

DOW, LOHNES & ALBERTSON, PLLC  
ATTORNEYS AT LAW

JAMES M. BURGER  
DIRECT DIAL 202-776-2300  
jburger@dowlohnesh.com

WASHINGTON, D.C.  
1200 NEW HAMPSHIRE AVENUE, N.W. · SUITE 800 · WASHINGTON, D.C. 20036-6802  
TELEPHONE 202-776-2000 · FACSIMILE 202-776-4300  
www.dowlohnesh.com

ONE RAVINIA DRIVE · SUITE 1600  
ATLANTA, GEORGIA 30346-2108  
TELEPHONE 770-901-8800  
FACSIMILE 770-901-8874

June 22, 2004

Susan Mort, Esquire  
Attorney Advisor  
Media Bureau  
Federal Communications Commission  
445 12<sup>th</sup> Street, S.W.  
Washington, DC 20554

Re: **TiVoGuard Digital Output Protection Technology  
MB Docket No. 04-63**

Dear Ms. Mort:

The attached White Paper explains how TiVoGuard transports and protects Marked Content. It was prepared by TiVo's technical staff in an effort to help the Commission better understand the transport method employed by its digital output protection technology to transmit Marked Content securely between TiVo devices in a secure viewing group. In addition, the White Paper addresses the technical aspects of constraining Marked Content to some artificially defined "local environment" using standard internetworking protocols (TCP/IP).

The enclosed White Paper describes some methods that could be used in an effort to constrain content to a "home network." Nevertheless, TiVo does not concede that the Commission should alter its initial decision to permit secure, limited redistribution of Marked Content. As detailed in the White Paper, TiVo's system relies on proven authentication and encryption methods to ensure that content flows in a usable form only between a very few devices registered with TiVo under one customer's credit card. Moreover, any method that relies on TCP/IP to restrain content is either inherently insecure or will frustrate consumers' use and enjoyment of DTV.

The Motion Picture Association of America (MPAA) and its members were the sole objectors to TiVo's restricted ability to transfer Marked Content over the Internet. As noted in TiVo's Reply, the MPAA's demand for a distance-limitation on retransmission contradicts the Commission's goals set forth in this proceeding.<sup>1</sup> Moreover, since the MPAA could not claim that TiVo's limited content transmission system would result in unrestricted mass redistribution of Marked Content, it relied on a series of unspecific and unsupported claims that, at best, are outside the scope of this proceeding.<sup>2</sup>

---

<sup>1</sup> See Reply of TiVo Inc. in MB Docket No. 04-63 (filed April 16, 2004) ("TiVo Reply") at 19-24.

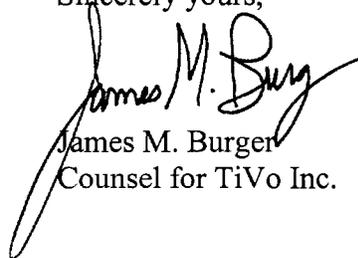
<sup>2</sup> *Id.*

Susan Mort, Esquire  
June 22, 2004  
Page 2

TiVo supports DTV transition and desires to have a leading role in promoting DTV on its DVRs. TiVo believes that secure distribution of digital broadcast content over the Internet is in the public interest and will benefit consumers. If, however, the Commission decides to reverse its policy determination not to “foreclose use of the Internet to send digital broadcast content where it can be adequately protected from indiscriminate redistribution,”<sup>3</sup> TiVo would be willing to restrict access to Marked Content by TiVo devices on the same subnet.<sup>4</sup>

Please do not hesitate to contact the undersigned if you have any further questions regarding TiVo transport and protections systems.

Sincerely yours,



James M. Burger  
Counsel for TiVo Inc.

cc (by mail or facsimile):

Richard Chessen  
Alan Stillwell  
William Johnson  
Alison Greenwald  
Jeffrey Neumann  
Michael Lance  
Steven Broeckaert  
John J. Gabrysch

---

<sup>3</sup> *Digital Broadcast Content Protection, Final Rule*, MB Docket No. 02-230, 68 Fed. Reg. 67599 (released December 3, 2003).

<sup>4</sup> See attached White Paper at note 6. Home networks normally consist of a single subnet.

**TiVo Inc.**

**How TiVoGuard Transports and Protects Content**

TiVo Inc.  
2160 Gold Street  
Alviso, CA 95002-2160

June 22, 2004

# How TiVoGuard Transports and Protects Content

Networking technology and the Internet were designed to be as open as possible. TiVo uses TCP/IP, the networking standard used by most home networks and the Internet. TCP/IP is well-known, well-documented, and easy to manipulate. In order to make networks safe for protected content (and the Internet safe for financial transactions) it was necessary to create methods of rendering data useless to anyone but the intended recipient. Because open standards such as TCP/IP are employed worldwide, the data must be self-protecting. Two mechanisms work in tandem to prevent unauthorized use of data: authentication and encryption.

