Couch Wars

The true untold story about the weekend before the Superbowl, dynamic nanos, card condoms, loopholes, unloopers, Canadian pride, the soverignty of nations, the profit imperative, the quest to build an unhackable system and the never ending celestial battle between DirecTV and the video pirates.

Peter Wayner

Copyright Notice

This is a free version of a document I distributed in 2001 on a pay-per-read basis. Much of the information is still current, but the legal environment changed dramatically on April 26th, 2002 when the Canadian Supreme Court effectively made satellite piracy illegal. This will certainly affect some parts of the business and make it riskier, but it won't remove the desire of Canadians to view American TV.

You're welcome to distribute this version to anyone you want as long the document remains unaltered. Please don't strip out the ads or convert it to another format. The ads are for two of my new books, Disappearing Cryptography: 2nd Edition *and* Translucent Databases.

If you have any questions or comments about the piece itself, please write me.

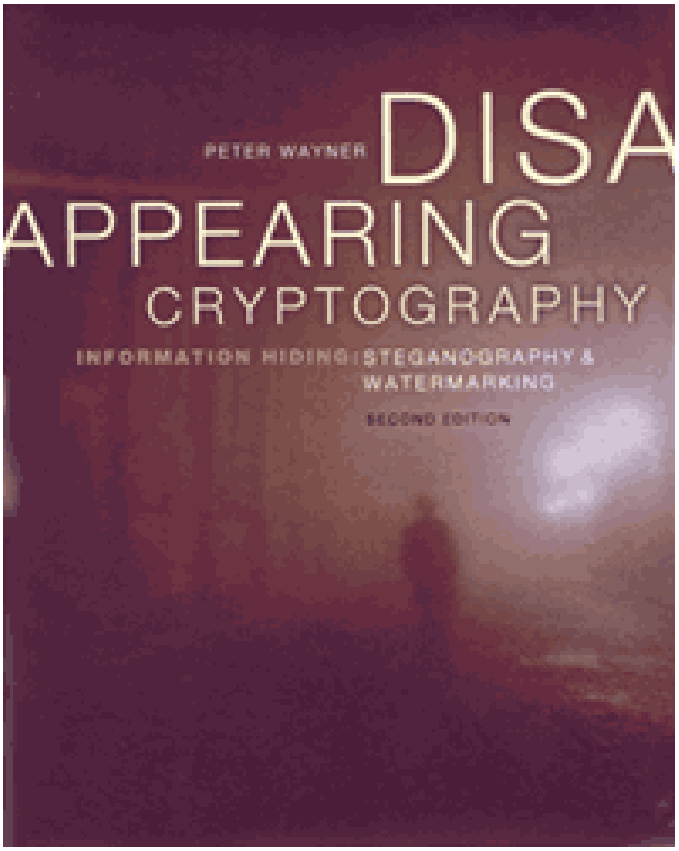
Peter Wayner p3@wayner.org

Disappearing Cryptography, 2nd Edition

Information Hiding: Steganography & Watermarking

by Peter Wayner

ISBN 1-55860-769-2 $44.95
To order, visit:
http://www.wayner.org/books/discrypt2/



Disappearing Cryptography, Second Edition describes how to take words, sounds, or images and hide them in digital data so they look like other words, sounds, or images. When used properly, this powerful technique makes it almost impossible to trace the author and the recipient of a message. Conversations can be submerged in the flow of information through the Internet so that no one can know if a conversation exists at all.

This full revision of the best-selling first edition describes a number of different techniques to hide information. These include encryption, making data incomprehensible; steganography, embedding information into video, audio, or graphics files; watermarking, hiding data in the noise of image or sound files; mimicry, "dressing up" data and making it appear to be other data, and more.

The second edition also includes an expanded discussion on hiding information with spread-spectrum algorithms, shuffling tricks, and synthetic worlds. Each chapter is divided into sections, first providing an introduction and high-level summary for those who want to understand the concepts without wading through technical explanations, and then presenting greater detail for those who want to write their own programs. To encourage exploration, the author's Web site www.wayner.org/books/discrypt2/ contains implementations for hiding information in lists, sentences, and images.

"Disappearing Cryptography is a witty and entertaining look at the world of information hiding. Peter Wayner provides an intuitive perspective of the many techniques, applications, and research directions in the area of steganography. The sheer breadth of topics is outstanding and makes this book truly unique. A must read for those who would like to begin learning about information hiding."

--Deepa Kundur, University of Toronto

"An excellent introduction for private individuals, businesses, and governments who need to understand the complex technologies and their effects on protecting privacy, intellectual property and other interests."

- David Banisar, Research Fellow, Harvard Information Infrastructure Project, & Deputy Director, Privacy International.

- **Do you have personal information in your database?**

- **Do you keep files on your customers, your employees, or anyone else?**

- **Do you need to worry abou European laws restricting the information you keep?**

- **Do you keep copies of credit card numbers, social security numbers, or other information that might be useful to identity thieves or insurance fraudsters?**

- **Do you deal with medical records or personal secrets?**

Most database administrators spend some of each day worrying about the information they keep. Some spend all of their time. Caring for information can be a dangerous responsibility.

This new book, ***Translucent Databases***, describes a different attitude toward protecting the information. Most databases provide elaborate control mechanisms for letting the right people in to see the right records. These tools are well-designed and thoroughly tested, but they can only provide so much support. If someone breaks into the operating system itself, all of the data on the hard disk is unveiled. If a clerk, a supervisor, or a system administrator decides to turn traitor, there's nothing anyone can do.

Translucent databases provide better, deeper protection by scrambling the data with encryption algorithms. The solutions use the minimal amount of encryption to ensure that the database is still functional. In the best applications, the personal and sensitive information is protected but the database still delivers the information.

Translucent Databases, a new book by Peter Wayner, comes with more than two dozen examples in Java and SQL code. The book comes with a royalty-free license to use the code for your own projects in any way you wish.

Order today at
http://www.wayner.org/books/td/

On January 21st, 2001, the elite forces of DirecTV gathered in their high security bunker in southern California and launched an all-out attack. The officers planned this moment for months. They sent turncoats and moles to slumber behind enemy lines waiting for a signal to awaken and deliver a crushing blow in the mother of all electronic battles. The generals in DirecTV's bunker pushed the button, activated the stealth units and fried hundreds of thousands of brains. The damage was permanent.

The news of the crushing victory echoed through the tattered forces of the enemy who struggled to understand the extent of the damage. Large portions the rebel forces sustained devastating destruction. Yet, DirecTV managed to execute the assault without hurting the 9.5 million loyalists. The entire operation unfolded with clockwork precision and yielded few, if any, collateral injuries. It was the perfect war.

Ah, hype. Rolling out the martial rhetoric is an easy trick for writers and politicians. In many ways, using the word "war" to describe the events of January 21st is unkind to the millions who died at Antietam, Ypres, Waterloo and countless other battlegrounds. No one died on January 21st. The vanquished were barely inconvenienced. They were not forced into refugee camps, infected with disease, or led on long marches. The most heinous damage inflicted by DirecTV's terribly swift vengeance was a sentence to spend the night without satellite TV. The beer was still cold, the chips were still crispy, the couch was still inviting, but there wouldn't be any flickering light from the screen.

The target of the attack was a loose-knit guerilla army skilled in fiddling with the black boxes on top of their television set. These pirates found a way to make their TV show all of the pay-per-view, all of the movies, all of the local channels, all of the porn, and all of the Worldwide Wrestling Foundation events without paying. On Saturday, the guerillas sat complacently on their couches surfing with abandon. On Sunday, they cried.

It may not be fair to call this war, but not all wars are fought over high-minded goals like slavery and genocide. The Opium War pitted the English against the Chinese in one of the bigger "War on Drugs". The U.S. Marines still sing about the time they stomped the Barbary pirates who were preying upon American ships. Sometimes a battle needs to be waged to make the world safe for commerce. Tom Brokow may never

write a book about the "Greatest Generation" at DirecTV, but that doesn't mean the fight wasn't real. If too many people start stealing the satellite signal, there's no money to launch the satellite, pay for the power, or pay for the programming.

The outcome of the battle affects everyone in the content generating factories. DirecTV writes some of the biggest checks to cable programmers like HBO. If the money stops flowing, the television industry needs to go back to advertiser support. The average DirecTV customer spends $59 per month and about 40% of it flows back to the content creators. That $224 million per month pays for an army of creative people devoted to entertaining the world. If the piracy spreads far enough and wide enough to threaten that flow of cash, the new material stops flowing. The actors go back to their day jobs in the restaurants, the agents scramble for other schemes and the Networks start shopping around for more low-rent game shows to fill the time.

