

Lieing to Hackers Is OK By Me

“All warfare is based on deception.”

Sun Tzu

“In war (conflict), truth is so precious, it must be protected by a bodyguard of lies.”

Winston Churchill

“Make a noise in the East and attack in the West.”

Anonymous Chinese

I believe in lying. Sort of. Let me explain.

The bad guys will do anything they can to get you. You know that and it doesn't seem quite fair. They get to cheat, while real companies have to play by the rules. They can lie. They can use social engineering or pull any sort of nasty trick they want to break into your networks or otherwise try to make your life miserable.¹ But there are some new innovative means to defend our networks, if we just apply some common sense.

I'm saying that we need to create an even playing field. *“Do unto other as they do unto you,”* and in Cyberspace and Infowar, such logic makes impeccable defensive common sense. If the hackers lies to you why shouldn't you lie right back? There is a way. It is your right and defensive duty to

- Lie to your adversary.
- Deceive him in any way possible
- Force him to waste time/resources
- Makes his attacks a much riskier proposition
- Protect Your Assets by the same means he attacks you
- Use automatic responses and hands-off management
- Apply Time Based Security concepts
- Use Deception

¹ Much of which is legal!

Lieing to Hackers Is OK By Me

The Military View:

The world is currently full of nations that are militarily weak, but ruled by despots who do not lack for cleverness or the willingness to use deception to maintain and expand their power.

Winn's Translations for Networks:

The Internet is currently full of criminal hackers, punks and goofballs that are morally handicapped, ethically weak, but who do not lack for cleverness or the willingness to use deception to maintain, project and expand their power.

and...

The Internet is currently full of networks that are defensively weak, but ruled by the technically and financially challenged who only need the willingness to use deception to maintain their systems integrity and expand their power

The main goal of your network defense is to keep your company functioning; keep the business process intact, and maintain day to day integrity so that there are no interruptions. Let's explore another tool that can create victory without battle and impose your will on your network adversary – just as the great Chinese warrior, Sun Tzu expounded 2,500 years ago.

That technique is deception. Lying. If you ask your legal counsel, there is no law against lying... especially to the bad guys.

- You goal is reduce the amount of time the bad guys have to attack you.
- You want your detection and reaction mechanisms to be as fast as possible.
- You may choose to invite the attacker to stay around for a longer period of time to give you more opportunity to collect forensic evidence and/or identify him.

Deception has been used throughout the history of warfare, from ancient time to today. Certainly the Trojan Horse fits the definition. Military leaders such as Phillip of Macedonia, Alexander the Great, Hannibal, Julius Caesar, and William of Hastings all the way to Saddam Hussein have successfully used deception to gain military advantage.

When undersized armies took on a larger force, their horses pulled weighty logs behind them over dusty roads to give the impression that more manpower was coming to battle. Small armies would light 1,000's of fires at night

to give opposing forces the false impression of size. Psychological operations fit right into the deception mode with the philosophy, *"It doesn't hurt if your enemy thinks he's smarter or tougher than you."* Think about that. Playing it stupid is good?

During World War II, MGM Studios was making military support films, but worried about becoming a potential target for aerial bombing if the Pacific war came to America. Studio executives complained to the War Department who said they would take care of everything. The government response was to send out experts who painted the roof of MGM studios to look exactly like a munitions plant. D-Day planners convinced the Germans that the invasion would not be at Normandy, but some distance to the Northeast.

When a German Enigma encoding machine was captured by the Allies, we figured out how to decode high level German transmissions. But we never let the Germans know that we could read their private mail, even if it meant sacrificing civilian targets to keep the secret. Thus, Churchill allowed Coventry to be bombed without an air raid notice to the population.

In modern warfare, electronic chaff is tossed from airplanes to confuse enemy radar. The Soviets poured thousands of electronic diodes into the concrete construction of the new American Embassy in Moscow. The intent was to confuse American counter-surveillance devices that can't tell the difference between the non-linear junctions of the diodes and those in a real eavesdropping transmitter. Problem was the Russians over did it, we found their plan early in the construction process and we canned the new Embassy.

Some experts maintain that Star Wars was nothing more than an elaborate technical public relations hoax of the first order to convince the Soviets we were willing spend a gazillion dollars on space-based defense. And then there was the Gulf War. Did the Patriot missile system work as well as was claimed? Probably not, but the media and folks at home ate it up. Saddam's grand deception scheme kept us shooting our smart bombs at Scud launchers that were nothing more than cardboard facades or shells of real ones. Deception clearly works.

Back to the Network

Now, let's figure out how to apply deception to network security. It's time to even the odds!

It is legally arguable to aggressively go after the bad guys. Corporate vigilantism is still only mentioned and knowingly approved by law enforcement in dark corners. They can't officially sanction the good guys to break the law to nab the bad guys, but the desire is certainly there. Nonetheless, an active defense is absolutely called for.