Authentication ensures that the recipient of the data is “authentic.” This means two things: first, the recipient’s identity has been verified; and second, the recipient is authorized to receive and use the data. TiVoToGo uses authentication to ensure that content is never transmitted to an unauthorized device.

Encryption scrambles data, encoding it in such a way that only someone in possession of a unique key can decode it. Encryption is a mathematical process based on very large numbers (often over 100 binary digits). There are a number of well-tested encryption methods that cannot reliably be broken by foreseeable computer technology. TiVoToGo uses such methods to protect all content from unauthorized access.

Authentication and encryption are the foundation for security on the Internet (where they keep credit card numbers safe) as well as for the secure transmission of corporate, government and military information on both public and private networks. The following sections provide an overview of data transfer over networks using TCP/IP, a discussion of how TiVo uses authentication and encryption, and an explanation of why TCP/IP itself does not secure data—why authentication and encryption must be used instead.

## ***I. Transfer of Protected Content Using TCP/IP***

On a home network, digital information travels using what is called “TCP/IP” (Transmission Control Protocol/Internet Protocol).<sup>1</sup> If no security measures are taken, this content can be made freely available to any capable device within the home or on the Internet at large. This is the foundation of the World Wide Web—the ease with which information can be distributed has sparked the huge growth of the Internet itself.

TiVo uses TCP/IP to transfer video between TiVo® DVRs and to personal computers (PCs) using TiVoToGo. Certain content, especially copyrighted material such

---

<sup>1</sup> TCP/IP is an industry-standard suite of protocols designed for large-scale internetworks, such as the Internet, that span local area networks and wide area networks. In effect, it is a language commonly understood by all devices on the network and by programmers writing networking applications. The language’s “dictionary” is freely available with thousands of “grammar” books and articles explaining the most intricate details of how to use the language.

as video content covered by the Digital Broadcast Protection Rules (“Rules”), should be protected to prevent its arbitrary distribution without hampering the ability of an authorized person to use the material. This requires security measures that protect the content itself; such content must be protected from widespread unauthorized redistribution by rendering it unintelligible to unauthorized devices. The open nature of TCP/IP makes it difficult to physically restrict content from flowing between devices connected to the Internet unless the device is connected to a local network not connected to the Internet.<sup>2</sup> Fortunately, good authentication and encryption techniques can ensure that only authorized devices are able to receive the content in a usable form.

Before discussing methods to protect data on a network, it is necessary to present a brief explanation of how TCP/IP works.

## **A. How TCP/IP Works**

TCP/IP determines how data transmission occurs across both local networks (such as wired or wireless home networks) and the Internet. An important function of the design of TCP/IP is to facilitate traffic on busy networks without creating unnecessary delays. Networks generally consist of computers and other devices connected by wires (or wirelessly). The data that flows across networks is broken up into manageable pieces called “packets.” Breaking the data up in this way reduces traffic jams, because packets sent by one computer can travel interspersed with packets from other machines. The packets are reassembled once they reach their destinations.

Each device connected to the network has an address called the “IP address” to identify it as a source or destination for data packets. Each packet includes information called the “packet header.” The packet header contains the IP addresses of the packet’s origin and intended destination, along with other information.

When a computer sends data across a network – whether within a single building or across the country – it rarely travels directly over a single cable to the destination machine. In most cases, the network consists of large numbers of wires connected to devices called “routers.” A router’s job is to direct packets to the correct destinations, using the information in their headers.

## **B. Protecting Data During Transmission over TCP/IP**

Because TCP/IP is an open standard, and because every router or computer in a network is able to change information in the packet headers, it is impossible to guarantee that individual packets travel only to their intended recipients. Packets cannot be secured or protected. The only way to safeguard against the use of private data by unauthorized individuals is to protect the data itself. TiVoToGo accomplishes this by encrypting the data, authenticating the intended user of the data, and limiting the number of authorized devices. These three techniques make up the TiVo secure viewing group discussed in the following section.

---

<sup>2</sup> Most, if not all, home networks are connected to the Internet.

## **II. Why the Secure Viewing Group is Secure**

TiVo restricts the distribution of proprietary content to a specific group of TiVo devices—DVRs or PCs—called a secure viewing group. All TiVo devices in a secure viewing group must be associated with the same TiVo service account, which must be billed to a single credit card. A TiVo device can transmit content only to other devices in the same secure viewing group and can never transmit content to any device outside the secure viewing group. Generally, there is a maximum of ten devices in any such group. A given TiVo device can only belong to a single secure viewing group.

Each device in the secure viewing group uses TiVoGuard to protect the content from unauthorized distribution. To keep the content within the secure viewing group, TiVoGuard uses both authentication and encryption when transmitting content.