Of course, that's Hollywood vision. Some of the pirates see themselves as Robin Hoods battling monopolies in the United States and Canada. Television used to be free, they say. Now you've got to pay for decent reception and the price keeps going up and up and up. The money never seems to buy better customer service or more channels. The profits some how end up in the pockets of the rich.

In the deepest sense, the battle of January 21st is just part of a larger struggle to regulate the flow of information. The content companies dream of bundling their beautiful jewels up in tamper proof cases so that no one will steal them on the way to market. The Hollywood legal infrastructure continues to push for tougher laws protected by bigger punishments aimed at stopping anyone who even thinks about how to watch a show without paying. The industry employs some of the best mathematicians and cryptographers to develop sophisticated mechanisms for encoding the precious content so it can't be stolen.

Despite all of these efforts, piracy also flourishes. The secrets to DirecTV's signal are locked away in a tamper proof smartcard hardened against attacks with radiation, heat, razors, diamond paste, scanning electron microscopes and other tools, but the pirates succeed. They found a backdoor in DirecTV's smartcard and they can now reprogram it to do anything they want.

Well, almost anything they want. On January 21st, DirecTV sent down a virus-like bot that searched for evidence that someone had been exploiting the loopholes. If the bot found a smoking gun, it executed the card right then and there.

The battle that raged across North America on January 21st may not be in the same class as the ones which ended the lives of our freedom fighting forefathers, but it is an important part of deciding the rules of information commerce. Will the rightsholders be able to keep the genie

corralled enough to charge admission? Will information just slip out of the bottle into the air where no one can even dream of owning it? Will the pirates or the engineers prevail?

Something New

The pirates like to call January 21st "Black Sunday" and the attack itself an "ECM" or "electronic countermeasure." DirecTV has always fought the pirates since they began broadcasting in 1994. In the beginning, the pirates were too few to grab DirecTV's attention, but by the late-1990s the DirecTV engineers started searching out and launching ECMs with regularity. The attack they started on January 21st was a new and more devastating ECM designed to permanently wipe out pirate cards by destroying crucial bits in the memory. Fortunes were lost. Dreams of watching the latest WWF pay-per-view were scuttled. Hundreds of thousands of smartcards– some put the estimate at more than a million– turned into what the pirates sometimes call "icescrapers."

"Black Sunday was an excellent hit for Dave!!!" says a pirate who travels under the nom-de-guerre of "Rayzor." For some odd reason that no one can really explain, the pirates refer to DirecTV as "Dave". [1]

"Dave planned an attack and over several months, corralled everyone in for the kill. The impact [of this] was devastating, the test card world was knocked to its knees and then everyone realized just what they had been doing over the previous months– setting us up for a rude awakening."

Pirates use the euphemism of "test card" to describe the cards that have been altered to deliver free television. The coy presumption is that hacked smartcards are just used to test a satellite dish and make sure all of the channels are functioning correctly.

Rayzor continued, "I fell into the trap myself, knew something was cooking but went along and was taken for the ride just like everyone else."

Rayzor was not the only one. On January 21st, tens of thousands of similar stories flooded the websites where the satellite pirates trade their information. These Internet chatrooms are not as much fun as the saloons filled with whiskey and women, but they are even more anonymous and efficient at spreading the news. On Black Sunday, there was nothing happy for anyone to say.

A pirate known as DeeEssEss posted this news to his site, `www.hack-hu.com`: "Quite simply put, at this time, there is NOTHING you can do but sit and wait. Do not email me saying 'so-and-so said this would work' or reporting that 'X glitch setting gave me my ATR back' because I can as-

[1] Here's one possible explanation: For a short time, MTV pretended to change its name to 'DTV' and put the heavy metal singer, David Lee Roth, in charge of choosing the videos. DirecTV also uses the abbreviation 'DTV'.

sure you that anything you report is already widely-known. I cannot stress this enough: at this point, your cards are DEAD."

Some pirates held out hope for a solution. Some talked about "card condoms" and programming their PC to act like a smartcard. Most were depressed.

Another pirate who calls himself Alientech, told me, "My emotions were really low after Black Sunday. I thought, 'Oh no, this is the end of the game.'"

The Never Ending Game

Satellite signal piracy is not a new game. It began in the mid 1980's after big six-foot satellite dishes grew cheap enough to be popular in rural America. When networks like HBO discovered that people were watching their shows without paying, they started encrypting their signal and requiring people to pay monthly bills. The average Joe fought back by purchasing unofficial descramblers that cracked the signal without requiring a monthly fee.

The DirecTV system emerged in the 1990's after the business learned its first lessons. (See Charles Platt's excellent story in Wired issue 2.08). The new generation was built with the best technology using the best engineers with the best resumes. The signal could be picked up with a smaller pizza-sized dish. Anyone who tried to listen in, however, found the signal scrambled using an encryption mechanism designed by the best minds from Stanford or MIT. The technologists held prestigious patents and are well-known in the field.

Despite the best efforts by the talented engineers, a new generation of engineers and garage hackers poked, proded and found ways around the security mechanisms. They might not have the same pedigree or the same intellectual arsenal as the designers, but teams of hackers in strange corners of Canada and the Caribbean have found ways to slip into the smartcards and reprogram them to display all of the channels all of the time.

Pirate Games

Some say the pirate engineers come from Bulgaria or Russia. Some say that they are disgruntled employees from DirecTV or the companies that manufacture the dish. Some say that the hackers are just looking for something interesting to do during the long Canadian winter. In any case, the tricks for breaking open the cards circulate among the pirates, the dealers, and the enthusiasts who treat the search for free television as a very sophisticated hobby or game.

The motivations of the pirates vary. The dealers are the easiest to understand. They run stores on line and market their goods through clandestine networks of friends and junior dealers. They use cell phones and register their websites under fake names. They sell tools with names like the "Terminator Boot Loader" or the "Vector Super Unlooper" that range in price between $75 and $400. Some offer "card cleaning" services that remove the nasty software buildup that gets in the way of receiving all of the channels all of the time.

The business can be quite lucrative and dangerous. Reg Scullion helped many customers in Canada receive DirecTV without paying until the Royal Canadian Mounted Police raided his home and confiscated more than 10,000 smartcards and more than $6 million dollars. All of the charges were dropped, though, and Scullion is now battling to get his money and equipment back.

The hobbyists are a bit different. They're interested in learning. They buy tools for reprogramming the cards and many actually write software themselves. They're as motivated by the quest for knowledge as the wish to expand their channel selection. Sometimes this devotion to pure art even causes them to lose sight of the goal. It's not uncommon to see one pirate hobbyist insult another on a website by saying, "You're just after free television."

This game can be quite expensive. Pirates routinely spend $200 to $1000 a year stealing a signal that routinely sells for about $250 to $1000 a year.

Of course, there is no irony for many of the pirates who are after channels that they can't legally buy. DirecTV, for instance, cannot legally broadcast to Canadian residents even though the signal from its satellite hits most of the North American continent. Dave hasn't purchased Canadian broadcast rights from its U.S. content creators and Canada hasn't issued him a license to broadcast inside its borders.

Canada has a set of stiff regulations that forbid broadcasters from serving the country unless they follow a complex set of regulations that specify the percentage of content that comes from Canadian sources.

"It really has nothing to do with subject matter," says Ian Angus, a Canadian lawyer who has defended many pirates. "It has to do with the number of Canadians employed in the production. If you get a whole number of Canadians down in New Orleans doing a show about New Orleans taxi drivers, then that's Canadian content. But if you get a very thoughtful introspective history of say the Inuit from ABC, then that wouldn't be Canadian content. It has nothing to do with Canada per se, it has to do with employing Canadians."

If someone in Canada wants to watch the American television, they often have no choice but to steal it. Or they can buy Canadian satellite television from two licensed Canadian companies, Bell Express Vu and

Star Choice. Of course, keeping the people drinking from the right teat is not so simple when there's a choice. In the past, Canadians could pick up a DirecTV dish in the US, bolt it to their house and suck in all of that American content without a bit of respect for the border line defined by the Wars of 1776 and 1812.

