Fraunhofer SIT

Tatort Internet

Claudia Eckert
Fraunhofer-Institut SIT, Darmstadt & München
Technische Universität München

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

By RANDY JEFFRIES / *Weekly World News*

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Fiktion oder Wirklichkeit?

smithereens!

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

puter crime is concerned, we've only seen the tip of the iceberg.

"The criminals who knocked out those three major online businesses are the least of our worries," Yabenson told *Weekly World News*.

"There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

"It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

"As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers."

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

"As dangerous as this technology is

scarier," Yabenson said.

"Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

"Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

"And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

"That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

Tatort Internet

Fraunhofer SIT

IT als Tatwaffe

- Überwachen, spionieren, fälschen, erpressen, stehlen, zerstören, betrügen, verletzen, **töten**

Neue Dimensionen des organisierten Verbrechens: Cybercrime

- **Allgegenwärtige IT**: immense Abhängigkeit von IT , hohe Verletzlichkeit, Erpressbarkeit!
- **Wer die IT-kontrolliert, hat Macht**

IT ist aber auch unverzichtbar für Maßnahmen der

- **Prävention, Aufklärung**, Gefahrenabwehr, zum Schutz

Tatort Internet

Fraunhofer SIT

Cybercrime als Geschäftsmodell

Handel mit Schwachstellen, Werkzeugen und BOT-Netzen

Fraunhofer SIT

Der „virtuelle Waffenhandel" mit Softwarefehlern, die dazu verwendet werden können, wichtige infrastrukturelle Regierungsnetzwerke auszuspionieren und anzugreifen, nimmt zu.

Quelle: McAfee Criminology Report 2007

Schätzung: Etwa fünf Prozent aller Rechner weltweit sind Zombies (~ 20 Mio.)
Quelle: Bericht des britischen Oberhauses über Sicherheit von Privatpersonen im Internet (Personal Internet Security, ISBN: 0104011386), 2007

- **Offener Handel mit Schwachstellen**
  - Hohe Prämien für Produkte namhafter Hersteller (Cisco, Microsoft, ...)
- **Angriffssoftware**
  - Eigene Schattenwirtschaft
  - **Jeder kann kaufen, mieten, nutzen!**
- **Beispiel BOT-Netz**
  - Zusammenschluss infizierter Rechner
  - Anmietung von BOT Netzen:
    ab 10$ für BOT-Netz pro Woche für Netz mit 5000-10000 Rechnern

Botnetze: sehr beliebter Angriff

Fraunhofer SIT

- 6-7 Millionen Rechner weltweit sind Zombies in Botnetzen
- 300.000 bis 400.000 davon gehören deutschen Internetnutzern
- Bis zu 120.000 Rechner steuert ein einzelner DOS-Angreifer

Quelle: BKA

Nicht die allmächtigen Russen waren es, sondern **ein Student, mit Bot-Netz**

Die Masse macht‘s
Viagra-Spam-Verbreitung über Botnetze

Fraunhofer SIT

Spiced **P**orc **a**nd **M**eat,
ohne jeglichen Nährwert

Anzahl der Spam-E-Mails	469.000.000
Klickrate der Empfänger	Bis zu 0,00001%
Umsatz hochgerechnet auf das ganze Botnetz **pro Tag**	**9.500$**

Quelle: Kanich et al.: Spamalytics: An Empirical Analysis of Spam Marketing Conversion, http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf,

Ebay für Sicherheitslücken

Fraunhofer SIT

Tatort Internet

Fraunhofer SIT

Beispiele „alltäglicher" Angriffe

Passwortknacken und Erpressen

Fraunhofer SIT

RainbowCrack 1.4
Am 17.08.2009 gab das Projekt RainbowCrack eine verbesserte Version 1.4 ihres Passwort-Crackers frei: Auf einem mit der Grafikkarte NVIDIA GForce 9800 GTX+ ausgestatteten PC prüft sie knapp 104 Milliarden NTLM-Hashwerte pro Sekunde – eine 40-prozentige Steigerung. Alphanumerische 10-Zeichen-Passwörter sind damit nach spätestens 1,5 Monaten geknackt.

Spektakulärer Hack

Erpresser verlangt zehn Millionen Dollar für ein Passwort

Der Diebstahl von 35 Millionen Rezeptverschreibungen von mehr als acht Millionen Patienten zeigt die Gefahren von Web-vernetzten Gesundheitsdatenbanken. Die Drohung des Erpressers: Zehn Millionen Dollar Lösegeld - oder er werde die Daten meistbietend verkaufen.

