Global Information Assurance Certification Paper

A STUDY ON: BREAKING IN TO A TOP LEVEL CLEARANCE SECURITY INSTALLATION AND OBTAINING SENSITIVE DATA – APPLICATION OF MILITARY STRATEGY

SANS GIAC **GSEC Practical (v.1.4b)**

ANDREW WAN - 26/06/04

This white paper focuses on a step-by step guide on how to obtain hypothetically highly sensitive classified information from a top-level clearance security installation. It focuses primarily on the physical component whilst covering other aspects in general on IT security. This is followed by a summary with some possible suggestions to prevent such a scenario from happening. Where possible incorporation of the thoughts, learning's found from the speakers, authors and documentation of the SANs training has been used.

The white paper is broken in to five sections:

1) **Basic Theory guide:** outlines the general principles. Applying and translating 24 Chinese military strategies to IT Security has been added to look at IT security from a different approach.
2) **Practical guide:** covers a successful hypothetical operation.
3) **Summation guide:** closing statements and review of the practical with guide to possible suggestions to prevent such a case from happening in the future. It is not intended to cover further military strategy and briefly covers surveillance, biometrics, physical security and methods for taking information out of an installation.
4) **Appendix A:** Research survey.
5) **References**

NOTE: This Step by Step guide is a **hypothetical guide only used for the purposes of this assignment**.

Any comments and detailed information on **how to complete of covering your tracks and a successful closing** are probably beyond the scope of this assignment.

THEORY

PROLOGUE

I have created this work based on information I have collected from work, personal experiences or various sources, documentation, conversations in the past. Thus I am not able to document the correct source or the sources for some of the ideas presented. To give credit where credit is due, and I am sure a lot of these ideas are not new and have been cycled for many years in various forms and used in a wide array of applications. Therefore, I would appreciate if you could send an email to myself and I will endeavour to have these updated in the reference section so that others will know the original source and have an up to date base to research further on.

Comment [AW1]:

BASIC DEFINITIONS TO UNDERSTAND FIRST

Top-Secret clearance – There are many definitions for this, depending on individual policies. For this assignment it refers to a high level security facility that requires advanced biometrics to enter.
Installation – In this case this refers to a physical building, or group of buildings belonging to an entity whether this is an individual, corporation or group of corporations.
Attacker – Refers to the individual, or group whether professional, amateur, agencies etc conducting the attack on a target
Company/Companies – Refers to Corporation, agency, departments etc. to keep integrity of information without over revealing exact source.
Target/Defender – Refers to the individual, or group whether professional, agencies etc on the receiving end of the Attacker

MOTIVES TO HACK IN THIS SPACE

Motives are an important determinant as to why an individual or group of individuals would want to compromise a top-secret clearance security installation. Rather than trying to work out any psychological and intransient reasons for an individual to engage in this activity, it would be more productive to outline the groups people may tend to fall in.

Comment [AW2]: delete

Outlined below are many of the major motives for an attacker to breach the target's defences.

Some of these motives are summarised by:

Personal gain / Financial root cause

"Why do people rob banks?" – "That's where the money is". This is probably the most significant reason to take in to account before looking at other causes. In a lot of cases personal gain in terms of financial benefits is a big

consideration for professionals in this field. This highlights the dangers of other root causes, which may hire this particular group of people.

Financial gain is significant factor basing this on receiving a large of money versus the amount of effort required to pull off such an act.

In a lot of cases there may be no reason for these individuals to destroy information unless there is a need to cover up their true intentions, rather they would use this to their advantage, or manipulate / change it to their favour (examples: banking, taxation, identification fraud)

There are a number of highly trained, well-funded groups of individuals who commit IT based crime in order to profit. An example of this is extortion attempts aimed at large companies and enterprise companies. This trend has been in existence historically due to human nature, and something that will continue to grow in the near future.

The national program manager for the FBI's Awareness of National Security Issues & Response (ANSIR) unit has stated, “Certain business information is more valuable than heroin,"

The United States Congress passed the Economic Espionage Act of 1996 (EEA). This act imposes prison terms up to 15 years and fines up to $10 million for stealing trade secrets. This shows the seriousness of Economic Espionage.

The National Counterintelligence Executive (NCIX) reported that for 2001, the combined costs of foreign and domestic economic espionage, including the theft of intellectual property, are as high as $300 million per year and rising.[1]

Political / Ethical / Religious root cause

The principal reason is to cause harm (based on one’s agenda), or make a stand or viewpoint in society (by nefarious means). This could range widely from people wanting to use IT either directly or indirectly to harm others such as interruption to electricity facilities, stealing harmful weapons, to corporate web site or government web site defacement.

Examples:

“Multiple US Military web sites defaced”.
http://www.hackerscenter.com/ARCHIVE/view.asp?id=7&section=incidents
(12/03/2004, 03/01/2004)

Archive of defaced web sites, political, ethical, religious - including some large security vendors: www.zone-h.com

[1] Luong, Minh. “Corporate Espionage: A Real Threat”. Optimize Magazine.
http://www.optimizemag.com/article/showArticle.jhtml?articleId=17700988 (14 October 2003)

Analysis of Defacement statistics of top five defacers of Indian based websites.

Defacer	Number of defacements	Percentage
AIC	160	22.28
GForce Pakistan	116	16.16
Silver Lords	101	14.07
WFD	53	7.38
TheBuGz	12	1.67

[2]

Intellectual root causes – the need to show intellectual prowess

There are few people who fall in to the category of this field. Although many professionals would like to think they do.

There is a vast amount of dedicated information regarding motives for example:

Hare D, Robert. Without Conscience: The Disturbing World of the Psychopaths Among Us The Guilford Press, January 8, 1999

Collins, John. "Hacker Motivation – Reason for Hacking". 2004. AKA MARKETING.COM. http://www.akamarketing.com/hacker-motivation.html

Sollfrank, Cornelia. "Women Hackers - a report from the mission to locate subversive women on the net". Next Cyber feminist International 1999 http://www.obn.org/hackers/text1.htm

[2] Srijith, K. N. "Analysis of Defacement of Indian Web Sites" http://www.firstmonday.dk/issues/issue7_12/srijith/ (29 November 2002)

BASIC STEPS

GETTING IN

This is easier said than done. There are two focuses on this area: Physical access / Remote access. This paper focuses on physical access related also to IT security systems. There is other numerous papers that focus on Remote access.

"Once you have physical access to a machine – Game over" – Eric Cole, SANs Sydney, 2004.

APPLYING ANCIENT CHINESE MILITARY STRATEGIES IN TO IT SECURITY TO ASSIST

24 Strategies were used to take a different look at IT Security, breaking in to a company and stealing information. These are based on applying famous strategies from various famous Chinese Military generals such as Li Shi Min Cao Cao and Zhuge Liang. The Military strategies have been recorded in history in various historical books. The most famous of these including Sun Tzu, The Art of War and Romance of the three kingdoms.

