Off-line Economies for Digital Media

Darko Kirovski and Kamal Jain
Microsoft Research
One Microsoft Way
Redmond, WA 98052, USA
{darkok,kamalj}@microsoft.com

ABSTRACT

We propose a novel platform for building off-line markets for digital content. The key objective is to enable an arbitrary user of specific digital content to resell it to other users in an **off-line peer-to-peer** manner so that part of the proceeds go to content's copyright holder. Most importantly, one part of the revenues is retained by the seller as an incentive for participating in the distributed economy. To address this objective, a transaction is finalized and incentives distributed to the seller **on-line** using a **client-server** architecture. Technologically, such systems can be readily created, for example, by adding a communication tool such as Bluetooth to a portable media player such as the iPod. We present a threat model for the proposed system and devise a novel protocol that relies on traditional public-key cryptography to ensure secure and efficient off-line transactions of arbitrary digital content. As a consequence, in our system copyright holders can control the pricing and recruit a powerful marketing and sales force with marginal investment and via various types of incentives, users are offered the ability to sell or purchase content they like anywhere, anytime, and to/from anyone.

1. INTRODUCTION

There exist two proliferated classes of content distribution mechanisms: centralized on-line stores and file-sharing networks. The first class is based upon an on-line system that markets, recommends, sells, and stores digital content onto users' personal computers or portable media players. A popular example of such a system is Apple's combination of an on-line store, iTunes, with a media player device, the iPod [1]. There, majority of the marketing, storage, and processing burden is imposed upon the servers while limiting the customers to purchase clips only when they are connected to the Internet. Such systems do not let demand influence content pricing. Most importantly, such an economic platform does not address the widespread phenomenon of file sharing [3], where convenient search mechanisms and media availability are not supported with the possibility to purchase content at the benefit of the copyright holder. Thus, in most file-sharing networks, content distribution is economically isolated from copyright holders.

In this paper, we propose a novel platform for marketing digital content, which enables several key features:

- **off-line sales** – an owner of a copy of particular digital content, can sell it to a third party without the immediate assistance of the copyright holder or service provider. This feature is important for several reasons: energy efficiency (the energy bill for a transmitter is proportional to $\mathcal{O}(r^3)$, where r is the distance to the receiver), usability, and ability to commit a transaction independent from location and existence of wireless service providers. The localized nature of viral marketing commonly creates a sense of community. Recent proliferation of portable media players makes this feature particularly attractive to end-users.
- **immediate purchase** – pending a successful data transfer, the buyer can play the content immediately. This feature is particularly attractive as verbal or perceptive viral marketing can be immediately converted to revenues and content ownership – a feature that no other content delivery system supports.
- **incentive-based sales** – proceeds from the transaction are partitioned into two parts: one assigned to the copyright holder and another credited to the participating sales-force; they are credited towards all parties once either seller's or buyer's device establishes a connection to some form of global communication.

Thus, the aim of the platform is to enable selling digital content by anyone, anywhere, and anytime – posing almost no restrictions to the network and business models that can be established within the platform. Since content owners have the incentive to resell their content, they may engage in countless marketing strategies. The platform can support both push and pull marketing, where traditional approaches to push are local and global broadcasts and multicasts, and to pull is, for example, data search in a network of storage systems. The platform can also enable sophisticated forms of trade such as market-basket, subscriptions, trade-for-fee, and multi-party or multi-item discounts.

The proceeds of each trade are processed upon connecting seller's or buyer's portable media player to a global network such as the Internet or a wireless access point. This poses a requirement for an efficient cryptographic protocol

NOSSDAV '06 Newport, Rhode Island USA

that should enforce integrity of payments despite the lack of tamper-proof hardware. We assume that media players can be tampered with, i.e., all DRM secrets can be revealed and altered – as a consequence, players will be able to share arbitrary files with other players outside of the proposed economic ecosystem, just as is the case nowadays. Even with their devices "broken," sellers and buyers should not be able to claim benefits from transactions that did not occur or alter details of existing transactions. Hence, the system deploys only "best-effort" anti-piracy mechanisms such as existing DRM technologies [2] and tamper-resistant hardware [4], while relying on incentives to sellers to build the economy. In other words, if the incentives are not significant, users are likely to participate in file sharing without the control of copyright holders – for sufficient incentives, users are likely to drive sales for their and copyright holders' economic benefit.

