

# Topics in Cable and Security: Selective Encryption and Economic Lock-In

Tom Lookabaugh and Douglas C. Sicker  
Department of Computer Science and Interdisciplinary Telecommunications Program  
University of Colorado at Boulder  
[Tom.Lookabaugh, Douglas.Sicker]@colorado.edu

Presented at National Cable Television Association Academic Seminar  
New Orleans, Louisiana, May 1-2, 2004

## *Abstract*

*A customer experiences lock-in when the extra value it might obtain from a new supplier's product or services is exceeded by the cost of switching from its current vendor. Security technology is particularly potent as a source of lock-in, and the cable industry presents a powerful example of such lock-in. Cable system operators are locked-in by their equipment suppliers via the conditional access security systems used to secure programming from unauthorized viewers. We develop this example and its consequences. We then evaluate a particular technological strategy proposed to weaken this form of security technology based lock-in: selective encryption. We analyze the application of selective encryption to MPEG-2 video compression, the standard used in digital cable television. We find that selective encryption can be effective when carefully applied, but that it is important to pay attention to whether compression systems are configured in an antagonistic or cooperative mode relative to encryption, an issue of some concern if compression is provided by a vendor that competes with the security system provider.*

## **1. Economic Lock-In**

A customer experiences “lock-in” when the extra value it might obtain from a new supplier’s products or services is exceeded by the cost of switching from its current vendor<sup>1</sup>. Customers may regret this if they would have been better off having secured the alternative product from the start or if they cannot secure additional value unless such value exceeds the switching costs (in which case they will switch but only capture the additional value less the switching costs). Conversely, an incumbent supplier might appreciate and indeed encourage lock-in to the extent it can convert lock in into additional profit. These two interact in the sense that a supplier would likely forego additional profit (and a customer would receive lower prices) if switching costs were lower, even if the customer does not actually switch. Less apparently, though potentially more importantly, lock-in may impede access by a customer to product and service innovations.

Computer and communication security is a potent source of lock-in by virtue of several factors: (i) it can

be manifested as a technical compatibility requirement that must be met by a variety of applications and pieces of equipment communicating locally or across a network, and reverse engineering of the interface may in some cases be made equivalent to breaking a strong encryption system, (ii) suppliers may explicitly or implicitly suggest that proprietary security is better than open security since the supplier can control access to information about the system, (iii) it may be difficult to segregate legally permissible competitive reverse engineering from efforts to enable illegitimate piracy.

### *1.1. The Role of Security in Lock-In*

Many security systems include protocols that describe how messages are to be transmitted securely or how various components of a system (local or distributed) are to interact to perform a secure action. Conformance to such protocols creates a compatibility requirement across system components. A supplier that wishes to sell a system component will either need to be compatible with the necessary security protocols, or must provide sufficient additional value to motivate a customer to replace all other system components that require those security protocols. In this latter case, the cost of replacing other system

---

<sup>1</sup> A complementary concept is “lock-out”, the extent to which a competitor is precluded from serving an incumbent provider’s customer.

components becomes a switching cost and a source of lock-in. If the installed base that must be replaced is large, the cost can be prohibitive.

New suppliers attempting to circumvent security based lock-in without requiring wholesale replacement of compatible components by a customer will typically look to implement the necessary existing protocols. If the necessary protocols are not publicly known (they are proprietary), the new supplier may attempt to do so without the permission of those that originated, own, or otherwise control the required protocols. This may be technically feasible, but can be stymied by intellectual property law: the necessary information may be protected by various copyright and patent rights. This is, in fact, also true for the general case of technical compatibility based lock-in, but the effect is sharpened in the case of security because of the potential difficulty in distinguishing what might be considered legally protected reverse engineering activities for competition reasons from attempts to foster piracy for reasons of illegitimate access to messages or content. This particular effect has been manifested recently in controversy around application of the Digital Millennium Copyright Act. Originally created to outlaw circumvention by pirates of technology to protect intellectual property, the act is seeing broader application in preventing reverse engineering, such as a recent case in which an injunction was secured by Lexmark against a developer of chips that enable “clone” printer cartridges [Nowell].

