Alice und Bob im Wunderland

Was wir aus Krypto-Fails lernen können

Internet Security Days 2018

Inés Atug, Managing Consultant

HISOLUTIONS

Über mich

Inés Atug

- Managing Consultant bei der HiSolutions AG
- seit über 7 Jahren in der Informationssicherheit tätig
- berät und begleitet Unternehmen bei der Einführung von ISMS und Erstellung IT-Sicherheitskonzepten
- Spezialthemen: Cloud-Security, Kryptographie und Verschlüsselung, KRITIS
- Postgraduate Certificate in Mathematics, Open University, UK
- Bachelor of Science (hons) Mathematics, Open University, UK
- Master of Science in Applied IT Security, Ruhr-Universität Bochum
- U.a. zertifizierter Penetrationstesterin (GIAC)

Leistungsportfolio im Security Consulting

Penetrationstests/
Technische Audits

Cyber-Response/
Forensik

ISMS
ISO

ISMS
Grundschutz

Datenschutz

Auditierung/
Zertifizierung

Business
Continuity

Crisis
Management

IT- Notfall-
management

Konzepte/
Risikoanalysen

Notfall- und
Krisenübungen

Outsourcing/
Auslagerungsmgmt.

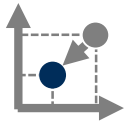
Wirtschafts-
grundschutz

Corporate
Security

Sicherheits-
strategie

Industrial
Security

Kritische
Infrastrukturen

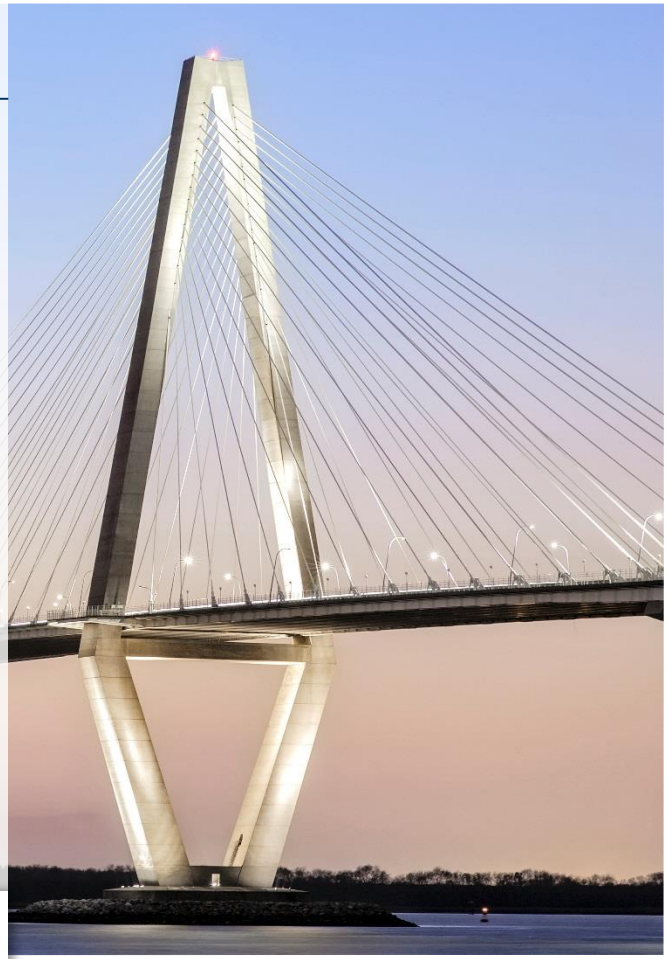


Risk Management

HISOLUTIONS

AGENDA

1 Erreichbare Schutzziele
2 Kerckhoff‘sche Prinzip
3 Schlüsselmanagement
4 Integrität wird nicht durch Verschlüsselung sichergestellt
5 Fehler bei der Implementierung
6 Ausblick: Quantencomputing



HISOLUTIONS

Mit Kryptografie erreichbare Schutzziele

Vertraulichkeit	• Eine Nachricht soll nur vom bestimmten Empfängerkreis gelesen werden können.
Integrität	• Eine Modifikation einer Nachricht kann bemerkt werden.
Authentizität	• Der Verfasser einer Nachricht kann eindeutig identifiziert werden.
Verbindlichkeit	• Der Verfasser einer Nachricht kann die Erstellung nicht abstreiten.

