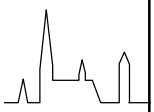
Telematik 4
IT - Sicherheit

1 - Einführung



Prof. Dr. Günter Müller

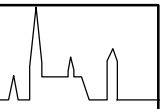
Wintersemester 04/05

http://www.telematik.uni-freiburg.de/

Institut für Informatik und Gesellschaft – Telematik

Gliederung

IIG
Telematik



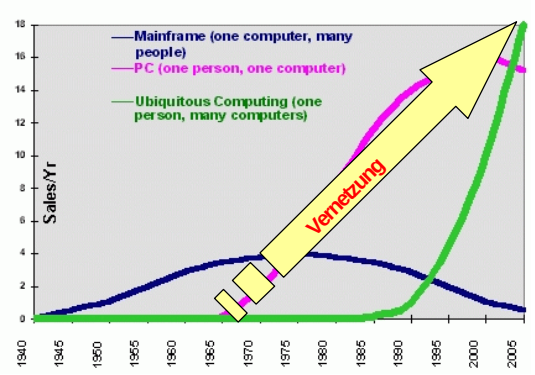
Technologien und Vernetzung

IIG Telematik

Mainframe
- homogene Nutzer
- zentrale Zugangsreglung
- zentrale Datenhaltung
- → niedrige Vernetzung

Personal Computer
- heterogene Nutzer
- dezentrale Datenhaltung
- → hohe Vernetzung

Allgegenwärtiges
- dynamisch und „stateless“
- „mixed-mode“ Netze
- → spontane Vernetzung

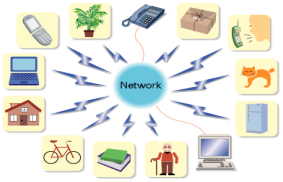


Quelle: http://kdg.mit.edu/ikspre/x009.html

Vernetzung = (Un)Sicherheit?!

Metapher: Epochen der Sicherheit

IIG Telematik



Epochen	Mittelalter	Internet	Allgegenwärtiges
Metapher	„Gute“ Bürger sind drinnen	Mit wem rede ich?	Computer ist symbiotisch

Zeit

menschliche Interaktion → autonom

Epoche Mittelalter

IIG Telematik

Herausforderung

- Verteidigung der Burg
  - von außen, nicht berechtigte Bürger bleiben draußen
  - von innen, ein Bürger „spioniert“ die anderen nicht aus

Angreifermodell

- von außen, „Outsiders“ oder „Intruders“
- von innen, „Insiders“ oder „Saboteurs“

Schutzziel

- Vertraulichkeit der Kommunikation

Lösung

- „reaktives“ Vorgehen
  - gegen Outsiders, strenge Zugangskontrolle (Firewalls) und Intrusion-detection Monitors
  - gegen Insiders, Kryptographie und Prozessisolierung auf Betriebssystem Ebene

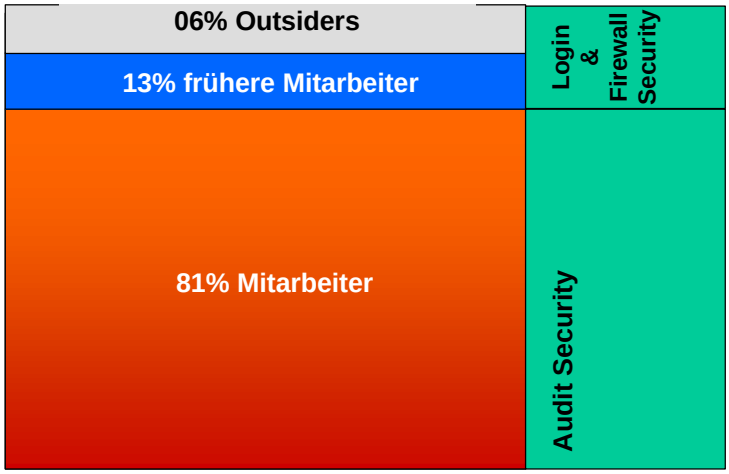
Thema

- Privatsphäre der Bürger

Mittelalter: Quelle der Angriffe

IIG Telematik

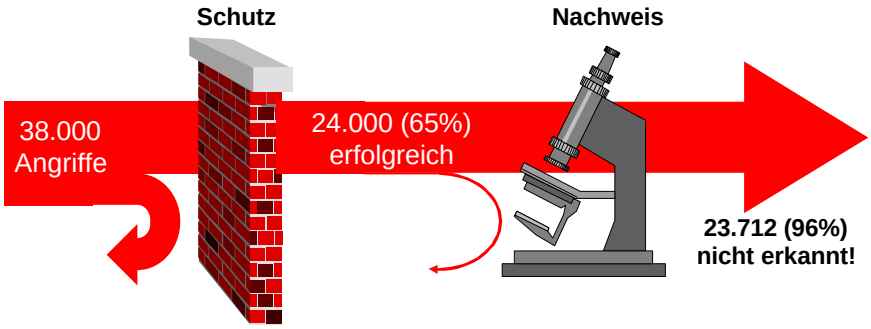
Der Angreifer saß überwiegend im eigenen Unternehmen!