### **A. Authentication**

Before a TiVo device transmits encrypted content, it must establish that the intended recipient device is authorized to receive the transmission. The sending device must be sure of the recipient device's identity, and that the recipient device is authorized to receive the content. Authentication consists of both identification and authorization. Only after authentication can the content be transmitted.

#### **Identification**

Before transmitting any content, a TiVo device must identify the recipient device and determine whether it is in the same secure viewing group. If the device is not recognized, or is not in the same secure viewing group, or is not authorized to receive content, then the sending device does not transmit the content to the recipient device.

#### **Authorization**

The TiVo service<sup>3</sup> keeps a record of which devices are authorized to transmit and receive content, and the secure viewing groups to which they belong. As TiVo devices periodically contact the TiVo service, they receive updated information about the devices in their own secure viewing group. Before transmitting content to another device, a TiVo device checks to make sure the receiving device is in the same secure viewing group and is allowed to receive content.

If a TiVo device does not contact the TiVo service, the information about other devices in the sharing group expires. A TiVo device that fails to regularly contact the service loses the ability to transmit content to any other device, because it no longer has the information needed to authorize and transfer content to other devices in its secure viewing group in a usable form (*e.g.*, as discussed below, the other devices' public keys).

---

<sup>3</sup> The TiVo service is the package of services administered by TiVo on central servers described in TiVo's Certification at 3-4.

## **B. Encryption**

All content on TiVo DVRs is encrypted. Encryption scrambles the content to make it unintelligible to any unauthorized device or person. The level of encryption used is strong enough to make unauthorized decryption virtually impossible.

### **How Encryption Works<sup>4</sup>**

Encryption is a way of scrambling data using a “secret code” so that only someone who can decode the data is able to read it. To an unauthorized person (or machine), the encrypted data looks like a meaningless jumble of unrelated junk. When an authorized person decrypts the data, it is restored to its original form so that it can be read easily.

Encryption is a mathematical method of scrambling the data—but if it were only a method, anyone who knew the method could unscramble the data. Because encryption methods are well-known and well-documented, this would defeat encryption as a means of protection. Of course, this is not the case: encryption also requires a number called a “key.” In order to decrypt a message, you must know the method (easy to guess) and the key (nearly impossible to guess).

Encryption keys are very large numbers, usually over one hundred binary digits long. In order to guess an encryption key, you must try each possible number, using the correct decryption method, and see if it works. With such large numbers, this effort becomes astronomically time-consuming. It would require hundreds of years on state-of-the-art computers to guess the keys used in modern encryption methods.

Even more secure encryption uses different keys for encoding and decoding data. The data is encoded using one key and decoded using a completely different key. Knowing the key used to encode the data provides no advantage, because it cannot be used to decode the data. In these methods, the key used to encode the data is often public. This is convenient, because knowing someone’s public key makes it possible to encode a message only that person can read—without compromising the security of the private data.

### **How TiVoGuard Uses Encryption to Protect Stored Content**

The TiVoGuard system uses encryption in specific ways to protect the transmission, storage, and use of content, and to prevent its use by unauthorized devices or persons:

- Every 5- to 15-minute segment of video content is encrypted with a different “clip” key. This means that even if one key were broken, it would prevent the unauthorized user from gaining access to more than a few minutes of content.
- Each TiVoGuard-compliant device (a DVR or PC) has its own “lead” key generated by the software. The clip keys are encrypted with the lead key.
- Each device also has a public key, which is used to encrypt the lead key.

---

<sup>4</sup> For a more detailed description of encryption, see Appendix A at 1-5.

- Any data encrypted with a device’s public key can only be decrypted by that device’s private key, which is stored in a secure microprocessor.

Each device has its own unique lead key, public key and private key. Any content that has been encrypted with a device’s public key can be decrypted only with the device’s private key. This is called “asymmetrical encryption.” The public key cannot be used to decrypt the lead key.

The private key is stored in read-only memory on the device, in a processor called the “cryptographic chip.” The private key cannot be modified, and is only accessible by the cryptographic chip itself. Because the content can only be decrypted using the private key of the device where it resides, the content is securely associated with that device. Moving the content to another device renders it useless. The software does not have direct access to the private key, so it is impossible to discover the private key using any software attack. Any physical tampering with the cryptographic chip results in the destruction of the chip (and the private key).

### **C. Transmission<sup>5</sup>**

Only after the recipient device has been identified and authorized can transmission of the content begin. Similar to protecting stored content, TiVo uses secure encryption to safeguard content during transmission.

#### **Transmitting Content Securely**

When content is transmitted between two TiVo devices, it is encrypted using a temporary key, as follows:

1. The sending device generates a temporary key.
2. The sending device uses its own private key to decrypt the content, and then re-encrypts the content with the temporary key.
3. The sending device encrypts the temporary key with the public key that belongs to the receiving device, and transmits it.
4. The receiving device uses its own private key to decrypt the temporary key.
5. The sending device transmits the encrypted content.
6. The receiving device decrypts the content using the temporary key, and then re-encrypts it with its own lead key and public key.