Today, DirecTV is making it a bit harder. David Fuss, a satellite dish dealer in Toronto, says, "Most Canadian [satellite TV watchers] are using hacked cards. It's illegal to pay and [DirecTV is] making it more and more difficult. They're insisting on Social Security numbers. They're insisting on credit cards and credit checks. They're making people go into a hacking situation."

In March this year, a Montreal man named Charles Perlman was convicted of arranging for Canadians to pay for their DirecTV service through post office boxes in the United States. He even created a redialing service which took the phone calls made by a DirecTV set top box and rerouted them through a United States number to make it appear as if they came from the United States.

Perlman is appealing the decision. At this point he is one of the few to actually be prosecuted successfully. People like Scullion who don't bother paying DirecTV's monthly fee have escaped through loopholes. In a gross simplification of a complex legal question, you can't be accused of stealing something if it can't be legally sold. Whatever you do, though, don't try to pay for it.

Some cynics see all of these prosecutions as just skirmishes between the big Canadian satellite television companies like Bell Express Vu and Star Choice with the US-based DirecTV. Perlman's real sin was that he was providing a legitimate way for DirecTV to gather Canadian customers.

DirecTV is far from the only satellite system being attacked by pirates. The Dish Network is not as easy to hack because the pirates must modify the base unit as well as the smartcard, but the piracy occurs none the less. Some like the channel selection better than DirecTV's. The various satellite services in Europe are also big targets for pirates. Each of the companies has teams like the one at DirecTV trying to keep the signal in the corral.

One Canadian pirate told me that stealing the signal from the Canadian provider Bell Express Vu was popular in the United States. "A lot Americans get it because the American hockey announcers suck." he explained. "A lot of Canadians in Florida get it to keep up on the hockey."

In the United States, many of the pirates are motivated by the search for channels they can't legally watch. Local television stations, for instance, are only available to a strange group of people in the right zip codes. If you're a transplanted New Yorker living in Minneapolis, you can't legally watch your home town nightly news on DirecTV even though the signal is beamed right to your box. If you get a magic test card, however, you can

watch the local news in dozens of towns.

Many people in the United States are also driven by the search for free pay-per-view. One of DirecTV's most popular programs are the weekly World Wide Wrestling and this may be why DirecTV scheduled the Black Sunday attack during one of the biggest ever. But then every fight on WWF is one of the biggest ever.

Some also speculate that the pirates are on a search for untraceable porn. The magic test cards also deliver all of the pay-per-view Playboy channel without leaving a mark on your monthly bill.

Counting the Casualties

How many pirates were fried on January 21st? No one can say for certain. Many mention the number 200,000, which has appeared in several news reports. BuddyX, one of the moderators at `www.dssware.com`, thinks that DirecTV knocked out as many as 1 million systems. Others offer estimates that range in between 100,000 and 1,000,000. DirecTV itself refuses to issue any official estimates, although they clearly try to measure them internally.

Many of the pirate web sites devote some time to keeping track of which is the most popular and these counts provide indirect estimates. The website `www.pirateden.com` which offers software, discussion groups, and tips to DirecTV pirates, claims that 263,000 visitors arrived during a bit longer than a week in March. Another pirate information site, `www.hackhu.com`, claims that about 5.3 million people visited that site between September 2000 and March 2001 and about 250,000 unique IP addresses showed up in the logs during the first ten days of March.

Sites like `www.pirateden.com` or `www.hackhu.com` are in the business of teaching people about how they might want to intercept the DirecTV radio signal. They're strictly aimed at moving information. The front page of many of the sites comes with long legal disclaimers say the site is hosted in Canada for use by Canadians in the interception of signals in Canada in a way that isn't forbidden by Canadian law. Employees and agents of DirecTV aren't allowed to trespass.

In any case, the sites also provide information, something that PirateDen's front page proclaims, " is protected by the fundamental right of free speech GUARANTEED by both the United States Constitution and Canadian Charter of Rights and Freedoms."

The site also notes, "As outlined above, although simple access of the information on this site may be legal and protected under various constitutions and charters, physical use may NOT be legal in certain countries and jurisdictions, in specific, The United States. If you are in doubt, you should seek legal advice BEFORE putting any information on this site to

a practical use."

Most of the sites offer chat rooms and fora where pirates and wannabe pirates can come to swap files, software and theories about how to overcome the latest defense deployed by DirecTV. On January 21st, the traffic on these boards grew so intense that they crashed many of these servers. Everyone was confused.

The sites also take advertising which clicks through to vendors who sell the latest tools. Running the sites is not cheap so many of the webmasters regularly ask for contributions to pay for the cost of the bandwidth. Some even offer premium membership which gives the user access to special rooms where, presumably, the really good information flows.

Many of the sites have a tacit understanding with the hardware manufacturers who advertise on the boards. The hardware is often not strictly sold to hack DirecTV's signal. The smartcard programmers, for instance, could be used to program any smartcard, not just the HU card buried inside the DirecTV set top box.

The websites and their back rooms offer software that knows the right commands so the smartcard programmers will be able to breach the security on DirecTV's cards. Both are useless without the other and so both seem innocent without each other. The hardware manufacturers are just selling generic tools. The software guys are just talking about how to hack the satellite system. And so both exist in their own rationalization for how it's all legal.

Most of the people who host the websites, though, have no illusions about how laws actually work in the real world. Many of the sites are registered to post office boxes in fake names. The phone numbers, if there are phone numbers, are for cell phones registered to fake names in fake locations. Just because some judge says the business is legal doesn't mean that the police won't come back. All of the charges were dropped against Reg Scullion, but that doesn't mean the RCMP is going to give him back his money without a fight.

The webmasters insist on using fake names. Most of the pirates mentioned in this article spoke only on the condition that I not use their real names. Some insisted on routing questions through email drop boxes. Others insisted on encrypting the entire conversation. Each had their own list of restrictions based upon their experiences.

DeeEssEss, for instance, refused to divulge any information about his personal life. Anything might be used to track him down and put him in jail. This caution eventually got the best of him. He and his site retired in late July.

Alientech, on the other hand, was happy to tell me about the test card business he runs out of his home near Toronto with the help of Aliengal, an office assistant, and Alienprincess, his 27 year old daughter. His three sons (21,19 and 17) aren't interested in the family business, although they

may change their mind.

Alientech runs two websites for his business. The first, `www.metaloid.com`, is "operated by Canadians for Canadians", offers articles and details " for educational purposes only." The second (`www.cardcleaners.com`) sells the hardware which he ships from his house after people pay with either a check, cash, or Paypal.

"I sell twenty or thirty card readers a week" he explains, but this only makes him a small player. "I know guys who sell 200 or 300 a week. I know guys who are driving around in Mercedes."

The 45 year old former medical equipment designer says that he's not breaking the law by selling the tools. "The RCMP has been directed to stop harassing satellite guys because they've lost every case. It's crazy. There's no law against it." he explains.

While he supports himself with the business, Alientech sees the process as fighting for a freedom of choice. "I don't watch much TV." he says. "The only reason I got the satellite is so I could watch the Ultimate Fighting Championship. The Canadian Company stopped carrying it."

Most of the technology Alientech sells comes from other hardware and software developers who, perhaps not so unsurprisingly, take their names from science fiction. He speaks of the "Rebel Alliance", a group of hackers who wrote very successful software with names like "Jedi", "Obi-Wan", and "Stealthy" that could be used for programming the smartcard. Then, they faded and the "Hickware group" and the "Cloakware group" took their place.

The pirates tell many stories about these elusive groups of engineers and programmers who shoot to prominence after developing a sophisticated tool for hacking the cards. Eventually, DirecTV gets wind of the matter and finds away to thwart them. Some retire, some regroup, and some decide to go work for DirecTV itself. There are hundreds of tales about dozens of groups, both real and apocryphal.

Alientech is just one small part of this amorphous, semi-underground economy. There are many dealers who purchase software and tools from the hacking groups and then sell fixes to the couch potatoes. Sometimes the people purchasing the hacked smartcards know what they're getting and some don't. One person told me that the man installing his satellite dish offered him a choice. He could either buy the monthly plan or purchase a "lifetime" plan for several hundred dollars. The dealer forgot to mention that the first plan was backed by DirecTV while the second was backed by the pirate community.

On January 21st, customers who purchased the lifetime supply of DirecTV for one low cost were not happy. DirecTV fried all of the cards and the customers could only go back looking for their dealer. Some could be located but others retired on the spot.