Quelle: Data Processing Management Assoc, 1997

Mittelalter:
Mangelhafte Abwehr der Burg

IIG
Telematik



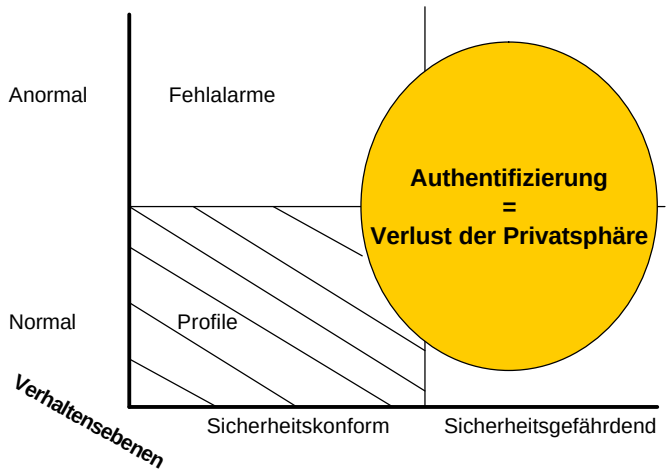
Quelle: Testangriffe US-Militär, Defense Information Systems Agency, Mai 1996

- Firewalls und Intrusion detection ➔ Hohe „Dunkelziffer“ **unerkannter** Angriffe
- Bedarf an **Authentifizierung**, Autorisierung und Abrechnung nimmt zu

Mittelalter:
Wer ist der (gute) Insider?

IIG
Telematik

Authentifizierung: Erkennung von Kommunikationspartnern, aber…



Epoche Internet

IIG
Telematik

Herausforderung

- (korrekte) mehrseitige Sicherheit
- Aufbauen von Vertrauen

Angreifermodell

- Mann in der Mitte
- „Impersonation“ von Kommunikationspartnern

Themen

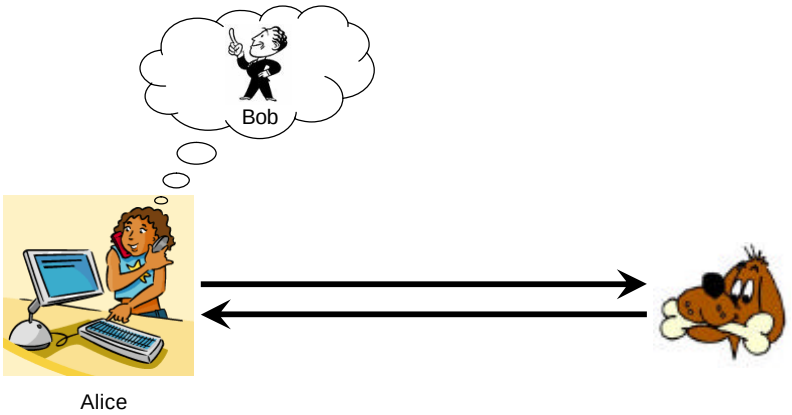
- Entwicklung von Sicherheitsmechanismen anhand von
  - Schutzzielen
  - Bedrohungen

  sind diese Mechanismen „korrekt“ bzgl. ihrer Ziele?
  → Verifikation wird erforderlich
- Vertrauen: basiert auf Software oder Hardware
  - Software → Sicherheitsprotokolle
  - Hardware → Trusted Computing

Internet: Alle sprechen mit allen…

IIG
Telematik

Auch mit dem Falschen!

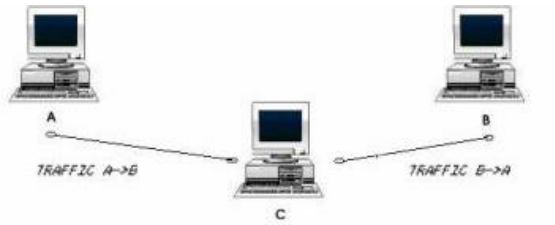


Und wenn der Hund „beißt“?

