[FIRST EDITION]

Decreasing Security in Increasingly Connected World: Uses of D.S.S. and Intelligent Systems in Computer Security ?

Written by Yakov Shafranovich, CIO of SolidMatrix Technologies, Inc.
Published on May 2nd, 2002, last updated on May 2nd, 2002.
[DOC. ID: YS-05012002-001]
?
Contact: research@solidmatrix.com
Published by Research Division, SolidMatrix Technologies, Inc.
Brooklyn, New York, United States of America
www.solidmatrix.com
?

1. Introduction.

As more computers are connected together than ever before, the need for better security becomes more urgent. What was unthinkable yesterday and theoretical today, becomes reality tomorrow. A teenager tapping away at a keyboard thousands of miles away can cause more damage to a military installation than a saboteur breaking in physically. With the increased need for security, the workload needed to secure and maintain secure systems becomes greater and greater with each passing day. While twenty years ago an average system administrator had to only worry about local users who amounted to tens or hundreds of people, nowadays one must take into account not only local users but for hackers from every corner of the world. The increased workload on system administrators everywhere increased the need for computer assistance with security tasks and various intelligent systems begun to be developed. On the other side of the fence, the hacker side, the increased security of systems called for intelligent systems to be used more often to assist in attacking. Thus, both sides are using decision support systems and intelligent systems to attack and defend computer systems around the world.

In the traditional sense DSS and intelligent systems are used by business to make better decisions and in the security arena they assist both the defenders and the attackers to make better decisions about offense and defense of their systems. However, unlike in business, many of the intelligent systems in the security field do not just support the decision maker but partly implement his or her decisions by automating some of the tasks involved. The load on both the attacker and the defender is too great to be borne by humans, and thus it is increasingly parceled off to computers.

2. Information Warfare Model.

Computer security is often compared and modeled after other things. Denning (1999) considers it part of a broader field called “information warfare” or war over information. Others consider it more like a game where the one side tries to attack while the other player defends. Still others think that security of computer systems

correspond to security of biological organisms where various systems of the body defend the organism from various attackers such as bacteria, viruses and other external forces.

Denning's model defines information warfare as an operation between two players: offense and defense. The two parties fight over information resources such as controls of computer systems and possession of data. Each information resource has a specific value to each player based on the combination of six factors: (1) player's concerns and commitments, (2) player's capabilities, (3) availability of resource to the player, (4) availability of resource to other players, (5) resource integrity and (6) time. The first two factors define the value of the resource to the player or to external processes that are valuable to the player. A good example of this would be classified information stolen either directly for a foreign government or by someone sympathetic with that government. The next two factors contribute to the value of the resource based on how available it is to the player and others. Something in public domain has no value compared to the Coke formula which is a trade secret. The last two factors define the value of the resource based on how reliable the resource is and how timely is the information.

The two players in information warfare are defense and offense. Even though we generally assume that offense is the "bad guy" and defense is the "good guy" this is not necessarily true. When the United States government targets terrorist organizations, it is considered an offense player but not the "bad guy" (at least to us). There are many offense players including insiders, hackers, criminals, companies, governments, terrorists, political activists and others. Offense players launch attacks against information resources which in turn are defended by defense players. The offense players seek to exploit the resource thus increasing its value to them while decreasing its value for the defense. The offense seeks to do so in three ways: increasing availability of the resource to the offense, decreasing integrity of the resource to the defense and decreasing availability to the defense. The defense seeks to reverse these three by preventing availability to the offense, ensuring integrity to defense and ensuring availability to the defense.

3. Overview of DSS and Intelligent Systems in Computer Security.

In the context of computer security various intelligent systems and decision support systems are increasingly used to assist both the offense and the defense players. However, due to the unique situations faced by both hackers and security professionals they are used in very unusual and innovative ways. Traditionally DSS systems were developed to assist managers with making decisions. Turban (2001) mentions some of the reasons that they were developed: ability to perform speedy computation, increased productivity, ability to combine many disparate data sources, increase quality of decisions, business process reengineering and overcoming cognitive limits of human beings. Many of these reasons also apply in the security arena albeit with a twist.