HISOLUTIONS

„Nearly every inventor of a cipher system has been convinced of the unsolvability of his brain child.“

David Kahn in seinem Buch „The Codebreakers“

Kerckhoff‘sche Prinzip:
Das Kryptosystem darf keine Geheimhaltung erfordern …

HISOLUTIONS

Algorithmus Magenta

- **M**ultifunctional **A**lgorithm for **G**eneral-purpose **E**ncryption and **N**etwork **T**elecommunication **A**pplications
- Entwicklung durch die Telekom
- Eingereicht für AES

- 1. AES Konferenz am 20. August 1998
  - Cipher wurde nicht zuvor bekannt gegeben
  - Während der 20-minütigen Präsentation fanden mehrere anwesende Kryptologen theoretische Angriffsmöglichkeiten.
  - Am gleichen Tag wurde eine Kryptoanalyse verfasst, die die praktischen Angriffe beschrieb.

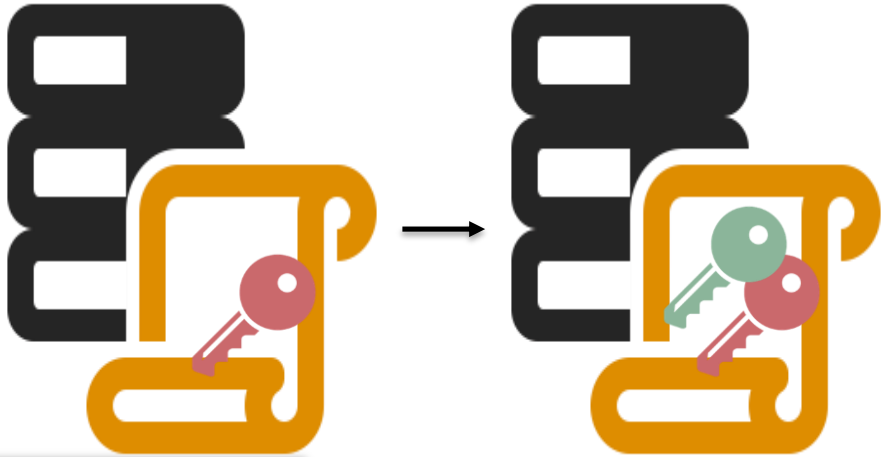
Laut Kerckhoff sollte nur der Schlüssel geheim sein. Wie kann ich dies sicherstellen?

Das muss das **Schlüsselmanagement** sicherstellen!

HISOLUTIONS

Schlüsselmanagement: Kompromittierte Schlüssel

- Szenario
  - Massendaten
  - Daten müssen hochverfügbar sein
- Wie gestaltet man den Prozess beim Austausch eines kompromittierten Schlüssels?
  - Alle Datensätze werden zusätzlich mit dem neuen Schlüssel verschlüsselt



HISOLUTIONS

Schlüsselmanagement: Kompromittierter Schlüssel

- Sobald erneut auf das Datum zugegriffen wird, wird es 2x entschlüsselt und anschließend mit dem neuen Schlüssel verschlüsselt.

HISOLUTIONS

Schlüsselwiederherstellung in HSMs

- Szenario:
  - HSMs stehen in zwei Rechenzentren (unterschiedliche Länder)
  - Key Recovery Verfahren: 3 von 5 Chipkarten
  - Lagerung der Chipkarten im Tresor des Hauptstandorts
  - Hochverfügbarkeit gefordert
- Was wenn ein HSM im Rechenzentrum (nicht Hauptstandort) ausfällt?

