Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

16. Energieworkshop „Digitalisierung der Energieversorgung: Neue Chancen, neue Risiken?“, Handelskammer Hamburg, 9. Oktober 2017

IT-Sicherheit und Datenschutz

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

Aktuelle Forschungsprojekte am Arbeitsbereich SVS

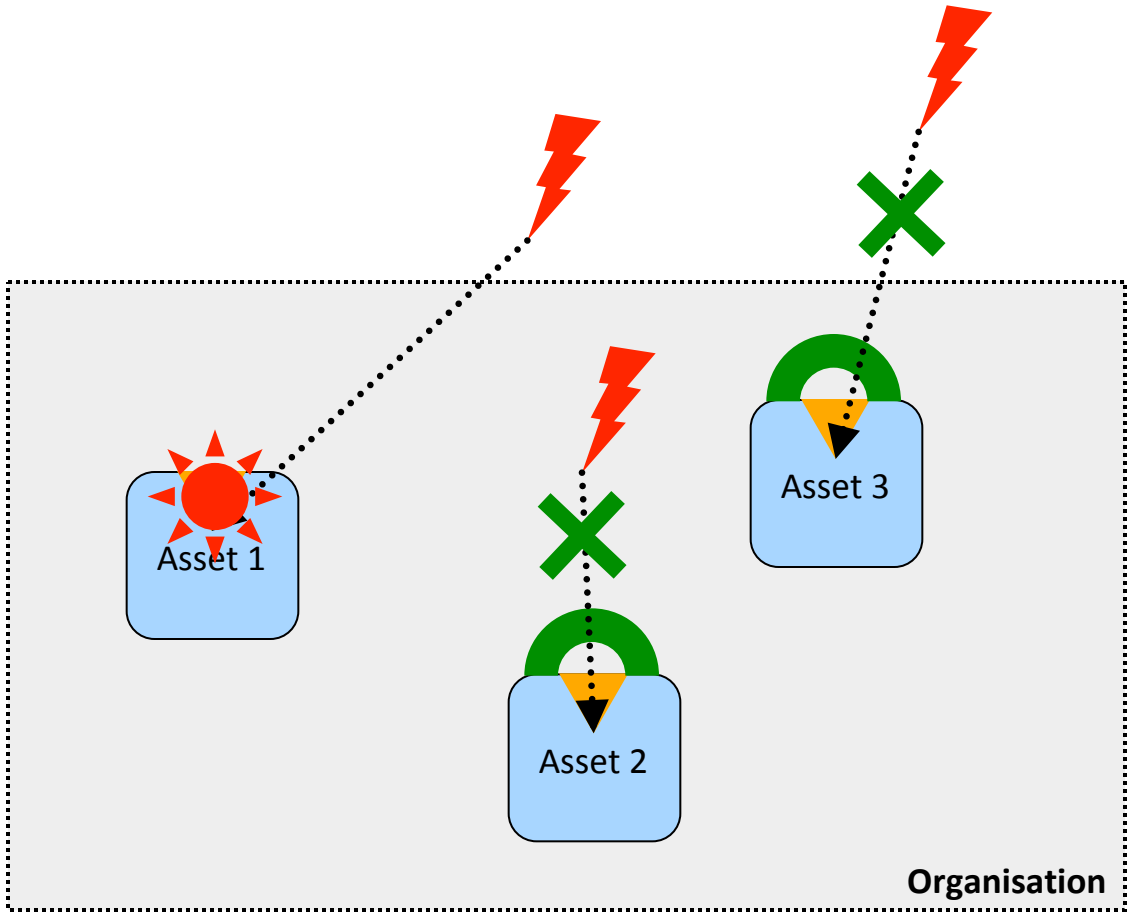
- AppPETs – Datenschutzfreundliche Apps ohne Kompromisse
- ANON-NG – Anonymität der nächsten Generation
- DREI – Datenschutz-respektierende Erkennung von Innentätern
- CANVAS – Constructing an Alliance for Value-driven Cybersecurity
- Information Governance Technologies – Ethics, Policies, Architectures, Engineering
- Idomeneo – Aufbau einer medizinischen Registerdatenbank

Aktuelle Forschungsprojekte am Arbeitsbereich SVS

- EnEff – Sichere IKT-Infrastruktur für Energie-Effizienz-Verbünde
  - Ziel: Technische Lösungen zum sicheren Aufbau von Virtuellen Kraftwerken
  - 5 Projektpartner
  - Gesamtkosten: ca. 2,4 Mio. €

- NEW 4.0 – Norddeutsche Energiewende 4.0 (BMWi)
  - Ziel: Versorgung der Region Hamburg-Schleswig-Holstein mit 100% erneuerbaren Energien bis 2035
  - 37 Projektpartner
  - 20 assoziierte Partner
  - Investitionsvolumen: fast 90 Mio. €

Von der Bedrohung zum Sicherheitsvorfall



Bedrohungen, z.B.
- Viren, Würmer
- DoS
- Hacking
- Spionage
- Social Engineering

Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

Schutzziele
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

vgl. Nowey, 2011

Von der Bedrohung zum Sicherheitsvorfall

- Präventive Maßnahmen
  - Einsatz kryptographischer Verfahren
    - obligatorische Datenverschlüsselung
    - gegenseitige starke Authentifizierung
  - Perimeterschutz mit Firewalls
  - Aufteilung Test- und Produktivumgebung
- Detektive Maßnahmen
  - Einsatz von Intrusion Detektion Systemen
  - Malware-Schutz
- Reaktive Maßnahmen
  - Systemtrennung
  - Fail-Safe-Prozeduren
  - Protokollierung

Bedrohungen, z.B.
- Viren, Würmer
- DoS
- Hacking
- Spionage
- Social Engineering