1.1 Related Work

Considering the size of the music market alone estimated at around $12B in the US, there has been surprisingly few solutions that uniquely address the distribution and economics of digital media. A technology particularly related to our work, and to the best of our knowledge, the first to address incentive-based digital media economies, has been deployed at Weedshare [6, 7]. In their system, all sales are executed on-line using traditional DRM as all participants are interconnected to their servers during transactions.

Other types of incentive-based systems have been proposed for peer-to-peer systems with an emphasis on the *free-rider* problem [8], i.e., the existence of users that participate in sharing files only as consumers, not contributors, thus, increasing contributors' costs. Golle et al. proposed a system where users pay for downloads and get paid for uploads using a quantized micro-payment system or receive "points"-incentives to share files [9]. In both cases, their system was focused on file-sharing systems without addressing copyright holders' benefits and a simplified economic model. Several other mechanisms address this problem with alternative but similar approaches [3, 10, 11]. Another class of problems associated with solutions to thwart free-riders is *whitewashing*, i.e., non-contributing users, who create new accounts under different pseudonyms, to avoid the penalties associated with free-riders [12].

Nearly all incentive-based peer-to-peer mechanisms are focused on limiting free-riders, who themselves are usually a consequence of the availability of free content on peer-to-peer systems. We aim at the other part of the content distribution spectrum where copyright holders are not isolated economically from the distribution channels. The goal is to, using the convenience of immediate off-line transactions, sway users from peer-to-peer distribution into another model which directly benefits both copyright holders for improved, inexpensive marketing and customers for media availability and economic participation in the distribution chain.

2. ATOMIC OFF-LINE TRANSACTION

In this section, we outline the cryptographic protocol that enables an off-line transaction of digital content between two connected devices isolated from a global network such as the Internet. The commitment to buy and optionally, content delivery as executed in peer-too-peer manner, whereas the actual transaction is executed later, during a separate client-server session. There exist four entities in an atomic off-line transaction: seller $\mathbf{s}$, buyer $\mathbf{b}$, service provider $\mathbf{p}$, and trusted authority $\mathbf{t}$. The service provider is contracted by the copyright holders to resell and/or organize the sales of their digital content. The service provider is responsible for realizing the payments in the system via credit cards or other form of banking. Similar to traditional e-commerce transactions, the trusted authority issues a public-private key-pair to each entity including certificates that authenticate the distributed public keys. This information is used so that users can authenticate each other and prove identities when buying clips or redeeming credits for transactions.

We assume that RSA is used as a public-key cryptosystem [14] by following the IEEE 1363-2000 standard IFSP-and IFVP-RSA [5]. For a given entity $\mathbf{x}$, we denote its public-private key-pair as $\{p_{\mathbf{x}}, r_{\mathbf{x}}\}$ respectively. In order to vouch for the authenticity of their public key, each entity other than $\mathbf{t}$, owns a certificate $c_{\mathbf{x}} = \{p_{\mathbf{x}}, s_{\mathbf{x}}\}$, which contains the signature $s_{\mathbf{x}} = SP_{r_{\mathbf{t}}}(p_{\mathbf{x}})$, where function $SP_a(b)$ denotes RSA's signing primitive of message b using private key a. Certificates are verified by proving $p_{\mathbf{x}} = VP_{p_{\mathbf{t}}}(s_{\mathbf{x}})$, where function $VP_a(b)$ denotes RSA's verification primitive of signature b using the public key a. Just as in modern certificate verification protocols, we assume that $p_{\mathbf{t}}$ is known to all devices. Finally, each device is assumed to contain a certificate of the service provider, $c_{\mathbf{p}} = \{p_{\mathbf{p}}, s_{\mathbf{p}} = SP_{r_{\mathbf{t}}}(p_{\mathbf{p}})\}$, upon enrolling in the off-line market service.

