraulichkeit | Verschlüsselungsverfahren | PGP, S/MIME | | Integrität | Veränderung verhindern | S/MIME, Signatur | | Nicht Abstreitbarkeit | Du hast das gesagt! | S/MIME, Signatur | | Vertragliche Bindung | Weil du das gesagt hast! | Signaturgesetz | |
| CEO |  |
| Public Key Infrastructure (PKI) oder Authentication and Authorization Infrastructure (AAI) | Infrastruktur zum Management von Zertifikaten durch CA für eine Gruppe von Anwender, die Public Key Kryptographie einsetzen. |
| ITU-T Standard: X.509 | * Ausstellung der Zertifikate für die Anwender * Betrieb von Verzeichnis – Servern mit den Zertifikaten der Anwender * Pflege der CRL (Certificate Revovation Lists) 🡪 Sperrliste, Missbräuchliche Zertifikate * Archivierung der ausgestellten Zertifikate |
| PGP Certfificate | Ohne hierarchische Zertifikats – Authoritäten (Root CAs). Schlüssel selber verwalten. Schlüsselverteilkonzept ist das Web of Trust. Das PGB – Konzept basiert darauf, dass sich Anwender gegenseitig die Zertifikate signieren und dass dieses Vertrauen über mehrere Stufen vererbt. (Peer – Trust) |
| Digitale Signatur  Wieso ist der Absender und wieso die Unversehrtheit der Nachricht damit überprüfbar?  *Hash – Wert muss gleich bleiben, falls er sich ändert wurde die Nachricht verfälscht.* | Der private Schlüssel ermöglicht es, die Nachricht mit einer persönlichen Signatur zu versehen, welche durch den ergänzenden öffentlichen Schlüssel überprüft werden kann. Die digitale Signatur ist eine kleine Datei, die mithilfe des privaten Schlüssel aus dem Hashwert des Dokuments berechnet wird. Sie ist also die Verschlüsselung des Hashwerts eines Dokuments, nicht des Dokuments selbst. Zu jedem Dokument gibt es nur einen Hashwert. Sobald die kleinste Veränderung an dem Dokument vorgenommen wird, ergibt sich komplett anderer Hashwert. Zur Überprüfung der Signatur fordert der Empfänger den öffentlichen Schlüssel vom Trust Center und überprüft den Hashwert. |
| **Bedrohungen auf den unteren OSI – Schichten** | |
| **Allgemeine Gefährdung** | |
| Allgemeine Gefahren | * Konzeptionsfehler (Planungsfehler)   + Unvorhersehbare Entwicklung, insbesondere durch Kommerzialisierung * Programmierfehler   + Oft ungeprüfte Eingabepuffer (SQL Injection)   + Stack – Overflow / Manipulation des Programmzeigers * Konfigurationsfehler   + Falsche Berechtigungsvergabe auf Ebene des Filesystems   + Zu hohe Privilegien * Systemanomalien   + Einnisten / Verstecken von Malware |
| Buffer – Overflow  Exploit = Ausnützen eines Programmierfehlers. | Gehört zu den häufigsten Sicherheitslücken in aktueller Software, die sich unter anderem über das Internet ausnutzen lassen können. Im Wesentlichen werden bei einem Pufferüberlauf durch Fehler im Programm zu grosse Datenmengen in einen dafür zu kleinen reservierten Speicherbereich, den Puffer, geschrieben, wodurch nach dem Ziel-Speicherbereich liegende Speicherstellen überschrieben werden. |
| 4 mögliche negative Auswirkungen | 1. Verlust der Vertraulichkeit (Confidentiality)   Beschrönkerter Einfluss auf Transportwege / Überwachungsmöglichkeiten   1. Verlust der Integrität (Integrity)   Veränderung von Datenpaketen unterwegs (Gefälschte Daten)   1. Verlust der Verfügbarkeit (Availability)   Mutwillige Verhinderung des Zugangs (Denial of Service)   1. Verlust der Verbindlichkeit / Nichtabstreitbarkeit (non – repudiation)   Folge der vielfältigen Möglichkeit der Fälschung von Absenderangaben |
| **Informationsgewinnung (Passive Angriffe)** | |
| Passive Angriffe | Passive Angriffe bedrohen die Vertraulichkeit der Kommunikation, beeinflussen aber nicht die Kommunikation oder den Nachrichteninhalt. Sie zielen ausschliesslich auf die unerlaubte Informationsbeschaffung. |
| Geschwätzige Dienste | * Telnet (Telecommunication Network)   Keine Sicherheitsfunktionalitäten – es werden z.B. Passwörter im Klartext geschickt   * SSH (Secure Shell)   Die von SSH-1 verwendete Integritätsprüfung weist Schwachstellen auf, die es einem Angreifer ermöglicht, eine Sitzung auszuspähen   * SMTP (Simple Mail Transfer Protocol)   Erfordert die Einrichtung eines Sicherheitssystems, wie eine Firewall   * HTTP (Hypertext Transfer Protocol)   Unverschlüsseltes Protokoll, kann gesnifft werden   * FTP (File Transfer Protocol)   Unverschlüsseltes Protokoll, kann gesnifft werden |
| Portscanning | Ein Portscanner ist eine Software, mit der überprüft werden kann, welche Dienste ein mit TCP oder UDP arbeitendes System über das Internetprotokoll anbietet. Der Portscanner nimmt dem Anwender dabei die Arbeit ab, das Antwortverhalten eines Systems selbst mit einem Sniffer zu untersuchen und zu interpretieren. 🡪 Systematische Suche nach Ports von Serverprozessen und Kontaktaufnahme mit bzw. Suche nach Trojanischen Pferden |
| Logfile einer Firewall | Bekannte Ports erzeugen kommentierte Fehlermeldungen. Serien von wilden Synchronisationen werden als mögliche Scans registriert. Diese werden in dem Logfile der Firewall gespeichert. |
| **Aktive Angriffe** | |
| Aktive Angriffe | Bei den aktiven Angriffen werden die Nachrichten, die Komponenten des Kommunikationssystems oder die Kommunikation verfälscht. |