➔ Drei Mitarbeiter müssen an anderen Standort reisen

➔ Am Hauptstandort sind max. 2 Chipkarten vorhanden

Wir benötigen eine Software, die die Integrität der Daten sicherstellt. Dies möchte der Hersteller mit Verschlüsselung erreichen. Geht das?

Verschlüsselung stellt **keine** Integrität sicher!

HISOLUTIONS

„Implementing cryptography involves getting everything right, and the more complexity there is, the more there is to get wrong.“

Bruce Schneier

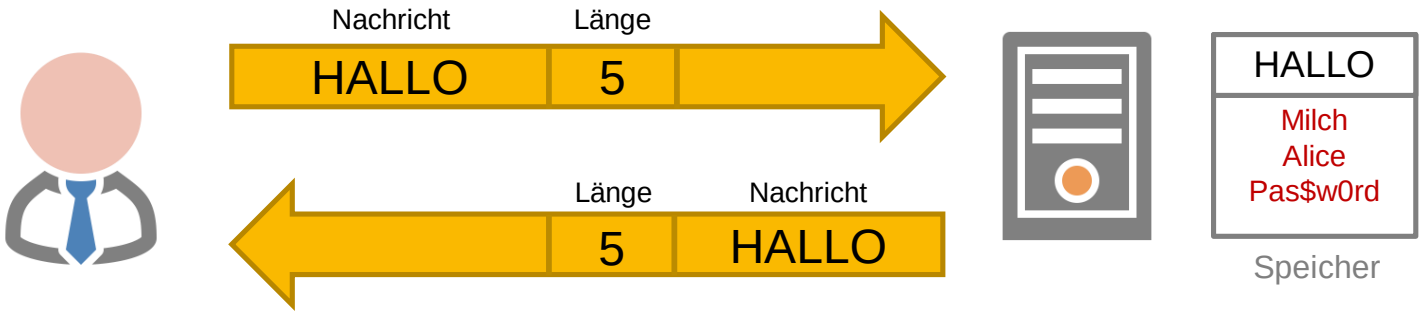
HISOLUTIONS

Implementierung von Kryptografie in Malware

- Ransomware: Petya
  - Stromchiffre Salsa20
  - 3 Verschlüsselungsfehler führen zu einem 512-Bit langen verschlüsselten Text, der aus 256 Bit Konstanten und vorhersagbaren Werten besteht.
  - Weitere Informationen unter: https://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/
- Ransomware: DirCrypt
  - Erste 1024 Bit mittels RSA verschlüsselt
  - Danach wird mittels RC4 verschlüsselt
  - RC4 Schlüssel wird jeweils an die verschlüsselte Daten angehängt
  - Weitere Informationen unter: https://www.golem.de/news/dircrypt-ransomware-liefert-schluessel-mit-1409-108940.html

Ausflug: Heartbeat-Erweiterung für TLS

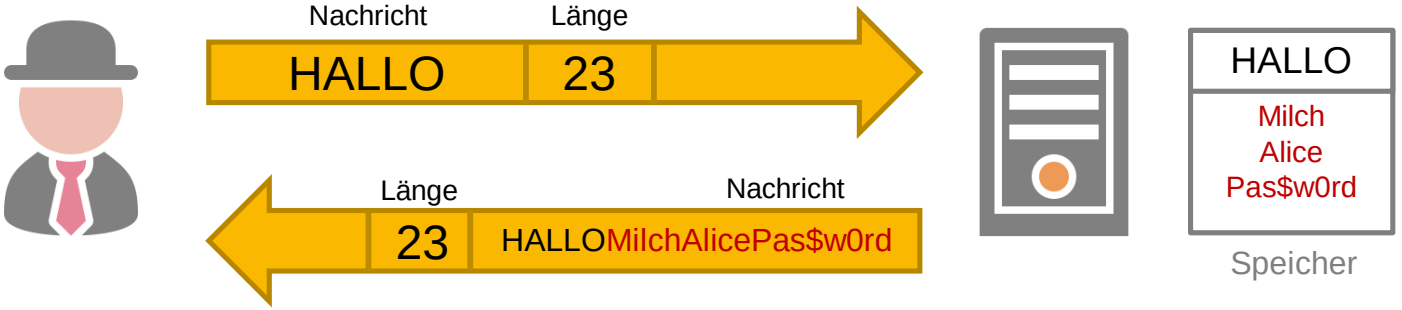
- Überprüfung der Verbindung zum Server mittels einer bis zu 16 kByte großen Menge an beliebigen Daten (Payload und Padding)



