

Hacking a Terror Network: Ch 2 - Unseen Planning

del.icio.us

Discuss in Forums {mos_smf_discuss:Book Reviews}

Written by a certified Arabic linguist from the Defense Language Institute with extensive background in decoding encrypted communications, this cyber-thriller uses a fictional narrative to provide a fascinating and realistic "insiders look" into technically sophisticated covert terrorist communications over the Internet. The accompanying CD allows readers to "hack along" with the story line, by viewing the same Web sites described in the book containing encrypted, covert communications.

This chapter is excerpted from the book titled "Hacking a Terror Network: The Silent Threat of Covert Channels" By Russ Rogers, Matthew G. Devost, published by Syngress. ISBN: 1928994989; Published: January, 2005

Chapter 2: Unseen Planning

March 19, 2004

Salah unlocked the dead bolt and stepped through the doorway into the barren space beyond. The apartment held no real emotional sway over Salah; it was a quaint dwelling, but only temporary. Walking across the stained brown carpet, he stopped at the window near his bed to look out over the city. The university was only a few blocks away, but even for a single person walking, it was sometimes difficult to navigate the traffic below. He watched silently as the cars on the road below battled to dominate the road, relentlessly working to carry their occupants home.

Salah had endured a very long and very detailed networking exam earlier that morning and afterward had gone to the university library to gather more information on steganography, commonly referred to as stego. The very name, steganography, meant covered writing in ancient Greek, and the concepts held great promise for Salah. Through its use, he and his team would be able to communicate in the open without anyone realizing what was there.

The Relationship Between Covert Channels and Steganography

The term steganography comes from two Greek root words. The first, steganos, is translated as covered. The second part of the word comes from the Greek work graphie, meaning writing. The two terms together help us describe the idea of hiding information of one type in some medium that normally would be unexpected to the average person. But over time, the term steganography increasingly has been used to describe the hiding of data inside binary files, such as audio files (.wav, .mp3, and .au), digital images (.jpg, .gif, and .bmp), and other binary formats, such as executables. In contrast, the term covert channels often is used to describe the idea of hiding any type of information in any type of medium. For our purposes, this term can be considered to be all encompassing, including steganography. For example, there are other means for hiding information that include everything from obfuscation of the information, appending the data to the carrier file, or including the data in network packets being transmitted across a medium. There are even algorithms that create digital information based on the input message supplied by the user. For example, programs exist that will create a music file using nothing more than the original data supplied to it by the end user. Using the term covert channels allows us to more adequately include a broader base of information-hiding mechanisms than normally is associated with the term steganography, although they are often used interchangeably. As you read this book, the term steganography is used to denote instances where information is hidden directly within a binary medium, and covert channels is used in those instances when obfuscation, appending, or packet modification is concerned.

The creation of steganography within images and the sheer difficulty of detecting legitimate steganography within files found on the Internet captured Salah's imagination. Tremendous information on the topic was available on the Internet. You just had to know what you were looking for and the key words for finding all of it. Salah had researched the topic numerous times over the past year. He had even more recently enjoyed great success toying with some of the applications that help create hidden information freely available on the Internet.

Tools like S-Tools, JP Hide-and-Seek, and Gif-it-up were free and powerful and could be used to hide information in digital images by anyone willing to simply download the software. Images were the perfect medium, at least initially, for communicating with his team. The amount of information that can be hidden in an image with a limited chance of detection is about 25 to 30 percent the size of the carrier file. That would provide enough storage and transmission space in the beginning. A carrier file, simply put, is like a suitcase. You put data inside the suitcase so that you can carry it around protected. The larger the suitcase, the more stuff you can put inside of it.

For example, if you had a 400-kilobyte carrier image within which you wanted to hide information, you would be better off limiting the data to not much more than 100 kilobytes. Any more data hidden within your carrier would start to cause noticeable distortion, and could compromise your hidden communication. His team currently didn't have a need to hide larger amounts of information, but if the need arose in the future, Salah had already decided to utilize audio files instead of images due to their average 5-megabyte file size. Peer-to-peer networking on the Internet had increased the number of audio and music files being exchanged by users all around the world. Programs like Kazaa, Acquisition, and Limewire already were allowing Internet users to search for music files by song name, artist name, and more. This

potentially could provide for a more anonymous distribution of information to all the relevant team members. But this was something he would address later, when the need arose.