| Spoofing | Spoofing (Manipulation, Verschleierung oder Vortäuschung) nennt man in der Informationstechnik verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität (Authentizität).   * IP Spoofing * ARP Spoofing * DNS Spoofing |
| IP Spoofing | IP – Spoofing zählt zu den Man-in-the-Middle Angriffen. Befindet sich der Angreifer innerhalb des Kommunikationsweges, kann er die nächste Sequenznummer vorhersagen und sich in die Kommunikation zweier Stationen einklinken (Session Hijacking). Der Grund, warum das möglich ist, dass die beiden Teilnehmer sich nur am Anfang der Kommunikation gegenseitig authentifizieren.   1. Angreifer flutet Client 1 mit einer Menge von TCP SYN Messages (TCP) Client 1 wird flachgelegt 2. Angreifer baut eine Anzahl von TCP Verbindungen zu Client 2 auf mit seiner wahren IP Adresse um die laufende Sequenznummer herauszufinden 3. Angreifer baut eine TCP Verbindung zu Client 2 auf mit der IP Adresse von Client 1 auf.   Massnahmen: Paketfilter sind eine mögliche Gegenmassnahme gegen IP Spoofing. Von aussen kommende Pakete, die Quelladressen von innenliegende Rechner haben, werden verworfen. Idealerweise sollten auch ausgehende Pakete gefiltert werden, wobei dann Pakete verworfen werden, deren Quelladresse nicht innerhalb des Netzwerk liegt. |
| DNS Spoofing | DNS Spoofing bezeichnet einen Angriff, bei dem es gelingt, die Zuordnung zwischen einem Hostname und der zugehörigen IP – Adresse zu fälschen.   * Ausnutzen von Sicherheitslücken in der Software des DNS Servers * Betreiberseitige Manipulation des DNS Servers * Falscheinträge in der Host – Datei des anfragenden Clients (DNS IP ändern) |
| ARP Spoofing | Beim ARP Spoofing gibt der Angreifer seine eigene MAC – Adresse als die eines anderen Endgerät aus. Ist nur möglich, wenn sich der Angreifer im selben lokalen Netzwerk befindet. |
| DoS – Denial of Service | DoS sind Angriffsversuche auf einen Rechner, Server oder ein ganzes Netzwerk. In der Regel wird dabei ein Dienst, ein Server oder ein ganzes Netzwerk mit Verbindungsversuchen überflutet (SYN – Flooding). Wichtig dabei ist, dass die Antworten (Response) irgendwohin geschickt werden, nicht auf sich selbst sonst ist man auch vom Response flach. Grössere Überlastungseffekt erzielt man durch gleichzeitig agierenden Zombies (Botnetzwerk). |
| DRDoS – Distributed Reflection Denial of Service | DrDoS ist ein Angriff bei dem der Angreifer sein Opfer nicht direkt angreift, sondern dieser von Dritten angegriffen wird. Der Angreifer sendet Anfragen an Internet Services, die diesen beantworten. Da der Angreifer mittels IP Spoofing eine falsche IP Adresse angibt, nämlich die seines Opfers, beantwortet die Internet Services die Anfrage an die vorgetäuschte Adresse. Rückverfolgung ist unmöglich. |
| Gegenmassnahmen | * IP – Adresse Sperrliste durch Firewall (TCP – SYN / ICMP – Pakete) * Serverlastverteilung (Bereitgestellte Dienste mithilfe Virtualisierungstechniken auf verschiedene Rechner verteilt) * IP – Spoofing unterbinden |
| **Gefährdung und Sabotage auf höheren Ebenen** | |
| Code Injection / Script Injection | Code – Injection ist die Ausnutzung eines Computerfehlers, der durch die Verarbeitung von ungültigen Daten verursacht wird. Code – Injection kann von einem Angreifer verwendet werden um einem Programmcode zu injizieren der die Ausführung des Programms ändert.    Sobald der nächste Benutzer die Seite besucht wird der injizierte Code ausgeführt. |
| SQL Injection | Diese Technik wird benutzt um Datengetriebene Programme anzugreifen. Dies wird getan indem bei einem Eingabefeld SQL – Anweisungen eingetragen werden, welche die Website dazu bringen sollen, neue SQL – Anweisungen in die Datenbank zu schreiben. |
| Cross Site Scripting (XSS)  Nichtpersistentes XSS | Bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden. Ziel ist es meist, an sensible Daten des Benutzers zu gelangen (Identitätsdiebstahl). |
| Cross Site Request Forgery (CSRF) Persistentes XSS | CSRF funktioniert dann, wenn ein Benutzer eine authentisierte Verbindung zu einer Website im Browserregister #1 hat und im Register #2 eine bösartige Website besucht. Der böswillige Code von dieser Site kann die authentisierte Verbindung der anderen Site missbrauchen.  Massnahmen:   * Verhinderung durch Token, welcher mit Session gestartet wird * Ausloggen nach Login (Session Destroy) * Inkognito Modus |
| Drive By Injection | Der Begriff Drive By Injection bezeichnet einen möglichen Infektionsweg, wie Schadsoftware auf ein Clientsystem gelangt. Dabei ist immer auch eine Interaktion des Opfers notwendig. So muss es beispielsweise auf einen Link in einer Email klicken oder aktiv eine Website ansteuern. Ist dies der Fall und der Rechner des Opfers weist eine Schwachstelle im Webbrowser auf, wird diese automatisch ausgenutzt. Erst in einem zweiten Schritt wird dann der eigentliche Schadcode nachgeladen. Der Opfer merkt überhaupt nichts von dem Angriff. Je nach ausgenutzter Schwachstelle kommt es jedoch vor, dass der Webbrowser unverhofft beendet wird. |
