

## Security in Media Distributed Systems

Description:

This presentation will concentrate on security flaws in the telecommunications field.

These flaws are currently being exploited by “script kiddies” with no forthcoming fixes.

Most of the cryptographic algorithms developed for protection of streaming and stand alone video broadcasts have been broken. This document will demonstrate what products are broken, why they are broken, what manufacturers are doing about it, and what breaking them allows the user to do.

### HDTV (High Definition TV)

All HDTV sets require encryption from content providers. This encryption is necessary for the authenticity and content protection of the digital signal. Media companies do not want people to be able to digitally replicate their transmissions. The protocol, named HDCP (High Bandwidth Digital Content Protection), and developed by Intel, was implemented on all HDTV sets manufactured after spring, 2002. If an individual bought an HDTV set, or a more expensive plasma TV before spring, 2002, the product is obsolete and will not be able to display an HDTV quality broadcast of 1080i. As of last year, HDCP has been broken by Niels Ferguson. Working in the crypto field for many years, Ferguson does not want to reveal his discovery due to the fear of prosecution from United States because of Digital Millennium Copyrights Act (DMCA) act.

HDTV is superior to any other current display technology on the market, including DVD's. Some TV stations already started broadcasting at HDTV

quality, but most of them have not. FCC gave the industry six years to start displaying HDTV quality back in 1992. Unfortunately, due to faulty security engineering high definition broadcasting needs more time to appear on the screens. Even when watching DVD's, HDTV is not used to its fullest capacity. DVD's store about seven to nine gigabytes of data, while a truly 1080i movie takes about twenty gigabytes of the high definition signal.

### Cable Descramblers

Cable Descramblers decode a signal that a cable TV company sends into the cable box. Each channel like HBO, Cinemax, Showtime, Playboy, and Pay-Per-View broadcast at different frequencies. Cable Descramblers demuxes these frequencies to present all the available channels to the customer. This is accomplished through a two stage process where a person sets the receiver to the test mode and then descrambles all the channels sent while in test mode. The cost for the usual setup of this technology is anywhere from eighty to one hundred dollars and allows the individual to view all channels including Pay-Per-View and premium channels.

### *Hughes DirecTV/DISH Networks*

DirecTV satellite networks have been compromised for some time. These systems use a smart card technology with authentication over phone lines. This protocol allows Hughes to update the firmware against current hacks to the system.

The simplest and safest way to hack a DirecTV system is to use an active account and modify it to advertise all channels. Since the customer is valid and pays a basic subscriber rate, Hughes cannot disconnect him/her from their broadcasting network. This kind of a hack is accomplished by taking the smartcard, modifying it by rewriting the byte codes to accept all channels and unplugging the phone line. The owners' receiver thinks the person owns the subscriptions to all the channels, but since telephone line is unplugged the receiver cannot confirm it, nor can it send the data to Hughes for validation. The Hughes receiver will now decode all the content available on the satellite broadcast.

Another way to hack the DirecTV system is to create an artificial account. Once the artificial account is located, the hacker performs the same actions to receive TV programming. Hughes scans their broadcast paths every few months for unlawful users and shuts them out by looping their smartcards.

Looping occurs when DirecTV authentication servers receive a signal from an unknown, but valid account. Since the account is valid, DirecTV servers start to talk to the receiver via satellite to find out if the account is indeed real or a fabricated one. This method of scanning has about seventy percent success rate.

Looping sets the smartcard ID to double zero and destroys it about twenty percent of the time. The other eighty percent of the time the card can be unlooped and used again.

Hughes and DISH networks realized how big of a problem satellite receiver hacking is and developed new 4<sup>th</sup> generation cards. These cards have been released on April 2002. Some information has leaked out from Hughes engineers regarding the implemented security algorithm and the cards have been cracked a short time after their release date.