The content is always encrypted during transmission and then it is stored on a TiVo device. No unencrypted content is ever transmitted or stored.

In the transmission sequence above, the content is encrypted using a temporary key. The temporary key is encrypted using the receiving device’s public key. In this (asymmetrical) encryption scheme, the encrypted data (in this case, the temporary key) can only be decrypted by the private key corresponding to the public key used to encrypt

---

<sup>5</sup> For an illustrated explanation of TiVo’s system of secure transmission see Appendix A at 5-7.

the data. That is, only the device intended to receive the content can actually decrypt it. Thus, in the unlikely event an unauthorized device hijacks the encrypted content, that device cannot display the content or convert the encrypted content into usable video.

### **III. The Open TCP/IP Protocols Will Not Effectively Restrain Content to Artificially Defined “Local Environments”**

The goal of the FCC’s Rules is to prevent the widespread, unauthorized redistribution of DTV Marked Content. In addition, the over-arching FCC goal is to advance the DTV transition. Thus, any system must not interfere with a viewer’s normal and reasonable expectations, *e.g.*, time and space-shifting free over-the-air TV. If public policy required constraining content to a “local environment” such as a home network, on the surface it might seem that a two-pronged approach makes sense—that is, not only the protection of each packet’s contents (by encryption) and restricting the devices that may receive the material in usable form, but by limiting where each packet can travel.

Two pieces of information about each packet may seem to provide a way to do this: TTL, or “time to live,” and RTT, or “round trip time.”<sup>6</sup> However, it is easy to defeat both of these methods of limiting a packet’s freedom to roam, and RTT will most likely also result in consumer dissatisfaction.

#### **A. TTL Relies on Factors that Cannot be Controlled**

TTL is a piece of information, contained in a packet header, that determines how many “hops” a packet is allowed to make. Each time a packet passes through a router or other device, it counts as one hop. Most routers subtract one from the TTL of each packet as it passes through.<sup>7</sup> When the TTL reaches zero, the packet is deleted by the next router it encounters.

Most home networks contain one or a small number of routers that connect all the devices in the house. The Internet, by contrast, contains many thousands of routers. Traveling between any two devices in the home, a packet is likely to make as few as two hops; traversing the Internet, a packet may make many more. Setting the TTL value in the packet header to a small number (*e.g.*, five) may seem like a logical way to prevent a packet from traveling too far from home.

---

<sup>6</sup> A third method, also relying on TCP/IP, would be to restrict delivery of content to devices that only reside on a “subnet.” A subnet is a portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. Commonly, a home network is a single subnet.

<sup>7</sup> TTL was not created for security but to prevent corrupted or misaddressed packets from becoming “Flying Dutchman” packets, *i.e.*, traversing the Internet forever looking for a destination that doesn’t exist, clogging the networks with packets that won’t otherwise die.

## B. Router Vulnerability

Because a router is essentially an open computing device, it is quite easy to modify a router so that it adds to the TTL instead of subtracting from it. A router that added a large number to the TTL of each packet would substantially increase the distance the packets are allowed to travel, thereby defeating the TTL method.

## C. Encapsulation

A packet can be inserted into another packet, in a process known as “encapsulation.” A packet that is thus hidden can travel incognito until it reaches its destination. Encapsulation is a common and legitimate strategy for purposes such as allowing employees to gain access to a private corporate network remotely.

Most corporate networks are “closed”—that is, only on-site devices have access to the network. To give employees remote access to the network, the company installs a VPN (virtual private network) server to exchange data packets with employees who connect via the Internet. Data packets exchanged between a remote employee and the VPN server are encapsulated during transit. When the packets arrive at the company, the VPN server removes the outer packet (thus “de-encapsulating” them). The de-encapsulated packets appear to the network exactly as if they had originated from on-site.

Encapsulation renders a packet immune to the TTL method. When a packet is encapsulated in another, outer packet, it is the outer packet’s TTL value that diminishes as it travels. The inner, encapsulated packet is unaffected by travel through routers.

The end effect is that it would be relatively simple to transmit content across the internet that is only allowed one or two hops by encapsulating it.

## D. RTT Relies on a Time Threshold

RTT is an estimate of the time a packet will take to travel to its destination plus the time it will take for the packet sender to receive an acknowledgement from the recipient—the round trip time between the sender and the recipient and back again. The TCP layer on the sending computer calculates the estimated RTT. Checking the actual travel time against the RTT might seem like a good way to measure the distance between devices in a network.

Under *ideal* conditions, RTT would be a reliable way to measure network proximity. If there were no network delays, and every router were the same, and every wired or wireless connection operated at the same speed, then RTT could be used to calculate the actual distance each packet travels.

