Angewandte Informatik

Hochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Plausible Deniability

Daniel Becker
d.becker@student.htw-berlin.de

Agenda

- *Einführung*
- *Deniable Encryption*
  - *Grundlagen*
  - *File in File*
  - *Empty Space*
  - *Decoy*

Agenda

- *Steganographic Filesystems*
  - *Angriffsszenarien*
- *Password Storage*
  - *Buch-Methode*
  - *Biometrie*

Agenda

- *Fazit/Ausblick*
- *Diskussion*

Einführung

- *Zur Person*
  - *Master Student an der HTW Berlin*
- *Thema*
  - *Im Rahmen des Seminars “Wissenschaftliches Arbeiten”*

Deniable Encryption

Daniel Becker

Grundlagen

- *Baut auf Steganographie auf*
  - *Steganographie ist erfolgreich, wenn kein Rückschluss durch Dritte möglich*

Grundlagen

- *Der Begriff "Plausible Deniability"*
  - *Eingeführt von Julian Assange und Ralf Weinmann (~1996/1997)*
  - *Im Rahmen des Rubberhose Filesystems*

Grundlagen

- *Im Paper "Deniable Encryption" 1997 weiter betrachtet*
  - *Hier hauptsächlich Kommunikation in der Theorie*

File in File

- *Idee: Daten innerhalb einer Datei verstecken*
- *Unauffällig möglich z.B. in Bildern oder Musikdateien*

File in File

- *Ersetzung bzw. Veränderung von "unwichtigen" Informationen*
- *Beispiel: Bilddatei*

Quelle: wikipedia

File in File

+ *Simple Implementierung*
- *relativ wenig Informationen versteckbar*

Empty Space

- *Idee: Volume innerhalb des freien Speicherplatzes*
- *freier Speicher wird zunächst mit Random-Werten gefüllt*

Emty Space

- *Partitions Header an definierten Stellen*
- *ohne entsprechende Passphrase nicht erkennbar*

Emty Space

- *Beispiel: TrueCrypt*

Emty Space

+ *Simple Implementierung*
+ *Platz für viele Daten*
– *u.U. auffällig*

Empty Space w/ Decoy

- *Idee: Crypto Volume im Crypto Volume*
- *Vorgehen gleicht zunächst Empty Space*

Empty Space w/ Decoy

- *Dann aber: zweite Partition innerhalb der Ersten*
- *innerhalb des freien Speichers*
- *zwei Passphrases (inner/outer Volume)*

Empty Space w/ Decoy

- *Beispiel: TrueCrypt*

Empty Space w/ Decoy

+ *Relativ simple Implementierung*
+ *Platz für viele Daten*
- *problematisch, wenn inneres Volume nicht gemountet*
- *Decoy Daten müssen gut gewählt werden*

Steganographic FileSystems

- *Idee: Keine extra Software, FS kümmert sich um alles*
- *Theoretisch von Ross Anderson, Roger Needham & Adi Shamir 1998 vorgestellt*

Steganographic FileSystems

- *Daten können selektive verschlüsselt werden*
- *ohne jeweilige Passphrase keine Kenntniss über die existierenden Daten*

Steganographic FileSystems

- *Beispiele:*
  - *Rubberhose FileSystem*
  - *PhoneBookFS*
  - *StegFS*

Steganographic FileSystems

- *StegFS als aktuellster Vertreter:*
  - *bis 2001 entwickelt*
  - *kein stable release vorhanden (im Original)*
  - *fortgeführt auf SourceForge*

Steganographic FileSystems

+ *Relativ komplexe Implementierung*
+ *Platz für viele Daten*
– *Manche Szenarien, die zu Datenverlust führen sind nicht vermeidbar*

Angriffsszenarien

Watermarking Attacken

- *Idee: Nachweisen der Existenz durch wiederkehrende Muster*
- *funktionierte bei vielen (älteren) Systemen*

Watermarking Attacken

- *Verschlüsselung funktioniert Sektorweise*
  - *da Daten über die Festplatte verteilt sind*
- *Daher: ein IV pro Sektor benötigt*
  - *Berechnung anhand der ersten 16-bit Sektor Id*

Watermarking Attacken

- *16 bit = 65535 unique Ids*
- *32 MB*

Watermarking Attacken

- *Suche nach vielfachen, sich wiederholenden Mustern*
- *Genügt meist als Indiz*