Corporations around the world had even helped his cause, without knowing it, by standardizing the practice of watermarking the images they posted to the Internet. Watermarks effectively provided the means to let everyone know the image was the corporation's intellectual property. Those images were downloaded by millions of users around the world, every day, littering the world's hard drives. They are, in essence, standardized steganography within images and would aid in hiding his group's activities from prying eyes.

Present-day detection software still has difficulty distinguishing some forms of digital watermarks from legitimate steganography. All of this obscurity should work to his advantage. It's nearly impossible to find a single and specific fish in the ocean, he thought to himself. We are simply a smaller fish in a much larger ocean — the Internet.

Another standardization within the industry has made his team's work easier as well. This time, through the creation of the standard JPEG (Joint Photographic Experts Group) image format. In the early years of the "popular Internet," as he often referred to the early 1990s, many images on the Internet were GIFs. But the GIF (Graphics Interchange Format) image was littered with copyright and intellectual property issues for any organization that wanted to implement the standard into their own software. Most companies stopped using the GIF for this reason and were more likely use the open JPEG format. This was mostly in an effort to avoid paying royalties to CompuServe, which still owned the patent on the GIF technology. In the end, most companies that deal in digital images preferred to support the JPEG image format.

Nearly all modern, digital cameras on the market created and stored their images in JPEG format as a .jpg file. Digital cameras have been growing more and more popular, partially due to the sheer popularity of computers and the rapid descent of their cost to consumers. JPEG images also can be created using everyday graphics programs available freely on the Internet or in inexpensive commercial versions. Images created by these applications oftentimes were passed off as artwork and posted to various web sites for visitors to admire.

With all of these factors standing solidly behind his efforts, he wondered what could actually stop him. Salah had been working toward a single goal for the last 13 years. His father had made him swear that he would avenge the death of his brother by striking at the heart of America, its people. The concepts were simple, the effect devastating. Using the Internet to communicate would only increase the dismay of the attack because every detail would be passed under the Americans' noses, in public forums. Their miscalculations about the true threat of covert channels would prove deadly.

His team consisted of 27 technologically knowledgeable Muslims who all had one thing in common: they hated the United States. And because of their experience with computers and networking, the days of suicide bombs would be coming to a close. Salah had always thought it seemed a little melodramatic and silly to strap explosive compounds to your body and detonate the bomb, along with your body. In the new world, none of your own people need to die to accomplish your mission. In fact, no one even needs to know you have people or a plan. All activity, all communication, and all your planning could occur without anyone else knowing. There was simply no need for young men to strap explosives to their waists, waltz into a crowded plaza, and blow themselves up along with the target. The new terror attacks could be completely planned, arranged, and organized online.

Inshah Allah, he thought, the only deaths in this arrangement will be Americans. It seemed logical to Salah that if his team survived these attacks, they would live to fight another day. Experienced fighters were much more useful than

young amateurs willing to die for a cause. Repeated attacks resulting in very little collateral damage were best planned for and waged online. He was proud of his ideas. "Some day soon," he had told his team in a recent e-mail, "we will all organize online. We will have no need to hide in the mountains or the desert in order to avoid capture. Instead, we will hide online. We will appear as no more than wraiths before the eyes of the West. Our normal lives will go on without notice while the bad fruit withers on its vine."

The ease at which JPEG images could be created meant that his team would have the ability to use unique images they created on their own. Using unique images would ensure that no other versions of the digital pictures would be available for comparison with the carrier file. Detection would be much easier for law enforcement if the original image were publicly available on the Internet, because the original image could be compared with the one containing hidden information. This was most commonly done by comparing the hash signatures of both images and looking for clues that could indicate steganography within the image.