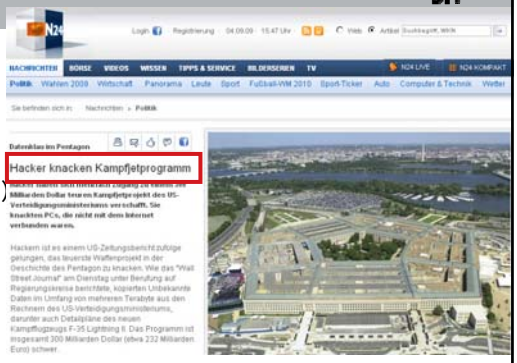
"Aufgepasst Virginia" war am 30. April mit einem Mal auf der Website einer staatlichen Gesundheitsbehörde in den USA zu lesen: "Ich habe Euren Scheiß!"

Hacken kritischer Infrastrukturen

Fraunhofer SIT

Kriminelle, Terroristische Akte:

- Transport und Verkehr
- Elektrizität (Öl, Gas, Strom)
- Finanz-, Geld- und Versicherungen
- Versorgung (Gesundheit, Wasser,…)
- Behörden, Justiz, Polizei, Militär



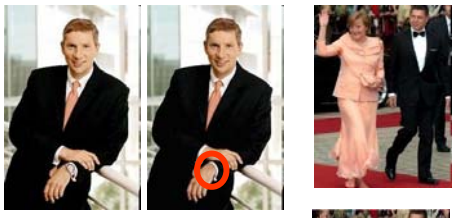
Ändern/Manipulieren/Fälschen

Fraunhofer SIT

- Vortäuschung falscher Sachverhalte durch Bildmanipulation

Ziele: u.a.

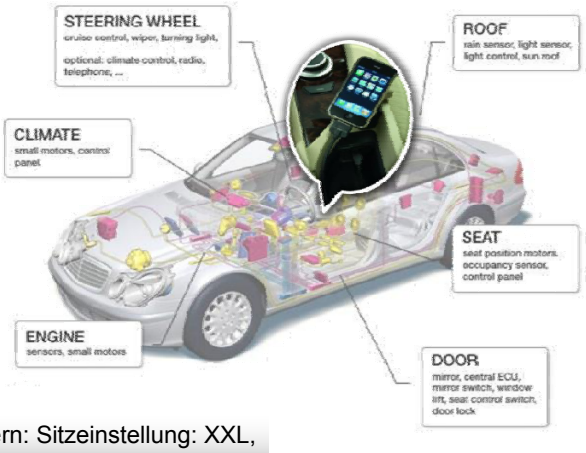
- Beweismaterial manipulieren
- Stehlen
- Öffentliche Meinung beeinflussen
- …



Heute noch nicht, aber

Fraunhofer SIT

sicherlich bald:
Angriffe auf Autos



„Mal sehen, Einstellung ändern: Sitzeinstellung: XXL, Heizung: 45°, Fahrzeugverriegelung: vollständig, Radio: max.Vol., Aktivierung: über 150km/h …“

Tatort Internet

Fraunhofer SIT

Datenspuren im Netz: Informationsbeschaffung: nie war es so einfach wie heute

Wirtschaftsspionage

Fraunhofer

Dumpster Diving

Tatort: Soziale Netze: facebook, StudiVZ, ...
Social Engineeering statt Dumpster Diving

- Informationen über Privat- und Geschäftsleben, werden von Spammer gesammelt
  - z.B. Geburtsdatum oder Lieblingstier
  - Passworten-Knacken ist damit viel einfacher

Sometimes, the greatest treasures are found beneath piles of trash.