Internet: Mann in der Mitte

Attacke

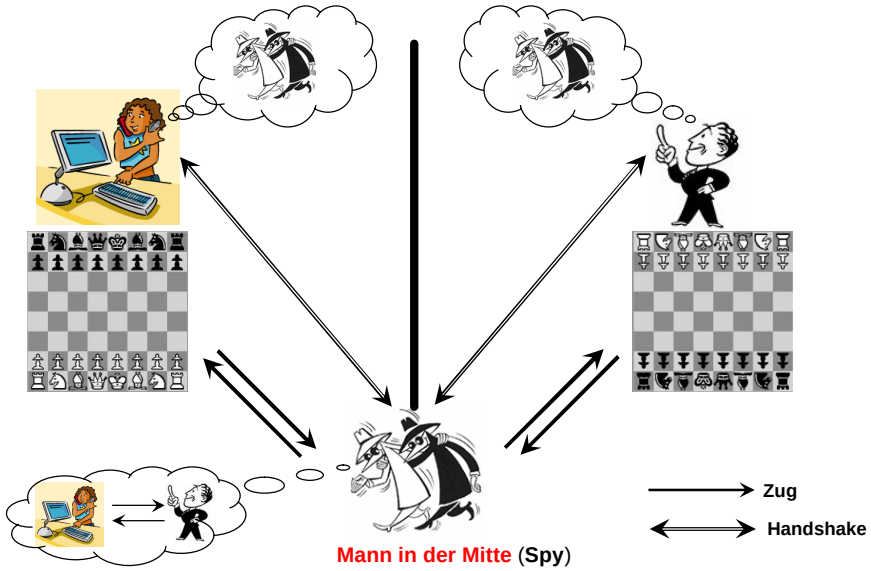
einem Angreifer gelingt es, den Kommunikationskanal soweit unter die eigene Kontrolle zu bringen, dass die „Abgehörten“ nicht feststellen können ob sie tatsächlich miteinander oder mit dem Angreifer kommunizieren



Nutzung

- abhängig vom Ziel eines Protokolls
- Angriffe können genutzt werden, um sich unberechtigt Zugang zu Informationen zu verschaffen, sie zu manipulieren oder komplette Datenverbindungen zu übernehmen („*connection hijacking*“)

Mann in der Mitte: Wie besiegt man einen Schachmeister

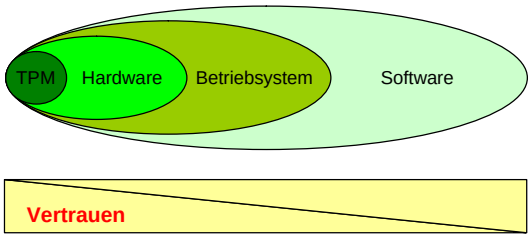


Mann in der Mitte (**Spy**)

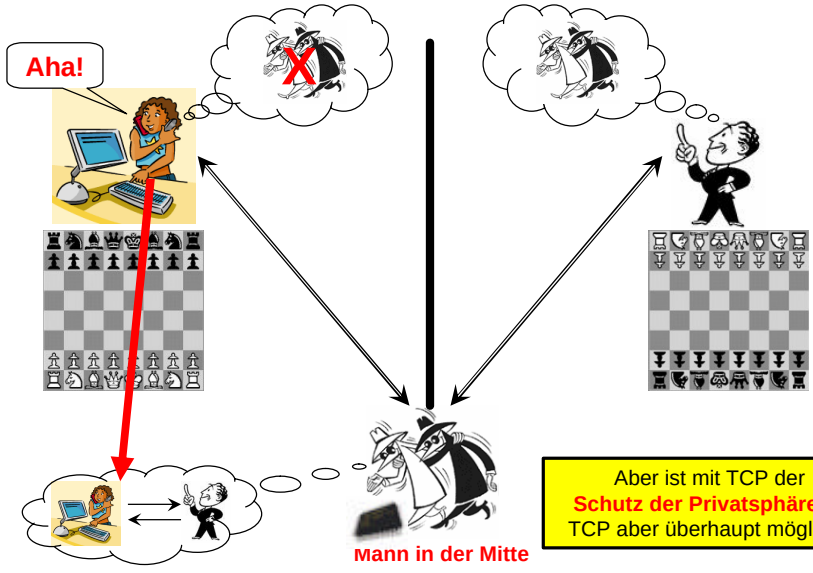
Internet: Trusted Computing Platform (TCP)

Vertrauensaufbau durch vertrauenswürdige Hardwaremodule (TPM)

- Funktionalität in Kürze:
  - schützen und generieren von geheimen Schlüsseln
  - sichere Ablage von als vertrauenswürdig eingestuften Systemkonfigurationen
  - Bereitstellung eines speziellen Schlüssels, mit dem die Plattform von Dritten als vertrauenswürdig erkannt werden kann
  - Verwaltungsfunktionen, mit denen u. a. das TPM von einem Benutzer ein- und ausgeschaltet werden kann
- Realisiert durch rekursive Reihefolge kryptographischer Hash-Funktionen



