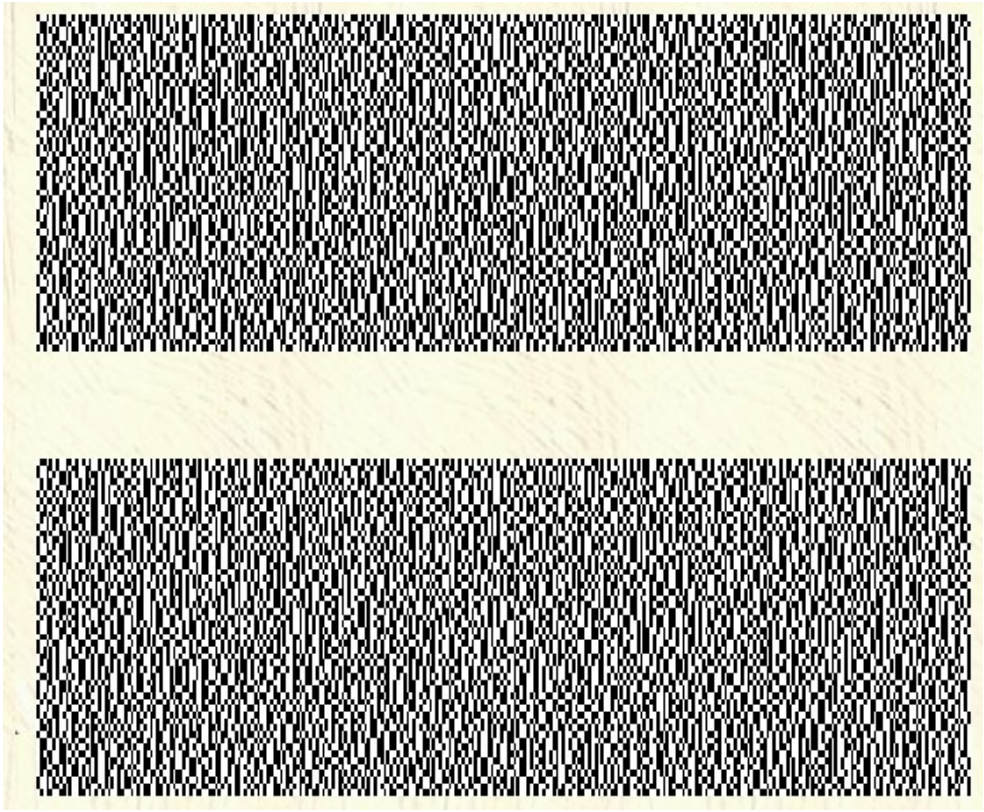
Visuelle Kryptographie

- Ausprägung der Kryptographie für Pixeldarstellungen
  - Geheimnisverteilung über Folien
  - „Schlüssel“ = Besitz aller Folien