| Waledec Botnetz | Mit einigen hunderttausende infizierten Rechner war das Waledec Botnetz eines der grösste Botnetze weltweit. Versand von mehr als 1.5 Milliarden Spam Emails pro Tag verantwortlich. Microsoft schaltete alle .com Domains zur Kontrolle und Pflege des Botnetzes ab. Nach und Nach löschte VeriSign die Verweise im Domain Name System und schnitt den Zombies den Kommunikationskanal zu den acht sogenannten Command & Control Server ab.  **Spammer**: Sie versenden die eigentlichen Spam Mails und verursachen damit den massiven Verkehr. Sie verfügen aber nicht über öffentlich erreichbare IP – Adressen, sondern sitzen hinter NAT-Router. **Repeater**: Das sind die Einstiegspunkte für neue Bots, die ins Netz aufgenommen werden. Sie sind auch die Anlaufpunkte für aktive Bots. Daher müssen sie unter einer öffentlicher IP erreichbar sein. Spammer kontaktieren die Repeater, um neue Aufträge vom Botmaster zu erhalten, oder um den erfolgreichen Abschluss einer Operation zu melden. Diese Request werden von den Repeater an geeignete Backend – Servern weitergeleitet. Eine weitere Aufgabe der Repeater ist das Vermitteln von HTTP Verbindungen zur Pflege des Fast Flux Netzes von Waledac.  **Backend – Server**: Sie beantworten die an sie vermittelten Anfragen der Spammer sowie die Queries der Repeater zur Pflege des Fast Flux Netztes. Diese Server sind perfekt synchronisiert mit nginx. |
| SCADA Angriffe – Supervisory Control and Data Acquisition | In erster Linie sind SCADA – Systeme für kritische Operationen und die nationale Infrastruktur verantwortlich. Im Falle eines erfolgreichen Angriffss führt dies nicht nur zum Verlust von Daten, sondern auch zu hohen Schäden und Menschenleben. (Stuxnet, Flame) |
| **Angewandte Kryptologie** | |
| **PKI – Anwendungen** | |
|  |  |
|  |  |
| Class 1 Certificates (Wenig Sicherheit) | * Keine Überprüfung der Identität des Antragsstellers * Zertifikat eingetragene Name ist einmalig in der CA – Subdomain * Gratis, Identitätsprüfung mithilfe Email Ping * PERSONA NOT VALIDATED |
| Class 2 Certificates (Mittlere Sicherheit) | * Überprüfung mithilfe von Dokumenten und Datenbanken   + Private (Kopie von Pass, Domänenregistereintrag)   + Firmen (Unterschrift, Kopie von Pass & Handelsregisterauszug) |
| Class 3 Certificates (Hohe Sicherheit) | * Überprüfung durch persönliches Vorsprechen & Pass zeigen * Weitere Prüfungen analog zu Klasse 2 |
| Qualified Certificates (Höchste Sicherheit) | * Analog Klasse 3 * Zusätzlich steht die CA unter staatlicher Kontrolle * Nur natürliche Personen ausgestellt |
| Extended Validation Certfificates (Höchste Sicherheit) | 🡪 SSL – Zertifikat (Grüne Adresszeile im Browser).   * Rechtliche und operationelle Existenz geprüft werden * Nahestehende Drittperson der Firma mitunterzeichnet werden * Zustellung des Antrags per Post und telefonisch überprüft * CA muss ihre Prozesse jährlich auditieren lassen |
| SSL / TLS | SSL ist die Abkürzung für Secure Sockets Layer und wurd für den sicheren Transport von Daten im Internet entwickelt. Konkret ist SSL ein Übertragungsprotokoll, mit dem verschlüsselte Kommunikation über das Internet möglich ist, wobei eine Reihe von kryptographischen Verschlüsselungsverfahren genutzt werden. Transport Layer Security (TLS), weitläufiger bekannt unter der Vorgängerbezeichnung SSL, ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.    4) Nur der Server kann die Zufallszahl Ze2 mit PK entschlüsseln  Masterkey wird aus den drei Daten Ze1 (unverschlüsselt), Ze2 (verschlüsselt) und den Zufallszahl ZS (unverschlüsselt) gewonnen. |
| Angriff auf PKI | Wenn es gelingt, das Zertifikat einer Zwischenzertifizierungstelle zu fälschen, kann man beliebige gültige Zertifikate erstellen, die zur Root – CA zurückverfolgt werden können.   * CA verwenden MD5 als Signaturhash * CA beglaubigt Zertifikate online * Seriennummer sind vorhersehbar   Das Zertifikat wird aus dem Antrag generiert, dem die Zertifizierungsstelle nur eine Seriennummer und einen Zeitstempel hinzugefügt. Nur der Hashwert des Zertifikat wird signiert. |
| Hash – Kollisionen | Da Hashwerte kürzer als die Eingabezeichenkette sind, gibt es je nach verwendeten Algorithmus eine gewisse Wahrscheinlichkeit gleicher Hashwerte. Die gleichen Hashwerte für unterschiedliche Eingabezeichenketten werden als Kollision bezeichnet. Beim Angriff wurde mehrere Zertifikate erzeugt durch die identischen MD5 Hashes. |
| Folgen des erfolgreichen Kollisionsangriffs (identischer Hash generieren) | * Phising Attacken durch gültige Server – Zertifikate * Man-in-the-Middle Attacken auf SSL – Verbindungen |
| Gegenmassnahmen | * SHA – 1 statt MD5 (Angeblich aber auch nicht mehr sicher 🡪 China) * OCSP (Online Certficate Status Protocol)   + Erlaubt Prüfung des Zertifikates auf Widerruf zur Laufzeit |
| SSL – Gau  (Comodo) | Iranische Hacker, haben sich gefälschte Sicherheitszertifikate verschafft. Mit diesen Zertifikaten wäre es möglich als eine bestimmte Website auszugeben. (login.yahoo.com / mail.google.com / addons.mozilla.com) 🡪 Phising Attacke  Desweiteren wird vermutet das die iranischen Hacker zugriff zu DNS Servern hatten, um DNS Adresse auf ihre Website mit den falschen Zertifikaten umzuleiten. Weiteres Problem die Abfragen via CRL und OCSP waren blockiert, somit mussten Updates über Browser eingeführt werden. |
| **Firewall Konzepte** | |
