Angriffe im Internet

Roland Büschkes, T-Mobile Deutschland GmbH

T · · Mobile ·

Angriffe im Internet
Übersicht

Teil 1: IT-Sicherheitsmanagement

1. Grundlagen
2. Ziele, Strategien und Policies
3. Prozesse
4. Wechselwirkungen
5. Schutzziele
6. Durchsetzung von Schutzzielen

Teil 2: Angriffe

1. Zielauswahl
2. Informationssammlung
3. Angriff
4. Systemmodifikation
5. Spurenbeseitigung

Teil 3: Klassifikation von Angriffen

1. Transaktionen
2. Transaktionsbasierte Klassifikation von Angriffen
3. Transaktionen und Kommunikationsmodelle

Teil 4: Angriffserkennung (Exkurs)

1. Grundtechniken
2. Transaktionsbasierte Anomalieerkennung

Teil 5: Fazit

1. Zusammenfassung
2. Ausblick

T · · Mobile ·

Angriffe im Internet
Teil 1

IT-Sicherheitsmanagement

T Mobile

Angriffe im Internet

IT-Sicherheitsmanagement

- Systematisches Vorgehen für die Identifizierung der Anforderungen an IT-Sicherheit sowie für die Implementierung von IT-Sicherheit und ihre fortlaufende Verwaltung in einer Organisation erforderlich
- Prozess wird als IT-Sicherheitsmanagement bezeichnet und umfasst:
  - Entwicklung einer IT-Security-Policy
  - Identifizieren von Zuständigkeiten und Verantwortlichkeiten in der Organisation
  - Risikomanagement, einschließlich der Identifizierung und Beurteilung von:
    - Werten
    - Bedrohungen
    - Schwachstellen
    - Auswirkungen
    - Risiken
    - Schutzmaßnahmen
    - Restrisiken
    - Zwängen

T · · Mobile

Angriffe im Internet

IT-Sicherheitsmanagement

- Konfigurationsmanagement
- Änderungsverwaltung
- Pläne für den Katastrophenfall
- Auswahl und Umsetzung von Schutzmaßnahmen
- Laufende Kontrolle unter Einbeziehung von
  - Wartung
  - Sicherheits-Audits
  - Überwachen
  - Begutachten von Vorfällen
  - Behandeln von Vorfällen

T · · Mobile

Angriffe im Internet

Ziele, Strategien und Policies

- Formulierung von organisationsweiten Sicherheitszielen, -strategien und -Policies notwendig, die die Geschäftsvorgänge einer Organisation unterstützen und gemeinsam die Übereinstimmung aller Sicherheitsmaßnahmen gewährleisten:
  - Ziele: Was soll erreicht werden?
  - Strategien: Wie sind diese Ziele zu erreichen?
  - Policies: Was muss getan werden?
- Organisationsweite Security-Policy
  - Sicherheitsprinzipien und -richtlinien für die gesamte Organisation
- Organisationsweite IT-Security-Policy
  - Spiegelt die wesentlichen Sicherheitsprinzipien und -richtlinien, die für die organisationsweite Security-Policy zutreffen, und die allgemeine Nutzung von IT-Systemen wider
- IT-System-Security-Policy
  - Details zu speziellen Sicherheitsanforderungen und Schutzmaßnahmen sowie Details zur richtigen Benutzung

