Zusammenfassung - NASS

SK

14. Januar 2016

> Korrektheit und Vollständigkeit der Informationen wird nicht gewährleistet.

Inhaltsverzeichnis

1 Introduction

1.1 Taxonomie der Angreifer

- einzelner Angreifer
  - sozialer Hintergrund
  - öffentliche Aufmerksamkeit als Antrieb
  - evtl pol. Statements
  - geht gewöhnlich niedrige Risiken ein
- organisierte Kriminalität
  - Geld als Antrieb
  - mittlere Risiken
- Terroristen
  - politische oder gesellschaftliche Motivation
  - hohe Risiken
  - Zerstörung/Verwirrung als Ziel
- Konkurrenten
  - möglichst niedriges Risiko der Aufdeckung(abhängig vom wert der Information)
  - Informationsdiebstahl oder Zerstörung als Ziel
- Regierungsorganisationen
  - Industriespionage zum Wohl einheimischer Firmen
  - Militärspionage udn hybride Kriegsführung

1.2 Angriffe gegen einen Computer

Informationsdiebstahl führt zu:

- Wettbewerbsvorteilen
- Verwirrung
- Erpressung

Zerstörung führt zu:

- Spaß und Selbstverherrlichung
- Politischen Stellungnahmen

Sammlung von Informationen

- Infos werden zu Angreifer gesendet
- an Netzwerk angeschlossene Rechner mit höherem Risiko
- Zugriff für Angreifer durch:
  - Social engineering
  - Viren/Trojaner/Würmer
  - Physischer Diebstahl von Datenträgern
  - Sniffing

Zerstörung von Infos

- Infos gehen verloren
- physische Angriffe/Feuer/Naturkatastrophen
- Beabsichtigte Löschungen durch
  - Social Engineering
  - Viren/Trojaner/Würmer

Viren

- Infektion von Dateien
- Infektion von System und Boot record
- Zerstörung, Verwirrung und öffentliche Aufmerksamkeit als Ziel

Würmer

- Mailing Worms - Verbreitung durch E-Mails
- Viren/Trojaner evtl als „Nutzlast“
- Network worms - Verbreitung durch Ausnutzung von Softwaremängeln(bspw Bufferoverflows)
- Ablauf:
  - Zielauswahl
  - ausnutzen(exploit)
  - Infektion
  - Verbreitung

Backdoors und Trojaner

- Schadsoftware wird in nützlicher Software versteckt
- mögliche Funktionen:
  - mitschneiden von Daten(logging)

  - Zerstörung
  - Installation weiterer Software(DoS Clients, root kits etc)
  - bedingter Start von Prozessen (time bombs)

Identitäts Spoofing

- Angreifer übernimmt die Identität von jemand anderem
- Angreifer und Ziel müssne normalerweise ein Netzsegment teilen
- Angreifer liefert evtl falsche Infos über Routen oder Namen
- Grundsätzlich sind alle Antworten eines Protokolls potentielle Spoofingsubjekte(subject of spoofing?)

DoS

- Angreifer möchte einen Dienst der von einem Rechner oder Gerät angeboten wird überladen
- Angriffe gegen Konkurrenten, als pol/gesellschaftliche Aussage oder um andere Aktivitäten zu verbergen
- bösartige Anfragen sind nicht von normalen Anfragen zu unterscheiden
- BSP: HTTP, DNS DoS, SYN Flooding

Bot Network

- Fernsteuerung mehrerer Rechner um bösartige Aktionen auszuführen
- bsp: DDoS, aufwändige Entschlüsselungen berechnen

Password/Schlüssel Attacken

- Brute Force
- Raten/ Wörterbuchangriffe
- Mängel in der Implementation(z.B. Password als Klartext gespeichert)

Port/Network Scanning

- während der Aufklärungsphase um Sicherheitslücken und geeignete Ziele zu finden
- Angreifer möchte Informationen über das System erlangen
- Sniffing/Mapping/Port Scans

Session Highjacking

- Angreifer bricht in einen bestehender Session ein ohne sich einloggen zu müssen.

ZSF: viele unterschiedliche Angriffsmöglichkeiten $\Rightarrow$ $unüberschaubare Anzahl anverschiedenen Attacken Angreifer unters$

2 Einführung und Rekapitulation

2.1 Sicherheitskomponenten

- Firewalls
- Intrusion Detection/Prevention Systems
- Proxies
- interne oder private Netzwerke / Netzwerkzonen / Entmilitarisierte Zonen
- VPNs

2.2 Firewalls

entscheidet ob Verkehr ins Netzwerk gelangen darf oder nicht Typen:

- Paketfilter
- Zustandsbehaftete Firewall
- Proxyfirewall

2.3 Intrusion Detection Systems

Identifizierung von Attacken / verdächtigem Verkehr
Hilfe beim Einrichten/ konfigurieren von Firewalls
Normalerweise transparent für Nutzer und Angreifer.
hauptsächlich 2 Arten:

- Mustererkennung
- Anomalieerkennung

2.4 Proxies

strickte Trennung von internen und externen Netz
Üblicherweise auf Application Layer. Verhindert dass bestimmte Informationen(Viren, Pornos, illegale Infos) in das interne Netz gesandt werden.
Verhindert, dass bestimmte Informationen nach außen gesendet werden.
Kombinationen mit anderen Systemen(Virenfilter/ Spamfilter / IDS...)