Alternatively, a new supplier may seek to license the necessary security protocols from the owner. If the owner is the incumbent supplier, this should be feasible providing the incumbent supplier can extract the profit it forgoes for each product not sold from the new supplier through a license fee or equivalent compensation. But, it may be difficult to achieve this solution. If, for example, the new supplier’s advantage is more efficient manufacturing and it can offer the product to the customer for a lower price than the incumbent, the manufacturing efficiency cost improvement must exceed the sum of the incumbent supplier’s required unit profit *plus* the new supplier’s required unit profit. Anything short of this will not present a solution as the licensed new supplier’s product would, in fact, be more expensive than the original incumbent’s product and hence not salable (rendering a licensing agreement moot). A second problem is that the incumbent supplier may correctly calculate the cost of profit foregone as larger than the apparent difference between product price and product cost by taking into account other costs such as reduced economies of scale and learning, effects on cross-subsidization among the suppliers products (for example, in the printer industry, low printer margins are offset by high cartridge margins), reduced marketing and sales effects that are driven by market share, and increased costs in terms of supporting licensees (for example, restricted ability to unilaterally

make system changes that involve security protocols). Importantly, even if a licensing arrangement is feasible, the full cost of lock-in is still borne, now by the customer and the new supplier jointly, and continues to accrue as profit to the incumbent supplier.

In some cases, security protocols are not secret at all but are openly available (e.g., based on an open standard like the Data Encryption Standard or Advanced Encryption Standard [Burr]) or licensing is available at a sufficiently low cost. Lock-in may still occur, though, if successful interaction across the interface requires information (e.g., a cryptographic key) that is only available with the permission of another party, such as a competing vendor. In this case, although the protocol has been implemented, successful interoperation without permission of a hostile party may be equivalent to the problem of breaking a cryptographically strong system. A well designed cryptographic algorithm can be quite secure against such attacks making it economically infeasible to interoperate.

Security also has the potential to play an enhanced role in lock-in by virtue of the perceived value of system secrecy. Suppliers may explicitly or more discretely claim that their proprietary system is more secure than, say, a potential or actually openly available alternative, since the supplier can control access to information about the system itself. This has the virtue of appealing to a common sense proposition that for a system of a given security level, reduced knowledge about the system will not help and could reasonably be expected to hinder an attacker (at a minimum, by increasing the cost of attack by the amount required to learn about the system). Notwithstanding the potential effectiveness of this position in sales calls, it is one of the most controversial points of philosophy in security system design, designated by its critics as “security by obscurity.”

The case against security by obscurity derives from original design principles of Auguste Kerchoffs, a 19<sup>th</sup> century French military cryptographer who maintained that good security system design means relying only on the secrecy of the key and the strength of the algorithm and not the fact that the algorithm itself is secret [Kerchoffs]. From the military cryptography perspective, this reasonably accounts for the likelihood that security devices will eventually fall into enemy hands (either by capture or treason). Interestingly, this eventuality also arises in the case of current commercial information technology security: a temporary worker at a document processing firm published the details of DirecTV’s security system on the web after seeing them as part of DirecTV’s litigation with its security supplier [AP]. But, more recent arguments against security by obscurity tend to rest on two related points: (1) security inventors who rely on secrecy tend to over rely on it, making mistakes in security implementation that are later

discovered by attackers, often resulting in catastrophic security failure and (2) there is a large community of peer experts who are willing to review security protocols if made public and who are likely to uncover critical flaws prior to use of a system (and perhaps even recommend appropriate fixes) [Schneier].

The arguments for and against the beneficial role of system secrecy in security do not appear to be resolvable in any universal fashion. The debate has been sharpened recently by discussions of the relative security of open source and closed source software development. While many treatments take a position of orthodoxy (almost everyone cites Kerchoffs) or speak to the experience of the community, treatments that attempt to delve deeper into whether obscurity never helps or whether open peer review is always superior (or even usually superior) tend to come up ambivalent [Anderson02, Lipner, Neumann, Schneider]. The lack of a simple and compelling argument that “proves” Kerchoffs means that we can expect “security by obscurity” to continue to play a role in security induced lock-in.