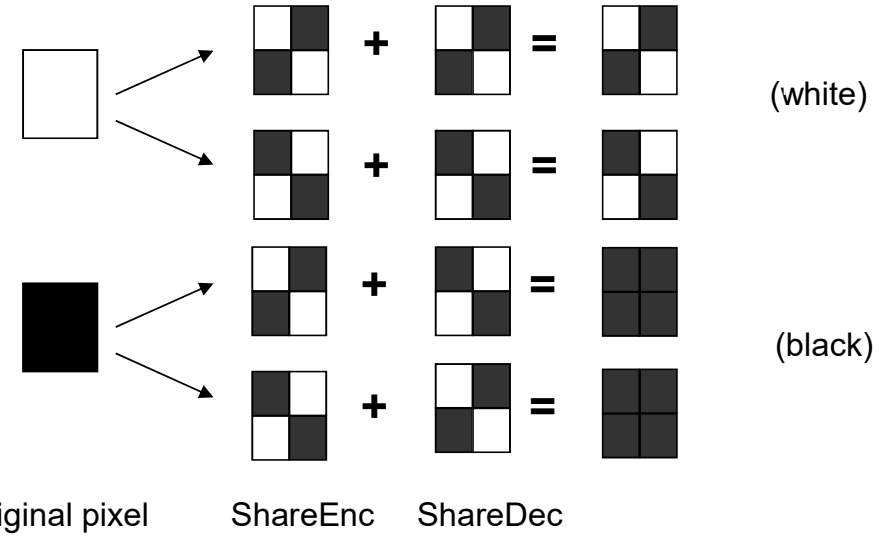
Visuelle Kryptographie

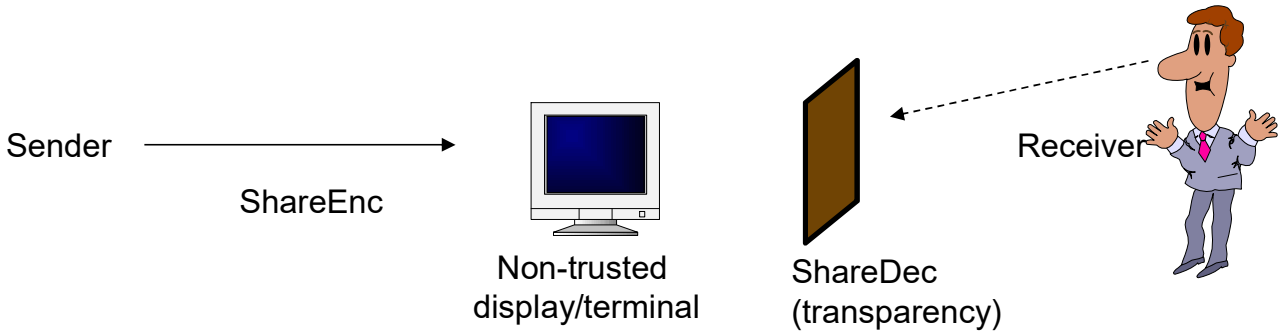
- http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html
- Doug Stinson's Visual Cryptography Page

Visuelle Kryptographie



Visuelle Kryptographie


+
=
(white)
(black)
Original pixel
ShareEnc
ShareDec

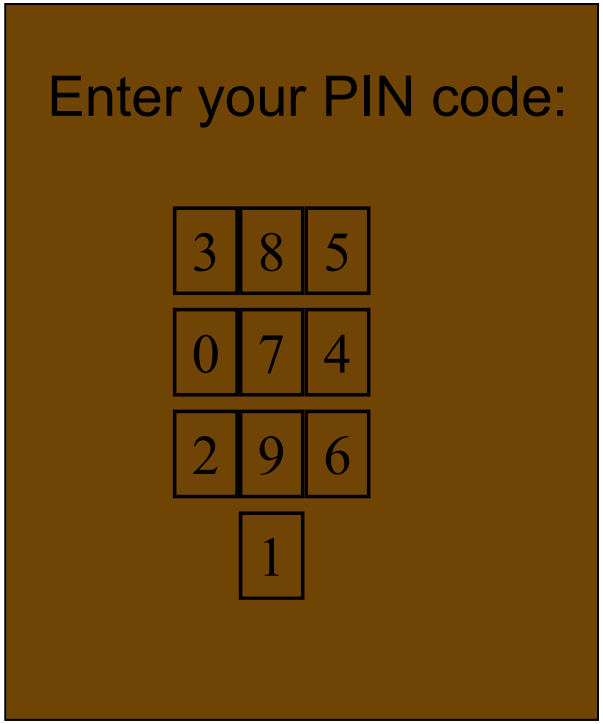

Sender
ShareEnc
Non-trusted
display/terminal
ShareDec
(transparency)
Receiver

- Alice will auf ihre Kontodaten zugreifen und befindet sich in einem Internetcafe
- Dieser Umgebung vertraut Alice nicht, nicht einmal den Rechnern
- Die Bank führt eine visuelle Verschlüsslung der Daten durch
- Der Rechner erhält eine visuell verschlüsselte Datei und zeigt diese an
- Alice kann mittels ihrer Folie die Informationen lesen

