Informations- und Netzwerksicherheit: Anforderungen, Ziele und Konzepte

Motivation

Bedrohungen

Fundamentale Anforderungen

Modelle

Schwachstellen in IT-Systemen

Einige Fallbeispiele

Warum ist Sicherheit überhaupt ein Thema?

- Verteilte Informatiksysteme sind kritische Ressourcen
- Globalisierung der Kommunikationsbedürfnisse und -infrastruktur (Internet!)
- Neue Formen der "grenzüberschreitenden" Kooperation: E-mail, Informationssysteme, Desktop-Conferencing
- Offene Systeme
- Daraus folgt: Erhöhung des Angriffs- und Schadenpotentials
- Physische Sicherheit kann nicht mehr gewährleistet werden.
- Wem vertraue ich, wem nicht?
- -> Vertrauen als wichtige Ressource, Ziel eines Sicherheitsdienstes

ZISC

Bedrohungen

- Bedrohungen zufälliger Art:
  - Stromausfall
  - Benutzerfehler
  - Systemfehler (Software, Hardware, Übertragungsfehler)
- gezielte Bedrohungen:
  - „Hacker“
    - Die Kreativen
    - „script kiddies“
  - kriminelle Einzeltäter
    - Elektr. Bankraub
    - Insider
  - kriminelle Organisationen
  - Behörden

Motivation der Angreifer:

- Neugierde, Kick
- Gesteigertes Selbstwertgefühl
- Mitläufertum, Protesthaltung
- Kriminelle Bereicherung
- Racheakte
- Unterstützung oder Vorbereitung von illegalen Geschäften
- Geheimdienstliche Tätigkeit
  - Militärisch
  - Wirtschaftlich
- Verdeckte Ermittlung

Was kann ein Angreifer tun?

- Mithören
- Nachrichten senden
  - Oft mit einem nicht authentischen Absender (IP-Adresse, e-Mail-Adresse)
- Aufgefangene Nachrichten unverändert noch einmal senden
- Aufgefangene Nachrichten verändern und absenden
- Code mit speziellen Eigenschaften erzeugen
  - Viren: Modifizieren Funktion eines „Wirtsprogramms“
  - Würmer: Verwenden eine Sicherheitslücke und ein Transportmittel, um sich fortzupflanzen
  - Trojanische Pferde: Fremder Code wird eingeschleust und von unbedarften Benutzern oder Programmen ausgeführt

- Gegenüber einem Kommunikationspartner (Mensch, IT-System, Prozess) eine falsche Identität annehmen
- Zugangsrechte erwerben, auf die er keinen Anspruch hat
- Bewusst kritische Systemressourcen überbeanspruchen (Speicher, CPU, Kommunikationskanäle, Datenstrukturen, ...)

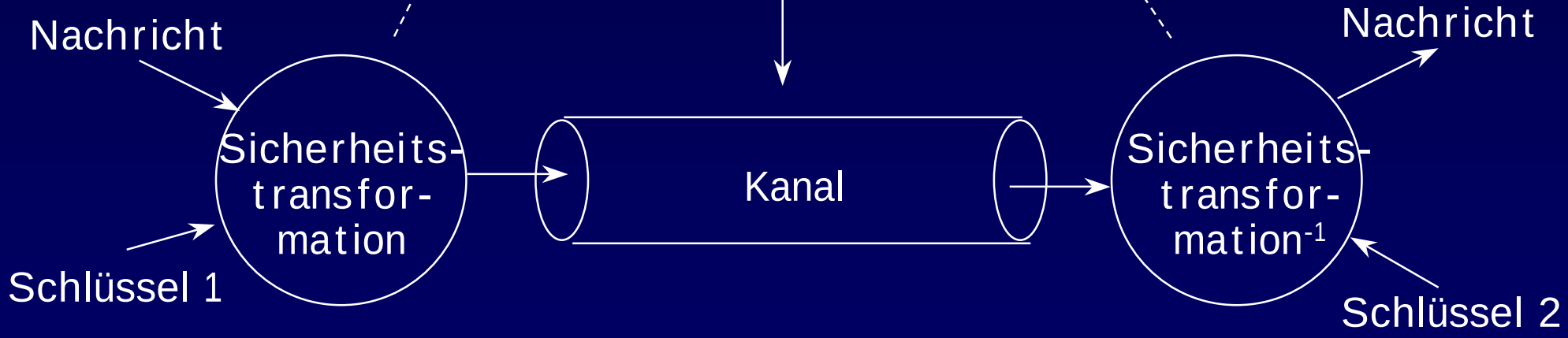
Fundamentale Anforderungen

- Verfügbarkeit
- Authentizität und Integrität von
  - Information
  - Benutzer
  - Hardware
  - Software
- Vertraulichkeit

