Electronic Commerce und das Street Performer Protocol

John Kelsey Bruce Schneier
{kelsey,schneier}@counterpane.com
Counterpane Systems, 101 East Minnehaha Parkway, Minneapolis, MN 55429

(Aus dem Englischen übersetzt von Andreas Neus, andreas@neus.net)

Zusammenfassung

Wir stellen hier das Street Performer Protocol vor, ein Electronic-Commerce Verfahren zur Erleichterung der privaten Finanzierung öffentlicher Werke. In Verwendung dieses Protokolls würden Menschen Spenden in die Obhut eines Treuhänders geben, die an dann an einen Autor ausgeschüttet werden, wenn das versprochene Werk der Allgemeinheit zur Verfügung gestellt wird (Public Domain). Das Protokoll hat das Potential, alternative oder "marginale"Werke zu finanzieren.

1 Einleitung

Stellen Sie sich eine Welt ohne Copyright vor. Menschen schreiben Bücher, Musik, etc., aber sie werden nur für eine einzige Aufführung oder Drucklegung bezahlt. Sobald das Werk veröffentlicht ist, kann jeder, dem es gefällt, es kopieren und verbreiten. In jener Welt würden qualitativ hochwertige, leicht kopierbare Werke wie Geschichten, Romane, Nachschlagewerke und Musikstücke wirtschaftlich ein "öffentliches Gut". Das heißt, die Schöpfer dieser Werke müßten knappe Ressourcen zur ihrer Produktion aufwenden, obwohl sie davon nicht den überwiegenden Nutzen hätten.

Dies läßt vermuten, daß in jener Welt deutlich weniger solche Werke produziert würden, als in unserer, und auch ein gutes Stück weniger als die Konsumenten dieser Werke es wünschten. Aufgrund verschiedener technischer Entwicklungen jedoch scheinen wir uns in Richtung einer Welt zu bewegen, die viel weniger wie die uns vertraute und viel mehr wie jene Welt aussieht, in der Copyright nicht durchgesetzt wird.

In diesem Artikel betrachten wir einen sehr einfachen und allgemeinen Ansatz zur Finanzierung der Produktion öffentlicher Güter wie werbefreie Radio- und Fernsehsender und spontane Musikdarbietungen an öffentlichen Plätzen. Die Künstler bieten an, die Produktion ihrer freien Werke so lange fortzusetzen, wie ausreichend Geld in Form von Spenden eingeht, um sie für ihren Aufwand zu entschädigen. Wir diskutieren soziale, finanzielle und technische Regelungen, die dieses Verfahren recht gut funktionieren lassen, obgleich wir nicht glauben, daß es jemals eine vollständige Lösung für das Problem der Bezahlung der Schöpfer für ihre Werke sein wird. Vorrangig diskutieren wir, wie eine spezielle Ausführung dieser Idee, "Street Performer Protocol" genannt, funktionieren kann.

Im Rest dieses Artikels erläutern wir, warum wir glauben, daß die aktuelle Situation der Durchsetzung des Copyright, selbst durch technische Mittel erweitert, wahrscheinlich nicht mehr gut funktionieren wird — und wie soziale, finanzielle und technische Strukturen aufgebaut werden können, die diesen Ansatz praktikabel zu machen, und die wahrscheinlichen Angriffe auf das System. Wir schließen mit einer Betrachtung der vielen offenen Fragen zu dem dargestellten und ähnlichen Verfahren.

2 Warum Copyright in der Zukunft schwer durchzusetzen sein wird

Bevor wir detailliert diskutieren wie das Street Performer Protocol funktioniert, möchten wir erläutern, warum wir bezüglich der Durchsetzung von Copyright in der relativ nahen Zukunft so pessimistisch sind. Unsere Skepsis basiert auf zwei Schlüsselannahmen.

Erstens ist die Durchsetzung des Copyright einfacher, wenn Produktion und Distribution qualitativ hochwertiger Kopien von Information relativ teuer

und aufwendig sind. Eine Fabrik, die raubkopierte CDs preßt, und ein Verteilernetzwerk von LKWs und Verkäufern, ist relativ schwer zu verstecken. Einmal entdeckt, gibt es keien Zweifel über die illegale Unternehmung. Letztendlich spiegelt der Verlust der Investition in die Geräte und die Zerstörung des Distributions-Netzwerkes einen echten Nutzen für Rechte-Inhaber, weil eine signifikanter Anteil aller möglichen raubkopierten CDs eliminiert wird.

Moderne Technologie wird all das ändern. Perfekte digitale Kopien büßen auch über die Zeit ihre Qualität nicht ein und benötigen nur relativ preiswerte Geräte zur Wiedergabe. Ein Distributions-Netzwerk ist heute bereits verfügbar – das Internet. Mit dem Internet (und Funktionen wie e-Mail Verschlüsselung, anonymen Remailern und dem vorgeschlagenen "Eternity Service") und neuen Speichertechnologien wie DVDs benötigt ein künftiger Raubkopierer nur noch sehr wenig Kapital um anzufangen und wird (im Gegensatz zu bisher) vermutlich eher ein Amateur sein, der Kopien verschenkt, als ein Unternehmer, der viel Geld mit CD-Raubkopien verdient.

Unser zweiter Grund: Die strikte Durchsetzung von Copyright würde automatisch eine Reihe von Maßnahmen verlangen, die stark an einen Polizeistaat erinnern. Die Aufklärung von Copyright-Verletzungen durch "Traitor-tracing"(Verräter-Ermittlung) verlangt die Offenlegung der Identität jedes Käufers eines geschützten Werkes und vermutlich auch eine Datenbank aller Werke, die von einer bestimmten Person gekauft oder aus einer Bücherei ausgeliehen wurden. Auch können technische Maßnahmen verwendet werden, um die Verbreitung bestimmter Texte zu begrenzen. Ein Großteil der jüngsten (politischen) Aktivität zur Eindämmung von Copyright-Verletzungen bestand darin, beim (US-)Kongress für drakonische Gesetze gegen Copyright-Piraterie, Gesetze zur Einschränkung der Forschung über Computersicherheit und Kryptographie, sowie Gesetze, die den Vertrieb von Aufnahme- und Computergeräten für die Allgemeinheit beschränken würden, zu werben.