DirecTV

All of this piracy is confusing to Dave Baylor, the executive vice-president at DirecTV responsible for technology. He clearly enjoys talking casually about the five Hughes satellite "buses" parked 22,300 miles up in geo-stationary orbit, the 40 megabits per second streaming through each of the 32 transponders on the bus, the launch process designed to conserve hydrazine fuel, and the hundreds of other different technological challenges surrounding beaming more than 400 channels to the United States.

The pirates, however, confound him. They're taking what he's selling without paying for it, but their motivation is strange and unfathomable. He can't really understand how "the same person who would never steal an apple of a fruit stand will invite you into their living room and brag that they're getting free satellite."

"Many of the people are kind of nerdy with a different focus." he says and then adds, "I was one myself."

But somewhere along the way, some engineers took a different path. Baylor chose corporate respectability and the comfort of a smoothly running, sophisticated organization, others rebelled and embraced an outlaw existence. He worked in the television business until Hughes hired him to help the company morph from a defense contractor into an entertainment powerhouse.

Baylor has a large office in a non-descript building just to the south of the Los Angeles International Airport, about halfway between the defense contractors in Long Beach and the content kings in Hollywood. The security at the building is tight– I needed to register the serial number of my laptop when I entered. They have one control room with more than 400 televisions wired to their own DirecTV set top box just so controllers can monitor every channel all of the time.

Some of the signal begins several miles away in Marina del Rey where DirecTV keeps its satellite dishes just a few miles from an airstrip where Howard Hughes used to land. The sailboats, the beach, and the other icons of southern California living are just a few minutes away. The entire operation is not lavish nor baronial, but it is exudes the corporate crispness and security-clad, official demeanor of the establishment. Forms must be filled out and security id cards must be worn at all times before the paychecks float through the direct-deposit ether to the bank accounts.

Somehow, Baylor understands that this is a world away from the lonely pirate redoubts on the Canadian plain where the rebel geeks torture the smartcards into revealing their secrets.

"[The pirates] travel in a different social circle than the population at large. And they start to develop their own culture. That's what we see in the hacking community. They have a different set of drivers, a different set of loyalties." Baylor says.

"It's a very different world. It's a subculture that has a different view of responsibility, rights, freedoms than the general populace. I believe that some people truly believe what they say. I think others hide behind those statements to justify their criminal acts. There are true revolutionaries and there are anarchists who have no agenda except to cause disorder."

Baylor understands that some of the pirates are cloaking themselves in the same First Amendment that protects the broadcasters. The average episode of "MacGyver", for instance, has more information on hacking or pirating some technology than the pirate websites.

The people in the technical world are constantly pulled between this order and anarchy. Hacking a satellite system is a great challenge, a mano-a-mano feat in a world that's tamed all of the lions, tigers and bears. Building a smoothly running mechanism that delivers hundreds of channels to millions of viewers is a different kind of challenge.

Baylor is on the Board of Trustees at Harvey Mudd College, a top flight engineering school just up the road in Pasadena. When he discovered that the students were regularly swapping copyrighted music files over the Internet with Napster, he started pushing the school and the students to think about the importance of intellectual property.

"What's our moral responsibility about informing our students about their responsibility to IP?" he asks.

"Why do you go to school. To get smart and to be able to go out and sell your brainpower to companies or to start your own company." he says he asked the students. "Show me the economic model where you go and sell your ideas. How does that company survive? How do you get paid?"

Cash flow

Baylor is more than happy to list the expenditures that go into keeping DirecTV's signal flowing. "Typical satellite launch and insurance is about $200 to $250 million per satellite" he says, most of which is paid to DirecTV's corporate parent and satellite manufacturing company, Hughes Electronics. "That's a billion and quarter bucks in satellites. We're launching two more satellites this year. And they have a design life of 12 to 15 years."

Another portion of DirecTV's budget goes into running broadcast centers in Los Angeles and Colorado as well as providing for legitimate customers. Holding 9.5 million customers' hands while they watch TV is surprisingly time consuming. Baylor explains that the company routinely fields plenty of calls on its 800 line asking when a rain-delayed baseball game will resume.

With 9.5 million customers paying on average $59 per month, Dave's 2000 revenues from customers come to about $6.7 billion per year. The

total revenue including other sources topped $7.2 billion. That's a significant amount of money, although about 40 percent of that flows back to content producers.

Large numbers have strange effects. Some pirates see themselves responding like Robin Hood faced with an unfeeling leviathan. Some pirates justify their actions with tales of bad customer service from DirecTV. Others see the commercialization of pay TV as a crime of another sort.

One pirate who travels under the nom-de-guerre of RCAMAN told me, "I knew [RCA television pioneer] Dr. Sarnoff personally and remember several conversations with him regarding the future of TV. The whole satellite TV business is his concept. When Dr. Sarnoff called the engineers working on the project to his death bed, his last words were 'And just think of it, orbiting satellites, transmitting crystal clear signals to homes, FREE OF CHARGE!' That's right, Dr. Sarnoff's dream was free TV via satellite transmission paid for by the advertisers just exactly as broadcast TV is."

Of course, there are others who see DirecTV as a savior who emerged to challenge the cable television monopoly. When DirecTV first started broadcasting, many of the early customers were cable refugees filled with bitter stories of their local cable system's bad signals, terrible service and indifferent management.

The Making of a Crime

DirecTV's fight against piracy is not just limited to technological feats like their Black Sunday attack. A number of U.S. laws criminalize the act of stealing the DirecTV signal, selling tools for stealing the signal, even possessing a hacked smartcard, or even, in the most extreme case, describing how to hack the system. The Hollywood legal infrastructure worked hard to create a network of laws that make the punishment for copyright infringement more serious than many basic violent crimes.

Larry Rissler, the director of DirecTV's office of signal integrity, is more than happy to read off long lists of arrested dealers who have been sentenced to jail. Breaking encrypted radio transmissions is a violation of up to five different statutes he says and can yield fines of up to $500,000 and jail terms of 5 years or more.

"We just had a defendant sentenced to 27 months in jail," says Rissler. "They threw in money laundering which increased the time." Many had to pay restitution as well. The sentences will be increasing because the new guidelines add stiffer penalties for theft of intellectual property in the United States.

Rissler is an ex-FBI agent who says that satellite piracy is the most fascinating case he's ever worked. In our interview, he told stories of dozens of raids and investigations that played across the United States, Canada,

and the Caribbean.

"We've support 63 enforcement actions nationwide this year." he says, explaining that a typical "enforcement action" comes when a team of officers raids a home or business with a search warrant. If there's enough evidence, someone goes to jail. Taking the computer systems apart and understanding exactly what the pirate was doing, however is a complicated chore.

"We had one pirate who was searched, arrested, and serves time. He had his computer rigged so if the computer detected in a sufficient change in the data stream, it would call him on his cell phone and he could come home and get to work." he explains.

Rissler and his team work with all levels of the government including the US Customs, the FBI, and many local forces. Framing the crime as a new Internet-era intellectual property theft often draws the interest of the best officers.

The net is beginning to widen. DirecTV is just starting up a new push to go after the end user. The company has long lists of names and addresses gathered from raids on pirate dealers. In the past, they ignored the little guy because the cost of prosecution was high and the gains small. Now, the enforcement team is starting to investigate prosecuting casual users who steal the signal without paying.

"We get good cooperation", he says from US agencies. We did a sweep in LA and got tremendous press coverage. The bureau arrested 15 satellite hackers. 10 were in the LA area. At the press conference, the FBI official talked a lot about the use of the internet to advertise these devices."

As soon as one pirate drops out of business, others often emerge. I visited the store of one pirate in Southern California who sells card hacking hardware from spiffy glass display cases. The pirate operated in a strip mall across from a doughnut shop just a few minutes drive from DirecTV's headquarters. The business is not officially selling pirate hardware. There are no glamorous neon signs spelling out a name like "Pirates-R-Us" or "Free TV". There's no indication that the secrets to intercepting the DirecTV signal can be purchased inside. It's just a normal business that happens to have one display case devoted to bits of electronics with names like "Unlooper."

While the display case occupies only a small part of the store, the pirate did explain to me that he makes a bulk of his profits from the machines for turning a regular smartcard into a powerful "test card."

This pirate shop sells only the hardware for reprogramming. When I asked whether the board on the left was going to help with the Black Sunday attack, he turned coy and told me, "You know I can't answer that question."

Like many American dealers, he abides by the letter of the law and sells the tools for accessing the smartcard as tools for experimentation.