2.5 VPN

VPNs erschaffen einen gemeinsamen Addressraum.
VPNs schützen die Kommunikation über ungesicherte Netzwerke als würde sie in einem Netzwerk stattfinden.
Gegenseitige Authentifizierung der Kommunikationspartner.
VPNs bieten signifikante Einsparungen über dedizierte Verbindungen.

2.6 Zonen - DMZ

kleine Netzwerke, welche öffentlich erreichbare Dienste beeinhalten (z.B. HTTP)
DMZ oft durch Firewalls etc geschützt.
DMZ befinden sich außerhalb des internen Netzes.
sind unsicherer als das interne Netz.
Abgeschirmte Teilnetze sind isolierte Netze innerhalb des internen Netzes

2.7 internes Netz

eingeschränkter Zugriff auf das externe Netz nur über gut bekannte Ports
Internes Angriffsrisiko hängt ab von:

- Anzahl der Nutzer
- Vertrauen in die Nutzer
- Zugriffswege der Nutzer(Notebooks?)
- Fähigkeiten der Nutzer

Hosts müssen trotzdem noch mit firewalls etc geschützt werden

2.8 Basis Kryptografie

Kerkhoff's Prinzip: Sicherheit hängt nur von Schlüssel ab und nicht von der Kenntnis der kryptografischen Funktion.

2.8.1 symmetrische Verschlüsselung

Beide Teilnehmer benutzen zum ver- und entschlüsseln denselben Schlüssel.
Stromchiffren: Klartext wird Zeichen für Zeichen ver- und entschlüsselt.
Blockchiffren: arbeitet mit festen Blockgrößen und entschlüsselt mehrere Zeichen in einem Schritt.

One-Time Pads Stromchiffre deren Schlüsselstrom ein Strom aus echten Zufallsbits ist
Uneingeschränkt sicher(einziges bisher „bewiesen“ sicheres Verfahren).
Schlüssel muss zu verschlüsseln mindestens so lang sein wie der Klartext.
Jeder Schlüssel darf nur einmal verwendet werden.
Nachteil: viel Speicherbedarf für Schlüssel.

2.8.2 asymmetrische Verschlüsselung

Sender und Empfänger nutzen jeweils unterschiedliche Schlüssel.
Es ist schwierig den Entschlüsselungsschlüssel(k') aus dem Verschlüsselungsschlüsselungsschlüssel(k) zu berechnen
k kann öffentlich gemacht werden (public-key-Verschlüsselung).
Nachteil: Verteilung der Schlüssel

2.8.3 hybride Verschlüsselung

Kombination aus symmetrischer udn asymmetrischer Verschlüsselung.
symmetrischer Session Key mit dem die Daten symmetrisch verschlüsselt werden.
Session Key wird asymmetrisch mit public Key des Empfängers verschlüsselt.
löst Verteilungsproblem der asymmetrischen und behält Geschwidigkeit der symmetrischen Verschlüsselung

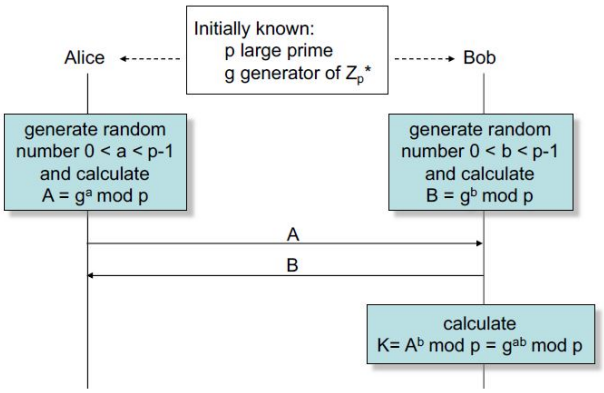
2.8.4 kryptografische Hashfunktion

Anforderungen:

- einseitig: wenn Hashwert y gegeben ist, ist es rechnerisch unmöglich eine Nachricht x zu finden, sodass $h(x) = y$
- schwacher Kollisionswiderstand: bei gegebener Nachricht ist es rechnerisch unmöglich eine andere Nachricht mit gleichem Hashwert zu finden
- starker Kollisionwiderstand: Es is rechnerisch unmöglich zwei Nachrichten mit gleichem Hashwert zu finden.