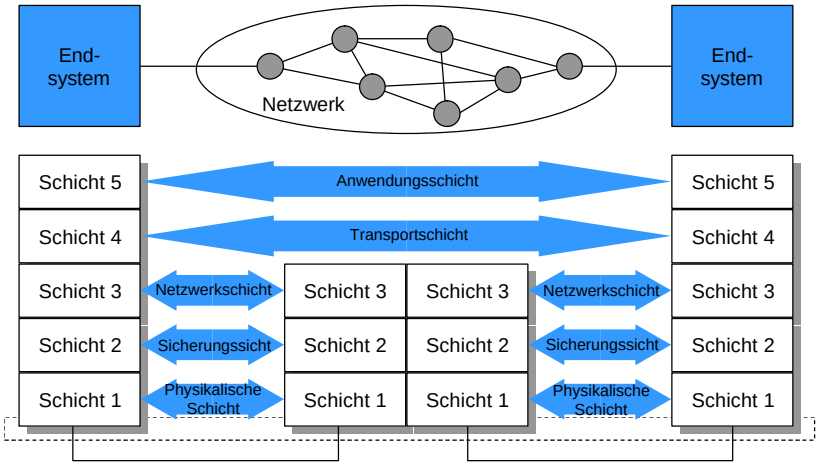
Internet mit TCP: Langfristiges Ziel



Aber ist mit TCP der **Schutz der Privatsphäre** mit TCP aber überhaupt möglich?

Sicherheit in Schichtenmodellen

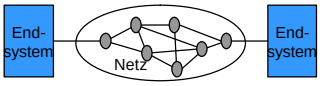
IIG Telematik



Einbauen von Sicherheit in Netzwerken: Was ist zu tun… und wo?

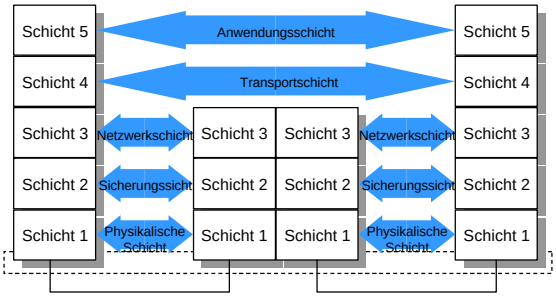
IIG Telematik

Zwei Dimensionen, in den Netzwerksicherheit berücksichtigt werde kann



Dimension 1

Welche Knote soll welche Sicherheitsmechanismen implementieren?

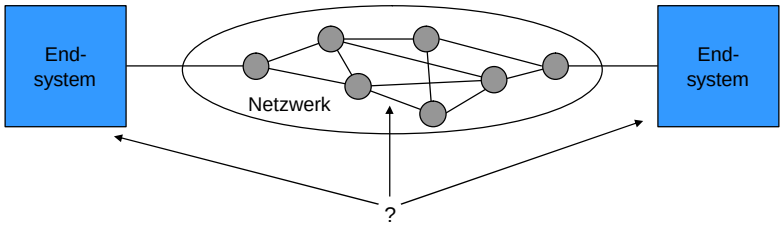


Dimension 2

An welcher Schicht soll welche Sicherheitsmechanismen implementiert werden?

Sicherheitsanalyse des Schichtmodells: Dimension 1

IIG Telematik

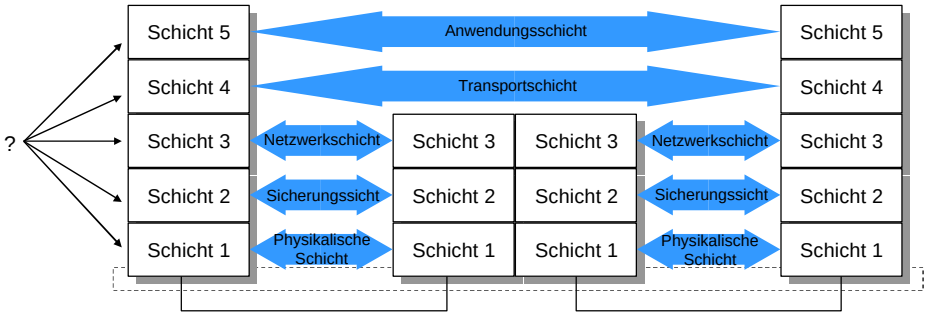


Dimension 1

– An welcher Schnittstelle findet der Angriff statt?

Sicherheitsanalyse des Schichtmodells: Dimension 2

IIG Telematik



Dimension 2

– An welcher Schnittstelle findet der Angriff statt?