2.1 Transaction Objectives

Each atomic transaction must fulfill several objectives related to the associated threat model. The basic premise is that either buyer's or seller's device is likely to eventually connect to a global network following an off-line transaction. This way, transactions are eventually committed with $\mathbf{p}$ so that the buyer is billed and the seller is credited with the incentive. To commit a transaction, it is sufficient that only one of the participants connects with $\mathbf{p}$. The objective is to prevent manipulations that may benefit either of the entities in an unfair manner. As shown in Figure 1, an adversary can "break" the tamper-resistance of her media player. Then she could use the player both as a buyer and seller to commit fraudulent transactions. While it is hard to prevent two "broken" devices from engaging in unlimited data exchange, we want to prevent "broken" devices from communicating with protected devices in any other way but via the proposed communication protocol. For example, the system should allow for a "broken" player to buy or sell content via regular economic channels and with the originally assigned identity.

A – Transaction integrity. Both buyers and sellers must not be able to alter any data about committed transactions. A buyer must not be able to repudiate a transaction after which she downloaded the digital content from the seller.
B – Mutual initiation. A seller must not be able to create an arbitrary transaction with any buyer unless he gains control over buyer's player either physically or via a software virus. The latter case can be prevented by demanding physical action to initiate a transaction such as a "purchase" button that enables data transmission on contact only.
C – Limited damage in case of device loss. A lost media device could enable the party who finds it to realize only limited financial gain γ defined by the user. Amount

γ equals the total purchasing power that a device may have between two synchronization events with **p**.

D – Media piracy prevention via traditional methods. The platform should protect copyright holders from piracy via traditional DRM methods such as symmetric encryption and licenses [2]. Such systems are vulnerable as encryption keys can be reverse engineered and/or decrypted media can be captured either digitally or using an analog recorder.

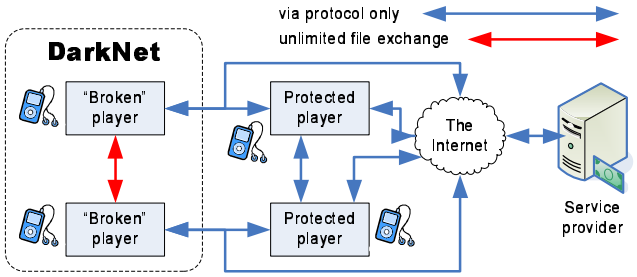

Figure 1: The type of data exchange enabled after "breaking" a protected media player. DarkNet players can exchange files with no limitations - however, when they talk to players in the protected world, they can only do so via the proposed protocol.

E – Device revocation. As a buyer, a "broken" player can obtain media from a valid seller off-line; the seller would discover that the transaction was fraudulent when connecting to **p**. To prevent this, lost or misused devices should be identified and their list distributed to (i.e., updated with) all devices upon connection with **p**. Thus, an updated seller device should be able to verify buyer's financial validity before participating in a transaction.

F – Certificate expiration. In order to prevent ever-growing revocation lists, **p** should set expiration dates on certificates issued to protected players.

G – Exclusive sales point. As a seller, a "broken" device must be prevented from distributing its content to *protected* devices without any boundaries. Such a device could collect payments (if any) using an alternative payment channel (e.g., cash). This can be prevented by mandating that buyers report to **p** all purchased content since their last update.

H – Robustness to communication failure. Upon communication failure, a buyer or seller must not be able to enjoy the benefits of the transaction without all its details being reflected. For example, a buyer could pay for a media clip and lose connection during download. When connecting with **p**, the buyer should present her transaction receipt to resume download.

J – Enforcing clients to commit transactions. Certain sellers may refuse to take their sales credits to benefit their "buyers" with free content. A user may certainly decide never to connect its media device online or "break" its device and remove its history of non-committed transactions. In both cases, the user pays an indirect price by not being able to participate in the distributed economy. A user can always "break" her player and reset its DRM state – this should occur only if the adversary invests non-trivial effort and funds into "breaking" the tamper-resistant media device. As a consequence, just as illustrated in Figure 1, a "broken" player could engage in unlimited file exchange with another "broken" player but communicate with protected players and **p** only via the proposed protocol. Thus, "broken" players must not be able to claim benefits to transactions that did not occur.

