Verschlüsselung

ProSeminar Speicher- und Dateisysteme

Florian Wilkens

Gliederung

- Allgemeines zur Verschlüsselung
- Anwendungsbeispiel – Truecrypt
- Anwendungsbeispiel – PGP
- Verschlüsselnde Dateisysteme

ALLGEMEINES ZUR VERSCHLÜSSLUNG

- Einleitung / Motivation
- Verbreitete Konzepte

Einleitung / Motivation

- Was ist Verschlüsselung?
  - Informationsumwandlung
  - Eingabe: Klartext (bzw. Daten)
  - Ausgabe: nicht trivial interpretierbare Zeichenfolgen
- Warum Verschlüsselung?
  - Wachsende Vernetzung/Digitalisierung
  - Sinkende Möglichkeiten zum Erhalt der Privatsphäre
  - Steigende Risiken

Verbreitete Konzepte

- Symmetrische Verschlüsselung
  - Wichtigstes Merkmal: 1 Schlüssel
  - Sowohl zum Ver- als auch Entschlüsseln
  - Bekanntes Beispiel: Caesar-Verschlüsselung (~50 v. Chr.)

- Asymmetrische Verschlüsselung
  - Wichtigstes Merkmal: 2 Schlüssel
  - Öffentlicher Schlüssel <-> Privater Schlüssel
  - Vergleichsweise neu, daher kein triviales Beispiel
- Viele verschiedene Umsetzungen (nicht nur digital)!

ANWENDUNGSBEISPIEL – TRUECRYPT

- Warum symmetrische Verschlüsselung?
- Funktionsweise
- Performance

Warum symmetrische Verschlüsselung?

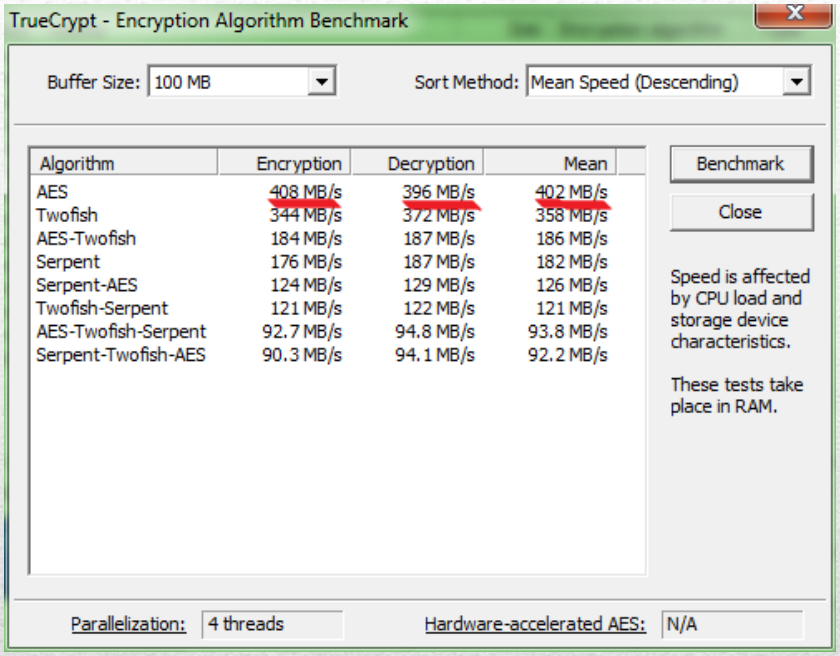
- Lediglich ein Schlüssel ist zu erinnern
- Hier: Kein Verlust an Sicherheit
- Erweiterte Konzepte werden schlicht nicht benötigt
- Allgemeines Merkmal von „lokalen Verschlüsselungen“

