```
-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
    (NNNNNN. (NN)                  (NN)      (NN)   (NN)           ___                   NNN    NNNN)   JNN   .NN)
    (NNNNNNN (NN)    ___.    ___   (NN) ___  (NN)   (NN)  .___    NNN     .___     .__ NNN   JNNNN)(NNNNN NNNNN)
    (NN) NNN (NN) (NNNNNN  (NNNNN) (NN)(NN)  (NN)   (NN) JNNNNN.(NNNN) NNNNNN.  (NNNNNNN  .NN4NN)`"4NNN ""NNN)
    (NNL_NNN (NN) NNN (NN) NNN (NN (NN)NNN   (NN)   (NN) NNN (N)`NNN"`(NN) NNN (NN) NNN  JNF(NN)   NNN   (NN)
    (NNNNNN) (NN) NNN.JNN) NNN (NN (NNNNN`   (NN)   (NN) NNNL/"` NNN  (NNNNNNN (NN) NNN (NN`(NN)   NNN   (NN)
    (NN) NNN (NN) .NNNNNN) NNN     (NNNNN)   (NN)   (NN) `NNNNN  NNN  (NNNNNNN (NN) NNN NNN_JNNL.  NNN   (NN)
    (NN) NNN (NN) NNN`(NN) NNN (NN (NN)NNL   (NN)   (NN) __`NNN) NNN  (NN) NNN (NN) NNN NNNNNNNN)  NNN   (NN)
    (NNLJNNN (NN) NNN (NN) NNN (NN (NN)(NN.  (NNNNN(NN) NN (NN) NNN  (NN) NNN (NN) NNN NNNNNNNN)  NNN   (NN)
    (NNNNNNF (NN) NNNNNNN) (NNNNN` (NN)`NNL  (NNNNN(NN) 4NNNNN` NNNN) NNNNNN) (NNNNNNN     (NN)   NNN   (NN)
    `"""""""  `""`  ""``""`   """   `""` """ `"""""`""`   """     """`  `"""    `"" """     `""`   """   `""`
-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_-_
```

"BLACKLISTED 411 .NET"

Edition 1

10.14.2005

-=-

Table of Contents

-=-

[1] ==Introduction to Online Magazine Format==

Well first off, we would like to welcome you to the first ever, monthly edition of BlackListed411. Since this is our first-ever online magazine, we are going to give a brief explanation about what you can expect from this publication. Just to clear the air, this is not an online version of the print magazine version of Blacklisted411, and won't contain any of the articles published there. The main purpose of the online edition of Blacklisted411 is to fill in the gaps between the quarterly issues and provide small, yet informative articles for your entertainment and education.

**The Articles*

Since this is the online edition, no payment will be provided for articles, but we encourage you to use this as a means of sharing information you think may benefit the hacking community.

**Article Guidelines*

- 1000+ words
- Article may not be published on other sites (It is redundant to republish an article)
- Proper grammar is appreciated
- Most importantly, please don't plagiarize. Site your sources!

**How to submit*

If you already have an article written, please proofread it (for those nasty mistakes we all seem to make) before sending it to me. All submissions should be sent to, ustler@blacklisted411.net. We will respond within 2 to 3 days (maybe sooner). If we are unsatisfied with your work or feel that it needs some improvement, we will provide you with an explanation and give you the opportunity to correct the problem before resubmission.

**Publish dates*

We expect to release the online edition on the 15th of each month. Release date may be altered with or without notice, depending upon support. Please note that the support of the community is crucial to the success of the online edition.

**Layout*

First off, we will have an introduction giving you up to date information on how the magazine is doing, and what to expect in that edition. This will be followed by our edition quote, which is randomly chosen. After that, we will have the tools section. Here, you can find new and interesting tools to help with pen testing and securing vulnerable machines. Then we have the links section, which will contain some random, yet interesting links for you to browse on your free time. The main portion of the magazine will be the articles section. Each issue will contain anywhere from 3-5 articles, organized by title name. We then have the product and services review section, which is self-explanatory. The "In the News" section is an area where we have a brief commentary about a current issue. The included cryptogram is a fun, yet educational way of learning simple cryptography. Eventually, it may turn out to be a contest, but we are unsure of when and if this transition may take place. The favorite photo section is either a user submitted photo, or a photo that we find in our spare time. Please note: this is a security/hacking related magazine. No porn will be published under the favorite photo section. Last but not least, credits and a shout out!

**Conclusion*

Well, that's pretty much it. If you have any questions, feel free to drop me an email and ill get back to you as soon as I can.

[2] ==Edition Quote==

"There is no security on this earth. Only opportunity"

Douglas MacArthur

[3] ==Tools==

Pentesting tools
Metasploits - http://metasploits.com

Live Security CD's
Auditor - http://new.remote-exploit.org/index.php/Auditor_main
Insert (Incident Handling) - http://www.inside-security.de/insert_en.html
Helix (Forensics) - http://www.e-fense.com/helix/
Knoppix STD - http://www.knoppix-std.org/
Pentoo (Gentoo Pentesting CD) - http://www.pentoo.ch/
Whax (Previously known as Whoopix) - http://www.iwhax.net/

[4] ==Links==

@stake Bluetooth paper - http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf
Astalavista (Everyone should know this one) - http://astalavista.com/
DIY Wifi Antennas - http://www.usbwifi.orcon.net.nz/
Doom9 (Your DVD Backup Source) - http://www.doom9.org/
NewOrder (One of the Best Sites I've seen) - http://neworder.box.sk
Phrack (Another, well know, published hacking magazine) - http://www.phrack.org/
Phreak (Phreaking/Hacking/Anarchy site. Trust me this is awesome) - http://phreak.com/

[5] ==Articles==

[a] Wireless Network Security by *Dr. Fibes*

Wireless network security

By Dr. Fibes

==========

OK. You've got that cool wireless router. You've got the cards for all of the computers in the house. No more wires, no more crimping on connectors, and even better, no more troubleshooting poorly crimped connectors (yes, it happens to everybody). It's the new millennium. What could be wrong with that?

How about the wardriver driving down the street just looking for access points like yours? The spammer, just looking for an open connection to send out 500,000 emails. And guess who gets left holding the bag at the end?
Or maybe he's looking for your data. That Word doc you've got with all your passwords and credit card numbers (don't do that!). I can't tell you how many times I've been to acquaintances solving computer programs and noticed a file named password.doc on there somewhere. Pwd.doc and passwrd.doc are popular too. Folks have been convicted of exactly these things, it happens. Many more have done it and got away with it.

Perhaps it's just a neighbor sneaking in to get free broadband. And he's slowing your MP3 downloading to a crawl. I've never heard of anyone being prosecuted for this, so it's pretty tempting with broadband clocking in at $30-40/month.

While the vast majority of wardrivers are just out there for fun and never really hook up to your system, why take the chance?

I don't know. Maybe it's just me. But every time I hook up a wireless system it seems I have to dink with it for awhile. It can be frustrating and time-consuming. It seems the best way is to leave all the default settings (zero security) in place while you just get the darn thing running.

If you're like 2 out of 3 people, by the time you finally get your remotely connected computers running, you're so excited about the magic of wireless access and the fact that you've finally got it going that you say to yourself "I'll do that security stuff later." Of course, for more than 66% of the folks out there in suburbia land, later never comes.

Hey, don't take my word for it. After you get your stuff working, snoop around. All of the wireless cards have a little utility that will show the "available networks." Or they at least use the operating system wireless utility, same thing. Chances are you'll see at least a couple of available networks in there besides your own. Unless you live off by yourself like the Unibomber.

With odds like 2 out of 3, chances are good that you can hook up to them no problem. Maybe with a commercial or homemade external antenna added to improve reception, though often in the close quarters of the city even that's not necessary.