Selected Strategies have been used for the theory component. Majority have been derived from:

Wang, Xuan Ming. Translated by Hoon, Yeo Ai. 100 Strategies of war: Brilliant strategies in action — Asiapacbooks. (December 1993)

The numerous strategies used in Wang Xuan Ming's book have come from records of numerous battles culled from 21 historical books from the Spring and Autumn Period to the Five Dynasties, spanning more than 1,600 years of history.

Strategy 1 - Know thy enemy long before a battle

Research is one of the most important aspects of any successful operation. It can take anywhere from 10 minutes to many prolonged years variable on how well the individuals are prepared and their motives, as well as their targets. 50 years may not be a long time.

How to research will vary for each operation and is briefly covered in this paper. There are numerous dedicated papers existing on this topic.

Good research is the difference between success and failure.

Strategy 2 - Identify the battlefield target(s)

In many cases you will not be able to choose your targets, rather within the target you are given, you will need to conduct research to identify target opportunities that are weak or can be compromised.

Strategy 3 – Spoiling the Enemy's processes and plans

This means knowledge of the their security policies, plans, evacuation policies etc. Once you know the Enemy's plan, careful study of their plans and policies could expose vulnerabilities.

An simplified example of this: Knowing the day the Target plans to launch a new biometric security system could mean that very day they could be left exposed during the transition period.

Strategy 4 – Using local guides, espionage, and understanding the battleground carefully

It's important to understand the local terrain. In a lot of cases the attack can be expedited through consulting of local people familiar with the terrain and systems. In present days this still holds, however, this could mean using a local system to find out more about other systems (example: remote attack) – or in the sense of a physical attack – finding out about other physical installations from one installation. This is important in order to gather information about the defence's activities, strengths, capabilities and weaknesses. This can be done using an insider or intelligence agent.

For example, once you now know that the target plans to use a new biometric security system via the knowledge of an insider, it means there is the possibility of being able to use espionage when the company installs their biometric systems. This is relevant in today's modern environment of delivering IT systems where several companies rather than one have been contracted out to in place components of security systems has it's own weaknesses. It means an attack could potentially bid to become the installer of the biometric system.

In military strategies if you attack hastily, one will generally only see defeat.

Strategy 5 – Using Reconnaissance

It's important to stay up to date with the target. Timely information and data gathered on the target will greatly aid in any preparations for attack and possible fallback scenarios.

It's important to increase the reconnaissance activities and understand the movements of the enemy.

On the defence side: If there has been a significant increase of reconnaissance activities based on intelligence then it may be a good time to go to a higher alert level.

- Who works there? What do they do?
- What do they use?
- What tools or weapons are needed to infiltrate?
- How many people need to be involved? Example: Military personnel slowly took over civilian company in a period of 6 months through normal hiring process.
- Where? Location

Strategy 6 – Seize the Opportunity to attack and attacking the right targets with a quickly launched attack

If there is a situation that rises to make the enemy ineffective it should be taken. Launch an attack at the right time. Considering a lot of companies are unprepared or even know if they are prepared may mean a quick attack is possible.

An example for the modern day is Blitzkrieg used by Adolf Hitler. The element of surprise with brute force concentrated in one area means that you penetrate in one clearly defined spot where the targets resources are to overcome their defences. By attacking one weak spot, before they have time to regroup you can take over the country. One key requirement in using this technique is that your resources need to outnumber their resources. Hitler believed that the Soviet Union would not be able to sustain a barrage from his troops because they were weak.

"We only have to kick in the front door and the whole rotten edifice will come tumbling down" - Adolf Hitler

An example of this is in IT Security is launching a concentrated Distributed Denial of Services attack rather than on several individuals. In IT sometimes, the infrastructure deliver such as the ISP may also be hit at the same time.

Strategy 7 - Building up One's Forces for Battle, Training of Soldiers and using Elite Troops as the Vanguard

Training of soldiers for battle is essential. Untrained troops will generally mean trouble. You also need the right numbers, dependant on the scenario.

In the industry today, finding an Elite or 3l33t3 hacker is something a lot harder than most people presume from watching movies. Arguably the ones who are Elite are never known and do not want to be known, even in Elite communities based on IT experience of 15+ years, there are possibly few people who fit in to this category dated before the Internet and even before BBS'. There are also famous people in this industry from research areas however, by nature historically have been focusing on developing these technologies in a rapid manner to have them working, leaving possible security vulnerabilities open, and working then on newer technologies or functions. It would be hard to find all rounders that can cover the wide arrange of security areas, and people who were able to soak up the knowledge from

the beginning or start. On the other hand from 15+ years ago, there are groups that would like to be known, and still are there, some of these people have moved on to work at fairly well known companies to day, others still dabble on the "black hat" area. Also, there are numerous groups who may fit in to this category of newly acquired knowledge thanks to the Internet era. Arguably there is not even a need for this group to understand historical architecture, platforms, systems, programming or software. There is also no need to understand military strategy. Some techniques and tools are fairly automated

Using an Elite Troop would have the advantage of versatility. "Being able to look like a bumbling fool" – to avoid attention, as well as being able to "deliver the pizza"

Strategy 8 – Deployment of Soldiers and the artillery

"A wise person must know how best to use his tools. Make use of one's equipment wisely and one will be able to defeat the enemy despite having fewer weapons" This means after understanding the defence being able to correctly use the right type of tools, deploy and utilise them is a skill in itself, even if you have all the tools you need to have a plan on how to use them.

Even a CIP (Change Implementation Plan) – contains a detailed document of what tools will be used in a change as well as how they will be used and when.

You don't use a 56K connection to directly launch a flood attack on a large ISP. Likewise you do not need to use explosives to break down to front door, when you can "shadow" someone in.

Strategy 9 - Forming Alliance with Neighbouring States

This means, that groups can work towards a target. For example: One party may only be interested in logistical information, another group may be interested in stealing technology and one group may be only interested in destruction.

The benefits here, is that you have more resources. Each group will get what they want, and final group also benefits the earlier parties in the fact that the evidence has now gone.

From the defence perspective, it means you may want to link yourself with similar groups in the industry, perhaps via a forum to stay ahead of the attackers and learn from each other as well as share experiences. In the case of Denial of Service extortions, companies in the gaming industry have been regularly talking to each doing just that

Strategy 10 – Fighting from Afar

Many other papers discuss this in terms of a general IT security remote attack.

Strategy 11 – Fighting during the day and fighting during the night

During the day, there are more people at work, it is harder to perceive the number of attackers or be drawn out. This means that the target's ability to judge the situation could be affected.