Funktionsweise

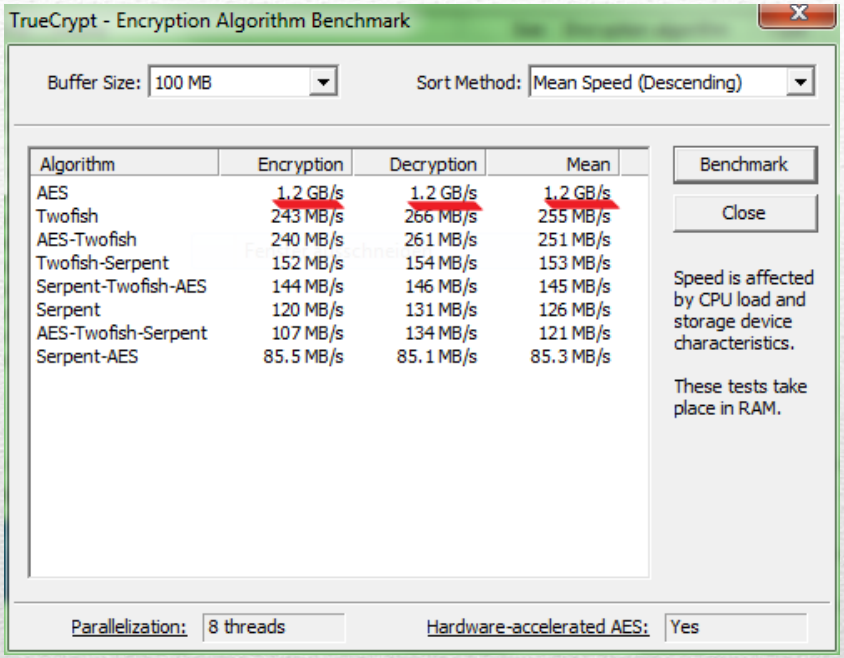
- Mehrere Möglichkeiten
  - Verschlüsselter Container
  - Verschlüsselte (Daten-)Partition
  - Verschlüsselte (System-)Partition

- Wahl eines Algorithmus (AES, Twofish, Serpent)
- Mounten des Containers / der Partition
  - „On-the-fly“ encryption
- Daten vorher nicht einsehbar
  - ➢ „Plausible Deniability“