In that case, it would be theoretically possible to use RTT to determine whether a given packet originated within a given home network. Any packet whose actual travel time exceeded the expected RTT would be from outside the home network. An RTT-based security method would send a packet to a receiving device, time its actual round trip travel, and compare the result to the anticipated RTT.

In the real world, RTT is an unreliable way to estimate the distance between two devices in a network. There are many factors that influence network performance in the home, dramatically (if temporarily) increasing actual travel time. Large downloads or online game play can affect the speed of a wired network; wireless networks are even more susceptible to delays, and are also vulnerable to interference from common radio frequency sources, such as cordless phones and microwave ovens.

Wireless networks can be extended to cover nearby apartments or houses, without necessarily introducing additional delay. Any RTT-based security method that reliably allowed content to be transmitted within a single home could be used to share content outside the home.

The delay within a home network can be equal to or greater than the time it would take a packet to travel across the United States. A packet traveling between two devices within a home might take long enough that it would appear to have come from outside the home; these packets would be rejected by an RTT-based security method. It would be impossible to reject all packets that travel outside the home without also rejecting a significant number of packets that travel only within the home. This would frustrate consumers' use and enjoyment of DTV.

The nationwide broadband networks are now fast enough that a packet traveling far outside the home might return quickly enough to appear to have remained within the home network. It is not uncommon to see round trip times across the United States as low as 50 milliseconds, which is also a reasonable travel time on a home network. An RTT-based security method would not reject packets that travel very long distances, if they travel quickly enough. Any time threshold that an RTT-based security method used to screen "long-distance" packets is likely to both wrongly reject delayed packets traveling within the home, and wrongly accept packets traveling elsewhere. The result of "false negatives," i.e., stopping an otherwise legitimate Marked Content transfer would result in consumer dissatisfaction with DTV – not a desirable goal.

## **E. RTT Vulnerability**

RTT is calculated by the TCP/IP software (commonly referred to as the TCP/IP "stack") by comparing the time the original packet was sent out and the time the acknowledgement by the recipient device is received back by the TCP/IP stack in the receiving device. That RTT is reported back to the application. It would be trivial to write a piece of code to be simply inserted into the stack to report back a time under the threshold that would otherwise prevent transfer of the content.

## **IV. Conclusion**

It is impossible to reliably use packet header information (i.e., TTL) or round trip time to determine whether packets are traveling only within a given home network. Packet header information such as TTL can be changed by an intermediary device or hidden by encapsulation; and round trip time is subject to network unreliability, variability, and can be falsely reported.

If a packet's origin, travel time, and distance traveled cannot be determined, it is impossible to restrict the transmission of the data packet. The only way to control the distribution of particular data is by protecting the contents of each packet using both authentication and encryption. Attempting to corral packets within a given home network is both futile and unnecessary.

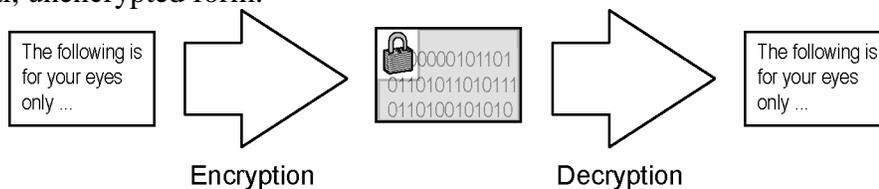
Thus, TiVo's system gives effect to the broadcast flag by limiting content retransmission to a maximum of ten devices tied to a single customer account using proven authentication and encryption methods, and protects the content from mass unrestricted redistribution while promoting DTV transition by offering consumers attractive alternatives for viewing DTV programming.

## Appendix A: How TiVoGuard Uses Cryptography to Transmit Digital Television Content Securely

The following sections provide additional detail about encryption, and how TiVoGuard technology uses encryption to protect DTV content.

### Digital Cryptographic Ciphers

TiVo uses digital cryptographic ciphers to protect secrets and to protect data from unauthorized use. Digital cryptographic ciphers encrypt and decrypt data. The purpose of encrypting data is to protect it by rendering it unintelligible. Encryption accomplishes this by scrambling the data according to a set of rules (an “algorithm”). In its encrypted form, the data is protected because it cannot be understood. Decryption is the reverse process: it starts with encrypted data and applies an algorithm to return the data to its original, unencrypted form.



### Cryptographic Algorithms and Keys

Digital cryptographic ciphers commonly employ an algorithm that requires a “key.” An algorithm of this kind requires two inputs – the data to be encrypted or decrypted, and a key that determines how the algorithm will change the data.

For example, one simple algorithm for encrypting English is: “For each letter from A to Z, replace it with the letter that is N positions to its right in the alphabet. When you get to the end of the alphabet, wrap back to the beginning.” The output of this algorithm will change depending on the value of N. If N equals 5, the word “big” becomes “gnl”; if N equals 6, the word “big” becomes “hom.”

