UNIVERSITÄT ZU LÜBECK
STIFTUNGSUNIVERSITÄT
SEIT 2015

CyberSecurity in der Hospital IT

Thomas Eisenbarth

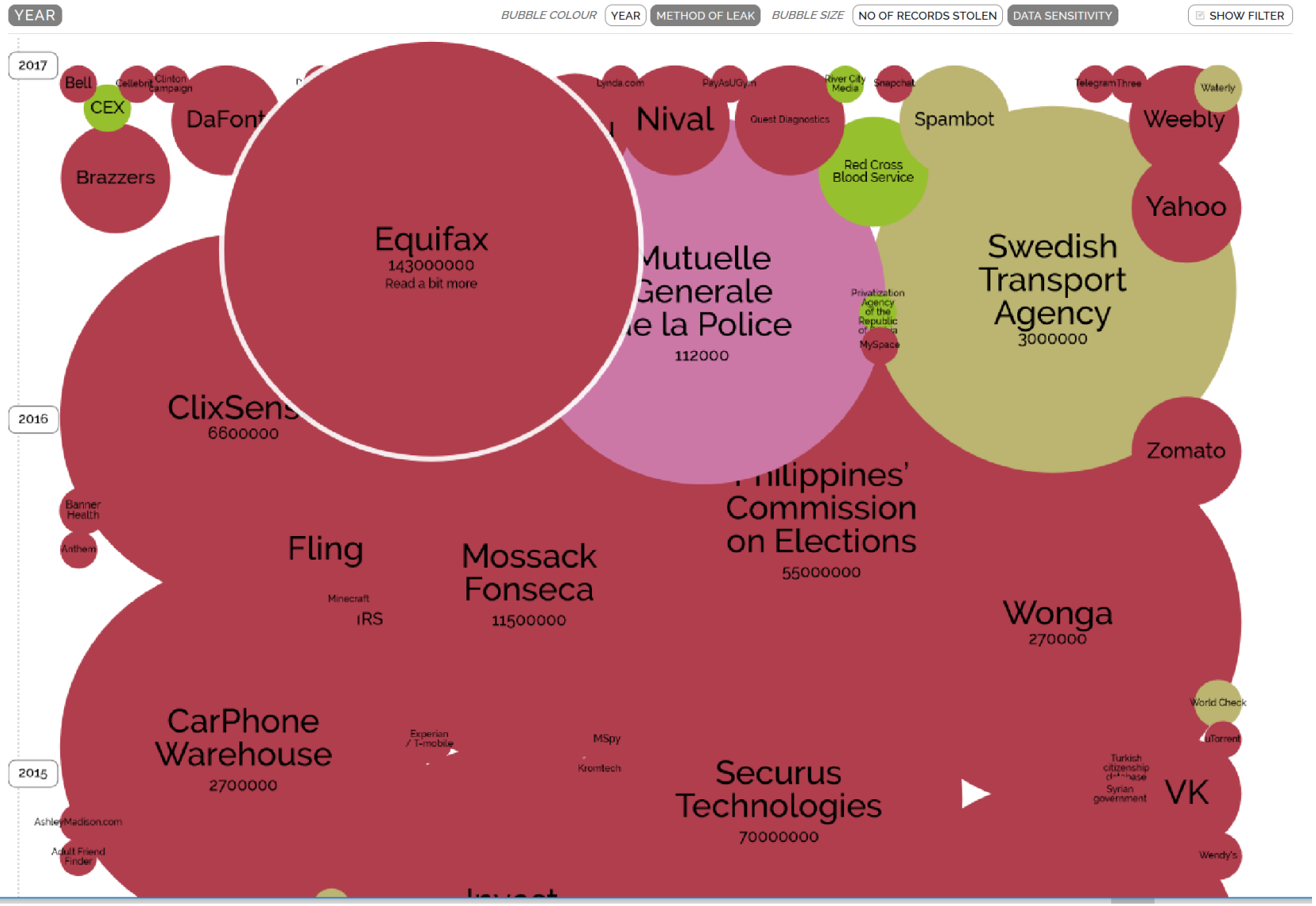
Insitut für IT Sicherheit – Universität zu Lübeck