J – Transferring sale proceeds to the lawful copyright holder. The crucial issue here is that an adversary can use an existing digital content copyrighted by holder $\mathbf{h}_1$, alter its DRM information to point to holder $\mathbf{h}_2 \neq \mathbf{h}_1$, and sell the content for the benefit of $\mathbf{h}_2$. To prevent this, **p** must authorize only trusted entities as copyright holders.

2.2 Transaction Protocol

In this subsection, we introduce a protocol that satisfies the list of requirements from the previous subsection. In essence, the buyer and seller must authenticate each other, the buyer sends a signed incentive to buy, the seller sends a receipt, and only after the acknowledgment of the buyer that she received the receipt, the atomic transaction is executed. Then, the seller may send the content to the buyer.

I – Authentication and Key Exchange. Initially, the two parties must authenticate each other. This is a task already provided in traditional cryptographic protocols such as TLS1.0 [15]. According to the TLS version 1.0 Handshake Protocol, the opposing sides perform several tasks:

- exchange certificates, $c_{\mathbf{b}}$ and $c_{\mathbf{s}}$; then, each side verifies the opposing side's certificate by proving that $p_{\mathbf{s}} = VP_{p_{\mathbf{t}}}(s_{\mathbf{s}})$ and $p_{\mathbf{b}} = VP_{p_{\mathbf{t}}}(s_{\mathbf{b}})$,
- exchange information to compute a 48-byte master-secret used to create session keys,
- establish a way of encrypting and compressing data during the following private communication, and
- establish a session identifier as well as a flag specifying whether the session is resumable.

II – Checking the Revocation List. Each device must verify whether the other device participating in the transaction has a valid account with **p**. For that reason, **p** must continuously update players with the latest list of revoked players. In order to prevent the list from growing excessively, each account has an expiration date specified in the account's certificate. Players with expired accounts cannot purchase or sell content.

III – Marketing. It is important that the buyer receives the content that is marketed. As a marketing ploy, the seller may forward to the potential buyer a version of the content that may be of superior quality compared to the copy that is later uploaded to the buyer. When committing to a purchase, the buyer wants to receive assurance that the clip of interest, a, is of particular identity and quality. There may be several versions of this assurance subprotocol. Here, we outline two examples.

III.a – Buyer likes clip, does not know author, title. Here, the seller provides clip's cut-out, a_c, which has been approved by the copyright holder as an advertisement, to the buyer. The holder also provides the purchasing data:

$$m'_1 = \{ID(a), s'_1 = SP_{r_{\mathbf{p}}}(H(a_c, ID(a)))\}, \quad (1)$$

where $ID(a)$ returns a distinct identifier and descriptor of clip a. The descriptor may include clip's coding quality, version, copyright holder, license agreement, and price. Function $H(a)$ returns a cryptographic hash [17], of the clip a.

By listening to a_c, computing $H(a_c, ID(a))$, and verifying against s'_1 using provider's public key $p_{\mathbf{p}}$, the buyer can get assurance that she will ultimately receive a, the clip that **p** associated with a_c.

Most importantly, note that the seller can keep competitive advantage on the market by not revealing the author and title of the advertised clip to a prospective buyer. Our system enables this feature – the party who owns a can ask **p** to provide $\hat{m}'_1 = \{\hat{ID}(a), s'_1 = SP_{r_{\mathbf{p}}}(H(a_c, \hat{ID}(a)))\}$, where $\hat{ID}(a)$ does not contain identifying information for a. The advertisement receipt $\hat{m}'_1$ can also be provided to a buyer by a seller. An additional economic tool is system's ability to attach a price to $\hat{m}'_1$ which a buyer (i.e., potential seller) must pay to obtain. Finally, after purchasing the clip, the buyer obtains the full $ID(a)$.

III.b – Buyer knows author, title, buys clip from seller w/o preview. Here, the seller sends out:

$$m''_1 = \{ID(a), s''_1 = SP_{r_{\mathbf{p}}}(H(ID(a)))\} \quad (2)$$

to the buyer who can verify that the seller is offering the desired clip without media preview.