| Firewall | Eine Firewall (Brandmauer) ist ein Sicherungssystem, das ein Netzwerk oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt und ist weiter gefasst auch ein Teilaspekt eines Sicherheitskonzepts.   * Netzwerkkomponenten (Hard- und Software) an der Schnittstelle zweier Netze * Gewähren Einhaltung von Sicherheitsrichtlinien zwischen zwei Netzen * Entscheidung auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren Netzes aus dem privaten Netz heraus nutzbar sind * Wer hat Zugriff (Identifizieren und Authentifizieren) * Welche Protokolle * Logfile schreiben * Sicherheitsrichtlinie (Guideline) notwendig * Je weniger Besucher desto sicherer * Effizient dank Zentralisierung, alles muss über Firewall laufen (Flaschenhals) |
| Firewall Konzept | Damit effektiv Schutz geboten wird:   * Auf einer Sicherheitspolitik aufsetzen * Korrekt implementiert und konfiguriert * Korrekt administriert und überwacht * Regelmässig auditiert werden |
| Sicherheitsanforderungen | * **Zu schützende Ressource**: Daten, Rechnersysteme, Kommunikationssystem * **Zugangskontrolle auf Benutzer** (Authentisierung), Anwendungs- und Netzwerkebene (Authentifizierung) * **Verbergen** der internen Netzstruktur * **Vertraulichkeit** von Nachrichten * **Schutz gegen Angriffen**   + Auf Verfügbarkeit, z.B. Informationsserver   + Durch das Bekanntwerden von neuen sicherheitsrelevanten Softwareschwachstellen   + Gegen das Firewall – System selber * Behandlung von **sicherheitsrelevanten Ereignisse** (Reaktion auf Ereignisse, Proaktive Handlung) |
| Kommunikationsanforderungen | * **Verfügbarkeit** (wann...) * **Datendurchsatz** (wieviel...) * **Dienste und Anwendungen**   + Unterscheidung von internen und externen Nutzer   + Richtung der Dienste und Anwendungen   + Anforderungen wie Authentisierungsverfahren, Verschlüsselung, Protokoll * **Information**, welche (nicht) nach aussen gelangen darf * **Filterregeln** für die unteren Schichten (IP, ICMP, ARP, TCP und UDP) und für die Anwendungsschichten (SMTP, DNS, HTTP,...) * **Default Policy:** Alles ist verboten, was nicht erlaubt ist |
| **Firewall Generationen** | |
| Firewall der 1. Generation  Paketfilter  Grosses Problem stellen in diesem Zusammenhang Smartphones mit Tethering Funktion dar. Mit diesen lässt sich über das Mobilfunknetz eine Netzwerkverbindung zwischen den lokalen und dem Internet herstellen, welche von keiner Firewall erfasst wird. | Nur ein Paketfilter. Ein Paketfilter ist eine Software, die den ein- und ausgehenden Datenverkehr in einem Computernetz filtert. Dies dient in der Regel dem Schutz des Netzes vor Angreifern. Ebenso wichtig wie der Schutz gegen Angreifer von Aussen ist der Schutz gegen ungewollt ausgehende Pakete; damit kann man z.B. erschweren, dass der eigene Rechner ungewollt und unbemerkt Viren im Internet verbreitet.  Die Daten werden in einem Netz von dem sendenden Host in Datenpakete verpackt und versendet. Jedes Paket, das den Paketfilter passieren will, wird untersucht. Anhand der in jedem Paket vorhandenen Daten, wie Absender- und Empfänger Adressen, entscheidet der Paketfilter auf Grund von Filterregeln, was mit diesem Paket geschieht. Ein unzulässiges Paket, das den Filter nicht passieren darf, wird entweder verworfen (DENY oder DROP), an den Absender zurückgeschickt mit der Bemerkung, dass der Zugriff unzulässig war (REJECT), oder weitergeleitet (FORWARD oder PERMIT) beziehungweise durchgelassen (ALLOW oder PASS) wurde.   * Kennt nur Adressen * ALLOW und DROP (IP – Adresse) * Filterregeln pro Interface * Nur statisches Routing * Misslungene Versuche reinzukommen (Drops) werden protokolliert  |  |  | | --- | --- | | Vorteile | Nachteile | | Geringer Funktionsaufwand, hoher Durchsatz | Direkter Austausch von IP – Paketen zwischen den angeschlossenen Netzen, daher Angriffe auf Protokoll Stacks der beteiligten Rechner | | Geringe Kosten | Viele ständig offene Ports auf der externen Seite | | Fast jeder Service wird unterstützt (Ausnahme: Protokolle mit dynamischen Port) | Schwerer Überblick bei komplexen Anwendungen für Konfiguration | | Transparent für Endbenutzer | Keine Benutzer Authentisierung, Angriff durch IP – Spoofing | |  | Keine Inhaltskontrolle | |  | Protokollierung nur bis zum OSI Layer 4 möglich | |  | Adressverschleierung nur durch NAT möglich | |  | Offenheit für fast jedes Anwendungsprotokoll führt leicht zu „Quick and Dirty“ – Freischaltungen ohne Risikoanalyse und Policy Prüfung | |
| Firewall der 2. Generation  Circuit Level Proxies | * Generischer Proxy – Server für TCP und UDP * Keine möglichkeit protokollspezifische Regeln * UDP Relay bzw. TCP – Replay * Kennt Verbindung |
| Firewall der 3. Generation  Application Level Proxies | * Proxy – Prozess für ein spezielles Protokoll (z.B. HTTP – Proxy) * Für jedes Protokoll ein Proxy Prozess nötig * Inhaltsabhängige Regeln Contentfiltering („Was steht im Header?“) |
| Firewall der 4. Generation  Dynamische / Zustandsabhängiger Paketfilter  Stateful Paketfilter  Stateful Inspection Firewalls | * Zuordnung Anfrage zu Antwort nicht per se möglich * Für Zeitspanne t zusätzliche Allow – Regel anwenden (Welche Anfragen sind raus und wo kommt wieder was rein?) * Risiken: SIP – Protokoll 🡪 Internettelefonie, ist der hinter der Firewall erreichbar? Instant – Server   Ein Paketfilter heisst Statefull, wenn er für ein ausgehendes Paket automatisch eine Regel erzeugt, die in einem bestimmten Zeitfenster (im Minutenbereich) die Antwort auf dieses Paket akzeptiert. Kommt die Antwort nicht oder wird die Zeit überschritten, verfällt die Regel. Pronzipiell können solche Filter auch mit Protokollen umgehen, die auf zwei Ports arbeiten, zum Beispiel FTP.  Unter Stateful Packet Inspection (SPI), deutsche Bezeichnung „Zustandorientierte Paketüberprüfung“, versteht man eine dynamische Paketfiltertechnik, bei der jedes Datenpaket einer bestimmten aktiven Session zugeordnet wird. Die Datenpakete werden analysiert und der Verbindungsstatus wird in die Entscheidung einbezogen. Bei dieser Technik, die in Firewalls eingesetzt wird, werden die Datenpakete (Segmente) während der Übertragung auf der Transportschicht (4. Schicht des OSI) analysiert und in dynamischen Zustandtabellen gespeichert. Auf Basis des Zustands der Datenverbindungen werden die Entscheidungen für die Weiterleitung der Datenpakete getroffen. Datenpakete, die nicht bestimmten Kriterien zugeordnet werden können oder eventuell zu einer DoS Attacke gehören werden verworfen. |
| Application Level Gateway /  Proxy Firewall | Dieser Firewall Typ konzentriert seine Überwachungsfunktionen auf die Anwendungsebene. Für jedes behandelte Anwendungsprotokoll gibt es ein spezielles Prüfprogramm, Proxy (auch Relay oder Gate) genannt, das den Datenstrom dieser Anwendung genau analysiert. Daher wird dieser Typ auch als Proxy – Firewall bezeichnet. Ein Proxy überprüft auf jeden Fall die Einhaltung des Anwendungsprotokolls, für das er geschrieben wurde.   * Proxy heisst Bevollmächtigter 🡪 handelt nach innen oder aussen für Client * Kann auch Nutzdaten (nicht nur Header) in Analyse einbeziehen * Inhaltsbezogene Filterung 🡪 Hoher Aufwand * Anwender kommunizieren nicht mehr direkt mit Server sonder über Application Gateway      |  |  | | --- | --- | | Vorteile | Nachteile | | Protokollüberprüfung | Hohe Ressourcenbelastung | | Unterstützt Benutzer Identifizierung und – Authentifizierung | Hoher Entwicklungsaufwand | | Untersuchung auf Schadsoftware plus Einbindung von zusätzlichen Diensten (Virenscanner) | Jede Anwendung wird ein spezifischer Proxy benötigt | |
| Fragen zu Gateways | Unter welcher IP – Adresse sieht ein Webserver einen Client Browser, der via HTTP Proxy arbeitet? Vom Proxyserver / Gateway  Wie können Circuit Level Proxies für verschiedene Clients Verbindungen zu unterschiedlichen Zielen im Internet herstellen? NAT (Matchingtabelle, welcher Port greift wohin)  Transparente ALGs (Application Level Gateways) arbeiten von den Clients unbemerkt. Wieso kommen dann die Requests überhaupt zu ihnen? Es ist der Gateway wo es durchgeht.  Welche IP Adresse werden von transparenten ALGs ersetzt und welche nicht? Transparente ALG werden keine Adressen ersetzt. |
| Fazit Gateways |  |
| **Konfigurationsmanagement** | |
| 3 Varianten des Konfigurationsmanagements | * Turnschuh – Schnittstelle: (Direkt vor Ort konfigurieren): Praktisch, da mit Backup Konzept für Konfigurationsdaten koppelbar * Dedziertes Management – Netz: (Rote Leitung nur für Management (LAN)) Erfordert zusätzliche bauliche Massnahmen, hat aber den Vorteil, dass auch Authentisierungsmechanismen in die Regeln eingebaut werden können, ohne die dazu notwendigen Daten oder Verbindungen zusätzlichen Risiken auszusetzen.   + Physisch getrenntes Netz für die Firewall Administration   + Keine Administration über andere Netzwerkschnittstellen   + Zugriff auf Benutzer Datenbank zwecks Authentisierung und ind. Regeln * HTTPS oder SSH: Riskant – einschränken auf internes Interface und bestimmte Adressen |
| **Firewall Architekturen** | |
| Allgemein | * Position   + Firewall so weit draussen wie möglich   + Möglichst viele Rechner innen * Zweistufigkeit   + Zwei Filterstufen (eventuell mit unterschiedlicher Hard- und Software z.B. Paketfilter mit dual homed Application Gateway)   + Unterschiedliche Betriebssystem (nicht die gleichen Schwachpunkte durch die Hersteller der Software)   + Unterschiedliche Konfiguration der FW Regel (nicht die gleichen Fehelr bei der Formulierung der Regeln machen) |
| Nur ein Application Layer Gateway (ALG) | * Dual Homed Application Gateway * Bastion Host * Wann sinnvoll?   + Wenn alles dahinter die gleiche Sicherheitsstufe hat |
| Screened Subnet mit Single Homed ALG | Die Architektur führt eine Demulitarisierte Zone zwischen beiden Teilnetzen ein.   * Zwischen dem Internet und dem lokalen Netzwerk befindet sich ein weiteres Netzwerk, die DMZ, welche jeweils durch Paketfilter von den anderen beiden Netzen abgetrennt ist. * Möglichst alle Dienste, die aus dem Internet erreichtbar sein sollen, befinden sich in der DMZ. (Öffentliche Web-Server oder Mail-Server) * Dienste, welche aus dem Internet erreichbar sein sollen, aber im lokalen Netzwerk laufen (müssen), können nur über ein ALG in der DMZ erreicht werden. * Zusätzlich können Dienste aus dem lokalen Netze, welche für Dienste in der DMZ gebraucht werden, aus der DMZ aufgerufen werden. (Datenbank-Server für Web-Server) Damit ist keinerlei direkte Verbindung aus dem Internet ins lokale Netz möglich. |
