

Der Schutz technischer Sicherheitsmaßnahmen im UrhG

IT im Spannungsfeld zwischen Technik, Wirtschaft
und Recht

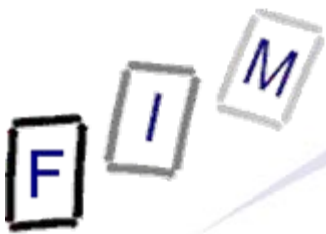
Kapfenberg, 23.4.2010

Institut für Informationsverarbeitung und
Mikroprozessortechnik (FIM)
Johannes Kepler Universität Linz, Österreich

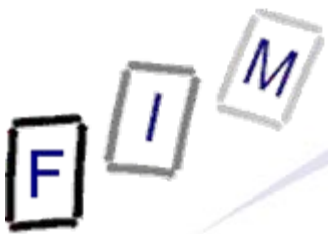
E-Mail: sonntag@fim.uni-linz.ac.at
<http://www.fim.uni-linz.ac.at/staff/sonntag.htm>



- Urheberrecht ist im Internet-Zeitalter besonders verletzlich
 - Raubdrucke von Büchern waren eher selten...
... anders als (P2P-)Filesharing (Musik, Videos) es jetzt ist!
- Technische Schutzmaßnahmen sollen dem abhelfen
 - Problem: Gegenmaßnahmen sind schwer herzustellen, aber sehr leicht zu verbreiten und einzusetzen
 - „Lösung“: Vorfeldschutz
 - » Herstellung, Besitz, Einsatz, ... von Mitteln zur Umgehung von Sicherheitsmaßnahmen ist in weitem Umfang verboten
- Hierzu existieren mehrfach Regelungen:
 - Zugangskontroll-Gesetz: Hauptsächlich für Pay-TV
 - » Gilt aber auch für „Dienste der Informationsgesellschaft“
 - Urheberrechtsgesetz: Computerprogramme (§ 90b UrhG) bzw. sonstige Werke/Leistungsschutzrechte (§ 90c UrhG)



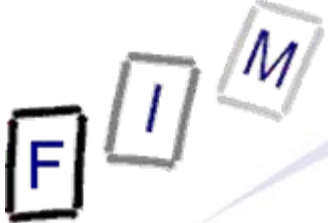
- Hier wird nur der Urheberrechts-Schutz betrachtet
- Wichtige Probleme:
 - Geschützt sind nur „wirksame“ Sicherheitsmaßnahmen
 - Bei Software: Keine solche Einschränkung!
 - » Aber wann liegt das vor?
 - Was ist mit „Multimediawerken“, z.B. Computerspielen?
 - » Programm (→ 90b) + Grafiken/Musik/Filme/Texte (→ 90c) = ???
 - Wann dient eine Sicherheitsmaßnahme dem Schutz von Ausschließlichkeitsrechten nach dem Urheberrechtsgesetz?
 - » Schutz von Geschäftsmodellen?
 - » „Alibi-Programm“ in Druckerpatronen?
- Fallstudie: Aktuell veröffentlichtes Urteil aus Deutschland
 - Beide Gesetze basieren auf EU-RL → Praktisch identisch!



Schutz in Bezug auf Nicht-Software

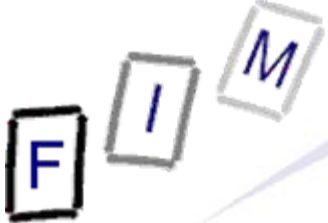
§ 90c UrhG

- Inhaber eines Ausschließungsrechts nach dem UrhG
 - Ausgenommen Rechte an Computerprogrammen
- Wirksame technische Maßnahmen zur Verhinderung oder Einschränkung von Verletzungen dieses Rechts
- Verboten sind:
 - Umgehung mit Kenntnis oder fahrlässiger Unkenntnis
 - » Tatsächlicher Einsatz eines Umgehungsmittels
 - Herstellung, Einfuhr, Verbreitung, Verkauf, Vermietung, Besitz zu kommerziellen Zwecken von Umgehungsmitteln
 - » Vorfeld: Verbot von Umgehungsmitteln
 - » Nicht verboten: Besitz zu privaten Zwecken!
 - Werbung für Verkauf oder Vermietung von Umgehungsmitteln
 - Erbringung von Umgehungsdienstleistungen