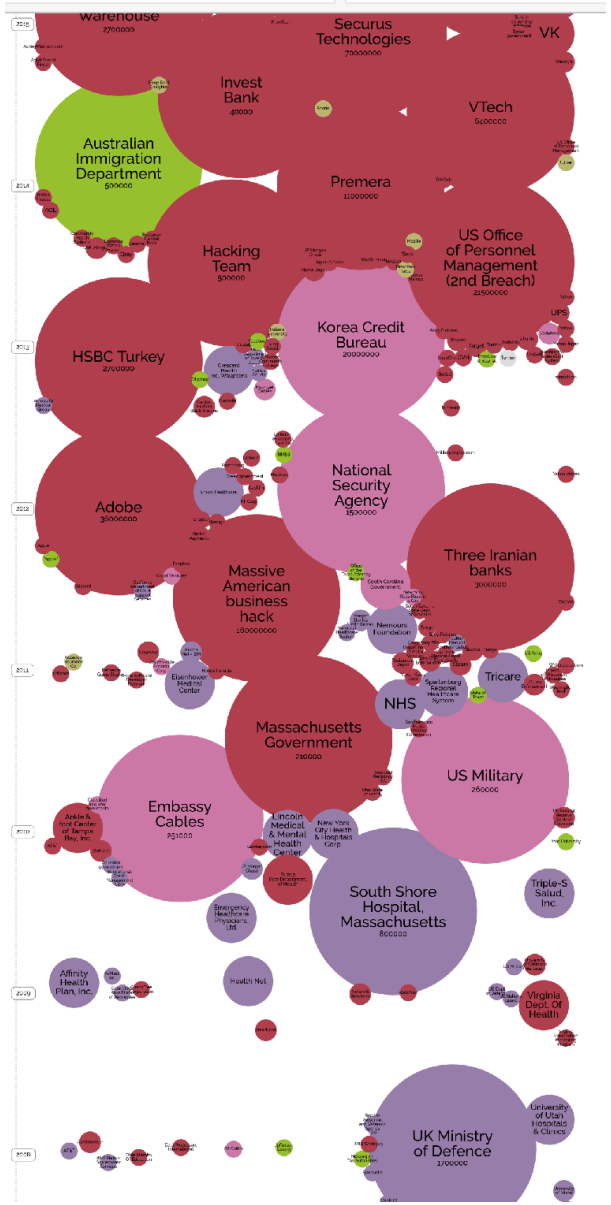
14.10.2017 Innvoationsforum Krankenhaus 4.0

World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 10th Sep 2017)





http://www.informationisbeautiful.net

Digitalisierung

- Zunehmende Vernetzung sämtlicher Lebensbereiche
- Nutzerdaten werden erfasst, gespeichert, verarbeitet

Quelle: 2015 Cost of Data Breach Study" by Ponemon Institute

Herausforderungen:

Sicherheit

Zuverlässigkeit

Privatheit

Digitalisierung im Krankenhaus

Internet of Things

- Vernetzung von medizinischen Geräten
- Patient Empowerment
- Telemedizin
- Gesundheitskarte

Cloud und Big Data

- eHealth und Elektronische Patientenakte
- Datenbanken

Internet of Things: Herzschrittmacher

- **Herzschrittmacher:**
  - Lebenswichtiges Gerät, **im Körper**, Betriebszeit ca. 10 Jahre
  - Konfiguration über Funkschnittstelle → Was könnte schief gehen?