| Screended Subnet mit Mutli Homed ALG |  |
| Name Server Splitting |  |
| Probleme aktive Inhalte | * Benutzerverantwortung (eingeschränkte Zulassung)   + JavaScript, Applets, FTP, verteilte Protokolle, Mail Attachments * Auf Proxy entsprechende Tags analysieren   + Schwierig bei komprimierter Übertragung   + Praktisch unmöglich bei verschlüsselten Inhalten * Auf Signaturen prüfen   + Erfordert aktuelle Signatur DB gefährlicher Inhalte |
| Verhalten bei Angriffen | 1. Erkennung (ungewöhnlicher Verbindungen, Zeiten, Änderungen,...) 2. Erste Bewertung der Schwere / Erste Reaktion festlegen    1. Ein / Mehrere Systeme? Schutzwürdigkeit?    2. Layer 1 Interrupt (Kabel ziehen) 3. Genauere Analyse (in Ruhe)    1. CERTs konsultieren (Ist allgemein was bekannt?) 4. Beweismittel sichern (Logfiles, gesamte Disk, ggf. signieren) 5. Wiederherstellung eines sicheren Zustundes inkl. Integritätsprüfung 6. Dokumentaion des Vorfalles und abschliessende Bewertung |
| Risiken und Grenzen | * Komplexität der Tools für die Firewall – Konfiguration * Kontinuierliche Administration mit Audits nötig: Kein eigentlicher Abschluss des Firewallprojekt * Firewall bieten keinen primären Schutz vor Malware * Mobile Geräte 🡪 BYOD * Umgehung des Single Point of Entry durch Modems oder WLAN * Hohe Verbreitung von Webservices ist eine Gefahr * Voice- oder Multimedia Applikationen, welche Ports freiprügeln (STUN) * Unübersichtlich grosse Applikationen mit diversen Features und Plug Ins * Zu wenig auf Sicherheits ausgelegtes Programmdesign |
| Tunneling | Wenn im Regelwerk der TCP Port 80 für HTTP freigeschaltet ist, kann darüber trotzdem ein anderes Protokoll laufen. Bettet die Software die zu übertragenden Daten also in HTTP ein, ohne dabei den Standard des Protokoll zu verletzen, ist auch diese Firewall dagegen machtlos. (Teamviewer, Skype) Tunnel werden auch verwendet, um unsichere Netzwerkprotokolle mithilfe eines gesicherten und verschlüsselten Netzwerkprotokoll abhör- und manipulationssicher zu transportieren (SSH, VPN).  Lösung dafür: Logs lesen |
| Ausblick | * Zunahme der Datenübertagungsrate   + Begrenzte Parallelisierung (Höherer Aufwand durch Konfiguration)   + Paketfilter ≈1000 Mbps, ALG≈500 Mbps * Verschlüsselung   + Mailverschlüsselung macht Inhaltsfilterung unmöglich * Endgerätsicherheit * Einbezug der Anwender   + Eigenverantwortung hat zentrale Bedeutung   + Ubuquitous Computing (Smart Devices) |
| **Hacking** | |
| **Begriffe** | |
| Hacking  Friendly Hacker | Exzellente Programmier mit aussergewöhnlichen Kenntnisse der Hard- und Software. (z.B. Computersysteme verbessern, optimieren oder schützen, indem neue Wege beschritten werden) |
| Cracker | Besitzt oft dieselbe Fähigkeiten wie Hacker, setzen diese aber in böswillige Absichten ein (z.B. unberechtigte Systemzugriffe und Passwörter um cracken) |
| Weitere Typen | * Ethische Hacker (Rechtskonform / firmenintern / forensisch) * Script Kiddies (Können nicht abschätzen wie gross der Schaden wird) * Phreaks („Phone Freaks“, Manipulation von Telefonverbindungen) * Whitehats (Fachleute, Hinweise nur an Hersteller) * Greyhats (Generelle Offenlegung von Sicherheitslücken 🡪 Exploits) * Blackhats (Illegal, Straftaten, Publizieren Exploits, Entwickeln Trojaner) |
| Organisation | * Meistens in Gruppen * Gut organisiert durch IRC Kanäle * Gruppenanlässe (DefCon, Blackhat Briefings, Chaos Communication Congress) |
| **Sicherheit von Wireless** | |
| Es gibt sichere WLANs | * Impementation nur mit aktueller Sicherheitstechnologie   + PKI   + Sichere kryptographische Protokolle (Fehlerfrei implementier) * Verzeichnisdienst zur Verwaltung   + Benutzer   + Zertifikate   + Zugriffsrichtlinien * Autorisierungsdienst   + Abgestimmt auf Verzeichnisdienst |
| **WEP (Wired Equivalent Privacy)** | |
| WEP | WEP ist das ehemalige Standard – Verschlüsselungsprotokoll für WLAN. Es sollte sowohl den Zugang zum Netz regeln (Authentifzierung), als auch die Vertraulichkeit und Integrität der Daten sicherstellen. Aufgrund verschiedener Schwachstellen gilt das Verfahren als unsicher. Die Berechnung des Schlüssels aus einigen Minuten an aufgeziechneten Daten dauert normalerweise nur wenige Sekunden. Daher sollten WLAN – Installationen die sicherere WPA2 – Verschlüsselung verwenden. |
| Probleme | * WEP – Key bleibt gleich * Initialization Vector ist zu klein (Zufallszahl mit dem man startet, können nur 16777216 Schlüssel erstellen) * CRC 32 ungeeignet |
| **WPA (Wireless Protected Access)** | |
| WPA | WPA ist eine Verschlüsselungsmethode für ein Drahtlosnetzwerk. Der Nachfolger ist WPA2. WPA enthält die Architektur von WEP, bringt jedoch zusätzlich Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren und bietet zur Authentifizierung von Teilnehmer Pre-shared key (PSK) oder Extensible Authentication (EAP) über IEEE 802.1X an. |
| Probleme | * Angriff auf Preshared Key (Ein einziger Passwort für alle) * Schlüssel ändert sich ständig |
| **WPA2 (Wireless Protected Access 2)** | |