WEP? What a joke, don't bother; it's not even a factor. And, even scarier, you can have more sophisticated WPA encryption turned on and still be tapped into.

There's a plethora of stuff out there that is capable of breaking the encryption code. It just logs thousands, sometimes millions of packets and then it's able to sniff out the code. Yikes! Good thing you got that MIMO extended range capability.

The best way to avoid becoming a target is to learn to hack these systems yourself. Then you'll know how best to protect yourself.

Everybody knows that although locks don't keep people out if they want in, most thieves will take the easy hit over one that is secured. Same thing applies here: hackers are so clever and insidious, it's nearly impossible to completely secure anything. But somebody looking for a wireless link is going to drive a few houses more down the street where someone's got an open system, rather than spend time trying to figure out how to break into a secure system. So you just put up all the barriers that you can in the hopes that is what they'll do.

A good start is to install NetStumbler. This is an old favorite of wardrivers. It's a ready to go sniffer that gives loads of information about any networks in the vicinity. Even though it's a wardriver, there's no reason you can't just run it on your desktop at home. You'll see what the guy who's driving down your street sees, as many wardrivers still use it.

Another benefit of NetStumbler is that it's a nice, pretty and compiled Windows program. There's better wardrivering software out there now (Kismet for one), but many have to be compiled and configured. With NetStumbler it's no muss, no fuss, just install it, start it up and get a window into the RF world. Of course, if you don't mind compiling by all means, try some of the other wardrivers.

Then if you want to see what your data looks like to a hacker, get Ethereal. This is a great, free packet sniffing program. Many wardrivers use this to view what people are sending/receiving. I used to use it when I was hacking into Ebay to scrape information off of their CGI pages (no longer necessary since they've got the developer API's. If you can't beat 'em, join 'em, I guess).

Now that you see what they see, what do you do about it? Here are some general guidelines to start:

1. Change the default password. The wardriver knows the default password on every available AP, so if you don't change it you've given him the key to the front door. He can configure it any way he pleases, even locking YOU out.

2. Change the default SSID and don't broadcast your SSID! Although it's a small thing, it's one more barrier. Do you really need to broadcast your ID to the other computers in your house? You know what it is. This is a feature for open-system Wi-Fi hotspots, not necessary for the average home.
3. Don't use your home address or name or anything else identifiable with you as your SSID. Duh! But many people do exactly that.
4. Activate the wireless security. It's turned off by default (?). Don't use WEP at all! It's easily broken. Unless that's the only thing it has. Use WPA or even better on the new systems, WPA2. They can still break it, but it's a lot more trouble. Use a passcode that is 16 or more characters and numbers in length and is not a dictionary phrase (make it meaningless, impossible to guess).
5. Choose to allow access only to trusted stations and limit that to the computer(s) you know of at your home.

Have you heard of warchalking? They say that back in the day, 'gypsies' (whatever that is) would make secret marks with chalk on the street or sidewalk in front of your house if you were a 'mark' for a free meal, sucker for substandard work, etc. Then other 'gypsies' would walk down the street and know who to hit. Also the origin of the term 'mark' I believe, don't quote me.

The wardrivers do a version of this by posting a picture of your house and details about your wireless on the net. This is NOT cool if it's you.

Here's the most famous site for that kind of thing:
http://www.wigle.net/gps/gps/GPSDB/onlinemap/

You can go there and put in an address, it'll even show you a map with the 'chalked' *marks*. Hopefully, you won't see your place there. It's very comprehensive.

Er, I don't know about you, but it makes me nervous to input my address to see if they've logged me though. You can just look in your general area. Whew! I just went there and checked for my street (I didn't give the address, only the street). There's three logged on my street, I'll have to look up the GPS coordinates. I told you it was comprehensive.

Will this make your system secure? Nah. But it'll certainly make it more hassle than your neighbor's, get it? Or help your neighbors too; let 'em drive down another neighborhood. Bound to get you a meal or something. Like their old tech products in the garage.

And I didn't talk at all about the firewall, that's a whole different subject. Most AP's have a built-in firewall, you'll definitely want to use it. Don't mistake my brevity for a lack of interest in that area.

If it's security you're looking for, sorry, you lost all that when you popped out of the womb. That internet thing, it's so full of holes, I'm amazed every day that we're still on it. We can only do all we can and pray for the best.
Just don't be an easy target.

Editors Note: Airsnort!!!! If you're looking for a cool way to load Linux with all the tools pre-installed, check out Whax or Pentoo

[b] The Real Problem with Real ID by *Ustler*

The Real problems with Real ID
By Ustler
==========

In today's society, terrorism has become a major concern. To help prevent acts of terrorism, congress has passed a myriad of laws which have violated many of our personal freedoms. One of these acts is the "Real Id" Act of 2005. Already having been denied by congress in 2004, the bill has been passed through congress under the "2005 Emergency Supplemental Appropriations for Defense: The Global War on Terror and Tsunami Relief" Act." The main reason for its passing, according to CNN.com, is the "serious political liability for a congressperson to vote against funding for the war on terror and tsunami relief." It was, like many acts, tacked on to the end of an already long bill which was guaranteed to pass. This new law will result in major violations of our most important right, the right to privacy. Like a magician, the U.S. has successfully tricked the congress and the American people into believing that this is a major and necessary step in the fight against terrorism. While this law and the technology that will be used to implement it may provide some benefit, the disadvantages and resulting violations of privacy will far outweigh the good.

For some time, the talk about a national or even global identification system has taken place behind closed doors, unheard by American citizens. The purpose: to fight terrorism and prevent fraud. While fighting terrorism and preventing fraud is necessary and good, the Real ID will not provide much of a benefit. One thing that history blatantly shows is the fact that there is no real way of preventing forgery. With billions of dollars in drugs, fake identification and other black market activities, the Real ID system is bound to be exploited and cracked.

The Homeland Defense Department suggestion about implementing Radio Frequency Identification (RFID) has opened up an even greater security problem. As proven by Defcon, a National Hackers Conference, RFID is not limited to the proposed distance of 20 feet or less that companies claim. Using two antennas and six nine-volt batteries, a world record distance of 69 feet was achieved during this conference. Just imagine the danger of carrying an ID card that allowed someone, from only 69 feet, to read your personal information. Visiting a third world

country would become even more dangerous because of the threat of high tech kidnappers. With proper equipment and training, kidnappers around the globe could instantly target rich U.S. citizens by cross referencing names with financial databases.

While it is clear that higher forms of identification are needed to protect one's identity, the use of Real ID is overstepping a serious boundary. Not only would these IDs carry a person's name, address and Social Security number, but Homeland Security is also allowed to insist on the storing of retinal scans and digital fingerprints. Talk from insiders also suggests that the storing of DNA might be a future possibility, though this has not yet been confirmed. With a person's DNA, fingerprints and retinal scan available, police would no longer need to obtain subpoenas for such information. A few clicks on there computer would allow them to run DNA and fingerprints against the total U.S. population. Sure this might solve crimes, but could such technology be used against citizens that the government considers problems?

Real ID may be required for anything from banking, medical care, and school registration as well as at the local grocery store or pharmacy. The purchase of alcoholic beverages, firearms, and everything in between may eventually require the use of Real ID. The government tells us that this is just another form of identification similar to the current state licenses, but these IDs are not linked to a national database capable of tracking just about any activity a person may engage in.

The possibilities, once Real ID is implemented, are limitless. Since RFID uses a wireless medium, the government could even set up RFID readers on roads and buildings, giving them the ability to track a persons every move. Even speeding tickets could be issued to citizens by triangulating the RFID signal to measure distance traveled. To ensure our freedom, the issuing of Real IDs must be prevented.