There is the disadvantage of being clearly singled out at night if spotted. The general rule used in war is to make use of drums and fire during a night battle. Here it could mean setting up a diversion.

Strategy 12 – Fighting in the different locations and taking up advantageous locations

Depending on the target, sometimes they may choose to take the proactive approach and attack you first or send out an early party. This is sometimes a good opportunity to find out more about the attacker and gather information. Also at the same time they are distracted with their current proactive attack. Sometimes advantageous locations are better than good timing. Even if you know the target's weakness if you are not in an advantageous location you are still only 50% there. You have to plan for what you want to attack first down to the detailed level based on reason. To a micro management level – this means in a physical attack, securing the key locations – this could be the comms room, which could then give you access to the MDF and so on. At a system level this means you could be gaining access to one system to gain access to other systems.

Zago-Swart, Adrienne. "how two computers were used to gain access to government computers" Advanced Incident Handling and Hacker Exploits SANs Practical Assignment. http://www.sans.org/rr/papers/index.php?id=825 (November 5, 2001)

Strategy 13 – Being on the offensive

Sometimes you don't want to show all your cards. However, you would like to see a real life demonstration of what the target has on hand. This is important to see how they respond to attacks and if they always respond in the same manner.

From an IT remote attack perspective – this could mean only taking down certain infrastructure. From this vantage the attacker is able to view how long it takes for the target to acquire a solution followed by a fix or repair. During this time, other attacks could take place.

From a defence perspective, if you can stop attackers gaining valuable resources from an attack then by all means do so proactively. Sometimes an upgrade via a technology refresh in network infrastructure may also help.

Strategy 14 - Should you be on the defensive or be the first to attack?

If that attacker knows they cannot win the battle from the current time, then it is important for them to adapt a defensive strategy. Saying this, in history a lot of battles have been won by being the first to attack. In the case of IT security, although the focus of this paper is for a highly secure infrastructure. In some cases, the target may not know they are highly secure, or with a company, may not even be ready. This is a good time to attack.

Strategy 15 – Biding for Time in Battle

Sometimes the target may be alert and ready, so it may not be the right time to attack. However, it may mean that you need to wait for a vulnerability to appear such as a change in leadership or in staff. In the IT security world – anyone worth his or her grain of salt is sometimes quickly seconded by another company and may be difficult to acquire. The higher learning's of this, is that if you are able to forecast natural disaster from the elements, earthquakes, typhoons and other natural phenomena's it has advantages

Strategy 16 – Staying on Guard

This goes both ways from the attacker and defender. Even more intense preparations need to be made. One of the bad things about this is that it normally leads to an arms race, where companies and arms dealers are the winners, which depends if the attacker is one of them.

Staying on Guard should be covered for each individual scenario in the planning if possible. It is important to understand the implications for actions taken both from the attacker's perspective as well as others. It's also important to step away and evaluate the larger picture. In a lot of cases, for the individual the worse case scenario is torture, personal injury, not succeeding, death. This means you need to stay on guard as an attacker, likewise as a defender knowing that there is a possibility of the unknown attacker.

Strategy 17 – Withdrawing when Outnumbered

Sometimes there is not point in attacking and a retreat is in order when outnumbered.

Example: Recent case of attacks causing international cooperation between several countries and law enforcement agencies to track down attackers that were primarily located in one particular country in Eastern Europe.

Strategy 18 – Fighting a Bamboozled Target

When the enemy forces are in a state of confusion, take the opportunity to attack them.

This highlights the dangers of recent events in the world where there were clashes (even physical) between different agencies such as police, federal police, fire service, ambulance services and intelligence as outlined in the September 2001 Commission review. A further attack would have caused even more damage, as the group was bamboozled.

Strategy 19 – Avoiding a Battle

Sometimes they come under attack, though cleverly, applying strategy of fighting for a strategic location, there may be no need for your attacks, to accidentally target any of these companies for the attackers greater purposes.

In the case of worms and viruses, it means Virus companies will be slightly behind in the race to catch up to the latest worm which they can not see, but their customers are experiencing. Once a general virus code has been received, it's a fairly easy process to create a clean. The basic process of this has not changed from its early foundations.

From the defence point of view, there is little you can do other than take prevention steps.

Strategy 20 – Using small gains to entice the Enemy

For enemies that are not adept in using strategies, entice them with small gains. The enemy sometimes believes they are making great progress but forget about the impending dangers. Laying ambushes can then defeat them.

This is something that some companies are now using with Honeypots / Honeynets etc. Honeypots are discussed in depth in other papers. When using a honey pot it is important to understand the all the advantages and disadvantages of their use.

For example:
Spitzner, Lance. "Definitions and Value of Honeypots".
http://www.governmentsecurity.org/articles/HoneypotsDefinitionsandValueofHoneypots.php

Some dangers include not setting up the Honeypot correctly, which can lead to vulnerabilities or a back door to your network (depending on the implementation and how you view the data). There are designs to circumvent this. Making it too obvious that it is a Honeypot is also an issue. The danger of Honeypots is that a lot of people only intend on using these as resources to then launch an attack on the real target.

Strategy 21 – Setting up Barriers along Strategic Locations

In the IT sense, the easiest example of this is the firewall. In the physical sense, examples of this are from SANS: Castle moats, walls, doors etc. The trend is for most companies to extend their DMZ. In the cases of small companies – you may be limited to the extent of what a typical service

provider may be able to help with as well as financial constraints. In the case of a large company, you probably can have some influence over a commitment over what your service provider will do to extend your DMZ deeper than a typical smaller company because of the business you bring them. Some service providers are large enough to cater for both groups.

This is where you ask specifically what the service providers companies have to offer and what security practises they have in place, and also with their partners. Do they have international security accreditation standards in place, redundant architecture set up for you? Even the knowledge of how the current Internet service you receive comprised down to the router level. For some of the larger companies, the service provider may provide dedicated resources for these purposes specific to each company.

Sometimes although the world is littered in the commercial sense, it makes sense for you to form allegiances with strategic partners, delivery companies and even help and support them. After all, it would be difficult to do business without them.

Strategy 22 – Ensuring Sufficient Food Supply

An army with no adequate food supplies will eventually be destroyed. This means, that the financial backing needs to be strong as well as the resources and infrastructure.

On the counter side for defence, this means stopping the root source of the funding. It may mean international cooperation. Ceasing financial institutions from issuing / transferring / doing business with the attackers (if they are known). Therefore limiting their supply of money to purchase supplies needed. In the age of I.T the cost of these tools are fairly cheap. However more sophisticated tools come at the cost of money. Examples of these tools are generally restricted to few. After this, going to the suppliers directly or companies that do business with the attackers to impose sanctions.

