Kryptographie und Fehlertoleranz für Digitale Magazine

Stefan Lucks

Professur für Mediensicherheit
Bauhaus-Universität Weimar

13. März 2013

Wie kam es zu diesem Beitrag?

- Projekt “Digitales Magazin” im Freistaat Thüringen
- “Bedrohungsszenarien” des Staatsarchiv
- Stellungnahme:
  - Methoden der Informatik um derartige Bedrohungen abzuwehren
  - konkrete Empfehlungen zu jedem einzelnen Bedrohungsszenario

Gefahren für Digitale Magazine
. . . und was die Informatik zu ihrem Schutz leistet

Gefahr	Teilgebiet der Informatik
Zufälle menschliches Versagen Naturkatastrophen	Zuverlässige Systeme
gezielte und vorsätzliche Angriffe Datenmanipulation Ausspähung	Kryptographie

Zuverlässige Systeme für Digitale Magazine

Schutz vor Verlust und zufälliger Verfälschung durch Datenredundanz:

Fehlererkennende Codes.

Fehlerkorrigierende Codes.

Vollständige Kopien.

Heute schon verbreitete Praxis.

Schwellwert-Verfahren. ("k aus n").

Verteile Daten auf n Stellen so daß jede beliebige Gruppe von k Stellen die Daten vollständig rekonstruieren kann.

Kryptographie für Digitale Magazine

Schutz der	symmetrisch	asymmetrisch
Vertraulichkeit	Verschlüsselung	Verschlüsselung
Authentizität	MACs*	Digitale Unterschriften

- symmetrisch: der gleiche Schlüssel für "Sender" und "Empfänger"
- asymmetrisch: ein öffentlicher, ein geheimer Schlüssel

Sonderfall: Kryptographische Hashfunktionen brauchen gar keinen Schlüssel.

---

* "Message Authentication Codes"

Kryptographische Sicherheit

Komplexitätstheoretische Sicherheit:

- Angriffe brauchen mehr Rechenzeit, als Angreifern je zur Verfügung stehen kann ("z.B. $10^9 *$ Google).

Informationstheoretische Sicherheit:

- Selbst Angreifer mit *unbeschränkter Rechenkapazität* sind garantiert erfolglos.

Risiken beim Einsatz der Kryptographie

Wachstum der SicherheDtsparameter. "Gesetz von Moore": die Rechenleistung eines neuen Computers verdoppelt sich alle 18 Monate.

Neue Erkenntnisse der Kryptanalyse. Bisher unbekannte Angriffe auf ein verwendetes Kryptosystem werden bekannt.

Schlüsselverlust. Die legitimen Nutzer kennen ihren eigenen Schlüssel nicht mehr.

Schlüsselkompromittierung. Der geheime Schlüssel wird Angreifern bekannt.

Bewertung der Risiken

Wachstum der Sicherheitsparameter. (Nicht relevant bei informationstheoretisch sicheren Kryptosystemen.)

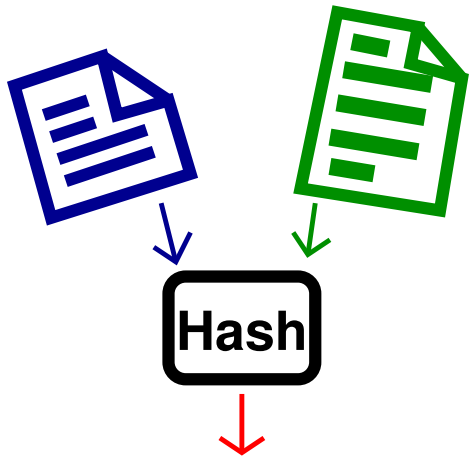
Neue Erkenntnisse der Kryptanalyse. (Nicht relevant bei informationstheoretisch sicheren Kryptosystemen.)
Problem für die asymmetrische Kryptographie, sollte jemals ein funktionsfähiger Quantencomputer gebaut werden!

Schlüsselverlust. (Nicht relevant bei Hashfunktionen.)
Vertraulichkeit: Totalverlust der Daten!
Authentizität: Ärgerlich, aber reparabel.

Schlüsselkompromittierung. (Nicht relevant bei Hashfunktionen.)

