Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Warfare: The Unconventional Art In A Digital World

Conventional warfare with the use of tanks, aircraft, ground-troops, submarines, missiles, and defense systems, is starting to be replaced by the firing of binary digits across a vastly different battlefield then in decades past. Information warfare is the new art of subverting your enemy in the new battles of the 20th century and beyond. Today you don't have to physically be on the battlefield, or even be a part of the military to be surrounded by a new evolution in war that has reached it's outstretched arm into the ...

Copyright SANS Institute
Author Retains Full Rights

AD

Beating the IPS?

STONESOFT
Can't be Beat

Learn More

Information Warfare: The Unconventional Art In A Digital World
Eric Hrovat
June 30, 2001
Ver 1.2e

Am I In A War?

"The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeros, little bits of data. It's all just electrons…There's a war out there…and it's not about who's got the most bullets. It's about who controls the information. What we see and hear, how we work, what we think, it's all about information"(2). –Unknown-

Conventional warfare with the use of tanks, aircraft, ground-troops, submarines, missiles, and defense systems, is starting to be replaced by the firing of binary digits across a vastly different battlefield then in decades past. Information warfare is the new art of subverting your enemy in the new battles of the 20th century and beyond. Today you don't have to physically be on the battlefield, or even be a part of the military to be surrounded by a new evolution in war that has reached it's outstretched arm into the homes of many. How can this be true?

The Air Attack Scenario vs. A Cyber Attack

An enemy aircraft is sent on a mission to penetrate your defense system and destroy everything in sight. The aircraft leaves it's home base and enters your airspace, early warning radar has just sent you the alert. Is it friendly, foe, or exercise? The soldier is scrambling to decide if he should launch countermeasures, the enemy aircraft launches a missile, and your chaff system is deployed. You now have realized the danger, and start to bring up your physical barriers, but it is too late. Your last resort is to grab a shoulder launcher and destroy the aircraft, you shoot, and bang the enemy aircraft is destroyed.

Like the aircraft scenario, an information warfare attack can be surprisingly similar. Instead of an enemy aircraft, it is an enemy packet. A denial of service packet is sent to destroy your network. The intrusion detection system sends an alert to the console, the analyst must decide if this is a false positive or not. Time is ticking and the packet is still flying, it passes through your firewall like a rocket through the sky, and impacts into one of your core routers, shutting it down like a building crumbling to the ground. As you can see the warfare maybe different, but the overall techniques and methods are quite similar.

Information Warfare Defined

Information is defined by the American Heritage dictionary as; 1. Knowledge derived from study or experience. 2. Knowledge of an event or situation: intelligence. 3. A collection of facts or data. 4. Informing or being informed; communication of knowledge. 5. A non-accidental signal used as input to a computer or communications system. (1)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The definition of warfare is defined by the American Heritage as; 1. The act of waging war. 2. Conflict: strife. (1)
Combining the definitions, you have a definition of information warfare as, the act of waging war, or conflict by knowledge, study, experience, data, or the non-accidental signal inputted into a computer or communications system.

Dr. Ivan Goldberg defines information warfare as, "the offensive and defensive use of information systems to deny, exploit, corrupt, or destroy, an adversary's information, information-based processes, information systems, and computer-based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries." (4)

If you dissect Goldberg's definition of information warfare, you will notice that the tactics of war have not been changed dramatically, only the medium has changed. Utilizing either definition, you have a maturation of a warfare tactic that has been around for centuries. Information gathering, corruption, denial, exploitation, and intercept have been around for centuries.

Evolution of Information Warfare

Information gathering has been around since the first spoken or written words evolved. Dating back to the first wars, information has played a major role in warfare. In decades past, information was passed between allies on written mediums, spoken words, radio waves, and even smoke-signals. The art of information warfare also dates back in history to these types of communications. Agents were sent into enemy lines to impersonate allies to gather information that may be spoken, or written, between the opposing sides. The art of information gathering has not dramatically changed over the course of history.

World War II marked some evolutionary changes in warfare and tactics to include large-scale air-to-air combat, strategic bombing, naval carriers, and the use the atomic bomb. WWII also marked cornerstones in the use of information warfare as a new tactic in defeating your enemy. World War II was a milestone in communications with the use of radio waves to transmit information over great distances and enemy lines to allies in support of strategic, and tactical planning. The transmission of communications also spawned the need for offensive and defensive measures. The Germans employed a defensive measure of encryption using the infamous Enigma machine to send enciphered messages over the airwaves to troops on land, sea, and air. The tactics of intercept and deception were employed during World War II against the Enigma cipher and have proven to be key to the Allies success in defeating the Germans. The Allies used offensive measures in information warfare by intercepting, and deciphering Enigma messages, as well sending enciphered messages for deception. The art of information warfare employed in this part of history has proven to be a major advantage and key in the Allied victory in World War II.