Strategy 23 – Using illusion and disguises

This covers the area of getting in using disguises, fake id and background. There are many resources on the Internet that cover this area in depth.

Strategy 24 – Pillaging the Enemy's Food Supply

Both Defence and attack

An example of this in the IT sense with the DDOS attacks, where numerous systems from private home users are used in a distributed denial of service. Having a large supply of "zombie" computers determines the capability for an attack. Already there are examples of companies stepping up to solve this issue, free fixes, worms to combat other worms and patch up systems, free antivirus, free personal firewalls etc. In regards to viruses / worm / antispam etc, companies are using this medium or using these private home resources

as their supply. This in itself is a very lucrative battlefield, for using these resources to calculate the stars, to assisting with spamming or DOS attacks. Some IT Security companies and courageous individuals even see themselves as do-gooders in this field rather than companies out there to make a quick buck.

PRACTICAL

HYPOTHETICAL SCENARIO

Background:

Contact has been made to discreetly investigate the vulnerabilities of information leaking from a top-secret clearance security installation and complete a formal report with findings. The installation is not aware of authorisation has been given for the investigation. This is a secret and they are not to be informed if possible. The installation is known as the Chillips Aero Space Laboratory, which is involved in a fictitious Air Wars Laser program. The task is scope the installation and infiltrate and gain access as a third party, and mock steal sensitive information and distribute it to a third party.

Maximum time for task:

1 year or less

Budget:

1 Million dollars

Initial Personnel:

1 person - Agent Alpha

Additional Notes:

- To gain this information, physical access to the network will be required.
- If personnel are met whilst on the mission, appropriate force or interrogation methods have been authorised.
- Damage to the information and systems should not take place unless needed or after the information is re-secured.

PRELIMINARY START

Agent Alpha has been able to contact an Insider Personnel named Agent Cosgrieve. This was done by finding out the employees who already worked there. Then short-listing potential candidates who may help due to financial situation, politics, trust, personal values, mistreatment from current employer or country or other levers. The Insider Personnel was a willing participant although they also do not know that you have prior authorisation. The Insider Personnel has been able to provide Agent Alpha with intelligence. However the knowledge of their assistance cannot be known. Therefore Agent Cosgrieve will not be able to give you an easy pass in to the installation, or his

or her own biometric information. The Insider Personnel has been able to give the following information:

- What security systems are in use within the installation.
- What the security plan is.
- What the evacuation plan is.
- What kind of systems will be there and what to look for with a detailed map.
- Information that this is a high security installation and therefore has minimal staff and relies heavily on technology for protection.

Agent Alpha has put together Recon team 1. Recon team 1 has only been given selected information and is unaware of the Insider or any other Recognisance teams. They have now done a brief scope and physical surveillance of the compound on top of this. Additionally satellite surveillance and imagery has provided a deeper insight to the installation and confirmation of the information from the Insider Personnel.

Surveillance:

- The installation uses a civilian 24-hour physical security patrol - 2 security guards - 2 shift changes per day.
- Civilian security company is called "Grubb" to protect it's identity.
- The Recon team 1 has found that the installation uses a Protective Security Alert System. The rating system was upgraded from the WeatherSock Alert System implemented in the 1980s
- Note: the name of the alert system has also been changed to protect the good work from this system which needed to be updated to reflect international standards
- In summary of this system the codes used are Safe Base - Anteater, Beaver, Cockatoo, Dingo and Emu
- Anteater being the lowest rating whilst Emu representing the highest security measure.
- Currently Beaver is being used.

Based on the information above, there is no need to place an insider in “Grubb” as the timing of their shift work has been able to be decoded.

Time taken so far: 3-4 weeks
Cost so far: $270,000

Software and other necessary tools have been now collected for the job. Agent Alpha now has formed a task team to infiltrate and steal the information known as Team Delta. Team Delta has only been fed selected information that is needed for their task and has been deliberately made unaware of any other groups that have assisted so far.

DDAY:

Team Delta consisting now of 2 physical staff are ready. They have approached the installation and passed physical perimeter security.

Encounter with Security Guards:

Tactic employed: Although uniforms, and ID have been acquired and duplicated. Team Delta was able to avoid the physical confrontation of the security guards altogether with assistance and planning. There was no need for force to be displayed. Other additional back up preparation was ready.

Swipe Card system encountered:

A swipe card system is present on the perimeter door. They are unable to proceed further.
To enter the complex a swipe card was used which was stolen. Team Delta was aware of other measures to bypass Swipe Card systems if needed.

Team Delta is now in the foyer of the complex. In the foyer and throughout the installation there are biometric face recognition cameras installed. These are able to pan the room without the aid of a human with artificial intelligence.

Biometrics encountered – No.1: Biometric Face recognition cameras.

Team Delta has fooled this technology with cheap digital photos attached to their faces of legitimate and authorised users. The 2-Dimensional cameras were useless in this scenario. Plastic and cosmetic surgery would have been taken as a precaution for a more advanced recognition camera or to bypass a mix of physical guards and Biometric Face recognition cameras.

Team Delta has now entered a further secure area of the installation and now requires additional biometrics. They are unable to proceed pass this physical barrier.

Biometrics encountered – No.2: Finger print scanner.

Team Delta has opted in rather than chopping someone's finger off to enter. They have opted for a Jelly device with basic thermal warming to fool the system. As a back up, a legitimate copy of the fingerprint was taken and added on top of their own fingerprints to stimulate basic warmth and heartbeat.

Note: There are some more advanced biometric systems than this available in the marketplace. This is taking the basic example of a biometric system implemented poorly.

Biometrics encountered – No.3: Iris scanning.

An Iris scanner has been recently set up just before meeting an additional physical barrier for a further secure area of the facility.

Team Delta has chosen not to take a physical eye in this case to bypass the system. The copy to an advanced fake eye has taken place. This is more advanced than basic fake eye or contact lenses or image printing - testing from one-company shows they can detect this - other tests show that this depends on dye and also quality of the fake eyes or contact lens. However, the issue is that you need to hold the subject to take gather accurate information to duplicate their eye.

Physical security barrier encountered – Pin code for the door / optional keys / individual servers.

A strong and thick vault like metal door was encountered that was linked to a manual pin code that was needed to open the door. In some cases, depending on the manufacturer and design a master code will exist used by security professionals. Similarly to master keys. There are many documents which cover this component in depth ranging from the basics of probability – from brute force physically and by trial and error – knowing which keys have been used the most (which is a fairly easy tell tale sign by observing the pin pad in some cases). Some have optional keys depending again on the manufacturer. There are many documents again to cover this area. Some of the fastest methods for key locks include professional hydraulic guns for doors to using chemicals/compounds.

Generally for a secure Data Centre, there is also glass, as well as emergency procedures.