Watermarking Attacken

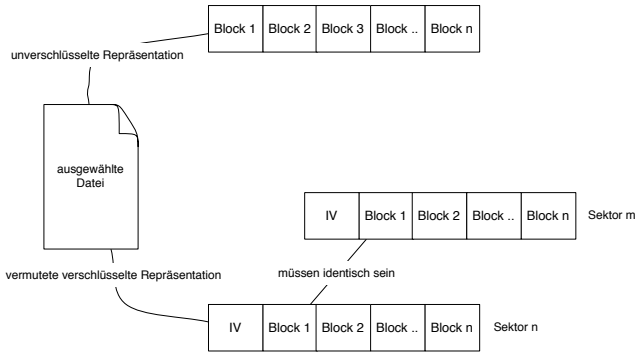
- *Es geht noch besser!*
- *Existenz-Nachweis von Dateien*

Watermarking Attacken

- *Datei muss bekannt sein*
  - *Es eignen sich z.B. Betriebssystem Dateien oder untergeschobene Daten*
- *Crypto-Algorithmus muss geraten werden*

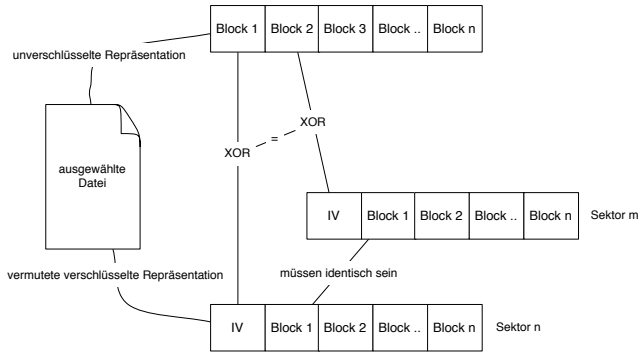
Watermarking Attacken

Ausgangssituation



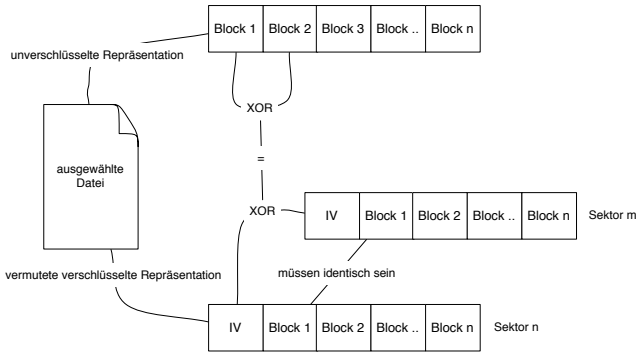
Watermarking Attacken

XOR Operation durchführen



Watermarking Attacken

Daraus folgt



Password Storage

Daniel Becker

htw

Password Storage

- *Passwörter sollen so lang und komplex wie möglich sein*
- *Daher: so gut wie nicht merkbar*
- *kaum Entwicklungen in den letzen Jahren*

Buch Methode

- *Idee: Merken eines Hinweises auf das Passwort*
- *Buch aus dem Regal auswählen*
- *Buch, Seite und Methode merken*

Buch Methode

- *auch andere Passwort-Quellen denkbar*
- *sollten möglichst langlebig sein*

Datenträger

- *Ablage auf einem Datenträger*
- *sichere Verwahrung dessen*

Datenträger

- *Kompromiss nötig*
- *Location vs. Comfort*

Biometrie

- *einfache Passwortgenerierung*
- *immer dabei*

Biometrie

- *meist einfach identifizierbar (eingebauter Fingerprint Scanner o.ä.)*
- *u.U. einfach fälschbar (Fingerprint)*

Fazit/Ausblick

Fazit

- *Verschiedene Techniken des Information Hiding*
- *Auch so sind die Informationen nicht 100% sicher*
- *Kann auch Probleme schaffen*

Fazit

- *Password Storage nicht das Gelbe vom Ei*
- *Wenig Alternativen (?)*

Ausblick

- *Steganographic Filesystems werden hoffentlich weiter entwickelt*
  - *möglicherweise als DFS*

Angewandte Informatik

Hochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Plausible Deniability

Daniel Becker
d.becker@student.htw-berlin.de

Diskussion

Angewandte Informatik

Hochschule für Technik und Wirtschaft Berlin
University of Applied Sciences

Plausible Deniability

Daniel Becker
d.becker@student.htw-berlin.de