One might ask: "How could the government force lawful citizens to acquire these IDs?" The answer is this: By creating a major inconvenience for those who refuse to register. In just three years, anyone without a Real ID could be prevented from airline travel, Social Security payments, opening a bank account, or the use of other government services. This would take essential rights away from any citizen who refuses to comply. It might even create a group of "Second Class" citizens.

Bruce Schneier, a renowned cryptologist and author of award winning books such as "Applied Cryptography", says; "it's a bad idea, and is going to make us all less safe. It is also very expensive. And this is all happening without any serious debate in Congress." Congress has ignored the outcry of over six hundred various organizations concerned with the use of Real ID. Serious concerns such as the access granted to private businesses and individuals have arisen only to be ignored.

The need for more adequate and secure forms of identification is very clear but money spent on Real ID could be used to improve and secure current forms of identification. In fact, the need for Real ID is really not an issue. Under the "the Intelligence Reform and Terrorism Prevention Act of 2004", states were required to issue and maintain stronger forms of identification.

The fact remains that until the government decides to listen to its citizens, they are only driven by politicians and technology giants who lose perspective of what is wise and prudent. A thin line exists between the existence of secure identification and the destruction of privacy. Sure the government could easily prevent terrorists with technology like Real ID, but is it safe to give up our existing privacy for this security? Like a child who has just found his fathers gun, the government, left unchecked, will continue to wield its power even though dire consequences are evident.

Editors Note: Real ID = BAD!!!

Spy Stations, Letter Substitution and Crypto-Quotes

M L Shannon

==========

Some of the strange sounds I heard as a kid with the surplus radio may have been 'spy' stations. The radio-teletype signals might have been secret agents, and they might have been from governments other than the US.

There are many such stations, but the ones that are the most well known are those who broadcast Spanish language numbers. The digits Uno, dos, tres, quatro, cinco... repeated endlessly in groups of five.

Now, like any shortwave station, they serve a purpose. Consider the effort in setting up and maintaining a station with sufficient power to broadcast thousands of miles. This is not a prank, joke, hobby, whatever; there is some serious stuff going on here.

So, I was motivated to do some searching and I found a Yahoo newsgroup
http://groups.yahoo.com/group/enigma2000/?yguid=48814325

Here, you will find in one place much of the information available on what may be spy stations.

There is a great deal of speculation about the spoken numbers Spanish language stations, what they could possibly mean. As there are only zero and nine digits but 26 letters in the English and 29 in Spanish alphabet, one might wonder how these digits can make meaningful messages.

Uno, dos, tres, quatro, cinco, seis, siete, ocho, nueva, dios

One possibility would be that two consecutive digits represent letters. So, uno cinco (1,5) would be 'O'. Now, if someone were to take samples over a long period of time and analyze them for appearances of two-digit groups that, all starting with uno and dos, and they do appear more often than what seems to be random, maybe this is part of the answer. Part. It can't be that simple.

Another combination, perhaps tres, ocho, tres, might signify the beginning of a new paragraph, so repeated occurrences of tres ocho tres separated by what logically would be sentences or paragraphs might have such a meaning.

Or, maybe tres ocho tres signifies that the following is intended for a particular person or agency.

But so far, no one has been able to decode any of this; that is except those to whom it was intended.

The One-Time Pad

One logical explanation for this, that with super computers working on decoding the messages, is that the numbers are part of a 'one-time' pad. The letters are substituted based on a certain document, such as a book. On a given day, the encoder might go to a particular page, down so many lines, say five, and start with the fourth word. The first letter of the first word of the secret message would be substituted with the first letter of the fourth word on the fifth line. This is well illustrated in The Key to Rebecca' by Ken Follett.

Even with high speed computers, the one time pad is believed to remain unbreakable, because every possible combination of letters would spell every possible combination of words. An infinite number of monkeys with an infinite number of typewriters. Or rather, word processors.

It was listening to these Spanish numbers, as a kid, that got me interested in letter substitution. In the days of the RBBS (Before the WWW) we used to make the codes up in BASIC and then others would try to break them.

Simple Letter Substitution

As an example, look at the crytoquotes in the daily newspaper. You are given a hint, one sample letter, and with that and a little practice, most of them can be solved. Just as with crossword puzzles where there are standard or often used clues, there are certain letter patterns you learn to look for. A single letter has to be either A or I. Words with an apostrophe have only so many possibilities. Like zr'k how many such words exist. There is 'it's' and 'he's' and a few others. Compare these letters; Z, R, and K with other letters, particularly the Z (I) and see if Z appears alone. If so, it has to be A or I, so it may fit.

Letter Frequency

The letters E, I, S, T and others are often used where Q, X and J are not. Remembering this is one of the basic tools in solving letter substitution messages.

Mixed Doubles

Look for double letters, especially words that look like this: 'ZKKZ'. How many words fit that pattern? Not very many. So, put your brain in digital mode and scan. Let the Z become A and then go through the alphabet. A then AA. No. A, then BB. Hmmm, could it be ABBA? Fits the pattern but as you learn with experience, somewhat unlikely to appear in a cryptoquote. A with DD, A with EE and etc. Go all the way to Z. What did you find? Next, substitute Z to B. BAA, BBB, BCC... and you come to O. It could be BOOB! Keep going, while comparing your temporary results with the other words.

Double Doubles (With apologies to Macbeth)

Some words have two (or more) pairs of doubles. Suppose you saw 'ZJJRRSSQQKWA'. There is only one word in the English language that this could be and you probably have already guessed it. And from this, you can probably solve the rest of the puzzle. The state Mississippi should be another easy one.

Five digit groups and nulls

So, as you can see, simple letter substitutions are not difficult to decode. To make it more difficult, break the message into groups of five letters. Thus, ZJJRRSSQQKWA becomes ZJJRR SSQQK WA and to make even groups, nulls (which can be any letter) are added. Now we have XVZJJ RRSSQ QKWAV. Still fairly easy but remember that whoever is doing the encryption is going to avoid such words. If it were necessary to send BOOKKEEPPING it would probably be broken into something like 'document manager' or 'ledger person'.

Fairly simple, as long as A=B, B=C and so on. More complicated algorithms were developed such as Vernam and Playfair, but even these could be broken by hand; pencil and paper. Even the most secure known cipher of its time, the German Enigma, was supposedly cracked by hand by the "Banbury Girls". Another version is that "The Colossus machine", one of the earliest computers, was responsible.

The computers of today would make short work of the Enigma, but, again, the one time pad is still believed to be unbreakable. And if the information being broadcast by the Spanish language numbers stations, which anyone with a shortwave radio can intercept, are really top secret, then it is probable that the one time pad is indeed being used.

[d] RIAA Anti-P2P Strategies Revealed *by Ustler*

RIAA Anti-P2P Strategies Revealed
By Ustler
==========

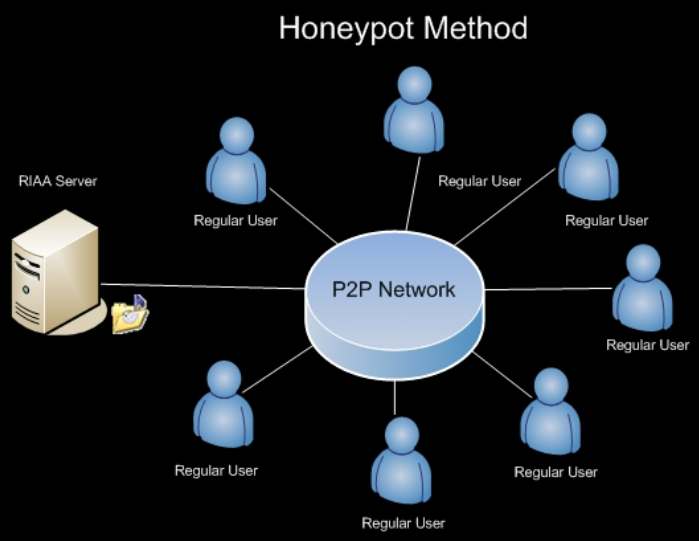
First off, I have to admit that it was very hard to come up with this information. The RIAA is very vague with its tactics and methods. This is probably due to the fact that they don't want the P2P community informed. In this article, we will be covering the theories behind anti-P2P technology. Illustrations will be included to help you understand how anti-p2p and p2p tracking works. With this knowledge, you can structure an appropriate defense or at least understand what the RIAA is doing. Of course, some of the theory is hypothetical, and may not be practiced by the RIAA and its agents (Very hard to come by rock solid proof).