| WPA2 | WPA2 ist die Implementierung eines Sicherheitsstandards für Funktnetzwerke nach den WLAN Standard IEEE 802.11 a,b,g und n und basiert auf dem Advanced Encryption Standard (AES).   * Nicht mehr nur ein einziger Preshared Key * Benutzer Credentials beim Aufbau der verschlüsselten Verbindung 🡪 Individueller Schlüssel * Kein Abhören der Nachbarstation im gleichen Netz mehr möglich |
|  | 1. Der WLAN Client muss dem Authentifizierungsdienst seine Anmeldeinformationen bereitstellen, bevor der Zugriff auf das WLAN erfolgen kann. 2. Wenn sich der Client im Empfangsbereich des WLAN – Access Point befindet, verscuht er eine Verbindung zu dem WLAN herzustellen, das an diesem Zugriffspunkt aktiv ist. Das WLAN wird über seine SSID (Service Set ID) identifiziert. Der Client erkennt die WLAN – SSID und bestimmt anhand dieser SSID, welche Einstellung und welcher Typ von Anmeldeinformationen für dieses WLAN zu verwenden ist. 3. Der RADIUS Server gleicht die Anmeldeinformationen des Clients mit dem Verzeichnis ab. Bei erfolgreicher Authentifizierung des Clients stellt der RADIUS – Server Informationen zusammen, anhand derer er entscheiden kann, ob der Client für die Nutzung des WLANs autorisiert werden kann. 4. Wenn dem Client der Zugriff gewährt wird, sendet der RADIUS – Server den Clienthauptschlüssel an den WLAN – Access Point. Der Client und der WLAN – Access Point verfügen jetzt über gemeinsame Schlüssel, mit denen sie den gegenseitigen WLAN Verkehr ver- bzw. entschlüsseln können 5. Der Access Point stellt dann die Client WLAN – Verbindung zum internen LAN her, so dass der Client uneingeschränkt auf die Systeme im internen Netzwerk zugreifen kann, Der Verkehr, der zwischen dem Client und dem Access Point gesendet wird, ist nun verschlüsselt. 6. Falls der Client eine IP – Adresse benötigt, kann er jetzt einen DHCP – Lease (Dynamic Host Configuration Protocol) von einem Server auf dem LAN anfordern. Sobald die IP – Adresse zugewiesen wurde, kann der Client normal mit Systemen im übrigen Netzwerk kommunizieren. |
| Gegenüberstellung WPA und WPA 2 |  |
| 802.1X | Am Netzwerkzugang, einem physischen Port im LAN, einem logischen IEEE 802.1Q VLAN oder einem WLAN, erfolgt die Authentifizierung eines Teilnehmers durch den Authenticator, der mittels eines Authentifizierungsservers (RADIUS – Server) die durch den Teilnehmer (Supplikant) übermittelten Authentifizierungsinformationen prüft und gegebenenfalls den Zugriff auf die durch den Authenticator angebotenen Dienste (LAN, VLAN oder WLAN) zulässt oder abweist. |
| Temporal Key Integrity Protocol – TKIP | TKIP wurde entwickelt um WEP zu ersetzen ohne dass neue bzw. zusätzliche Anforderungen an die Hardware gestellt wurden. |
| Counter – Mode / CBC – Mac Protocol - CCMP | Es wird ein 128 Bit starker Schlüssel mit 48 Bit starken Intialisierungsvektor verwendet |
| MIC | Die Datenpakete werden fortlaufen durchnummeriert. Diese laufende Nummer wird im verschlüsselten Teil mitübertragen. Beim Empfänger wird auf die laufende Nummer geprüft und Pakete, die nicht zu dieser laufenden Nummer passen, werden ohne weitere Bearbeitung verworfen. |
| Was ist Beaconing und was bedeutet Vulnerability (Angreifbarkeit)? | Der Infrastruktur – Modus ähnelt im Aufbau dem Mobilfunknetz. Ein Wireless Access Point oder ein drahtloser Router übernimmt die Koordination aller Clients und sendet in einstellbaren Intervallen kleine Datenpakete, sogenannte Beacons (Leuchtfeuer), an alle Stationen im Empfangsbereich. Die Beacons enthalten unter anderem folgende Informationen.   * Netzwerkname (SSID) * Liste unterstützeter Übertragungsraten * Art der Verschlüsselung   Dient zur Erkennung des Access Point. Software zur Suche nach ESSID gibt es. |
| Unterschied Authentication und Association? | Authentifizierung ist der Nachweis (Verifizierung) einer behaupteten Eigenschaft einer Entität, die beispielsweise ein Mensch, ein Gerät, ein Dokument oder eine Information sein kann, und die durch beispielsweise mit Login und Passwort.  Eine Assoziation ist eine physische Verbindung (Übergabe) von Access Point zu Access Point. |
| Bedeutung des Monitor Mode einer WLAN Karte. | Monitormodus bezeichnet einen bestimmten Betriebsmodus eines Wireless Adapters, bei dem sämtliche empfangenen Netzwerkframes an das Betriebssystem und die Anwendungen weitergeleitet werden. (Password Sniffing) |
| **Steganographie und DRM** | |
| Steganographie | Die Steganographie ist die Kunst oder Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium (Container). Beispielsweise in einem Bild. |
| **Digital Rights Management (DRM)** | |
| DRM | DRM bezeichnet Verfahren, mit denen die Nutzung (und Verbreitung) digitaler Medien kontrolliert werden soll. Vor allem bei digitalen vorliegenden Film- und Tonaufnahmen, aber auch bei Software, elektronischen Dokumenten oder elektronischen Bücher findet die digitale Nutzungsverwaltung Verwendung. Sie ermöglicht aus Sicht von Anbietern, die solche DRM – Systeme zur Nutzungskontrolle ihrer Daten einsetzen, prinzipiell neue Abrechnungsmöglichkeiten, um beispielsweise mittels Lizenzen und Berechtigungen sich Nutzungsrechte an Daten, anstatt die Daten selbst, vergüten zu lassen. Andersherum wird dies aus Sicht von Endnutzern oft als Beschränkung gesehen. |