With many Data Centres, is there will be clear view glass. This may provide an alternative means of access if required.

To complement the SANs training course, there are a range of new chemicals used to reduce fire other than water, or Halon mixed with sensitive smoke detection systems such as VESDA (Very Early Smoke Detection Apparatus). Examples include: Various Gas-flooding fire suppression systems – e.g. FM200, FM 2000, NASF3 dry gas fire, etc. Pre-action sprinkler system. There are also systems, which only lower the oxygen level to still allow most humans to live, although most could be knocked out either from the force or oxygen levels which mean physically the life support systems only remain active.

Emergency exit plan / physical harm or torture / removal of hardware

The Delta team could possibly take advantage of this if there was a party inside as they have reached the source destination for the information and are no longer concerned as much with triggering alarms as once final access is granted, removal of the hardware could take place.

In some Data Centres – the safety precaution for Halon, or other dangerous gases would trigger emergency doors opening. This is not the case in all situations.

In some highly secure environments, some personnel may be required by law to sustain inflicted harm.

What to do with physical access to the systems, hardware and infrastructure?

There are numerous methods covered in other papers to retrieve the data. For the Delta team, this included IT security software methods and tools. Alternatives would be to physically remove the hardware for forensic analysis to take place. Counter intelligence tools to be installed.

Also note: SANS assignment: “How an Exploit in the Computer System of a Small Company Was Used to gain Access to Two Major Government” - Adrienne Zago-Swart.

Methods for taking information out of the company

To then test the internal systems. Team delta then sent “mock” information using SMS, telephone, modem transmission, fax, mobile phone, email, and FTP. Security and counter-surveillance tools were also discreetly installed in to the systems.

PRELIMINARY FINISH:

4 weeks in total delivery
Under budget

SUMMATION GUIDE

The practical highlighted a remote possibility of a secure installation being "hacked in to" in approximately 1 year.

If applied on a normal commercial company - the actual resources and costs could be significantly less.

Informers / Having company information/plans leaked:

In some organisations there are staff that release sensitive information either knowingly or unknowingly.

Possible suggestions:

- Updating Security policy
- Training and understanding of the sensitive nature of the information
- Appropriate reward for staff
- Instilling loyalty in staff
- A possible solution to protecting critical plans is to align company plans with the CIA (Confidentiality, Integrity, Assurance) principles when possible and ensure that top-level confidential information stays private and confidential.

Surveillance:

Aerial surveillance: – typically spy planes or equivalents that are able to monitor various signals and are equipped to gather near real time intelligence.
Aerial photography: – known as Ortho-photography. Aerial photography is a component of Aerial surveillance. Pictures are taken via aircraft, air balloons etc.

Possible defence suggestions:

Restrict aircraft or flying objects. In some countries there are areas covered by law which have restricted flying zones.

Photoreconnaissance satellites:

Possible defence methods: Outside the scope of this paper. Either political, physical, or technical. During conflicts, ISPs from certain countries are banned from purchasing live pictures of certain areas. American based commercial satellites are restricted in the quality and detail that can be provided to civilians.

What can you legally image if you are in the United States?

The only off-limits spot on the planet isn't even inside the United States. In 1997, Congress blocked U.S. companies from photographing Israel at a resolution higher than 2 meters.
Space Imaging will sell pictures of Central Intelligence Agency headquarters or even the secret military installation in Nevada known as Area 51.

Examples of providers of images from satellites:

www.digitalglobe.com – located in Colorado, USA
There are certain free pictures available as well pictures you are able to purchase. Prices range from US$100 for their services, up to thousands and hundred's of thousands of dollars. Digital Globe's top resolution is .6 meter.

www.spaceimaging.com – located in Colorado, USA
There are free satellite images up to a 16-meter resolution. Other images need to be purchased. The satellite circles approximately 423 miles from the Earth.

Indian, Russian, Israeli, French and Indian and companies also sell satellite imagery to civilians. Branches within government agencies sometimes may share or own their own satellite.

Quality of the satellite images:

Legally images up to 50cm resolution are possible. Images of someone's iris for biometrics from my research is not possible. Military satellites can see objects around 20 inches or smaller, but the precise resolution is classified. Space Imaging's top resolution is .82 meter. However, dust, water vapour and clouds may shroud the visibility of the target.

An example given by Mark Brender from Space Imaging is between Israel's Dimona nuclear reactor with North Korea's Yongbyon reactor. The .82-metre pictures of Yongbyon nuclear reactor are much clearer than the allowed 2-meter picture Dimona nuclear reactor.

There are also companies that provide near real-time monitoring information from their satellites even dedicated staff.

The pictures generally can come in different formats. There is physical media such as magnetic tapes, hardcopy and softcopy such as JPEG.

Benefits of using JPG

- JPG format is fairly useful as it can be stored and read on a wide range of devices and different platforms and operating systems example: your mobile phone, some MP3 players, Apple OS, Solaris, Linux, Windows.
- JPG is also fairly easy to manipulate in terms of adding authentication, steganography etc.

- Another benefit of purchasing in JPG is that files are easily edited using any basic photo editing software program on majority of platforms, OS' and devices.
- The size of the files can range from several 1-3MBs (low quality) to much larger sizes. The benefit of this, is that using a wide range of popular software tools, they are easy to zoom in and out to obtain detail as required.
- These can also be dispersed providing appropriate licensing is purchased and can be reduced in size, or specified segments of information can be delivered to various teams.

D-DAY

After preparation this is the day the starting of the attack will occur. This could take place from anywhere from 30 days to years. If an attack or infiltration is done over a prolonged time successfully, it makes it easier for the attacker to bring in extra staff and steal valuable information. An example in Australia is highlighted with a defence exercise, in which a factory was slowly "over taken" be defence personnel through normal means of human resources.

Encounter with Security Guards:

This is becoming a more difficult situation, as the level of technology and resources required to reproducing uniforms, and ID, plastic surgery etc. have become less expensive and easier to source in a lot of cases.

With this, there is a lot of work which can be done to enhance the physical Security Guard capability including linking this with surveillance systems that trigger a forced response from the Security Guard.

In high-level security installations, where there is little staff. A prior booking needs to be made in advance for any personnel visiting the premises. In this manner, taking in to account the minimal number staff, it's important for

Swipe Card system encountered:

Stealing a Swipe Card means you can generally use it until the company is alerted. Labeling of what the Swipe Card is used for or the areas it can open should be avoided.

It may be possible for a fake Swipe card that acts as an alert sensor when used. This way, if it is swiped an alarm will be set off. Of course, this may also mean a significant increase in false alarms for the company. However, the chances of the attacker entering first time may have been reduced.