Tatort Unternehmen

Spionage, Informationsweitergabe

- 2005: Verluste von 4,2 Mrd € in D ca. 50% des Gesamtschadens
- 89% unter Beteiligung von Insidern

Mittwoch, 19. August 2009, 12:00 Uhr

manager-magazin.de Suche

Wirtschaftskriminalität

In einem Drittel aller Unternehmen wird abgezockt

Veruntreuung und Cybercrime sind die häufigsten Delikte, durch die Mitarbeiter deutscher Konzerne ihren Arbeitgeber schädigen. Laut

Rubriken stern.de Suche: Artikel

Digital: Computer | Internet | Telefon | Technik | Spiele

Soziale Netzwerke

Der Spion, der mich kopierte

Von Anne Meyer

Soziale Netzwerke wie StudiVZ oder Facebook tun nicht genug, die Privatsphäre ihrer Nutzer zu schützen. Eine Studie des

Datenspuren beim Surfen

Fraunhofer

- Orts-Information
  - mit hoher Genauigkeit möglich
- Beobachten des **Surfverhaltens**
- Ausnutzen von bekannten **Sicherheitslücken**

Google™ Deutschland

illegal d

illegal downloaden	634.000 Ergebnisse
illegal download	25.700.000 Ergebnisse
illegal danish	3.330.000 Ergebnisse
illegal downloads	27.100.000 Ergebnisse
illegal drugs	19.000.000 Ergebnisse
illegal downloading	35.900.000 Ergebnisse
illegal drogen	357.000 Ergebnisse
illegal danish 3	2.790.000 Ergebnisse
illegal download strafe	49.700 Ergebnisse
legal definition	25.200.000 Ergebnisse

Schließen

Erweiterte Suche
Einstellungen
Sprachtools

Such … schland

ben m … m in English

SPIEGEL ONLINE

11. Oktober 2008, 15:14 Uhr

Sicherheitsleck bei der Telekom

Millionen Kontodaten von T-Mobile-Kunden waren manipulierbar

Die Telekom wird von einem neuen gigantischen Datenskandal erschüttert: Nach SPIEGEL-Recherchen konnten sensible Daten von über 30 Millionen Handy-Kunden - inklusive Bankdaten - relativ leicht abgerufen und manipuliert werden. Weltweit. Inzwischen ist das Leck geschlossen.

Ohne die Suchanfrage tatsächlich abgeschickt zu haben, weiß Google, dass der Benutzer sich für „illegal d…“ interessiert!

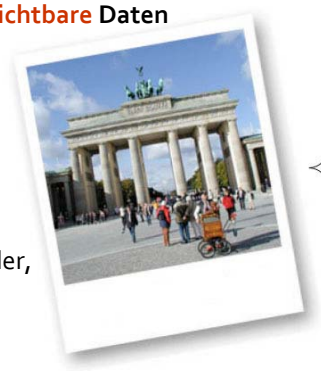
Persönliche Daten über Internet wegen Lücke für alle zugreifbar!

Datenspuren in Anwendungen

Fraunhofer SIT

Anwendungen: PDF, Word, PowerPoint, …

- **Automatisch eingefügte, unsichtbare Daten**
  - Identität des Urhebers
  - Datum der Erstellung, Änderung
  - Inhalte vor und nach Änderung
  - Gerätebezeichnung: z.B. bei Digitalkamera: Hersteller, Modell, Seriennummer



```
<meta-data>
name:       IMG001.jpg
date:       01-05-2009
time:       13:15:53 MET
camera:     NIKON Coolpix 600
serial-No:  NIK00123axAF
latitude:   52° 30' 58.57'' N
longitude:  13° 22' 40.00'' O
location:   BERLIN, DE
...
</meta-data>
```

- **Ausnutzbar z.B. für**
  - **Wirtschaftskriminalität, Ruf-Schädigung, Fälschung, Erpressung, ….**

Datenspuren beim Bezahlen

Fraunhofer SIT

Datenspuren bei Verwendung von

- Zahlungssystemen
- Buchungssystemen (ERP)
- Kundenbindungssystemen

Ausnutzbar z.B. um zu

- **Stehlen/Betrügen:**
  - Kreditkartenummern für illegale Transaktionen
- Erpressen, **Verkaufen**
  - Benutzerprofile für Datensammler

18.08.2009 Drucken | Senden | Bookmark | Feedback | Merken

DATENDIEBSTAHL IN DEN USA Schrift:

So lief der Millionen-Hack

Es war der bisher erfolgreichste digitale Raubzug überhaupt: Monatelang belauschte eine Gruppe von Hackern die Kommunikationskanäle mehrerer US-Unternehmen, erbeutete die Daten von mehr als 130 Millionen Kreditkarten. Der Attacke gingen aufwendige Vorbereitungen voraus.

