Sicherheit für Dienste in mobilen Endgeräten

Märkte und Anwendungen für UMTS

Münchner Kreis Fachkonferenz: 14.November 2001

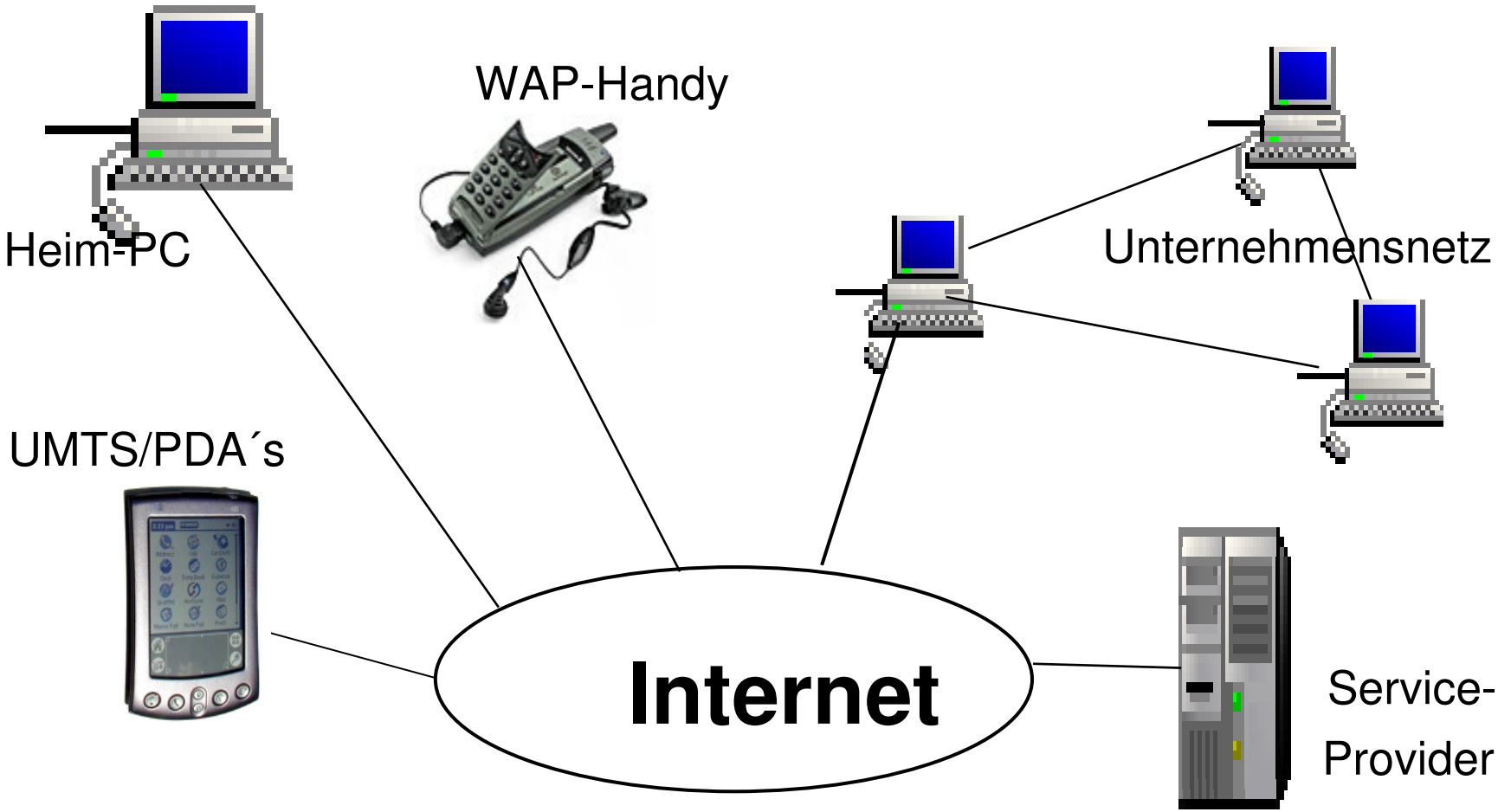
Prof. Dr.-Ing. Heinz Thielmann, Fraunhofer Institut SICHERE TELEKOOPERATION (SIT)