One of the common tools that the bad guys use to attack networks are scanning tools. Whether it's a purloined legal scanner by a real company or an underground tool, attackers want to understand and map out their victim's sites

before “entering.” So what happens? Companies spend hours and weeks to scan their own networks, fix as many vulnerabilities as they can... but there are always a few left. You can’t remove all functionality in the name of security.

And what happens? After you’ve done your best, the bad guys come along, use their scanning tools and your defensive efforts now tell them exactly where to attack. They won’t go after the things you have fixed; they’ll go after the open electronic doors and windows... which their scanner points out to them. Your best Protective security efforts are now working against you! You’ve reduced your target suite and told them exactly where to attack. Counterproductive, don’t you think? So try using some Deception against them! Some of the benefits are seemingly obvious.

- Works against insider and outsiders
- Apply tried and true techniques
- Ambush the attacker
- Make attacks riskier proposition
- The enemy is never really certain
- Automatic hands-off management detection/response

The Many Faces of Deception

Deception comes in many guises, and no one deception reaction is “Just Right” for everyone all of the time. (Common sense, by now, I hope!) Deception offers an entire suite of capabilities, and they should be picked judiciously in any application. The following is a useful Deception taxonomy based upon military experiences and history.

Concealment

Physical: Hiding through the use of natural cover, obstacles or great distance. Trees, branches; Terrain; Mountain Passes; Valleys

Virtual: Use best defensive practices for ‘real’ network services: Patches, Service Packs, Policy, Configuration. The object is to properly use and manage those basic security services that come with protective products and general applications.

Camouflage

Physical: Hiding movements and defensive postures (troops) behind natural camouflage.

Virtual: Hide the vulnerable points with network access rights, archiving, etc.

False/Planted Information

Physical: Letting opposition have the information you want them to have. Planting information you choose. False radio broadcasts, morphed pictures, videos and other misleading information aimed at enemies, leadership and general populations.

Virtual: Broadcast false network information from servers that are being scanned. Use the wrong IP address and the right IP address and other conflicting information to confuse your network adversary.

Ruses

Physical: Where equipment and procedures are used to deceive the enemy; carry their flag/colors; march troops in the same formations; use the same uniforms and adversary radio frequencies (false orders). Initiate cries of help as if from the enemy troops.

Virtual: Have the computer tell the attacker it senses a legitimate scan being conducted. Reinforce to the attacker that he is safely doing what he is doing. Pretend to be another hacker working on the same system. Again, one goal is to keep the hacker there for longer periods of time to gather forensic information.

Displays

Physical: Make the enemy see (or think he sees) what isn't really there. Horses pulling logs, 1,000's of campfires, Fake artillery, Rubber Tanks, Dummy Airfields.

Virtual: Tell attacker you are calling the IP-Police; create a fake CERT alert; tell them you are 'Tracing' them; show fake firewalls and IP barriers

Demonstrations

Physical: Make a move that suggests imminent action; moving troops to the left, when really want to attack on right; move troops constantly back and forth.

Virtual: Create an automatic defender which seems to follow the attacker; create a daemon which appears to launch a log/sniffer action or a trace.

Feints

Physical: An attacking demonstration. Use false attacks as a means of covering up the real mission/movements. Use false retreats to encourage chase by other side

Virtual: Appear to be only looking at the attacker when really switching defense modes. Appear to be helpless and defenseless when launching other means. Start an automatic response then stop and seem to try something else,

but really maintain first one. Be loud about all moves by telling your adversary, or appearing to be so stupid, he thinks he listening to your moves and you don't know it.

Lies

Physical: Lie to the enemy in any way that suits your needs. Use the media to lie. Use perception management. Creative perception management based upon what you want the attacker to believe. Initiate protracted, but futile negotiations. Circulating false reports to the Net. Fabricating treasonable letters

Virtual: Use electronic lying in same way. Let the system tell the attacker anything that furthers *your* goals. Creatively use perception management. Initiate protracted, but futile negotiations. Circulating false reports to the Net. Fabricate treasonable letters

Insight

Physical: Outthink one's adversary. Study their past engagements and learn from their mistakes. Know your enemy better than he knows you. Stay one step ahead. It's a chess game: predict your opponent's moves.

Virtual: Understand their motivation. Learn the techniques. Collect logs of previous activities. Recognize ankle-biters from serious attacks from professional attacks. Research is currently being done to understand hacker motivations, map those against technical skills and techniques and then develop predictive models based upon early attack detections.

Honey Pots

Physical: Make something so attractive a target, your enemy comes running into your trap. Think Indians (oops! Native Americans from the 1800s) and employ sneak attack/ambushes.

Virtual: Clifford Stoll placed seemingly valuable national secrets on his computer to draw in the attackers. Create files with attractive information. Come and get it! Privacy Violations: medical, salary, etc. Rich intellectual property. Corporate secrets. New products. Classified military information. Secrets of Saddam. Then Trap, Track & Trace.

Anything goes with Deception!