"You must realize that the enemy is probably listening to every message you pass on the air and is well aware that there is a possibility that he is being bluffed. It is therefore

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

vitally important that your security is perfect; one careless mistake may disclose the whole plan" (5).

The Gulf War also marked historic events in the use of information warfare as a key to winning in the battlefield. The use of space assets, both military and commercial, provided Coalition forces with communications, navigation, surveillance, intelligence, and early warning in the victory over Iraqi forces. The lack of defensive measures in the arena of information warfare proved to be a key in defeating the Iraqi troops.

A more recent display of information warfare began after the emergency landing of a United States recon aircraft, the EP3-E Orion, on Hainan Island, a Chinese island in the South China Sea. After the release of the aircrew from Chinese control, heated debates began on the return of the aircraft to the United States. The debates also induced conflict, or war between Chinese and American cyber-warriors, or hackers. The attacks concentrated on each rival country's Web sites. Chris Rouland, of Internet Security System's X-Force, was quoted to NewsFactor as saying, "that there are now 40 to 50 attacks on Chinese and American Web sites per day by hackers in opposing countries, versus one or two per day before the spy plane incident." In retaliation to U.S. attacks on Chinese websites, Chinese hackers were quoted as to be preparing to fight back with a weeklong attack on U.S. based Web sites, beginning on May 1st. During the cyber stand off the departments of Interior and Energy, National Park Service, and even the White House were victim to cyber warfare. This event was not the first time Chinese hackers have united to wage information warfare on the United States. After the U.S. bombed the Chinese embassy in Kosovo, in May 1999, government sites were crippled for days by Chinese hackers. (7)

The year 2000 witnessed a report of as many as 155 U.S. government computer systems that were targets for cyber warfare. (3) The increase in information warfare over the Internet has increased awareness around the globe, and the development of response teams such as the National Infrastructure Protection Agency, to help protect American systems from being targets of such attacks. Like the formation of the National Security Agency after the Morse code intercepts during World War II, new organizations are being developed across the globe to help protect the Internet from this unconventional art of warfare. Computer Emergency Response Teams have been assembled in government sectors, to include the military, and even in the civilian sector to help combat the storm of bit wars e being waged over the new battlefields.

Offensive Tactics

Information warfare in the computer age has developed new offensive tactics much like the tactics of old, but over a new transmission medium. The offensive tactics that are being employed are deception, intrusion, denial, corruption, and passive intercept, to name a few.

For example, instead of someone transmitting Morse code to deceive the sender or receiver, they are now using the art of deception over the Internet. Deception can be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

accomplished on the new battlefield by IP spoofing, and mail spoofing, as examples. IP spoofing is defined as when a system attempts to illicitly impersonate another system by using another IP network address. For example, if a network had an address of 204.189.72.x, and attacker would use special software to impersonate a host, or server on that network to gain access. Impersonation and intelligence gathering can be accomplished with a well-known Linux tool called NMAP. If the IP was already in use, the attacker would have to deploy another technique known as denial, in able to impersonate the attacked system.

In warfare of past troops denied their enemy from receiving supplies, now it is used for denying your enemy information. Similar warfare techniques use jamming or denial, by radio signals, radars, or even microwave, and created the same technique in the digital age. Denial is accomplished by a method known as a denial of service. Denial of service is defined as an action or actions to prevent any part of an AIS from functioning in accordance with its intended purpose. (6) Some of the most well known denial of service attacks are; Smurf, Teardrop, Ping of Death, and Land Attack. Distributed denial of service is also another method in denying a system from its intended purpose. The difference between the two is that a DDOS is staged from multiple systems, where a DOS is from a single system, and the damage can be much more devastating. Examples of DDOS attacks are Trinoo, TFN, and TFN2K.