T · · Mobile

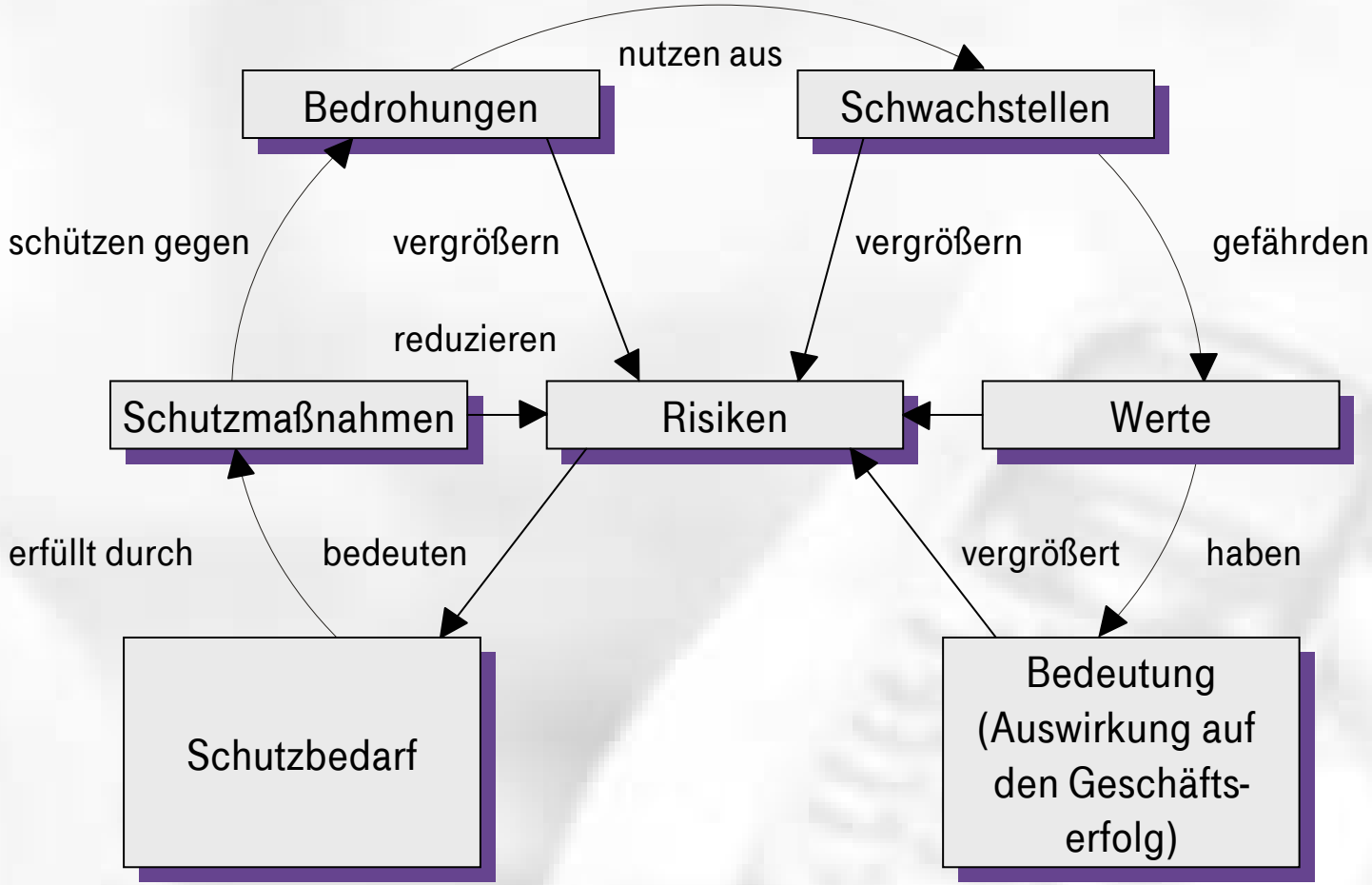
Prozesse für das Sicherheitsmanagement

1. Konfigurationsmanagement
   - Prozess zur Verfolgung von Änderungen am System
   - Änderungen am System dürfen nicht die Wirksamkeit von Schutzmaßnahmen und die Gesamtsicherheit der Organisation verringern
2. Änderungsverwaltung
   - Prozess zur Identifizierung neuer Sicherheitsanforderungen, falls Änderungen des IT-Systems eintreten
3. Risikomanagement
   - Prozess zum Vergleich von abgeschätzten Risiken mit dem Nutzen und/oder den Kosten für Schutzmaßnahmen sowie zur Herleitung einer Implementierungsstrategie und System-Security-Policy
4. Risikoanalyse
   - Prozess zur Identifizierung von Risiken, die unter Kontrolle gehalten oder hingenommen werden müssen

Prozesse für das Sicherheitsmanagement

5. Zurechenbarkeit
   - Klare Zuordnung und Anerkennung von Sicherheitsverantwortlichkeiten
6. Sicherheitsbewusstsein
   - Wirksames Programm für ein Sicherheitsbewusstsein in einer Organisation notwendig, da Einzelpersonen in einer Organisation allgemein als schwächstes Sicherheitsglied anzusehen sind
7. Überwachung
   - Einsatz von Schutzmaßnahmen sollte überwacht werden, um sicherzustellen, dass sie richtig funktionieren, dass Änderungen im Umfeld sie nicht wirkungslos gemacht haben und dass die Zurechenbarkeit durchgesetzt wird
8. Pläne für den Katastrophenfall
   - Pläne für unvorhersehbare Zwischenfälle enthalten Informationen darüber, wie die Geschäftsabläufe zu handhaben sind, wenn die unterstützenden Prozesse einschließlich des IT-Systems verlangsamt oder nicht verfügbar sind

Wechselwirkungen beim Risikomanagement



T-Mobile

Angriffe im Internet

Schutzziele

- Klassische Schutzziele (CIA-Eigenschaften):
  1. Vertraulichkeit (engl. Confidentiality)
     - Schutz vor unbefugtem Informationsgewinn
  2. Integrität (engl. Integrity)
     - Schutz vor der unbefugten Modifikation von Informationen
  3. Verfügbarkeit (engl. Availability)
     - Schutz vor dem Verlust der Verfügbarkeit

T · · Mobile

Angriffe im Internet

Schutzziele für Kommunikationsnetze

1. Vertraulichkeit
   - Nachrichteninhalte sollen vor allen Instanzen außer dem Kommunikationspartner vertraulich bleiben.
   - Sender und/oder Empfänger von Nachrichten sollen voreinander anonym bleiben und durch Unbeteiligte (inkl. Netzbetreiber) nicht beobachtet werden.
2. Integrität
   - Fälschungen von Nachrichteninhalten (inkl. des Absenders) sollen erkannt werden.
   - Gegenüber einem Dritten soll der Empfänger nachweisen können, dass Instanz x die Nachricht y gesendet hat.
   - Der Absender soll das Absenden einer Nachricht mit korrektem Inhalt beweisen können, möglichst sogar den Empfang der Nachricht.
   - Niemand kann dem Netzbetreiber Entgelte für erbrachte Dienstleistungen vorenthalten. Umgekehrt kann der Netzbetreiber nur für erbrachte Dienstleistungen Entgelte fordern.
3. Verfügbarkeit
   - Das Rechnernetz ermöglicht Kommunikation zwischen allen Partnern, die dies wünschen und denen es nicht verboten ist.

T · · Mobile

Durchsetzung von Schutzzielen

- Durchsetzung der Schutzziele durch:
  1. Prävention
     - Zugangskontrolle (Identifikation und Authentifikation)
     - Zugriffskontrolle (Autorisierung)
     - Kryptographie (Verschlüsselung, digitale Unterschriften, digitales Bargeld etc.)
     - Firewalls
     - Scanner
  2. Erkennung
     - Intrusion-Detection-Systeme (IDS)
  3. Reaktion
     - Intrusion-Response-Systeme (IRS)
     - Administration

Angriffe im Internet
Teil 2

Angriffe

T Mobile

Angriffe

Definition: **Angriff**

Ein **Angriff** ist eine Menge von Aktionen, die versucht, die

- Vertraulichkeit,
- Integrität, oder
- Verfügbarkeit

eines Systems zu kompromittieren.