The presumption is that you might want to buy a smartcard programmer to add smartcard access protection to your garage or your washing machine. If so, there are a number of places waiting to serve your needs.

I also located another dealer near my house in Baltimore. He agreed to meet and show me his wares if I promised to show him a driver's license proving I was a journalist. The meeting fell through after I pointed out that it was much easier to clone a driver's license with a laser printer than it was to hack into the DirecTV smartcards.

This pirate had reason to be afraid. The local Maryland police had just raided another pirate. The police are now setting up sting operations to purchase cards. This is now a sexy, Internet-based crime and that attracts police attention. As Rissler says, "We get good cooperation" from the U.S.

Oh Canada

The news from Canada is not as good for DirecTV. The Royal Canadian Mounted Police rounded up several pirate dens and collected tens of thousands or more hacked cards in raids only to be rebuked in court. In some cases, the warrants weren't issued correctly. In others, the activity just wasn't considered illegal. Canada does have a law against stealing the signal of lawful broadcasters, but this doesn't seem to apply to DirecTV because DirecTV doesn't have a license to sell its product in Canada. To oversimplify a legal matter, DirecTV is the real pirate stealing Canadian airwaves.

The court decisions in Canada have been so one-sided that some of the pirates up there are now considering going completely legit. One confessed he was paying his taxes in preparation for coming out of the closet. Others have paid their taxes all along.

The loophole has been tested enough that people are treating it as a certainty. "It comes down to very bad draughtsmanship when the law was set up." says Ian Angus, a lawyer who defends many of the people accused of receiving DirecTV signals without paying for them.

"If the Canadian government says that 'No you can't market your product in our country', then DirecTV isn't in a position to complain that it doesn't have customers in Canada. It becomes a non-issue." Angus explains. They've lost nothing to the piracy because they shouldn't be getting anything from Canada in the first place.

Some pirates pin their hopes on the idea that the radio waves are free and owned by no one. If someone is broadcasting a signal through your house, you can do whatever you want with that signal including unscramble it. This ideal of a digital commons is an old tradition that dates to the early days of radio before encryption made it possible to close access.

Surprisingly, Angus dismisses this idea. "That doesn't hold any water.

There are private signals up there. There are certain things that the owner attaches ownership rights to. They want to be paid. The paperboy leaves a pile of papers at the end of my street. So I'm going to take one?"

If anything, Angus has built much of his success out of pointing out the rough tactics and overzealous behavior of the RCMP.

"There are some people who say that the seizures were intended to shut down the companies, but I don't know it that's the case. But certainly they've taken much more than they needed." he said.

"I have one case where they actually seized his screwdriver. When I got before a judge, the judge, he kept asking the crown, 'Why did you seize the screwdriver.' The poor lawyer couldn't answer that one. That probably turned the case toward me."

Many of the pirates are pursued with civil litigation, but some are prosecuted as criminals.

Reg Scullion, a Canadian target of an RCMP investigation, said. "I was charged criminally because they seized a bunch of my money. They seized some 6 million bucks. Apparently, the government would not be able to seize the money without a criminal prosecution."

Scullion's trial ended with the charges being dismissed– a common occurrence in these cases.

"If there's any evidence against you, [the judge] must send you to trial. If there's a total absence, he must acquit you." he says. The 10,000 or more smartcards and other tools for pirating the DirecTV signal were not evidence of a crime because intercepting DirecTV isn't illegal.

Today, Scullion likes to pose in a t-shirt proclaiming the RCMP to be the largest street gang in the world. He claims it came from the RCMP's own ranks, presumably made by a wise-ass officer trading on the same kind of rebel charm as Scullion. They would probably even be friends if the war for the control of content didn't put them on different sides. In fact, many pirates went out of their way to tell me that RCMP officers were some of their best customers. At the end of the day, they go home to a small house where they're just a little guy too.

Lawyers or Nerds?

Can the lawyers, guns and police ever shut down the pirates? Rissler is guarded. His legal team can point to a steady stream of police raids, prosecutions, and jail terms but there's only so much that can be accomplished by passing a law. If there's not broad support for the punishment, then the justice system starts failing.

"There's a lack of appreciation of intellectual property ... People who are law abiding citizens in all other ways don't have the same restraints when it comes to signals that they can't see. " says Rissler. The law may

provide some protection, but he predicts that the only hope for a perfect solution lies with the engineers and the technologists.

Angus is more direct. When asked to choose between legal and technical solutions, he says, “Oh, technical protection every day of the week. There’s all sorts of technology out there. The government isn’t in to properly into the business of deciding what people should watch. That’s just sticking their nose into business that’s not there. They know nothing about it.”

The Idea of the Attack Itself

The Black Sunday attack on January 21st was an excellent example of a technological solution to a technological problem. Most of these pirating tools became close to useless that day, at least for a short time. The attack permanently wrote data into a special part of the smartcard’s memory that could only be written once.

DirecTV buys the smartcard system from NDS, a relatively small company with over 1000 employees owned by Rupert Murdoch’s News Corporation. The company made its name selling the security system used in Murdoch’s Sky system. When DirecTV entered the American market, it licensed the technology from NDS. In many cases the engineers who developed the attacks against the pirates are largely employees of NDS. The company, however, will not speak on the record about the services it provides its client, DirecTV.

The system from NDS itself is quite sophisticated and scrambles every channel with a different key. Every time a person changes the channel, the DirecTV box needs to look up a different key for unscrambling the signal. To add an additional level of complexity, the system also switches the key every 8 to 30 seconds even if the channel isn’t changed.

To place another big roadblock in the path of the pirates, DirecTV bundled all of the software for managing these keys in a tiny chip embedded in a credit-card sized piece of plastic. These smartcards were designed to resist tampering and prevent anyone from taking them apart to see how the keys were created, changed or juggled. If DirecTV wanted to upgrade their system, they are also easy to remove and mail.

There have been three generations of smartcards used by the DirecTV system and the pirates name them by the prefixes attached to the serial numbers on the cards. First, there were the “F” cards which only controlled the access to the data. When the pirates figured out how to stop them, DirecTV recalled them all in 1997 and replaced them with the H cards. In 1999, DirecTV rolled out a new card known as the “HU” card. DirecTV itself refers to these as the P1, the P2 and the P3 cards.

The pirates made short work of the F card leading to its withdrawal.

The H card was supposed to withstand the assaults, but the pirates found a way to circumvent the security features. At the time I started writing this article, the HU card seemed pretty impregnable, at least to the average human. By the time I finished, freeware for reprogramming the card was common on the Internet.

"Every card has been compromised," Alientech told me. "There's really nothing they can do to stop us."

Of course, his statement must be put in perspective. The cards are compromised until Dave sends down an attack like Black Sunday and then the pirates must find a new way to attack them. And then the game begins again.

One pirate named Tallcans puts it in perspective, "Free TV? Nothing in life is free! You want Free TV you will need a complete DirecTV system. (Aprox $55) Now do you want to program the cards yourself? A valid H card on Ebay goes for about $250-$300. Now you need a programer, let's say $70 and a unlooper for those pesky ECM's or for when you screw something up $150. Do you want to test without putting your card at risk? You need a emulator $75 + at least a 486 computer with two COM ports. You can find them cheap. That's $650 to get going. Then let's say you want to test with your BS (Black Sunday) card in the receiver you need a DPBB/boot loader that's $100-$150."

The sophistication of these attacks can be surprising. In the old days, The pirates figured out a set of instructions that would let them seize control of the H cards and reprogram it. They accomplished all of this with a small box that connected the serial port of a basic PC directly to the smartcard. Although this setup was often called a "smartcard programmer", it is little more than a tool that passes the signals from the PC to the smartcard. The software on the PC did all of the work.

At the beginning, the pirates found a backdoor that could be exploited by sending the right combinations of signals. Some say that the backdoor was left in place by the engineers in order to make their life easier if they made a mistake. Others say it was just a bug. In any case, the pirates programmed their PC to exploit it and send new instructions to the smartcard. They could reprogram it to do anything they wanted, a power they soon used to give themselves access to all of the channels all of the time.

That success was fleeting and fragile. DirecTV soon found ways to test for new pirated software installed on the smartcard and re-reprogram the reprogrammed cards sending them into infinite loops. When you inserted the card into the smartcard programmer, it would just sit there acting like an ice scraper.