- **2016-08-25** MedSec und MuddyWaters veröffentlichen Schwachstellen
  - Report attestiert St Jude Medical (Abbott) Schrittmachern katastrophale Sicherheit
  - Sicherheitsfirma und Finanzinvestor wetten auf fallende Kurse → Kurs bricht ein

- **2017-08-29** FDA: Produkt Rückruf
  - 13.000 Patienten zu Update ins Krankenhaus **in Deutschland** (ca. 100.000 weltweit)

https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

Aktuelle Forschungsthemen in Kryptografie

- Sicherung von neuen Technologien wie IoT Geräten und Cloud
  - Damit Geräte sicher und zuverlässig vernetzt werden können
- Post-Quantum Kryptographie
  - Damit heute erfasste Daten auch in >30 Jahren sicher sind
- Fully-Homomorphic Encryption und Alternativen
  - Damit sensible Daten sicher und ohne Verletzung der Privatsphäre des einzelnen verarbeitet und ausgeertet werden können.

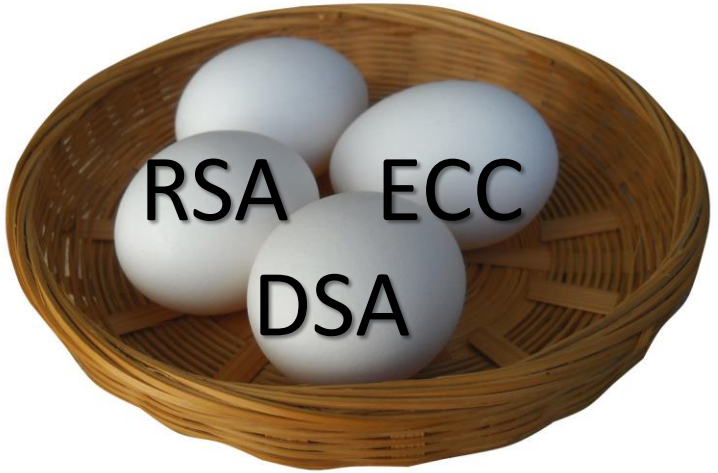
Sichere Produktentwicklung

Wie kann man Fälle wie bei St. Jude Medical verhindern?

- Besseres Design
  - Security Experten einbinden (Consulting)
  - Penetration Testing
- Prozesse anpassen
  - Incident Response Team
  - Secure Updates
- Zertifizierung (Common Criteria)
  - Prüfung durch Speziallabore: teuer und langwierig
  - Hohe Zuverlässigkeit für statische Produkte

Post Quantum Kryptografie

- Gängige Asymmetrische Kryptografie
  - RSA
  - ECC
  - DSA
- Beruhen auf gleichen Annahmen
- Physik: Quantencomputer in 10-20 Jahren
  - Alle gängigen asymmetrischen Verfahren unsicher