On the offense side the main reasons driving the development of these systems is increased productivity, ability to perform speedy computation and pushing cognitive limits. The offense side mainly seeks to increase the performance of attacks while decreasing the time spent by the human attacker on analyzing and attacking each system. This is accomplished by implementing DSS and other intelligent systems that assist the human attackers with making decisions about how to attack and also take off some load from the human attacker by partly automating the attacks. In certain situations such as when the attacker is a government or an intelligence agency, they will usually also maintain an extensive knowledge base about their targets. Good examples of this are the extensive databases maintained by the Central Intelligence Agency and the National Security Agency. An unclassified example of such database is the CIA's World Fact book which contains a brief synopsis of every single country and government in the world. Other examples of DSS systems used by the offense are worms, coordinated DoS systems, port scanners such as SATAN and packet sniffers.

On the defense side the same reasons apply in order to properly counteract the offense. However, a need to combine data from many sources such as network management programs on several platforms is also present. The other reasons mentioned by Turban (2001) stand out more on the defense side rather than the offense side since the defense side is usually more coordinated and more resources are required for defense. Example of DSS systems used in defense are intrusion detection systems, network monitoring programs such as Unicenter® and knowledge bases of prior attacks.

In the business world, the development of DSS systems had slowly shifted from structured problems to semi-structured and unstructured problems. The computer security field lags behind, and has only recently begun to implement DSS systems for semi-structured problems. Majority of DSS systems used in computer security are intended to solve structured problems such as finding an open TCP/IP port on the target system or detecting excessive network activity. More complex problems such as automatic detection of virus-like activity and network intrusion, coordinated denial-of-service attacks and viruses detecting anti-virus programs are semi-structured problems and have only recently begun to be covered with intelligent systems. Most of semi-structured and unstructured problems in the security field remain under the control of a human operator with various intelligent and DSS systems assisting the operator with more simple tasks.

Even though in the traditional definition, DSS use is categorized by operational, managerial and strategic levels, in the security field these categories are blurred. Most of activity in the computer security is done on the operational level with various players attacking and defending each other. Only recently have we seen DSS systems being developed to assist with planning out managerial and strategic levels of offense and defense. Mainly these have been left to government and intelligence agencies which have the skills, resources and the incentive to develop them. DSS systems that figure out how to best attack other systems, intelligent agents traveling throughout the network looking for security holes and plugging them, intelligent systems that figure out the best defense plans for a specific situation, remain mainly in the realm of science fiction at the moment. However, government and various intelligence agencies are much more advanced in the field and may very well already have developed these.

4. Transaction Processing Systems (TPS).

In a business, a transaction processing system (TPS) is usually a system that is used to run the business. This system processes the most basic transactions in the business such as accounts payable, recordkeeping, inventory, etc. In computer security there are several systems than handle the most basic day-to-day security tasks. On the defense side there are various tools that keep track and process routine security requests. On the offense sides there are various types of attack programs.

4.1. Defense: Password Files, System Logs, Firewalls and Cookies.

First of all, there are many databases that maintain login information and passwords for users. Most modern operating systems ranging from Microsoft® Windows® to Linux support multiple users. To differentiate between users, each user is assigned a unique login name and a password. This information is stored special databases, usually protected or encrypted in some way to safeguard the information. The encryption methods vary from system to system, from UNIX's crypt() function to Microsoft's weak encryption.

Most of the time these databases are also linked to system logs which record various events that take place on the computer. Depending on the operating system and settings used, logs can capture basic information like a user logging in and out to extensive data like every keystroke and command that the user types. These logs are the workhorses of the security world: most of every-day work revolves around them. These can be compared to a financial transaction system in the business world. In the computer world, these systems perform a similar function: recording every basic security transactions which are user logins and logouts. In additional various other logs such as website logs, file logs, etc. keep track of many other events that happen to the computer and when combined with the security logs provide a more complete picture.

Firewalls are also basic systems used in computer security. The name "firewall" originates from the coal-powered railroads of the late 1800's. In the coal locomotives of those days, the back of the locomotive contained a large steel wall to separate the locomotive from the rest of the train. The intent was that in case the locomotive catches fire (because of the coal dust and the coal stored in the back), the rest of the train will survive unscathed. In computer security, a firewall separates an internal network from a public network such as the Internet OR from another private network. The firewall acts as a filter between the two networks deciding which data goes through and which data does not. Firewalls are basic systems used in computer security to protect and direct network traffic.

Cookies are a special example of a security TPS. Cookies, first invented and used in Netscape's Navigator v2.0, are small pieces of text residing on the computer of the user. These pieces are deposited and read by the various websites that the user visits. In the security field, they are used to keep track of session information and determine who is currently logged in. Much discussion in the recent news revolves around the privacy aspects of cookies since they can be used to track someone's browsing habits over time.

4.2. Offense: Denial-of-Service Tools, Password Crackers, Network Sniffers, Viruses, Trojan Horses and "Other Creatures That Go Bump in the Night ".

There are many systems and utilities that are used for every-day hacking attempts. These can be classified under TPS since they usually do not possess much intelligence and are used for routine "hacking transactions". The lowest and simplest are Denial-Of-Service tools (DOS) which are basic programs or utilities that are used to generate useless network traffic. These tools are usually used in many numbers when attempting to slow down or shut down a system by generating huge amounts of traffic. These vary from basic "email bomb" programs to sophisticated distributed systems running on thousands of computers. Their methods also vary from simple email or network traffic, to complicated tricks that exploit various security holes in software (e.g. 'Ping of Death'). They are the most commonly used tools on the offense side.

Various password cracking tools are used to guess passwords. Many times these tools are used either directly on the target system or more often with a password file that is stolen from the target. Since password files are usually encrypted, password crackers utilize a variety of techniques to guess them. These range from using common words and passwords, to sophisticated "dictionary" attacks utilizing a dictionary of words and trying them against the target.

Network sniffers are used to "sniff" or record network traffic as it passes through a specific system. Many times passwords and other sensitive information are sent without being encrypted. Email, which is the most popular application on the Internet, is usually sent like a postcard – bouncing from server to server, open for anyone to be read. Network "sniffers" are usually installed in a router or some computer that sits between two networks and just record passing traffic. They are also used in law enforcement, especially by the FBI. The FBI's system called DC-100, or more commonly known as "Carnivore", is installed at ISP's and record network packets.

Viruses, trojan horses and similar program that are the most common attack tools used. The difference between viruses and trojans is that a virus usually hides from the user while a trojan masquerades as a legitimate program. Viruses also tend to replicate from computer to computer while a trojan doesn't necessarily do that. The difference between the two as well as other associated "creatures" is becoming blurred. The intent of both can be two-fold: one is to cause havoc and second to obtain confidential information from the user's computer. One of the most famous trojans is called "AOL Gold", which was used to steal password from AOL users. The author of the virus or the trojan doesn't necessary create or release them for those reasons – sometimes it could be simple bragging.

5. Management Information Systems (MIS).

MIS systems are a step above TPS and are usually imbued with some intelligence. However, their intent is more to provide information rather than make decisions. The same applies for the MIS systems used in the security field – they collect and compile information.

5.1. Defense: Networking Monitors and Antivirus Utilities.

On the defense side there are networking monitoring programs and antivirus utilities. Programs that monitor network traffic ranging from firewalls to software utilities and antivirus programs both record and analyze activity. While the network monitors concentrate on network activity, antivirus programs look for file and program activity on individual computers and email systems. Both are usually set to look and record some form of indicators, and alarm the system administrator or the user if they find something unusual. However, most of these tools do not collect enough information to be full-fledged DSS systems. Antivirus utilities usually also contain some mechanism to quarantine and/or clean the infected files but not smart enough to be

considered a DSS. This is in line with the general trend in computer security to automate menial and repetitious tasks in order to give more time to humans.

5.2. Offense: War-dialers and Network Scanners.

On the offense sides there are war dialers and network scanners. Both are intended to scan and collect information about target systems. "War dialers" are software programs dial all or a range of phone numbers in a specific area code looking for fax machines and modems. "Network scanners" such as SATAN (**S**ystem **A**dministrator's **T**ool for **A**nalyzing **N**etworks) are used a similar fashion to find "open" TCP/IP ports on target systems. Open ports are analogous to modems on phone lines – they indicate that there is a computer program on the target system that is listening to traffic on those ports. The information from these tools is compiled and presented to the offense player so he or she can take action.

6. Group Support Systems (GSS): IRC, Newsgroups, Mailing Lists and Bulletin Boards.

In security knowledge and information is everything. Both the defense and the offense sides (usually security professionals and hackers) exchange and distribute security-related information via a variety of technologies that can be classified as GSS systems.

IRC (**I**nternet **R**elay **C**hat) and similar "live" chatting technologies allow hackers and security professional to meet together online in a virtual environment and exchange information and tips live. This is very similar to telephone conferences and IRL (**I**n **R**eal **L**ife) meetings. Sometimes hackers utilize the anonymous aspect of IRC and chat with newspaper reporters in order to brag about their exploits. IM (**I**nstant **M**essaging) is also another similar technology that allows people to exchange messages live. Unlike chatting which is akin to a telephone conference, IM is more a like a telephone call between two people.

Newsgroups, mailing lists and message boards allow security professionals to exchange information about different security holes and procedures. However, unlike chatting they are not done live and are usually disturbed to thousands and sometimes millions of people. The downside is that it is not done live so there is a delay while the information is being distributed. This delay sometimes is significant enough to make or break a specific security problem. Hackers likewise utilize these technologies, albeit to a lesser extent to exchange tools, pirated software, credit card numbers and tips.

BBS (**B**ulletin **B**oard **S**ystems) used to be the main GSS technology used by both security professionals and hackers alike. A BBS system is usually a piece of software running on a computer with one or more modems. Users dial-in and get connected to the software. There they can exchange files, email and chat (on multi-modem systems). However, due to advent of the Internet their use is rapidly dwindling except in less connected areas of the world and they are still widely used by hacking groups to distribute pirated software.

7. Decision Support Systems (DSS): Enterprise-wide Security Monitoring and Target Evaluation.

The real DSS systems in security are the ones that aggregate and assess information from the entire enterprise. They parse various log files, interact with MIS systems, collect data from expert systems and intelligent agents, evaluate the data based on information from KMS, GIS and GSS systems, and produce results that assist the decision makers. In some systems, the decision maker can direct the DSS system to implement his or her decisions. Example of DSS systems are ACID, Tivoli's UniCenter, and product sold by ISS (Internet Security Systems).

On the offense side, there are various systems possible in theory that would aggregate information from various attack tools, analyze them and present the results to the user similar to the systems used on the defense side. But, unlike the defense side where there is a commercial incentive to develop these systems hackers usually do not possess the same incentive. Thus, DSS use in offense is very limited except for government agencies like the NSA where the usage cannot be assessed because of their classified nature. However, eventually the use of DSS systems by the defense, increased effort needed when attacking systems and the

increasing amount of information needed to attack a system, will force the hacker community into developing more advanced DSS systems.

8. Expert Systems, Neural Networks and Intelligent Agents.

There are various intelligent systems that are increasingly used in security. Since more and more tasks are required to be performed by both defense and offense sides, there is always a great demand for automatic and semi-automatic tools to lighten the load.

8.1. Defense: Intrusion Detection Systems and Heuristical Virus Detection.

On the defense side, the most advanced use of intelligent systems is in intrusion detection. IDS or **I**ntrusion **D**etection **S**ystems are a more advanced version of network monitoring utilities. They started off by looking for anomalies in network traffic as opposed to just record traffic. These anomalies can be reported to the user OR the system can respond to the automatically. Most of today's IDS systems only report attacks and do not respond to them. The response capability is something that has only been recently being built in. However, IDS systems have one major flaw: they look for predefined attacks either hard-coded into the IDS or based on the data contained in a KMS or GSS system. Recently a push has been towards more automated response capabilities and towards more flexible IDS systems. This flexibility is expressed by having an IDS look to unknown or suspicious activity even if it not a known attack. Many of these proposed IDS systems are based on the knowledge and workings of the immune system in our bodies. Lee (2001) proposes such system called "CDIS" that combines several intelligent systems techniques including evolutionary and genetic programming, neural networks and expert systems to detect suspicious behavior. Also, Allen (2001) cites many examples of practices for system administrators on how to look for suspicious activities, many of which can be semi or fully automated in an IDS system.

A more specific application of the IDS concepts cited above is heuristical virus detection. Anti-virus utilities have been around for much longer and there is a bigger commercial incentive to develop better anti-virus utilities. Therefore, many anti-virus companies started researching heuristical virus detection method where the program doesn't look for predefined "signatures" of viruses but rather tries to detect virus-like activity. As of today, most of commercial anti-virus packages incorporate some form of activity detection technology. However, IBM's research division went a step further. They have created a technology where the anti-virus program sends a suspicious file over the Internet to the main server where the file is analyzed automatically for virus activity and if the central server decides that it is in fact a virus, and then it sends out information about it to all other computers.

8.2. Offense: Network Analysis, Viruses Targeting Specific Systems, and Anti-virus Detection.

On the offense side there are also similar tactics are used to look for passwords and similar unprotected security information in network traffic. However, as mentioned before about DSS systems used for offense side, since there is little or no incentive to develop such systems. Thus, there are very few advanced detection systems that can analyze network traffic for security data. Also, hackers use IDS systems to protect themselves against counter-attacks by the defense.

In the virus field, it is a whole different story: there is a tremendous incentive to "protect" viruses from being detected by anti-virus programs. This started with polymorphic viruses that mutate and encrypt themselves to more advanced viruses that hide masquerade as other programs to viruses that detect and erase anti-virus software. Thus, virus writers are increasingly adding features to hide viruses from being detected and to automatically detect anti-virus programs.

A more recent and scary phenomenon have been viruses that have a specific payload which are mainly used for commercial espionage. These viruses are usually sent into the competitor's computer network and are written to seek and find specific information. Once that information has been found, like for example financial figure or merger information, the virus sends them back to its originators and erases itself. This trend will increase more as time goes on.

10. Knowledge Management Systems (KMS).

These consist of various databases that store information to assist security professional and hackers with various tasks. These are usually public Internet databases.

10.1. Defense: Security Holes and Antivirus Databases.

The defense side uses various public and private databases to keep track of various security holes and exploits. These vary from mailing lists, to websites and books like Allen (2001). In addition, antivirus databases are used to keep anti-virus programs up to date. Security holes databases are usually public maintained either by the government, industry associations, security companies or vendors. Private KMS systems are usually maintained in-house or by government agencies for internal use only, or to be shared within a closed group. Anti-virus databases are kept by the anti-virus vendors and security companies.

10.2. Offense: Hacking Manuals and Security Holes.

The offense side also uses the security holes databases to attack unprotected systems. Unlike the defense, the offense usually has access only to public databases which can sometimes give an advantage to the defense by withholding information from the offense. Hacking manuals and tips are shared among the hacking community and help various parties to attack systems. They also draw in amateur hackers who usually start off by using techniques describes in these manuals and eventually develop into more mature attackers. If the offense side is a government agency such as the NSA, they will usually have the widest scope of information available drawn from public and private databases. In addition, sometimes vendors will disclose helpful information or even cooperate with the government.

12. Geographic Information Systems (GIS): The Domain Name System, Internet Traffic Maps and Routing Tables.

In the security field various GIS systems are used to ascertain a location of a specific computer. The Domain Name System (DNS) managed by ICANN (Internet Corporation for Assigned Names and Numbers) provides contact information for every single domain name on the Internet via WHOIS. The IANA organization (part of ICANN) manages the IP numbers database of all computers on the Internet via regional registries such as ARIN and RIPE. These databases can provide both the offense and the defense with detailed location of almost any system on the Internet.

In addition to these, various routing tables and information is found on the Internet that can pin down a virtual path between two computers and mapped it in the physical world. A trace route command combined with ping and whois information, as well as the IP information maintained by IANA, can help trace any computer on the Internet to its physical location. Hackers hide from these methods by utilizing a variety of techniques ranging from taking over computers in order to launch attacks (zombies) to "spoofing" (hiding) the originating computer's address so it cannot be traced.

13. Miscellaneous: Open Source Intelligence, Psy-ops, Social Engineering, Insiders, SIGINT, and Encryption.

In addition to the systems describes above, both sides utilize many other techniques in the security field. Information culled form public sources (Open Source Intelligence) can provide a helpful insight into possible attackers or defenders of a specific system. Psy-ops and Social Engineering where in the attacker gets access into the system by fooling a human defender are also popular methods. As the matter of fact, the famous hacker Kevin Mitnick, used social engineering for to gain access to many of the systems he attacked. Psy-ops are usually some kind of psychological operations performed by either the military or intelligence agencies. Social Engineering is talking or convincing human defenders into granting access. Since humans can be fooled easier, more care must be taken into strengthening the human aspect of the defense.

Perhaps the biggest security threat to both offense and defense are insiders. There are many stories of when an insider broke into the system or allowed outside attackers in. At the same time many stories also exist of hackers ratting out their fellow hackers. Humans are not predictable and thus it is very hard to protect against these kinds of attacks.

SIGINT (**SIG**nal **INT**elligence) and encryption technology go hand in hand. The National Security Agency of the Unites States government (NSA) is charged with two missions: protecting US signals from being detected and read by others (using encryption as one of many tools), and recording and decoding signals from others (SIGINT). Each is an opposite of the other: one seeks to protect information while the other seeks to unprotect it. Over the years both have become more sophisticated in scope and promise to increase in the future.

13. The Future: A Brave New World.

The security field is rapidly expanding in scope and breadth. As many more devices are being hooked up to the Internet the need for security becomes greater. At the same time, the possible damage caused by attackers is increasing, while the number of people needed to perpetrate it is decreasing. Both aspects of security: offense and defense are continuingly fighting against each other as the world around them becomes more digital and more depended on outcome of their battles than ever before. It is indeed "a brave new world" where millions of people can be left without electricity by a remote hacker from the other side of the world, while a single security professional can sometimes protect entire corporations. Both are made possible by the increased use of intelligent systems and the increased automation of security. As the future comes closer, the stakes will be raises higher and the side with the better technology shall prevail.

A. Appendix A – Bibliography.

- Allen, Julia H., *"The CERT® Guide to System and Network Practices"*, Boston, MA, USA: Addison-Wesley (2001)
- Denning, Dorothy E., *"Information Warfare and Security"*, Reading, MA, USA: Addison-Wesley (1999)
- Erbschloe, Michael, *"Information Warfare: How to Survive Cyber Attacks"*, Berkley, CA, USA: McGraw-Hill (2001)
- InterNet, The
- Lee, Wenke; Me, Ludovic and Wespi, Andreas (Editors), *"Lecture Notes in Computer Science #2212, Recent Advances in Intrusion Detection"*, New York, NY, USA: Springer-Verlag (2001)
- Turban, Efraim and Aronson, Jay E., *"Decision Support Systems and Intelligent Systems"*, Upper Sadle River, NJ, USA: Prentice-Hall (2001)