Biometrics – "something that is you"

Although some people think this is a pain in their life having to use something from their body which is unique to them, in certain cases there is a false sense of security due to the vulnerabilities of biometrics which can work in the

Attacker's favour. Although this may mean an implied disadvantage to the Target. Having more security is sometimes better than having none, some high quality biometric technology is very good indeed depending on implementation and technology which is recommended. Ideally you want to have more of "Good Security" and less of "False Security".

Biometrics coupled with physical humans is important. To compare Intrusion Detection Systems which are not manned 24x7x365 is similar to the situation of installing physical surveillance cameras without anyone monitoring them. The same can apply to good Biometric systems implementation to stop abuse.

Biometrics encountered – No.1: Biometric Face recognition cameras.

High quality Face recognition cameras are available which can circumvent the cheap method of fooling these systems with a 2D picture. Obviously a good approach is to ensure there are physical security guards present. Full facial masks, or plastic surgery is a slightly harder task, however is a good test for this type of system.

Biometrics encountered – No.2: Finger print scanner.

There are some more advanced biometric systems than the example used in the practical that are available in the marketplace that won't be fooled by cheap tricks. The example taken in the practical outlined a poorly implemented biometric system. Ideally you would want to integrate several forms checks together. Similar to a two-phase authentication for example: Password and Biometrics combination.

Those wishing to beat finger printing going to the extent of an example seen in the Philippines of cutting someone's ligaments off even with anti-technology of heat etc. This can generally be beaten with counter technology from the attacker.

Biometrics encountered – No.3: Iris scanning.

The example for iris scanning used in the practical was cheap and not current. Vendors report that advanced scanners are reported to be fool proof against forgeries. I have not been able to verify or confirmed this. Theoretically the advanced scanners check for appropriate pupil contraction, which reduces the risks of an attacker wanting to remove the eyes from the target's personnel.

Physical security barrier encountered – Pin code for the door / optional keys / individual servers.

This is a large area of physical security which is better covered in conventional security manuals. The advancement in this area, has lead to patented technologies in locks and even the materials used to make doors and locks which may be useful. The technology has also extended to individual servers and devices. Example: Server with built in keyboard which

will only open with a key. Similar to a self enclosed rack/cabinet with a lock in a Data Centre.

Emergency exit plan / physical harm or torture / removal of hardware

Emergency exit plan

Emergency exit plans is something that clearly has to be marked for safety reasons. Thus this knowledge is something that can be known about in "public space". A lot can not be done in this space, except for careful planning when designing the exit plan. In a Data Centre it may be dangerous if a personnel is required to "sign out" using biometrics for example when there is a fire if the system is no longer functional. Another example in a Data Centre, is for a physical switch where you have to break glass located on the outside. This then releases chemical poisons to smother the fire. However, if it was used by an attacker on the outside, it may kill the people on the inside, to avoid a confrontation if the personnel inside were carrying weapons. An alarm would be sent, however, and alarm being registered does not always mean you can catch the attacker. Emergency exits opening may even speed their progress to safety.

Physical harm or torture

Concerning physical harm or torture, taking an example from the United States Military Code of Conduct. In Article IV and Article V. The conduct states that you will give no information or take part in any action which might be harmful to my comrades. It also mentions if interrogated, that I am required to give name, rank, service number and date of birth. It also instructs the personnel to evade answering any further questions to the best of their ability.

There is nothing that can be done in this area, other than relying on other aspects in Security practices. Eventually most personnel will give information. Capturing personnel does not need to happen within the confines of the installation.

Removal of hardware

Some easy examples of stealing physical hardware include: Laptops, PDAs, Computers and Servers all which may contain sensitive data. By taking the hardware physically, it may allow you to analyse the data more carefully and have a more complete forensic analysis of the systems.

Laptops – Fast and easy targets. Light and designed in nature to be portable.

How to Protect against this vulnerability:

Can be locked down with rudimentary locks (similar to bicycles). Various quality and methods exist. Some use patented technology.

Recent Real life confidential example:
A floor where senior management of a large multinational company were working had their laptops stolen. The information could have been used to see current bids, the companies' strategy, policy, etc. This information could have been used in a company take over or via rival companies. Not only was critical business information stored on these laptops, personal information was stored too, which could hypothetically be used in some form of blackmail in the future. Also, the company's policies, as well as information containing knowledge of "secret" hot sites for the company was now vulnerable.

The floor was meant to be secure, and had biometric access, swipe cards, security guards to inspect physical employee IDs, and had cameras deployed on every entry and exit.

Due to the nature of the attack, the attack itself could not be published in the newspapers, however knowledge of this passed from senior management to the public.

The entire floor was reportedly cleared in broad day light within 30 minutes. It is assumed the attackers knew ahead exactly what they were looking for.

Servers / Mainframes / Computer Systems

More complicated targets than laptops due to their size. However the size of servers has gradually been decreasing. Information on servers can include vital information such as databases, bank records, new schematics, live processing information etc.

The difference between laptops and servers, is that some servers by nature are able to hold tremendous amounts of information or are powerful computers, once compromised provide a launch platform.

Recent Real life published example:

"Inquiry reopens over airport security blunder", Sydney Morning Herald. September 5, 2003

Rossi , Sandra. "Customs airport security review could tighten EDS outsourcing". Computerworld 24/09/2003 12:34:32
http://www.computerworld.com.au/index.php/id;1567200777;relcomp;1

It was reported in the newspapers that high level security clearance servers had been compromised and were taken from customs / defence.

It is argued that these servers contained the knowledge of who they were searching for, what methods they used to detect these people, as well as access to a database of information regarding details of people. The systems attacked are known to contain information on "bad guys" such as organised crime, terrorists etc that the "good guys" hold and share. The method and way to communication between all the different parties was known. It is rumoured

that these servers were linking several further secure government agencies – customs/defence/intelligence agencies…

How was the theft accomplished?

Very little information was officially released. Based on the news, the attackers knew about how the systems were connected, they were also aware of what information they were looking for. Also were prepared to cover their tracks with a successful closing. They also conducted research on the various vulnerabilities and weakness of all targets to be able to a simultaneous attack. It was found that a third party contract was in charge of the maintenance contract for these systems. This information was gathered via the third party contract directly (via foreign powers) or this third party had been infiltrated, either by one of the target agencies itself, or "bad guys". For the purposes of this assignment, the name of the company has been changed to FDS. FDS has several main offices around the country. Uniformed people wearing FDS uniforms knew of the protocols and procedures beforehand to get in. They were also very professional in leaving and causing disruption and mistrust between the target agencies. Later on, it was revealed from FDS that one of the employees had been employed with FDS during December 2001 to January 2003.

What to do with physical access to the systems, hardware and infrastructure?