*Distribution Methods

The following methods are ways that the RIAA can perform different attacks or obtain an IP addresses for which it can get a subpoena for. These are the delivery methods.

Honeypot Method

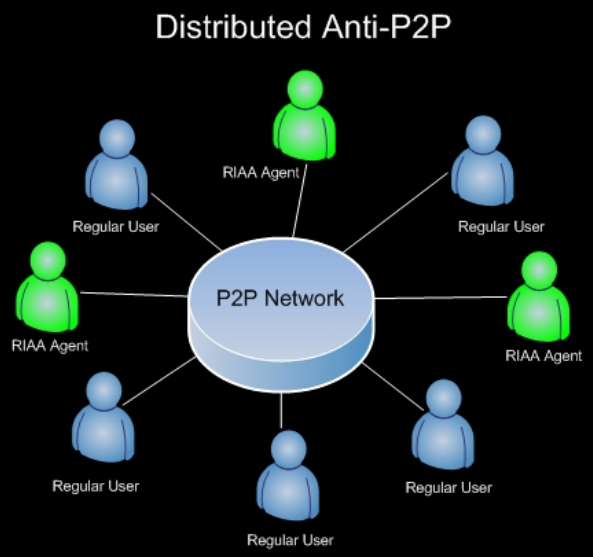
The first tactic we will talk about is the Honeypot method. This method is quite simple. Host a bunch of music files, have appropriate logging going to and from the server, then open it up to the P2P community. How could P2P users resist the option of downloading from an RIAA server that has an average upload of 2-3 mbps? This method is probably the simplest methods of trapping P2P users. After the connection is initiated and the file is downloaded, the RIAA takes the logs, brings them to a friendly judge, gets a subpoena, hands it to your ISP, and heads off to court.



The best countermeasure would probably be the use of IP filter, such as Peerguardian 2 and Protowall.

Distributed Anti-P2P

The next method is a hybrid of the Honeypot method. The main difference is that the server isn't hosted by the RIAA, but rather paid agents. Running special software, these agents freely download P2P music and allow users to retrieve it from them. This method can either send the info to the RIAA, or use a poisoning technique (See below). The main advantage for the RIAA, in this method, is it's very hard for a regular user to block free agents if they are home users. Blocking a range of home users would also block off a lot of legitimate users. Unfortunately I can't remember the name of the company that was doing this. I learned about this technique 2 years ago, when I got an anonymous tip about a company that was recruiting home users for this purpose. The user would download some software, install it, and let it run in the background, thus giving the anti-P2P company another node to trap pirates with.

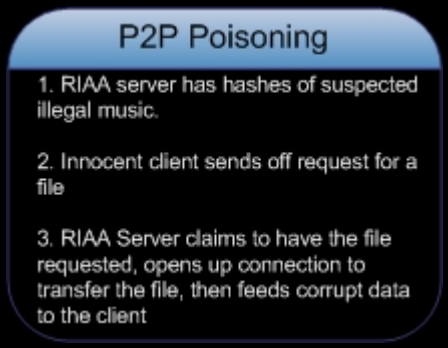


This sort of method is very hard to detect. The best method to prevent such an attack is having developers build fingerprinting functionality into P2P software. Custom software could easily have a client identification that is renamed or tampered with. Another method of preventing this kind of attack is creating closed P2P networks, using some sort of identification scheme, and possibly using an anonymous P2P network (Future article will explain how these work).

*File Destruction and Corruption Methods

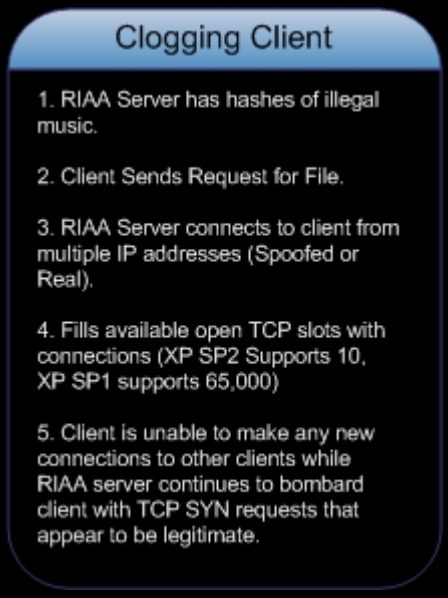
The next set of methods are what the RIAA claims to be ANTI-P2P technology. These are the actual attacks.

File Corruption



This method will be referred to as P2P Poisoning. The concept behind this method is to corrupt existing good files. By corrupting the file itself, the anti-p2p company further prevents the distribution of that file. The main reason why this attack is successful is because certain software uses weak hashing or doesn't hash the data as it's received. If a client requests, for example "Music.mp3", a RIAA server or agent could claim to have the file. It then starts to feed the client data, but instead of feeding it the proper data, it feeds garbage to the client (For Example: Instead of "010110101" it might feed the client "000000000"). This attack is particularly hard to detect since certain hashing schemes only hash the whole file. So if I'm downloading a 700 MB file, which finishes after 2 hours, ill then try to open it (Maybe its an Video file or Archive). Since the RIAA server/agent fed me corrupt data, the file will probably be unusable or crippled. The best example would have to be the corruption of a WAV files. If you downloaded a WAV file that was attacked with this method, you may be able to play 70% of the file, but after that, you might get a high pitched noise or some other weird sound (Which is the corrupt data). As I said before, depending on the delivery method, this attack could be easy or hard to block. P2P clients normally hash the whole file which would only let you know when the file was finished downloading. To prevent this attack, P2P software should hash blocks of the file, instead of only hashing the whole thing at the end. The P2P client would download an index containing the block hashes. (Hashing the index would prevent corruption of the index by attackers. This hash would be included alongside the file hash). If a server/agent is feeding you corrupt data, the P2P client would be able to detect, discard the corrupt data and block the attacker. P2P networks that don't implement this method might rely on getting block hashes from clients as the information was being requested. This isn't a security method, since the attacker could corrupt the block, hash it, and then send you that hash. Another way to do this (Which would probably work better) is by requesting block hashes from multiple clients. The main problem with this method is you wouldn't be able to detect which block hash is correct (if an attacker is just randomly sending block hashes off to clients).

DOS, DDOS and Clogging Clients



This is a DOS and DDOS attack and is intended to clog up clients. In P2P programs, you normally have "Max Connections", "Max Sources", and "Max Queue" settings. These settings ensure that your PC doesn't become overwhelmed by upload and download requests. Anti-P2P companies exploit this by finding and targeting clients that either have illegal downloads or are trying to obtain them. Using special software, the Anti-P2P company fills up all the Max Connections or Max Sources with fake ones. For example: creating 400 sources with a queue length of 3000. This would cause the client to wait for the source to become available, but since it may never become available it will prevent any other valid sources from connecting. As you might have noticed, Windows XP SP2 supports only 10 new connections per a second. This is supposed to slow down worms and port scanning, but if you're running a decent firewall and anti-virus, this provides no real security. If you want to remove this "security" feature, I would suggest you check out this http://www.speedguide.net/files/xp_sp2/EvID4226Patch211a-en.zip. This program will let you increase that limit.