Each person on the team had already been told to purchase a digital camera; the higher the resolution the better. "Carry the camera with you at all times," he had told them several months ago in the same e-mail. "Take pictures of everything that attracts your eyes." He was certain that, at the time, it seemed like an odd request, but they trusted Salah's technical knowledge.

"We won't foot the costs of this project for much longer," he told them in his last e-mail. "I have arranged a meeting with the leaders of Al Qaeda where I will tell them of our bold plan. They will likely provide for our needs until this attack is carried out. We will strike terror into the Western heart and show them the powerful hand of Allah in action."

The real key to carrying out this plan was secrecy and anonymity. Salah knew that you could easily find millions of images on the Internet. Different people from all over the world were posting images from their digital cameras on personal web sites. Pages and pages of personal images about family events, vacations, and even bedroom events littered the World Wide Web. Everyone on the Internet felt as if they had a voice, and that surely someone would have an interest in their little piece of the web. Hiding critical plans and information within images such as these was a perfect fit. Even if the American authorities knew he was hiding something, they would have a terribly difficult time locating his images among all the others already on the Internet.

He had decided to start with JPEG images and move to audio files later, if a need arose. He remembered the images and rules he had learned in his research. JPEG images were created much the same way as other digital images, at least initially. If a person takes a picture with a digital camera, the image is stored by software in the camera as a matrix, or grid, of picture elements known as pixels. Generally speaking, the greater the number of pixels in an image, the greater the resolution, or ability to discern detail, is in the image. The number of pixels in a digital image is called dots per inch (dpi) or pixels per inch (ppi).

Pixels per Inch

Each pixel within an image is assigned a value that represents the color of that pixel: either black or white or one of 16.7 million possible colors. Each pixel color is represented as a binary number consisting of 1s (ones) and 0s (zeros). These 1s and 0s are referred to as bits. Some images have 8 bits that combine to give a color value to the pixel, whereas others use 24 bits to define the color value for the pixel. When you combine enough pixels, you create an image. Digital

cameras actually recreate the image shown in the camera viewfinder as an image consisting of all these colored pixels.

The 16.7 million possible colors refer to the number of colors mathematically possible in a 24-bit image—8 bits by a power of 8. This actually results in exactly 16,777,216 possible colors in a 24-bit palette. An 8-bit image takes 256 of these 16.7 million colors and creates a palette that is used to display the image. So any 8-bit image is created from a maximum of 256 colors. The number stored in each bit of an 8-bit image is actually a pointer to one of the colors in our 256-color palette. An 8-bit image tends to be smaller in size but carries less color detail than 24-bit images because of its restrictive color palettes. This is evident in the math associated with having 8 bits of information that can all be a 1 or a 0. There are 256 different combinations of 1s and 0s in an 8-bit image, thus limiting the color palette of the image to 256 colors.

However, 24-bit images, are created using all 16.7 million colors available mathematically. Since 24-bit images use all the available colors, they don't create a restrictive palette. But unlike 8-bit images, there are actually three sets of 8 bits that define the color for each pixel in a 24-bit image. Each of the primary colors—red, blue, and green—has 8 bits to itself. If we count all 24 bits, we realize 16.7 million different combinations of 1s and 0s are available to define a color. Thus, each pixel can represent one of over 16.7 million different colors. The 24-bit images are called true color for just this reason. They are capable of representing every actual red, green, and blue color value available.

8-Bit Image Pixel Color Definition

24-Bit Image Pixel Color Definition

The most popular method for hiding information within an image was called Least Significant Bit (LSB) modification, and is a form of steganography. LSB modification takes the 1s and 0s from the secret message (often referred to as a payload) and inserts those into each pixel, starting at the bit least likely to make a noticeable change to the color of the pixel. Since a 1 or a 0 already exists in that spot, there is only ever a 50% chance that the bit will need to be changed.

Bit Significance

Most steganography applications start at the least significant bits in each pixel and then move down the line toward the more significant bits as data is inserted into the carrier. The more significant bits will make greater changes in color for the pixel when changed. Inserting too much data into a carrier will distort the image to the point that it can be seen with the naked eye. Human eyes are wonderfully designed, with the exception that discrete changes in shades of color or in dark colors in general tend to go undetected.