The basic ECM from DirecTV checks the software buried inside the card like a virus scanner checks for malicious code on your PC. In a sense, the metaphor is a bit backwards because the ECM is a virus-like bit of code that's downloaded from the satellite into the smartcard. The pirate code is

sitting around running the show.

Every time the scrambling key is changed, DirecTV gets to download a small piece of code to execute. In the case of an ECM, the software tells the DirecTV box to put aside decoding the signal for a second and check the memory for pirate code. The ECM scans a few important locations to if the wrong instructions are there. If pirate code is found, the ECM tries to disable the card.

The early ECMs unleashed by DirecTV reprogrammed the card by changing a memory location visited soon after the card is powered up. The minor change was enough to create an infinite loop that sidetracked the card everything it started. Once these cards hit the loop, there was nothing a regular card programmer could do to pop them out.

This led the pirates to develop a new tool known as the "unlooper." It is essentially a sophisticated version of the smartcard programmer that is bundled with a built-in computer chip of its own for controlling the power supplied to the smartcard.

The extra chip in the unlooper is a relatively cheap embedded processor with flash memory know as an Atmel It's sort of a smartcard without the card. The chip's job is to exploit one weak spot in the armor of the smartcard by lowering the voltage entering the smartcard at the right time. When that happens, the smartcard malfunctions and fails to execute the instructions.

The pirates call this operation "glitching" and they discovered several years ago that there were many places where the code could be "glitched". One of the popular moments is about 575 steps from the moment the smartcard is powered up. If the power dips from the regulation 5 volts to something around 2.2 volts, then the basic security check run when the card starts up gets ignored and the loop disappears.

Glitching requires an intimate knowledge of the software being executed by the smartcard so the power can be lowered at the right moment. Imagine an old house with creaky floorboards. A burglar breaking into the house is bound to step in the wrong place and wake someone up. But a teenager sneaking back in at 2am knows which steps to avoid. The Atmel chip is programmed to lower the voltage at exactly the right time causing a glitch that skips over the creaky alarm software.

Glitches like these happen all of the time and send electronics into strange paroxysms. The line spikes from refrigerators and air conditions crash computers all of the time. Some think that the pirates discovered glitching when they're powered dimmed in the middle of nowhere in Canada. Others think it was just a smartcard engineer who used the technique to debug the chip. No one is certain, but it sure is powerful.

Of course, glitching has limits. The atmel chip controlling the power line is never completely synchronized with the smartcard. Reg Scullion explains, "A glitch has a carry time. If you glitch 32 hex bytes, that would be

difficult to overcome. You could glitch 6 bytes here and 8 bytes in several places in the ROM. But large blocks would be virtually unglitchable."

Exploiting this problem with electronics was probably never anticipated by the designers of the DirecTV box. Or perhaps they figured that the pirates would never be savvy enough to buy Atmel chips and program them to dip the power at exactly the right moment. Or perhaps they never figured that the folks who were smart enough to dip the voltage wouldn't develop a business of selling the unloopers by the truckload.

One engineer working for DirecTV told me, "Do you realize how hard it is to make a device for $70 and market it?"

Some pirates even think that the glitching technique was left in place deliberately by the chip designers as a debugging technique. One former digital television engineer who is now a serious pirate explains that the back doors are usually inserted by the engineers to help them debug the circuits.

"Serious design problems were averted only because we, the design engineers, were forward thinking enough to provide a backdoor into the [circuit] so as to accommodate faulty code." he explained via email.

He also explains that most design engineers are usually forward thinking enough to close the door before shipping the product.

Fry Time

As 2000 drew to a close, DirecTV found itself in a strange position. They made a nice profit from selling a television signal to the 9.5 million legitimate customers, but it was clear that the pirates were becoming more and more sophisticated. DirecTV realized that it was quite possible that there could be more than one million pirates out there who could do anything they wanted with the H cards, but no one could be sure.

DirecTV had a number of choices. First, they could simply ignore the pirates. Tracking them down and prosecuting them cost money. The Canadian courts seemed to take a perverse glee in twisting the nose of the big American imperialist corporation. DirecTV lost nothing when yet another satellite dish started receiving their signal. The advertisers who bought time on the channels like MTV certainly didn't mind that their message was seen by a few extra eyes.

On the other hand, content providers charge DirecTV by the viewer and piracy cuts into their revenues. The DirecTV executives hate to be across the table from the HBO executive with a print out from a website offering free satellite access. And Dave himself hates to watch revenues falter: DirecTV practically gives away the dishes in the hope that they will recoup their costs from the monthly payments. People who buy the dish and fail to subscribe never pay off this debt.

Another solution would be to simply recall all of the H cards and replace them with the HU or a newer model. But upgrades are costly. Even at $1 per card, recalling 9.5 million units is a big charge for the books. Besides, there were already plenty of rumors about weakness in the HU card that began circulating in late 2000.

The third solution was to fry the cards as they did on that Black Sunday by downloading a new ECM. Dave may not be able to control the Canadian courts or the pirate websites, but they can control the data flowing through their satellite.

Each of the ECMs sent squeals of pain through the pirate community when it first appeared. In time, the pirates would develop yet another counter solution to work around the code. They pioneered "stealth scripts" that would silently watch the cards and block out any attempt by Dave to send them into a loop. They found ways to protect their "access tiers" (the blocks of channels) and prevent them from being wiped away. When Dave came looking for a particular stealth script the pirates installed on their cards, the pirates developed randomized mutating counter-counter-Stealth versions that would change in slight ways. If DirecTV sent an ECM looking for a particular stealth script, they wouldn't find it because it had already mutated. The pirates found ways to be certain that they could keep getting everything, the local channels, the football, the porn, the music, and everything else.

By the end of 2000, DirecTV realized that ignoring the piracy just wouldn't work. Swapping all of the cards was too expensive. They needed a newer and better ECM and luckily their engineers had a big one ready.

The problem they faced was simple. The smartcards acted like little computers and the pirates discovered how to install whatever software they wanted on the machine. Their stealth scripts could block out the commands and keep the channels flowing. DirecTV needed an even more dramatic way to retake control of the smartcard and ensure that only their software was on the card. In November 2000, they started launching their plan.

Dave began with a complex collection of software updates for the cards. The cards all came with a mechanism for distributing large, new blocks of software to the card. In the past, Dave had sent down 26 or so to fix bugs and add new security solutions. This time, they downloaded three sets of updates that took their place on the card. By November third, three sets of 9 blocks of code were distributed to all of the chips.

The pirates were at a loss. The veterans wanted to keep the updates off the cards, arguing that anything from DirecTV would be aimed at shutting them down. All the updates could do would be block their tools.

Others speculated that the new software was really just a way for DirecTV to offer more services. The company was publicly describing a tool it called "Wink" that allowed couch potatoes to push a button and receive

information about a product being advertised. Perhaps these new blocks of code were there to help Wink?

Many pirates, however, felt a strange sense of foreboding because the updates gave Dave a brand new tool the pirates called “dynamic code”, “dynamic nanocommands” or just “dynamic nanos” for short. Every time the key changed, Dave could insert a short instruction to be executed by the smartcard. Some pirates called these “nano updates” because they were just a small bit of software that was run once and discarded.

The power of the nanocommands is limited because it can only invoke software that is already on the card. There are only a few short bytes in a nanocommand and they can only encode so much piracy-fighting information.

The new updates strengthened the nanocommands by including the power to check arbitrary regions of the card. The new solution was dynamic and this expanded Dave’s power. It’s not much different from a security guard getting an x-ray machine. Before, the guard would need to feel each bag and search a few. Hand searching, however, was limited by time, energy, and patience. A new x-ray machine lets the guard scan complete bags and focus on particular ones if necessary. Dynamic code gave the nanocommands the ability to scan large parts of the card for pirate code quickly and easily.

The new nano assaults expanded the power of the searching that could be done after each change of the channel. Every nano could now be tuned to check any part of the card’s memory by computing what is known as a hash function. The term is common in cryptography where it is used as a part of a digital signature. A hash function examines a block of data and produces one short number that can act as a surrogate of the data. If any bit is changed, the result of the hash function should change too. In this case, Dave could check blocks of the smartcards memory by hashing the block and checking to make sure that only the correct value emerged.

If the nano hashed a block of memory and found pirate code, Dave could just shut down the card. In the past, Dave would need to send down a special software upgrade to search particular regions. Now, he could change the region every time someone changed the channel.