Fake and Trojan Files

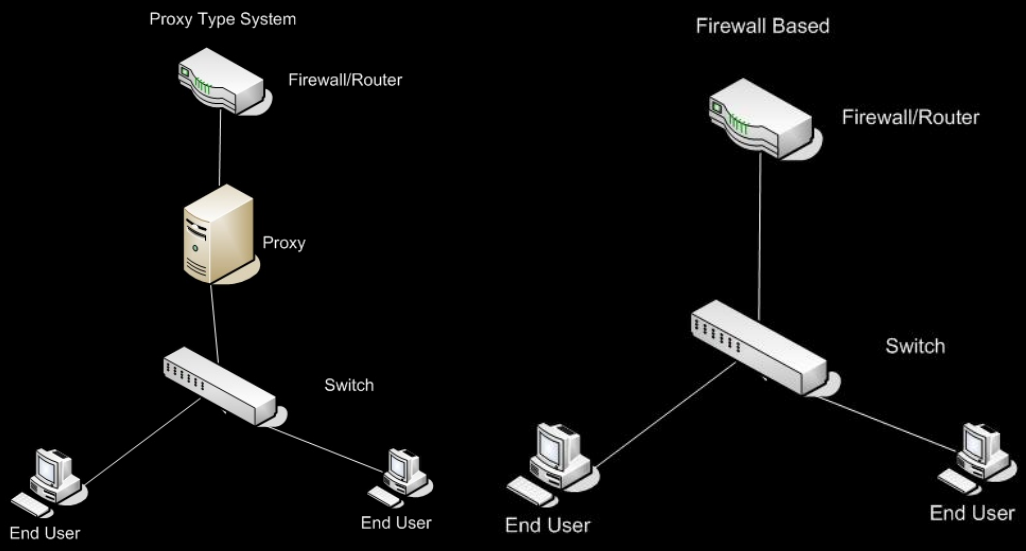
The next form of attack may not be implemented by the RIAA, but is being used by a lot of script kiddies. Essentially, the attacker would upload a virus or Trojan and rename it to something like "Music Name.mp3 .exe". The spaces are meant to hide the extensions (Usually we have 250 spaces). After the user downloads the file, and tries to execute it, a program is run that allows the attacker to gain access to the computer. Probably the best way to prevent these attacks is to use your COMMON SENSE. If an MP3 has a really long name, or the file size is 25kb, when it should be 3 MB, delete it! Plus, use some sort of up to date anti-virus. Certain viruses also flood the shared folder with replications of it to allow others to download it (Each with a different name). Clever script kiddies will attach a program to the head of the file, and then execute the MP3 that is trailed after the program. This decreases suspicion, since the MP3 did play.

Anti-MP3 Viruses

This is an extension of the Fake Files attack. But instead of giving access to a hacker, the program's sole purpose is to remove MP3 files. We saw this type of attack in the Nopir-B worm http://www.theregister.co.uk/2005/04/22/nopiracy_worm/ . It posed as a legitimate file and when executed it searched the user's hard drive for MP3's and then deleted them. Now I wonder who sponsored this kind of virus. Could anti-p2p companies pay a virus writer to release such a virus? Ill leaves the conclusion up to you.

***P2P Blocking in Educational and Business networks: A Quick overview**

Corporations, colleges and schools have been encouraged by the RIAA to take on an offensive against P2P. The main driving force behind this is the fear that the police will come in, seize everything, and take a LONG time to investigate, thus crippling the organization. Now in a business network, we have two types of protection when it comes to firewalls. The first type is very basic, and allows all outgoing connections while limiting incoming connections. The second type limits both the outgoing, and incoming connections. Depending on the firewall, this filtering would probably be port based. The second option we have is to implement a proxy type filtering system. This is a layer 7 device, and filters on a set of rules that apply to the data in the packet. The proxy type filtering system can be transparent or forced. Usually we have a direct connection between the proxy and the firewall, hence the only way out of the network is via the proxy. A transparent proxy will not be seen by a user's computer, while a non-transparent proxy would require a user to manually configure his PC to use the proxy.



As you can see from the examples, it's very hard to avoid these methods since the only way to the internet is via the device filtering. But of course, where there is a will, there is always a way. The firewall based filtering is easier to bypass. The user can easily bypass this system by using a different port (Other than the P2P ports). Another option is to use a proxy, if the firewall isn't too strict. It's even possible to connect and transfer data on port 80, if the server you're connecting to is configured that way. Since the firewall is only a layer 3 device, it will allow the packet to pass through (There are layer 3 and 4 firewalls).

Proxies or application proxies are very different. These offer layer 7 filtering. As you should know, Layer 7 is the Application layer of the OSI model. These actually filter depending on the data in the packet, instead of the TCP IP headers. These are probably the most common devices in colleges and schools. This allows the school to search for keywords, patterns and even log stuff your sending (Email etc). Some proxies even offer image scanning, which scans an image for certain, amounts of flesh tone skin and considers it porn if it exceeds a certain amount. When it comes to P2P and IM, these devices do a very good job of restricting and logging their uses. Proxies accomplish this goal with pattern files. A sample example, from an opensource layer 7 filtering program called l7-filter, has the following pattern to define AOL Instant Messaging connections (You can filter on a wrt54g/s with this program):

"^(*[\x01\x02].*\x03\x0b|*\x01.?.?.?.?\x01)|flapon|toc_signon.*0x"

This patter identifies the logon sequence, and blocks it. But of course, there is a way around this. One of the possible solutions to bypassing this protection is by using a program to transfer data formatted as HTTP, and ICMP packets. Of course you have to have a server on the other end to accept, reformat and resend the packet to the proper destination. This is sort of like a VPN connection, but it's cloaked as "Regular" traffic (Normally called tunneling). The only sign that might catch an admin's eye would be the excessive amount of large ICMP packets (If you're tunneling via ICMP). Probably the best means of protecting your tunnel is by using some sort of encryption. Tunneling can almost totally bypass a proxies filtering system, but of course, they could easily write rules that slow down HTTP traffic from one client, patterns that can identify tunneling and they can also use a white list to define allowed webservers. There are a lot of other methods that you can use to bypass a proxy, but they are out of the scope of this article.

*Conclusion
As you can see, Anti-P2P measures can be very successful in crippling and preventing P2P traffic. Of course, we can always use a countermeasure to bypass and avoid such prevention methods (Some where shown above). Just a quick note, this was written in a very short time span, so there may be a few errors or techniques that might not be properly represented. Some methods have been left out on purpose. Any corrections, additions will probably be posted on the forum.

And note to the RIAA: "This is what you call free speech, and is not "Corporate [trade] Secrets". This article was meant to be informative and entertaining, not to encourage illegal P2P usage. Of course, no one at BL411 uses P2P."

The writer, publisher, editors, and contributors to this article will not be held responsible for the actions of the readers.

[6] ==In the News==

-On P2P-
Sometimes I wonder if the US government is on pot or something. I mean for goodness sake, they make so many costly mistakes, it's unbelievable. It's not enough that they're allowing the effort to stop P2P to continue, but now they are spending OUR tax money in an effort to reprogram OUR children. Yeah, that's right! Now children in Elementary school are being targeted with a massive anti-p2p effort. Essentially, to my understanding, law enforcement visits the school and shows this video

(rtsp://wsd-ais-03.uspto.gov:554/piracy_video.rm). I don't mind the first 2 minutes of it, but scroll into it to about 3 minutes and you'll see what I'm talking about. Now let's look at how they intend to "reprogram" OUR children.

Watching it at first shows us that the government has no ability to make any sort of educational video (Even thought they probably spent thousands of dollars to produce this piece of crap), but pay attention to key things they say. Especially how they mention 9/11 and how the music he was "illegally" downloading was actually meant to give money to starving children in Afghanistan. This is essentially brainwashing. It's telling children that don't have the ability to perform logic that P2P is bad, and if they use it, they are stealing from poor children in Afghanistan. Of course, as adults, we understand that this sort of tactic is logically wrong, but to Children under the age of eleven, this makes perfect sense. Seriously, WTF?? Why doesn't the government make a video of people stealing music, going to jail, being raped and killed, then arriving in hell!