Prof. Dr. Claudia Eckert, Fraunhofer Institut SICHERE TELEKOOPERATION (SIT) und TU Darmstadt, FG Sicherheit in der Informationstechnik

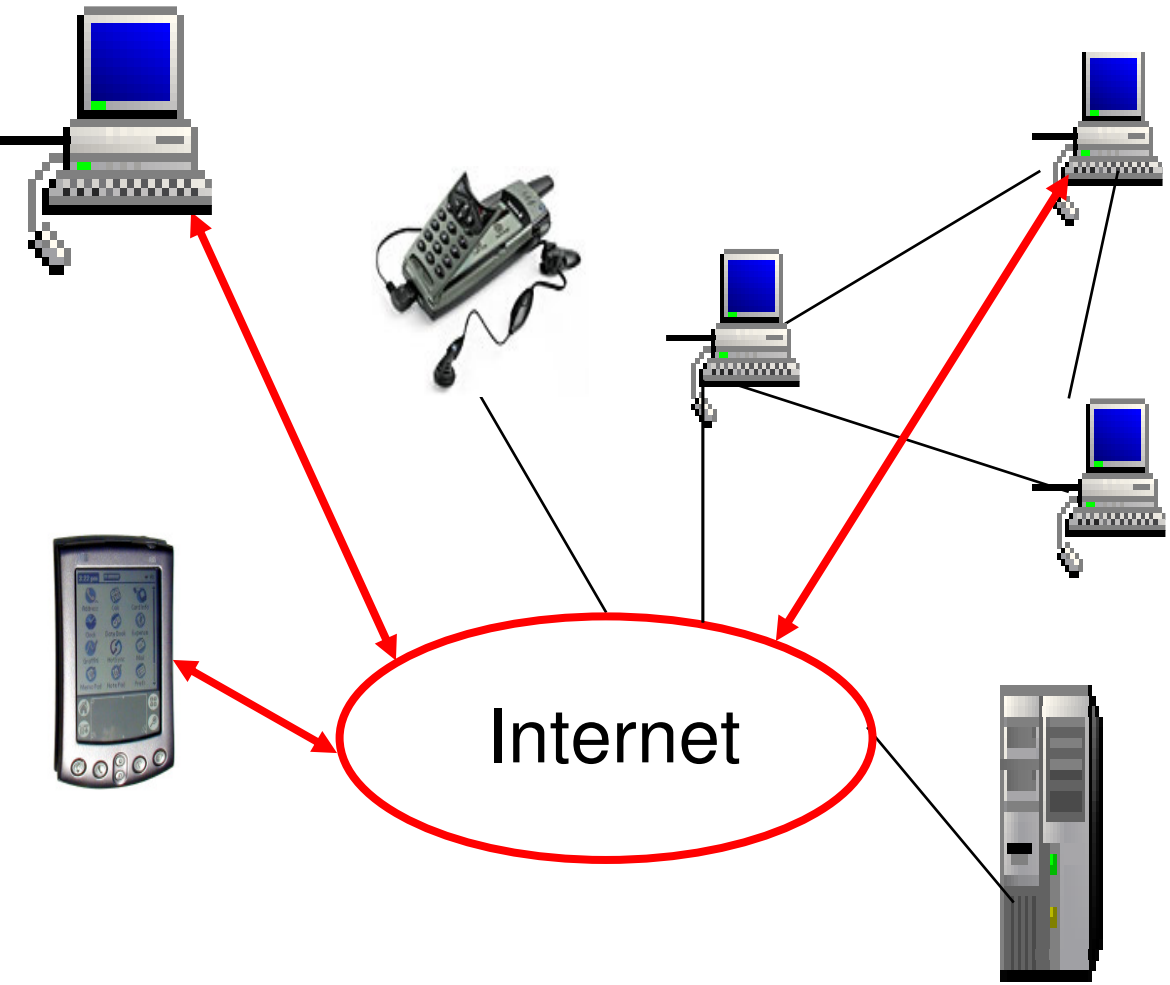
Prof. Dr. Uwe Baumgarten, TU München, Fakultät für Informatik