## 1.2. *Implications of Lock-In*

The economic theory of lock-in has been playing an increasing role in economic, business, and policy thought, particularly since the 1980's. The key impetus for this interest comes from explicit consideration of increasing returns to scale, in which each increment of economic activity is increased in value by the amount that has already occurred, resulting in the potential of positive feedback. Much traditional economics relies on diminishing marginal returns to scale, resulting in negative feedback, and reasonably associated with limited resources; as production increases, the price of inputs ultimately is bid up, resulting inevitably in declining marginal returns. But two phenomena particularly important in the information age have the potential to show unbounded increasing returns: information or knowledge itself and network effects in which the value of access to a product increases with the number of other users of that product.

Modeling of economic processes with positive feedback deviates from traditional analysis of declining marginal returns; in particular, the usual and powerful proofs that market based systems converge to unique and globally optimal equilibrium no longer apply. It is conceivable, in the presence of positive feedback, that more than one stable equilibrium may exist, and that an economic system will tend to get locked-in to only one of them, not necessarily the globally optimal one [Arthur].

While the theoretical possibility of such lock-in is not contestable, the empirical evidence and the practical importance of lock-in is. Liebowitz and Margolis, for example, question first whether popular examples of lock-in actually demonstrate a non-trivial penalty

between the locked-in state and a feasible alternative state, and secondly whether the effect is in fact important if there is a tendency for switching costs to ultimately be overcome regardless, typically by technological upheaval, leading to a more benign process of serial lock-in [Liebowitz]. Their critique is a strong argument for the necessity of careful collection and analysis of data to support the potential theoretical consequences of lock-in.

Beyond the need for empirical evidence of lock-in and its significant and detrimental effects, we also need to consider the possibility that customers and suppliers correctly anticipate the effect of lock-in and negotiate offsetting compensation [Shapiro]. This seems particularly feasible when customers are concentrated and so can more easily internalize the effects of decisions across the customer set (importantly, internalizing network externalities). A customer and a supplier, anticipating the cost of lock-in before it has occurred might simply negotiate a compensating up front discount that is sufficient to compensate for the lock-in. Of course, they may be wrong (in either direction) as to the cost of lock-in, but this is equivalent to the normal uncertainty in negotiating current contracts intended to cover future eventualities.

An effect that may be substantially more difficult to correctly anticipate, though, and one that has been less examined in the literature in spite of its importance to the premise of serial lock-in (but see [Redding]), is the impact of lock-in on access to innovation. A locked-in customer will not access the potential benefit of an innovation that is not compatible with its supplier's product unless that benefit exceeds the necessary switching costs. This occurs whether the innovation is a direct product innovation or one that arises in complementary products.

Does lock-in, or more generally, a lack of competition retard innovation? The oldest hypothesis here is the neo-Schumpeterian thesis that innovation is optimal in firms with monopoly power. However, empirical work over the last several decades suggests that monopoly power is not strongly beneficial to innovation, that a mixture of competition and limited monopoly power maximizes innovation, and that both larger firms and smaller firms have innovative strengths [Kamien, Scherer]. We would not want, then, that security lock-in is so strong as to result in an effective monopoly; although a locked-in customer can reasonably expect some important types of innovation to be executed by its supplier, there is also a high likelihood that other potentially interesting innovations will not, so that the cost of denied access to innovation via lock-in could be substantial up to the point that such costs exceed the switching costs. Even harder to gauge but, again, potentially quite significant, is the possibility that useful innovations will never be pursued at all because of the perceived

low likelihood of exceeding substantial switching costs in the customer base.

## 2. Economic Lock-In and the U.S. Cable Industry

The U S cable industry’s purchase of set-top boxes represents a particularly rich example of security based lock-in.

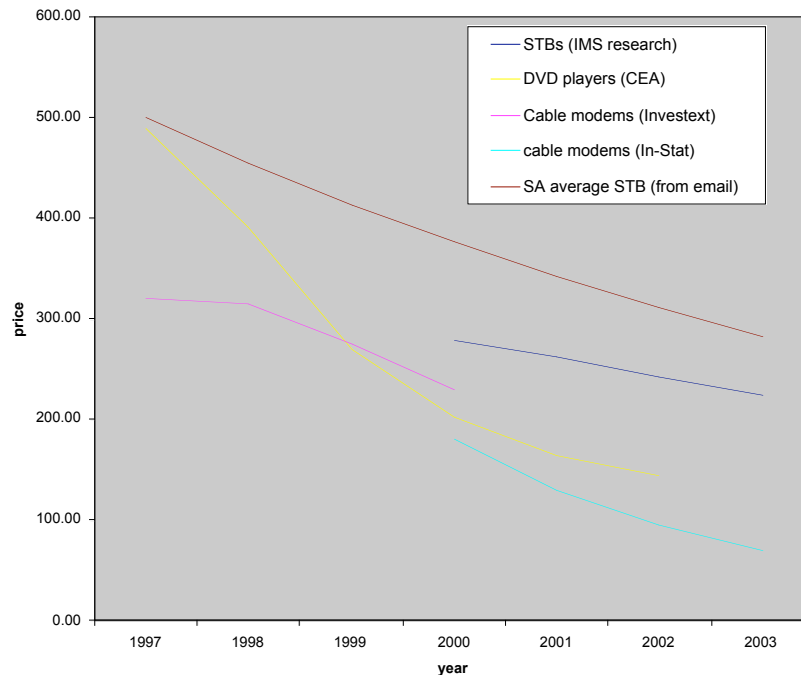
The U. S. cable industry purchases set-top boxes and uses them to provide its subscribers with access to programming. Over the last decade, the industry has increasingly been deploying digitally based set-top boxes to replace analog ones. The cable operators buy their set-top boxes almost exclusively from two suppliers, Motorola (which purchased the former General Instrument) and Scientific Atlanta. Each supplier maintains a proprietary conditional access (rights management) system and the programming provided in each cable operators’ cities is compatible with the conditional access system of one or the other supplier. Interestingly, the case can be considered as a proprietary extension of an open standard, since the underlying scrambling is the openly available triple-

non-compatible alternative would include replacing all currently deployed set-top boxes in that city plus a substantial portion of the network equipment that processes programming (typically called “head end” equipment).

An alternative set-top box vendor attempting to create a compatible set-top box without the agreement of the incumbent set-top box supplier is confronted with the expected barriers: the overall security protocol is not known; even if it is known, using a secure stream requires access to cryptographic information (keys) controlled by the incumbent supplier, the incumbent suppliers hold patents covering the security technology, and intentionally breaking the security system would likely be prosecutable as a violation of the Digital Millennium Copyright Act [DMCA]. Thus, even if an MSO customer were interested in enabling another supplier for price or innovation purposes, security technology makes the incumbent set-top box vendor’s lock-in potent.

In this case, the customers exhibit substantial market power: a handful of large MSOs control most of the cable systems in the United States and represent a substantial fraction of sales for their suppliers.<sup>2</sup> Consequently, we would expect the MSOs to be

price comparison



DES standard [NIST], but the mechanism for managing and distributing the necessary keys to each set-top box is proprietary to each vendor. Consequently, the cable operators (called multiple system operators or MSOs) are locked-in in each city to one of the two suppliers; the switching cost for a

sophisticated about the potential for lock-in and to

<sup>2</sup> For example, Scientific Atlanta’s top three customers, all MSOs, have accounted for well over half of its total sales in each of the fiscal years 2000, 2001, and 2002 [Scientific Atlanta].

negotiate some compensation at the beginning of each major lock-in cycle. Indeed, one of the most celebrated deals in the cable industry represents a creative way to extract just such compensation. In 1997, John Malone, then CEO of the largest MSO, TCI, led a buying consortium to commit to the purchase of 15 million set-top boxes from General Instrument (GI) (10 million for TCI) at a cost of \$300 each. Committing to a large multi-year purchase at an attractive price is consistent with effort to reflect the cost of a lock-in cycle in an up front discount. But, the compensation was more sophisticated than a simple discount. In the deal, TCI (and the other MSOs) also received warrants to purchase shares of GI at a price set before the deal was announced, totaling 16% of the shares of GI, with warrants vesting as set-top boxes were purchased. And Liberty Media (controlled by Malone) received a further 10% of GI in return for ownership of a digital television transmission service. The deal had a substantial affect on GI's perceived market position – "in a single day, GI looked like the new dominant manufacturer of set-top boxes" [Robichaux, p. 221] – but through their equity positions in GI, TCI and the other cable operators were able to re-capture a portion of the present value of profit transferred to GI via lock-in. TCI and Liberty Media in particular had acquired rights to more than 20% of GI through the deal.