In the example above, you must select a value for N before encrypting the text. The value you select becomes the encryption key. You use the same value with a related algorithm to decrypt the text, making it the decryption key as well. (In this example, the decryption algorithm uses ‘shift to the left’ instead of ‘shift to the right.’)

### Symmetric and Asymmetric Key Ciphers

Most commonly used digital cryptographic ciphers fall into two broad categories: symmetric key ciphers and asymmetric key ciphers. Symmetric key ciphers use only one cryptographic key – *i.e.*, they use the same value for both the encryption key and the decryption key.

If neither the cryptographic cipher nor the decryption key is secret, then encryption provides no security. Modern cryptographic ciphers are generally widely understood. Consequently, for symmetric key ciphers to provide security the key must

remain secret.<sup>8</sup> A classic problem for symmetric key ciphers is how to securely distribute the key.

Asymmetric key ciphers use a pair of cryptographic keys. Information encrypted with one key can only be decrypted with the other key. When an asymmetric key cipher generates a pair of keys, one is generally designated as the “public key.” This key may be widely distributed and is not considered a secret. The other key is the “private key” and is kept secret. Anyone may encrypt data using the public key, but only those who know the private key can decrypt that data. Asymmetric key ciphers are sometimes referred to as “public-key ciphers.”

### **Levels of Protection**

Assuming that a symmetric cryptographic cipher’s key remains secret, two factors determine the level of security it provides: the strength of the algorithm used and the number of possible keys. The example used in “Cryptographic Algorithms and Keys,” above, is a very weak cipher. If you do not know the decryption key, analyzing it sufficiently to determine the key requires only a trivial effort. In addition, the number of values for N that yield unique results is only 26. This makes it easy to find the decryption key using the “brute force” approach of trying each of the 26 unique keys.

The algorithms used by most modern cryptographic ciphers have not been broken through analysis despite being widely published and understood. This leaves the size of their “key space” – the number of possible keys – as the critical factor determining the level of protection they provide. The key space is represented by the “key length,” usually expressed in bits, such as a “50-bit key length” or a “128-bit key length.” Each increment represents a factor of two, so a 51-bit key length has twice as many possible keys as a 50-bit key length. In real terms, a 50-bit key length represents roughly  $1.1 \times 10^{15}$  possible keys; a 128-bit key length represents roughly  $3.4 \times 10^{28}$  possible keys.

TiVoGuard uses 128-bit keys with all of its symmetric cryptographic ciphers. Although breakthroughs in mathematics and computing are impossible to predict, the best estimates of cryptanalysts suggest that strong symmetric ciphers with keys 128-bits long should be secure against brute force attacks for several decades. Well-regarded estimates conclude that at the current level of understanding, a brute force attack employing 100 billion dollars of today’s computing power would require roughly 10,000,000,000,000 years to break such a cipher.<sup>9</sup>

In the context of the mathematics used to create most asymmetric ciphers, key length has a different significance than it does for symmetric ciphers, and acceptable key lengths must be much longer. TiVoGuard currently uses an El Gamal cipher with an

---

<sup>8</sup> The DVD Content Scramble System uses symmetric keys. Once broken, unless the keys can be replaced with new secret keys, the system is compromised. In the case of DVD video, however, the secret keys gave the movie industry sufficient time to establish a successful market regardless of the fact that the keys were eventually used without authority by DeCSS.

<sup>9</sup> Bruce Schneier, *Applied Cryptography*, 2<sup>nd</sup> Edition (New York, NY: John Wiley & Sons, Inc., 1996), 153.

894-bit key length for asymmetric encryption operations, providing for a different unique key of this length to protect the content of each TiVo Device. Extrapolating from the widely accepted estimates in Bruce Schneier’s *Applied Cryptography*<sup>10</sup> and assuming today’s understanding of cryptanalytic techniques, a 10 million dollar investment in a brute force attack on one of these keys would break the cipher for a single TiVo Device in roughly 2400 years. The TiVoGuard system further protects critical private keys by embedding them in cryptographic chips from which they cannot be extracted. The chip performs cryptographic operations very slowly, which further reduces the likelihood of a successful brute-force attack by increasing the time required to iterate through all possible values.

### **Sending Digital Media Content**

TiVoGuard protects digital media content as it transmits the content from one TiVo Device (the “sender”) to another (the “receiver”) as follows.