Fraunhofer Institut Sichere Telekooperation

Vernetzte Infrastrukturen



Nutzungsszenarien



- Versenden und Empfangen von E-Mails
- Web-Dienste: Informationen anbieten, sammeln
- Download von Software Spiele, Musik, Updates ...
- Einkaufen über das Netz Bücher, Tickets

Zusammenwachsen von:

Unterhaltungselektronik, Datenverarbeitung, Telefonie

- **Konsequenz:** starke Vermischung von privaten und beruflichen Belangen
- **unterschiedliche Sicherheitsbedürfnisse**:
  - Schutz der Privatsphäre, Recht auf Privatheit, Datenschutz, Anonymität
  - Vertraulichkeit, Integrität und Verfügbarkeit der Geschäftsdaten, Wirtschaftlichkeitsaspekt
- sehr unterschiedlicher Bedarf an Aufwand für Sicherheit, kontextabhängig

Beispiele für neue Formen der Telekooperation

Kooperationen zwischen Bürgern und Unternehmen: **C2B, B2C**

- Web-Services:
  - Einkaufen von Konsumgütern auch des täglichen Lebens, automatische Lagerhaltung
  - Reise und Touristik: ortsgebundene Angebote, Gesamtlösungen (Hotel, Auto, Kultur,...)

Kooperationen zwischen Bürgern/Unternehmen und der Verwaltung: **C2G, G2C, B2G**

- E-Government, Stadt- und Verkehrsplanung:
  - Einwohnermeldeamt, KfZ-Anmeldung, Gewerbeanmeldung
  - aktuelle Informationen, z.B. Bebauungspläne, Bauauskunft, -genehmigungsverfahren
  - Koordinierung von Ausschreibungen und direkte Weiterverarbeitung von Anträgen

Beispiele für neue Formen der Telekooperation (cont.)

Kooperationen innerhalb eines Unternehmen

- Mobilität:
  - mobile Geschäftsabwicklungen (Außendienstmitarbeiter, Geschäftsreise, ...),
  - Zugriff auf Unternehmensdaten aus verschiedenen Arbeitskontexten:

    beim Kunden, beim Geschäftspartner, von unterwegs, von zuhause

- Globalisierung der Arbeitsabläufe:
  - direkte Zugriffe auf räumlich verteilte Unternehmensdaten, ERP-Software etc.
  - virtuelle kooperative Arbeitsumgebungen: gemeinsames Projektmanagement,