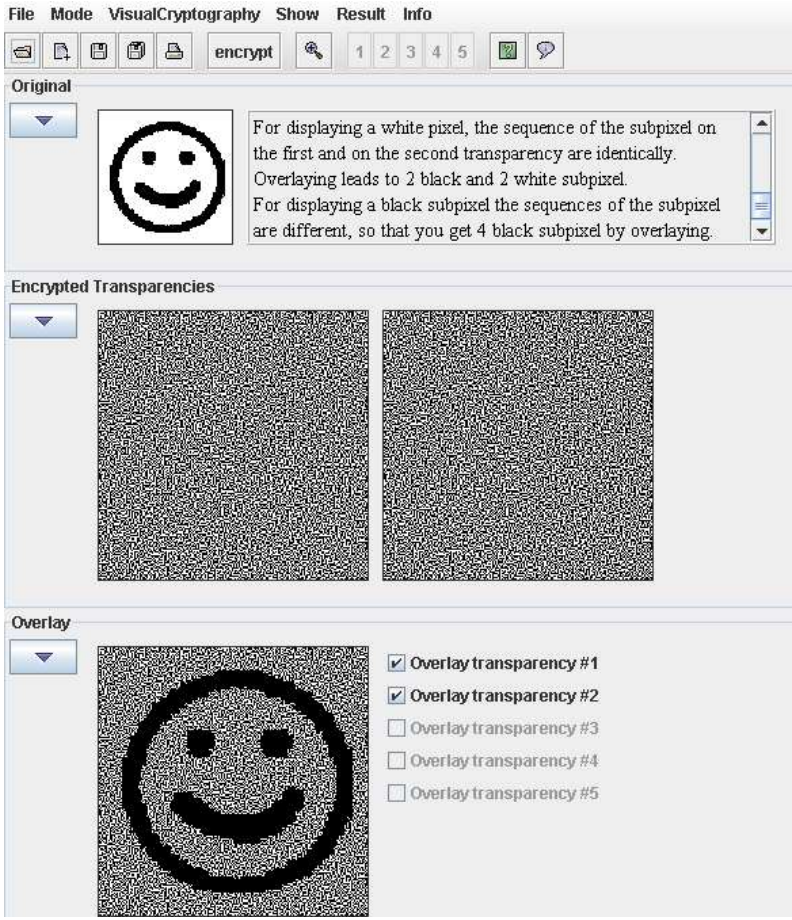
Visuelle Kryptographie / Nachteile

- Nachteile:
  - Folien zum Entschlüsseln können gestolen werden
  - Folien müssen zu Bildschirm passen
  - Verlust von Auflösung und Qualität des Bildes

- Gegenmassnahmen
  - Gesteuerte Kombination aus zwei LCD Displays
  - Nur eines wird vom Rechner angesteuert
  - Das zweite wird durch Schlüssel von Alice gesteuert

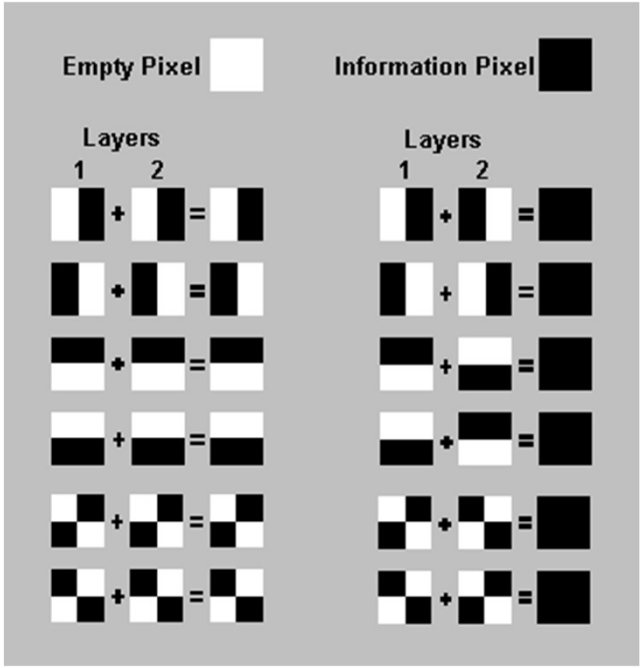

Enter your PIN code:
3 8 5
0 7 4
2 9 6
1

- Screenshot:
  http://www-sec.uni-regensburg.de/vc/#applet
- Inzwischen leider offline…



- Es können auch andere Muster verwendet werden

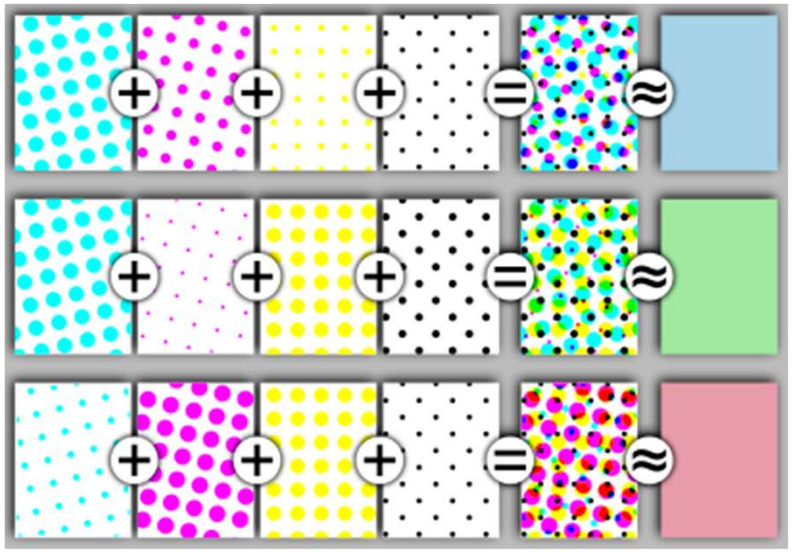
http://users.telenet.be/d.rijmenants/en/visualcrypto.htm



- Extended Visual Cryptography
  - Für Graustufen
  - Kontrast geht verloren
  - Pixel werden so unterschiedlich hell dargestellt.