2.1 Technische Lösungen: Copyright Commerce Systems

Technische Lösungen zum Schutz des Copyright wurden vielerorts vorgeschlagen. Diese fallen normalerweise in zwei Kategorien:

1. Einige Ansätze versuchen den zu schützenden Inhalt solange verschlüsselt zu lassen, wie er sich außerhalb einer gesicherten Umgebung befindet. Das sichere Gerät spielt, zeigt oder führt den Inhalt nur dann aus wenn es dazu autorisiert wurde. Wir nennen diese Verfahren "Secure Perimeter Schemes"(Sichere Perimeter Ansätze).

2. Einige Ansätze verlangen von Käufern des zu schützenden Inhalts das Vorweisen einer Identifikation, um diese dann mit dem Inhalt in einer Weise zu verbinden, die ein nachträgliches Entfernen stark erschwert. In diesem Fall würde die Verbreitung des Inhaltes im Netz den Käufer entlarven, der vermutlich über enorme Summen auf Ersatz des Schadens am geistigen Eigentum des Rechteinhabers verklagt wird. (In fast allen Fällen wird die Abschreckung anderer vor der zukünftigen Verletzung geistigen Eigentums eher das Ziel sein, als die Wiedergutmachung von Schäden.) Wir nennen diese Ansätze "traitor tracing"(Verräter-Rückverfolgung).

Die Kombination beider Ansätze im selben System ist durchaus möglich.

2.1.1 Secure Perimeter Schemes

Mit Secure Perimeter Schemes gibt es verschiedene Probleme. Das grundlegendste besteht schlicht darin, daß bei Graphiken, Video, Audio und Text ein Wert für den Nutzer nur dann gegeben ist, wenn er sie sehen oder hören kann. (Ausführbare Inhalte wie Computer-Programme können genutzt werden, ohne die gesicherte Umgebung zu verlassen, daher ist dieses Argument darauf nicht anwendbar.) Dies bedeutet, daß sogar in einer idealen Welt mit "wasserdichtem" Kopierschutz und vor Mißbrauch geschützten, speziell versiegelten Geräten für Copyright unterliegende Inhalte, das Anfertigen von nichtautorisierten Kopien des geschützten Inhalts immer noch möglich ist. Mit speziell zu diesem Zweck hergestellten Geräten kann dies vermutlich relativ einfach geschehen. (Musik kann vermutlich einfach und mit nur geringem Qualitätsverlust kopiert werden, indem dasselbe Stück mehrfach abgespielt wird und die Ausgaben zusammengemischt und neu aufgenommen werden, um dann das Ergebnis so weit wie möglich zu säubern. Das Kopieren von Video-Ausgaben von einem Bildschirm erscheint, obwohl natürlich möglich, ein ganzes Stück schwieriger.)

Es gibt auch ein wirtschaftliches Problem. Der Kunde sieht im Kauf eines Sicheren Perimeters kaum Mehrwert. Der Verkauf eines mißbrauchgeschützten

Gerätes, dessen einziger Nutzen das sichere Abspielen Copyright-geschützter Inhalte ist (z. B. eine versiegelte Box mit Lautsprechern und einem Bildschirm) erscheint schwierig. Es ist leichter, Software zu verkaufen oder zu verschenken, um den Secure Perimeter zu erzeugen, in dem das zu schützende Material aufbewahrt wird. Auch dies ist jedoch ziemlich einfach zu umgehen, sogar für relativ ungeübte Angreifer. (Wenn der Angriff beendet ist, kann die Methode vermutlich ins Internet gestellt werden.)

Schwieriger, jedoch immer noch gangbar, ist das Verkaufen oder Verschenken einer speziellen, mißbrauchgeschützten Box zum Anschluß an den PC oder den Fernseher des Nutzers, die den Copyright-geschützten Inhalt entschlüsselt, wenn sie dazu autorisiert wird. Die Satelliten- und Kabelfernseh-Industrien haben hierfür verschiedene Beispiele gezeigt und ihre bisherigen Erfolge beim Abwehren von Angriffen geben nicht viel Anlaß zur Hoffnung für die Zukunft dieses Ansatzes. Neben verschiedenen Angriffen gegen die Sicherheits-Box selbst, gibt es auch allgemeinere Attacken – den Output vor dem Bildschirm oder den Lautsprechern abfangen und speichern, um ihn ins Internet zu stellen. Wiederum erwarten wir, daß auch die Software, mit der dies bewerkstelligt wird, im Internet verfügbar wird. (Nebenbei bemerkt wurde diese Klasse von Attacken bisher gegen Kabel- oder Satellitenfernsehsysteme kaum verwendet, wahrscheinlich aufgrund eines Mangels an verfügbarer Bandbreite und Speicherkapazität sowie der Existenz anderer, leichterer Angriffe.)

Beachten Sie auch, daß dann, wenn der Inhalt in vielen Formen existiert (z. B. standard Musik-CD, Broadcast-Audio-Signal, oder ein verschlüsseltes Audio-Format zum Herunterladen aus dem Internet), der Angreifer die Musik immer noch von einer CD aus (die mit Bargeld gekauft wurde) in einer Audio-Datei speichern und dann ins Internet stellen kann. Dies könnte nur verhindert werden, wenn Copyright-geschützte Musik niemals außerhalb dieser sicheren Perimeter gelassen würde. Musik oder Filme könnten demnach nie ausgestrahlt werden, da sie dann aufgenommen und illegal ins Netz gestellt werden könnten.