A second manner in which MSO customers can manage lock-in is by causing the two vendors to compete for new cities that are as yet uncommitted. Not only can an MSO use negotiation for purchases for the new city as the beginning of a new lock-in cycle for which it can hope to recover some of the cost of lock-in through discounts or other concessions, but the likelihood of important future competitions can be used to discipline the supplier to a degree in cities in which the MSO is already locked-in. However, although the dual vendor competition may provide important advantages relative to lock-in by a monopoly supplier, the structure represents a tradeoff between the cost to an MSO customer of working with multiple suppliers and the limits to competitive pricing and innovation possible in a duopoly.

The particular role of security in lock-in of set-top boxes is fairly easy to trace by examining both standardization of technology components and regulatory action. Although both General Instrument's and Scientific Atlanta's first digital set-top box offerings included a number of proprietary technologies, components other than security have migrated to industry standards and third party technologies, including video format (now MPEG-2, an open standard), audio format (now Dolby AC-3, licensed from a neutral third party), modulation (now follows the International Telecommunication Union's J.83 standard), signaling (currently migrating to an IP system based on the DOCSIS standard) and so on.

Security maintains its position in both vendors' products as proprietary.<sup>3</sup>

The special role of security can also be seen in the partitioning specified by the FCC in its effort to enable retail distribution of set-top boxes. The FCC has mandated that technology that is uniquely required to enable the functions of a set-top box (that is, beyond openly available standards or technology licensable from third parties that could be implemented, for example, by a television manufacturer or other consumer electronics manufacturer not currently supplying the cable market) be captured in a "point of deployment" module separately available from an MSO, and that this technology be limited to security,<sup>4</sup> with implementation by the beginning of 2005. The FCC's point-of-deployment module ruling could have an important impact on the consequences of lock-in albeit without eliminating the lock-in itself. Since the price of the module is not regulated, the original manufacturer can continue to extract profit due to the lock-in of an MSO in a particular city. However, the consequences of lock-in on innovation can be weakened since the remainder of the set-top box functionality (anything that doesn't interact with security) can be competitively innovated and manufactured by a number of different suppliers.

Evidence that lock-in of set-top boxes (via security as argued in the previous paragraph) has had effect on pricing can be seen by comparing prices for cable set-top boxes with those of Digital Versatile Disk (DVD) and Cable Modems. The latter two devices contain between them essentially all the components that would be found in a cable set-top box with the exception of security. Yet, as shown in Figure 1, both have been experiencing substantially faster rates of decline (25% a year over the last several years) compared to set-top boxes (10% a year or less during a period in which the vast majority of set-top boxes sold continued to be "basic" in function).<sup>5</sup>

---

<sup>3</sup> A position recently confirmed at the Consumer Communications and Networking Conference, Las Vegas, January 2004, where a Motorola (purchaser of General Instrument) representative on a panel stated that security will uniquely continue as a proprietary technology, albeit subject to some cross-licensing by different security technology providers.

<sup>4</sup> In Section 47 of Implementation of Section 304 of the Telecommunications Act of 1996, Commercial Availability of Navigation Devices, Order on Reconsideration, CS Docket No. 97-80, May 13, 1999, the FCC states "We clarify that Section 76.1204(a) regarding the components of the security module allows for inclusion of circuitry used for conditional access functions. We agree with Circuit City that, were the security modules to contain features and functions not related to security, commercial availability of navigation devices could be impaired." [FCC]

<sup>5</sup> Indeed, in a rare public disclosure of pricing, Motorola notes in its 2002 annual report that set-top box average selling price declined by 4% in the preceding year.