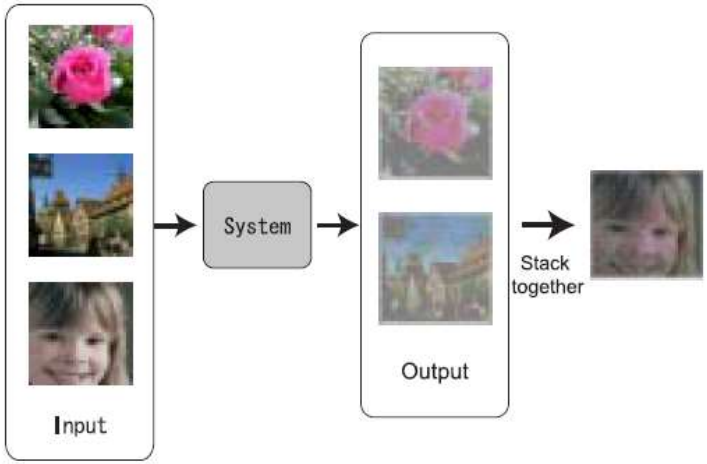
M. Naor and A. Shamir. Visual cryptography,advances in cryptology. *Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995*

- Extended Visual Cryptography
  - Basiert auf dem Konzept des Halftonings
  - Für farbige Pixel



http://en.wikipedia.org/wiki/File:Halftoningcolor.svg
Wikipedia Commons

- Extended Visual Cryptography
  - Statt Rauschmuster werden Bilder verteilt



Aus: EXTENDED VISUAL CRYPTOGRAPHY FOR NATURAL IMAGES, Mizuho NAKAJIMA und Yasushi YAMAGUCHI; http://wscg.zcu.cz/wscg2002/Papers_2002/A73.pdf

Partielle Verschlüsselung

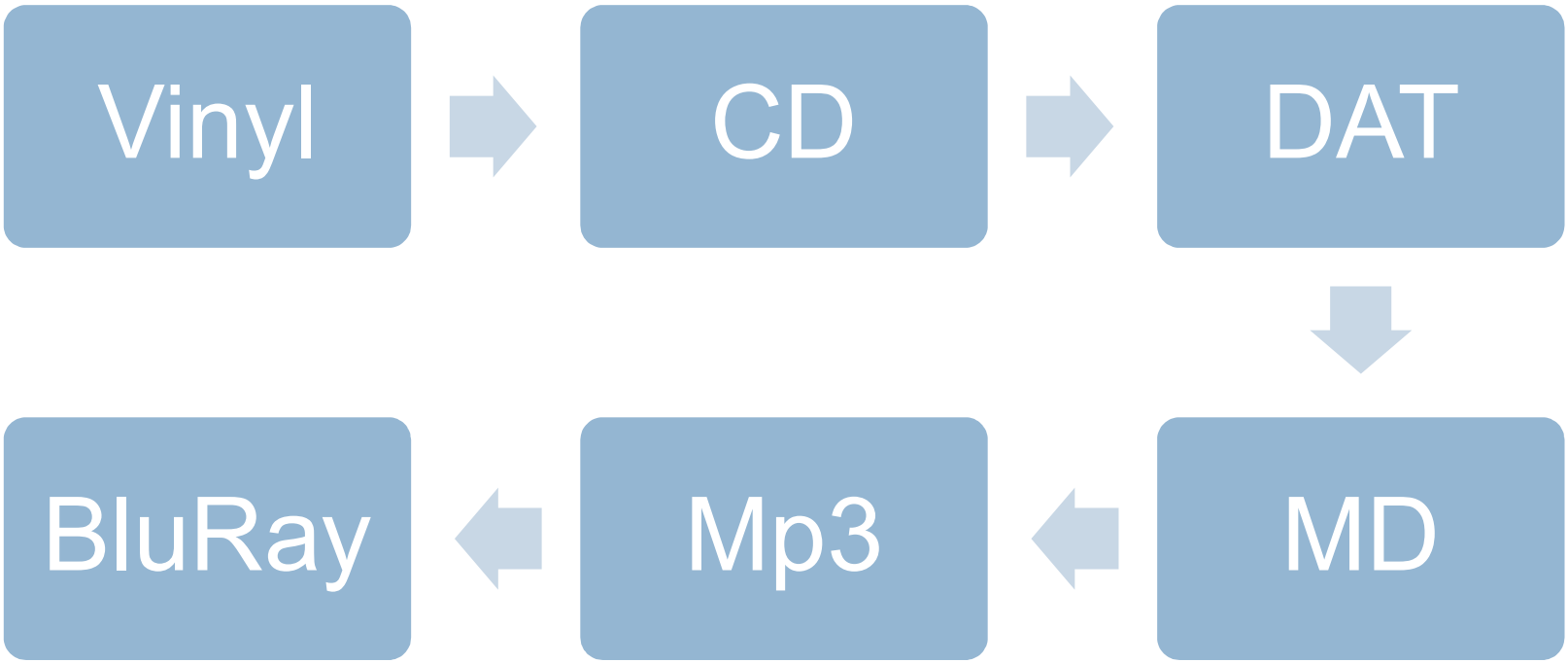
- Identifizieren und Verschlüsseln relevanter Medienanteile
- Relevanz abhängig von Schutzziel
  - Partiell: Vertraulichkeit/ Zugriffsschutz
  - Transparent: Zugriffsschutz/ Preview

Robuste Verschlüsselung

- Verschlüsselung von Medien vor gestörten Übertragungskanälen
- Schwache Verschlüsselung
- Resistenz gegen z.B. verlustbehaftete Kompression