Verwundbarkeiten, z.B.
- Konfigurationsfehler
- Buffer Overflows

Schutzziele
- Vertraulichkeit
- Integrität
- Verfügbarkeit

Maßnahmen
- Präventiv
- Detektiv
- Reaktiv

Technologien

.net / C#

MS-SQL

MongoDB

Windows Server

IPsec, OpenVPN

JSON, HTTPS / TCP/IP

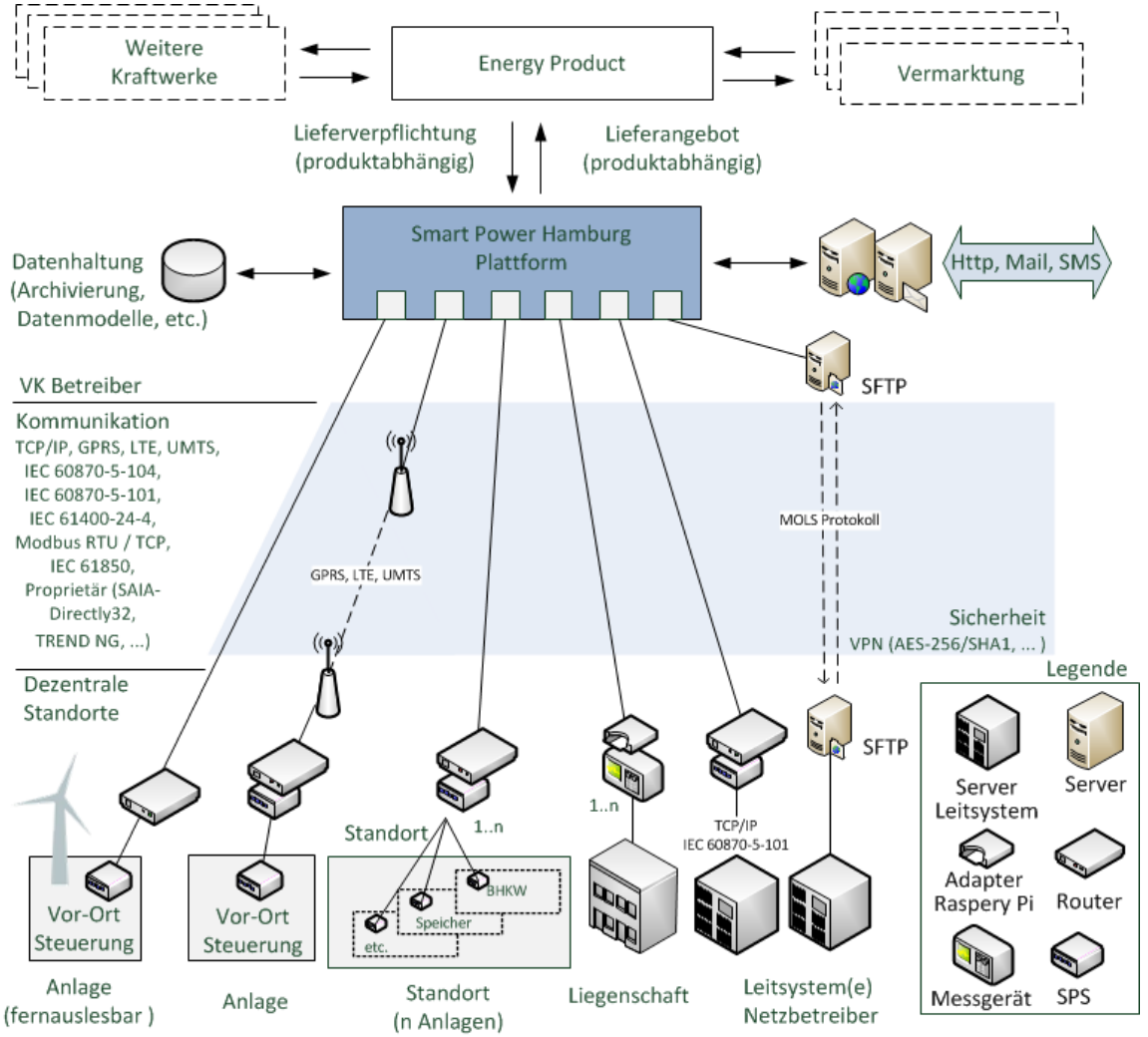
Apache Web-Server

PHP

Javascript

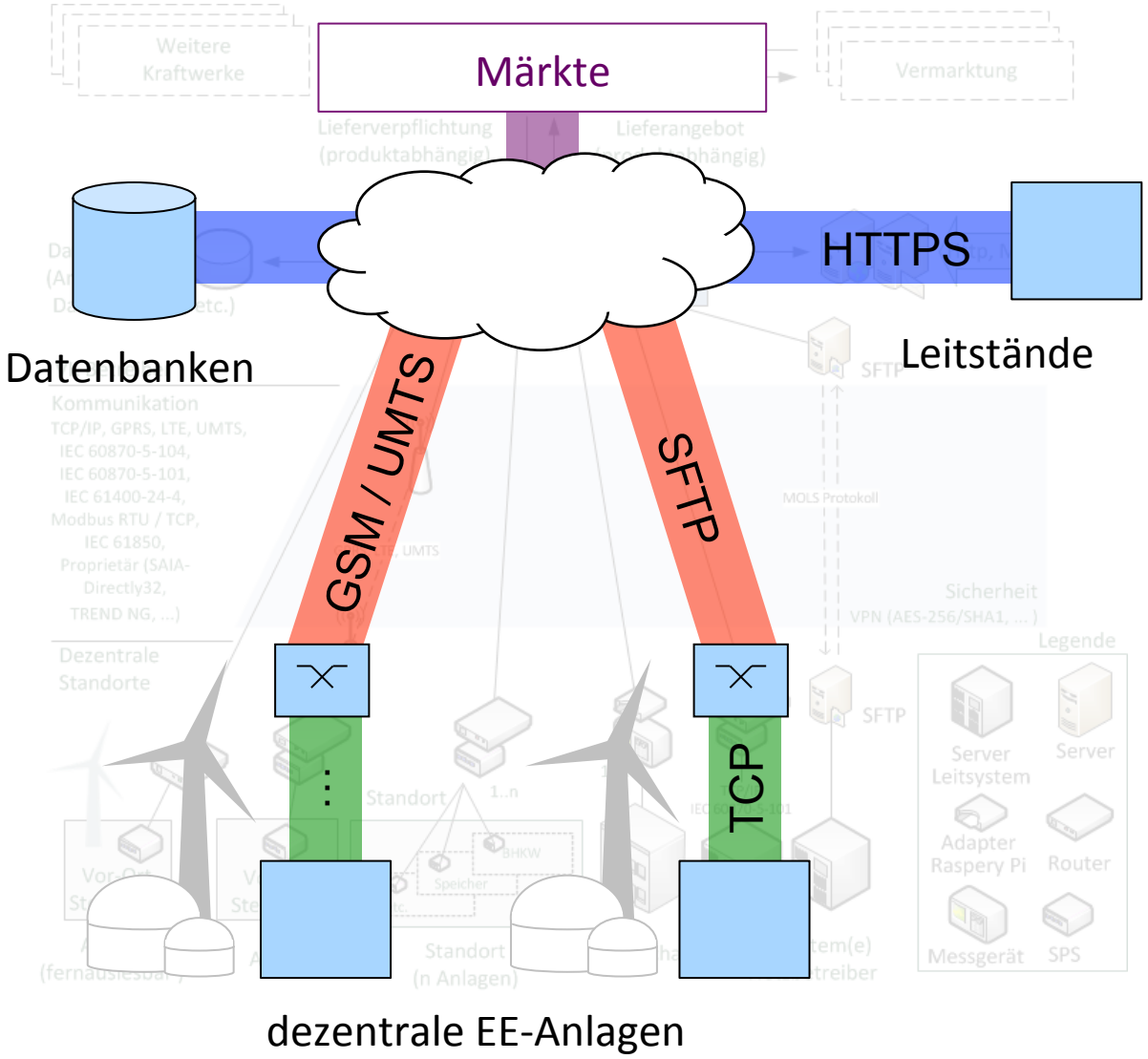
JQuery, Bootstrap.js, …

…



Technologien

- Basistechnologien
  - .NET
  - JAVA
  - SQL
  - ...
- Sicherheitstechniken
  - Kryptographie
  - Redundanz
  - sichere SW
  - sichere HW
  - ...



Konkrete Versuchsaufbauten und Arbeitspunkte 1/2

- Anbindung von Anlagen über Mobilfunklösungen
  - Standard-Sicherheit im Mobilfunk
  - Zusätzliche IP-basierte Schutzmaßnahmen
  - Redundanz zur Verbesserung der Verfügbarkeit

- Rechtemodelle für Zugriffsschutz
  - Anlagenanbindung mittels Kryptographie
  - Gestaltungsoptionen für das Schlüsselmanagement
  - Einsatz von Hardware-Token (TPM, Chipkarten)

- Updatemechanismen
  - zuverlässigen Schutz vor Schadsoftware
  - Problematik von Insider-Angriffen
  - Schutz durch physische Systemtrennung