Verbotene Handlungen

- Das Verbot ist unabhängig davon, ob die Handlung ohne eine Sicherheitsmaßnahme erlaubt wäre:
 - Privatkopie ist erlaubt, aber
 - muss ein Schutz hierfür umgangen werden, so ist die Kopie zwar noch erlaubt, aber die Umgehung dennoch verboten!
 - » „Abschaffung“ der Privatkopie (Beispiel: DVDs!)
- Fahrlässige Unkenntnis → „Kennzeichnungspflicht“
 - Es ist nicht zu vermuten, dass jeder Medienträger eine Sicherheitsvorkehrung enthält
 - Daher: Hinweis darauf nötig → „Hätte wissen müssen“
 - » Weiters: Meist nicht mehr standardkonform → Sonst „fehlerhaft“!
- Vorgesehene Nutzung ist immer erlaubt: „Analoge Lücke“
 - Abfilmen des Fernsehers ist eine legale Privatkopie
 - Kopierschutz wirkt dort nicht mehr/soll dies nicht behindern
 - » Achtung: Verzerrung + Spezialbrille (3D?) → Verboten!



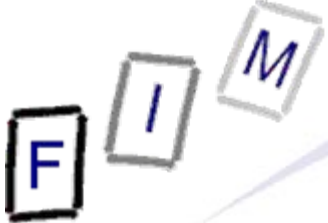
Was sind „Umgehungsmittel“?

- Vorrichtung, Erzeugnisse, Bestandteile
- Werden zur Umgehung von techn. Maßnahmen beworben
 - Unabhängig von Eignung/Möglichkeiten!
- Erforderliche Eigenschaft:
 - außer Umgehung nur begrenzten wirtschaftlichen Zweck
 - » „Dual-use-Tools“ mit minimaler legaler Funktion
 - oder hauptsächlich entworfen/hergestellt/angepasst, um eine Umgehung zu ermöglichen oder erleichtern
 - » „Hacker-Tools“ mit ev. Legalen Alibi-Funktion
- Hauptzweck muss die Umgehung sein, der legale Einsatz nur ein unbedeutender Nebenaspekt
 - Relevanter legaler Nutzen → Kein Umgehungsmittel mehr
 - » Beispiel: Fehlerkorrektur bei Audio-CDs → Zerkratzte CDs
 - » Beispiel: Passwortqualitäts-Prüfung → Kein Knacktool
 - Achtung: Keine Bewerbung der Umgehungsfunktionalität!



„Technische Schutzmaßnahme“ = ???

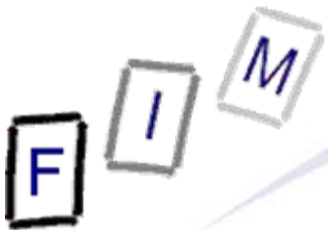
- Technische Schutzmaßnahme → Technisch
 - Nicht: Vertragsbestimmungen, Personenaufsicht, Audits, ...
 - Muss sein: Zugangskontrolle, Verschlüsselung, Verzerrung, Mechanismus zur Vervielfältigungskontrolle
 - » Das scheint eine wenig wirksame Einschränkung zu sein!
- Im Normalbetrieb dazu bestimmt, Verletzungen eines Ausschließlichkeitsrechts zu verhindern oder einzuschränken
 - Ziel des Schutzes muss das „Werk“ sein
 - Sonstige, z.B. wirtschaftliche, Ziele fallen heraus
 - » Beispiel: Handy SIM-Lock → Hereinspielen der Handy-Subvention; Zugriff auf SW, Icons, ... soll nicht behindert werden!
 - Ebenso nicht Rechte nach anderen Gesetzen, z.B. DSGVO!
- müssen dieses Schutzziel tatsächlich erreichen
 - Was nicht zumindest einigermaßen/gelegentlich funktioniert, darf „umgangen“ werden



- Nur „wirksame“ Schutzmaßnahmen sind geschützt
- Zwei Varianten möglich:
 - Absolut: Wirksamkeit unabhängig vom Angreifer
 - » Wenn es für irgendwen wirksam ist, dann für alle!
 - Relativ: Wirksamkeit in Bezug auf typische Angreifer
- Relativ passt besser:
 - Absolut unwirksam → Hängt dennoch oft vom Angreifer ab
 - » Windows-Kopierschutz auf Linux-PCs
 - Gesetz erwähnt „Schutzziele“ → Diese beziehen sich (techn. gesehen!) auf bestimmte Angreifer(-gruppen)
- Maßstab: „Durchschnittlich gebildeter Nutzer ohne besondere technische Kenntnisse“
 - „Durchschnittliche Nutzer“ sind rechtstreu → Kein Bedarf
 - Daher eher: „Durchschnittliche Angreifer“