Visuelle Verschlüsselung

- Verschlüsselung von Informationen, die dann als Medium verbreitet werden
- Prinzip eines One Time Pads
- Hohe Sicherheit bei korrekter Anwendung


Vinyl
CD
DAT
MD
Mp3
BluRay

Kopierschutz Historie: Spoiler Signal

- Piraterie von Musik auf LPs wurde zum ersten Mal in den 60er Jahren zu einem Thema
- Auch hier galt: neue Technologie (MC) ermöglicht Kopieren auf triviale Weise
- Erste Person, die mit dem Entwickeln einer Gegenmaßnahme beautraft wurde:
  "Magic Alex" Mardas
- Auftraggeber: Apple Music, das Label der Beatles
- Konzept: “Spoiler Signal”
  - 20-kilohertz Ton wird Musik hinzugefügt
  - Unhörbar für Menschen
  - Bei Kassettenaufnahmen kommt es zu einer Interferenz mit einer im Kasettenrekordern verwendeten Freqzenz
    - "bias frequency“
    - Notwendig für das Anregen der Magnetpartikel
  - Effekt: Es entsteht eine niedrigere Frequenz, die hörbar ist

http://www.haushinka.co.uk/library/science/New%20Scientist/computing/New%20Scientist%20The%20pirate's%20tale.htm

Kopierschutz Historie: Spoiler Signal

- Funktioniert unter Studioumgebungen
- Erste Veröffentlichtung mit Schutz "*Sergeant Pepper*"
- Probleme in der Praxis:
  - Signal zu Schwach zur Wiedergabe durch Plattenspieler
  - Signal wird über die Zeit hinweg "abgeschliffen"
  - Filter in den Geräten löschten das Signal
- Konzept wurde aufgegeben

http://www.haushinka.co.uk/library/science/New%20Scientist/computing/New%20Scientist%20The%20pirate's%20tale.htm

Kopierschutz Historie: Spoiler Signal

- Piracy got its big break in the 1960s when Philips launched the first cheap audio cassette. Before that, tape only came on bulky spools and had to be laced through the complicated mechanism of a tape recorder. Philips's compact cassette did away with all that and, overnight, copying music became a doodle.
- It didn't take the recording industry long to see the danger. When the Beatles founded the company Apple, they hired a colorful Greek character called "Magic Alex" Mardas. Together they hatched a plan to put a "spoiler" signal on the Beatles's next album, *Sergeant Pepper*. The record would play normally, but anyone who tried to copy it onto a blank cassette would find their recording ruined.
- Magic Alex added a 20-kilohertz tone to the music, a frequency just above human hearing. But when the signal was copied onto tape, it interfered with the similarly high "bias frequency" which analogue tape recorders use to mobilize the magnetic particles in recording tape. The two signals produced a lower "beat frequency" that sounded like a whistle.
- Although the spoiler worked in the lab, with engineers who wanted it to work using high-quality equipment, the real world is nothing like this ideal. Needles on domestic record players ignored the signal, often physically destroying the delicate groove in the vinyl that produced the spoiler. Even if the stylus did read the signal, it was usually filtered out by unwanted capacitance and inductance in the connecting leads. So people who bought *Sergeant Pepper* found that it copied perfectly. Apple and Magic Alex abandoned their idea.

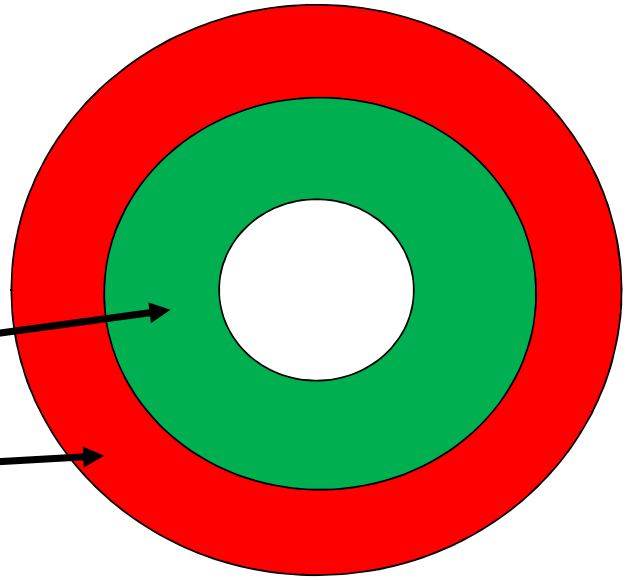
http://www.haushinka.co.uk/library/science/New%20Scientist/computing/New%20Scientist%20The%20pirate's%20tale.htm