Konkrete Versuchsaufbauten und Arbeitspunkte 2/2

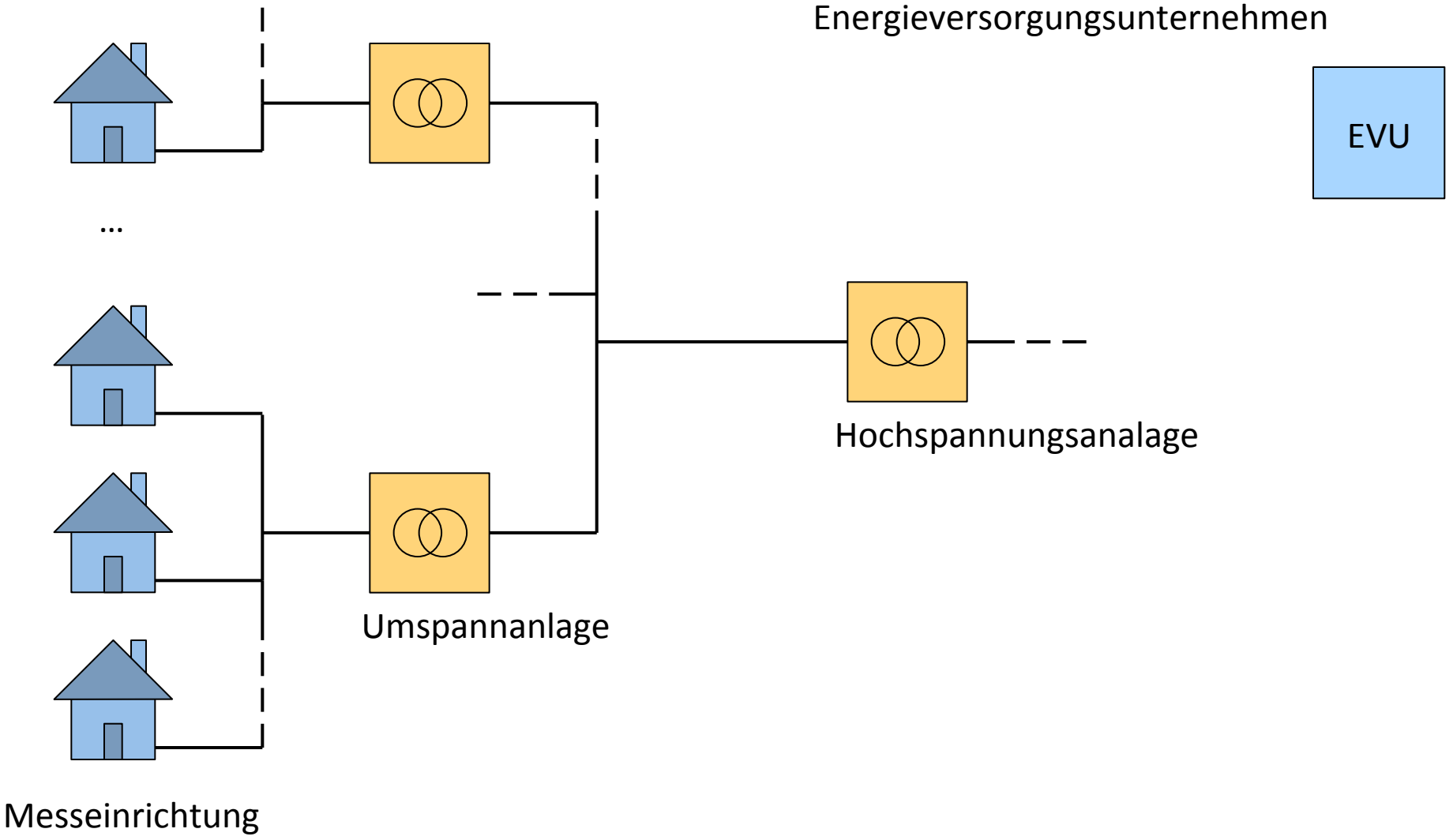
- Gestaltungsoptionen für das Schlüsselmanagement
  - Anlagenanbindung mittels Kryptographie
  - Virtuelles Kraftwerk von zwei Projektpartnern

- Erstellung von Lehr und Schulungsmaterialen für das Sicherheitsmanagement von verteilten Anlagen zur verteilten Energieerzeugung
  - Sicherheitsmanagement
  - Grundlagen der IT-Sicherheit

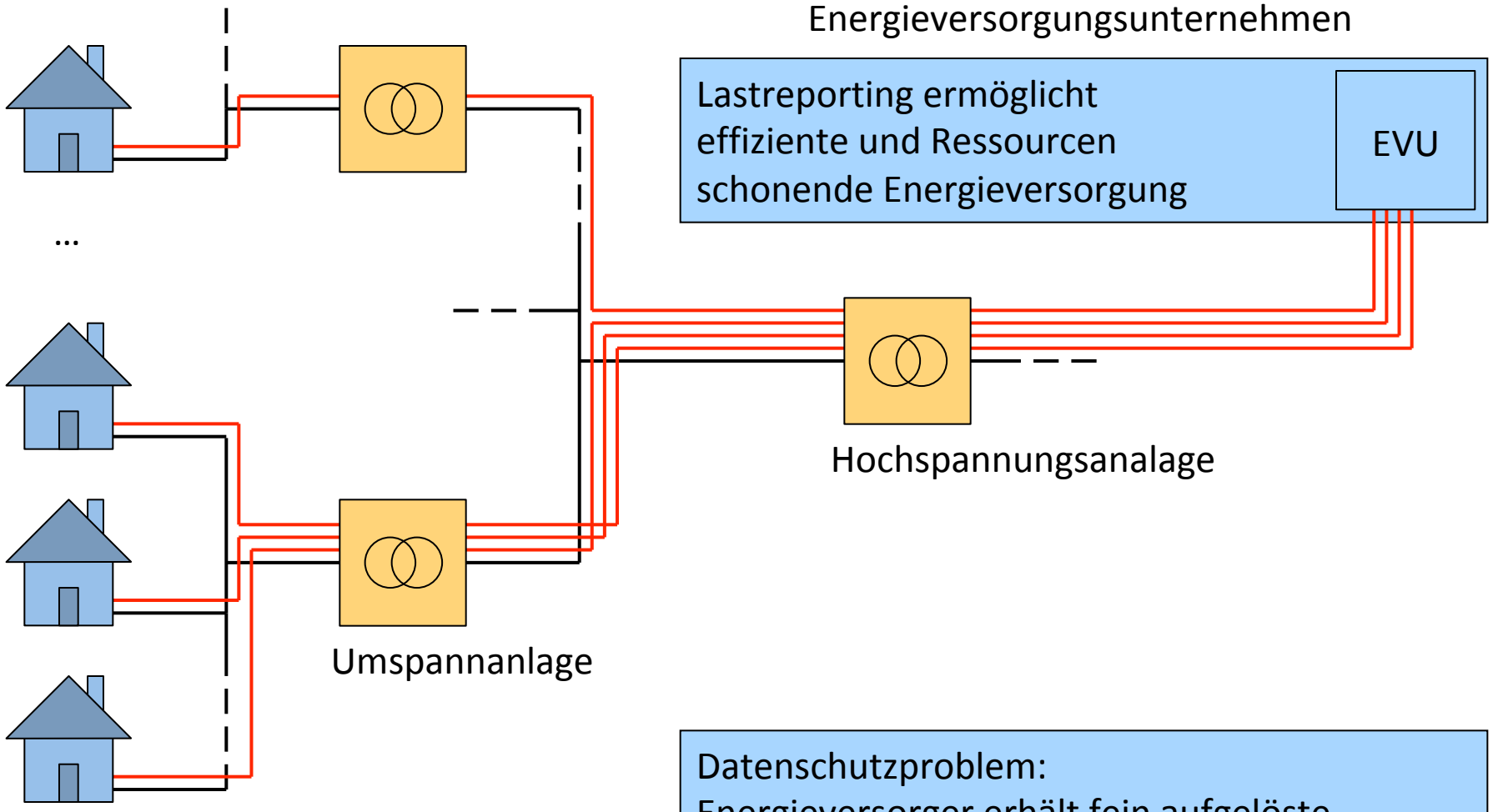
Smart Meter und technische Lösungen zur Wahrung des Rechts auf informationelle Selbstbestimmung?