The effect of lock-in on innovation is less easily observed than pricing, beyond industry anecdotal and trade press discussions of MSO frustration at the relative rate of innovation in the direct broadcast satellite industry, the consumer electronics industry overall, and the cable industry. However, a glimpse of frustration is occasionally available in public announcements.<sup>6</sup>

### 3. Selective Encryption

Since conditional access systems represent an effective source of lock-in in the cable industry, we are interested in proposals to reduce lock-in. A proposal to provide an alternative security system that entails deployment of new, incompatible set-top boxes and removal of existing set-top boxes does not reduce lock-in (although if sufficiently compelling, such a proposal would motivate a MSO to pay the necessary switching costs – but we see no evidence of such a proposal). Selective encryption, proposed by Sony in the form of its Passage system [Baumgartner] represents an approach that explicitly lowers switching costs. Sony’s proposal is based on a technique known as selective encryption.

Selective encryption is the application of encryption to a subset of a bitstream with the expectation that the entire bitstream will be rendered useless to anyone who cannot decrypt that subset. Selective encryption may not be particularly effective if the subset is small and it’s relatively easy to guess or ignore elements in the subset. For instance, obscuring every fifth letter of an English sentence does not make it particularly hard to read. Selective encryption is effective, on the other hand, if

- it’s hard to use the message with the missing subset obscured,
- it’s hard to attack the encryption applied to the subset.

Compression of otherwise redundant source material makes a substantial difference in the effectiveness of selective encryption, first by reducing the predictability in the source material (a property Shannon first recognized in layered encryption [Shannon]) and second by organizing the bitstream in such a manner that obscuring some bits can have a profound affect on the usability of the rest of the stream. This second is not an inevitable factor of compression algorithms but is far from unusual. Selective encryption has been proposed in a number of specific applications but rarely with a thorough security motivated analysis. Selective encryption can

- reduce computational complexity of the overall system by only applying encryption to a subset of the material, with positive affects on silicon area and cost, battery life, etc.
- create an opportunity to efficiently add multiple different encryption systems to the same bitstream by only encrypting a fraction of the data under each encryption system, while sending the remaining information in the clear (the focus of the Sony Passage application)
- permit different ways to organize data; for example caching large amounts of in the clear data close to users while providing the remaining necessary portions from a distant but more secure site at the time of use.
- provide a method for efficiently making a low quality version of a bitstream that can be viewed by all while the full quality version is reserved for those who pay (a variation on the selective encryption strategy in which the encrypted data is not that required to view even a poor reproduction, but rather the additional data required to view a good reproduction).

But, to see widespread success in these applications, selective encryption cannot be deemed to be secure on the basis of the failure of a particular unauthorized decoder (or indeed a large class of decoders) to produce a useful reproduction. Rather, a convincing security analysis must be presented, plausibly considering all the strategies available to an intelligent and resourceful attacker intent on breaking the system. This important concept is introduced in [Lookabaugh].

### 4. Selective Encryption of MPEG-2 Video

The MPEG-2 standard defines video compression, audio compression, and multiplexing and timing issues. It is widely used in the delivery of entertainment of various types, including cable television, satellite television, DVD, and HDTV. MPEG-2 contains elements that concentrate important information necessary for successful decompression of the bitstream but which do not consume substantial bandwidth, making MPEG-2 a candidate for selective encryption.

Relative to the criteria we defined in Section 2.1, in this work we are interested in:

*Security Criterion* – we are primarily interested in “degraded” rather than “secret” content; in other words, we are more interested in digital rights management applications than in interpersonal communication privacy.

*Security Validation* – we adopt a cryptanalytic approach to validating security.

<sup>6</sup> For example, John Malone, frustrated at the availability of advanced set-top boxes from General Instrument, made a colorful public joke at GI’s expense before a large crowd at a Cable industry trade show in 1996 ([Robichaux], p. 171).

*Complexity* – since layered encryption is a straightforward and widely adopted alternative, we are interested in a substantial savings in order to motivate selective encryption. In particular, we are interested in systems which require under 10% of the material be encrypted. This is ambitious, but note again that we are pursuing degraded rather than secret content.

*Compression Efficiency* – although we could see a small reduction in compression efficiency as a reasonable compromise, we are interested in system contexts in which bandwidth is at a premium (hence motivating a relatively complex but high performance compression algorithm like MPEG-2 in the first place). So our primary interest is systems which do not impact compression efficiency.