Mit Werkzeugen wie anonymen Remailern und dem Eternity Service können Inhalte, die einmal ins Netz gestellt wurden, schlicht nicht mehr gelöscht werden, ohne praktisch den gesamten Dienst zu zerstören. Das bedeutet, daß eine einzige Veröffentlichung eines Copyright-geschützten Musik-, Video- oder Text-Werkes im Internet dieses kostenlos (oder zumindest sehr billig) für die Öffentlichkeit verfügbar macht. Ja, sogar ohne den Eternity Service ist Information, die einmal ins Internet gestellt wurde, sehr schwer zu löschen, auch wenn juristische Drohungen sie vermutlich aus den großen Suchmaschinen entfernen können.

2.1.2 Traitor Tracing Schemes

Traitor Tracing Ansätze versuchen diejenige Person, die das Copyright-geschützte Material ins Netz gestellt hat, zu ermitteln und sie für Verluste des Urhebers zur Verantwortung zu ziehen. Da die Verluste wahrscheinlich sehr hoch sein werden, und da sowohl strafrechliche als auch zivilrechtliche Strafen drohen, könnte dies die Person davon abschrecken, die Copyright-Verletzung überhaupt zu begehen. Dieses Vorgehen hat den zusätzlichen Vorteil, daß es vollständig innerhalb des bestehenden Vertragsrechts umsetzbar ist, indem von jedem, der Copyright-geschütztes Material kauft, verlangt wird, sich vertraglich zur Haftung zu verpflichten, wenn seine Kopie irgendwo auftaucht.

Das erste Problem, bei diesem Ansatz liegt darin, daß der Käufer von Copyright-geschütztem Inhalten das Risiko eingehen muß, wirtschaftlich ruiniert oder eingesperrt zu werden, falls er beschuldigt wird, das geschützte Material ins Netz gestellt zu haben. Er hat keinen guten Grund, anzunehmen, daß das Traitor-Tracing System fehlerfrei arbeitet. Sogar wenn wenn das Traitor-Tracing System selbst funktioniert, kann das umgebende System (die Verbindung der eingebetteten Seriennummern oder sonstiger Identifikation mit einer bestimmten Person) Ziel eines Angriffs werden.

Noch gravierender ist, daß eine Plattenfirma oder ein Verlag nur einen geringen direkten Anreiz hat, die richtige Person zu erwischen. Um vor künftiger Copyright-Verletzung abzuschrecken, muß an irgendjemandem ein sehr sichtbares Exempel statuiert werden. Wenn es die richtige Person trifft, um so besser. Aber die meisten Leute, die durch das Exempel abgeschreckt werden sollen, haben keine Ahnung, ob die Person schuldig oder unschuldig ist, so daß der Abschreckungseffekt essentiell derselbe ist. Die Plattenfirma oder der Verlag werden vermutlich versuchen, die richtige Person zu erwischen; aber ihr einziger finanzieller Anreiz, ist die Eliminierung eines weiteren Copyright-Verletzers und die Vermeidung kostspieliger Gerichtsverfahren von der fälschlich beschuldigten Person.[1]

[1] Dieses Anreizproblem tritt auch in vielen anderen Situationen auf, z. B. das Bombenattentat auf den olympischen Park und Geldautomaten-Betrug in den UK.

In einer Welt, in der Copyright-geschützte Werke sehr stark an Wert verlieren, sobald sie einmal im Netz auftauchen, kann man vermutlich den Copyright-Verletzer für den größten Teil des Verlustes gar nicht in Anspruch nehmen. Normalerweise wird er schlicht nicht genug Geld haben. Weiterhin sind nur sehr wenige PCs oder Häuser sicher genug um Informationen zu beherbergen, die, wenn anonym im Internet gepostet, ihrem Besitzer auch nur ein paar Tausend Dollar kosten, von Millionen von Dollar ganz zu schweigen. (Zum Vergleich möge der Leser überlegen, ob er gewillt wäre, einen Koffer mit nur einmal $10.000, die seinem Chef gehören, bei sich zuhause zu haben, ohne zusätzliche Sicherheitsmaßnahmen oder Versicherung.)

Das zweite Problem dieses Ansatzes ist, daß er von jedem Käufer von Copyright-geschütztem Material das Vorlegen einer extrem schwer zu fälschenden Identifikation verlangt. Wie oben beschrieben, ist dies für jede Art von Medium notwendig, nicht nur für das Herunterladen digitaler Inhalte über das Internet; andernfalls kauft ein kluger Angreifer einfach eine CD mit Bargeld, lädt sie in seinen Computer und postet sie anonym ins Netz. Diese schwer zu fälschende Identifikation muß allgemein verfügbar sein und letztendlich vermutlich mit einer nationalen Identifikationskarte verbunden werden. Ein hartnäckiger Angreifer kann versuchen, die Identifikation zu fälschen oder eine leichtgläubige oder verzweifelte Person dazu bringen, den Inhalt an seiner Stelle zu kaufen.

Das dritte Problem mit diesem Ansatz liegt darin, daß er mit an Sicherheit grenzender Wahrscheinlichkeit letztendlich irgendwo die Existenz einer Datenbank verlangt, mit jedem Stück urheberrechlich geschützter Information, das irgendjemand je gekauft hat. In einer Welt, in der fast alle Bücher, Filme und Musik online gekauft werden, erzeugt dies eine wirklich unangenehme Zerstörung der persönlichen Privatsphäre. Es wirft auch einige interessante Fragen auf. Werden Regierungen diese Information vorhalten? Wie steht es mit großen Medienkonzernen? Werden die Einträge in der Datenbank auch Scheidungsanwälten und unabhängigen Strafverfolgern zugänglich gemacht? Werden Werbefirmen in der Lage sein, für Marketingzwecke Listen darüber zu kaufen, wer welches Buch gekauft hat? Wie steht es mit der Sicherheit dieser Datenbank? (Wie viel ist die Liste von allen Leuten, die *Die Satanischen Verse* gekauft haben, auf dem offenen Markt wert?)

2.2 Juristische Lösungen

Die juristische Durchsetzung existierender oder neuer Copyright Gesetze wird durch das Internet und andere neue Kommunikationstechnologien außerordentlich erschwert. Diese Technologien erlauben es, Information frei zu verbreiten, selbst wenn Regierungen diese Information lieber nicht verbreitet sähen. Dies trifft für urheberrechtlich geschützte Information ebenso zu wie für jede andere Information.

Das grundsätzliche Problem der Durchsetzung mit den neuen Technologien ist, daß in der nahen Zukunft fast jeder mit einem Computer und einer Internetverbindung in der Lage sein wird, Copyright-geschütztes Material ins Internet zu stellen. Dieses Material wird, sobald es einmal ins Netz gestellt wurde, von fast jedem abrufbar sein und auch ohne einen funktionierenden Eternity Service nur sehr schwer wieder aus dem Netz zu entfernen sein.

Dies wird für die Durchsetzung von Copyrightansprüchen vermutlich bedeuten, daß für jeden einzelnen Copyrightverletzer zehntausende Dollars an Polizei- und Gerichtsressourcen dafür aufgewendet werden müssen, die von ihm begangenen Verletzungen zu unterbinden, der jedoch nur wenige Ressourcen zur Wiedergutmachung des Schadens hat und nur einen verschwindend geringen Bruchteil der gesamten Copyrightverletzungen verursachte. Das bedeutet nicht, daß die Durchsetzung nicht versucht wird. Jedoch kann die Ökonomie dieser Art von Gesetzesvollzug bereits heute im Kampf gegen Drogen beobachtet werden, ebenso wie ihre Effektivität. Unterschiedliche nationale Gesetzgebungen machen das Problem nur schwieriger.

Und zuletzt laufen die notwendigen Maßnahmen zur Unterbindung weitverbreiteter Copyrightverletzungen darauf hinaus, die juristische und technische Infrastruktur für weitverbreitete Zensur zu schaffen.

3 Alternative Finanzierung copyrightgeschützter Werke

Im letzten Teil haben wir diskutiert, warum wir nicht glauben, daß traditionelle Copyright-Durchsetzung weiterhin funktionieren wird, was auch bedeutet, daß viele Schöpfer von Inhalten vermutlich künftig nicht mehr auf dieselbe Weise bezahlt werden, wie sie traditionell bezahlt wurden. Dies wird vermutlich Probleme für viele Arten von Content Providern verursa-

chen, insbesondere Filmstudios, da selbst die Herstellung ein relativ billigen Films eine Menge Geld kostet. (Romane können geschrieben und Musik komponiert und aufgeführt werden, ohne einen großen Overhead. Aber nur sehr wenige gute Filme können in jemandes Garage entstehen und viele sehr gute Filme könnten schlicht nicht mit solchen Budgets realisiert werden.)

Wenn die Urheber nicht mehr durch traditionelle Tantiemen bezahlt werden, dann ist es sinnvoll zu überlegen, welche alternativen Quellen der Finanzierung verfügbar sind. Während wir nicht vorhaben, eine abschließende Liste zu erstellen, sind einige Alternativen offensichtlich:

1. *Freiwillige Zuwendungen* Einige Leute werden Auftragsarbeiten finanzieren, wie sie es schon immer getan haben; einige werden bereit sein, Geld zu spenden, damit ihr Lieblingsautor ein weiteres Buch fertig schreibt. Das Street Performer Protocol ist eine Möglichkeit, um dies zu realisieren.

2. *Werbung* Der Inhalt könnte von Servern angeboten werden, die sich durch Werbung finanzieren. Wenn die Server kostenlos und so eingerichtet sind, daß das Herunterladen dieses Inhaltes sehr schnell geht, dann können sie eine gute Stange Geld verdienen, da die meisten Nutzer es vorziehen werden, den Inhalt kostenlos vom schnellsten Ort zu bekommen und sich dabei an ein paar Anzeigen nicht stören werden. Copyright-Verfolgung ist dann nur gegen andere Sites gerichtet, die den Inhalt herunterladen und versuchen, ihn weiterzuverkaufen. Wir sehen dies als eine der vielversprechendsten Alternativen an und das Street Performer Protocol kann und sollte mit dieser Alternative genutzt werden. Wir weisen auch darauf hin, daß viele kommerzielle Web-Sites dies bereits in der einen oder anderen Art tun; beispielsweise bezahlen die Anzeigen auf verschiedenen Nachrichten- und Suchmaschinensites für die Verfügbarkeit dieser Sites. Es gibt keine Mechanismen, die den Nutzer davon abhalten, die Inhalte weiterzuverbreiten, abgesehen von gelegentlichen Copyright-Warnungen.

3. *Product Placement* Product Placement geschieht, wenn ein Werber den Urheber des Inhaltes dazu bringt, sein Produkt oder seine Idee in einem positiven Licht zu erwähnen. Beispielsweise haben viele neuere Filme Product Placement als eine zusätzliche Geldquelle für den Film verwendet. Wir erwarten, dies öfter zu sehen. Jedoch weisen wir auch darauf hin, daß dies nur für einige Medien gut funktioniert und daß viele Künstler und Konsumenten solches Product Placement ablehnen werden, besonders wenn sie zu offensichtlich sind.

4. *Staatliche Förderung* Viele Länder haben eine Form staatlicher Förderung der Künste, und dies könnte noch populärer werden, wenn Copyrights sehr schwer durchsetzbar werden. Es gibt jedoch offensichtliche soziale Konsequenzen, wenn (beispiesweise) alle Romanautoren und Musiker, die überhaupt für ihre Werke bezahlt werden, von einer staatlichen Einrichtung bezahlt werden. Außerdem ist es unwahrscheinlich, daß selbst sehr generöse Budgets für die Förderung dieser Werke mit der Geldmenge vergleichbar wären, die momentan für urheberrechtlich geschützte Bücher, Musik, Filme, etc. ausgegeben wird.