Lets not mention that the RIAA has so far successfully settled with 15,000 "Illegal" downloader's for around $3,500 a piece. Lets see, that's around $12 million. Now let's look at how they catch a P2P "Pirate". First off, they get some music to bait the trap (The Illegal kind). They then wait for someone to find it, and download it. After that, they pull the IP address from some sort of logging program, and turn around and get a subpoena for the billing address from your ISP. Doesn't that just seem wrong!!! First off, they are committing a crime themselves by sharing music. Second, they are doing something along the lines of entrapment (Even though it only applies to law enforcement). This would be the equivalent of the RIAA taking three hundred dollars and placing it in the middle of the road. When someone finally notices it, and picks it up, the RIAA runs out and sues you for stealing their property.

If you don't believe that I am right, check this out. In 2003, tons of songs from Madonna's unreleased album appeared on P2P networks. People quickly started downloading them, but when they finally finished the download, they where confronted with a voice saying "What the fuck do you think your doing!" (If you don't believe me, check it out http://wendy.seltzer.org/media/Madonna%20-%20What%20The%20Fuck.mp3). And it wasn't a fake, it was our beloved RIAA showing their true colors. Let's just say this didn't go over well with the hacking community. Not long after, Madonna's site was hacked and the legitimate songs where slapped up there (Here is the proof: http://www.zone-h.org/defacements/mirror/id=232146/)

The RIAA has even gone as far as pushing a bill to install spy devices in every computer manufactured. This device would allow the government to shut down any computer they felt was participating in "Illegal" downloading. Pushed by senator "Orin Hatch" from Utah and backed by the RIAA, this technology was meant to prevent P2P traffic, but fortunately it didn't pass to my knowledge. Of course Senator Orin Hatch claimed that "Audit Trails" would be left to prevent malicious use. A former executive from Intel, who requested to remain unnamed called Orin Hatch's plan a "nutty, ludicrous, and beyond the pale.". This is probably the worst idea that I've ever heard of. Just imagine if the technology was cracked and included in a worm of some sort. Great, now we have an audit trail going to anyone that accidentally got the worm from an email or vulnerability.

In conclusion, I have some doubts about who actually runs this country. The RIAA has put itself above the law. Not only are they intruding into our private lives, but they hide behind the government while doing it. Sure, why not cut off the hands of every person convicted of piracy, or maybe we should execute them? That would solve the problem. Maybe the RIAA should wise up and figure out that as long as they are on the offensive, they're going to lose customers. Since their little war started, I've been boycotting them along with tons of other people. I don't download music, I'll just stick to the radio till the RIAA decides to wise up and figure out that suing 14 year old girls is probably not the best way to fight piracy.

[7] ==Product/Service Reviews==

[a] TrueCrypt

TrueCrypt: The Freeware alternative to commercial encryption
By Ustler
Have you ever wanted to protect your data without paying for those expensive encryption programs? Do you worry that someone might steal your laptop only to find your private information, or even worse, having the RIAA barge your door down and seizing your computer? Truecrypt is a wonderful piece of freeware that offers you the ability to do all that, and more. Of course it lacks some features that commercial applications might have, but it's better than nothing.

Commercial Applications Vs Truecrypt
A good freeware encryption program is hard to find nowadays. Commercial applications dominate the market, but offer no re-assurance that their product is actually secure. The government could easily require these companies to place "Backdoors" into there software, for "National Security" reasons. Just take a look at some of the products that companies offer, toting a password recovery option. How can this software be secure if the company has the ability to decrypt it with there "Secret" code? One of the basic laws of security says "Security cannot be achieved by Obscurity". Essentially this means, if you hide something from plain sight, it isn't security! Just imagine if banks where to hide your money under their mattresses and called it security! Now you may wonder "Why is Truecrypt more secure?" Well the answer is simple; you have access to the FULL source code. This allows anyone with a programming background to spot security vulnerabilities in the software.

Truecrypt at first glance
At first glance, Truecrypt seems like a regular encryption program. But trust me, it offers a lot of features that can't easily be found anywhere else. Unfortunately, a Linux version is not available yet at the time of this writing. A future "Major" release is planned for October/November, but we have yet to hear any news about the current progress. Future plans include the following options:

- Linux version
- Language packs
- Keyfiles
- Support for Windows XP/2003 x64 Edition
- Hash algorithms structurally different from SHA-1 and RIPEMD-160
- Auto-dismount (on volume/user inactivity)
- Hotkeys
- Tray icon (optional)
- 'Raw' CD/DVD volumes
- Network volumes (UNC paths)
- TrueCrypt API

(Sorry Linux users. keep checking the website for the Linux release. If you're looking for something that supports Linux and Windows, try CrossCrypt. It doesn't have all the features that truecrypt offers, but at least it supports Linux and Windows.)

Enough with the future of Truecrypt, it's time to take a look at the actual program. One of the best features of Truecrypt is its wonderful GUI. No more stumbling around on the command line to try and get your encryption working.