*Algorithmic Constraints* – we restrict ourselves to unmodified non-scalable MPEG-2 video compression.

We have applied this approach to the selective encryption of MPEG-2 video in [Lookabaugh]. Some of the key points we report there include:

(1) Typical high performance MPEG-2 encoded bit streams only use a small portion of bits (around 1%) in important headers (video sequence, group of pictures, picture, and slice). It can be simple to obscure such headers because of a usual practice in encoding of aligning these headers and the multiplex (transport) level at which encryption is performed.

(2) However, fields in such headers can be quite vulnerable to attack, even if obscured by selective encryption, for a variety of reasons: the fields are often static, they can be guessed from external information that is probably available to an attacker, they can be guessed from other information in the bit stream (e.g., picture type can be guessed from picture size, an example of the cryptanalytic technique of “traffic analysis”), or they can be ignored, albeit with non-trivial consequences to decoded image quality. We evaluate each of these fields and propose and test attacks. For example, we showed that a perceptual attack on the *quantizer\_scale\_code* syntactic element is feasible albeit with non-trivial picture degradation. Conversely, a deeper parsing of the MPEG-2 bitstream allows us to inflict substantial damage on an attacker’s reconstruction if we encrypt about 20% of macroblock\_type bits (less than 1% of total bits).

(3) Consequently, the effectiveness of MPEG-2 video selective encryption when high performance (in terms of only needing to encrypt a very small portion of the bitstream) is targeted is quite dependent on how a compressor is operated.

(4) We distinguish between three ways to operate a compressor: “cooperative,” “neutral,” and “antagonistic.” A cooperative compressor is one which performs compression in a manner likely to enhance the security of a selective encryption scheme, by, for example, concentrating important information (so that only a small fraction of bits need be encrypted) and insuring that this important

information itself is hard to guess from outside factors and is not static. A neutral compressor does not make any particular effort to compress in a way to enhance selective encryption (for example, it may be optimized for compression alone), and an antagonistic compressor compresses in a manner intended to make it unrewarding to apply selective encryption (e.g., by attempting to make selective encryption ineffectual unless nearly all of the bits are encrypted). A cooperative encoder can, in fact, make even aggressive selective encryption secure. An antagonistic encoder can render aggressive selective encryption quite insecure.

In the case of MPEG-2 video, an antagonistic encoder can render header encryption above the macroblock header largely ineffectual by making limited or externally predictable choices with respect to header fields. This would permit an attacker to circumvent a selective encryption system. For the cable industry, the concern would be that an incumbent vendor who also provides software that controls compression might be motivated to facilitate an attack by a third party on a competitor’s selective encryption system. The MSO customer would be wise to take measures to prevent this if it wishes to take advantage of the potential reduction in lock-in afforded by selective encryption.



Figure3. Movie frame showing effect of perceptual attack on encrypted *quantizer\_scale\_code* (fixed at 5 in the reconstruction) (top) and sports frame showing effect of 20% encryption of *macroblock\_type* (bottom).

## 5. Conclusion

Security technology can play a special role in economic lock-in and has done so in the case of the purchase of cable set-top boxes by cable MSO's. The resulting switching costs are visible in the form of set-top box prices and access to innovation. This is not to say that lock-in is intrinsically evil; it is a characteristic of many markets and it may well be the best choice for a customer to accept lock-in in return for access to a particular technology or market solution. This is particularly true if the customer is able to extract most of the future cost of lock-in through up front concessions from the vendor at the time of lock-in or if the customer can secure a form of bilateral lock-in in which the vendor simultaneously acquires significant switching costs if it tries to develop an equivalent revenue stream from some other customer. Arguably, both these factors are present in the case of cable MSO's and their set-top box providers. However, the particular tactic of trading up front concessions against the cost of future lock-in requires a degree of prescience that may be too much to ask in a market changing as quickly as cable. All players and analysts of the cable market can be served by careful consideration of and active management of lock-in.