After the last block of new code was in place, the company began firing off nanos that checked to make sure that the updates were available. If they were, then they acted like the blood of a lamb above the front door. Those smartcards were passed over. If the updates weren’t there, well, then it was time for the card to die. It was all kind of circular.

The result from the nanocommand could also be used to determine the key. This dramatically limited the ability of the card reprogramming pirates. Adding extra instructions to turn on extra channels would corrupt the hash function which would, in turn, produce the wrong key value. The channels might be operating, but the key for decoding them would be

wrong.

The company held its fire until all of the pieces were in place. Then, on January 21st, they launched an all-out assault on the pirates and started frying the H cards. They released dozens and dozens of nanos looking for all particular kinds of pirate code.

DeeEssEss wrote, “As of 8:30 EST, DTV sent down a clone kill. This type of attack is not script related. If you have a clone, there is a very big chance it is down, or will soon go down.”

The clone kill was an old ECM that was designed to stop people who posted a legitimate card’s ID number on-line so others could clone them. DirecTV kept track of these and regularly sent a list of expired IDs and sent them into endless loops. This time, the damage was permanent.

Then, DirecTV began launching a “jump point ECM” that looked for stealth software installed on the smartcards. If it found a card with malformed jump points that took the software to the wrong place, then Dave burned it. These usually occurred when the pirates installed special filtering software to block out ECMs by jumping to a different location.

After that, Dave followed by looking for people who had inadvertently activated too many channels. DeeEssEss wrote, “DTV is working VERY late tonight.”

This time Dave did not spare any of the cards. Whenever a nano discovered a suspicious piece of code, it would start writing new information to the write-once section of the memory with addresses 8000h-8003h. When the card starts up it checks location 8000 early in the boot sequence and starts looping if it doesn’t find the value 33h. The nanos wrote new values to this spot with permanent marker. No unlooper could ever delete it.

That Sunday, DirecTV also allowed itself a bit of fun. In the middle of the nanos, the company also broadcast inserted the message “GAME OVER” just for the pirates who logged the data stream.

Rebirth

The cards were permanently fried on Black Sunday, but the pirates were resilient. The experts started studying the problem, the websites cautioned patience, and the average satellite pirates went off to Walmart or Best Buy to purchase a new dish with a replacement smartcard. Many of the stores which sell DirecTV dishes ended up hosting impromptu meetings for the local pirates in the aisles that evening as everyone went off to look for a replacement card.

Many couch potatoes went legit that night because it was easiest path. They took one look at the cost of possible fixes and just stopped buying pirate cards. Many realized that they were spending hundreds of dollars

on stop gap hacks that were quickly being erased by ECMs. Sure, the pirates were very clever at finding ways to work around whatever DirecTV delivered, but was it really worth the time and effort? After Black Sunday, many decided otherwise.

Some pirates claim that DirecTV scheduled the ECM to help it in negotiations with Rupert Murdoch. For most of the time I've been working on the article, General Motors has been trying to sell DirecTV to Murdoch. The deal may or may not be completed by the time you read this because the negotiations are taking some time. The ECM shut down pirates and sent them scurrying back to legitimate subscriptions boosting the revenue and the price.

Vista, the pirate that runs the website `www.watchintv.com`, told me, "We knew it was coming. They were obviously going to impress their buyers. It was conveniently when they were talking about selling the company. Might as well juice up the sale and make it look like you've got the pirate market under control."

DirecTV refused to discuss this or any other theory about the timing of the ECM. They run plenty of ECMs and they run them all of the time. Black Sunday was just the latest and the most sophisticated. Sure, it may have come the weekend before the Superbowl. But that was just a coincidence. DirecTV makes no comment about the scheduling of the ECMs and considers the matter to be private.

Others thought the Black Sunday attack was just a gift to the pirates. Every time they sent down an ECM, the couch potatoes needed to go off looking for a new solution.

"We have an incestuous relationship." explained Alientech. "We give them good press by giving a hackable system so everyone buys them. But only the really good hackers know how to exploit them."

In his mind, the piracy is a selling point that draws more people to buy the DirecTV in the hope of getting free television. Then the lazy become legitimate subscribers after they grow tired of buying unloopers, programmers, boot loaders and who knows what else.

After Black Sunday, the dealers and the true believers began to regroup. In the beginning, the discussion on the websites dropped to next to nothing. There was nothing to say and nothing to even speculate about. Everyone assumed that Dave had won.

Not everyone was defeated. Over the next few weeks, though, news of a solution began to emerge. Some bright soul realized that the 8000 block of memory may be permanently fried on Black Sunday, but there's no reason why the processor needed to stop there every time. Why not glitch over that spot every time the smartcard booted?

Within three weeks after the fateful Sunday, the pirates were back in business selling a special device that many called a "boot loader", although some used the more risque "card condom". This was a special card that

slipped around the H card and intercepted the signals going between the set top box and the card. The embedded processor on it that monitored the data flow and whenever the 8000 block came around, it would lower the power and glitch over the moment. Zap. All it cost was about US$70-100 and you were back in business.

The news of the bootloaders spread widely and several dealers claimed they sold tens of thousands of the boards to their customers. Sure, Dave could fry their cards, but the pirates could find a way to glitch right over anything Dave could send them.

The pirates kept patting themselves on the back for several weeks. They had developed a nice cheap counterhack to Dave's brilliant Black Sunday assault. They were raking in the money selling the fixes.

Hacking HU Cards

While some pirates focused on selling bootloaders and emulator cards, others turned their efforts to the previously unhackable HU card. Near the end of 2000, a new solution for hacking HU cards appeared and pirate dealers began selling an Atmel chip containing the "HU Loader" for $3000 to $5000. The sales pitch explained that this was really quite a deal– anyone could recoup that money by reprogramming 30-50 HU cards and selling them for $100 each. Everyone was entranced. After the Black Sunday hack, this was one of the few games in town.

On March 12, the news got even more exciting as people woke up to find must of the HU Loader code available on the website `www.hack-hu.com`. The owner, DeeEssEss, explained that he was giving the software to the world for free in the hope of inspiring new pirates everywhere to break their way into the HU card. Suddenly the price of an Atmel chip containing the HU unlooping software dropped to $30. Anyone could get it off the Net for free. Boom.

Many dealers were livid. They were pirated by a pirate. Their livelihood was irreparably damaged. Their cash flow was in danger. All because some pirate stole their code.

Some of the more philosophical pirates thought this was just bad for the community. Risestar wrote on his site, `www.pirateden.com`, "The Hu loader operates something like a combination unlooper and card programmer for the Hu card. An unlooper, not in the fact that it can fix or clean cards, but that it seeks out and exploits "glitch points" on the Hu card. Once it has successfully glitched' the card, it then loads a 3m program [for accessing all the channels] onto the card. Take away the glitch points, and there is no way to program the card. So, for the moment, the Hu loader is the only way to program a card. Now, it is certainly possible to send an update down to the Hu card which would close those particu-

lar points on the card. Bingo. No more programmed Hu cards. No more alternative to H cards."

In some pirates eyes, the new pirated pirate software would just make life easier for Dave. All Dave had to do was wait a few weeks for everyone to start playing with the HU Loader. Then, perhaps the day before a big sporting event, he could just fry the cards again.

That's exactly what Dave did. On March 21st, Dave unveiled a brand new class of ECM that wiped out one popular script called Dynaceptor. This bit of dynamic code would sit comfortably on the smartcard and intercept all attempts to wipe out the extra access the pirates had granted themselves. It relied heavily on the fact that the ECMs would not set the byte containing the parental guidance rating for the program. That changed on March 21st and anyone caught using the Dynaceptor had their card fried, Black Sunday style.

Then on Sunday, March 24, Dave unveiled a new round of nano ECMs that kept checking the data at 8000h. Sure, the pirates could glitch past this location when the cards was starting up, but they couldn't fix it permanently. Now, Dave is regularly checking this point too with nano hashing ECMs. Every time anyone changes the channel, they might find their card checked to see if it was fried during Black Sunday. Glitching the card when it started was one thing, but glitching it every time a new nano came down was much more complex.

On March 29th, Dave followed with new ECMs that started frying the HU cards. No one really understood what happened, but suddenly those hacks stopped working too. It was a full-frontal assault that just happened to come during the NCAA basketball tournament.

Many pirates agree that the best thing DirecTV can do for itself today is launch a steady stream of constantly changing ECMs. The smart pirates may still find ways to evade them, but most people will be discouraged to discover that their satellite reception keeps getting fried. When they start counting up the money spent on unloopers, card condoms and help, they'll realize that going legit is a better proposition. This might not stop the hard core hobbyist, but it will remove much of the financial incentive.