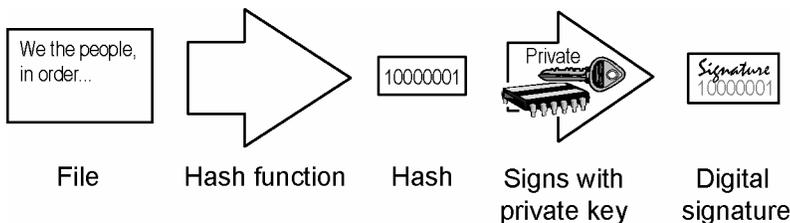
1. The TiVo service sends a “TiVoGuard certificate” to each device, that identifies the devices in the secure viewing group.
2. When each device receives a sharing certificate, using digital signatures, discussed below, it verifies that the certificate has actually come from the TiVo service.
3. Each device uses the sharing certificate when transmitting content, to ensure that only the single device for which a given transfer is intended can receive the content.

### **Verifying the Authenticity of the TiVoGuard Certificate**

When a TiVo device contacts the remote TiVo servers, the servers may send it a “TiVoGuard certificate.” If the device is part of a secure viewing group, the TiVoGuard certificate lists every device in that group. For each device in the group, the certificate includes a unique identifier and the device’s public cryptographic key. The TiVo service signs the TiVoGuard certificate, allowing the receiving device to verify the certificate’s authenticity and integrity.

The following example shows how TiVoGuard uses a digital signature to verify the authenticity and integrity of a communication from the TiVo service to a TiVo device.

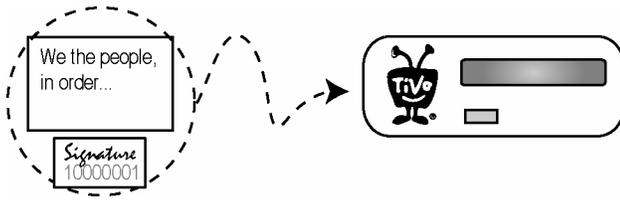
1. The TiVo service creates a digital signature for the communication.



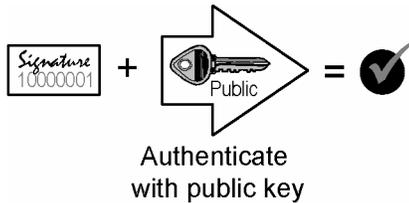

---

<sup>10</sup> *Id.*, at 153.

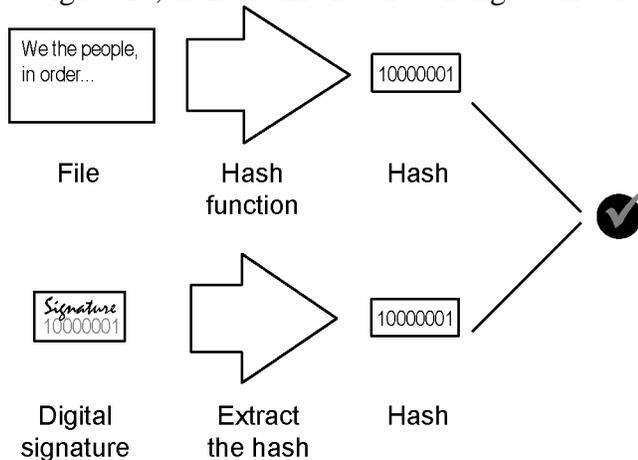
- The TiVo service then sends the signature and the communication to a TiVo device.



- To verify the authenticity of the communication, the TiVo device uses the corresponding public key to determine whether or not the correct private key signed the hash.



- The TiVo device calculates a new hash from the file, then extracts the hash from the digital signature. If the calculated hash matches the hash from the signature, then the file has not changed since it was sent.



TiVoGuard certificates also include an expiration date. In standard operation, the TiVo service regularly renews TiVoGuard certificates, extending their expiration dates. However, if a customer operates a TiVo device in a manner that does not allow contact with a TiVo server, the TiVoGuard certificate expires and the device loses its ability to send content to another device.

### Using the TiVoGuard Certificate to Authenticate Content Transfer

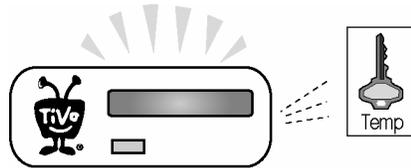
Two networked TiVo devices in the same secure viewing group may discover each other using a standard TCP/IP protocol. Each TiVo device in a secure viewing group has a TiVoGuard certificate that includes the public cryptographic key of all of the TiVo devices in that viewing group. This allows the two devices to use each other's

public keys to establish a secure channel on the network by encrypting and digitally signing communications. This use of the public key to encrypt all transmitted data performs the authentication between the sending and recipient devices.