Example of Data Insertion in an 8-Bit Image

[Click Here For Image](#)

The real problem for the Americans would be when their law enforcement actually tried to get the information out of images they may suspect of having hidden information. Steganography, combined with encryption, would prove their undoing. To top things off, American law enforcement had mostly ignored the issue of hidden information because it was not considered a real problem. In fact, there were even poorly conducted research projects that had come back conclusively indicating that it didn't even exist. Yes, he would use JPEG images and hide the American fate directly under their noses. They would never even notice because there was no such problem.

Salah shifted his weight and realized that he was still staring out the window into the city. He turned and laid his backpack on the door next to his makeshift bed, where it landed with a thud. Walking over to his desk, he turned on the monitor and watched as the screen came to life. He had apparently left his computer on all day. His landlord wasn't overly intrusive, but he chided himself to log off next time.

He glanced briefly at his e-mail to see how many new messages had come in since he had checked last, earlier that morning. Forty-seven new e-mails; it would appear that everyone had responded early at this point. Good. He would read those e-mails shortly, but first things first, some tea and perhaps a small snack.

He walked into the kitchen and filled his pot with tap water. Absently, he wondered if anyone had figured out his null cipher message. Please Allah, he thought to himself. Give me a few leaders among my team. Let them see the value of what we're doing. He walked over to the stove, lit the flame on one of the front burners, and set the water to boil. The name on the stove ignited his memory. His brother's frightened face filled his mind as he thought back to that fateful day at the coffee shop. He had relived his brother's death in his own mind for years, recreating the scene as he imagined the pain of it all. He wasn't there when it had happened, but he made up for that every night through his own nightmares of the event.

When his parents and he had first arrived at the site, he was sure there had been a mistake. "There's nothing here but a pile of stone," he recalled saying. But his father had seen him, his brother. At first, it was a disembodied hand sticking straight up out of the rubble. He remembered his father and several other men pulling large chunks of rock out of the pile until his brother's ravaged body was found.

The wet teapot hissed gently as the water still clinging to the outside of the pot sizzled into steam. He shuddered to himself and pushed the morbid details back into the recesses of his mind. His purpose flooded back into his heart and he reflected on his research today at school. One of the papers he had found was written back in the late 1990s and discussed a concept called stego-noise. The paper was written by Fabian Hansmann and described a mechanism for writing a benign Internet worm that would search for certain vulnerabilities. When computers were found with the appropriate security vulnerability, they would be compromised, allowing the worm to embed all suitable target files on the drive with steganography. Over time, these infected yet benign images would clutter the Internet with images, audio files, and other binary files that had useless steganography, making the detection of legitimate steganographic files extremely difficult. Salah knew that even the most advanced algorithms for detecting steganography today had a surprising number of false positives, making them somewhat unreliable. But this concept could threaten the fragile balance between the creation of steganography and the detection of it.

The premise of the paper had described a benign worm written to take advantage of vulnerabilities on computer systems around the world. As the worm located systems with the vulnerabilities it was looking for, it would infect every image on each system it had access to with a benign form of steganography. The worm was programmed to insert random information into each image, creating useless steganography, or stegonoise, within the image. When law enforcement officials attempted to scan a computer system or the Internet for images with potential hostile or hidden content, eventually they would be inundated with large numbers of images appearing to have steganography within them.

When the paper was originally written, the concept was intriguing to hackers, but largely ignored by the general Internet community, including law enforcement and the military. But in today's networked world, where worms are a daily reminder of the insecurity of the Internet, such a worm could actually generate a tremendous amount of stego-noise in a very short period of time. The Slammer worm was a good indication of how quickly a properly coded worm could spread.

The Slammer worm had taken the computer world by surprise, even though there had been a public announcement of the vulnerability that made the worm possible. The vulnerability was in Microsoft's SQL server, and allowed the worm to spread at an alarming rate. Microsoft had even taken steps to ensure a patch was issued and available before the announcement was made about the vulnerability. When the worm hit on January 25, 2004, it broke all records for the spread of a worm or other virus by doubling in size every 8.5 seconds. The worm eventually infected at least 75,000 hosts around the globe and hit its maximum scanning rate of 55 million scans per second after only three minutes. The scanning slowed after this point due mostly to the inundation of the various network infrastructures in place at the time. He remembered the enormous impact the worm had on the computing world and on the Internet in particular. Stego-noise had the ability to make it look like there were a lot more needles in this haystack than really existed. Salah wondered absently if such a virus already existed and how difficult it might be to develop one from scratch. Perhaps he would consider working on this project another time. The eventual amount of noise a worm of this magnitude could cause

would be enormous, allowing years of free communication via covert channels. Yes, he would definitely have to think seriously about pursuing this project.

The sharp whistle of the teapot snapped his wandering mind back to the present. And, for a moment, he was just an average college student standing over a teapot, waiting for it to boil. He fought back the brief wish that, for once, he could live a normal life and returned to the task at hand.

The tea was on the top shelf. He wasn't quite sure why he still kept it up there; he had ample cabinet space in his kitchen, but his family had kept it on the top shelf in their kitchen, and he supposed his mind was comforted by small reminders of home. He took a large tablespoon and dumped some of the dark black tea leaves into the boiling water. Picking the pot up off the burner, he placed the pot on a back burner and turned off the flames on the stove.

He was going to need to find out what they already understood. Could he bring a team together under this technology and coordinate an attack? What were his chances of success? He understood that if he expected to get backing from Al Qaeda he would need to demonstrate that his plan was foolproof and would result in a painful wound for the Americans.

Walking back to his computer, he read through the e-mails. He was scanning for a single person from the team, a person who had the most likelihood of having discovered the hidden message—Jimmy. Of course, Jimmy wasn't his real name. Like Salah, he had chosen a pseudonym for use online. "Besides," he had told Salah in a past IRC conversation, "Americans prefer names they can pronounce and understand. I'll fit in better if my name appears to be normal to them." Salah knew Jimmy was right. Ah, there he is, Salah thought as he located the e-mail he had known would be in his box.

He and Jimmy had discussed the possibility of using null ciphers in the past. In fact, it had been Jimmy's idea initially. "We'll start with something simple, to get the others comfortable with the concepts," he had told Salah. "Once they understand basic ciphers, we can change the position of the message characters. Eventually, you'll be able to introduce other covert channels of communication, and they'll pick up on those, too."

"Fight in the cause of God those who fight you…,"

Jimmy

That's all it said. Nothing more would be needed. Hopefully, the others had also read Salah's e-mail and figured out where the message was. This is going to work, he thought.

Salah shut down his computer. He still had studying to do tonight, and he couldn't be up late because he had work in the morning. Though Salah had received a scholarship from the university, it wasn't enough to cover his books, food, and housing. After a brief visit to the Student Welfare Office, Salah got a part-time job at the bookstore in the Student Center. The job didn't pay a lot, but it was more than enough to make ends meet. The important thing was that it didn't impact his studies or his side project. Working at the bookstore also provided Salah with some needed discounts on textbooks and supplies; discounts that allowed him to take more classes and graduate early. Shortly after the death of his father, Salah's family had run out of money to pay for school, leaving Salah on his own in a foreign country.

It wasn't Salah's style to worry about things out of his control; he was a survivor, and without hesitation, he willingly added this job to his set of responsibilities. He found that it was even a welcome break from his everyday existence. His routine had grown dull between the constant courses, studying, and his after-hours project. The job provided interaction with other students, many of whom Salah was beginning to consider friends. He had tried hard to distance himself and avoid the insidious emotional connections with the students around him, but he was so young. To many he was an average twenty-something student who needed the social interaction that was available only by having friends on campus, but he soon found himself fighting the internal battle to remain introverted and protected.

Salah walked back into the kitchen and prepared to make some dinner. I'll get some studying done while I eat, he thought. Maybe I'll even watch a little television. He pulled a frying pan from the drawer hiding at the bottom of the old stove and set it on the burner. Reaching inside the refrigerator, he grabbed a carton of eggs. Dinner would be quick and simple tonight.