There's every indication that Dave feels the same way. When I visited the company's nondescript building next to the LA International Airport, I was warned explicitly that the company did not want to comment directly on any of the particular tactical moves it made. We could speak about the battle in general, but talking about the ECMs in specific might let some information leak and "provide aid and comfort to the enemy."

The ECMs are, in a sense, just another way to convert the pirates into paying customers.

To Dream the Unhackable Dream

The technical fixes are glamorous and well-targetted. There's no need to bother with a judge, a jury, a prosecutor, or debates about legal loopholes. Illicit instructions on your smartcard mean you're guilty.

Many wonder if there's any way that the smartcard creators can't just turn the knob a bit further and zap everyone from the beginning. If they can blitz everyone on Black Sunday, why can't they build something that does it every day of the week?

This righteous efficiency, though, is beyond the capability of machine intelligence. The chips on the smartcards are as fickle as mistresses and politicians. If the definition of an honest politician is one who stays bought after being bought, then there are no honest smartcard chips. Any instructions in the memory can be rewritten by anyone. DirecTV wrote the original version, the pirates modified it, DirecTV rewrote them again on Black Sunday, and the pirates started rewriting it again. There is no loyalty in the chip world.

Dave Baylor is circumspect. He says, "As a practical matter, security is a balance between convenience and cost. We could go to an NSA quality security system for our set top boxes, but the boxes would cost $17,000 to $20,000 a piece. Or we could spend no money on security and save some money. What we've done is the right economic balance and the costs and attendant capabilities."

The smartcard designers continue to try to build this perfect cage as cheaply as possible. They worry about how to thwart attackers who arrive with scanning tunnelling microscopes for mapping the circuits, power meters for measuring their consumption, diamond dust for grinding off layer by layer, metal shielding to stop radiation and thousands of other techniques.

Blocking each of these loopholes stops the pirates for a time, but another one always emerges. One engineer told me with quite a bit of sadness in his voice, "The HU card has twice the memory [of the H card], twice the software and probably twice the bugs."

Even if the bugs aren't available, glitching gives the pirates the ability to skip over any instructions they don't like. Any security mechanism programmed into the card can be glitched over within limits. It is hard to glitch past long sequences of instructions with any precision.

On the other hand, the new dynamic code gives DirecTV a great tool, albeit one that needs to be actively used. The pirates can't reprogram the card at will because DirecTV is constantly hashing the memory looking for illicit code. The dynamic nanos gives DirecTV back control over the card. They can make sure that only DirecTV approved instructions are running at any time.

Together these two innovations tend to balance out. A smart, capa-

ble glitcher can work around anything Dave dreams up. At the same time, Dave can send hashes to target anything the pirate community creates. The result is a high-energy game that rewards only the fastest minds. The hobbyist after technological puzzles may love the action, but the businesses suffer. Keeping up with DirecTV takes more work. Legitimate subscriptions look better and better.

Emulation

The pirate community has one more ace up its sleeve. If the pirates know the entire contents of the smartcard, they don't need to use this information to glitch and reprogram the card. They can simply emulate it by teaching a PC to act and think like the smartcard.

Some pirate manufacturers sell a special board that plugs into the DirecTV set top box, hijacks the signal and reroutes it to a PC. This PC contains a copy of the software running inside the smartcard and it simulates everything that the smartcard does with one exception. When the Black Sunday nanos came down, they still fried the emulated memory at 8000, but the effect isn't permanent. The PC can just wipe it clean and begin again. The pirate has total control over the PC and can selectively erase the actions of DirecTV.

Some pirates think that emulators will ultimately make it impossible for DirecTV to ever fry anything again. The emulator can be programmed to ignore any ECM that comes down while decoding the video stream correctly.

There are some problems with emulators. Many pirates don't like them or trust them because there's little to sell. Others complain about the aesthetics. Hacked smartcards look exactly like legitimate cards, but emulators have cables running from the set top box to a PC.

DirecTV can also attack emulators if and when they can identify bugs in the emulator software. Emulator programmers make mistakes and leave holes just like the smartcard programmers who built DirecTV's card. If DirecTV finds areas where the emulator behaves differently from the smartcard, they may be able to crash the emulators routinely. This may not inconvenience the emulator authors for long, but they will drive the casual users nuts.

One of the biggest problems facing the emulators is the lack of a complete listing of the software running inside. The key scrambling the signal is actually computed by a special custom designed circuit that is much harder to reverse engineer. The basic part of the chip behaves much like a generic CPU, but this extra section is optimized to compute the key.

The pirates who build the emulators don't know how to make the PC act like this special circuit. This roadblock didn't stop them from building

an emulator. They simply took a generic H card and reprogrammed it to do nothing but compute this special key. The bulk of the work for juggling access tiers, pay-per-view codes, and other bookkeeping is handled by the PC running the emulator, but the smartcard must still be around to create the key. The solution is both a work of genius and a greesy, inelegant cob job at the same time. It also contains the portent of a dangerous ending.

The Future

Can DirecTV ever really control their data stream? Will any content king ever be able to keep their valuable information on a short leash? Will writers, actors, producers, and directors find themselves marching slowly and steadily toward poverty?

Writers like endings almost as much as they like writing about wars. Endings have gravitas and closure. They tie all of the themes, threads and discursive thoughts into a stunning climax that unfolds across the reader's mind like the final battle of Godzilla and Mothra. One editor told me to end this piece with the taunting message that slipped out over the DirecTV ether: Game Over.

Alas, wars never really end with a bang. The bloodiest battles are often near the beginning. Sometimes the wars last long past armistice and flare up again like WWI and WWII. Even Godzilla and Mothra keep coming back. At last count, there were 2X editions in the battle to end all battles.

It would be nice for DirecTV, if I could report that the events of January 21 ended the game of piracy. The pirates stumbled and fell, but then recovered with surprising resilience. The boot loaders that restored the previously dead cards appeared within a month. The emulators are an even greater threat and give the pirates more flexibility than ever before.

But it would also be nice for the pirates, if I could report that their technical exploits proved that the little hacker would always succeed. They may have found a backdoor in the card, but DirecTV managed to plug it. Every time the pirate found a new hack, DirecTV found a counterhack soon after. The new dynamic nanos gives them more power and more flexibility to dictate the contents of the card than ever before.

None of our institutions can offer any guarantees. The law has been a unsteady ally. While the police raids in the United States have driven the business out of easy view, the legal outcome in Canada has been troubling. The Canadian pirate movement is fueled by a mixture of patriotism and a devotion to free speech.

Nor can technology guarantee much. The current system works quite well at keeping most of the people honest. But eventually, it will wear thin and require replacement.

Historically, selling information at a premium over the distribution cost

is a difficult strategy. Most publishers print newspapers and magazines with vast economies of scale. Many newspapers and magazines don't cost much more than the cost of the paper, printing and distribution. Advertising is responsible for paying for the content creation. Even book publishers quickly issue paperback editions when demand is high enough. The winners always end up being the low-cost producer who gets biggest, fastest.

In many ways, DirecTV is already pursuing the same strategy as the print media. The satellite distributors may not have perfect laws, they may not have perfect technology, but they have the a well-tuned, low cost device that provides superior service at a low price. The satellites may cost a fortune, but once they're flying every new customer costs little. More customers mean lower average costs and higher profits. Cable companies need to keep stringing wires, climbing poles, fixing splices and drilling through walls.

While the pirates perform amazing feats of engineering derring-do, the pirate life ends up costing more than most legitimate subscriptions. If it wasn't for the high-priced information like pay-per-view, the socially conflicted information like pornography, and the legally constricted data like local television, there would be no reason to pirate the signal. Piracy is not so much a battle against DirecTV as much as a battle against the forces of censorship.

Until the laws change, DirecTV must fight a long, drawn out guerilla war against a bunch of techno-savvy rebels who are willing to ignore a few laws to get the television signal. Baylor concedes that the company can't stamp out piracy, but he is confident that they can make it unattractive enough to sell more legitimate subscriptions.

The pirates, he explained, "will get very little use out of [piracy]. We'll make it economically uninviting. If their market dries up in three weeks from the introduction of the device, there will, realistically, be a small window of opportunity for the hackers."

Of course, that small window of hope is just enough for a young programmer with nothing to do during the Canadian winter.