IV – Buyer's Commitment. In case the buyer desires to purchase certain digital content, she commits to the purchase by sending a signed intent of purchase to the seller. The intent is represented using $m_2 = \{i, s_2 = SP_{r_{\mathbf{b}}}(H(i))\}$, where $i = \{m'_1 || m''_1, \mathbf{b}, \mathbf{s}, P_c\}$ and P_c contains purchase information such as date/time/location,[1] license and price. Message P_c can also include a request to buy an advertisement receipt $\hat{m}'_1$ for a (see step **III.a**). The buyer sends m_2 to the seller as a transaction request. The seller can verify the purchase intent using buyer's public key $p_{\mathbf{b}}$. In order for both sellers and buyers to protect their privacy, their public keys $p_{\mathbf{b}}$ and $p_{\mathbf{s}}$ are used as pointers to transaction participants in message i instead of **b** and **s**.

Note that the price and license may be negotiated between **b** and **s**. Copyright owners must be careful in setting up pricing rules for their content as buyers and sellers can seek alternative payment channels (e.g., cash, trade). Here is an extreme example. A copyright holder did not assign a minimum price to its content a. The holder relied upon seller's incentives in the form of percentage of revenue to motivate selling the content at a higher price. Sellers could still sell a at high price but in cash, circumventing system's payment system. Then, they would report a transaction price of $0 to **p** and retain the full actual revenue to themselves. In order to account for this potential problem, the copyright holder has to use lower-bounded pricing. In addition, the holder has to incorporate this type of "incentive" in its economic model when setting up the price/incentive rules.

V – Seller's Receipt. In order for the buyer to claim her purchase to **p**, she must receive a receipt from the seller. The receipt is constructed as: $m_3 = \{P_r, SP_{r_{\mathbf{s}}}(H(j))\}$, where $j = \{m_2, P_r\}$ and P_r contains receipt information required by **p**. The buyer can verify the receipt using seller's public key $p_{\mathbf{s}}$. If the verification is successful, the buyer can claim a from the seller or if communication is terminated, from **p**. If the latter event occurs, **p** can credit the incentive to the seller's account even without synchronization with the seller's device.

[1]In case transaction participants want to protect their privacy, they should be able to chose whether to record such data within the transaction receipt.

VI – Buyer's Ack. Upon receiving and verifying seller's receipt, the buyer sends an acknowledgment signal, $m_4 = SP_{r_{\mathbf{b}}}(m_3)$, back to the seller. Upon receiving and verifying the acknowledgment, the seller can claim the incentive independent of buyer's communication with **p**. Hence, the buyer can commit the transaction with **p** independent of the seller after step **V**. For the seller to claim his incentives independent of the buyer, step **VI** must be finalized.

VII – Content Download. Upon receiving and verifying m_4, the seller starts with the upload of a. The content is encrypted with a session key derived from the session master key (created in step **I**). The buyer can immediately start enjoying her purchase. If the transaction included the corresponding advertisement receipt $\hat{m}'_1$ (see step **III.a**), then the seller must upload this data as well.

The act of downloading the media clip in this protocol is a matter of mutual agreement between the buyer and the seller. The act can be interrupted by lack of power, communication, or intentionally at either one of the devices. The overall transaction is not affected by unsuccessful step **VII**, as both the buyer and the seller have their receipts to claim the content and incentive independently. Subsection 2.3 discusses how the protocol can be altered so that the act of media transfer can be guaranteed and priced.

VIII – Claiming Incentives. The seller is credited with his incentives upon the following two events.

- The seller received a valid m_4, in which case he submits $\{m_3, m_4\}$ to **p**. Upon successful verification of signatures in m_3 and m_4, **p** credits the seller with the incentive and forwards the remainder of the revenue to the copyright holder associated with a.
- In the alternate case, the buyer never received a. When she contacts **p** to download the content from its server with a proof of purchase m_3, the seller is credited with his incentive. Both actions are executed pending a successful verification of signatures in m_3.

Hence, communication failure can occur in steps **VI** or **VII** and still the transaction can be committed in the first case by the buyer and in the second by the seller contacting the service provider. If communication failure or some other form of not conforming to the protocol occurs in steps **I**–**V**, the transaction is voided.