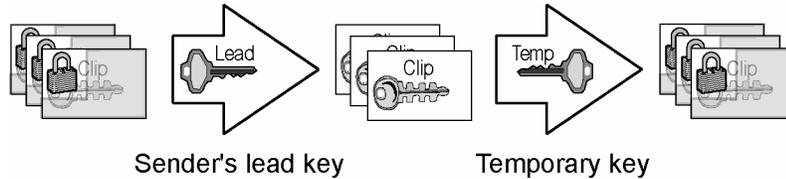
### Transmitting Content Securely After Authentication

Once the secure channel is established, communication occurs as described in the following steps:

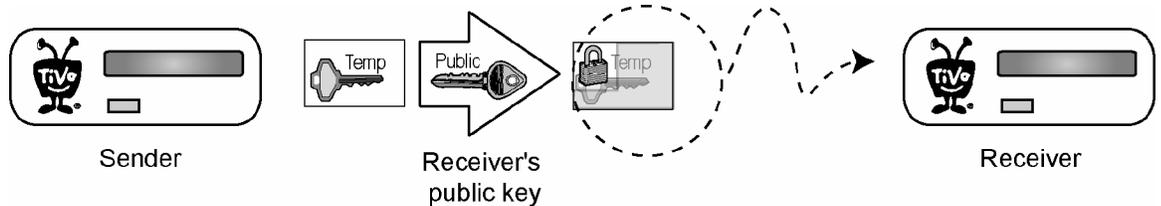
1. The sender generates a unique, temporary encryption key (like the lead key, the temporary key is a 128-bit Blowfish key).



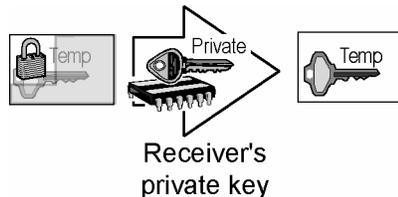
2. The sender uses its own lead key to decrypt the clip keys for content it will send, and then the sender re-encrypts the clips with the temporary key.



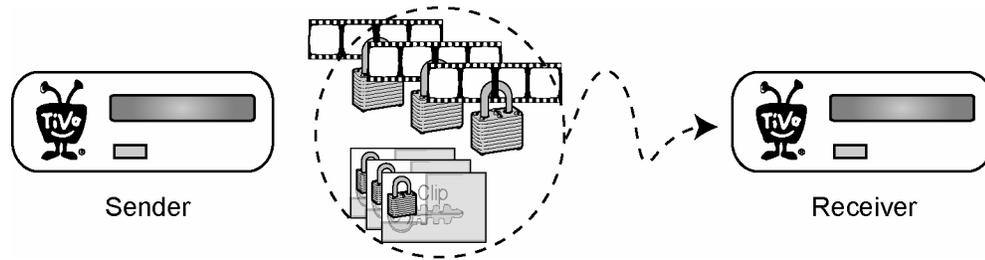
3. The sender uses the receiver's public key to encrypt the temporary key and then sends it to the receiver.



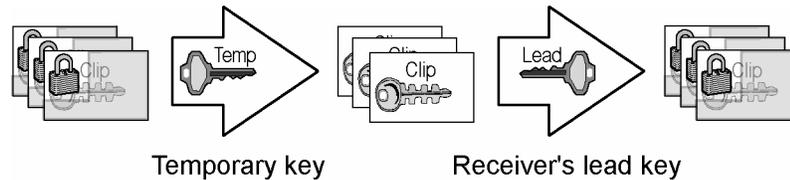
4. The receiver uses its cryptographic chip to decrypt the temporary key.



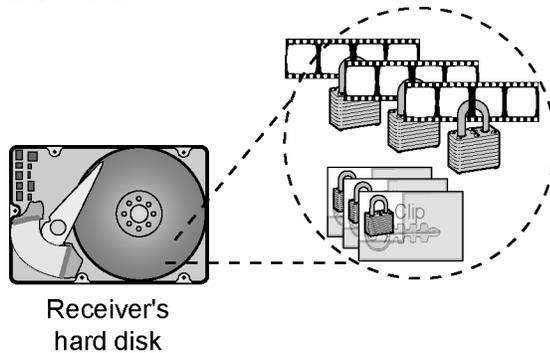
- The sender sends the encrypted clip keys and encrypted clips to the receiver. No content or clips are ever sent in the clear.



- The receiver uses the temporary key to decrypt the clip keys transmitted by the sender, and then uses its own lead key to re-encrypt them. In this way, the content stored on the receiver is uniquely associated with that device so that such recording cannot be accessed in usable form by another product except by TiVo's digital output protection technology, or, in the future, by another Authorized Digital Output Protection Technology.



- The receiver can now store the encrypted clips and encrypted clip keys on its hard disk.



This digital output protection technology accommodates consumers' use and enjoyment of unencrypted digital terrestrial broadcast content and facilitates the transition to digital television. By allowing consumers to exchange content only within a secure viewing group, TiVo provides content owners more than "reasonable assurance that DTV broadcast content will not be indiscriminately redistributed while protecting consumers' use and enjoyment of broadcast video programming."<sup>11</sup>

<sup>11</sup> *Digital Broadcast Content Protection, Report and Order and Further Notice of Proposed Rule Making*, MB Docket No. 02-230 (rel. Nov. 4, 2003) at ¶ 4.