Hashfunktionen

- Eine **Hashfunktion** h bildet einen potentiell *großen* Input auf einen *kleinen* Output ab.
- Kollisionen, also Inputs $X \neq Y$ mit $h(X) = h(Y)$ sind katastrophal.
- Sogar schlimmer ist es, wenn man Urbilder finden kann: Gegeben Z, finde X mit $h(X) = Z$ (oft auch: gegeben Y finde $X \neq Y$ mit $h(X) = h(Y)$).



Universelle versus Kryptographische Hashfunktionen

Universell:

Gegeben eine beliebig lange Nachricht X, *und einen geheimen Schlüssel* K berechnet H_K einen kurzen *Fingerabdruck* $H_K(X)$ der Nachricht. Selbst ein Angreifer mit unbeschränkter Rechenzeit kann, wenn er K nicht kennt, nicht mit signifikanter Wahrscheinlichkeit Kollisionen oder Urbilder berechnen.

Universelle Hashfunktionen hängen von einem geheimen Schlüssel ab und sind informationstheoretisch sicher.

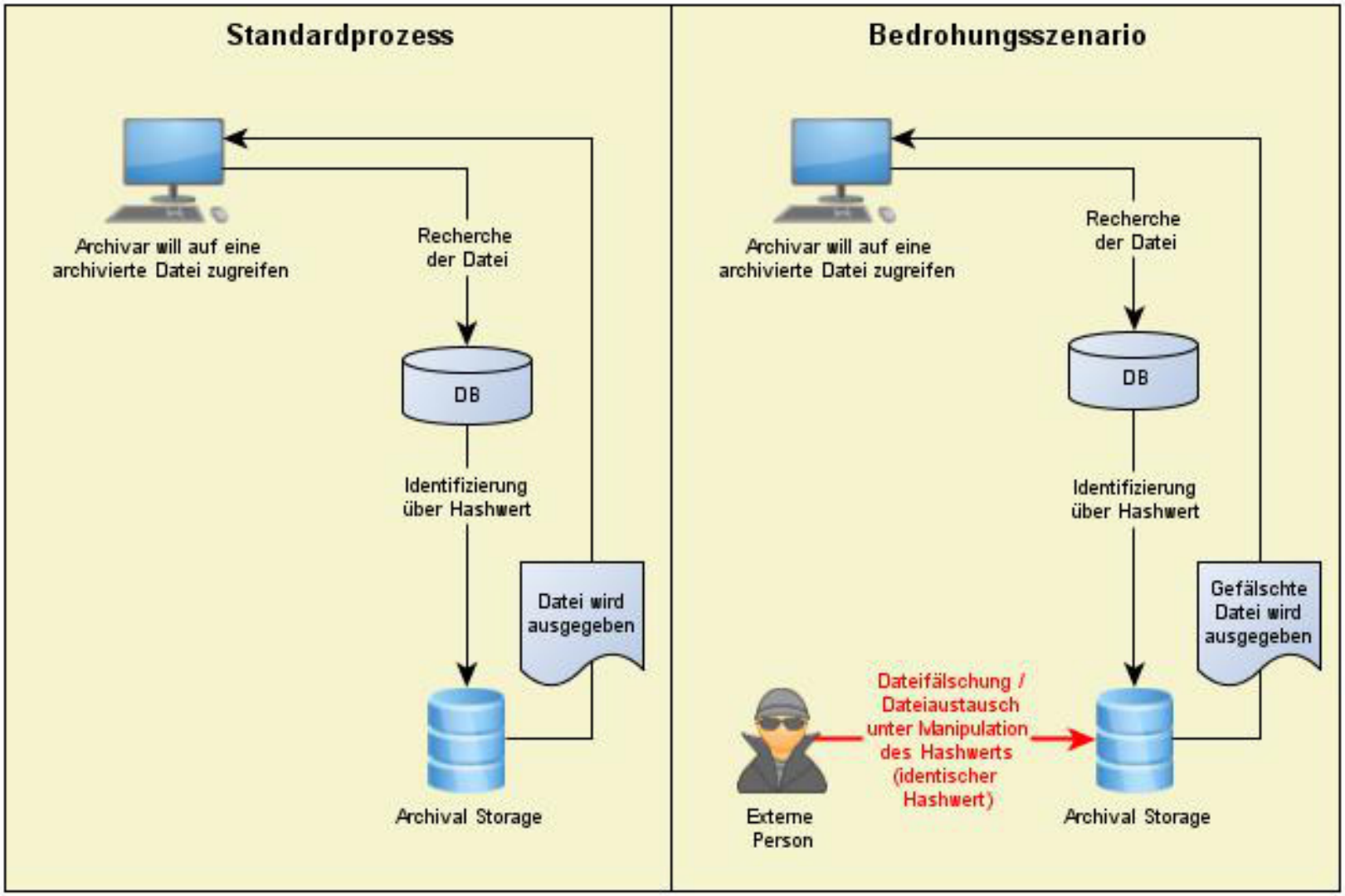
Kryptographisch:

Gegeben eine beliebig lange Nachricht X, berechnet H einen kurzen *Fingerabdruck* $H(X)$ der Nachricht. Die Standard-Sicherheitsanforderungen an eine kryptographische Hashfunktion H sind, das es praktisch unmöglich ist, Kollisionen oder Urbilder zu berechnen.

Kryptographische Hashfunktionen brauchen zwar keine Schlüssel, sind aber immer nur komplexitätstheoretisch sicher.

Beispielszenario

Fälschung/Austausch einer Datei im Archival Storage unter Manipulation des Hashwertes



Annahme

Wir unterscheiden zwischen einer Index-Datenbank (kurz “DB”) und dem eigentlichen Archival-Storage. Wir gehen davon aus, das bei einem Verlust der Index-Datenbank eine neue Index-Datenbank aus dem Archival-Storage neu erzeugt erden kann.

Drei Möglichkeiten für den Angreifer

1. Löschen regulärer Daten.
2. Hinzufügen irregulär Daten.
3. Manipulieren regulärer Daten
   - 3.1 Hash-Kollision tritt auf. In diesem Fall verweist die Datenbank auf ein manipuliertes Dokument, d.h. man hat es hier mit einer Urkundenfälschung zu tun.
   - 3.2 Hash-Kollision tritt nicht auf. (entspricht der Kombination des Löschens regulärer und des Hinzufügens irregulärer Daten)

Empfehlungen

Dei Verwendung von kryptographisch sicheren Hashfunktion mit mindestens 256 bit Ausgabelänge, z.B. SHA-256/384/512; um Manipulationen entdecken zu können.
Von der Benutzung von MD5 und SHA-1 wird dringend abgeraten!

Der Einsatz universeller Hashfunktionen ist eine mögliche Alternative oder Ergänzung zum Einsatz kryptographischer Hashfunktionen.

Datenredundanz (das Vorhalten von Kopien) ist unverzichtbar, um nach einer entdeckten Manipulation den regulären Inhalt wiederherzustellen.

Risiken der Kryptographie

- **Kryptographische Hashfunktionen** sind (nur) komplexitätstheoretisch sicher. Deshalb muss man das Wachstum der Sicherheitsparameter und das Risiko neuer Erkenntnisse in der Kryptanalyse beachten. Dafür brauchen sie keinen Schlüssel.
- **Universelle Hashfunktionen** sind informationstheoretisch sicher, hängen aber von einem geheimen Schlüssel ab. Deshalb ist die sichere Speicherung des Schlüssels essentiell, die Risiken sind deshalb Schlüsselverlust und Schlüsselkompromittierung. Ggf. kann man den Schlüssel mit Schwellwert-Verfahren (k aus n) schützen.

Zusammenfassung und Schluss

- Digitale Magazine werden sowohl durch Zufälle als auch durch gezielte und vorsätzliche Angriffe bedroht.
- Zum Schutz vor ersteren gibt ed die Methoden der zuverlässigen Systeme.
- Dem Schutz gegen vorsätzliche Angriffe dient die Kryptographie.
- Die Methoden der Kryptographie, ihre Vorteile und ihre spezifischen Riskien sind schwierig zu verstehen – manche Methoden sind schlüsselabhängig, manche nicht, manche sind informationstheoretisch sicher, manche nicht ...