2.3 Pricing the Bandwidth

Media download while both devices are off-line, has functional value for both the buyer and the seller. The buyer can play the content immediately. The seller consumes additional energy to transfer a relatively large media file. Particularly in the case of an anonymous transaction, the seller may chose to avoid uploading the media file to preserve energy as an act of unfairness. For example, with a cost of about US$5 per communication device, Bluetooth transfers data at a rate of at most 721Kbps, low-cost, low-power ZigBee at up to 250Kbps, and more expensive and energy-thirsty 802.11g devices at 54Mbps. As a common media clip is typically in the 2-8MB range, download can take substantial time and produce a significant energy bill. To address this issue, we propose an additional, optional sequence of steps to the protocol which enables the seller to price the actual download into the transaction. Thus, the buyer can obtain a purchase receipt for one price and both the receipt

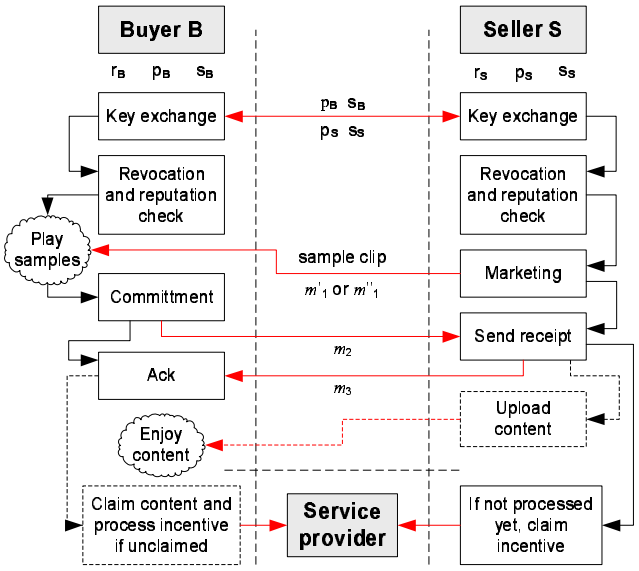

Figure 2: Illustration of steps in the protocol for atomic off-line transaction of digital goods.

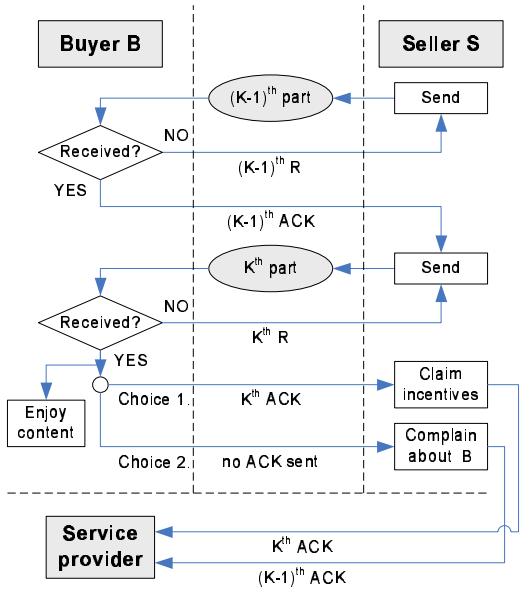

Figure 3: Events involved in uploading a purchased media file to a buyer. The buyer may not send the acknowledgment for two reasons. First, she has not received the last packet, cannot send a request to seller to resend. Second, she received the last packet but either cannot or does not want to send acknowledgment to seller.

and the content for another, higher price. The optional part of the protocol is illustrated in Figure 3.