Zwei exemplarische Lösungsansätze

Typische Architektur



Typische Architektur



Datenschutzproblem:
Energieversorger erhält fein aufgelöste Informationen über Energienutzung eines jeden Haushalts

Datenschutzrechtliche Einordnung

Lastreporting ermöglicht effiziente und Ressourcen schonende Energieversorgung

EVU

- Art. 5 (1) c) DSGVO

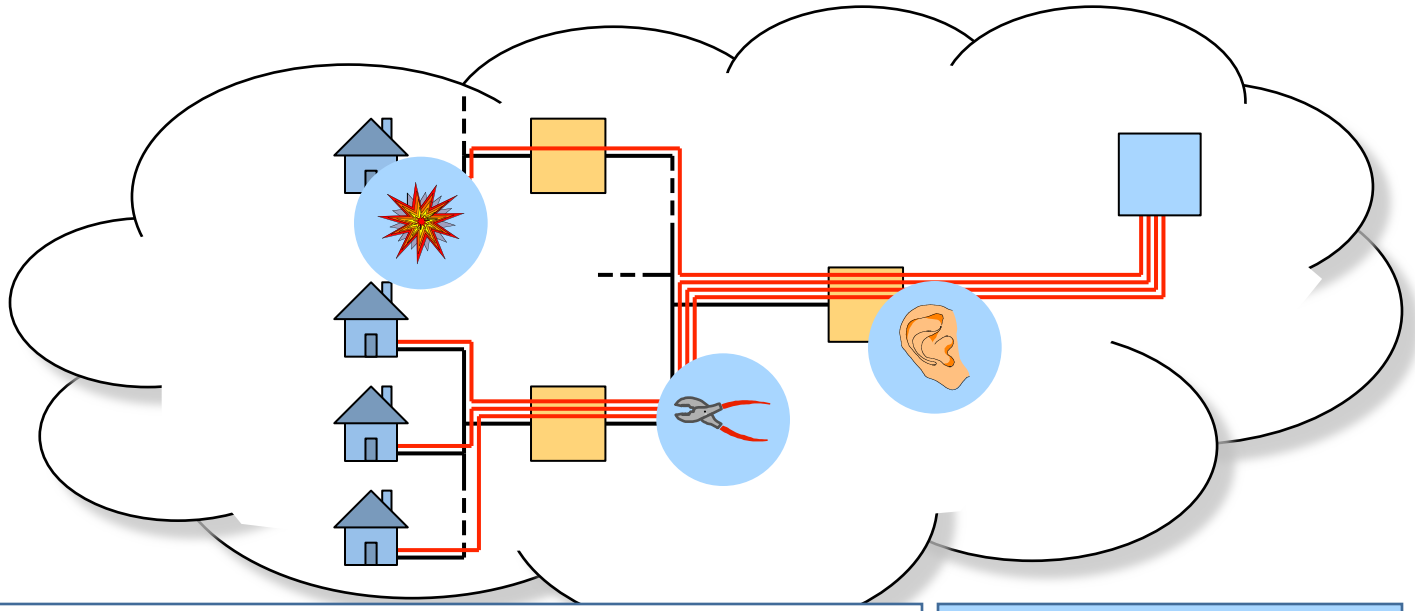
  Grundsätze für die Verarbeitung personenbezogener Daten

  Personenbezogene Daten müssen

  c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

Gesucht sind Lösungen, die ein Lastreporting zur Ressourcen schonenden Energieversorgung unter Wahrung der informationellen Selbstbestimmung ermöglichen.

Schutzziele und Angreifermodell



Bedrohungen

- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung der Funktionalität

Schutz der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Triviale Ansätze zur Datenminimierung

- Intervalle zur Datenerhebung vergrößern

  oder

- Aggregation mehrerer Haushalte

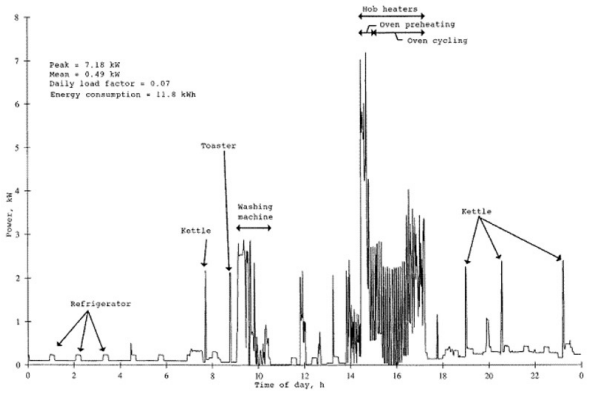
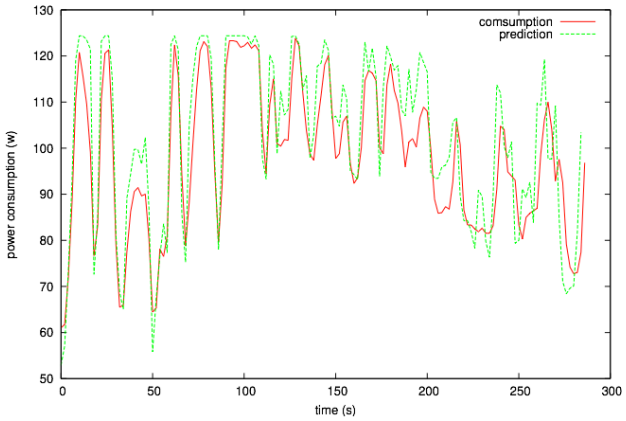


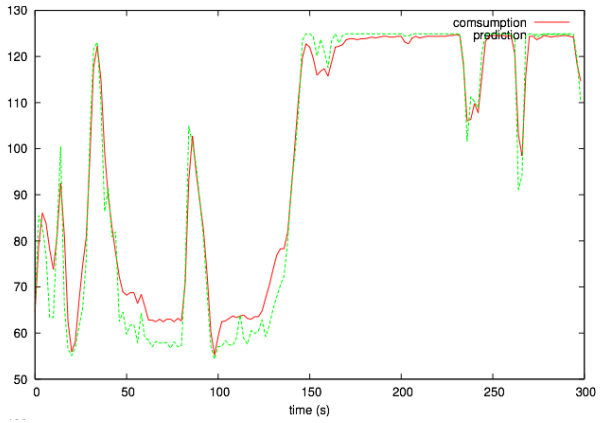
Bild: NIST

- Mit sekundengenauen Daten sind sogar Fernsehprogramme detektierbar (Greveler, Justus, Löhr 2012):