HISOLUTIONS

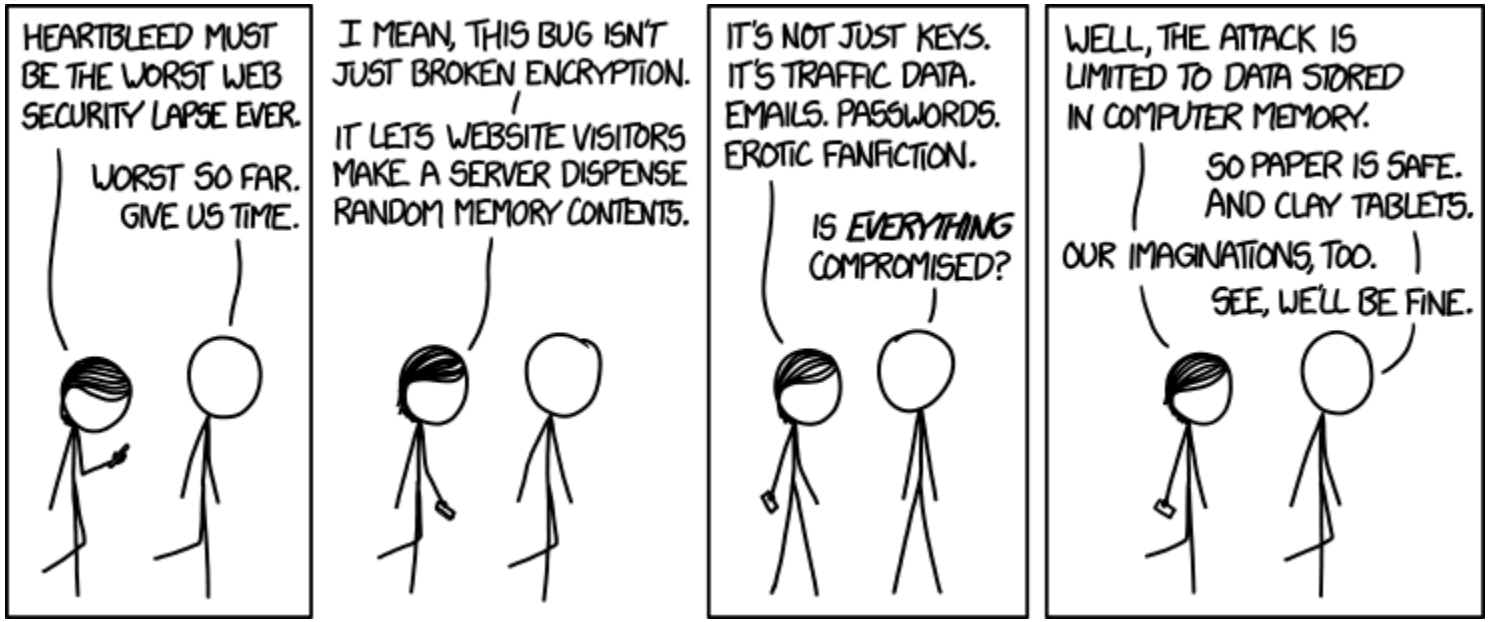
Heartbleed der Angriff

- OpenSSL-Versionen 1.0.1 bis 1.0.1f waren betroffen
- Fehler in der Implementierung, die Länge wurde nicht geprüft
- Aufgrund dessen kann der Angreifer bis zu 16 kByte auslesen.



HISOLUTIONS

IST HEARTBLEED DIE SCHLIMMSTE SCHWACHSTELLE?