4 Unsere Lösung: Das Street Performer Protocol

4.1 Übersicht

Angenommen, ein Autor möchte für seinen nächsten Roman in einer fortlaufenden Serie bezahlt werden. Unter traditionellen kommerziellen Mechanismen würde er einen Verleger finden, der im Endeffekt die Erstellung des Romans finanziert. Der Verleger würde den Roman dann dem Massenmarkt anbieten, in der Hoffnung, daß genügend Leute den Roman kaufen, um seine Kosten wieder einzuspielen. Falls der Autor keinen Verleger finden kann, könnte er das Buch selbst herausgeben und hoffen, seine Kosten einzuspielen. In jedem Fall gehen der Autor und/oder der Verleger ein finanzielles Risiko ein, in der Hoffnung, einen Profit zu machen.

Es gibt eine Alternative. Nach der Logik des Straßenkünstlers (Street Performer) wendet sich der Autor direkt an seine Leser, *bevor* das Buch veröffentlicht ist; vielleicht sogar bevor das Buch überhaupt geschrieben ist. Der Autor umgeht den Verlag und macht eine öffentliche Ankündigung, etwa so:

> "Wenn ich $100.000 an Spenden erhalte, werde ich den nächsten Roman in dieser Reihe veröffentlichen."

Leser können auf die Web-Site des Autors gehen, nachsehen, wie viel Geld bereits gespendet wurde, und Geld dafür spenden, daß der Roman veröffentlicht wird. Beachten Sie, daß es dem Autor gleich ist, wer dafür zahlt, daß der nächste Teil erscheint; ebensowenig braucht ihn zu interessieren, wie viele Menschen das Buch lesen, die nicht dafür gezahlt habem. Sein Interesse ist, daß sein $100.000 Topf gefüllt wird. Sobald das der Fall ist, veröffentlicht er das nächste Buch. In diesem Fall bedeutet "veröffentlichen" einfach "verfügbar machen", nicht "binden und durch Buchhandlungen vertreiben". Das Buch wird – ohne Kosten – jedem zur Verfügung gestellt; denjenigen, die dafür bezahlt haben und denjenigen, die das nicht taten.

Es gibt grundsätzlich drei Dinge, die bei dieser Art von System schief gehen können:

- Der Autor kann einen unpassenden Preis verlangen. Er und andere Autoren werden vermutlich aus ihren frühen Fehlern lernen und ziemlich gut in der Wahl passender Preise werden.
- Der Autor veröffentlicht das Buch bevor die gewünschte Menge Geld eingegangen ist. Dies scheint außer den Autor niemanden direkt zu schädigen, aber es könnte die Teilnahme an künftigen Aktionen dieser Art untergraben, insbesondere solche, die von demselben Autor durchgeführt werden.
- Der Autor erhält die gewünschte Geldmenge, aber veröffentlicht das nächste Buch trotzdem nicht. Dies wird die Reputation des Autors für künftige Vereinbarungen dieser Art ruinieren, aber das ist für den Autor nur dann schädlich, wenn er bereits eine Reputation aufgebaut hat und plant, weitere Bücher zu veröffentlichen. Es ist dieser Fall, für den wir den Nutzen von Kryptographie und einer "Trusted Third Party" (Treuhänder) für das Funktionieren des ganzen Systems sehen können.

Die ersten beiden sind Marktplatz-Probleme, die sich essentiell selbst korrigieren. Beim dritten Problem geht es um Vertrauen und dies ist eine nähere Betrachtung wert. Der offensichtliche Weg zur Lösung dieses Problems liegt darin, eine dritte Partei als Treuhänder einzuschalten, die die Transaktion handhabt. In Ermangelung eines besseren Ausdrucks nennen wir diese Partei "Verleger".

Der Autor reicht seinen Roman, oder Teile davon, falls es sich um eine Serie handelt, beim Verleger ein. Der Verleger läßt den Roman von seinen Lektoren prüfen um zu entscheiden, ob sich ein Verkaufsversuch lohnt (wie jeder Verleger – allerdings mit sehr niedrigen Druck- und Bindekosten). Falls dies der Fall ist, einigen sich Autor und Verleger auf einen Preis und ihre Anteile. Für unbekannte Autoren werden die ersten Kapitel, oder vielleicht sogar die ersten Bücher, frei verfügbar sein, mit dem Ziel, Kunden zu gewinnen. Für bekannte Autoren sind vielleicht die ersten beiden Kapitel frei, der Rest läuft durch den Zahlungsmechanismus. Der Autor hat den ganzen Roman und macht über seine Web-Site beispielsweise die Kapitel 1-3 kostenlos verfügbar. Kapitel 4 wird erscheinen, sobald $1000 dafür gespendet wurden, oder zu einem Zieltermin.

Jeder Spender von $N erhält ein unterschriebenes Zertifikat, das eine Sicherheit darstellt. Sollte der Roman am Zieldatum nicht veröffentlicht worden sein, kann das Zertifikat bei der Bank des Verlegers gegen $N plus Zinsen eingelöst werden.

Der Verleger kann in diesem Prozess so stark involviert sein, wie er möchte. Er könnte wie ein traditioneller Verleger agieren und Manuskripte auswählen, redigieren, veröffentlichen und promoten. Er würde dies in der Hoffnung tun, durch seine Marke als Verlag einen höheren Preis zu erzielen als der Autor alleine das könnte. Der Verleger könnte auch darauf hoffen, durch die Erstveröffentlichung auf seiner Web-Site zusätzliches Geld durch den Verkauf von Werbung zu verdienen. Auf der anderen Seite könnte er auch nur eine Art "Vanity Press" sein, also ein Verlag, der für Geld alles Druckt, ohne auf die inhaltliche Qualität zu achten und für den Autor als Inkassobüro arbeitet.

Wenn genügend Leser das nächste Kapitel lesen wollen, können sie eine Einzahlung machen. Der Verleger benötigt dazu keine Identifikation, daher würden anonyme Zahlungssysteme hierfür gut funktionieren. Der Verleger hält die Einzahlungen als Treuhänder, bis das Kapitel veröffentlicht ist, und schickt dem Autor dann seinen Anteil.

Beachten Sie, daß der wichtigste Grund für die Einschaltung des Treuhänders darin liegt, das Vertrauensproblem zu einer Instanz zu geben, die einen Anreiz hat, sich eine gute Reputation zu bewahren.