CD Kopierschutz

- CDs basieren auf dem RedBook Standard
  - Kein Kopierschutz vorhanden / definiert
  - Einziges digitales Medium ohne Kopierschutz
- Bekannte Methoden, die auf herkömmlichen Brennern ein Kopieren einer CD verhindern können
  - Manipulation Table of Contents (TOC)
  - Absichtliches Erzeugen von Fehlern
  - Übergrosse CDs
  - Pausen unter 2 Sekunden
  - „Musikstücke“ die kürzer als 4 Sekunden sind

CD Kopierschutz

- Nächste Generation CD Kopierschutz:
  - Trennung zwischen
    - Audio/ Hifi
    - Computer
  - Audio: Klassische PCM CD
  - Computer: Datenträger mit Audiofiles und DRM System
- Sichtweise abhängig von Laufwerk
  - Audio: Innere Session (erste)
  - Computer: Äußere Session (letzte)
- Problem: Computerlaufwerke in Autoradios



DRM/ CD Kopierschutz

- Wisschenschaftliche Diskussion z.B. in Evaluating New Copy-Prevention Techniques for Audio CDs von John A. Halderman, Princeton University
  - http://www.cs.princeton.edu/~jhalderm/papers/drm2002.pdf
- Getestete Schutzmechanismen
  - MediaCloQ Ver 1.0 von SunnComm
  - Cactus Data Shield von Midbar Technologies
  - Key2audio von Sony
- Kopierschutz verhindert Kopieren mit vielen Programmen
- Aber:
  - CloneCD (Stand 2002) kopiert erfolgreich alle geschützten CDs
  - Open Source Software kann einfach an Schutzmechanismen angepasst werden, um Schutz zu umgehen

Angriff mit Filzstift

- Suchen einer etwa zwei Millimeter breiten Trennlinie auf der CD
- Mit einem Folienstift Trennlinie und Teile des äußeren Tracks abdecken, ohne die letzte Audio-Spur zu berühren
- Erfolgreich gegen
  - Cactus Data Shield 100/200
  - Key2Audio

QUELLE: http://www.chip.de

DRM, Presse und Recht

- 2005: Abmahnung CHIP wegen Verlinkung von Software zur Umgehung von Kopierschutzmaßnahmen
- 2005: Verbot des Links als Teil der Störerhaftung
- 2010: Bundesgerichtshof erklärt Links als Teil der Pressefreiheit bzw. der notwendigen Berichterstattung

- http://www.urheberrecht.org

18.12.2007; 18:29 Uhr

Rüge des Presserats für Berichterstattung über Umgehungssoftware von Kopierschutz

DVD-Beilage mit »halblegalen Top-Tools« ist Verstoß gegen Verantwortung der Presse gegenüber dem LEser

Als mit dem Pressekodex nicht vereinbar rügte der *Deutsche Presserat* die Berichterstattung der Computerzeitschrift »PC Praxis« in der Ausgabe 7/2007, die die einschlägige Software zur Umgehung von Kopierschutzmechanismen zum Gegenstand hatte. Wie der *Bundesverband Musikindustrie* am 17.12.2007 mitteilte, sah der *Presserat* hierin und in der reißerischen Darstellung auf den Titelblatt (»Verbotene Top-Tools - Wo es sie gibt & wie sie funktionieren«, »Blacklist der 25 illegalsten Tools«, »Anonym bei BitTorrent saugen« und »Jeden DVD-Kopierschutz knacken«) einen Verstoß gegen die Präambel und Ziffer 1 des Pressekodex'. Danach müssen sich u. a. Verleger, Herausgeber und Journalisten bei ihrer Arbeit der Verantwortung gegenüber der Öffentlichkeit und ihrer Verpflichtung für das Ansehen der Presse bewusst sein.

Nach Ansicht des *Deutschen Presserats* hingegen würden die Leser zur Nutzung verbotener Software »fast schon animiert«. Dabei sei es ohne Bedeutung, dass die einschlägigen Programme ohne explizite Nennung der jeweiligen Bezugsquellen vorgestellt würden, da jeder »halbwegs kundige Internetnutzer« in der Lage sei, die Software über Suchmaschinen zu finden. Auch die beiliegende DVD, die auf dem Titel mit »30 halblegale Top-Tools« beworben wurde, stieß auf die Kritik des *Presserats*. Damit werde dem Leser Software zur Verfügung gestellt, deren Nutzung zumindest fragwürdig sei die Verantwortung der Presse gegenüber dem Leser erfordere jedoch, nur legale Software zur Verfügung zu stellen.