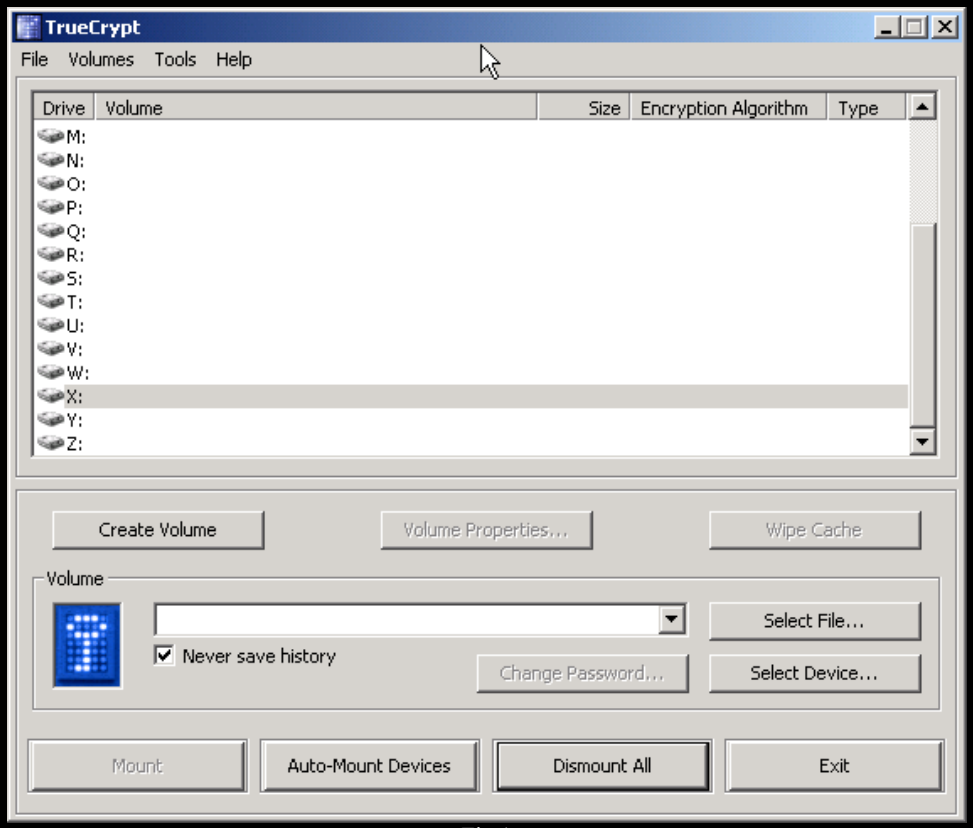
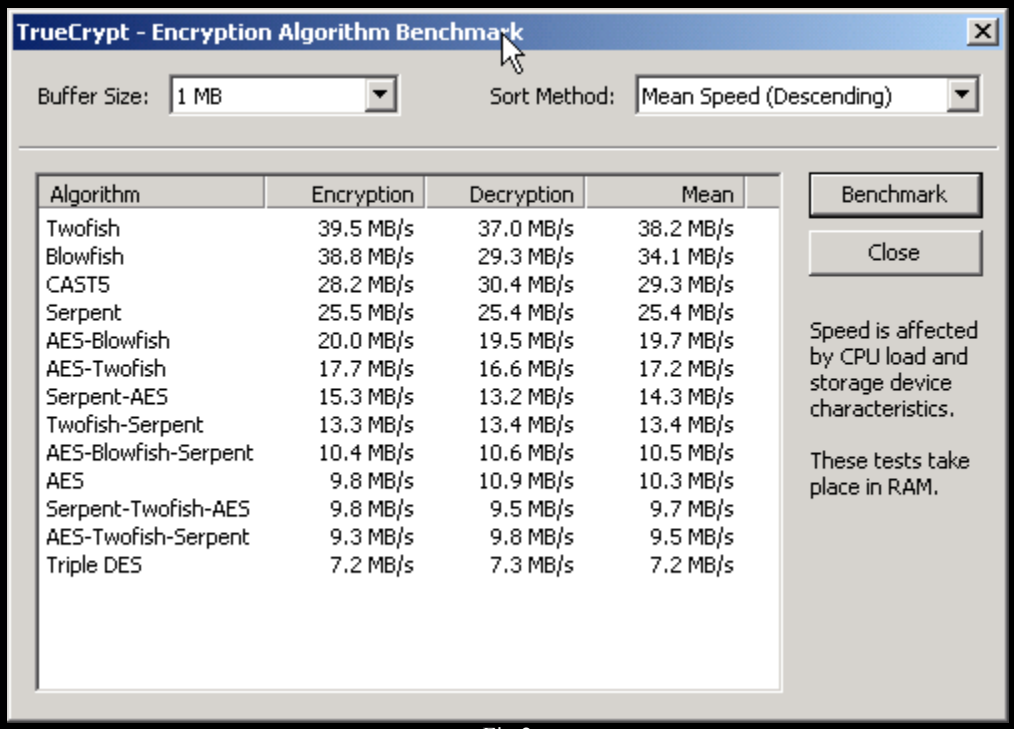


Fig 1

But of course, this is only one of Truecrypt benefits. Probably the feature that stands out the best is Truecrypt's support for a multitude of encryption algorithms. Better yet, Truecrypt lets you benchmark the algorithms to see performance differences.



Algorithm	Encryption	Decryption	Mean
Twofish	39.5 MB/s	37.0 MB/s	38.2 MB/s
Blowfish	38.8 MB/s	29.3 MB/s	34.1 MB/s
CAST5	28.2 MB/s	30.4 MB/s	29.3 MB/s
Serpent	25.5 MB/s	25.4 MB/s	25.4 MB/s
AES-Blowfish	20.0 MB/s	19.5 MB/s	19.7 MB/s
AES-Twofish	17.7 MB/s	16.6 MB/s	17.2 MB/s
Serpent-AES	15.3 MB/s	13.2 MB/s	14.3 MB/s
Twofish-Serpent	13.3 MB/s	13.4 MB/s	13.4 MB/s
AES-Blowfish-Serpent	10.4 MB/s	10.6 MB/s	10.5 MB/s
AES	9.8 MB/s	10.9 MB/s	10.3 MB/s
Serpent-Twofish-AES	9.8 MB/s	9.5 MB/s	9.7 MB/s
AES-Twofish-Serpent	9.3 MB/s	9.8 MB/s	9.5 MB/s
Triple DES	7.2 MB/s	7.3 MB/s	7.2 MB/s

Fig 2
(The test system was an IBM T42 running at 1.7GHZ and a 7200 RPM IDE hard drive)

Just look at the multitude of encryption methods. You've got everything from Triple DES to AES. You even have the ability to do 2-3 algorithms together. This means your getting 3 layers of protection. Please note, that each layer of Encryption uses its own key. If your running something a little faster than my Laptop, these speeds would probably be A LOT faster. Also note, that certain algorithms are faster on smaller blocks of data while others are perform better on larger blocks of data. If you don't believe me, try it out. Set your Buffer Size to 1 GB and see which algorithm performs better (Just make sure you have 1 GB of memory available since these benchmarks take place in memory. If it's using swap, its gonna kill your benchmarking).

The other thing that really stood out, was the fact that Truecrypt allows you to perform encryption on a full partition or in a file.(Fig 3) (Note: You cannot perform Full encryption on the root partition.) After choosing your encryption type, algorithm, and size, Truecrypt allows you to choose between NTFS and FAT. Also, Truecrypt takes a further step and actually fills the freespace with random data before encrypting it. This prevents someone from doing a Known Plain Text Attack. (A Known Plain Text Attack is when part of data that was encrypted is known to the attacker. He uses this knowledge to attack the cipher and determine the key.)

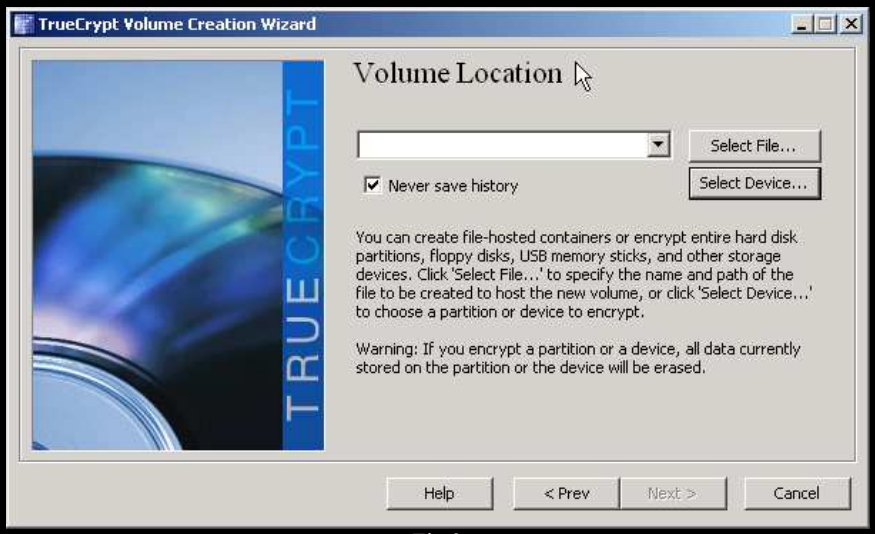


Fig 3

The only apparent weakness in Truecrypt, is the fact that it uses passwords instead of key files. To fix this, just use a 64 to 128 character password (If you have problems creating strong passwords, try https://www.winguides.com/security/password.php . To prevent any kind of logging, I would probably create ten, eight character passwords and then combine them in a random order. Also add and replace

some of the characters, just in case winguides is logging the password generation. Please note, we are running it over SSL to prevent local sniffing attempts.)

You might be wondering, how do the encrypted files/partitions mounted onto your system? Again, all you have to do is go and select the file/partition, select the drive, and click mount. You will then be prompted for your password. After that, you pretty much store the information just like you had a separate hard drive. It acts just like a partition. The other thing you might encounter is the fact that the encrypted partitions show up in My Computer, even though you didn't mount them. If you click on it, Windows prompts you to format it. Unless you want to loose all your data, I probably would suggest against this.