4.2 Motivation

Die Finanzierung des nächsten Romans in einer Reihe ist ein klarer Fall des Problems eines "öffentlichen

Gutes": Jeder Spender hat vermutlich sehr wenig Einfluß darauf, wann oder ob der nächste Roman veröffentlicht wird. Um einige mögliche Motivationslagen zu verstehen, müssen wir einige Situationen betrachten, in denen Straßenkünstler verschiedenster Art bereits jetzt bezahlt werden.

1. Ein Spender mag Geld teilweise aus der Motivation heraus spenden, als nette Person, Förderer der Künste etc. angesehen zu werden.

2. Es mag zusätzliche Anreize zum Spenden geben: Die Verlosung eines Mittagsessens mit dem Autor beispielsweise.

3. Ein Spender wird vermutlich eher Geld geben, wenn er sehen kann, daß sein Geld einen unmittelbaren Effekt hat. Daher haben öffentliche Radiostationen Ziele für Spendenaktionen, und für bestimmte Zeiten. Dies könnte dahingehend übertragen werden daß Romane in kleinen Teilen veröffentlicht werden, sobald kleine Zwischenziele erreicht werden. Erfahrungen im Markt werden zeigen, welche Preis- und Marketingstrategien am besten funktionieren.

5 Das Street Performer Protocol

5.1 Rollen

Im grundlegenden Street Performer Protocol gibt es drei Parteien: Den Autor, den Verleger und den Leser ("Der Leser" sind tatsächlich natürlich viele Menschen). Ihre Ziele sind einfach:

1. Der Autor:
   (a) Will eine angemessene Summe für sein Werk erhalten.
   (b) Will nicht, daß der Verleger sein Werk stiehlt.
   (c) Will, daß der Verleger sich an alle vertraglichen Vereinbarungen, wie Marketing und Exklusivität, hält.
2. Der Verleger:
   (a) Will eine angemessene Summe für die Bereitstellung des Werkes des Autors und die Administration des Prozesses erhalten
   (b) Will, daß der Autor sich an alle vertraglichen Vereinbarungen, wie Zeitplanung, Exklusivität, etc. hält.
3. Der Leser / Spender:
   (a) Will, daß das Werk veröffentlicht wird, sobald ausreichende Spenden eingegangen sind.
   (b) Will, daß seine eigene Spende ordentlich verrechnet wird und daß der Autor den Prozentsatz erhält, den er mit seinem Verleger vereinbart hat.
   (c) Will, daß über den "aktuelle Kontostand" der Spenden ordentlich berichtet wird.

Die meisten dieser Ziele bestehen zwischen den Parteien und können nur durch Verträge und Gerichte durchgesetzt werden. Einige können jedoch durch das Protokoll erleichtert werden.

5.2 Das Protokoll

Im folgenden wird der grundsätzliche Ablauf des Street Performer Protocol dargestellt. Wir nehmen an, daß das Werk ein Roman ist und daß dieser Kapitel für Kapitel veröffentlicht wird. Wir nehmen ebenso an, daß ein Verleger alle finanziellen Transaktionen handhabt und das Buch veröffentlicht. Selbstverständlich funktioniert dasselbe allgemeine Protokoll ebensogut für andere Arten digitalen Eigentums.

5.2.1 Einreichen des Werkes beim Verleger

Der Autor reicht einen bestimmten Teil seines Werkes beim Verleger ein. Das könnte ein kompletter Roman sein, oder nur die ersten paar Kapitel. Der Autor gibt dem Verleger auch das Resultat einer Hash-Funktion der nächsten paar Kapitel, oder sogar aller fehlender Kapitel des Romans. Der Autor und der Verleger verhandeln die Vertragsbedingungen bezüglich der Kosten für die Veröffentlichung des nächsten Kapitels (oder der nächsten paar Kapitel) und bezüglich der Verteilung des eingesammelten Geldes zwischen Autor und Verleger. Wenn die Verhandlungen abgeschlossen sind, stellt der Verleger die ersten paar Kapitel auf seine Web-Site, zusammen mit einem Hinweis darauf, wie viel Geld gespendet werden muß, damit das nächste Kapitel veröffentlicht wird.

Beachten Sie, daß der Autor dem Verleger in einigen Fällen den gesamten Roman geben wird, in anderen

Fällen nur die ersten paar Kapitel. Es ist sogar denkbar, daß der Roman in dem Moment der Verhandlung noch gar nicht zuende geschrieben ist, obwohl dies den Autor und den Verleger in eine schwierige Situation bringen könnte, sollte der Autor nicht in der Lage sein, den Roman rechtzeitig zu beenden. Für den Rest dieses Abschnitts nehmen wir an, daß der Roman geschrieben ist und der Verleger immer über den Text der nächsten paar zu veröffentlichenden Kapitel verfügt. Der Hash-Wert der Endfassung des Romans muß dem Verleger nun übergegeben werden.

5.2.2 Spenden einsammeln

Der Verleger sammelt Spenden indem er praktisch Wetten darauf annimmt, daß der Roman unter bestimmten Bedingungen veröffentlicht wird. Er verkauft den Spendern ein unterschriebenes Versprechen, alle Spenden zurückzugeben, eventuell mit Zinsen, falls das nächste Kapitel des Romans nicht zu einem bestimmten Termin erscheint.

Der Spender schickt $X an Spenden und zusätzlich eine eindeutige Identifikation, um anzugeben, wohin ggf. Rückzahlungen gehen sollen. Spender, die anonym bleiben wollen, können entweder ein anonymes Konto angeben, das letztendlich zu ihnen zurück führt, oder eine gemeinnützuge Organisation oder anderen Begünstigten ihrer Wahl. Die einzigen Begünstigten von denen abgeraten werden sollte, sind Autor und Verleger.