- Beurteilung daher nach Schutzzielen:
 - Was wird angegriffen: Muss ein Recht aus dem UrhG sein
 - Wer sind potentielle Angreifer?
 - » Ressourcen: Rechenzeit, Hard-/Software
 - » Zugang zu Hilfsmitteln oder Spezialisten
 - » Kenntnisse und Fähigkeiten
 - Welches Ziel soll erreicht werden?
 - » Aneignung/Nutzung/Zerstörung/...; Geheim/Offen
 - Motivation der Angreifer
 - » Welchen Aufwand sind sie zu investieren bereit (Geld, Arbeit, ...)
- Wirksam = Nicht-trivialer Aufwand erforderlich
 - Mit vorhand. Standard-Tools nebenbei beseitigt → Unwirksam
 - Nachdenken oder längere Internet-Recherche → Wirksam
 - Relevante Kosten (Tool kaufen) → Wirksam
- Niedrige Schwelle!



Schutz von Computerprogrammen

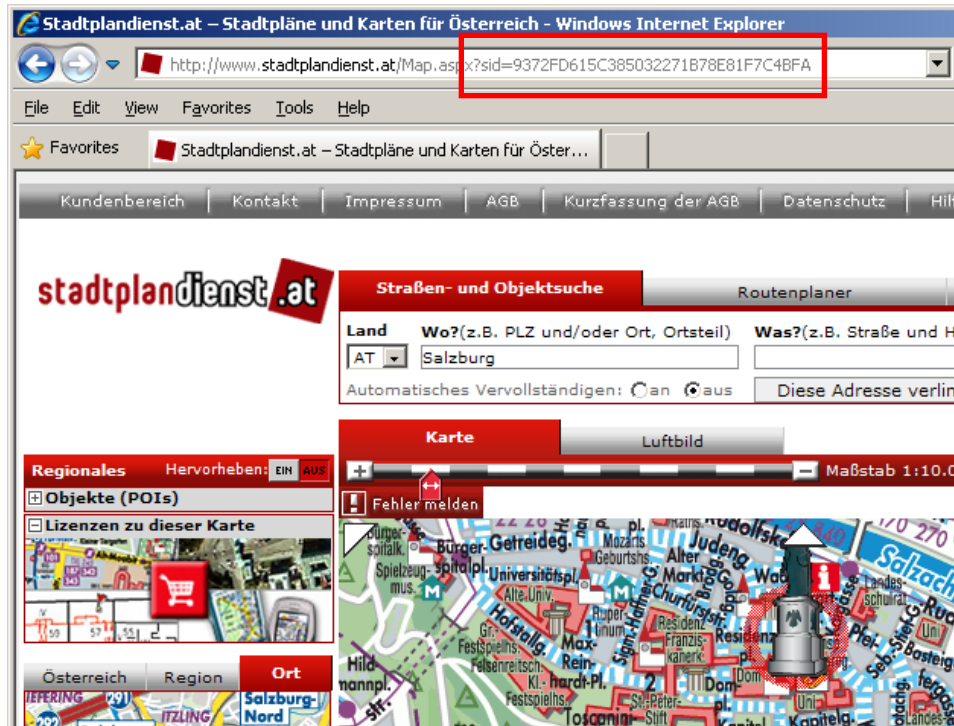
§ 90b UrhG

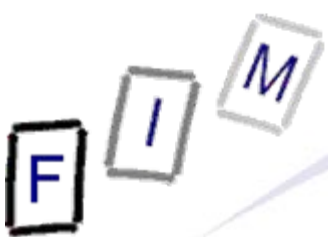
- Unterschiede zu § 90c (sonstige Werke):
 - Keine „Wirksamkeit“ erforderlich
 - » Jegliche Sicherheitsmaßnahme ist geschützt
 - » Ausgeschlossen ist nur, was gar nicht funktioniert (zB fehlerhaft)
 - Engerer Schutzzumfang
 - » Verboten : In Verkehr bringen und Besitz zu gewerbl. Zwecken
 - » Nicht verboten: Umgehung selbst, Werbung, Dienstleistungen
 - „Cracken“ eines Programms, das man legal besitzt, ist zumindest hiernach nicht verboten; Crack ins Internet stellen allerdings schon!
 - Umgehungsmittel müssen **alleine** zur Umgehung dienen
 - » Keine dual-use Problematik!
 - Sinnvoll zur Sicherheitsüberprüfung → Erlaubt
 - » Daher auch kaum praktische Relevanz ...
- Konkurrenz § 90b und § 90c
 - Ev. Beide gleichzeitig anwenden, da versch. Schutzobjekte
 - Sicher nicht hinsichtlich der Strafbestimmungen