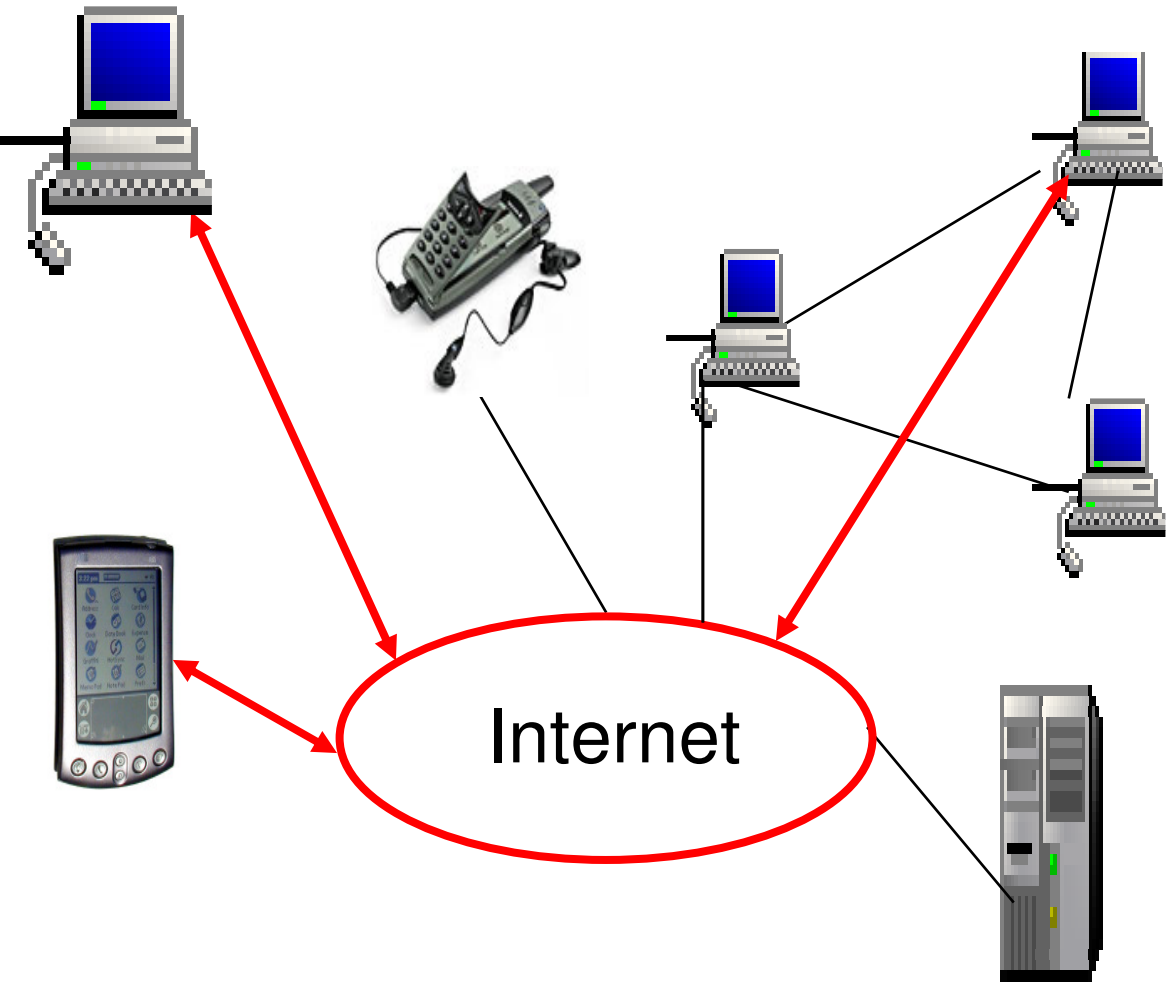
    gemeinsame IT-Infrastrukturen, Ressourcen

Beispiele für neue Formen der Telekooperation (cont.)

Kooperationen zwischen Unternehmen: **B2B**

- E-Commerce:
  - vereinfachtes Bestell- und Beschaffungswesen, u.a. Sammelbestellungen mit Rabatten
  - optimierte Lagerhaltung, just-in-time Einkäufe
- B-Commerce:
  - Vertragsabschlüsse über das Internet, rechtsverbindlich, vertraulich
- Globalisierung, u.a. Fernzugriffe:
  - Fernwartung, automatisches Updaten, Fernkonfigurierung (z.B. Firewalls)
  - Fernüberwachung von Unternehmensinfrastrukturen, z.B. Intrusion Detection
  - Application Service Providing (ASP): z.B. externe Verwaltung sensibler Informationen

Problembereich Mobile Internet



- Vertraulichkeit?
  Abhören! Sniffer
- Integrität?
  Modifizieren!
- Privatsphäre?
  Profilbildung!
- Authentizität?
  Maskierung! Spoofing

Fraunhofer SIT Institut Sichere Telekooperation

Offene Problembereiche (u.a.)

Einfache Nutzbarkeit:

- Integrierte Sicherheitsdienste, einfache Oberflächen

Wirksamer Schutz gespeicherter Daten:

- Verschlüsselte Dateien, differenzierte Kontrollen

Schlüsselmanagement:

- Schlüsselerzeugung, sichere Schlüsselverwaltung

Vertrauenswürdige Systemsoftware:

- zuverlässig und sicher vor Manipulationen

Wunsch: vertrauenswürdiges Sicherheitsmodul: z.B.:**PDA**

Personal Digital Asistant (PDA)

Charakteristika:

- Klein, leicht, beschränkte Ressourcen
- Benutzungsschnittstelle: Stift, Tastatur
- Kommunikation: Modem, Funk, Bluetooth, ...