Dass sich Straftaten wie die von Albert Gonzalez und seinen Komplizen häufen könnten, hält Erez Liebermann von der Staatsanwaltschaft von New Jersey für unwahrscheinlich. "Wir glauben nicht, dass es viele Hacker gibt, die dazu fähig sind", sagte Liebermann dem US-Magazin "Wired". Vielmehr gebe es wohl nur wenige "hochkarätige Experten", die derart gut geplante Aktionen durchführen könnten.

Der nun angeklagte Hacker Albert Gonzalez scheint einer dieser Experten zu sein. Das erkannte der US-Geheimdienst offenbar schon 2003, als der Mann zum ersten Mal wegen Datendiebstahls angeklagt wurde. Dem " Wall Street Journal" zufolge wurde Gonzalez daraufhin

arten auf asn.advolution.de… Proxy:

Fraunhofer SIT

IT zur Aufklärung und Prävention

Technologien und Verfahren: u.a.

- IT Forensik
- Watermarking
- Sicherheitstesting: Hacking
- Sichere Identität
- Überwachung

Aufklärung IT-Forensik

Fraunhofer SIT

Zielsetzung

- Aufklärung von Straftaten durch **Analyse von Datenspuren** in IT-Systemen
- Zurückführen krimineller Handlungen auf Personen, **Beweisführung**

Fragestellungen:

- Welche Aktionen hinterlassen **wo welche Spuren**?
- Wie **findet, analysiert** man die Spuren?
  Bem.: Riesige Datenmassen analysieren!
- Sind die Spuren **korrekt, gerichtsverwertbar**?
- Wie erzeugt man gewünschte Spuren?
- ...

Aufklärung IT-Forensik

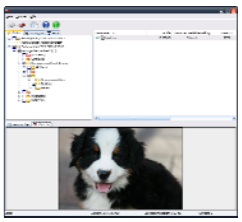
Fraunhofer SIT

Spuren auf der Festplatte

- Festplatte enthalten umfangreiche Datenspuren,
  - Löschen oder Formatieren:
    - entfernt nur Einträge im Inhaltsverzeichnis,
    - löscht jedoch nicht physikalisch

Teilweise wiederhergestelltes Bild durch File Carving (unterer Teil überschrieben)

- **Wiederherstellung von Daten:**
  - File Recovery: Analyse des Inhaltsverzeichnisses liefert noch bestehende Verweise auf gelöschte Dateien
  - File Carving: Untersuchung der Rohdaten auf Festplatte und Suche nach Signaturen bestimmter Dateitypen (Header, Footer)



File Recovery mit Standardtool

Aufklärung Bildforensik

Fraunhofer SIT

- Zielsetzung des Angreifers: Bildmanipulation
- Zielsetzung des Forensikers
  - Rekonstruktion zerstörter Bildinformation
- Techniken:
  - Finden von inversen Transformationen
  - Auswertung von Restinformation
  - Filterung

Beispiel: Enttarnung eines Täters (Kindesmissbrauch) durch Wiederherstellung von Originaldaten (Unterstützung des BKAs durch FhG)

Aufklärung
Digitale Wasserzeichen

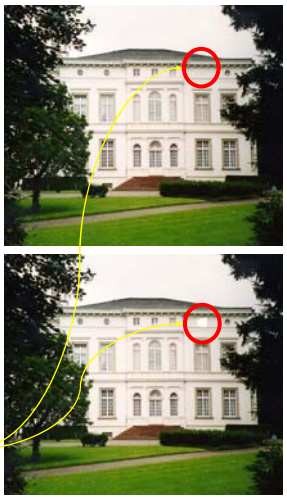
Fraunhofer SIT

Erkennen von Manipulationen bei

- Fotos, Videos, Graphiken, Musik, …
- **Was wurde, wie geändert**

Original

Fälschung

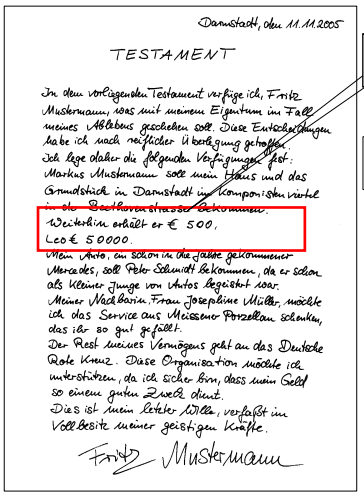


Erkennen der Manipulation an der Fälschung, Original wird dazu nicht benötigt

Aufklärung
Digitale Wasserzeichen

Fraunhofer SIT

Erkennen von Manipulationen an digitalisierten Texten, pdf-Dokumenten, Scans,…



Darmstadt, den 11.11.2005

TESTAMENT

In dem vorliegenden Testament verfüge ich, Fritz Mustermann, was mit meinem Eigentum im Fall meines Ablebens geschehen soll. Diese Entscheidungen habe ich nach reiflicher Überlegung getroffen. Ich lege daher die folgenden Verfügungen fest: Markus Mustermann soll mein Haus und das Grundstück in Darmstadt im Komponistenviertel in der Beethovenstrasse bekommen.
Weiterhin erhält er € 500,
Leo € 50000.
Mein Auto, ein schon in die Jahre gekommener Mercedes, soll Peter Schmidt bekommen, da er schon als kleiner Junge von Autos begeistert war. Meiner Nachbarin Frau Josephine Müller möchte ich das Service aus Meissener Porzellan schenken, das ihr so gut gefällt. Der Rest meines Vermögens geht an das Deutsche Rote Kreuz. Diese Organisation möchte ich unterstützen, da ich sicher bin, dass mein Geld so einem guten Zweck dient. Dies ist mein letzter Wille, verfasst im Vollbesitz meiner geistigen Kräfte.

Fritz Mustermann

Original Version

Weiterhin erhält er € 500,
Leo € 50000.

Manipulierte Version

Weiterhin erhält er € 50000.

Fälschung enthält Wasserzeichen:

Manipulationen sind genau nachvollziehbar

Weiterhin erhält er € 50000.
Leo € 50000.

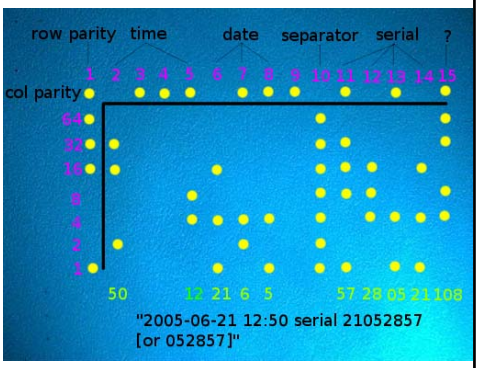
Die Farbe Blau zeigt eingefügte Zeichen
Die Farbe Rot zeigt gelöschte Zeichen

Aufklärung Markierungen

Fraunhofer SIT

Übergang: digitale in reale Welt

- Laserdrucker markieren Ausdrucke mit individuellen Wasserzeichen:
  - Identifizierbarkeit Seriennummer des Druckers, Datum, Uhrzeit
- **Tracking Dots**:
  - nahezu unsichtbare Markierungen,
  - jedoch maschinell gut lesbar
- **Rückverfolgbarkeit**
- **Fälschungssicherheit**



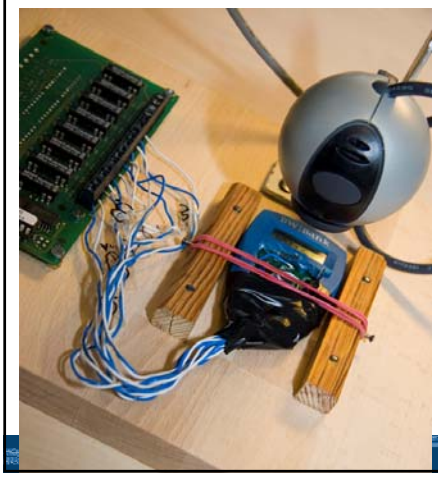
Prävention Sicherheitsanalysen

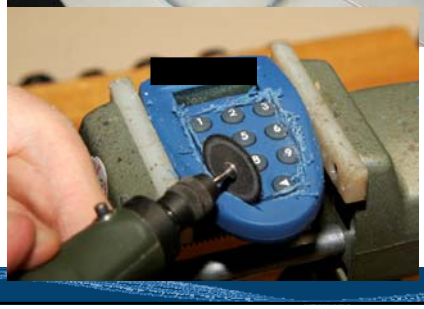
Fraunhofer

Erkennen von **Schwachstellen**

- Hacken, Angreifen, Eindringen

Schließen der Lücken!





Prävention
Sichere Identität

Fraunhofer SIT

Biometrische Verfahren zur Personen-Identifikation

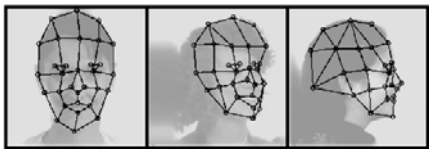
- Fingerabdrücke, handschriftliche Unterschrift, Stimme, Iris
- 3D-Gesichtsbilder

Überwindungssicher?

Attrappen-Bau und Test

Iris-
Check

Gesichtserkennung

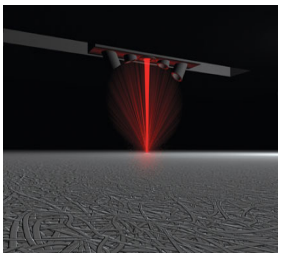


Prävention
Sichere Objekt-Identität

Fraunhofer SIT

Biometrische Identität von Objekten:

- Plagiaterkennung
- LSA Laser Surface Authentication: Fingerprint der Objekt-Oberfläche



Objekt-Identifikation

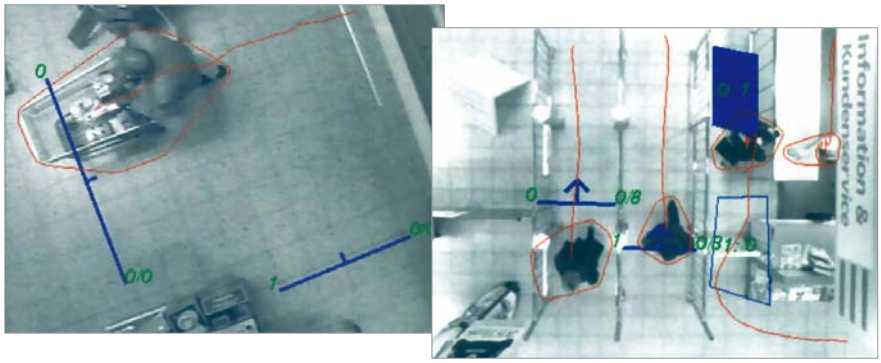
- RFID-Tags am Objekt

Aufklärung/Prävention Überwachung

Fraunhofer SIT

Optische **Überwachung von Kunden** z.B. in Läden

- Frühzeitige Erkennung von kriminellen Handlungen
- Nachweisführung



Quelle: Ingenieurbüro Piper GmbH / SiteView

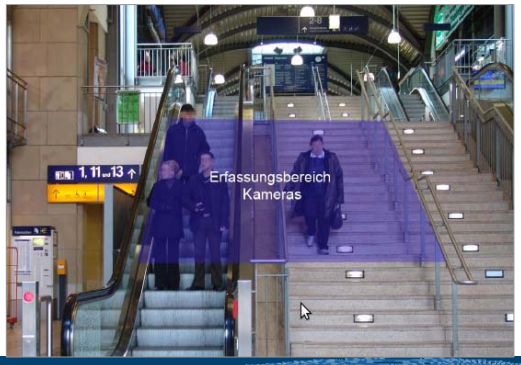
Aufklärung/Prävention Überwachung

Fraunhofer SIT

Feldversuch des Bundeskriminalamtes (Mainz Hbf)

- Ziel: Einzelpersonen anhand von Fahndungsfotos aus den Menschenmassen wiedererkennen, wenn Sie den überwachten Bereich betreten
- **Ergebnis:** IT noch nicht gut genug!

Quelle: Bundeskriminalamt



Aufklärung/Prävention Überwachung

Fraunhofer SIT

Im Polizeieinsatz (Groß Brittanien, USA) : **Drohnen**

- Mobile Überwachungs-Roboter
- Ferngelenkt

Quelle: microdrones

Forschung

Fraunhofer SIT

Beispiele aus Forschung und Entwicklung

Forschung Überwachung

Fraunhofer SIT

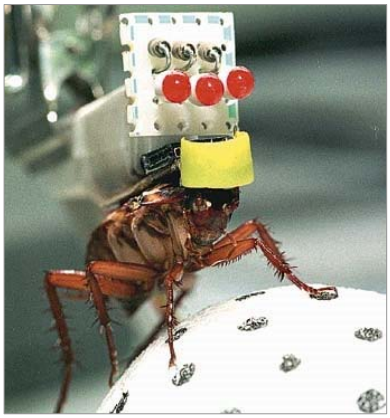
Forschungsprojekt: Großräumiges Verfolgen von Personen mit Videokamera-Netzwerken: z.B. flüchtende Kriminelle