Fallstudie: Session-ID Entscheidung

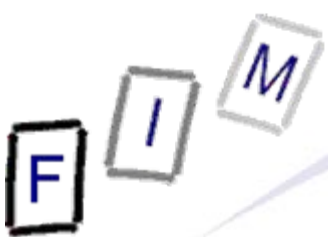
- Stadtplandienst: Kostenlos, keine Registrierung
 - Kommerzielle Nutzung/statische Links → Kostenpflichtig!
- Bei Aufruf der Seite wird eine Session-ID erzeugt
 - 3 Stunden lang gültig, dann Kartenabruf nicht mehr möglich
 - Eingegebene Adresse wird mit Session-ID assoziiert





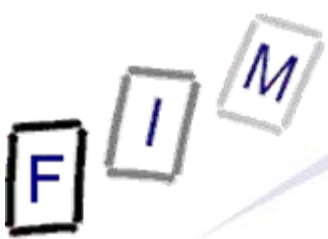
Fallstudie: Session-ID Entscheidung

- Beklagter: Immobilienunternehmen
 - Möchte „statischen“ Link ohne Bezahlung
 - Server ruft Formular ab und extrahiert Session-ID
 - Konstruiert mit Adresse und ID einen GET-Request-Link
 - Dieser Link wird auf der Haus-Seite angezeigt
 - Besucher klickt darauf → Direkt beim Plan
- Ergebnis: Kein Besuch der Startseite (→ Keine Werbung)
 - Keine Falscheingaben der Adresse, bequemer, gratis, ...
- Entscheidung: 2 Schutzziele durch Session-ID
 - Verhinderung dauerhafter Links
 - » Wurde erreicht und nicht umgangen
 - » Potentielle Optionen (hier anscheinend technisch nicht möglich):
 - Besondere ID, die nicht abläuft
 - Verlängerung der ID vor Ablauf
 - » Keine Umgehung → Keine Rechtsverletzung!



Fallstudie: Session-ID Entscheidung

- Zweites Schutzziel:
 - Unlizenzierte Benutzer sollen stets über die Startseite
 - Schutzobjekt: Karte (Werk? Nicht geprüft; wohl ja!)
 - Erfolgreich umgangen durch automatisierten Seitenabruf
 - » Wirtsch. Schaden wegen keiner Anzeige der Werbebanner
 - Wer möchte dies umgehen?
 - » Nicht: Privatnutzer
 - Kein Bedarf: Gratis; Adresse muss ohnehin eingegeben werden!
 - » Nur: Kommerzielle Nutzer, die anderen einen direkten (Deep-)Link zur Verfügung stellen möchten
 - Daher: Angreifer = Durchschnittlicher Webprogrammierer
 - » Für solche ist die Aufgabe trivial
 - Abrufen der Seite, Session-ID extrahieren, URL generieren
 - » Session-ID wird öffentlich dargestellt ([siehe Bild](#))
 - » Formularfelder in URL sichtbar, wenn leeres Form. abgeschickt
 - » Keine Spezialisten und keine „Spezialprogramme“ nötig



- Wirksamkeit: Relative Beurteilung
 - ① Schutzziele beschreiben
 - ② Potentielle Verletzer identifizieren
 - ③ Angreifer näher beschreiben
 - ④ Nur triviale Aufwendungen oder mehr?
- Bedeutet eine Einschränkung der Verbote/Strafbarkeit gegenüber der absoluten Beurteilung
 - Dürfte aber praxistauglicher sein
 - „Kriminelle Energie“ existiert nur bei nicht-trivialem Aufwand
 - » Strafbarkeit (§ 91 UrhG): 6 Monate Gefängnis!
- Muss dem Schutz der „Werke“ dienen
 - Nicht ausschließlich, aber zum überwiegenden Teil
 - Kein Schutz von Geschäftsmodellen
 - » Handy-SIM-Lock, Druckerpatronen, etc.

F I M

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!