### *DVD Copying*

DVD's have been around most of the decade. Media companies who manufacture DVD movies encode those using CSS (Content Scrambling System) for copyright protection and digital security of the content. This method prevents copying of a DVD onto a VCR media, or storing the DVD data on a computer. A DeCSS algorithm, released on the net on October 1999, actually breaks the algorithm completely allowing for copying as well as editing of the content on the DVD.

Many programs like DVDXCopy and DVD2One use algorithms like DeCSS to decode the information. These programs allow you to back up existing DVD movie onto the hard drive and reburn it afterward. A person "backing up" his or her movies is not breaking any laws and since DVD's shelf life is long, and the quality is higher than that of a VHS tape, so people see the benefits in doing it. These same programs can easily copy copyrighted DVD's for distribution.

It usually take anywhere from six to eight hours to descramble a DVD using DeCSS. The recent program, DVD Decrypt, copies the entire DVD onto the hard disk in about twenty minutes. It also allows selections of the DVD, for example the menu, to be omitted. This allows for faster transfer and compactness to fit the movie onto the current DVD recordable compatibility of 4.7 gigabytes. After copying the DVD to the hard drive using the DVD Decrypt, one would use DVD2One to transpose the DVD into the writeable format. This process takes about thirty minutes after which you can safely use Nero to burn the movie.

### *TiVo Systems*

TiVo is a playback system that digitally records broadcast video from the TV onto the hard drive. Some TiVo models where able to send recorded TV shows to other TiVo systems. This functionality was used widely until the TiVo, Inc. got sued because the technology allowed for sharing of pay-per-view content. There was no flaw in the design and the device was functioning appropriately, but using it to share pay-per-view material caught the legislators' sights. Now, TiVo is not able to send and receive any programs over the network.

TiVo uses a standard IDE hard drive as a storage device with the Linux operating system. People have found ways to expand the capacity of the TiVo system using miscellaneous hacks and advanced hard drive mounting commands found in Linux. TiVo revenues suffer because their pricing scheme is built upon capacity of the device. For example, a twenty gigabyte unit will cost 199 while an eighty gigabyte unit will cost 399. It is easily seen that a sixty gigabyte hard drive does

not cost 200 dollars and therefore, TiVo is losing money by not providing component security algorithms.

### Xbox

Console games have been around for a while and every one of them has been hacked. Knowing this, Microsoft designed the Xbox with security in mind. Sometime around June 2002, a mod chip called Enigmah was released. Enigmah chip requires precision soldering of 29 wires onto an Xbox mainboard, which takes around ninety minutes. This mod chip allows an Xbox user to play imported and burned DVD games that can be found on the net, burned from the original, or bought overseas. Second mod chip codenamed Xtender/Xecuter has only nine wires and requires fifteen minutes for the installation. This is a major security design flaw with the Microsoft hardware.

### PlayStation 2

Sony's PlayStation 2 has also been hacked. Magic 3.1 mod chip takes only nine wires to solder and can play burned DVD and imported games. Recent revision of the mod chip, Magic 3.6, allows for solder-free, five minute installation.

Sony is pursuing legal action against web sites who are distributing these mod chips. Unfortunately, Sony had little success in legal courts in Japan, where most of these chips come from.

## Future

Licensed products that require authentication and authorization are created on the basis of cost/benefit ratio. Competing companies want to offer the most “bang for the buck” to the end user and want to keep research costs to the minimum.

Lowering research costs and shortening the research time allows the product to be marketed faster and cheaper than the competition. The product must be fully featured and must have good user interface if it is to sell.

Usability and functionality will suffer if the security system is too strong. The product will not perform what it is designed to do and will have less features. On the other hand, if a security system is too lax then hackers will find the flaws fast and companies stand to lose revenue.

Future holds the balance between security and usability as well as price/performance of the product. Companies create new products every day and they want their devices to be secure, but at what cost. The cost of an ideal security system will require many months of research and millions of dollars in funds.

Companies understand that even if their design is compromised they will lose less money than what would be spent on security research.