Intrusion in the past may have been an enemy spy, a listening device, antenna, or even an aircraft. Today intrusion can be described as a set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource or system. Intrusion in the digital age can be accomplished by techniques such as password cracking, back doors, or social engineering. Password cracking can be described as brute force guessing a password with the use of a dictionary attack, or the use of social engineering to trick the victim into releasing their password to the attacker. Social engineering is described as impersonation, or trickery by language, to gain information about a person, place, or information system, and is used as a tool of deception. A back door is defined as a hole in the security of a computer system deliberately left in place by designers or maintainers. (6) Some of the most popular back door programs are Back Orfice, BO2K, NetBus, and Subseven. The combination of password cracking, social engineering, and back doors, can let an attacker gain access, or intrude on an information system.

Corruption is the intended or unintended changing of original information. Corruption is achieved after a system is intruded upon, or by a malicious program called a virus. A virus is a program that can "infect" other programs by modifying them to include, a possibly evolved copy of itself. Some of the most recent and well-known viruses have been Melissa, I Love You, and Miss World, to name a few.

Passive intercept is described as gathering information without the sender being aware. Passive intercept before the digital age could be accomplished by using a radio antenna to listen in on your enemy's communications. Today, passive intercept on the Internet is being done with the use of a tool called a Sniffer. Sniffer is a program to capture data

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

across a computer network. Sniffers are used to capture user ids, and passwords, without the sender being aware of it. (6)

Defensive Measures

Conventional warfare had to have defensive measures in place to combat the enemy attacks, and now new unconventional warfare must have the same defense measures to protect information. Physical defense measures of conventional warfare may be early warning radar systems, chaff, physical barriers, and troops, to name a few. Information warfare counter-measures are intrusion detection systems, firewalls, virus detection software, vulnerability scanners, encryption, and security analysts, to name a few.

Intrusion detection is defined as techniques that attempt to detect intrusion into a computer network by observation of actions, security logs, or audit data. (6) Intrusion detection systems are much like an early warning radar in an air defense system. An enemy packet is much like an aircraft intruding into your airspace. The aircraft will only be detected by the radar system and flagged as hostile or friendly. Much like the aircraft the enemy packet will be identified by a defined list of attack signatures and communicated to a central terminal for action. The ultimate responsibility for identification is still reliant upon the operator. The system will not stop the attack, but merely provide a warning that it is underway. Popular intrusion detection systems are Snort, ISS RealSecure, and Network Flight Recorder.

After the enemy passes the early warning system, another defensive measure must be in place. Conventional warfare uses chaff to block or deter incoming methods of destruction like missiles, or rockets. Information warfare deploys the use of a firewall, and much like chaff, firewalls are for deterring, or blocking, unwanted traffic from breaking your barriers. A firewall is defined as a system, or combination of systems, that enforces a boundary between two or more networks. (6) The firewall, like chaff, is used to block incoming enemy fire by a defined set of rules. Examples of firewalls include, Firewall-1, Raptor, and Gauntlet.

Virus software is like your physical barrier in the air defense system, and is there to protect the inner working of your system. Virus software identifies and eliminates programs intended to be destructive, or modify your information.

Vulnerability assessments are used to examine your information structure to determine the adequacy of security measures, deficiencies, and provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (6) In traditional warfare, air defense exercises to test the posture of your defense would resemble the art of vulnerability assessment in information warfare.

Your final line of defense in any system is your troops, or analyst, when dealing with warfare. Trained professionals, whether in the art of conventional, or information warfare, are your greatest assets in defense.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

1. American Heritage Dictionary 3rd Edition. Dell Publishing. New York. 1994.

2. FAS. Intelligence Resource Program. Information Warfare and Information Security on the Web. http://www.fas.org/irp/wwwinfo.html#infowar June 30,2001.

3. Gebler, Dan. NewsFactor Network. U.S. Government Computers Widely Hacked in 2000. Online: http://www.newsfactor.com/perl/story/8758.html April 6, 2001.

4. Institute For The Advanced Study Of Information Warfare. http://www.psycom.net/iwar.1.html June 30,2001.

5. McLendon, Col James. Information Warfare: Impacts and Concerns. Ch 7. http://www.airpower.maxwell.af.mil/airchronicles/battle/chp7.html June 30,2001.

6. NSA Glossary. SANS Institute. http://www.sans.org/newlook/resources/glossary.htm#D June 30,2001.

7. Sausner, Rebecca. NewsFactor Network. U.S., Chinese Hackers Wage Quiet War. Online: http://www.newsfactor.com/perl/story/9203.html April 24,2001.

© SANS Institute 2003, Author retains full rights.

Last Updated: September 5th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced