UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Institut für Informatik
Fachgebiet Sicherheit in Netzwerken

Sicherheit in der Datenkommunikation
Wie viel Sicherheit ist möglich und nötig?

Christoph Sorge
Universität Paderborn

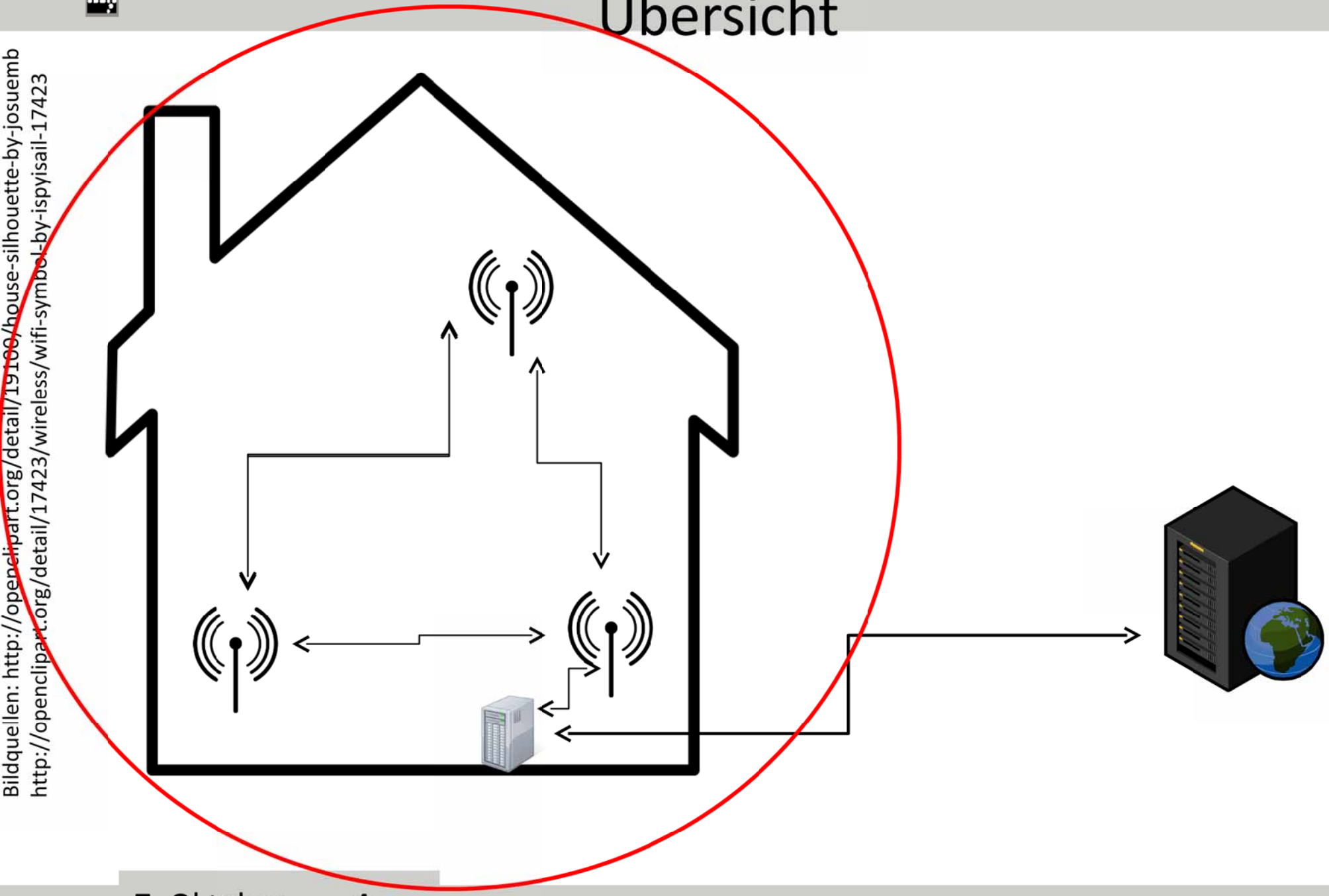
IT-Sicherheit an der Universität Paderborn

- Fachgebiet Codes & Kryptographie, Prof. Dr. Johannes Blömer
- Zentrum für Informations- und Medientechnologie, Prof. Dr. Gudrun Oevel
- Fachgebiet Sicherheit in Netzwerken, Jun.-Prof. Dr. Christoph Sorge
  - Anwendungen der Kryptographie
  - IT-Sicherheit und Datenschutz
  - Schnittstellen zu juristischen Themen
- Jährlich im Frühjahr: Tag der IT-Sicherheit – nächster Termin voraussichtlich 27. März 2014
  - Mit Workshops zu aktuellen Themen (sowie „Dauerbrennern“) der IT-Sicherheit

AAL und Smart Home: Wieso sicherheitsrelevant?

- Mögliche Ziele eines Angreifers
  - Informationen sammeln und für „klassische“ Straftaten nutzen (Anwesenheit von Bewohnern, Alter der Bewohner, Anzahl der Bewohner, …) → Einbruch, Betrug, …
  - Informationen sammeln und für Marketingzwecke nutzen
  - Rein böswillige Schadensverursachung (Einschalten von elektrischen Verbrauchern, Heizung etc.)
  - Umgehen elektronischer Türschlösser und ähnlicher Sicherheitsmaßnahmen
  - …

Übersicht



Bildquellen: http://openclipart.org/detail/19100/house-silhouette-by-josuemb
http://openclipart.org/detail/17423/wireless/wifi-symbol-by-ispyisail-17423

Sicherheitsrisiken drahtloser Kommunikation

- Drahtlose Kommunikation: Mithören oder Einflussnahme auf die Kommunikation auch von außen möglich

- Klassische Schutzziele der IT-Sicherheit
  - Integrität und Authentizität
    - auch für drahtlose Hausautomation mit Standardtechniken erreichbar
    - in der Praxis oft vernachlässigt (oder „Security by Obscurity“)
    - Techniken werden aber besser
  - Vertraulichkeit
    - mit Einschränkungen erreicht
    - Menge möglicher Nachrichten sehr klein

Sicherheitsrisiken drahtloser Kommunikation

- Verkehrsanalyse
  - Analyse von Mustern des Datenverkehrs auch ohne Kenntnis des Inhalts
  - Beispiele:
    - Es werden viele Nachrichten ausgetauscht → jemand ist im Haus
    - Es werden Nachrichten zwischen einer Fernbedienung und einem automatischen Türschloss ausgetauscht → jemand betritt oder verlässt das Haus

- Masterarbeit in unserer Arbeitsgruppe: Experimentelle Bestätigung dieses Angriffspotentials

Schutz vor Verkehrsanalyse

- Schutz vor Verkehrsanalyse
  - Eigentlich unproblematisch durch Versand zusätzlicher Nachrichten (Grundrauschen)
  - Widerspruch gegenüber effizienter Nutzung des Frequenzspektrums, Energieeffizienz und gegenüber Befürchtungen vor „Elektrosmog“

→Aus Sicherheits-Sicht: Momentan eher Verwendung drahtgebundener Systeme zu empfehlen

  - Risiko lokaler Angriffe allerdings kleiner als Risiko von Angriffen auf bewusst eingerichtete Schnittstellen nach außen