This means you will rely on the implementation of IT Security on each system, hardware and infrastructure once physical access has taken place by the attacker. In summary this may include things such as encryption, the standards used, and the methods stored on each system. It may also include things such as flash memory protection as well as the rest of the aspects of protecting IT security systems.

Methods for taking information out of the company

To then test the internal systems. Team delta then sent "mock" information using SMS, telephone, modem transmission, fax, mobile phone, email, and FTP.

How to stop information getting out once attackers are inside:

OVERVIEW ONLY

PABX – as this technology is old, some of the popular used vulnerabilities are well known and can be stopped. There are certain vulnerabilities that cannot be stopped easily depending on the implementation or standard of PABX.

FTP – A major issue, since a basic client/server can be less than 20K (historically such files were fairly large and could easily be noticed by administrators. Likewise historically 20K or less would have brought attention to administrators too, dependant on their familiarity with each system. There

are now numerous systems. Firewalls / IDS / IPS can help – in a lot of companies an FTP server or client is generally not needed in business, therefore firewalls are useful to segment the logical network and for legitimate use the added layer of secure authentication may help.

SMS/pagers/Mobile Digital phone/Analogue mobile phone - fairly easy to detect, although they can be altered to avoid some detection systems. There are methods available to jam signals and transmission

Satellite phone – fairly easy to detect, although they can be altered to avoid some detection systems. There are methods available to jam signals and transmission. Certain alterations may have ill health effects.

Local phone system – These should be known and mapped, and can be monitored. Some installations will ensure that all traffic passes certain gateways. There are extensive manuals which cover this beyond the scope of this assignment. Phreaking and counter phreaking.

Modems / Fax machines – Other than the obvious physical security checks and protection, pins (for fax machines)

Photocopying machine – pin number, some machines can be bypassed either physically or through the pin Example: guessing, root pins for example. How to by pass these devices are covered in other manuals. In nature it is similar to bypassing a basic security system. The modern day espionage kit will include a portable scanner / camera to by pass the need for a photocopying machine.

Portable scanner / Floppy disks media – In some secure meeting rooms all these devices must be removed and scanner before entry. Like wise in some corporations where information "such as software or code" – has required staff to go through scanning equipment to check for disks. At the time they were mainly looking for 5 and ¼ disks or 3 ½ floppy disks restricted to 1.44 MB. Note this is a rumour only for many years: that some devices contained large magnets that were used to possibly affect the memory of these devices "swipe clean".

Portable Storage Devices/Flash memory/USB/CDs/Hard drives/Camera/PDA (expansion from above) – With all the choices now available the market place has certainly changed. For an attacker it's now a case of deciding what exactly they prefer to use, which can be troublesome in itself. There is an assortment of tools ranging from the cheap to the expensive price range.

In general terms a device with high capability and storage, integrating a few forms such as camera etc. With an easily accessibly way to erase data permanently if needed (which can not be reconstructed) even using current means. Similar to the flash technology used in the older spy planes.

Hard drives are also fairly compact now, in the consumer market of today you can find portable storage devices that can cater for 200GB and fit in to a pocket.

Disadvantage of most hard disks – Data again can be easily recomposed if formatted. An example: http://www.killdisk.com/ is a software which claims to safely format the hard disk to ensure the data is erased to meet the CIA principles.

Disadvantage of CD-ROMs – they can be hidden with other CDs, however are bulky and the information cannot be easily deleted if needed. Even if broken the CD can be recomposed.

IP Phone – Similar to Local phone system. Slightly easier to monitor and apply content filtering.

Email/Web surfing/Web sites – This deserves a special section.

There are many solutions that will use one or more of this technology. The major difference in purchasing a ready made solution to think of is: Support from the manufacturer, or even better for IT managers and outsourced solution - Third party support, monitoring and reporting ideally by a large local company which has adequate resources to do this 24x7x365 and has staff which are aware of legal requirements and have appropriate training and security clearance which you can trust. This may reduce set up and operating costs, certain legal risks, legal training and other specialised training needed to get the functionality that you want from such a system.

Although many of the solutions promise to all do the same. There is a big difference in the quality of R&D and resources that are supporting these technologies. Some features based on information released on from Internet Security Systems on their content security application include:

Black and White lists – To restrict or automatically allow communication to other users.
Text Classification – In ISS's technology - Text is categorized using Bayes' statistic methodology and vector machine algorithms.
Object Recognition - This module searches for logos, symbols and other graphical elements in photos. Variations in size, colour and rotation are taken into consideration. This could be used differently for outgoing mail where companies require all email to have appropriate logo attached. To ensure emails are for business use and not personal use. Likewise it can be used for incoming mail from the companies that users are authorised to work with.
Optical Character Recognition (OCR) - OCR recognizes text in graphics and images, and can even analyse coloured type or transparent text on any background. This module supports a wide range of type fonts, colours, sizes and rotations. This stops basic attempts to hide data openly in picture format to stop older technology that was only able to work with standard text.
Pornography and Recognition of Nudity - This module identifies nudity by analysing the qualities of human skin and individual skin tones. This could be

potentially useful for combating information being released most likely using pornography with basic steganography that security professionals may not be able to look at manually due to the law and code of conduct.

Example of software, vendors or technology that may help:

Content filtering: Etrust, Brightmail, ISS (which acquired technology when they acquired Cobian) Google, Search engine companies, Research companies. Some companies will use authentication methods for email including digital signatures linked to biometrics.

Proventia content filtering technology uses fully automated Web crawlers to gather and analyse new data on a continuous basis. Currently their database is larger than Google. The technology is able to add more than 120 million Web pages per month to the Filter Database. Likewise this type of technology may be useful to employ on your own external as well as internal web pages.

Video streaming / Television and radio broadcasting – Example: Content Filtering services. There is software / hardware which allows virtually live capturing and content filtering of both Video Streaming, IP streaming, Television and radio broadcasting. These services have been available to consumer market as well. Example: When there is a live sporting event - marketing companies, third parties may get paid every time a sponsor's logo is shown. No matter where (billboards, signs, official merchandise, on people/spectators clothing or apparel etc)

This is fairly impressive technology, and can be applied as part of the process of securing valuable infrastructure or installations.

Managed Communications Service A sophisticated managed communications service system – would be able to audit communication, as well as prevent unauthorised communication as needed.

For the fixed telephone component only: Some large telecommunications companies offer a basic managed service, which include a dedicated personnel for voice conferencing which means they are able to verify each caller in to a conference as well as disconnect a particular caller if wished as well as other tools – such as fixing line noise. This can be incorporated in to a larger solution to force all calls to go through this customised managed service who is the only person able to connect to external calls. For a lot of these systems, there is an account number and pin. There is also a human factor for added safety rather than an automated machine. Some calls need to be pre-booked to be activated, and all incoming calls can be audited to determine their source. This would also hamper modem use on a fixed line.