- Beweisbarkeit von Vorgängen gegenüber Dritten
- Überwachung des Zugriffs zu Ressourcen
- Feststellen des ordnungsgemässen Funktionieren eines Systems

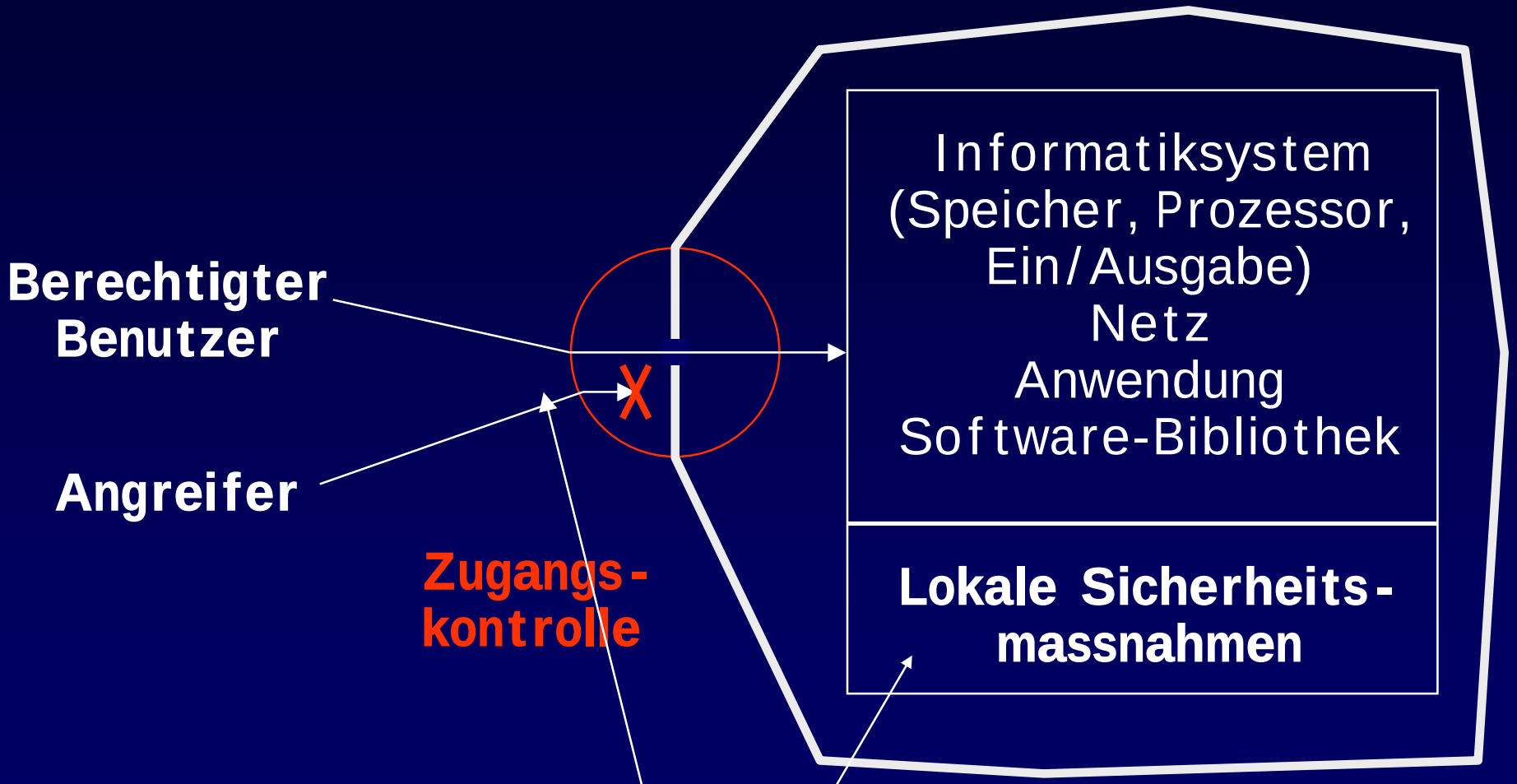
Modell I:
Sichere Kommunikation über einen unsicheren Kanal