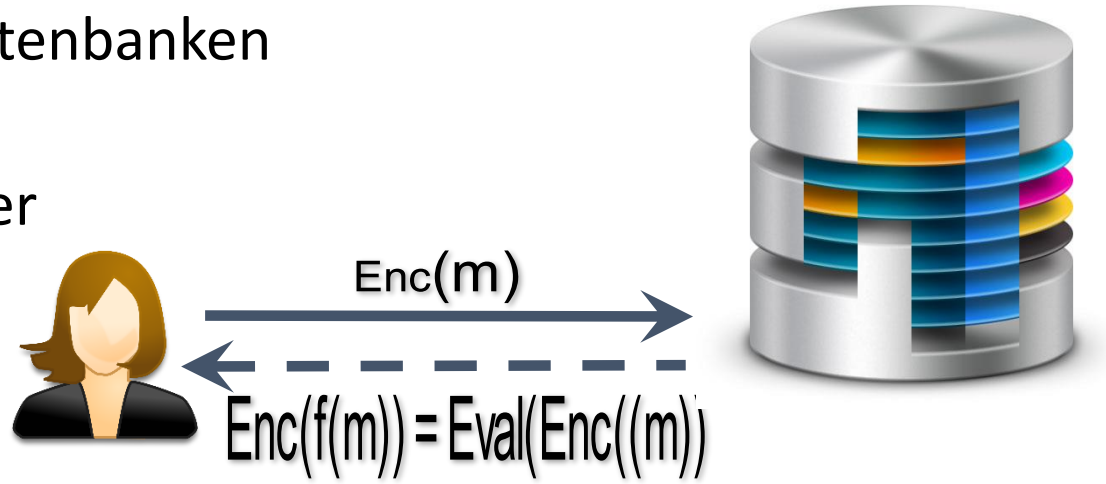


Post Quantum Kryptographie

- **NIST:** Call for Alternatives:
  - Lattices
  - Code-Based Kryptographie
  - Hash-based Crypto
  - Isogenies
- Standard in 2-5 Jahren
  - Verbreitung in Produkten: 10 Jahre?
- Übergang:
  - Kombinationslösungen: Etabliertes Verfahren + Post Quantum Verfahren

Fully Homomorphic Encryption

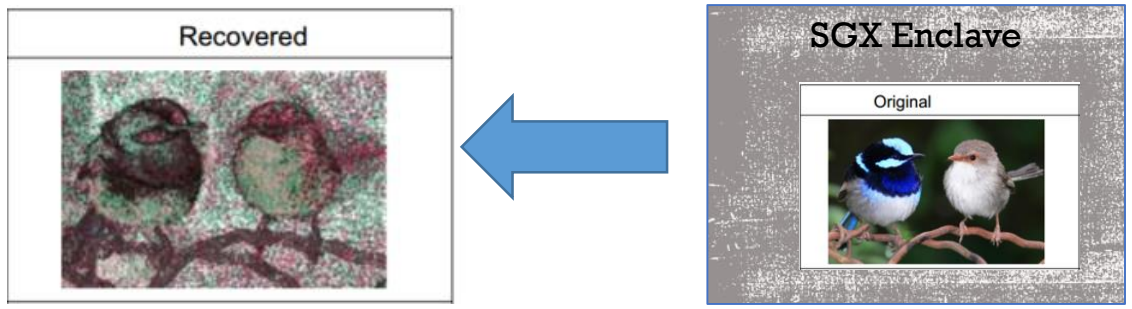
- Berechnungen auf verschlüsselten Daten
- **Vision:**
  - Datenverarbeitung auf verschlüsselten Datenbanken
  - Nur Ergebnisse werden entschlüsselt
  - Daten jedes einzelnen Patienten sind sicher

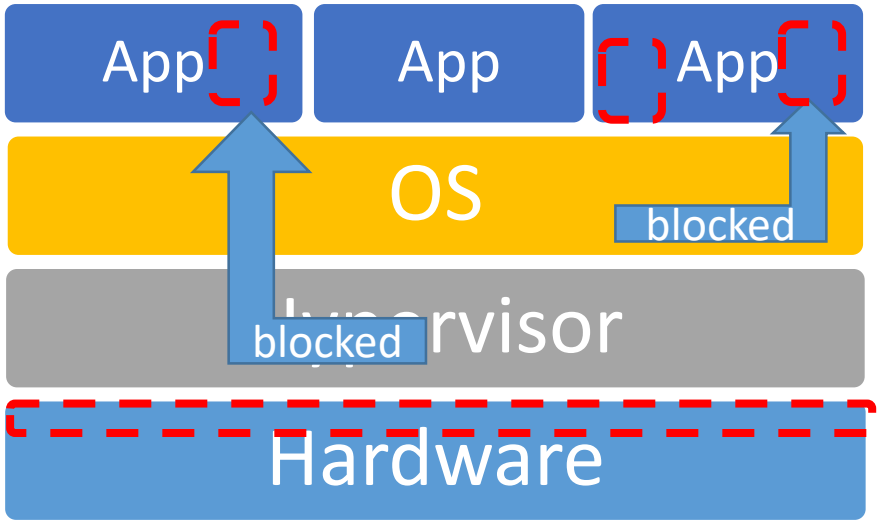


- **Realität:**
  - Verfahren sind extrem rechen- und Speicherintensiv
  - Einfachere Rechnungen für Spezialanwendungen möglich