Star Treck 11



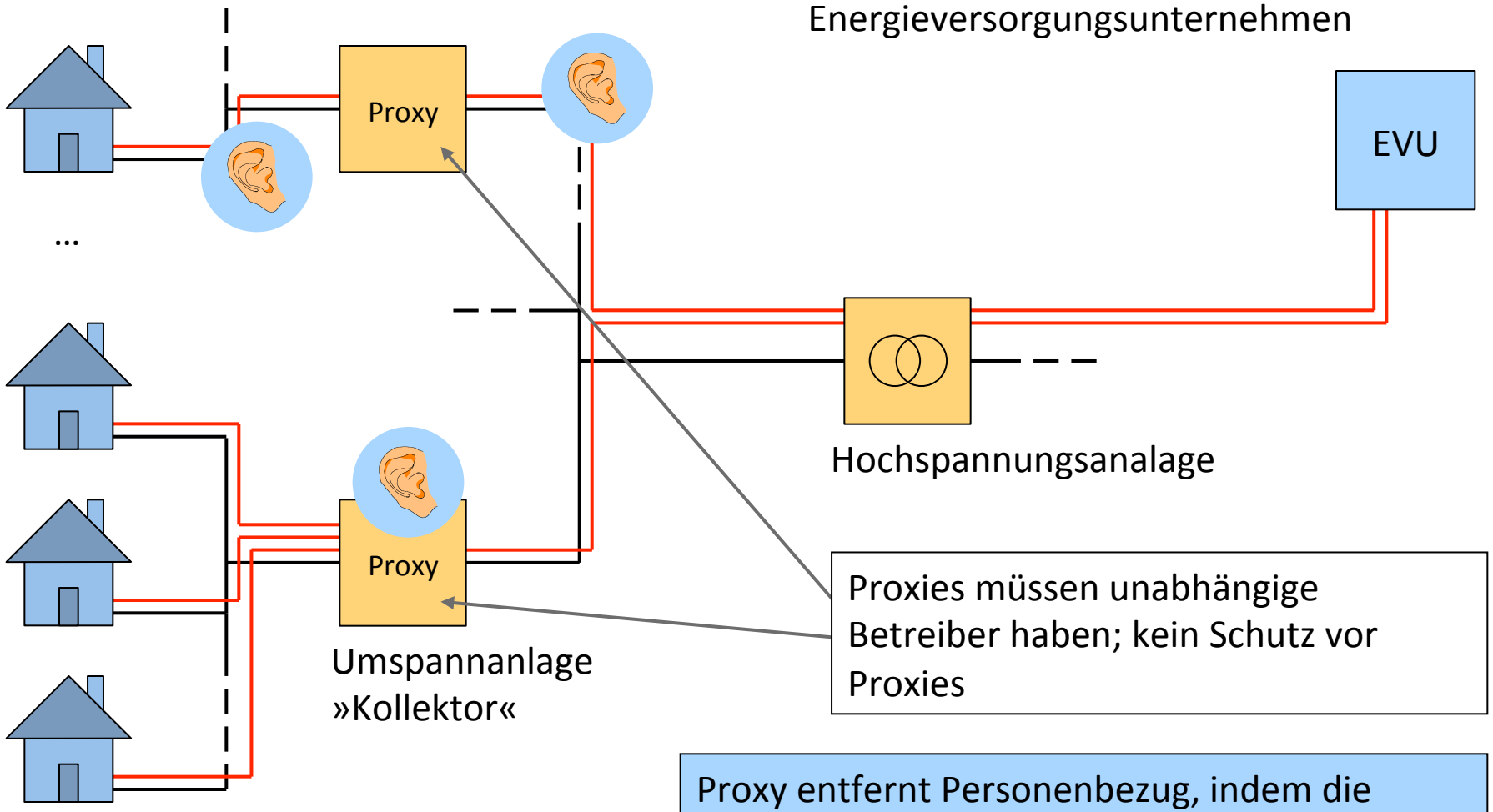
Star Treck TNG



Bilder: NIST, Greveler et. al.

Proxy-basierte Verfahren

Petrlic, 2011



Verfahren ohne Notwendigkeit eines vertrauenswürdigen Dritten

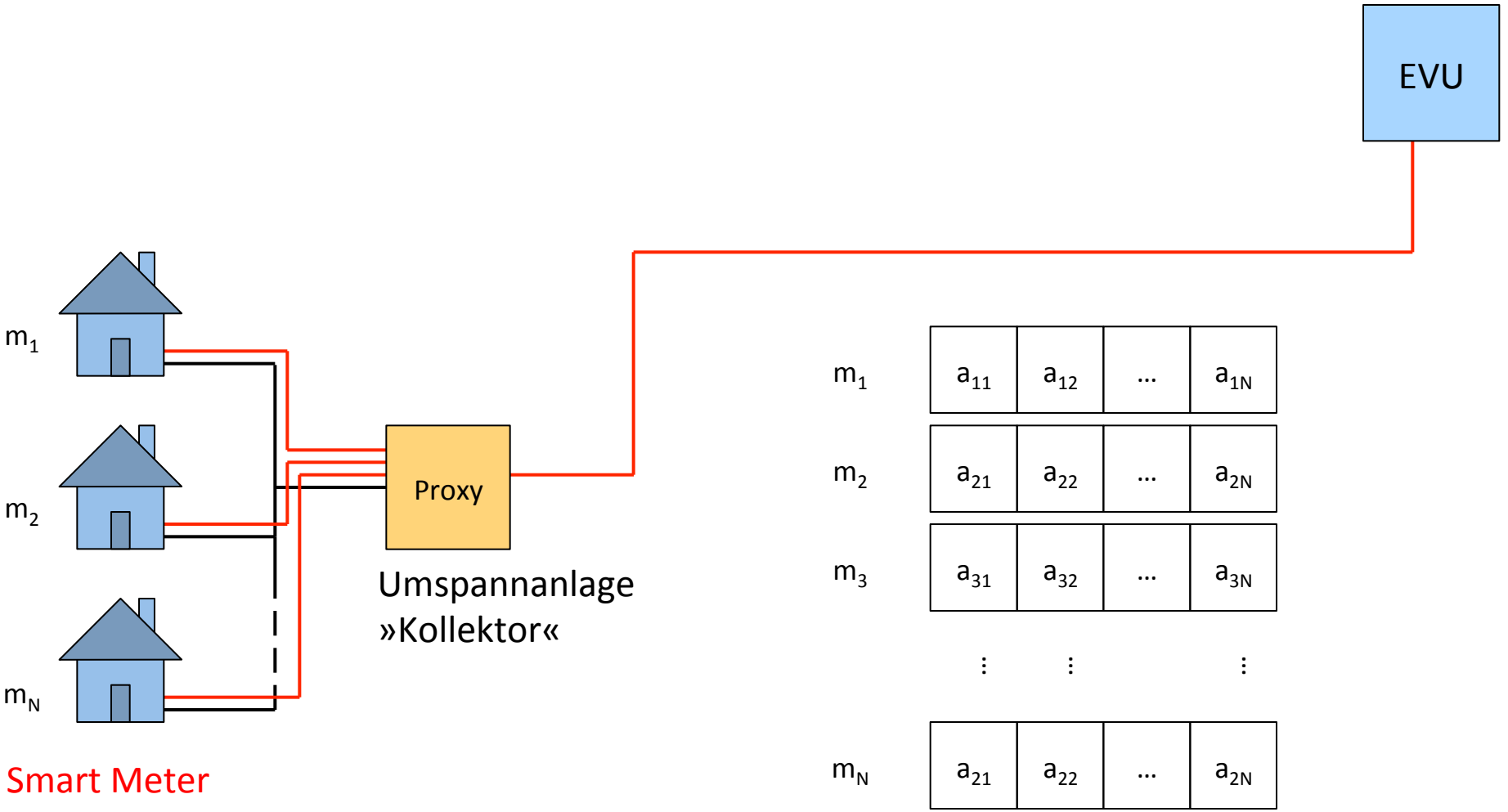
- Ziel: kein Vertrauen in einen zwischengeschalteten Proxy/Kollektor

- Ansatz Homomorphe Verschlüsselung (Garcia, Jacobs, 2010)
  - Zerlegen der Smart Meter Daten in N Teile
  - Teile werden einzeln verschlüsselt
  - Kollektor aggregiert summiert über verschlüsselten Teilen

- Ansatz Zero Knowledge Proof of Knowledge (Jeske, 2011)
  - Smart Meter Daten werden anonym an Kollektor übermittelt
  - Es wird bewiesen, dass die Daten von einem »echten« Smart Meter stammen, ohne dies identifizieren zu können
  - Wäre auch realisierbar mit anderen kryptographischen Primitiven
  - Setzt Schutz der Kommunikationsbeziehung voraus

Ansatz Homomorphe Verschlüsselung

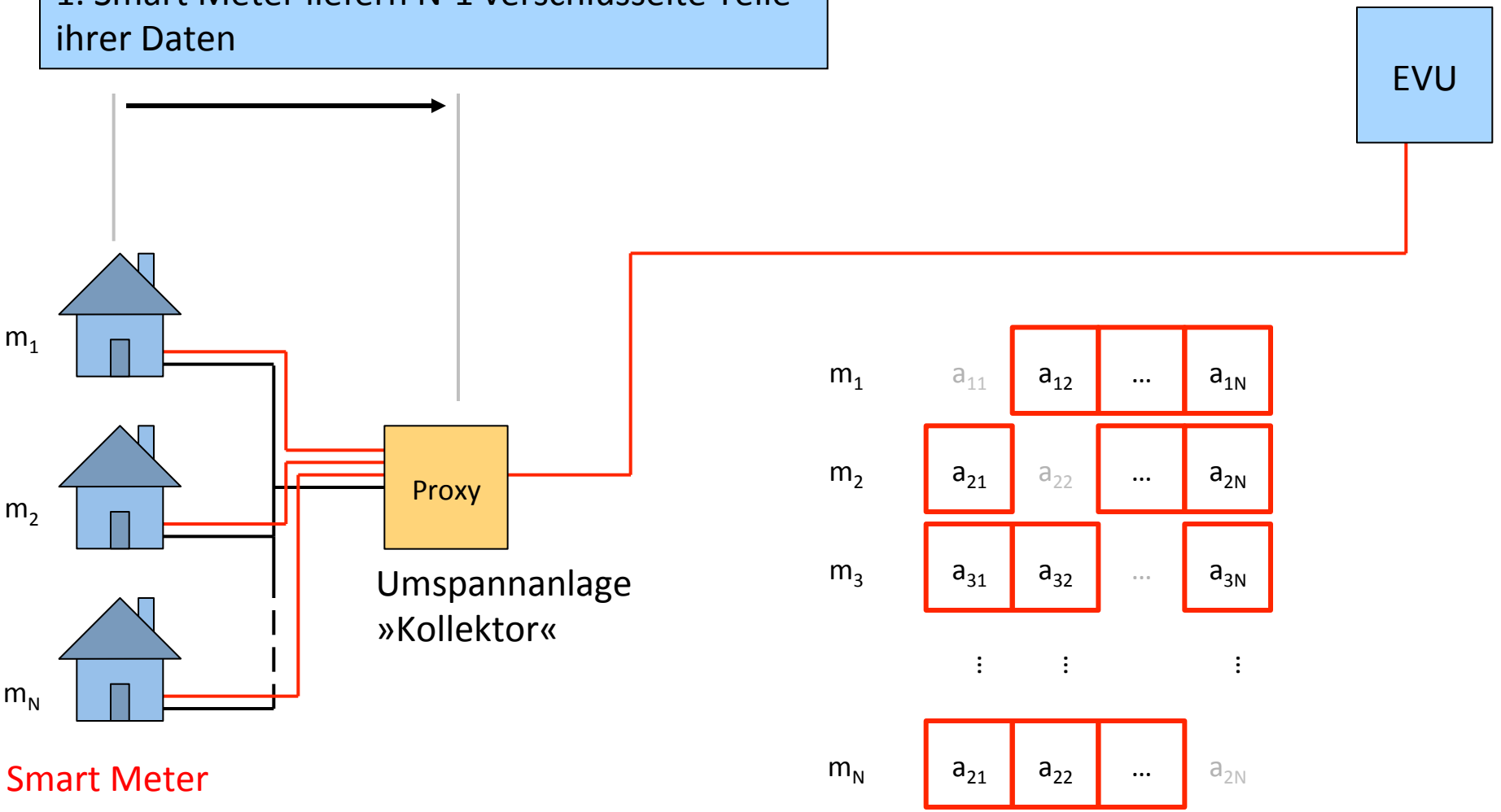
Garcia, Jacobs, 2010



Ansatz Homomorphe Verschlüsselung

Garcia, Jacobs, 2010

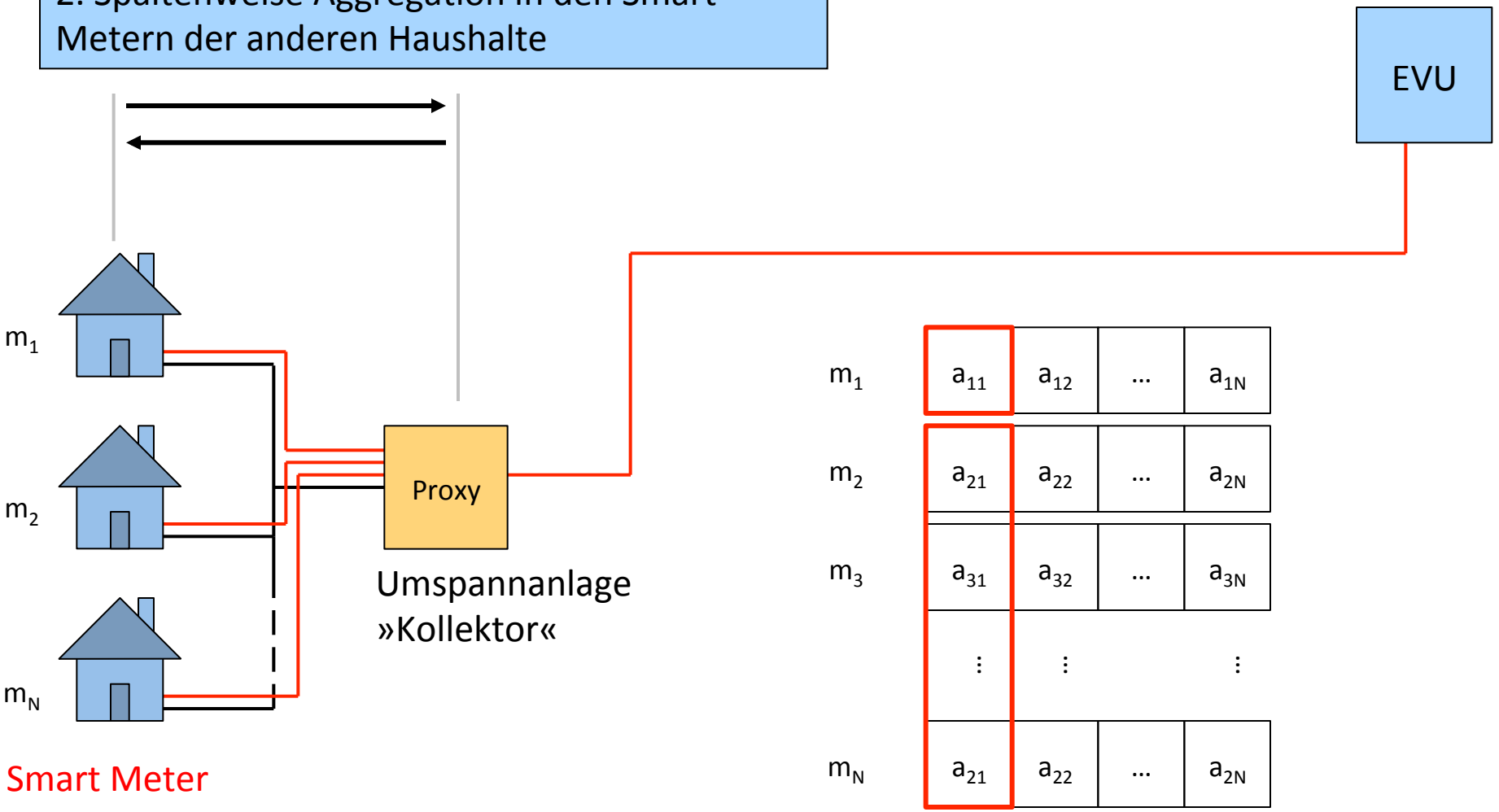
1. Smart Meter liefern N-1 verschlüsselte Teile ihrer Daten



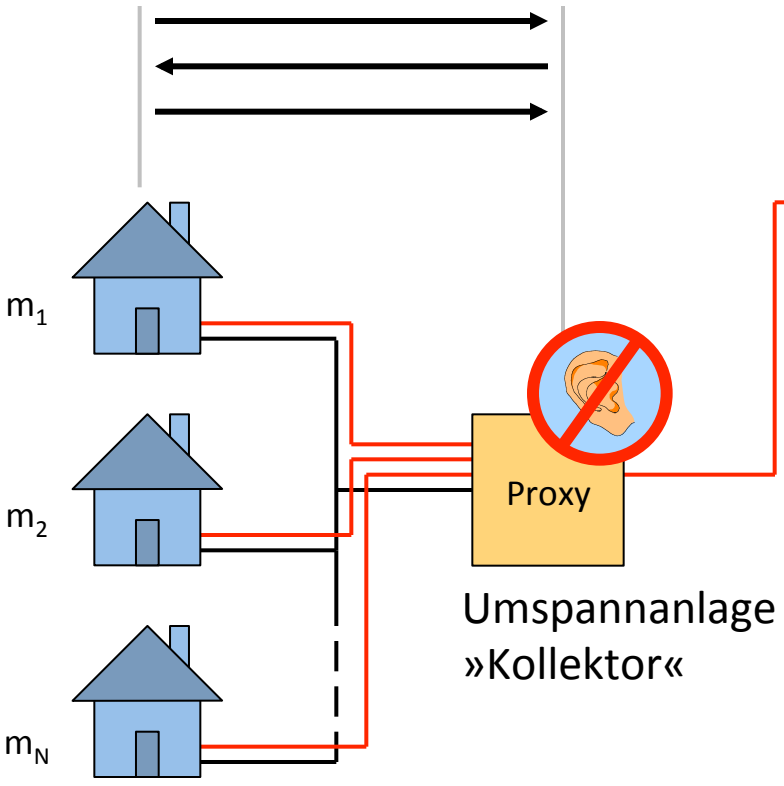
Ansatz Homomorphe Verschlüsselung

Garcia, Jacobs, 2010

2. Spaltenweise Aggregation in den Smart Metern der anderen Haushalte



3. Aggregierte Spalten werden an Kollektor übertragen

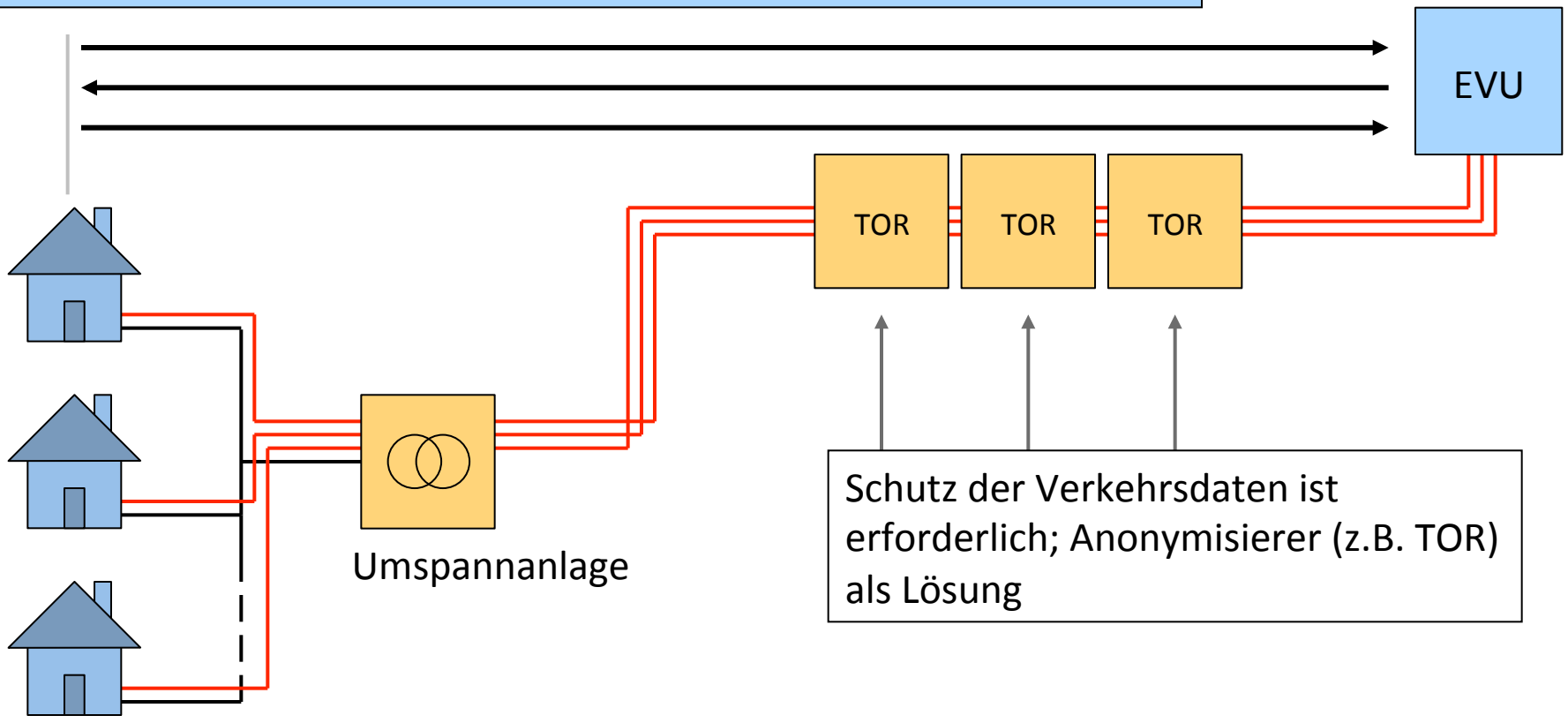


m_1	a_{11}	a_{12}	…	a_{1N}
m_2	a_{21}	a_{22}	…	a_{2N}
m_3	a_{31}	a_{32}	…	a_{3N}
	⋮	⋮		⋮
m_N	a_{21}	a_{22}	…	a_{2N}

Ansatz Zero Knowledge Proof of Knowledge

Jeske, 2011

Interaktives Protokoll ermöglicht ohne Identifizierung den Nachweis der Echtheit der Smart Meter Daten



www.informationisbeautiful.net/visualizations/worlds-biggest-data-

information is beautiful

ideas, issues, knowledge, data — visualized!

Home About Blog Workshops Contact

Information is Beautiful
the best-selling infographic classic
Now in Second Edition
revised, recalculated and reimagined

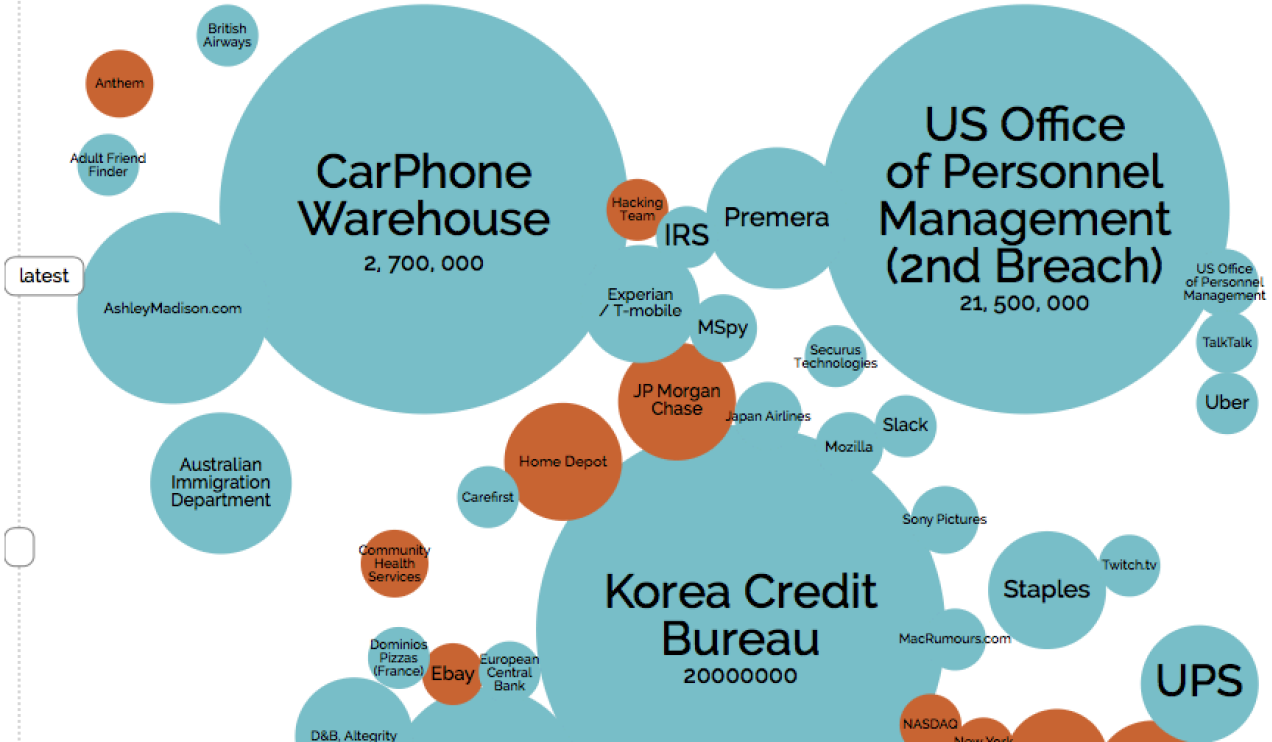
World's Biggest Data Breaches

Selected losses greater than 30,000 records

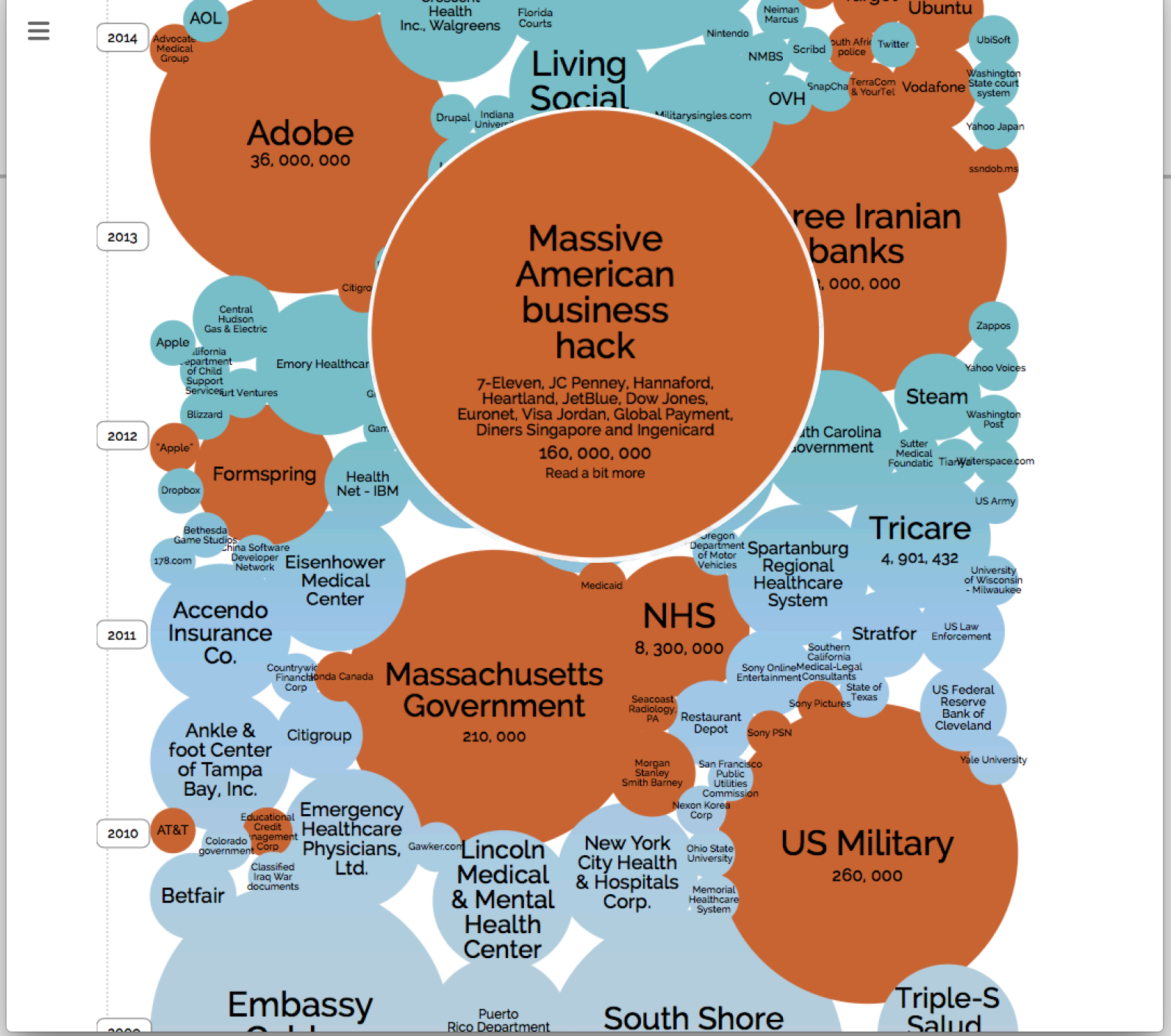
(updated 2nd October 2015)

interesting story

YEAR | BUBBLE COLOUR | YEAR | METHOD OF LEAK | BUBBLE SIZE | NO OF RECORDS STOLEN | DATA SENSITIVITY | SHOW FILTER



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Der Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)

- Unsere Forschungsthemen (Auswahl)
  - Informationssicherheitmanagement, IT-Grundschutz, ISO 27001
  - Privacy im Internet, Schutz vor Beobachtung, IT-Forensik
  - Sichere und datenschutzfreundliche Vernetzung von Fahrzeugen
  - Sicherheit und Datenschutz in mobilen Systemen

- Beiträge und (interdisziplinäre) Ergebnisse
  - Begleitung von Gesetzgebungsverfahren aus technischer Sicht
  - Erforschung des Spannungsfeldes von Freiheit und Sicherheit
  - Technische Lösungen zum Grundrechtsschutz
  - Informatik als gesellschaftliche Aufgabe

- Weitere Informationen
  - https://svs.informatik.uni-hamburg.de

Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

https://svs.informatik.uni-hamburg.de