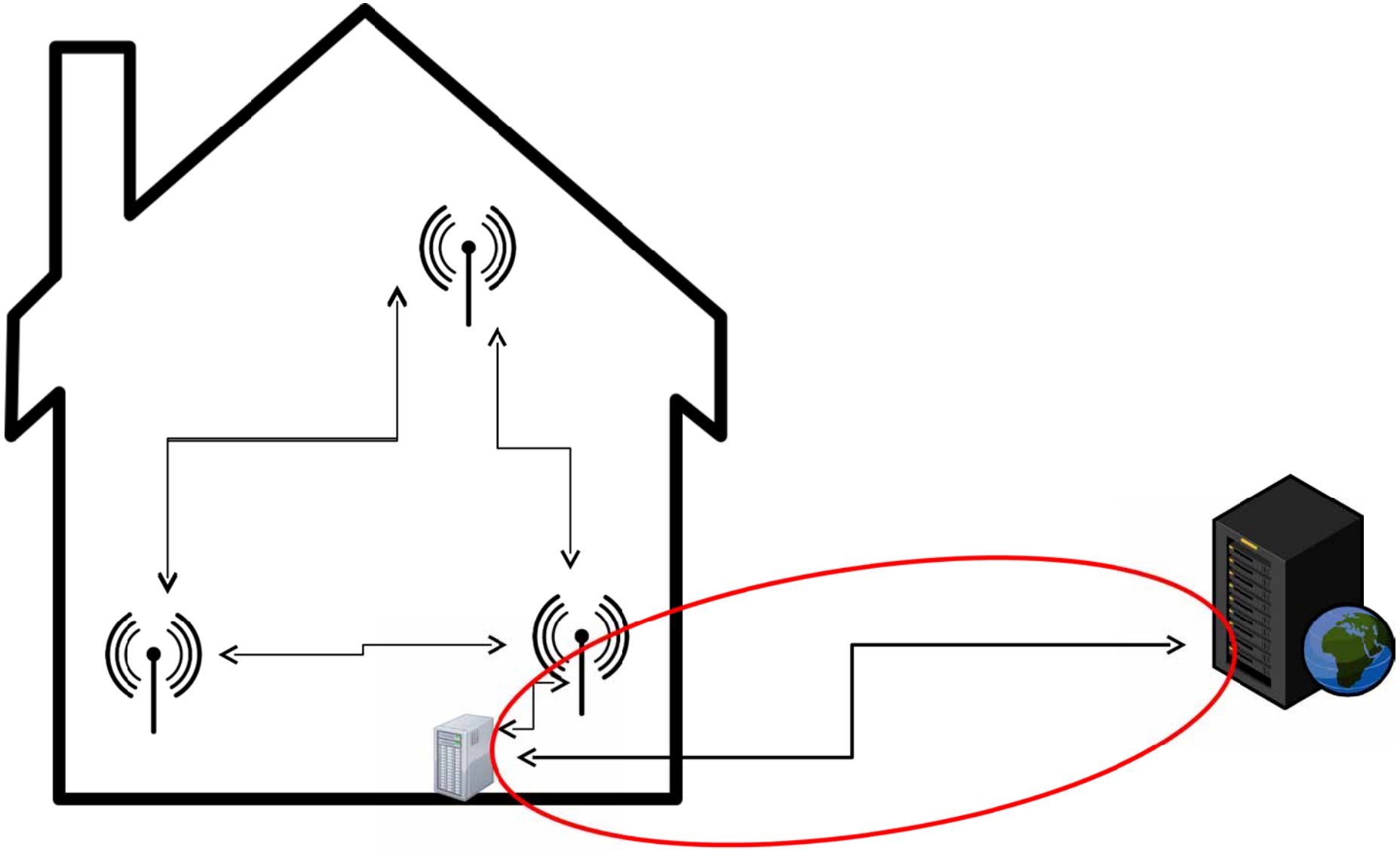
Kosten von Sicherheitsmaßnahmen im lokalen Netz

- Kosten von Sicherheitsmaßnahmen im engeren Sinn
  - Einsatz kryptographischer Verfahren erfordert höheren Rechenaufwand und ggf. mehr Datenübertragung → höhere Hardwarekosten – bei großen Stückzahlen aber praktisch vernachlässigbar
  - Sicheres System muss entwickelt werden – einmalig anfallende Entwicklungskosten aber bei hohen Stückzahlen nur bedingt relevant
  - Evtl. Kosten für Zertifizierungen etc.