Anwendungen: u.a.

- Adressbuch, Terminplaner
- Pocket Office: Word, Excel, ...
- E-Mail, Surfen via HTTP
- Mobiler Code: Java Applets, ActiveX

Bedrohungen

Portabilität:

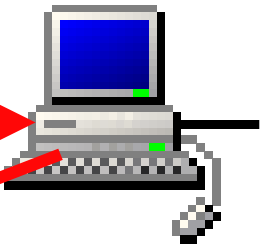
- Diebstahl,
- Datenverlust,

Zugriff nach Diebstahl

Vernetzung:

- Abhören, Profile
- Zugriff von Außen

Abhören



Zugriff auf offene Ports

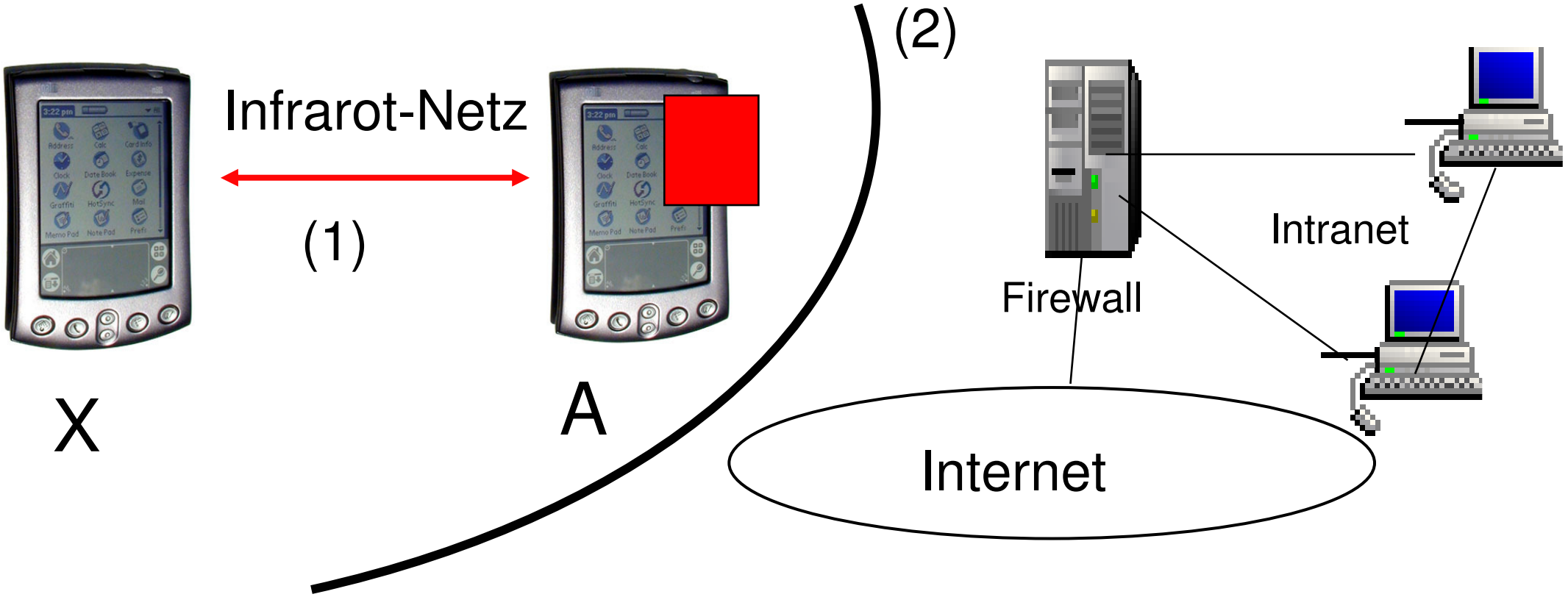
Downloads, Mails:

- Viren,
- Trojanische Pferde
- Einschleusen von Viren in Unternehmensnetze

Bsp: Angriffsszenario

(1) X transferiert über Infrarot-Netz Virus in PDA A

(2) A ist außerhalb des Intranetzes



Persönliches Sicherheitsmodul

Sicherer, persönlicher Datenspeicher:

- Geschützte private, Firmen-interne, Kunden-bezogene Daten
- Automatisches Ver- und Entschlüsseln
- Kontrollierte Zugriffe und kontrollierbare Wechselwirkungen

Vertrauenswürdiger Benutzerrepräsentant:

- Sichere e-Aktionen (-Commerce, -Government, -Business)
- Vertrauenswürdige BS-Software, evaluiert
- Sicheres Management von Schlüsseln, Zertifikaten, ...