Phasen eines Angriffs:

1. Zielauswahl
2. Informationssammlung
3. Angriff
4. Modifikation des Systems
5. Beseitigung von Spuren

Angriffe im Internet

Phase 1: Zielauswahl

Motivation für einen Angriff:

- Neugier
- Habgier
- Geltungssucht
- Rachgier
- ...

T Mobile

Angriffe im Internet

Phase 2: Informationssammlung

Informationssammlung bzgl.:

- Struktur des Netzwerks
- Betriebssysteme
- Software
- Benutzerkonten

Informationsquellen:

- Kommunikation mit Nutzern
- Aktionen vor Ort
- Aktionen an den Rechnern
- Kommunikation mit Experten
- Kommunikation mit anderen potenziellen Angreifern

T · · Mobile ·

Angriffe im Internet

Phase 2: Beispiel Netze

Identifizierung:

- Domänennamen
- Adressen

Werkzeuge:

- Suchmaschinen
- Registrierungsdienste und -verzeichnisse
- Domain Name System (DNS)

Angriffe im Internet

Phase 2: Beispiel Netze

Beispiel:

- Abfrage RIPE Network Coordination Centre (Whois, Volltextsuche)
  - Registrar Query
  - Organisational Query
  - Domain Query
  - Network Query
  - POC Query

- Abfrage Domain Name System
  - Zone Transfer
  - MX Records
  - ...


```
Büschkes>nslookup
Standardserver:  www-proxy.BN1.srv.t-online.de
Address:  212.185.249.50

> www.ibr.cs.tu-bs.de
Server:  www-proxy.BN1.srv.t-online.de
Address:  212.185.249.50

Nicht autorisierte Antwort:
Name:    agitator.ibr.cs.tu-bs.de
Address:  134.169.34.18
Aliases:  www.ibr.cs.tu-bs.de

>
```

T · · Mobile ·

Angriffe im Internet

Phase 2: Beispiel Zugriffspfade

Identifizierung:

- Wege und somit alle Zwischenknoten auf dem Weg zum Zielnetz/-rechner unter Berücksichtigung alternativer Startpunkte

Werkzeuge:

- traceroute
- Firewalking
- ...

T Mobile

Phase 2: Beispiel Zugriffspfade

Beispiel:

```
Büschkes>tracert www.ibr.cs.tu-bs.de

Routenverfolgung zu agitator.ibr.cs.tu-bs.de [134.169.34.18] über maximal 30 Ab-
schnitte:

  1    71 ms    59 ms    59 ms  217.5.98.50
  2    59 ms    59 ms    59 ms  217.237.153.134
  3    69 ms    69 ms    69 ms  H-EB1.H.DE.net.dtag.de [62.154.49.138]
  4    69 ms    69 ms    69 ms  ir-hannover2-po1-0.g-win.dfn.de [188.1.62.1]
  5    69 ms    69 ms    69 ms  cr-hannover1-ge5-0.g-win.dfn.de [188.1.88.61]
  6    69 ms    69 ms    69 ms  ar-braunschweig3-po0-0.g-win.dfn.de [188.1.88.66]
  7    68 ms    69 ms    69 ms  ciscobsw.rz.tu-bs.de [134.169.3.222]
  8    69 ms    69 ms    69 ms  ibrgate.rz.tu-bs.de [134.169.246.34]
  9    69 ms    69 ms    69 ms  agitator.ibr.cs.tu-bs.de [134.169.34.18]

Ablaufverfolgung beendet.
```

T · · Mobile ·

Phase 2: Beispiel Scanning

Identifizierung:

- Netzwerkstruktur
- verfügbare Rechner
- verfügbare Dienste

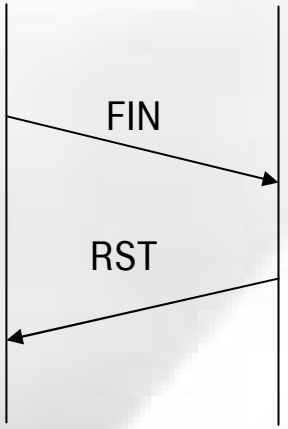
Werkzeuge:

- Scanner

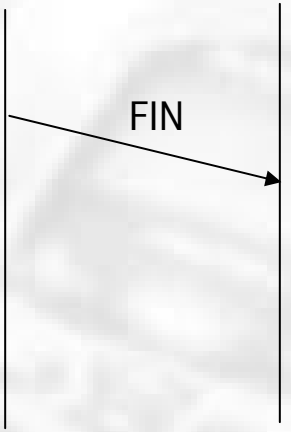
Beispiel:

- FIN Scan

a) Port geschlossen:



b) Port offen:



Phase 2: Beispiel Scanning

Beispiel:

Nmap

- Werkzeug zum Scannen großer Netzwerke
- Liefert eine Liste der interessanten Ports auf den gescannten Maschinen
- Port hat als Ergebnis einen der drei folgenden Zustände:
  1. Open: Zielrechner akzeptiert Verbindungen auf diesem Port
  2. Filtered: Firewall oder ähnliche Komponente verhindert die Analyse des Ports
  3. Unfiltered: Zielrechner akzeptiert keine Verbindungen auf diesem Port

Optionen:

- `-sT` TCP Connect() Scan
- `-sS` TCP Syn Scan
- `-sF` Stealth Fin Scan
- `-sX` Xmas Tree Scan
- `-sN` Null Scan
- `-sP` Ping Scan
- `-sU` UDP Scan
- `-sO` IP Protocol Scan
- `-sA` ACK Scan
- `-sW` Window Scan
- `-sR` RPC Scan
- `-b <ftp relay host>` FTP Bounce Attack

Phase 2: Beispiel Scanning

- `nmap -v target.example.com`
  Scannt alle reservierten TCP-Ports des angegebenen Rechners. Die Option -v schaltet den "verbose"-Modus ein, d.h. es werden mehr Informationen über das aktuelle Vorgehen ausgegeben.
- `nmap -sX -p 22,53,110,143,4564 198.116.*.1-127`
  Führt einen Xmas-Tree-Scan gegen die erste Hälfte der in einem der 255 möglichen Subnetze des Class-B-Adressraums liegenden Rechner durch. Dabei wird überprüft, ob auf den Rechnern SSH, DNS, POP3, IMAP oder Port 4564 angesprochen werden können.
- `nmap -sS -O target.example.com/24`
  Führt einen SYN-Scan gegen jede im Class-C-Subnetz des angegebenen Rechners liegende Maschine durch. Gleichzeitig wird versucht, das Betriebssystem der entsprechenden Rechner zu bestimmen (-O).

Phase 2: Beispiel OS-Fingerprinting

Identifizierung:

- Betriebssystem

Beispiele:

1. Identifizierung über Banner

```
[malaria:roland] 44> telnet aoxo
Trying 137.226.12.58...
Connected to Aoxomoxoa.informatik.rwth-aachen.de.
Escape character is '^]'.

SunOS 5.6

login:
```

2. Identifizierung über DNS-Host-Record
3. Identifizierung über SNMP

Angriffe im Internet

Phase 2: Beispiel OS-Fingerprinting

4. Identifizierung über spezielle Systembefehle

```
payfonez> telnet ftp.netscape.com 21
Trying 207.200.74.26 ...
Connected to ftp.netscape.com.
Escape character is '^]'.
220 ftp29 FTP server (UNIX(r) System V Release 4.0) ready.
SYST
215 UNIX Type: L8 Version: SUNOS
```

5. Identifizierung über spezielle Anwendungsinformationen

```
00000030                    48 54 54 50 2F 31 2E 31 20 33       HTTP/1.1.3
00000040  30 34 20 4E 6F 74 20 4D 6F 64 69 66 69 65 64 0D 04.Not.Modified.
00000050  0A 53 65 72 76 65 72 3A 20 4D 69 63 72 6F 73 6F .Server:.Microso
00000060  66 74 2D 49 49 53 2F 34 2E 30 0D 0A 44 61 74 65 ft-IIS/4.0..Date
00000070  3A 20 54 75 65 2C 20 31 35 20 4D 61 79 20 32 30 :.Tue,.15.May.20
00000080  30 31 20 31 31 3A 35 39 3A 31 39 20 47 4D 54 0D 01.11:59:19.GMT.
00000090  0A 45 54 61 67 3A 20 22 63 30 30 64 63 64 64 65 .ETag:."c00dcdde
000000A0  30 35 39 63 30 31 3A 31 66 36 34 22 0D 0A 0D 0A 059c01:1f64"....
```

T · · Mobile ·

Phase 2: Beispiel OS-Fingerprinting

6. Anspruchsvollere Methoden basieren auf der Identifizierung von charakteristischen Eigenschaften verschiedener Betriebssysteme bzw. Protokollimplementierungen:

   a) Bogus Flag Probe
   Setzen eines undefinierten TCP-Flags (z.B. 64 oder 128) im TCP-Header eines SYN-Pakets. In Abhängigkeit vom Typ der Implementierung behält der Server in seiner Antwort das ungültige Flag bei oder setzt die Verbindung zurück.

   b) TCP ISN Sampling
   Suche nach Mustern bei der Generierung der Initial Sequence Number (ISN) für TCP-Verbindungen. Verschiedene Implementierungen benutzen verschiedene Verfahren zur Generierung der ISN (z.B. festes, zufälliges oder zeitabhängiges Schema).

   c) Don't Fragment Bit
   Bit wird von verschiedenen Implementierungen in verschiedenen Situationen gesetzt.

   d) TCP Initial Window
   Überprüfen der Fenstergröße für Antwortpakete

Phase 2: Beispiel OS-Fingerprinting

e) ACK Value
In bestimmten Fällen unterscheiden sich Implementierung in dem für das ACK-Feld benutzten Wert (z.B. beim Senden eines FIN/PSH/URG-Pakets an einen geschlossenen TCP-Port).

f) ICMP Error Message Quenching
Verschiedene Implementierungen senden Fehlermeldungen mit unterschiedlichen Raten.

g) ICMP Message Quoting
Verschiedene Implementierungen senden verschiedene Teile eines einen Fehler auslösenden Pakets zurück.

h) ICMP Error Message Echoing Integrity
Verschiedene Implementierungen verändern Teile eines einen Fehler auslösenden Pakets, das sie an den Sender als Bestandteil einer Fehlermeldung zurücksenden.

i) Type of Service
Verschiedene Implementierungen tragen im TOS-Feld einer ICMP-Port-Unreachable-Nachricht unterschiedliche Werte ein.

Phase 2: Beispiel OS-Fingerprinting

j) Fragmentation Handling
Verschiedene Implementierungen handhaben überlappende IP-Fragmente auf unterschiedliche Art und Weise.

k) TCP Options
Nicht alle Implementierungen unterstützen dieselben Optionen.

l) Exploit Chronology
Verschiedene Implementierungen reagieren unterschiedlich auf verschiedene Angriffe.

m) SYN Flood Resistance
Verschiedene Implementierungen handhaben SYN-Flood-Angriffe unterschiedlich.

Phase 2: Beispiel Service Enumeration

Identifizierung:

- Details bzgl. der verfügbaren Rechner
- Details bzgl. der verfügbaren Dienste
- Details bzgl. der verfügbaren Benutzer-Accounts

Beispiele:

1. Identifizierung über Banner

```
[malaria:roland] 44> telnet agitator.ibr.cs.tu-bs.de 80
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>501 Method Not Implemented</TITLE>
</HEAD><BODY>
<H1>Method Not Implemented</H1>
exit to /index.html not supported.<P>
Invalid method in request exit<P>
<HR>
<ADDRESS>Apache/1.3.26 Server at www.ibr.cs.tu-bs.de Port 80</ADDRESS>
</BODY></HTML>
```

Phase 2: Beispiel Service Enumeration

2. Identifizierung von Rechner- und Service-Informationen
   - BGP
   - SNMP
   - HTTP
   - MS/UNIX RPC
   - NetBios Session
   - SMTP
   - NIS
   - SQL
   - NFS
   - ....
3. Identifizierung von Benutzer-Accounts
   - SMTP
   - Finger
   - NetBios Name Service
   - NetBios Session
   - LDAP
   - ...

Angriffe im Internet

Phase 3: Angriff

Ausgenutzte Schwachstellen basieren auf:

- Fehlern beim Design und der Implementierung
- Fehlern beim Systemmanagement
- Fehlern bei der Einschätzung der Vertrauenswürdigkeit

Erweiterung der Zugriffsrechte nach Erstzugriff durch:

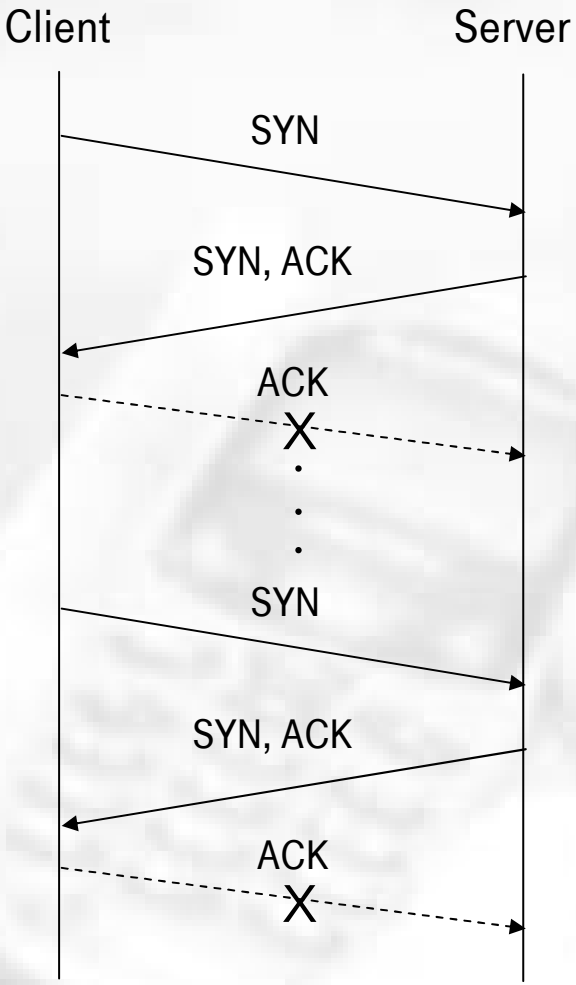
- Erlangen des Passworts eines legitimen Nutzers
- Ausführen eines (modifizierten) Programms durch andere Nutzer
- Ausnutzen von Hardware-Schwachstellen
- Ausnutzen von Software-Schwachstellen
- Ausnutzen von Schwachstellen in den Zugriffsberechtigungen

T · · Mobile ·

Phase 3: Beispiel SYN Flood

SYN Flood:

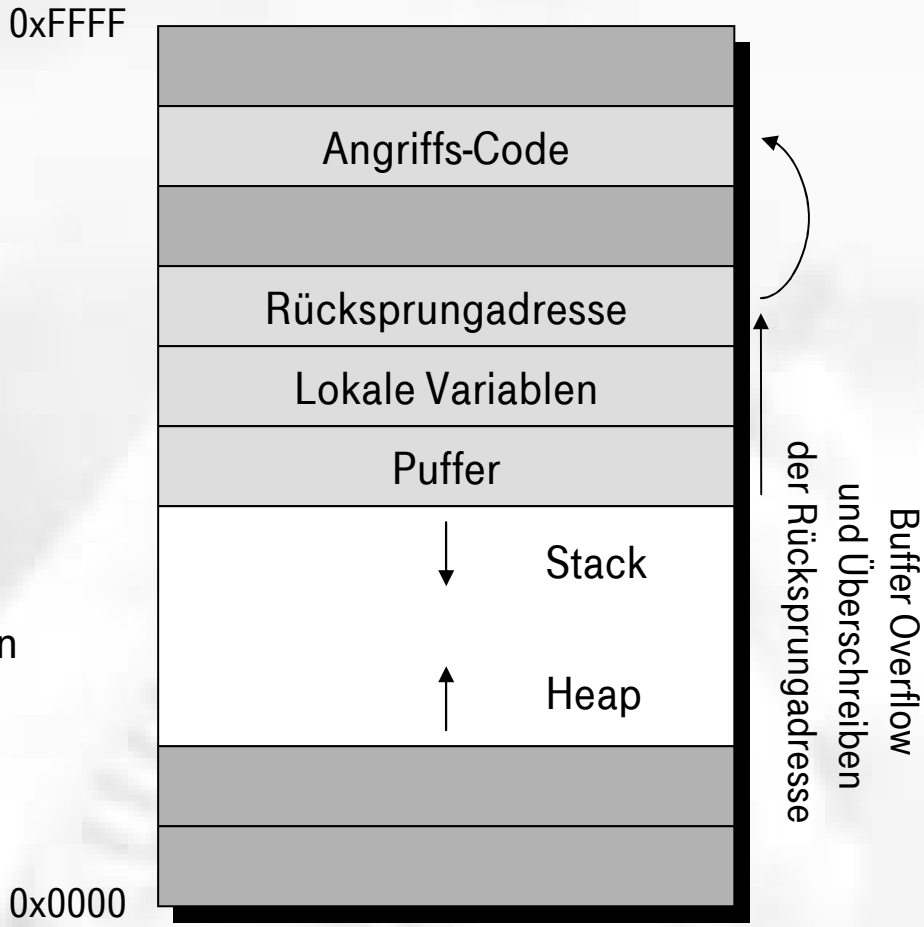
- Denial-of-Service (DoS) Angriff
- Aufbau einer bestimmten Anzahl halb-offener TCP-Verbindungen, um das Zustandekommen weiterer Verbindungen zu verhindern
- Angreifer sendet mehrere SYN-Pakete, die vom Ziel mit den entsprechenden SYN/ACK-Paketen beantwortet werden
- Angreifer antwortet auf die empfangenen SYN/ACK-Pakete nicht (unvollständiger 3WHS)
- Halboffene Verbindungen werden vom Server durch Timeouts entdeckt, aber Angreifer sendet Verbindungsanfragen mit einer höheren Rate



Phase 3: Beispiel Buffer Overflow

Buffer Overflow:

- Stack verwaltet die Rücksprungadresse für einen Prozeduraufruf
- Modifikation des Stacks kann das System zu einem Sprung an eine beliebige Adresse veranlassen
- Angreifer kann dadurch das System zur Ausführung von beliebigem Code bringen
- Angreifer generiert eine Zeichenkette, die den Puffer mit der Rücksprungadresse überschreibt
- Veränderter Wert veranlasst das Programm, einen Befehl auszuführen
- Besonders interessant im Zusammenhang mit Prozessen, die mit entsprechend hohen Rechten ausgestattet sind



Phase 3: Beispiel Race Condition

Race Condition:

- Existenz eines Zeitfensters zwischen dem Zeitpunkt, zu dem ein Attribut überprüft wird, und dem Zeitpunkt, zu dem es benutzt wird

Beispiel:

- rdist (Remote File Distribution Programme)
- rdist und rdistd verfügen über Root-Rechte
- rdistd erzeugt eine temporäre Datei (1), schreibt die neuen Daten in diese Datei (2)(3), ändert den Besitzer (6) sowie die Berechtigungen (7), sodass diese mit der Master-Datei übereinstimmen, und benennt die temporäre Datei um (8)
- chmod ändert die Berechtigungen von /bin/sh so ab, dass das setuid-Bit gesetzt wird

Phase 3: Beispiel Race Condition

Zeitlicher Ablauf:

Schritt	Systemaufrufe durch rdistd	Systemaufrufe durch den Angreifer
0		execv("/usr/ucb/rdist");
1	fd=creat("/ko/rdista768");	
2	write(fd, ...);	
3	close (fd);	
4		rename("/ko/rdista768", "/ko/tmp");
5		symlink("/bin/sh","/ko/rdista768");
6	chown("/ko/rdista768", owner);	
7	chmod("/ko/rdista768", pmode);	
8	rename("/ko/rdista768", "/ko/data");	

Zeit-
fenster

Angriffe im Internet

Phase 2/3: Weitere Beispiele

Schicht	Angriff
ICMP	Ping of Death
	Ping Sweep
UDP	UDP Scan
TCP	SYN Flood
	SYN Scan
	FIN Scan
	SYN/ACK Scan
	SYN/FIN Scan
	RST Scan
	Xmas Tree Scan
Anwendung	FTP Bounce Attack
Prozess	Deadlock
	Buffer Overflow
	Race Condition

T · · Mobile ·

Angriffe im Internet

Phase 2/3: Weitere Techniken

Weitere zum Einsatz kommende Methoden:

1. Eavesdropping
2. Password Guessing
3. Password Cracking
4. Denial-of-Service-Angriffe
5. Directory Traversal
6. ...

T Mobile

Angriffe im Internet

Phase 4: Modifikation des Systems

Erreichen des eigentlichen Angriffsziels durch:

- Diebstahl von Software
- Diebstahl von Geschäftsgeheimnissen
- Diebstahl von Informationen
- Diebstahl von Ressourcen
- Modifikation von Informationen
- Verhinderung der Diensterbringung
- Störung

Zusätzlich:

- Sicherstellen des Zugriffs zu einem späteren Zeitpunkt, d.h. Beseitigung der ausgenutzten Schwachstelle und Einrichten einer eigenen, versteckten Zugriffsmöglichkeit

T · · Mobile ·

Angriffe im Internet

Phase 4: Modifikation des Systems

Zum Einsatz kommende Methoden:

1. Privilege Escalation
2. Password Cracking
3. Remote Control und Backdoors
4. Port Redirection
5. ...

T Mobile

Angriffe im Internet

Phase 5: Beseitigung von Spuren

Datenvermeidung:

- Angriff über mehrere Zwischenknoten
- Fälschen der Absenderadresse
- Manipulation des Telefonsystems und von Nebenstellenanlagen
- ...

Datensparsamkeit:

- Verbergen von Netzwerkverbindungen
- Verbergen von Prozessen
- Modifikation von Log-Dateien
- Modifikation von Zeitdaten
- ...

T · · Mobile ·

Angriffe im Internet
Teil 3

Klassifikation von Angriffen

T Mobile

Modell - Spezifikation & Implementierung

Idee: Spezifikation von Protokollen und Prozessen als Deterministische Endliche Automaten (DEA)

Definition 1: **Spezifikations- und Implementierungs-DEA**

Die Darstellung der Spezifikation eines Prozesses oder eines Kommunikationsprotokolls als deterministischer endlicher Automat wird als **Spezifikations-DEA** $A = (Q, \Sigma, q_0, \delta, F)$ bezeichnet. Dabei wird vorausgesetzt, dass der Spezifikations-DEA keine Entwurfsfehler enthält, die in Sicherheitsverletzungen resultieren können. Insbesondere sei die vom Spezifikations-DEA erkannte Sprache endlich, d.h. es gelte $|\mathcal{L}(A)| < \infty$.

Die Darstellung der entsprechenden Implementierung eines Prozesses oder Kommunikationsprotokolls als deterministischer endlicher Automat wird als **Implementierungs-DEA** $A' = (Q', \Sigma', q_0, \delta', F')$ bezeichnet.

Definition 2: **Δ-DEA**

Für einen gegebenen Spezifikations-DEA A und einen Implementierungs-DEA A' ist der **Δ-DEA** $A^{\Delta} = (Q^{\Delta}, \Sigma^{\Delta}, q_0, \delta^{\Delta}, F^{\Delta})$ durch den minimalen deterministischen endlichen Automaten mit $\mathcal{L}(A^{\Delta}) = \mathcal{L}(A') \setminus \mathcal{L}(A)$ definiert.

T · · Mobile ·

Modell - Anomalie & Angriff

Definition 3: **Anomalie**

Mit Bezug auf einen gegebenen Spezifikations-DEA A und einen entsprechenden Implementierungs-DEA A‘, für die $\mathcal{L}(A) \subseteq \mathcal{L}(A')$ gilt, ist eine **Anomalie** ein Wort α mit $\alpha \in \mathcal{L}(A^{\Delta})$. Eine Anomalie entspricht damit einem akzeptierenden Lauf des Δ-Automaten. Die Menge der Anomalien $\mathcal{A}$ sei als $\mathcal{A} = \mathcal{L}(A^{\Delta})$ definiert.

Definition 4: **Angriff**

Ein **Angriff** entspricht einem Wort $\beta \in \mathcal{L}(A^{\Delta})$ und damit einem akzeptierenden Lauf des Δ-Automaten, der zu einer Verletzung der definierten Sicherheitspolitik führt.

Bezeichnet $\mathcal{B}$ die Menge der Angriffe, dann gilt offensichtlich $\mathcal{B} \subseteq \mathcal{A}$, d.h. die Menge der Angriffe ist eine Teilmenge der Menge der Anomalien.

Transaktionen

Idee: Modellierung von Protokoll- und Prozessläufen als Transaktionen

Transaktionen werden in ihren Eigenschaften durch das **ACID-Prinzip** charakterisiert:

1. Atomarität (engl. Atomicity): Eine Transaktion wird vollständig oder gar nicht ausgeführt.
2. Konsistenz (engl. Consistency): Eine Transaktion hält alle Integritätsbedingungen ein, d.h. eine Transaktion hinterlässt stets einen konsistenten Systemzustand, falls sie auf einem solchen gestartet wurde.
3. Isolation (engl. Isolation): Eine Transaktion läuft isoliert von anderen Transaktionen ab.
4. Persistenz (engl. Durability): Die von einer erfolgreichen Transaktion im Hinblick auf den Systemzustand erzeugten Effekte überleben jeden danach auftretenden Hard- oder Software-Fehler.

Klassifikation von Anomalien & Angriffen

Satz: **Klassifikation von Anomalien und Angriffen**

Mit Bezug auf einen Spezifikations-DEA $A = (Q, \Sigma, q_0, \delta, F)$ können die im Hinblick auf einen Implementierungs-DEA $A' = (Q', \Sigma', q_0, \delta', F')$ möglichen Anomalien und Angriffe jeweils als Verletzung einer der Transaktionseigenschaften Atomarität, Konsistenz und Isolation klassifiziert werden.

Beweisidee:

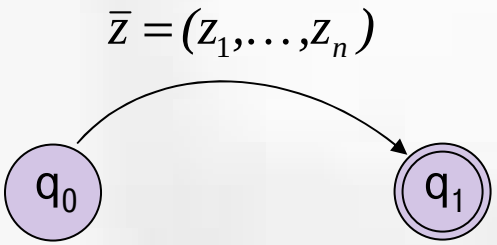
Gilt $\omega \in \mathcal{L}(A)$?

Fallunterscheidung bzgl.:

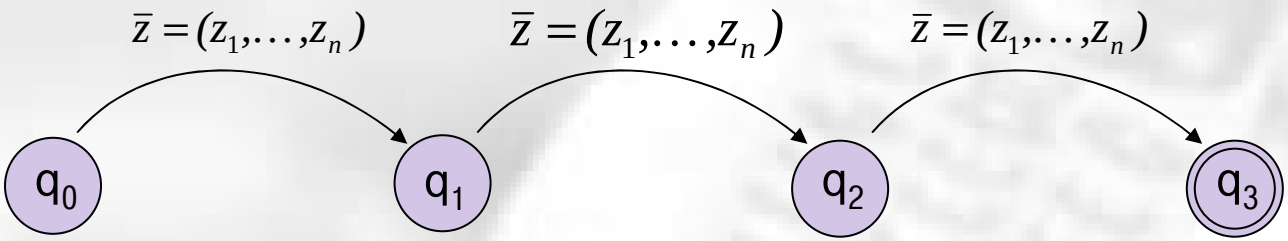
1. Anomalien im Hinblick auf die Transitionsfunktion δ'
2. Anomalien im Hinblick auf den Zustandsraum Q'

Kommunikationsmodelle und Transaktionen

- Verbindungslose Kommunikation:



- Verbindungsorientierte Kommunikation:



Kommunikationsmodelle und Transaktionen

Modellierung:

Kommunikationsmodell		Transaktion	Teiltransaktion	Beispiel
verbindungsorientiert		Verbindung	Verbindungs-aufbau	TCP-Verbindung
			Datenüber-tragung	
			Verbindungs-abbau	
verbindungslos	Frage/Antwort	Frage/Antwort	Frage	ICMP-Anfrage/Antwort
			Antwort	
	Ereignis	Ereignis	-	ICMP-Fehlermeldung

Angriffe im Internet

Klassifikation - Beispiele

Klassifikation von Angriffen:

Verletzung	Schicht	Angriff
Atomarität	TCP	SYN Flood
		SYN Scan
	Prozess	Deadlock
Konsistenz	ICMP	Ping of Death
	TCP	FIN Scan
		SYN/ACK Scan
		SYN/FIN Scan
		RST Scan
		Xmas Tree Scan
	UDP	UDP Scan
	Anwendung	FTP Bounce Attack
	Prozess	Buffer Overflow
Isolation	Prozess	Race Condition

T-Mobile

Angriffserkennung (Exkurs)

Angriffserkennung - Grundtechniken

Übersicht:

Policy			
Default Permit	Missbrauchs-erkennung	-	
Default Deny	Spezifikationsbasierte Anomalieerkennung	Profilbasierte Anomalieerkennung	
	Statisch	Dynamisch	**Objektverhalten**

Transaktionsbasierte Anomalieerkennung

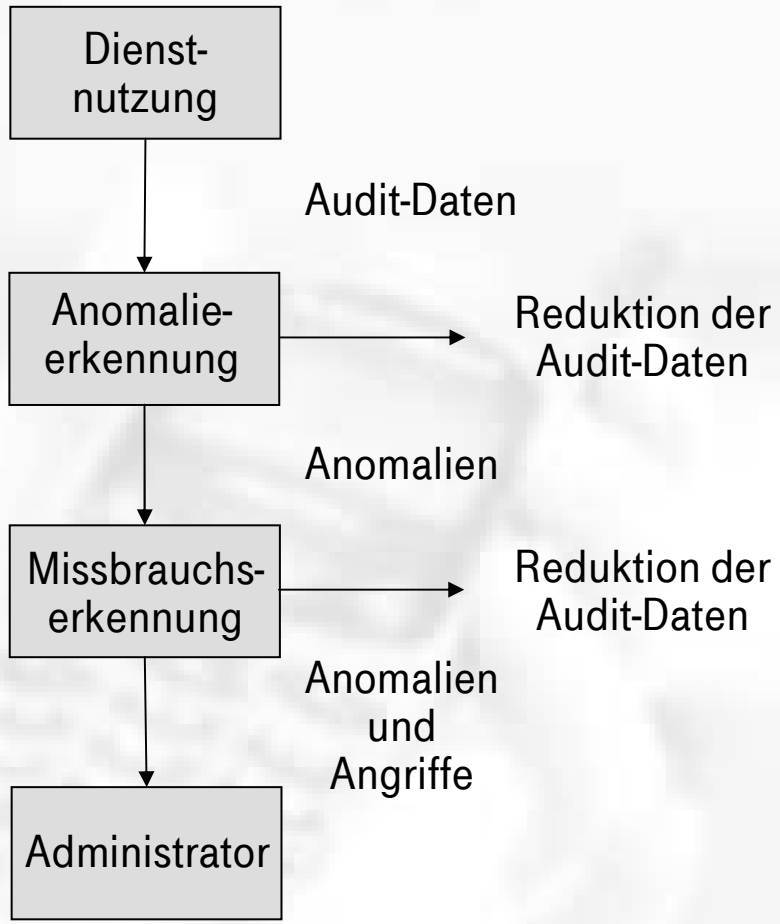
Transaktionsbasierte Anomalieerkennung:

- Beschreibe positives Verhalten durch die Definition zulässiger Transaktionen in Form von Automaten
- Überwache die Domäne im Hinblick auf mögliche Verletzungen der ACID-Eigenschaften der definierten Transaktionen
- Melde erkannte Anomalien zur genaueren Klassifikation weiter ($\mathcal{B} \subseteq \mathcal{A}$)

Problem: Zustandsexplosion bei Automaten

Idee: Automaten mit Variablen versehen

Ablauf:



Angriffe im Internet
Teil 5

Fazit

T Mobile

Angriffe im Internet

Zusammenfassung & Ausblick

Zusammenfassung:

- Einführung IT-Sicherheitsmanagement
- Einführung Angriffe
- Klassifikation von Anomalien und Angriffen mittels Transaktionseigenschaften (ACID-Eigenschaften)
- Transaktionsbasierte Erkennung von Anomalien und Angriffen (erweitertes Automatenmodell)

Ausblick:

- Transaktionsbasierte Anomalieerkennung für Prozesse
- Durchsetzung von transaktionsbasierten Sicherheitsrichtlinien

T · · Mobile ·

Literatur

[1] R. Büschkes: „Angriffserkennung in Kommunikationsnetzen, Dissertation, RWTH Aachen, 2001.

[2] DIN Deutsches Institut für Normung e.V.: „Leitfaden für das IT-Sicherheitsmanagement (GMITS) - Teil 1: Konzepte und Modelle für IT-Sicherheit", DIN-Fachbericht 66, 1997.

[3] S. McClure, J. Scambray, G. Kurtz: „Hacking Exposed – Network Security Secrets & Solutions", 4th Edition, McGraw-Hill/Osborne, 2003.

[4] A. Pfitzmann: „Sicherheit in Rechnernetzen: Mehrseitige Sicherheit in verteilten und durch verteilte Systeme", Skript zu den Vorlesungen Datensicherheit und Kryptographie, TU Dresden, Fakultät Informatik, 1990-1999.