In order to realize such a transaction, a buyer **b** has to specify the type of transaction (receipt or receipt+media) as well as the price when creating the intention to purchase. This is denoted in the field P_c in step **IV**. At step **VII**, a seller **s** partitions the content a into K packets and sends them independently to **b**. One of the objectives is to force **b** to upload all K packets in order to play any perceptually significant portion of a. Thus, **s** initially generates a fresh encryption key k, encrypts a in CBC mode (denoted as $E_k(a)$; [17], pp.229, §7.2.2), and creates a message $e = k||E_k(a)$. Message e is then partitioned into K parts, $\{e_1, \ldots, e_K\}$, which are then sent to **b** in decreasing order of their index, i.e., part e_1 is the last, K-th packet sent to **b**. Each packet transmission is followed by an acknowledgment of receipt. The last two acknowledgments, ack_{K-1} and ack_K, in the process are signed by **b**, where $ack_j = SP_{r_b}(H(i||j))$. After receiving ack_{K-1}, **s** sends the last packet e_K. The buyer can decrypt and play the content after this step. However, **b** is still required to send ack_K to **s**. When **s** receives ack_K, he can claim the additional pricing incentive to **p** by supplying ack_K with all other data as presented in step **VIII**.

Several incident cases may arise in this procedure:

(i) **b** may receive e_K but fail to send ack_K to **s** due to loss of power or communication. However, **b** can acknowledge the completion of this transaction when she synchronizes with **p**. Hence, in this case **s** depends upon **b** to communicate eventually with **p** in order to claim his incentives.

(ii) After receiving e_K, **b** may maliciously chose not to send ack_K to **s** so that she can obtain the service of downloading the content off-line for free.[2]

(iii) **b** may have not sent ack_K because she never received e_K ; **s** cannot distinguish between (ii) and (iii) because communication with **b** has ceased.

The system can address the problem of distinguishing between (ii) and (iii) using at least two strategies. First, users do not decide upon individual protocol actions – in order to be able to alter the protocol steps, **b** must "break" her player's tamper-resistance and alter its software; two actions that should incur substantial cost. Device tamper-resistance is discussed in Subsection 2.5. Second, after an incomplete transaction **s** can inform **p** about the incident. The report includes ack_{K-1} in addition to all other messages described in step **VIII**. Since the likelihood of case (iii) is relatively small, **p** can affect the reputation of **b** and possibly, additionally charge **b** and credit **s** with his incentive. Thus, user's reputation becomes a probabilistic reflection of its economic trustworthiness. Even a perfectly policy-obeying buyer is expected to have certain small percentage p of negative feedback. This expectation can be reduced proportionally to the size of e_K, i.e., for that reason, we assume that $e_K = k$. For systems where $p \ll 10^{-2}$, malicious parties can obtain negligible benefits by performing (ii) approximately every $\frac{1}{p}$ transactions. Finally, **s** can report a transaction incident with **b** even tough **s** received ack_K – in this case **s** wishes to discredit **b**'s reputation for some reason. To prevent this event, downloads are always reported by buyers to **p** so that any similar accusations can be cleared.

2.4 Privacy

In any setting where tamper-resistant hardware hosts protected software, typically the issue of privacy is raised. Pri-

[2]Note that **b** still must pay for the purchase receipt in order to download the content.

vacy and security often affect one another and in certain cases it is difficult to ethically resolve and define the rightful balance (e.g., separating crime reporting from privacy protection). We aim to adopt a common but controversial standard applied in banking and other services where the service provider as a trusted authority keeps record of all transactions in a manner that protects user privacy. With all the ambiguities of such a protection standard, the frontier for privacy protection can be defined from the perspective of the buyer and seller. Ultimately, a buyer or a seller should not be able to show a transaction receipt to a third party and reveal seller's or buyer's identity respectively.

The buyer and the seller exchange identifying information when they establish a secure connection in step **I**. As the public key of either of the users is sufficient to pinpoint its owner, it is important to anonymize user public keys while retaining their full functionality and system security. This can be achieved by distributing single-usage public-private key-pairs to users. A participant in a transaction can optionally use such a key-pair in case she wants to stay anonymous. Such key-pairs are supported with certificates issued by the service provider which can set correct expiration dates and reputation scores. Single-use key-pairs are not included in revocation lists.

2.5 Tamper-Resistance

It is crucial for the system that all media devices are protected using tamper-resistant hardware. All fraudulent activities are assigned a one-time non-trivial cost α for "breaking" a player. We can assume that $\alpha \approx \beta$, where device cost is denoted as β.