Persönlicher Informations - Agent:

- Gewährleisten der Privatsphäre
- Autonome Aktionen abgestimmt auf Benutzerprofil
- Sicheres Nachladen, Ausführen von fremdem Code

Wunsch:

- Wirksame Zugangs- und Zugriffskontrollen
- Automatisches Management kritischer Daten
- Vertrauenswürdige Betriebssoftware

Wirklichkeit?

Konsequenzen für die IT-Sicherheit?

- Kommunikation mit vertrauenswürdigem Partner sicherstellen!

  Notwendig: starke Authentifikationsmechanismen
  - Smartcards, biometrische Verfahren, Benutzerakzeptanz?
  - Multi-Point Verbindungen: skalierbare Lösungen

- Vertrauliche Information darf nur in berechtigte Hände gelangen!

  Notwendig: starke Verschlüsselungsverfahren,
  - Aushandeln, Abstimmen geeigneter Verfahren
  - automatisches Schlüsselmanagement (kein fehleranfälliges Verwalten von Passworten!)
  - sichere, vertrauenswürdige Speicherung von Schlüsseln, wo? Festplatte?!

- Verbindliche Abwicklung von Geschäften!

  Notwendig: digitale Signaturen,
  - PKI auch für heterogene Umgebungen
  - Haftungsprobleme, rechtliche Rahmenbedingungen, Standardisierung

Konsequenzen für die IT-Sicherheit? (cont.)

- Korrekte, integere Daten zur Verfügung stellen!

  Notwendig: Zugriffskontrollen, abgestufte Konzepte
  - Manipulation nur durch berechtigte Nutzer, Sicherheitspolicy erstellen
  - Sichere Verwaltung der Zugriffsrechte, Speicherung auf Festplatte?!

- Schutz der Privatsphäre gewährleisten!

  Notwendig: Anonymität gegenüber Dritten
  - Vermeidung von Datenspuren (z.B. Referer-Infos, Cookies, Adressinformationen)
  - Einsicht und Kontrolle über gespeicherte, personenbezogene Daten

- Mehrseitige Sicherheit durchsetzen!

  Notwendig: Schutzbedarf nicht nur an Daten/Objekten orientieren
  - unterschiedliche Interessen/Bedürfnisse der Beteiligten berücksichtigen
  - Aushandeln, Abgleichen von Sicherheitspolicies, gemeinsame Profile finden

Realität heutiger Systeme?

Fast täglich Meldungen über Sicherheitsprobleme/Angriffe
- **Wöchentlich:** Bekanntgabe von Schwachstelle in existierender Betriebssoftware
- **Täglich:** ca. 5 neue Viren/Würmer

Studie (Computer Economics): Schäden durch Viren etc. 17.1 Milliarden $ (10.7 in ´99)
- Schäden durch I Love You- Virus: über 8.7 Milliarden $
- Schäden durch Code-Red Wurm allein in Deutschland: über 500 Millionen DM

Studie Gardner Group: 86% der Befragten haben Sicherheitsbedenken,
Ablehnung von E-Commerce, E-Government, ASP- Lösungen
- Beispiel: Hacken des Homebanking Computers der Hypo-Vereinsbank:
  - 1.5 Millionen Onlinebuchungen mit Geheimnummern abgefangen,
  - direkter Zugriff auf Kundendaten
- Verlust durch Kreditkartenmissbrauch bei Online Händlern in 2000: 1.6 Milliarden $
  Umfrage: nur ca 30% der Online-Händler setzen Sicherheitstechniken ein!