Der Verleger schickt ein digital signiertes Dokument, in dem er verspricht, die Spende von $X zurückzuzahlen, es sei denn ein bestimmtes Ereignis oder eine Menge von Ereignissen geschieht. Das offensichtlichste Ereignis, das eingeplant werden muß, ist das Nichterscheinen des nächsten Kapitels zur gesetzten Deadline. Der Spender erhält mit dem signierten Dokument sowohl eine Garantie für die Rückerstattung, falls der Autor das Werk nicht bis zu dem versprochenen Termin veröffentlicht, als auch einen Nachweis, daß er $X für dieses Werk gespendet hat.

5.2.3 Rückzahlung an die Spender

Die Spenden werden treuhändisch gehalten bis alle Bedingungen erfüllt sind. Da diese Bedingungen leicht zu verstehen und zu beweisen sind (es gibt einen Hash-Wert des zu veröffentlichenden Materials), können sie von fast jedem objektiv überprüft werden. Falls das versprochene Werk nicht bis zu dem angegebenen Datum freigegeben wird, kann das signierte Dokument des Spenders verwendet werden, um Geld vom Verleger zu kassieren. Sollte dieser die Zahlung verweigern, können die Spender seine Reputation ruinieren, indem sie nachweisen, daß er sich nicht an die Vereinbarung gehalten hat.

5.2.4 Auslieferung

Sobald der notwendige Wert an Spenden eingegangen ist, gibt der Verleger das Kapitel in die "Public Domain" frei. Er könnte es auf seine Web-Site stellen und die Spender dann informieren, daß das Werk verfügbar ist. Werbung auf dieser Site wird vermutlich zusätzliches Geld einbringen.

5.3 Variationen und Verfeinerungen

Das grundsätzliche Ziel all dieser Verfeinerungen liegt darin, jede Partei mit finanziellen Interessenskonflikten durch jemanden zu ersetzen, der eine Pauschale für die Erfüllung einer Funktion erhält und keinen Anreiz hat, mit einer anderen internen Partei zu konspirieren.

5.3.1 Der Bankier

Wir können einen Bankier hinzufügen, um Zahlungen zu handhaben. Wir würden das Protokoll dahingehend ändern müssen, daß der Bankier das Geld Treuhändisch für den Verleger hält. Bankiers haben ein großes Reputations-Kapital und keinen finanziellen Anreiz, die Leser oder den Verleger zu betrügen. Wenn die Einzahlungen erfolgt sind, können die Leser dem Verleger ihre "Quittungen" zuschicken, die als ausreichender Nachweis dienen, um die Reputation des Bankiers zu ruinieren, sollte er betrügen.

Der Bankier darf die Spenden nicht herausgeben bis das Material veröffentlicht wurde. Dies muß ihm vorher zur Prüfung ausreichend beschrieben sein: Er erhält den Hash-Wert des zu publizierenden Materials, die Spenden werden angenommen, er benachrichtigt den Verleger und den Autor wenn der angestrebte Wert erreicht ist, und wenn er sieht, daß das Material veröffentlicht wurde, zahlt er.

5.3.2 Manipulation des Inhaltes

Dies betrifft verschiedene Dinge: Zu kurze Kapitel, qualitativ schlechte Kapitel, das Einsammeln von Spenden ohne den Inhalt fertig zu haben, etc.

All diese Dinge werden durch Reputation gelöst. Wenn der Verleger oder der Autor eine gute Reputation aufbauen oder erhalten wollen, dann dürfen sie solche Dinge nicht tun. Da die Leser/Spender eine direkte Sanktionsmöglichkeit haben (aufhören zu spenden), reicht dies aus.

6 Anwendungen: Finanzierung von Public Domain Werken durch die Öffentlichkeit

Das Street Performer Protocol ist effektiv ein Mittel zur privaten Finanzierung öffentlicher Werke. Es ist auf alle Arten alternativer öffentlicher Werke anwendbar: Literatur, Musik, Video, etc. Es kann verwendet werden, um Public-Domain Software zu verbessern: Firmen könnten Preise nennen, zu denen sie verschiedene Features einem existierenden Public-Domain Software Paket hinzufügen würden, und Nutzer könnten für diejenigen Features bezahlen, die sie wollen. Wenn genügend Leute ein bestimmtes Feature haben wollen, wird es designed und implementiert. Leute könnten dieses Protokoll verwenden um ihre Web-Site zu finanzieren: Wenn die Leute bereit sind, dazu beizutragen, wird die Site weiter gepflegt und verbessert.

Eine andere Spielwiese für das Protokoll sind Serien. Menschen finden Fernsehserien wie Party of Five oder ER sehr spannend, in denen langfristige Themen und Geschichten entwickelt werden. Es könnte möglich sein, eine Low-Budget Video-Serie über Jahre am Laufen zu halten, indem man immer die nächsten paar Episoden fertig hat. Das elegante an dieser Lösung ist, daß Werbetreibende und Boykotte hier nicht besonders viel bedeuten: wenn genügend Leute bereit sind, "mit ihren (e-)Geldbörsen abzustimmen", dann ist es egal, wie viele wütende Dan Quayle Unterstützer Morphy Brown[2] nicht mögen. Tatsächlich funktioniert das Public Broadcasting System (öffentliches Fernsehen) der Vereinigten Staaten auf diese Weise: Einige Leute spenden Geld um bestimmte Arten von Programmen zu sehen, aber alle genießen die Vorzüge dessen, was dann ausgestrahlt wird.

[2]Natürlich funktioniert dies in beide Richtungen: es gibt zweifellos einen Markt, wenn auch einen sehr kleinen, für ein paar KKK Serien mit rührenden Geschichten über einen liebenswerten Haufen Schwachköpfe, die Kreuze in den Vorgärten von Menschen mit der falschen Hautfarbe verbrennen. Freie Meinungsäußerung schneidet in beide Richtungen.