Sicherheitsaspekte der mobilen Kommunikation

Mobile Kommunikation

- gleichen Bedrohungen wie im Festnetze
- identische Gegenmaßnahmen

Mobilität erweitert die Angriffsfläche

- Zugang zu Diensten werden durch drahtlose Verbindung einfacher und dementsprechend unsicherer
- Roaming erzwingt regelmäßige Re-Authentifizierung
- Schlüsselverwaltung wird wegen des dynamischen Netzzugangs komplizierter

Besonderes Angriffsziel

- der Ort eines Gerätes oder Nutzers wird wichtigste Information

Sicherheitsszenario
wird erweitert!

→ Schutz der Ortsinformation ist notwendig!

Epoche allgegenwärtiger Computer

Herausforderungen

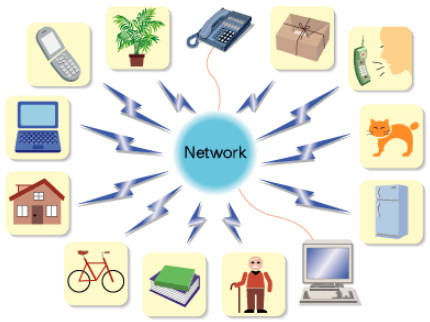
- hoch dynamisch und „mixed-mode“
- überall, jederzeit, alles

Angreifermodell

- Mann in den Extremen

Themen

- Ist Sicherheit überhaupt denkbar?
- Schwerpunkt „Security Engineering“
  - sichere Softwareentwicklung
- Vertrauensaufbau wird erschwert
- Sicherheitsrichtlinien werden wichtiger
  - Mechanismen zu deren Implementierung



Allgegenwärtige Computer: (Un)Sicherheit durch Software

IIG Telematik

- Softwareschwachstellen = fehlerhaftes Design + „buggy“ Implementierung
- Von CERT gemeldet Schwachstellen

Jahre	2000	2001	2002	2003	1Q-2Q 2004
Schwachstellen	1,090	2,437	4,129	3,784	1,740
Sicherheitslücken	21,756	52,658	82,094	137,529	?????

Quelle: http://www.cert.org/stats

Umgebungsspeziesche Gründe

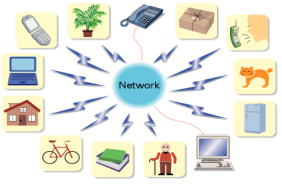
- zunehmend Abhängigkeit von Netzwerken
- Erweiterbarkeit: Patches und neue Module werden automatisch herunter geladen

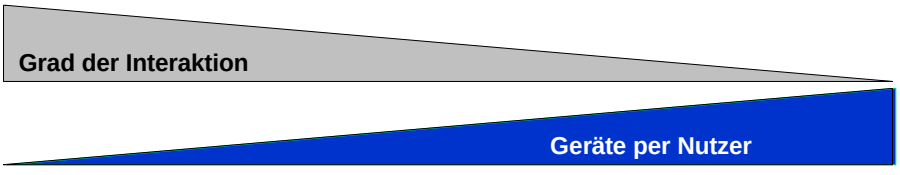
Ungeheuere Komplexität und Dynamik der Systemen

- Systeme befinden sich in keinem definiten, vorhersehbaren Zustand
- Sicherheit wird „holistisch“: überall, jederzeit und alles. Aber **wie**?

Drei Epochen in Vogelschau

IIG Telematik





- Was ist Sicherheit?
- Was will ich schützen und wie kriege ich das hin?

Gliederung

IIG Telematik

1 Einführung

1.1 Drei Epochen der Netzwerksicherheit
- Mittelalter
- Internet
- Allgegenwärtig

1.2 Grundlegende Definitionen
- **Akteure, Kanäle und Sicherheit**
- **Schutzziele, Bedrohungen und Sicherheitsmechanismen**

1.3 Zukünftige Herausforderungen der Sicherheit

Wer sind die Akteure und was dürfen sie?