CD-Kopierschutz: "Shift"-Tasten-Trick hat juristische Folgen

MÜNCHEN (COMPUTERWOCHE) - Der Kopierschutzspezialist SunnComm hat angekündigt, den Princeton-Studenten John Halderman zu verklagen. Halderman hatte Anfang der Woche auf seiner Website beschrieben, wie sich die Kopierschutztechnik "MediaMax CD3" des Herstellers mittels Drücken der "Shift"-Taste aushebeln lässt (Computerwoche online berichtete). Die Technik wurde erstmals von der Bertelsmann Media Group (BMG) auf einem Ende September erschienenen Album des Soul-Sängers Anthony Hamilton verwendet.
Laut Geschäftsführer Peter Jacobs erwägt SunnComm sowohl einen strafrechtlichen Prozess als auch eine Schadensersatzklage vor einem Zivilgericht. Der Student habe die Reputation des Unternehmens geschädigt. Außerdem habe er Urheberrechtsgesetze gebrochen, indem er Mittel zum Umgehen einer Kopierschutztechnik zur Verfügung gestellt habe. Dabei bezieht sich Jacobs auf Regelungen des amerikanischen DMCA (Digital Millennium Copyright Act), der wie das neue in Deutschland gültige Urheberrecht die Verbreitung von Tools und Informationen verbietet, die dazu geeignet sind, wirksame Kopierschutzmaßnahmen auszuhebeln. US-Rechtsexperten zufolge stehen die Karten für Halderman im Fall einer Prozesseröffnung schlecht. Mit der gleichen Begründung, die Jacobs anführt, hat bereits die Vertretung der US-Filmindustrie Motion Picture Association of America (MPAA) einen Prozess gegen den Internet-Aktivisten Eric Corley wegen Veröffentlichung des DVD-Crack-Programms "DeCSS" gewonnen.

[…]

10.10.2003

https://www.computerwoche.de/a/cd-kopierschutz-shift-tasten-trick-hat-juristische-folgen,541729

CD-Kopierschutz: SunnComm zieht Klage wegen "Shift"-Trick zurück

MÜNCHEN (COMPUTERWOCHE) - SunnComm will den Princeton-Studenten John Halderman nun doch nicht vor Gericht bringen. Ende letzter Woche hatte der Kopierschutz-Hersteller mit einer Urheberrechtsklage gedroht, weil Halderman eine Anleitung veröffentlicht hatte, nach der sich die gemeinsam mit der Bertelsmann Music Group (BMG) entwickelte Kopierschutztechnik "MediaMax CD3" aushebeln lässt (Computerwoche online berichtete).

Offenbar gab Angst vor negativer Publicity den Ausschlag, von der Klage abzusehen. Während SunnComm-Geschäftsführer Peter Jacobs am Freitag noch von einer Kampagne gegen sein Unternehmen sprach, räumte er nun ein, die Situation falsch eingeschätzt zu haben. Außerdem äußerte er die Befürchtung, ein Prozess könne sich über lange Zeit hinziehen und mit einem Urteil enden, das dem Gegenstand der Klage nicht gerecht werde.

[…]

(13.10.2003)

https://www.computerwoche.de/a/cd-kopierschutz-sunncomm-zieht-klage-wegen-shift-trick-zurueck,541765

- Security concerns have been raised regarding the use of CDs containing XCP software in computers. These issues have no effect on the use of these discs in conventional, non-computer-based CD and/or DVD players. This content protection technology was provided by a third-party vendor, First4Internet, and was designed to prevent unlimited copying and unauthorized redistribution of the music on the disc.
- http://cp.sonybmg.com/xcp/

SONY BMG's Reaktionen

- Stopp der Produktion von CDs mit XCP
- Entfernen der existierenden CDs aus dem Vertrieb
- Ersetzen aller CDs im Vertrieb mit nicht geschützten CDs
- Austausch für Kunden: CD gegen nicht geschützte CD plus mp3 Dateien
- Bereitstellen einer Software zum Aufheben des XCP-“Schleiers“
- Bereitstellen einer Vorgehensweise zum Entfernen von XCP
- Informieren der Hersteller von Anti-Viren-Software über die Arbeitsweise von XCP

- **Problems with XCP**
  Security researchers have shown that the XCP technology was designed to have many of the qualities of a "rootkit." It was written with the intent of concealing its presence and operation from the owner of the computer, and once installed, it degrades the performance of the machine, opens new security vulnerabilities, and installs updates through an Internet connection to Sony BMG's servers. The nature of a rootkit makes it extremely difficult to remove, often leaving reformatting the computer's hard drive as the only solution. When Sony BMG offered a program to uninstall the dangerous XCP software, researchers found that the installer itself opened even more security vulnerabilities in users' machines.

http://www.eff.org/IP/DRM/Sony-BMG/

DRM/ SONY XCP

- Want to cheat in your online game and not get caught? Just buy a Sony BMG copy protected CD.
- World of Warcraft hackers have confirmed that the hiding capabilities of Sony BMG's content protection software can make tools made for cheating in the online world impossible to detect. The software--deemed a "rootkit" by many security experts--is shipped with tens of thousands of the record company's music titles.
- Blizzard Entertainment, the maker of World of Warcraft, has created a controversial program that detects cheaters by scanning the processes that are running at the time the game is played. Called the Warden, the anti-cheating program cannot detect any files that are hidden with Sony BMG's content protection, which only requires that the hacker add the prefix "sys" to file names.
- Despite making a patch available on Wednesday to consumers to amend its copy protection software's behavior, Sony BMG and First 4 Internet, the maker of the content protection technology, have both disputed claims that their system could harm the security of a Windows system. Yet, other software makers that rely on the integrity of the operating system are finding that hidden code makes security impossible.

http://www.securityfocus.com/brief/34

"A personal computer is called a personal computer because it's yours," said Andrew Moss, Microsoft's senior director of technical policy. "Anything that runs on that computer, you should have control over."