If you have any other questions, I would highly suggest you take a look at the manual. Its around 51 pages and covers everything from troubleshooting to the formula's for the algorithms. It's by far, one of the best manuals I've ever seen. I've been using Truecrypt for along time, and am very happy with it. The only thing that exceeds it, is PGP 9, but you have to pay for it☹. And even PGP 9 doesn't offer the ability to choose your encryption algorithm. Just to brag, I've got three 300 GB hard drives running Truecrypt on different partitions, and no performance problems.

[b] PeerGuardian 2

PeerGuardian 2: Anti-RIAA Software for the people
By Ustler
It's often very hard to keep out the RIAA, but thanks to MethLabs, it just got a lot easier. Peerguardian 2 is a program that takes the first step in blocking RIAA networks from accessing you PC. Essentially, PeerGuardian 2 filters on Layer 3 of the OSI stack, which means, it filters by IP address. MethLabs has done an AWSOME job of compiling a list of networks that are currently held by the RIAA and other organizations (When I say networks, I am referring to IP classes leased out to companies by their ISP, Such as a class A network.) By far, one of the best things I like about PeerGuardian 2, is the ability to do the auto updates. Programs like, Protowall, which are also good, lack the feature of autoupdates and often require you to install a service to be able to filter (Referring to the service driver that is installed under your network adapter settings). Furthermore, Peerguardian 2, in my opinion, is a lot more stable than other programs. People complain that Peerguardian 2 uses too excessive system resources, while this may be true, anyone with at least a Pentium 3-4 should be fine. I wouldn't be complaining about performance with the sort of protection it offers. Let's take a quick look at the program itself.

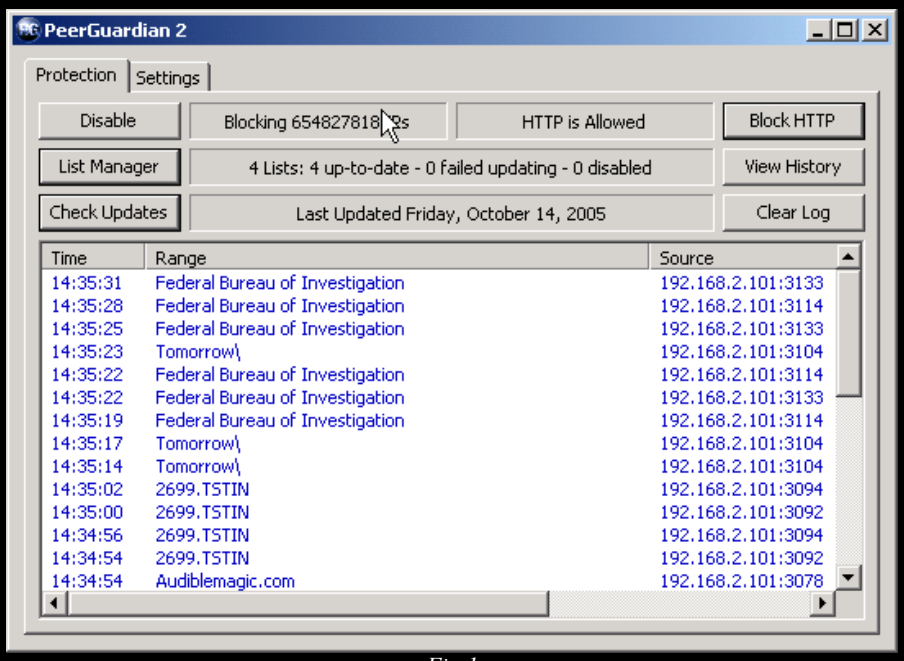


Fig 1

Here is the main part of the program. Essentially, it offers you the ability to view blocked sites, in real time. Also notice the bottom that says "Block HTTP". This option lets your remove the filtering for HTTP while still filtering P2P programs.

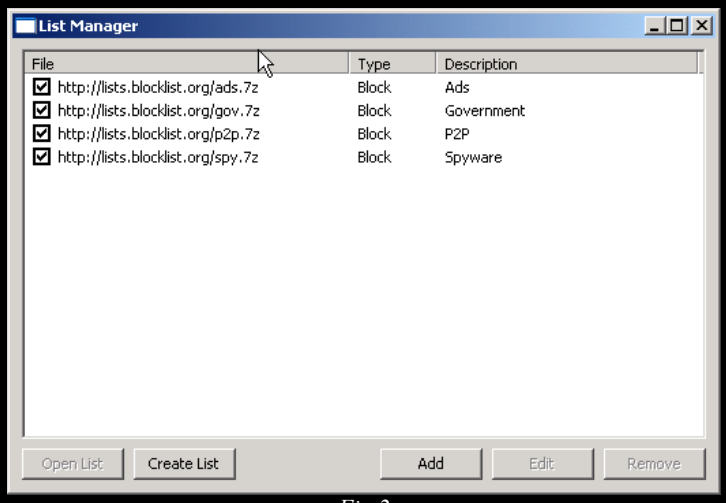


Fig 2

Fig 2 shows the window that allows us to manipulate the block lists. We have the options to use local lists, and specify a URL that we can download from. We have two types of lists, exceptions and blocks. Exceptions are those IP ranges that you want to allow. For example, I play some online video games when I get bored. Since the IP range is owned by Sony, It would normally block it. To prevent this, I had to make an exception. But don't fear, you don't have to format a list of exceptions for every IP range you need unblocked. If you need to make a quick exception, you have the option of right clicking on the IP address in Fig 1, and selecting one of the following options.

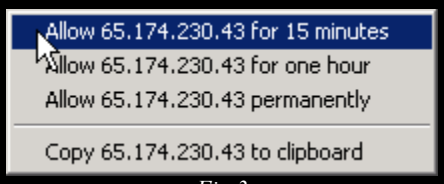


Fig 3

You can make a quick 15 min or 1 hour exception, or unblock it for good. As we mentioned before, the auto-update features is by far, my favorite. A couple clicks, and you can have an up to date list of Evil IP ranges.

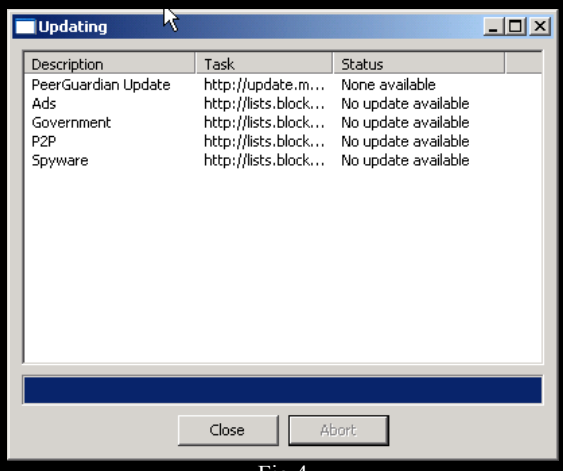


Fig 4

By far, PeerGuardian 2 is my FAVORITE anti-RIAA software. If you don't believe me, try it for yourself. Also note, MethLabs has just changed there name to Phoenix Labs. Check it out,
Phoenix Labs
http://phoenixlabs.org/

Phoenix Labs PG2 page
http://phoenixlabs.org/pg2/

[8] ==Cryptogram==

Hpwnzxp ez esp qtcde pgpc zywtyp potetzy

HINTS:
All upper case cipher text, is upper case plaintext
Simple encryption [One Function]
Mentioned in an article

Rules: One month to crack, email answer to crypto@blacklisted411.net. If answer isn't broken in one month we may give a second clue or just the solution. This one is SIMPLE

Prize: Solution and your name will be posted on the winners section of our site.

[9] ==Credits==

Editor: **Ustler**

Authors: **ML Sharron, Dr. Fibes, Ustler**

Shout Outs: Shouts Outs to Unic0der, Phrack, the staff at BL411, and anyone else I might have forgotten.