Quelle: https://xkcd.com/1353/

HISOLUTIONS

Dann kam Knuddels …

- Besteht seit 1999
- Zirka 1.872.070 Datensätze (Nickname, Passwort und zum Teil E-Mail-Adressen andere Profilangaben)
- Passwort wurde gehasht **und im Klartext** gespeichert.

„Im Jahr 2016 wurde die Speicherung der Passwörter als Hash eingeführt. Die nicht gehashte Version der Passwörter blieb allerdings erhalten, mit der Nutzer am Versenden ihres eigenen Passworts über unsere Plattform durch einen Filter gehindert wurden.“

Antwort der Anwaltskanzlei von Knuddels.de auf Anfrage von Golem (https://www.golem.de/news/datenleck-warum-knuddels-seine-passwoerter-im-klartext-speicherte-1809-136483.html)

HISOLUTIONS

AUSBLICK: QUANTENCOMPUTING

- Quantencomputer lösen mathematische Probleme in deutlich weniger Schritten, als dies mit klassischen Computer der Fall ist.
  ➔ Mathematische Probleme, auf denen die asymmetrische Kryptografie beruht, werden sobald ausreichende Rechenleistung vorhanden ist, gebrochen sein.
- Wahrscheinlichkeit laut Prof. Mosca
  - Wahrscheinlichkeit von 1 zu 7, dass die asymmetrische Kryptosysteme in 2026 gebrochen sind.
  - Wahrscheinlichkeit von 50%, dass dies in 2031 der Fall ist.

HISOLUTIONS

Das schwächste Glied in der Kette …

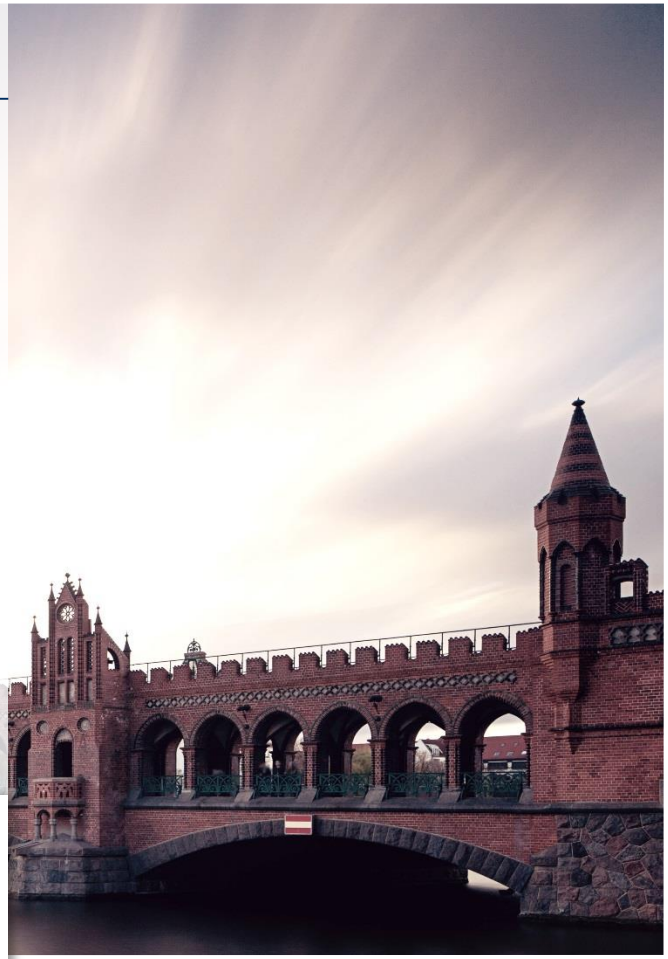
Kryptografie ist nur ein Kettenglied eines IT-Sicherheitskonzepts

HISOLUTIONS

HISOLUTIONS BEDANKT SICH FÜR IHRE AUFMERKSAMKEIT

HiSolutions AG

Bouchéstraße 12
12435 Berlin
info@hisolutions.com
www.hisolutions.com
+49 30 533 289 0



HISOLUTIONS