Hash und Signaturen Von Nachricht wird Hash gebildet. Dieser wird verschlüsselt und als Signatur an die Nachricht gehängt.
Empfänger entschlüsselt Signatur mit public key des Senders und vergleicht mit dem hash der Nachricht. Wenn gleich dann ist alles gut, wenn nicht dann wurde was verändert.

2.8.5 Diffie-Hellman Schlüsselaustausch



2.8.6 Zertifikate

Zertifikat ist eine Datenstruktur welche folgendes enthält:

- Öffentlichen Schlüssel
- Namen des Eigentümers des öff Schlüssels
- Namen des Ausstellers
- Ausstellungsdatum
- Ablaufdatum
- Möglicherweise andere Daten
- Signatur des Ausstellers

2.8.7 Certification Authorities (CA)

stellen Zertifikate aus.
sind normalerweise vertrauenswürdige Dritte.
Zertifikate werden über online Datenbanken verteilt(Certificate Directories) denen vertraut werden muss.

3 Paketfilter

3.1 Funktionsweise von Paketfiltern

Netzwerkpakete werden akzeptiert oder zurückgewiesen anhand von Parametern wie:

- Quelladresse/Ports
- Zieladresse/Ports
- Flags

3.2 Paketfilterregeln

Regeln können bzgl Flags, Adressen und Ports angewandt werden.
Paketfilter können auch bezüglich des Inhaltes von Paketen angewandt werden.
Zulassende Regeln:

- explizites Erlauben von Zugriff
- sämtlicher anderer Verkehr wird verhindert

Verhindernde/ablehnende Regeln:

- bestimmter Verkehr wird explizit abgelehnt.
- sämtlicher anderer Verkehr wird für gewöhnlich zugelassen.

Wichtig:

- Reihenfolge der Regeln ist wichtig.(erst alles verhindern und dann einige zulassen ist was anderes als erst einige zulassen und dann alles zu verhindern!)
- große Anzahl an Regeln kann verwirrend sein.
- „alles verbieten und solange es nicht explizit benötigt wird“ kann gute Herangehensweise sein.

3.2.1 Ingress-Filter

Filtern ankommende Pakete
blockieren Zugriff von verdächtigen Quelladdressen.

3.2.2 Egress-Filter

Filtern ausgehenden Verkehr.
Nur Pakete mit Quelladdresse im Netzwerk dürfen das Netzwerk verlassen so lange keine andere Regel greift.
Quellen von abgewiesenen Paketen sind gute Kandidaten für Überprüfung.

3.2.3 Protokollfilter

Dienste haben haben festgelegte Protokolle
Daumenregel: nur Verkehr zu Diensten zulassen die wirklich benötigt werden.

3.2.4 Probleme

Zugriff für bestimmte Netze zulassen
Gefahr des Spoofings: Angreifer nutzt evtl falsche Quelladressen
Source Routing:

- Pakete enthalten evtl Infos über die Route zurück zum Urheber
- Überschreiben die Routingtabelle des Routers

Gefahr das Filterregeln umgangen werden
Fragmentierung:

- Paketfilter untersuchen Headerinfos
- Paket wird so aufgeteilt dass der Header geteilt wird und Adresse und Ports nicht gefiltert werden können.

Löcher:

- Dienste müssen erreichbar bleiben für externe Netzwerke
- entsprechende Ports müssen geöffnet werden.

3.3 dynamische Paketfilter

Filterregeln werden on the fly so erstellt wie sie benötigt werden und nach schließen der Verbindung wieder gelöscht.
Filter beobachten ausgehenden Verkehr und erstellen zurückwirkende Regeln.(Ausgehender Verkehr zu einer Adresse bewirkt Regel dass eingehender Verkehr von dieser Adresse erlaubt wird.)
Probleme:

- Regeln sind angreifbar z.B. durch senden falscher reset Pakete
- ausgehender Verkehr wird nicht gefiltert. Gefahr von Trojanern/Viren.

4 Zustandsbehaftete Fierwalls

4.1 Funktionsweise

Kennen den Zustand von Verbindungen und wissen welche Pakete in welchem Zustand erwartet werden.
Es können Regeln angewandt werden die nur in bestimmten Zuständen wirksam sind.
Untersuchen hauptsächlich OSI 4 (transport layer), aber auch höhere Schichten.

4.2 Probleme

Hohe Leistung benötigt teilweise geclusterte Hardware. Zustandsbehaftete Firewalls lassen sich nicht einfach clustern.
Zustandslose Protokolle (UDP, ICMP, DNS, HTTP)

4.2.1 Zustandslose Protokolle

Zustandslose Protokolle definieren trotdem welche Pakete erwartet werden.
Timeouts werden genutzt um Pseudo-Verbindungen zu erzeugen.

4.3 Multi-Layer Inspection

Die meisten Protokolle basieren auf Protokollen aus niedrigeren Layern. BSP: HTTP nutzt TCP Verbindungen.
Zustandsbehaftete Firewalls können beide Layer beobachten.