| Hartes DRM | * Mit technischen Massnahmen durchgestetzt (Verschlüsselung, proprietäre Formate,..) * Erfordert SW – Installationen oder sogar spezielle Hardware zur Nutzung des geschützten Werkes * Missbrauch verhindern (Präventiver Ansatz, von Beginn an Schutz geben) |
| Weiches DRM | * Die Nachteile des harten DRM sollen vermindert werden 🡪 weitgehende Unabhängigkeit von SW oder Hardware * Sozialer Kopierschutz, der erst bei offensichtlichem Missbrauch greifen soll (Repressiver Ansatz) * Weniger Aufwand   + Digitale Signaturen / Wasserzeichen   + Hash – Wert     Individueller Schlüssel, welcher Aufschlüsse vom Anwender integriert. 🡪 Tracking Weitergabe wird nicht eingeschränkt aber die Verfolgbarkeit (Strafrechtlich). Nur wer Schaden anrichtet mach mehr Aufwand.   * Markierung URG – geschützter Werke * Erlaubt Tracking, ohne technische Nutzungsbeschränkung * Alternative zum Kopierschutz |
| Personalisierung satt Kopierschutz  Statt sie mit einem aufwändigen Kopierschutz zu versehen, werden die URG – Werke durch CoSee markiert. Die Markierung erfolgt pseudonym 🡪 Zurückverfolgung wer den Schaden angerichtet hat. Anonym kann keine Rückschlüsse ziehen. |  |
| **Authentisierung und Biometrie** | |
| Identifikation vs. Verifikation | Identifikation („one – to – many“) Das biometrische System vergleicht die Person mit vielen Personen, die in einer Datenbank bereits gespeichert sind. Diese Methode wird bei einer Anwendung einer grossen Menge an Daten bevorzugt aufgrund der zunehmenden Wahrscheinlichkeit von Fehlern.  Verifikation („one – to – one“) Das biometrische System vergleicht die Person nur mit der gespeicherten Datei, die mit dieser Person identifiziert werden kann bzw. übereinstimmt. Die Person präsentiert nicht irgendein biometrisches Beispiel (Was bist du) oder ein Passwort (Was weißt du) oder eine Smartcard (Was hast du), sondern eine spezifische Individualität. |
| Authentisierung vs. Authentifizierung | Der Benutzer authentisiert (Beweis) sich am Server mit seinem Passwort. Nur wenn der Benutzer dem System bekannt ist, wird der Benutzer vom Server authentifiziert (also als gültiger Benutzer erkannt, Verifikation). |
| Passwortverfahren | * Social Engineering beachten * Lock out bei Fehlversuchen * Verschlüsselung, Hash und Salt |
| Challenge Response Verfahren | Hierbei stellt ein Teilnehmer eine Aufgabe, die der andere lösen muss, um zu beweisen, dass er eine bestimmte Information kennt, ohne diese Information selber zu übertragen. |
| Zero Knowledge Verfahren | Dabei hat einer von zwei miteinander Kommunizierenden, der Beweiser, Kenntnis von einem Geheimnis und überzeugt den Kommunikationspartner, den Verifizierer, mit Teilinformationen, dass er das Geheimnis kennt. |
| Grundlegende Authentifizierungsarten | * Biometrie (Wer ich bin) * Geheimes Wissen (Was ich weiss) * Persönlicher Besitz (Was ich habe)   Aus Sicherheitsgründen ist es oft üblich, zwei oder drei der genannten Verfahren zu kombinieren. |
| Elliptic Curve Cryptography - ECC | Bei der ECC handelt es sich um eine asymmetrische Verschlüsselung. Der Vorteil beim Einsatz von ECC liegt in der schnellen Verschlüsselung und der grösseren Flexibilität. Ohne Abstriche hinsichtlich der Sicherheit in Kauf zu nehmen, kommt man mit deutlich geringeren Parameterlängen aus. Dies wirkt sich besonders beim Einsatz in Situationen aus, wo Speicher- oder Rechenkapazität knapp sind, wie z.B. Smartcards.   1. Alice und Bob einigen sich auf eine elliptische Kurve (= wählen öffentliche bekannte Parameter a,b,p) 2. Alice und Bob einigen sich auf einen öffentlichen Punkt P auf der Kurve (Public Key) 3. Beide wählen (geheime) ganze Zahlen ak und bk (Private Key) 4. Alice berechnet Ak = ak\*P und veröffentlicht dies 5. Bob berechnet Bk = bk\*P und veröffentlicht dies 6. Alice berechnet ak\*Bk, Bob berechnet bk\*Ak 7. Beide kennen nun akBk = ak(bkP) = bk(akP) = bkAk und können dies für z.B. klassische Verschlüsselung via AES benutzen |
| Sicherheit | Ein Teil der Transaktionsdaten wird über einen zweiten Kanal übermittelt und bestätigt. Dieser 2. Kanal ist vom klassischen Phisher nicht kontrollierbar. (Man-in-the-Middel Attacke) |
| Biometrische Merkmale | Fingerabdruck, Iris, Gesicht, Hand, Stimme, Retina, Schrift, Tastenanschläge  Anforderungen:   * Universalität * Eindeutigkeit * Beständigkeit (Keine Abnützung) * Performanz (Präzision und Geschwindigkeit) * Akzeptanz * Fälschungssicher |
| Abgleich von Referenzwerten | Falschakzeptanzrate (FAR): Die FAR ist die Häufigkeit, mit der nichtberechtigte Personen als berechtigt akzeptiert werden. Da eine falsche Akzeptanz in der Regel zu Schäden führt, ist die FAR ein sicherheitsrelevantes Mass.  Falschrückweisungsrate (FRR): Die FRR ist die Häufigkeit, mit der berechtigte Personen unberechtigterweise zurückgewissen werden. Die FRR ist in der Reel ein Kofortmerkmal, da falsche Abweichungen vor allem lästig sind.  Gleichfehlerrate (ERR): ist die Fehlerrate, die in der Einstellung erreicht wird, in der FAR und FRR gleich sind. Wird als aussagekräftiges Mass für die Güte eines biometrischen System angesehen. |