IIG Telematik

Objekte

Stellen die Information eines Systems dar
- passive Objekte speichern Information (z. B. Dateien, Programme)
- aktive Objekte verarbeiten und speichern diese (z. B. Prozesse, Prozeduren)

Subjekte

Aktive Instanz, die Anfragen an Objekte initiierten kann

Zugriff

Interaktion zwischen Subjekt und Objekt (oft mit Informationsfluss)

Zugriffsrechte

Erlaubnis eines Subjektes, auf ein bestimmtes Objekt zuzugreifen
- hat der Nutzer das Recht, ein Objekt zuzugreifen, ist er dafür **autorisiert**

```
rivejern:~> ll /home/goofy
-rw-------  1 goofy  acme   4679 Aug  6 17:00 roadmap.txt
rivejern:~>
```

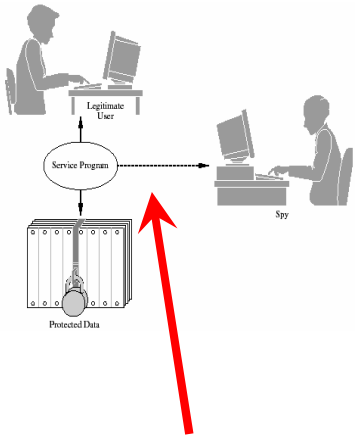
Zugriffsrechte Subjekt Zugriff Objekt

Informationskanäle

IIG Telematik

Kanäle: Wege, über die Information fließt

- **legitime Kanäle** werden von Subjekten i. d. R. für Informationsaustausch benutzt
  z. B. Nachrichten und Parameter einer Funktion
- **Speicherkanäle** können von Subjekten gemeinsam benutzt werden
  z. B. Dateien und Datenbanken
- **Verdeckte Kanäle** („*covert channels*"): nicht für Informationsaustausch vorgesehene Kanäle, die jedoch dazu missbraucht werden können
  - werden von „Betrachtern" nicht bemerkt!



Verdeckter Kanal

*-Sicherheit und Datenschutz

IIG Telematik

Funktionssicherheit („safety")

Nimmt das System keinen unzulässigen Zustand an, ist es **funktionssicher.** Die Ist- und die spezifizierte Soll-Funktionalitäten stimmen überein

Informationssicherheit („security")

Nimmt ein funktionssicheres System nur Zustände an, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen, ist es **informationssicher**

Datensicherheit („protection")

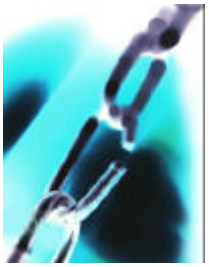
Nimmt ein funktionssicheres System nur Zustände an, die zu keinem unautorisierten Zugriff führen, ist es **datensicher**

Datenschutz („privacy")

Fähigkeit eines Nutzers, die Weitergabe von persönlichen Informationen zu kontrollieren

Fünf Aspekte der Sicherheit

IIG Telematik



Schutzziel („security goal“)
Stellt eine Soll-Funktionalität des Systems dar

Bedrohung („threat “)
Bestimmte Ereignisse oder Reihefolge von Aktionen, die zur Verletzung eines oder mehrerer Schutzziele führen könnten

Sicherheitslücke („vulnerability“)
Schwachstelle verschiedener Art, durch die eine Bedrohung für die Sicherheit des gesamten Systems entsteht
z. B. Buffer-Overruns, Fragment-Overwriting

Angriff („attack“)
Wenn ein Angreifer Anlass zu einer Bedrohung gibt und eine Sicherheitslücke ausnutzt, führt sein Angriff zu einer möglichen Gefährdung der Sicherheit

Sicherheitsmechanismus („security service“)
Dienst, der ein bestimmtes Schutzziel durchsetzt
– dieser kann u. a. durch kryptographische Algorithmen oder Hardware realisiert werden

Relevante Schutzziele in Kürze

IIG Telematik

Authentifizierung („authentication“)
Überprüfung der vom Benutzer vorgegebenen Identität bei der Systemanmeldung

Autorisierung („authorization“)
Recht eines Subjekts, gewisse Objekte zu verwenden

Vertraulichkeit („confidentiality“)
Stellt sicher, dass an allen Verbindungsstellen der Datenverarbeitung die erforderliche Geheimhaltung durchgesetzt wird, um eine nicht autorisierte Offenlegung zu verhindern

Integrität („integrity“)
Schutz der Genauigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden

Zurechenbarkeit („accountability“)
Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden

Verfügbarkeit („availability“)
Dienste sollen verfügbar sein und korrekt funktionieren

Mögliche Bedrohungen („STRIDE“)

IIG Telematik

Nachahmung einer fremden Identität („Spoofing“)

Illegale Beschaffung der oder den illegalen Zugriff auf die Authentifizierungsinformationen einer anderen Person

Unbefugte Änderung von Daten („Tampering“)

Böswillige Änderung von Daten

Abstreitbarkeit („Repudiation“)

Nutzer verweigert Durchführung einer Aktion, ohne dass andere Teilnehmer ihm dies nachweisen können

Informationsenthüllung („Information disclosure“)

Offenlegen von Informationen gegenüber Personen, die eigentlich keinen Zugriff darauf haben

Dienstverweigerung („Denial-of-service“)