Lies'R'Good in these cases, so use them. The construction of custom deception suites is an attractive means for specific applications and industries who want to use deception:

- Suck the attacker into a mirror of your Web banking applications to get the bad guys into a harmless area where you can watch, collect

information and trace. The main Web banking application remains uncorrupted and functional.

- Brokerage firms can Honey-Pot the attackers into private information files/directories which are really meaningless. Suck them in with “private confidential investment information.” Maybe even encourage them to lose money!

Law enforcement, military and government sites will be using the same approaches by picking and developing appropriate deception suites that meet their specific goals. I would recommend that you speak with legal counsel with real Cyber-knowledge, about the proper means to collect forensic information that can be used in subsequent prosecutions.

Deception is deceptively simple to use as long as you understand some of the fundamental Rules of Deception.

1. Hide your moves from your opponent
2. Never let your opponent see you as you are
3. It's all about time. Waste their time in their useless attacks and keep them around so you can trace them.
4. Announce your Deceptive existence to scare them away in short order.
5. Using TBS principles, Deception should operate at very high speeds, lowering (**D + R**).

Remember, *“There can never be enough deception.”*

Sun Tzu

Resources:

1. “Time Based Security” by Winn Schwartau
2. Go to Fred Cohen's ‘<http://all.net>’ for a look at his Deception Toolkit.
3. Search on “deception”, “Honeypots” and “network Deception”. This is so new, you may not find a lot.

SIDEBAR

How I Got Back At The Hackers

Homemade Detection and the DTK:

By Fred Cohen

The bad guys have been lying all of their lives.

They lie to get what they want from basically honest people who are trying to get along in life. Now I was brought up to believe that lying is wrong, and I try not to lie. But in 1998 I got tired of being lied to and tired of being prevented by law from doing to the bad guys what they have been trying to do to me for a long time. So I decided to get even. Here's how I did it.

For years people that break into computer systems have been harassing me because I work on finding new and improved ways of keeping people out of computers they don't belong in - while making those systems easy to use for the people who do belong there. A few years ago, I decided to try notifying the owners of systems every time somebody from their system tried to get into my system. The bad guys got really hot about it because a lot of them started getting caught or losing their access to computers they broke into. So they started telling lots of lies about me and publishing them all over the Internet. The people who put up these articles refused to allow me to put up my responses. Other folks tried to get my power and phones shut off, told folks all over the world that I had illegal software on my site, and on and on. After a while, I even got used to this.

But then recently, folks started using automatic tools to scan computers all over the Internet for vulnerabilities so they could run their programs all day and, when they got around to it, they could get the list of vulnerable systems and break in to them in their spare time. It started small, but these days, the average computer on the Internet full time gets 'tested' by one of the crackers a few times per week. The courts have even ruled that, like somebody who walks through a neighborhood turning doorknobs, until they actually break the plane of the doorway, or in this case, till they actually start to use your computer, nothing can be done.

I decided that enough was enough. If they were going to look for vulnerabilities, I decided they were going to find them - lots and lots of them. So many of them, in fact, that they would have to spend all of their time trying to figure out which of the supposed vulnerabilities were real, and hopefully, they would give up long before they ever got to a real opening. And - oh yeah - just like folks who enter the front door and are met with a second locked door, they have broken the barrier plane, and unless I miss my guess, they can be arrested and prosecuted.

That's when I invented the Deception Toolkit (DTK). The Deception Toolkit allows people who own computers to lie to the bad guys just like the bad guys lie to them. When a bad guy comes up to my computer and tries to guess a password, it works - except that it's all a lie. When they think they have gotten my credit card numbers, they have only gotten an invitation to get arrested. While they think they are fishing around in my system, I am tracking them down.

And the best part of it is, I have given this away for free so that hundreds and thousands of systems can put up similar lies and make the bad guys' jobs even harder.

Thousands of people, companies, government agencies, and others have now come to my web site (<http://all.net>) and gotten copies of the Deception Toolkit. Many of them have reported back to me that when they turned on the deceptions, the attacks they had been missing become clear as day. Others have reported finding new types of attacks through DTK's logs of activities. I don't know how many groups or sites places are using deception today, but I do know that the bad guys really don't like it.

Of course there are other things you can do with deceptions, and DTK is only a simple lie that makes it very hard to go completely unnoticed when you attack systems from afar. Against insiders with a lot of knowledge, DTK doesn't work as often, mostly because its lies are general purpose and people who work in a company can often tell the difference. So when you want to use the very best, you need to build a custom deception.

I have told many people about the idea of using deceptions for defense. In fact, I know of a few government projects that have started to look at the use of deception to protect critical infrastructures against bad actors and information warfare attacks. I hope it works for them as well as it has worked for me.

BIO:

Fred Cohen is a long time expert in information protection today. He teaches computer forensics at The University of New Haven, provides corporate security consulting for major corporations, and runs the **all.net** Web site where you can play computer security games, read articles, and check out his security database.

END SIDEBAR