Additionally at the actual telephones located in the installation, passwords/pins or locks can be added. Although these can be possibly bypassed or broken including some biometric implementations.

Scanning staff for material:

For staff entering a building the basic walk-through similar to airports is sufficient. Similarly used in some financial institutions as well. However, for top level security clearance areas another layer is added, which does not hinder the every day business of a company. The cost of course is however the physical aspect of three extra staff needed to cover the 24x7 role.

For the paranoid companies: The typical scanner can be upgraded to new x-ray devices. With adequate training (which is sometimes not taken as seriously as it should) – this can enhance physical security. Such things as containers with shielding devices such as lead etc. can be easily detected, although not full proof. If you go to the extent of purchasing these more expensive devices, then you need to hire professional staffs that are trained with appropriate salaries to reflect their level of expertise.

Implant tools – advantages for attacker: can be done at any time, does not have to be first visit. Gathers information such as "if a personnel has typical surveillance tools and where they are all located, and how they work and how to use them".

APPENDIX A

Survey Questions

Does your company feel it has adequate protection against corporate espionage?

Does your company/organisation/agency have an IT Security plan?

Does your company/organisation/agency have an IT Security plan that is being complied with and is in place?

Does your company/organisation/agency have adequate biometric systems that have been tested and audited to meet compliance issues?

Does your company/organisation/agency meet ISO 7799 standards or equivalent for example AS7799?

Does your organisation have methods/capabilities to prevent unauthorised out bound communication?

Please tick the boxes that apply.

- ❑ Telephone Phone
- ❑ Fax
- ❑ SMS
- ❑ Digital Mobile/Satellite/Analogue/Hand phone
- ❑ Email
- ❑ Web site / Internet
- ❑ FTP
- ❑ Other: Please state:

Research could not be completed due to insufficient amount of data returned.

The methodology was to collect this data and perform statistical analysis to be used to determine the state of readiness against corporate espionage in some Australian corporations and compare this with the company using:

- Biometrics
- Security policy
- Meeting international standards
- Methods for prevention of unauthorised outbound communication

REFERENCE

Tzu, Sun. Translated by Giles, Lionel. “The Art of War” http://classics.mit.edu/Tzu/artwar.html

Wang, Xuan Ming. Translated by Hoon, Yeo Ai. 100 Strategies of war: Brilliant strategies in action —- Asiapacbooks. (December 1993)

Hom, M. E. “The Original "Hidden Dragon"” http://www.jadedragon.com/archives/history/liang1.html http://www.jadedragon.com/archives/history/liang2.html

http://www.online-literature.com/suntzu/

“Multiple US Military web sites defaced” http://www.hackerscenter.com/ARCHIVE/view.asp?id=7&section=incidents (12/03/2004, 03/01/2004)

Archive of defaced web sites, political, ethical, religious - including some large security vendors: www.zone-h.com

Translation of Sun Tzu's The Art of War began. http://www.sonshi.com/learn.html (February 1999)

Data Centres http://www.itnews.org.uk/w_aboutus/w_colophon/p_datacentre.cfm

http://www.teluscentral.com/hosting/internet_data_centre.html

http://www.standingwave.co.uk/eng/infrastructure

Zago-Swart, Adrienne. “how two computers were used to gain access to government computers” Advanced Incident Handling and Hacker Exploits SANs Practical Assignment. http://www.sans.org/rr/papers/index.php?id=825 (November 5, 2001)

Luong, Minh. “Corporate Espionage: A Real Threat”. Optimize Magazine. http://www.optimizemag.com/article/showArticle.jhtml?articleId=17700988 (14 October 2003)

Hare D, Robert. Without Conscience: The Disturbing World of the Psychopaths Among Us The Guilford Press, January 8, 1999

Collins, John. “Hacker Motivation – Reason for Hacking”. 2004. AKA MARKETING.COM. http://www.akamarketing.com/hacker-motivation.html

Sollfrank, Cornelia. “Women Hackers - a report from the mission to locate subversive women on the net”. Next Cyber feminist International 1999 http://www.obn.org/hackers/text1.htm

Srijith, K. N. “Analysis of Defacement of Indian Web Sites“
http://www.firstmonday.dk/issues/issue7_12/srijith/ (29 November 2002)

The United States Military Code of Conduct
http://usmilitary.about.com/

“How a US spy plane works” http://people.howstuffworks.com/spy-plane.htm

Satellite Remote Sensing Services
http://www.rss.dola.wa.gov.au/leeuwin/

French National Space Agency (CNES).
http://www.csir.co.za/plsql/ptl0002/PTL0002_PGE038_ARTICLE?ARTICLE_NO=7049573

Wang, Jian Shuo. “Free picture satellite”
http://home.wangjianshuo.com/archives/20030529_aerial_picture_of_anyplace_in_us.htm (May 29, 2003)

Krane, Jim. “Satellite pictures of Iraq for sale”. Associated Press.
http://www.space.com/businesstechnology/technology/satellite_pictures_030324.html. (24 March 2003)

Komarnitsky, Alek. “Free Satellite Pictures of my Croquet Course”
http://www.komar.org/faq/satellite_photo/croquet.html

Cobion/ISS content filtering
http://zdnet.com.com/2100-1104_2-5140757.html
http://www.iss.net/products_services/mailfilter/

Aggarwal, Balaka Baruah.
http://www.dqindia.com/content/Trends/102101701.asp
(October 17, 2002)

http://www.killdisk.com/

Matsumoto. “Fingerprint identification flaws”. http://cryptome.org/gummy.htm

http://terraserver.homeadvisor.msn.com/famous.aspx

Principe, Loretta. “Security gurus share tips for guarding against foreign corporate espionage”. Network World.
http://www.nwfusion.com/careers/0330man.html (3/30/98)

Akhtyrskaya, Natalya. Computer crime statistics and Legislation. “Cryptographic Protection of Computer Information”. http://www.crime-research.org/ (Jun 26, 2004)

Spitzner, Lance. Roesch, Marty. Dittrich, David. “Definitions and Value of Honeypots”. http://www.spitzner.net (17 May, 2002)

"Interesting thing of the day: - Eye language".
http://itotd.com/index.alt?ArticleID=211 (June 10, 2004)

Iris Scans A new angle on photo identification "Interesting thing of the day: – Iris scans" http://itotd.com/index.alt?ArticleID=212 (June 11, 2004)

Sentinel. Operation Barbarossa
http://www.cs.mtsu.edu/~alex/ww2/barbarossa.htm (15 April 2001).

ANSIR
http://www.fbi.gov/hq/ci/ansir/ansirhome.htm

Blitzkreig tactic
http://eaglehorse.org/3_home_station/history_daley_barracks/kradschutzen_in_eisenstadt.htm