Nutzung eines Diensts für zugelassene Nutzer zeitweise unbrauchbar

Anhebung der Berechtigungen („Elevation of rights“)

Erhält ein unberechtigter Benutzer privilegierten Zugriff, der die Gefährdung oder eventuelle Zerstörung einer ganzen Systemumgebung ermöglicht

Bedrohungen und Schutzziele in Beziehung gebracht

IIG Telematik

Schutzziele	Nachnahme der Identität	Unbefugte Änderung	Abstreit-barkeit	Enthüllung	Dienstver-weigerung	Erhöhung der Berechtigungen
Vertraulichkeit	x	x		x		
Integrität	x	x				x
Zurechenbarkeit	x	x	x	x		
Verfügbarkeit					x	
Autorisierung	x				x	x

Bedrohungen werden meistens kombiniert, um einen Angriff auszuüben!

Sicherheitsmechanismen zur…

IIG Telematik

Authentifizierung

Grundlegender Mechanismus zur Überprüfung der von einem Subjekt vorgegebenen Identität

Integrität

Sichert, dass Daten während der Übertragung oder Speicherung nicht (unbefugt) modifiziert werden

Vertraulichkeit

Gewährleistet die Geheimhaltung von Daten

Autorisierung

Auf Authentifizierung basierter Dienst, der einem Subjekt die Rechte, die es besitzt, zuschreibt

Zurechenbarkeit

Entscheidet Fragen bezüglich Abstreitbarkeit

Diese Mechanismen werden durch Sicherheitsprotokolle mit Hilfe kryptographischer Algorithmen realisiert

Ein Blick auf kryptographische Algorithmen

IIG Telematik

Überwiegende Verwendungszwecke

- **Verschlüsselung** von Daten: Umwandlung von Klartext in Chiffretext und umgekehrt
- **Signierung** von Daten: Signatur und Verifikation der Authentizität des Senders einer Nachricht durch so genannte *digitale Signaturen*
- einige Algorithmen können für beide Zwecke verwendet werden, wobei die Performance und der Grad von Sicherheit möglicherweise dementsprechend variiert

Abgrenzung der kryptographischen Algorithmen

- in *symmetrischer Kryptographie* wird ein und derselbe Schlüssel verwendet
- in *asymmetrischer Kryptographie* wird ein Schlüsselpaar verwendet der private und der öffentliche Schlüssel
- Hash-Funktionen verwenden keine Schlüssel, sondern „one-way“ Funktionen

Kryptographische Verfahren sind die grundlegenden Bausteine für die Realisierung von kryptographischen Protokollen

Sicherheitsprotokolle

IIG Telematik

Definition

- Reihefolge von Nachrichten, deren Ziel die Schaffung einer Sicherheitsbeziehungen zwischen Kommunikationspartnern ist

Anwendungen

- Schlüsselaustausch
- Authentifizierung, wobei es zu unterscheiden ist zwischen
  - **Nachricht** („message authentication“): Empfänger einer Nachricht kann überprüfen, ob sie von einem bestimmten Sender generiert und nicht modifiziert worden ist
  - **Entität** („entity authentication“): erlaubt Kommunikationspartnern, ihrer Identität zu überprüfen
- Vertragsschließung und nicht Abstreitbarkeit der durchgeführten Transaktionen
- Erwerbung der Zugriffsrechte auf entfernte Ressourcen

Techniken

- Um die Ziele zu erreichen und potentielle Angriffe zu vermeiden, werden verschiedene Techniken verwendet, u. a.
  - *Challenge-response* durch „nonces“
  - *Zeitstempel* („timestamps“)

Gliederung

IIG Telematik

Neuer Trend: Sicherheit wird ein Softwareproblem

IIG Telematik

Ursache	Trend	1992-94*	2001*
Benutzerfehler	↑	98	176
Synchr. Patches	↑	100	175
Hardware	↔	49	49
System/Software	↓	15	14
Software-inkonsistenzen	↑	18	260
Attacke	↑	5	303

* Minutes (Mio. von Kunden Minuten/Monat)

Sicherheitsfehler #1: Bufferoverflow

IIG Telematik

Problem

Datenpuffer, der über seine Grenze hinaus gefüllt werden kann

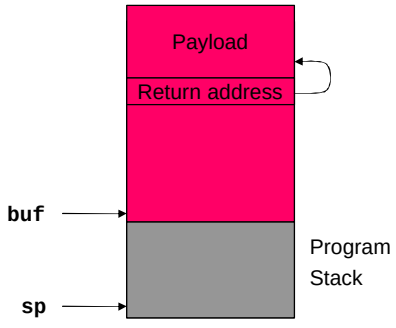
Exploit

das unkontrollierbare Überschreiben kann zum "Programmabsturz", aber auch zur Ausführung böswilligen Codes führen

Beispiel

```
char buf[100];
…
gets(buf);
```

- Angreifer gibt langen Input und überschreibt dadurch die Rücksprungadresse
- Rücksprung aus der Funktion übergibt **böswilligem Code** die Kontrolle



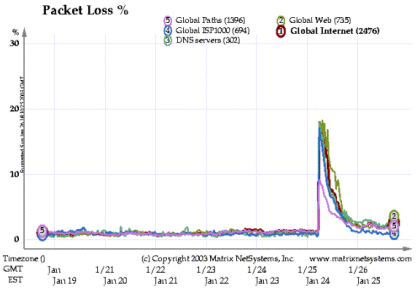
Bufferoverflow: MS-SQL Slammer Wurm

IIG Telematik

25. Januar 2003

MS-SQL Server zur Verteilung von „Würmern“ ausgenutzt

- u. a. Bufferoverflow-Schwachstellen und böswilliger Code
  z. B. Code Red
- Ausdehnung aufs gesamte Netz
  innerhalb von 10 Minuten



Patches

Man kann sich nicht auf Nutzer verlassen

- Patches für Schwachstellen waren bereits seit 6 Monaten verfügbar
- Microsofts eigene Server wurden ebenfalls infiziert

Sicherheit

Werkzeuge zur automatischen Erkennung Würmern?

Softwareproblem: Mögliche Lösungen

IIG Telematik

Ausschalten aller ausführbaren Inhalte

- diese können aber nützlich sein
  z. B. automatischer Kalender auf einer Webseite
- programmierbare Komponenten erlauben das Upgrade bestehender Software
  - codecs, elisp, allg. patches
- Sicherheitsgebot: „least privilege“
- das Ausschalten ausführbarer Inhalte ist an sich ein Angriff auf Verfügbarkeit

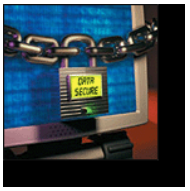
Auf böswilligen Code scannen?

- basierend auf syntaktischen Signaturen
  - lediglich „pattern-matching“
  - das Muster ist bereits vorher bekannt
  - „virus kits“ erleichtern das Verschleiern von Viren
- Lösungen sollen unerwünschtes Verhalten verhindern, ohne das „gute“ Verhalten ausschließen zu müssen

Neuer Trend zu Sicherheit: Softwarebasierte Sicherheit (SBS)

Ziel der SBS

- Sicherheitsrichtlinien sollen trotz aller Bedrohungen und Sicherheitslücken stets eingehalten und durchgesetzt werden



Sicherheitsrichtlinien („security policies“)

- Regeln zur Entscheidung, ob eine bestimmte Reihefolge von Aktionen stattfinden darf
- Sicherheitsrichtlinien definieren erwünschtes Verhalten
- werden durch Hardware- und Softwaremonitore überwacht und durchgesetzt

Zu welchen Zeitpunkten kann man auf Sicherheitsprobleme eingehen?

- vor der Ausführung
  - analyze, reject, rewrite
- während der Ausführung
  - monitor, log, halt, change
- nach der Ausführung
  - roll back, restore, audit, sue, call police

Softwarebasierte Sicherheit: Mögliche Richtungen

Erkenntnis

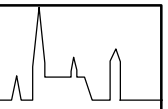
bestehende Annahme zu gegenwärtigen Sicherheitsmechanismen sind falsch

- Programme müssen keine „black-box“ sein

Was muss in Bezug auf Sicherheit gemacht werden?

1. Safety properties: kein unerwünschtes Verhalten tritt auf
2. Liveness properties: das erwünschte Verhalten wird stattfinden
3. Speicher- und Prozessisolierung
4. Sicherheit anhand von Datentypen
5. Vertraulichkeit und Integrität
6. Privatsphäre und Anonymität
7. Verfügbarkeit

Literatur



Grundlagen

Eckert, C.: „IT-Sicherheit“, 3. Auflage, Oldenbourg Verlag, 2003.

Gollmann, D.: „Computer Security“, John Wiley and Sons, 1999.

Müller, G., Rannenberg, K. (hrsg.): „Multilateral Security“, Addyson-Wesley, 1999.

Schäfer, G.: „Netzsicherheit“, dpunkt-verlag, 2003.

Schneider, F. B., Morrisett, G., Harper, R.: „A language-based approach to security“
http://www.cs.cornell.edu/Info/People/jgm/lang-based-security/finalcr.ps, 2000.

Umfeld

Definitionen der Sicherheitslandschaft
http://www.microsoft.com/germany/ms/security/guidance/modules/secmod133.mspx