Angreifer
- hat vollen Zugriff auf den Kanal
- kennt Mechanismen/Protokolle



Sender **Empfänger**

Modell II: Schutz durch Zugangskontrolle



intrusion detection, event logging, access control

Konkrete Beispiele von Sicherheitsproblemen („Incidents“)

IEEE 802.11b Wireless LAN

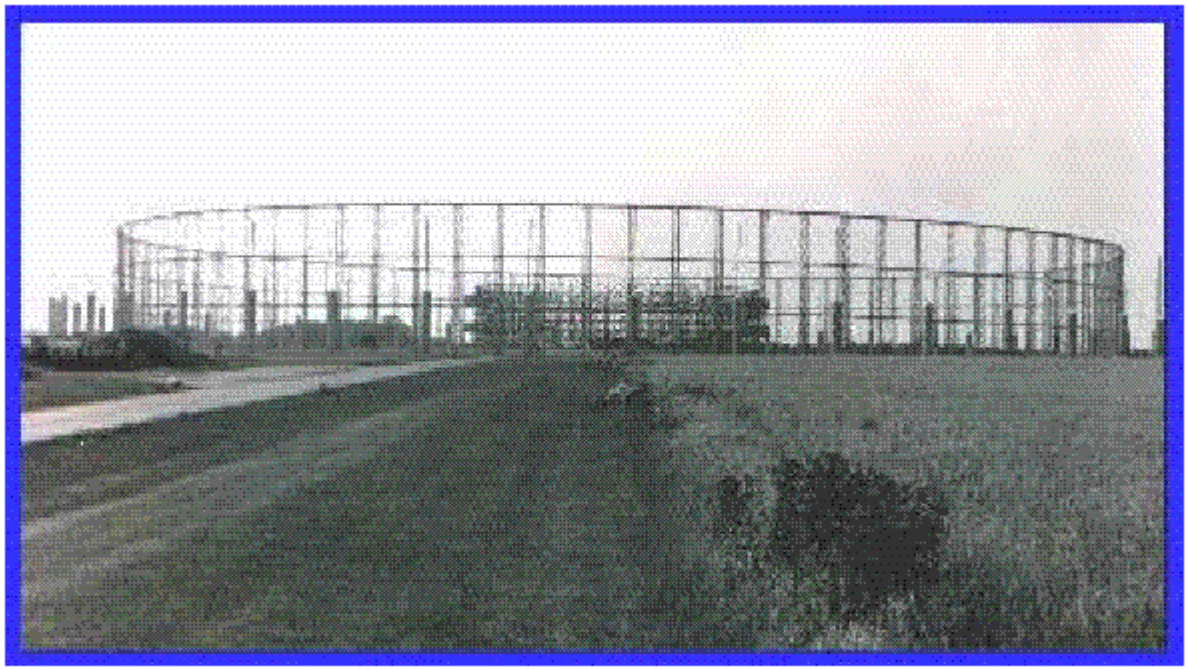
- IEEE 802.11b: Coole Wireless LAN-Loesung für Mobilitätsfreaks
- Problem: Wireless Link kann von jedermann mitgehört werden
- Bericht des Kassensturz (CH), ca. Frühjahr 2001
- Lösungsansätze
  - Verschlüsselungsfunktion von IEEE 802.11b verwenden („Wired Equivalent Privacy“, WEP)
  - Praktikabilität?
  - Sicherheit von WEP ist ungenügend, siehe http://www.sans.org/infosecFAQ/wireless/equiv.htm