Sony's Passage system proposal represents an ingenious effort to use selective encryption to weaken the affect of security based lock-in in the cable market. The system allows continued use of an installed base of incumbent vendor set-top boxes while overlaying a new vendor's boxes at a small incremental cost in bandwidth (to transmit the reduced portion of the bitstream that is still encrypted under each of the incumbent and new vendor's conditional access schemes). At the same time this appears as a potentially viable tactic for MSO's to use to reduce lock-in (and consequently capture more of the share of profit in the value chain at the MSO level rather than at the set-top box vendor level), it also requires particular care when considering the relative role of an incumbent vendor's compression system operation relative to a new vendor's selective encryption scheme.

## 6. References

[Anderson02] Anderson, R., Security in Open versus Closed Systems - The Dance of Boltzmann, Coase, and Moore. in Open Source Software: Economics, Law and Policy, (Toulouse, France, 2002).  
[AP] Student pleads guilty in DirecTV data case Associated Press, 2003.  
[Arthur] Arthur, W.B. Increasing Returns and Path Dependence in the Economy. The

University of Michigan Press, Ann Arbor, MI, 1994.  
[Burr] Burr, William E., "Selecting the Advanced Encryption Standard," IEEE Security & Privacy Magazine, vol. 1, issue 2, Mar-Apr 2003, pp. 43-52  
[DMCA] See <http://www.eff.org/IP/DMCA>  
[FCC] Commercial Availability of Navigation Devices, Order On Reconsideration, Section 304 of the Telecommunications Act of 1996, CS Docket No. 97-80, May 13, 1999.  
[Kamien] Kamien, M. and Schwartz, N. Market Structure and Innovation. Cambridge University Press, Cambridge, UK, 1982.  
[Kerchoffs] Kerchoffs, A. La cryptographie militaire. Journal des sciences militaires, IX. 5-38.  
[Lookabaugh] T. Lookabaugh, D.C. Sicker, D.M. Keaton, Y.G. Wang, and I. Vedula, "Security Analysis of Selectively Encrypted MPEG-2 Streams," in *Multimedia Systems and Applications VI*, Proceedings of the SPIE, vol. 5241, Orlando, FL, 8-9 September 2003.  
[Liebowitz] Liebowitz, S.J. and Margolis, S.E. Winners, Losers & Microsoft. The Independent Institute, Oakland, CA, 1999.  
[Lipner] Lipner, S.B., Security and source code access: issues and realities. in IEEE Symposium on Security and Privacy, (Oakland, CA, 2000).  
[Neumann] Neumann, P.G., Robust Nonproprietary Software. in IEEE Symposium on Security and Privacy, (Oakland, CA, 2000).  
[NIST] Federal Information Processing Standard 46-3, Data Encryption Standard, US Nat'l Inst. Standards and Technology, 1999, <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>.  
[Nowell] Nowell, P. Small firm irks printer giant; cartridges at center of legal tussle The Seattle Times, Seattle, WA, 2003.  
[Baumgartner] Baumgartner, J. Deciphering the CA Conundrum Communications Engineering and Design, March, 2003.  
[Redding] Redding, S. Path Dependence, Endogenous Innovation, and Growth. International Economic Review, 43 (4). 1215-1248.  
[Robichaux] Mark Robichaux, Cable Cowboy: John Malone and the Rise of the Modern Cable Business, Hoboken, NJ: John Wiley & Sons, 2002.  
[Scherer] Scherer, F. Changing perspectives on the firm size problem. in Acs, Z. and Audretsch, D. eds. Innovation and Technological Change: An International

- Comparison, The University of Michigan Press, Ann Arbor, MI, 1991, 24-38.
- [Schneider] Schneider, F.B., Open source in security: visiting the bizarre. in IEEE Symposium on Security and Privacy, (Oakland, CA, 2000).
- [Schneier] Schneier, B. Open Source and Security Crypto-Gram Newsletter, 1999.
- [Scientific Atlanta] Scientific Atlanta, Form 10-K for Fiscal Year Ended June 27, 2003, filed with U.S. Securities and Exchange Commission, September 23, 2003, available at <http://www.sec.gov/Archives/edgar/data/87777/000119312503052976/d10k.htm>.
- [Shannon] Shannon, C.E. Communication Theory of Secrecy Systems. Bell System Technical Journal.
- [Shapiro] Shapiro, C. and Varian, H. Information Rules: A Strategic Guide to the Network Economy. Harvard Business School Press, Boston, MA, 1998.