7 Schlußbetrachtung

Die Idee eines "Autors", der "Rechte" an einem "Werk" hat, ist noch relativ neu und geht auf die Zeit der Druckerpresse zurück. Vor dieser Zeit war es unmöglich ein Werk von seiner konkreten physikalischen Instantiierung zu trennen, daher hatte "Copyright" keine sinnvolle Bedeutung. Seitdem haben die relativen Kosten für das Kopieren und Verteilen von Werken Copyrights erst ermöglicht und zu ihrer Durchsetzung geführt. Zukünftige technologische Entwicklungen werden dazu führen, daß Copyrights nicht mehr aufrechtzuerhalten sind, da die Barriere für das Kopieren und Verteilen gegen null sinkt. Es wird unmöglich werden, über eine physikalische Instanz eines Werkes als etwas vom Werk getrenntes zu reden, da es beliebig viele Instanzen geben kann.

Das Street Performer Protocol ist zwar offensichtlich keine vollständige Lösung für das Problem, geistiges Eigentum in dem Zeitalter kostenloser und perfekter Kopien zu vermarkten, aber es ist in einigen Situationen nützlich.

Wenn ein vertrauter Zwischenhändler das System verwalten würde, könnte es ohne Vertrauen zwischen Autor und Leser implementiert werden. Autoren die vielleicht keine Publikationsmöglichkeiten in traditionellen Medien haben, könnten ein Beispiel ihres Werkes freigeben und zu Spenden für "mehr desselben" aufrufen. Auf diese Weise könnte die Fähigkeit des Netzes, Menschen mit ähnlichen Interessen zusammenzubringen, genutzt werden, um Werke zu finanzieren, die anderenfalls möglicherweise gar nicht finanziert würden.

8 Widmung

Dieser Artikel ist Ross Anderson gewidmet, der einen Teil seiner Jugend damit verbrachte, als Straßenmusiker auf Deutschlands Straßen seinen Dudelsack zu spielen.

Literatur

[And96a] R. Anderson, ed., *Information Hiding, First International Workshop Proceedings*, Springer-Verlag, 1996.

[And96b] R. Anderson, ed., "The Eternity Service," *Pragocrypt '96, Part 1*, CTU Publishing House, 1996, pp. 242-252.

[BGH+95] M. Bellare, J.A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, and M. Waidner, "KP – A Family of Secure Electronic Payment Protocols", *The First USENIX Workshop on Electronic Commerce*, USENIX Association, 1995, pp. 89-106.

[Bra93a] S. Brands, "Untraceable Off-line Cash in Wallets with Observers," *Advances in Cryptology—CRYPTO '93 Proceedings*, Springer Verlag, 1994 pp. 302-318.

[Bra93b] S. Brands, "An Efficient Off-line Electronic Cash System Based on the Representation Problem," C.W.I. Technical Report CS-T9323, 1993.

[CR93] CitiBank and S. Rosen, "Electronic-Monetary System," International Publication Number WO 93/10503; May 27 1993.

[Fer94] N. Ferguson, "Extensions of Single-Term Coins," *Advances in Cryptology—CRYPTO '93 Proceedings*, Springer-Verlag, 1993.

[FY92] M. Franklin and M. Young, "Towards Provably Secure Efficient Electronic Cash," Columbia Univ. Dept. of C.S. TR CUCS-018-92, April 24, 1992. (Also in Icalp-93, July 93, Lund Sweden, LNCS Springer-Verlag)

[LMP94] S. H. Low, N. F. Maxemchuk and S. Paul, "Anonymous Credit Carts", *The Second ACM Conference on Computer and Communications Security*, ACM Press, 1994, pp. 108–117.

[MN93] G. Medvinski and B. C. Neuman, "Netcash: A Design for Practical Electronic Currency on the Internet," *The First ACM Conference on Computer and Communications Security*, ACM Press, 1993, pp 102–106.

[NM95] B. C. Neuman and G. Medvinski, "Requirements for Network Payment: The NetChecque^{TM} Perspective," Compcon '95, pp. 32–36.

[Oka95] T. Okamoto, "An Efficient Divisible Electronic Cash Scheme," *Advances in Cryptology—CRYPTO '95 Proceedings*, Springer-Verlag, 1995, pp. 438–451.

[OO90] T. Okamoto and K. Ohta "Disposable Zero-Knowledge Authentication and Their Applications to Untraceable Electronic Cash," *Advances in Cryptology—CRYPTO '89 Proceedings*, Springer-Verlag, 1990, pp. 481–496.

[OO92] T. Okamoto and K. Ohta, "Universal Electronic Cash," *Advances in Cryptology—CRYPTO '92 Proceedings*, Springer-Verlag, 1992, pp. 324–337.

[ST95] M. Sirbu and J. D. Tygar, "NetBill: An Internet Commerce System Optimized for Network Delivery Services," Compcon '95, pp. 20–25.

[SK96] B. Schneier and J. Kelsey, "A Peer-to-Peer Software Metering System" *The Second USENIX Workshop on Electronic Commerce*, USENIX Association, 1996, pp. 279–286.

[TMSW95] J. M. Tenenbaum, C. Medich, A. M. Schiffman, and W. T. Wong "CommerceNet: Spontaneous Electronic Commerce on the Internet," Compcon '95, pp. 38–43.

Translator's comment: *This is a German translation of the article "Electronic Commerce and the Street Performer Protocol" by* John Kelsey *and* Bruce Schneier. *If your English is up to it, I strongly suggest reading the original, which should be available here:* `http://www.counterpane.com/street_performer.html`

I have tried to remain truthful to the original wording – occasionally perhaps to a fault. If you have a suggestion for improving this translation, please contact me at `andreas@neus.net`. *This is version 1.0.*

Anmerkung des Übersetzers: *Dies ist eine deutsche Übersetzung des Artikels "Electronic Commerce and the Street Performer Protocol" von* John Kelsey *und* Bruce Schneier. *Wenn es Ihr Englisch erlaubt, empfehle ich, das Original zu lesen, das hier verfügbar sein sollte:* `http://www.counterpane.com/street_performer.html`

Ich habe versucht, mit der Übersetzung möglichst nah an dem Original zu bleiben – stellenweise vielleicht zu nah. Wenn Sie Vorschläge zur Verbesserung dieser Übersetzung haben, teilen Sie mir diese bitte unter `andreas@neus.net` *mit. Dies ist Version 1.0.*