Fully Homomorphic Encryption: Alternativen

- Idee: Daten nur in sicherer Umgebung entschlüsseln
- Mögliche Lösung: Trusted Execution Environments
  - Daten werden im **geschützten Bereich der CPU** entschlüsselt und verarbeitet
  - Schnell, Günstig, Sicher (oder?)
- Ja, aber: Laufzeitverhalten
  - Mikroarchitekturangriffe sind möglich

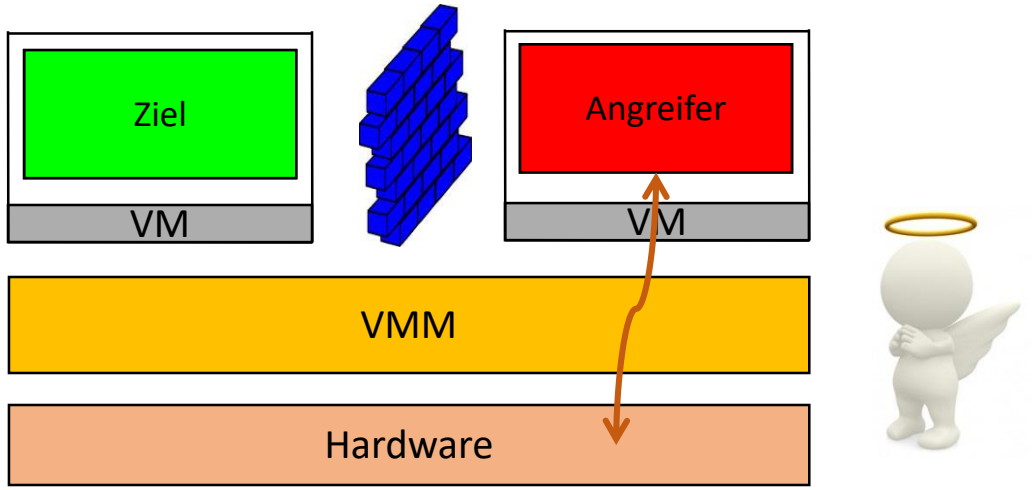




[XCP15] Yuanzhong Xu, Weidong Cui, Marcus Peinado. *Controlled-channel attacks: Deterministic side channels for untrusted operating systems*. IEEE S&P, 2015.
[MIE17] Ahmad Moghimi, Gorka Irazoqui, Thomas Eisenbarth. *CacheZoom: How SGX Amplifies The Power of Cache Attacks*. CHES 2017.

Cloud: Sicherheit durch Isolation

- Cloud: mehrere Nutzer teilen sich Rechnerinfrstruktur
- Hypervisor (VMM) sichert Isolation durch Virtualisierung
- VMs können gegenseitiges Laufzeitverhalten durch Nutzung von bestimmten Ressourcen beeinflussen
- Laufzeitverhalten: Schlüsselextraktion in schwachen Krypto-Bibliotheken auf EC2 möglich



[IGI+16] MS Inci, B Gulmezoglu, G Irazoqui, T Eisenbarth, B Sunar. *Cache attacks enable bulk key recovery on the cloud* CHES 2016

IT Sicherheit in Medizinischen Anwendungen

- Neue Kryptographische Dienste
  - Neue Services: Fully Homomorphic Encryption
  - Post-Quantum Verfahren machen Crypto zukunftssicher
- Neue Sicherheitsarchitekturen:
  - Hardwareunterstützung hilft Systeme zu sichern
  - Kann neue Services ermöglichen
- Security-Aware Design:
  - Bessere Prozesse und Entwurfsstrategien
  - Sicherheit durch Security Audits und Penetration Testing

Vielen Dank

Thomas.Eisenbarth@uni-luebeck.de

Institut für IT Sicherheit

www.its.uni-luebeck.de

UNIVERSITÄT ZU LÜBECK
STIFTUNGSUNIVERSITÄT
SEIT 2015