Kosten von Sicherheitsmaßnahmen im lokalen Netz

- Kosten von Sicherheitsmaßnahmen im weiteren Sinn
  - Sicherheitskonfiguration erfordert Aufwand
  - Beispiel: Kryptographische Schlüssel an alle Teilnehmer des lokalen Netzes verteilen
    - Neu hinzukommende Komponenten beachten
    - Nachträgliches Entfernen von Komponenten beachten
  - evtl. reduzierte Attraktivität sicherer Systeme bei schwierigerer Konfiguration

Übersicht



Schnittstelle nach außen

- Für intelligente Stromzähler: Schutzprofil des BSI
  - Anbindung eines Hausautomations-Netzes denkbar (aber nur sinnvoll bei Interaktion mit dem Energieversorger)

- Hausautomation im Allgemeinen: Viele Schnittstellen-Varianten denkbar
  - Web-Schnittstellen, Smartphone-Apps, ….
  - AAL-Anwendung: Fernüberwachung durch Dritte denkbar (Beispiel: Anbindung Hausnotrufzentrale)

Schnittstelle nach außen: Sicherheit?

- Web-Schnittstellen: Einfach zu programmieren… nicht einfach *sicher* zu programmieren
  - In vielen Anwendungen beliebtes Angriffsziel
  - Injection-Angriffe, Cross-Site Scripting, Cross-Site Request Forgery, …
  - Solche Angriffe sind Alltag

- Authentifizierung?
  - Nutzername/Passwort → oft Wahl zu einfacher Passwörter durch Nutzer

Schnittstelle nach außen: Datenschutz

- Herausgabe von Daten an externe Dienstleister u.U. wünschenswert
  - Beispiel: Zur Optimierung der Stromkosten u.ä.
  - Aber auch Betrieb einer Web-Schnittstelle u.U. schon mit Preisgabe von Daten verbunden
- Techniken aus der Kryptographie und IT-Sicherheit ermöglichen Weiterverarbeitung bei möglichst geringer Preisgabe von Daten auch gegenüber dem Dienstleister selbst
- Trotzdem: Vertrauenswürdigkeit des Anbieters von zentraler Bedeutung

Gemeinsames Problem im lokalen Netz und an der Schnittstelle

- Sicherheitslücken existieren
  - auch bei größter Sorgfalt
  - auch bei Systemen großer Unternehmen
  - auch bei Systemen von IT-Sicherheits-Firmen

→Planmäßiger Umgang mit Sicherheitslücken notwendig

- Möglichkeit, Updates einzuspielen
  - muss selbst sicher sein
  - muss *einfach* möglich sein (Fernwartung?)
- Kosten für Updates? (Abschreckung?)
- Insolvenz des Anbieters?

Warum sollte *ich* betroffen sein?

- Bei Millionen zukünftigen Smart-Home-Nutzern: Warum sollte *ich* das Ziel eines Angriffs werden?

- Problem: Kosten für Entwicklung eines Angriffs (Finden/Ausnutzen einer Sicherheitslücke) entstehen einmalig
  - Angriff auf (Web-)Schnittstelle eines Systems: Kosten nahezu unabhängig von Anzahl betroffener Haushalte

  →Angriffe u.U. gleich auf alle Nutzer des Systems

- Im Vergleich dazu höherer Aufwand für lokale Angriffe – aber auch hier: Entwicklungskosten nur einmalig

Security by Obscurity

- (Leider) gängiger Sichtweise: Verwendung selbst entwickelter Sicherheitsverfahren bietet besten Schutz – Prinzip „Security by Obscurity“

- Konzept funktioniert u.U., falls möglicher Ertrag eines Angreifers < Aufwand für Analyse des Verfahrens
  - Beispiel: Hausautomationssystem für wenige Privathaushalte
  - Problem: Ertrag des Angreifers muss nicht finanzieller Natur sein
  - Problem: Unerwarteter Erfolg des Anbieters

- Bisher häufiges Scheitern von Security by Obscurity

Fazit

- Wieviel Sicherheit ist *möglich*?
  - Wesentliche Schutzziele mit Standard-Techniken erreichbar
  - Schutz vor Verkehrsanalyse für drahtlose Systeme: Noch Forschungsbedarf
  - Probleme sonst vor allem in der Umsetzung – Systeme ohne Sicherheitslücken momentan kaum vorstellbar
    → Sicherheitslücken mit einplanen

Fragen?

- Kontakt:

Christoph Sorge

Universität Paderborn, Institut für Informatik

Fachgebiet Sicherheit in Netzwerken

Warburger Straße 100

33098 Paderborn

christoph.sorge@uni-paderborn.de