→ Ende-zu-Ende Verschlüsselung notwendig

Echelon

- Systematische Beobachtung internationaler elektronischer Kommunikation
  - HF Radio
  - Mikrowellenkommunikation
  - Unterseekabel
  - Satellitenkommunikation
- Analyse der aufgefangenen Signale
  - Dekodierung nach Typ (Sprache, e-mail, Fax, Telex, etc.)
  - Suche nach Schlüsselwörtern (Watch List)
  - Sprechererkennung (Spracherkennung technisch noch schwierig)
  - Verkehrsanalyse
- Verwendungszwecke: Militärisch, Strafverfolgung, Wirtschaftsspionage

→ http://www.europarl.eu.int/stoa/publi/pdf/98-14-01-2_en.pdf

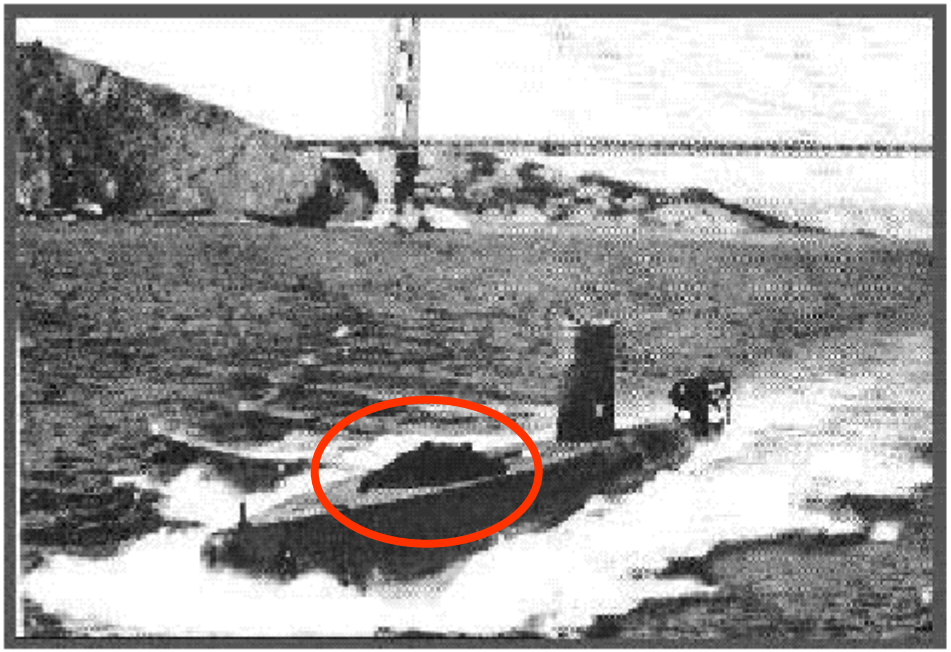


High frequency radio interception antenna (AN/FLR9)

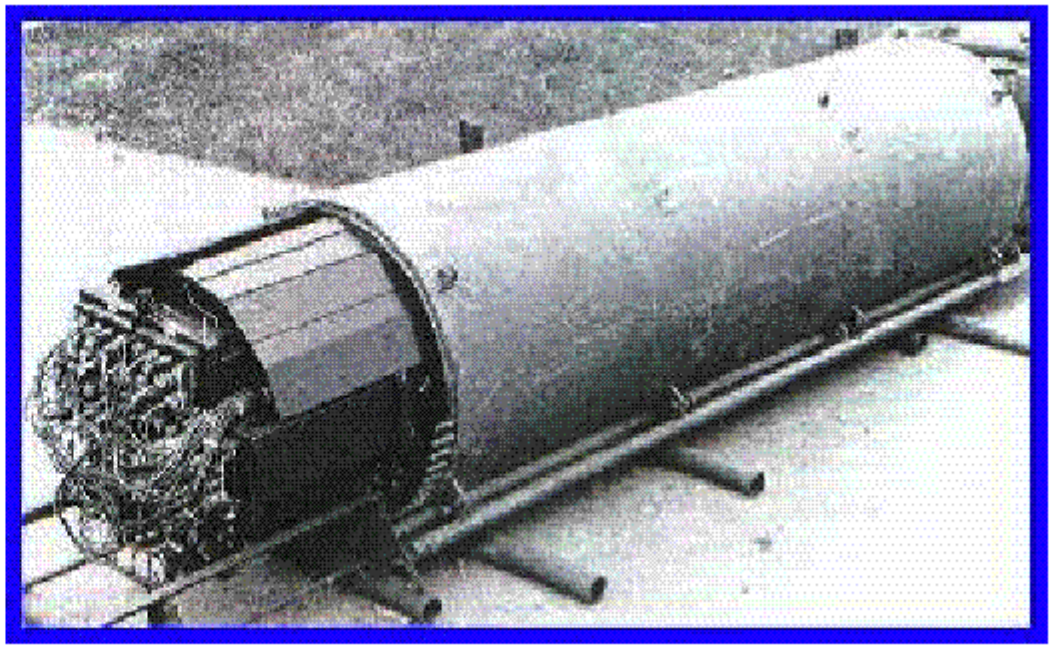
Satellite ground terminal at Etam, West Virginia, connecting Europe and the US via Intelsat IV