Ohne Hardwareunterstützung



Mit Hardwareunterstützung

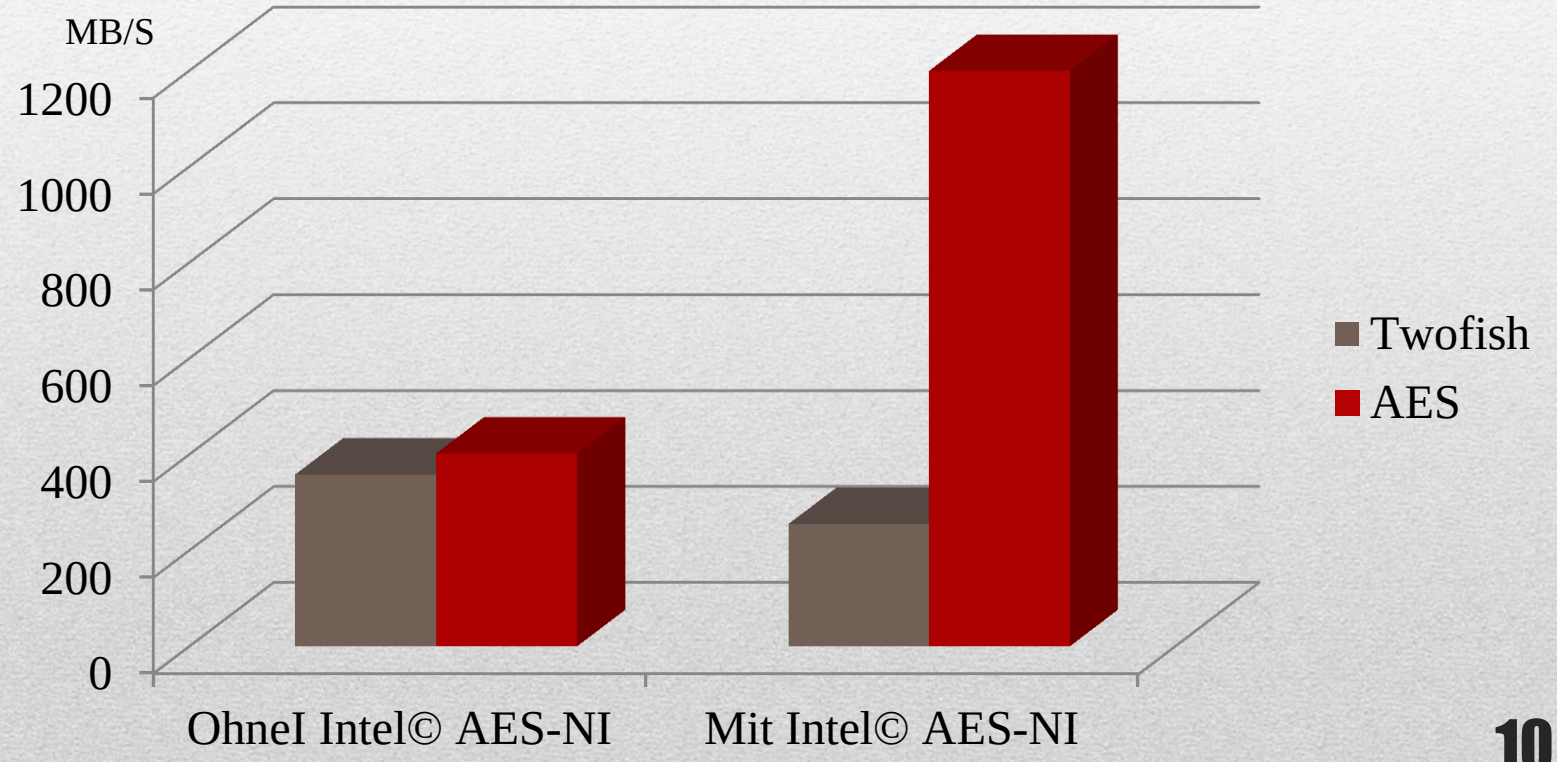


Intel Core2Quad Q9550@2.83GHz

Intel Core i7 Q2360M@2.00GHz

Performancevergleich I

Performancevergleich II



ANWENDUNGSBEISPIEL – PGP

- Warum asymmetrische Verschlüsselung?
- Verfahren

Warum asymmetrische Verschlüsselung?

- Erleichterter Schlüsselaustausch
- Erweitere Verifizierungsmöglichkeiten
  - Digitale Signatur
- Aber: Kein Gewinn an Sicherheit beim Verschlüsseln
- Oft ein Merkmal von „verteilten Verschlüsselungen“

Verfahren

- Verwendeter Algorithmus: RSA + ein symmetrischer
- Aus 2 Primzahlen werden 2 Schlüssel berechnet, sodass
  - Private Key (e, N) <-> Public Key (d, N)
  - $C \equiv K^e \ mod \ N$ und K $\equiv C^d \ mod \ N$ gilt
  - → deutlich erhöhter Rechenaufwand!
- Umgekehrt kann eine Nachricht auch signiert werden

VERSCHLÜSSELNDE DATEISYSTEME

- Idee / Ansatz
- Umsetzungen
- Allgemeine Probleme

Idee / Konzept

- Datei/Block wird mit “zufälligem“ Schlüssel symmetrisch(!) verschlüsselt
- Schlüssel wird mit Public Key(s) verschlüsselt in Dateieigenschafen/Ende des Blocks abgelegt
- Auch mehrbenutzerfähig, da asymmetrisch

- Diverse Probleme
  - Identische Blöcke
  - Was „darf“ das Betriebssystem?
  - Macht strenge Zugriffsrechte erforderlich

Umsetzungen

- EFS („Encrypting File System“) für MS Windows
  - Integrierbar in NTFS
  - Nur Datei-/Ordnerverschlüsselung
  - (Unsichere) Methode zur Datenwiederherstellung

- dm-crypt mit LUKS unter GNU Linux
  - Informationen im Partitions-/Blockheader
    - Leichte Erkennbarkeit
    - Plausible Deniability schwierig bis unmöglich

Allgemeine Probleme

- Diverse Angriffsmöglichkeiten
  - Watermark-Angriffe
  - Erlangen des Passworts
  - (Schwachstellen des Algorithmus)
- (Meist) nicht wirksam im Betrieb
  - Begrenzte Einsatzgebiete

Vielen Dank für eure Aufmerksamkeit!

Quellen

- http://de.wikipedia.org/wiki/RSA-Kryptosystem
- http://de.wikipedia.org/wiki/Verschlüsselung
- http://de.wikipedia.org/wiki/Plausible_deniability
- http://de.wikipedia.org/wiki/Encrypting_File_System
- http://de.wikipedia.org/wiki/dm-crypt
- http://de.wikipedia.org/wiki/Pretty_Good_Privacy

Quellen II

- http://de.wikipedia.org/wiki/Festplattenverschl%C3%BCsselung
- http://de.wikipedia.org/wiki/Wasserzeichenangriff
- http://www.intel.de/content/www/de/de/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html
- http://de.gentoo-wiki.com/wiki/DM-Crypt

symmetrisch

- „lokale Verschlüsselungen“
- 1 Schlüssel

- Einsatz in Dateisystemen
  - Direkte Verschlüsselung

- Resultierendes Problem
  - Identische Blöcke

asymmetrisch

- „verteilte Verschlüsselungen“
- 1 public + 1 private key

- Einsatz in Dateisystemen
  - Verschlüsselung des Schlüssels

- Resultierendes Problem
  - Zugriffsrechte

Übersicht