The difficulty of breaking tamper-resistant hardware is enforced using two different approaches: active zeroisation and passive techniques. Active zeroisation aims to destroy core information (in this case, user certificates) within a certain amount of time from detecting tampering with. Zeroisation is typically required in the absence of power supply; standards for such devices are outlined in standards ANSI X9.17 and FIPS 140-2. Commonly, such techniques are applied in hardware security modules [18], [19]. Passive techniques rely on chemical coating which is hard to tamper with [20, 21, 22]. Smart cards are widely deployed in numerous applications as their tamper-resistance makes them sufficiently cost-effective. Scale of piracy is estimated at being much lower than on-line credit usage of cards which is currently at 0.25% [23]. Thus, even with reports of ease of breaking earlier systems [24], modern systems have demonstrated economically efficient security and usability [25].

3. SUMMARY

Based upon a simple cryptographic protocol, we introduce a computing platform that enables users to sell their digital content to others. The resulting revenues are split between the copyright holder and the seller. The protocol has the ability to create an isolated economic ecosystem where free-trade is used to resolve any economic uncertainties. The operability and the efficacy of the entire platform depends upon sellers' incentives. In our system, media marketing can be based solely on the viral effect with dramatically reduced operating costs. As opposed to the "on-line store" model, computing resources required to run the viral economy, such as storage and bandwidth, are also fully distributed in our system.

4. REFERENCES

[1] Apple iTunes. `http://www.apple.com/itunes`.

[2] Microsoft Windows DRM. `http://www.microsoft.com/windows/windowsmedia/drm`.

[3] B. Cohen. Incentives Build Robustness in BitTorrent. Workshop on Economics of P2P Systems, 2003.

[4] Federal Information Processing Standards. Security Requirements for Cryptographic Modules. FIPS PUB 140-2, 2002.

[5] IEEE 1363-2000. Standard specifications for public key cryptography. IEEE, 2000.

[6] Weedshare Inc. `http://www.weedshare.com`.

[7] J. Beezer, et al. Redistribution of Rights-Managed Content and Technique for Encouraging Same. US Patent No. 10/326678.

[8] E. Adar and B. Huberman. Free riding on Gnutella. First Monday, Vol.5, no.10, 2000.

[9] P. Golle, et al. Incentives for sharing in P2P networks. ACM Electronic Commerce, pp.75–87, 2001.

[10] M. Feldman, et al. Robust Incentive Techniques for P2P Networks. ACM EC, pp.102–11, 2004.

[11] T.-W. Ngan, et al. Enforcing Fair Sharing of P2P Resources. Int. Workshop on P2P Systems, 2003.

[12] M. Feldman, et al. Free-Riding and Whitewashing in P2P Systems. Workshop on Economics and Information Security, 2004.

[13] The Digital Millennium Copyright Act of 1998. U.S. Copyright Office Summary, 1998.

[14] R.L. Rivest, et al. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, Vol.21, no.2, pp.120–126, 1978.

[15] T. Dierksa and C. Allen. The TLS Protocol Version 1.0. Internet draft, 1999. On-line at: `http://ietf.org/rfc/rfc2246.txt`.

[16] G. Doukidis, et al. Building Trust Online. Information Society or Information Economy? A combined perspective on the digital era, Idea Book Publishing, 2003.

[17] A.J. Menezes, et al. Handbook of Applied Cryptography. CRC Press, 1996.

[18] nCipher Technologies Inc. `http://www.ncipher.com/technologies`.

[19] SafeNet Inc. `http://www.safenet-inc.com/products/tokens/products_sc_330.asp`.

[20] Infineon Technologies AG. `http://www.infineon.com`.

[21] Axalto Inc. `http://www.axalto.com`.

[22] Gemplus Inc. `http://www.gemplus.com/smart/rd/publications`.

[23] G.R. Newman and R.V. Clarke. Superhighway Robbery: Preventing e-commerce crime. Willan Publishing, 2003.

[24] R. Anderson and M. Kuhn. Tamper resistance – A cautionary note. Usenix Workshop on e-Commerce, pp.1–11, 1996.

[25] J. Paynter and P. Law. An arms length evaluation of Octopus. University Of Auckland, Department of Management Science and Information Systems, working paper, 2005.