Quelle: Kingston University / ZDF

Forschung Überwachung

Fraunhofer SIT

Forschungsprojekt (USA, DARPA): Entwicklung von „Insect cyborgs“



Quelle: Tokyo University

Insect cyborgs

- Insekten mit elektronischen Komponenten
- erledigen Aufgaben
  z.B. eine Kamera zur Fernaufklärung
- **Vision:**
  - Insekten für militärische Zwecke,
  - Spionage, Aufklärung und auch
  - Verbrechensbekämpfung nutzen

Mikrocontrolller-kontrollierte Insekten:

- eine Elektronik kontrolliert z.B. die
- Muskeln des Insekts

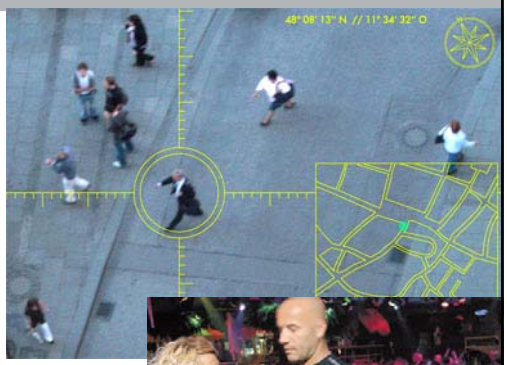
Nanoroboter

Forschung
Überwachung

Fraunhofer SIT

Implantierte Sensoren

- Überwachung der Körperfunktionen
- Funkübertragung
- Aufenthaltsorte

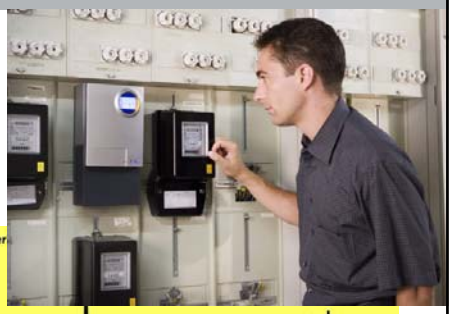


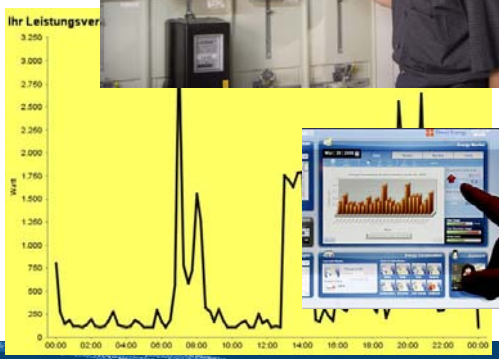
Forschung
Sichere Identität

Fraunhofer SIT

Fingerabdrücke als Identitätsnachweis
Einsatzbeispiele in der nahen Zukunft?

- **Intelligenter Stromzähler**
  - Stromnetz-Überwachung - Real-Time Residential Power Line Surveillance (RRPLS)
  - Verbrauchsprofile:
    Erkennen von Abweichungen
- **Digitales Schloss**
  - notiert das Verlassen der Wohnung:
  - Einbruchserkennung





SIT-Forscher als Berater

Fraunhofer SIT

- Fraunhofer SIT berät Autoren, Regisseure, ...
- Wir liefern keine Ideen, aber prüfen Geschichten auf technische Plausibilität (Angriffsmöglichkeiten und technikbasierte Alibis)

Fiktion?
Realität?

Zusammenfassung

Fraunhofer SIT

Tatort Internet

- **IT als Tatwerkzeug**, genutzt auch von organisierter Kriminalität
- Schattenmarkt existiert bereits:
  - kein Spezialisten-Know-How notwendig, Rent a Hacker
  - für wenig Geld große Wirkung erzielbar

Präventions- und Aufklärungstechnik:

- IT als **Werkzeug der Prävention und Aufklärung** zunehmend wichtig

Das Hase-Igel Spiel in neuer Dimension geht weiter

- Es bleibt spannend und herausfordernd

Kontakt

Fraunhofer SIT

Prof. Dr. Claudia Eckert
Telefon: +49 6151 869-285
Fax: +49-6151-869-224
E-Mail: claudia.eckert@sit.fraunhofer.de
Internet: http://www.sit.fraunhofer.de

SIT-PR Referent:
Oliver Küch
E-Mail: oliver.kuech@sit.fraunhofer.de