- http://news.com.com/Who+has+the+right+to+control+your+PC/2100-1029_3-5961609.html?tag=nl

DRM/ Sony XCP: Folgen

- Vielleicht hat Sony aber nur Pech gehabt, indem es beim Hacken seiner Kunden ertappt worden ist. Etliche andere Musikfirmen erproben ähnlich trickreiche Methoden, um ihre CDs vor dem Kopieren oder dem Übertragen auf tragbare Geräte wie iPods zu schützen. Digital Restrictions Management (DRM) ist dafür das Fachwort, und eine Fülle (inkompatibler) Lösungen und Teil-Standards existiert dafür inzwischen. DRM ist längst Bestandteil von Computer-Betriebssytemen wie Windows, so dass Firmen wie Microsoft eine wesentliche Kontrolle über die Mediennutzung ihrer Kunden erhalten. Hardware-Hersteller wie IBM/Lenovo haben begonnen, „Sicherheitschips“ in neue Computer einzubauen, die auch im Dienste des Kopierschutzes verwendet werden können.

  Besonders übel ist der Umstand, dass die meisten Programme spitzeln – sie informieren Sony oder Microsoft, wenn sich jemand eine bestimmte CD anhört. Ein anderes Problem besteht darin, dass viele DRM-Techniken legitime Nutzungen der Musik verbieten, wie etwa das Abspielen auf einem iPod.

http://www.zeit.de/online/2005/47/sony_kommentar?page=2

XCP

- https://www.youtube.com/watch?v=FUUfBzxsKrg
- Oddware: "Copy protected" audio CDs & installing the Sony rootkit
- Von VWestlife

Kopierschutz

- DAT – Digital Audio Tape
- Verhindern digitaler Kopien von Consumer-Geräten mittels „Copybit“
  - Serial Copy Management System

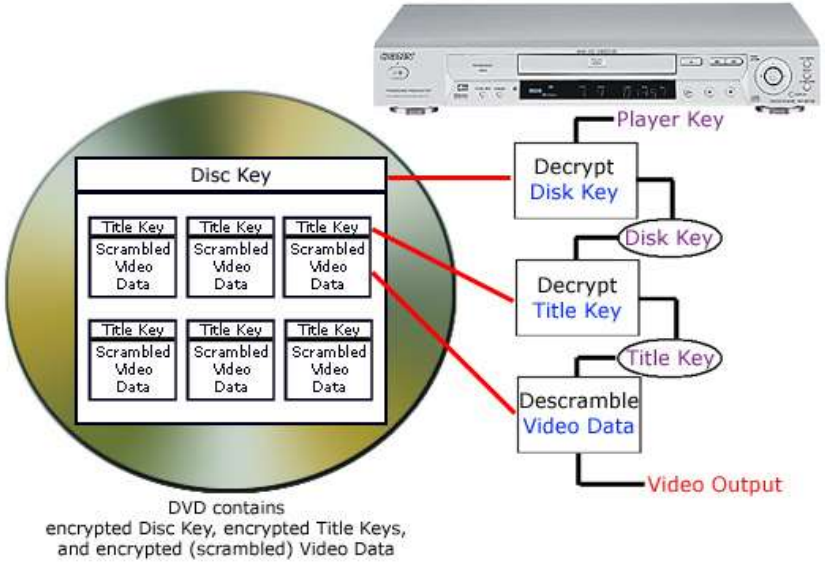
Kopierschutz

- MiniDisc
- Verwendet ebenfalls Serial Copy Management System
- Seit 2005 Lockung der Kopierschutzbestimmungen

Kuha455405 (CC) Wikipedia

Kopierschutz

- DVD-Video
  - Ein DVD Format von vielen
  - Enthält MPEG-Video
  - Oft geschützt vom Content Scramble System (CSS)
    - Eingeführt 1996
    - Gebrochen 1999 durch Brute Force Angriff
- CSS
  - DVD Player
    - hat einen Player Key
    - Liest disc-key-block und entschlüsselt mit Player Key den Disk Key
    - Liest Title Keys und entschlüsselt diese mit dem Disk Key
    - Title Keys entschlüsseln Inhalte
  - Schlüssel sind nur 40 Bit lang
  - Cryptoanalyse ermöglichte effiziente Angriffe
    - https://insecure.org/news/cryptanalysis_of_contents_scrambling_system.htm
    - 18 Sekunden auf einem Pentium III mit 450MhZ



Cryptography in Home Entertainment
A look at content scrambling in DVDs
Mark Barry, 2004