Studie Meta-Group: Umsatzeinbußen von 10 Milliarden $ im B2B-Bereich
5 Milliarden $ im B2C- Bereich

Zwischenbilanz?

- **Sicherheitslösungen für Standardprobleme existieren**:
  - E-Mail Verschlüsselung, verschlüsselte Kommunikation (SSL/TLS, IPSec,...)
  - digitale Signatur und Zertifikate, PKI
  - Firewalls, Content Filterung, Intrusion Detection Systeme (IDS), Virenscanner

Probleme: u.a.

- Mangelhafte Integration/Abstimmung der einzelnen Mechanismen, z.B.
  - Filterung verschlüsselter E-Mails in zentralen Firewalls?
  - Inkompatible Verschlüsselungsverfahren und Zertifikat-Formate?

- Fehlende Integration von Sicherheitsmechanismen in Geschäftsprozesse,
  - Absicherung einzelner Arbeitsschritte z.B. E-Mail,
  - Schutz der sensitiven Daten während des gesamten verteilten Arbeitsprozesses?!

- Langzeitarchivierung digital signierter Dokumente

- Sicherheitsprobleme durch vorkonfigurierte Anwendungssoftware: Paradigmenwechsel notwendig

- Mangelnde Akzeptanz von Sicherheitsprodukten, fehlende Benutzungsfreundlichkeit?!

Perspektiven für die IT-Sicherheit?

- **Notwendig** neue, erweiterte Sicherheitskonzepte:
  - verschiedene Sicherheitszonen innerhalb des Systems
  - Verschiedene Sicherheitslevels mit angepassten Maßnahmen (gering, ..., hoch sicher)
  - Abgestufte Sicherheitsmaßnahmen mit Failsafe-Konzepten

Perspektiven für die IT-Sicherheit? (cont.)

Mobilität: dynamisch wechselnde Arbeitsumgebungen

- Fernzugriffe auf Unternehmensdaten:

  lokale Verarbeitung im PDA in der Gastumgebung

- Zugriff auf Daten, Code in Gastumgebungen
- **Konsequenz:** mehrseitige Sicherheit
  - Policy der Gastumgebung

    (z.B. Kunde, Geschäftspartner, Firma, Behörde, Hotel, ...)
  - Policy des mobilen Endgeräts des Benutzer und

    Policy des Unternehmensnetzes

Perspektiven für die IT-Sicherheit? (cont.)

- **Notwendig:** neue Sicherheitskonzepte, integrierte Dienste
  - Automatischer Abgleich von Policies, Aushandeln von Verfahren
  - Kontextabhängige Rechtevergabe, dynamisch wechselnd
  - Weg vom Daten- hin zum sicheren Informations-Management

  über gesamte Wertschöpfungskette

Perspektiven für die IT-Sicherheit? (cont.)

Globalisierung und allgegenwärtiges, pervasives Computing

- Übergang von Ende-zu-Ende Sicherheit zu Multi-Point Sicherheit
- Kommunikation mit Vielzahl unbekannter,

  nicht vertrauenswürdiger Partner

Perspektiven für die IT-Sicherheit? (cont.)

Notwendig:

- Skalierbarkeit von Sicherheits-Mechanismen
- Ggf. stärkere Einbindung der Benutzer:
  Ausbildung, Weiterbildung unabdingbar
- Absicherung von Geschäftsprozessen, nicht nur einzelner Arbeitsschritte:
  integrierte Sicherheit, Systemsicherheit

Zitat G. Spafford:

„Using encryption on the Internet is the equivalent of arranging an armored car to deliver credit card information from someone living in a cardboard box to someone living on a park bench. „

Zusammenfassung

Sicherheitsprobleme heutiger Architekturen:

Integrität, Vertraulichkeit, Authentizität, Verbindlichkeit

Persönliches Sicherheitsmodul erforderlich!

PDAs könnten geeignete Basis sein

ABER: erhebliche Sicherheitsrisiken mit PDA-Betriebssoftware

Bedrohungen für Benutzer und seine Umgebung

Neue Architekturen/**Systemsoftware** notwendig!

Luca-Projekt mit Linux-basierter Lösung

Erste Schritte von **Wunsch** zu **Wirklichkeit**