GCHQ constructed an identical "shadow" station in 1972 to intercept Intelsat messages for UKUSA

USS Halibut, 1971 und 1972



USS Halibut with disguised chamber for diving



Cable tapping pod laid by US submarine off Khamchatka

Zwei recherchierte Fälle

- Thomson CSF and Brazil, 1994: $1.3 billion surveillance system for the Amazon rain forest
  - Raytheon gewinnt schliesslich gegen Thomson CSF
  - Raytheon ist Dienstleister der NSA für Echelon‘s Satellitennetz
  - "the Department of Commerce worked very hard in support of U.S.industry on this project".
- Airbus Industrie and Saudi Arabia
  - „ ... from a commercial communications satellite,NSA lifted all the faxes and phone calls between the European consortium Airbus,the Saudi national airline and the Saudi government.“
  - Boeing gewinnt schliesslich den Auftrag über US$ 6 Mia

Distributed Denial of Service Attack (DDoS)

- Mehrstufige Attacke
  - Angriff auf einige 10 schwach geschützte Rechner
  - Installation von DDos Software auf diesen Rechnern
  - Konzertierte Denial of Service Attacke (TCP SYN, ICMP oder UDP Flooding) auf eigentliche Zielsysteme
- Beispiele:
  - ETH Zürich, Univ. Zürich, Dezember 1999
  - Yahoo, e-Bay, Amazon, etc. Februar 2000
  - s. auch: http://grc.com/dos/intro.htm ☺
- „Tribe Flood Network“ (TFN), Code Red, Nimda

Aufzeichnung auf meinem privaten PC

Datum		Zeit	Absender	Ziel (mein Rechner)	Anwendung
Sep	23	09:01:38	SRC=195.223.249.110	DST=195.162.177.103	DPT=80
Sep	23	09:01:41	SRC=195.223.249.110	DST=195.162.177.103	DPT=80
Sep	23	09:49:23	SRC=195.1.206.2	DST=195.162.177.103	DPT=80
Sep	23	09:49:25	SRC=195.1.206.2	DST=195.162.177.103	DPT=80
Sep	23	10:03:13	SRC=195.151.183.210	DST=195.162.177.103	DPT=80
Sep	23	10:25:38	SRC=195.162.176.196	DST=195.162.177.103	DPT=22
Sep	23	10:37:52	SRC=195.195.152.150	DST=195.162.177.103	DPT=80
Sep	23	10:37:55	SRC=195.195.152.150	DST=195.162.177.103	DPT=80
Sep	23	14:44:32	SRC=195.250.250.52	DST=195.162.177.103	DPT=80
Sep	23	15:07:44	SRC=200.10.106.11	DST=195.162.177.103	DPT=80
Sep	23	15:07:47	SRC=200.10.106.11	DST=195.162.177.103	DPT=80
Sep	23	16:22:48	SRC=213.74.12.114	DST=195.162.177.103	DPT=23
Sep	23	16:22:51	SRC=213.74.12.114	DST=195.162.177.103	DPT=23
Sep	23	16:25:57	SRC=145.236.34.66	DST=195.162.177.103	DPT=21
Sep	23	16:26:00	SRC=145.236.34.66	DST=195.162.177.103	DPT=21
Sep	23	17:26:15	SRC=195.34.31.105	DST=195.162.177.103	DPT=80
Sep	23	17:26:31	SRC=195.34.31.105	DST=195.162.177.103	DPT=80
Sep	23	17:26:56	SRC=195.34.31.105	DST=195.162.177.103	DPT=80


BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER