

Ten Threats Your Probably Didn't Make Plans For

Andrew Bycroft, CISSP
January 2006

A Few Threats Can Make All The Difference

As an IT Manager or perhaps a more specialised IT Security Officer, you have your security policy in place, your physical security, network security and application security measures are all installed and functioning. Systems are patched up to date and for that split second it would seem that security is no longer an issue. Unfortunately, a second is probably as good as it gets, as there is bound to be another threat waiting around the corner. In today's fast paced electronic world, whilst it is not possible to maintain a totally secure environment, 98 percent secure is far better than 97 percent secure. Every bit counts, but when it comes to applying security there are many practices that are overlooked simply because we choose to ignore that certain threats exist or worse still, as this is the more likely to be the case, simply don't even realise that some threats exist.

When I speak of security practices I am, of course, referring to tasks that can be carried out to counteract threats. There are many threats that go overlooked and the purpose of this paper is to explore some of these to hopefully make that difference between 97 and 98 percent. Although many of these may not be considered "critical" threats, these often form the initial portions of an attack, carried out in the reconnaissance phase as attackers acquire all of the background information with which to launch an attack. Logically, it makes sense to prevent these threats from surfacing as thwarting these could prevent large-scale attacks from mounting.

What may also come as a surprise is the value of information outside of your organization. A network diagram for example can save an attacker a lot of reconnaissance work; names and contact details of customers could be valuable to competitors, trade secrets may have value to both competitors and extortionists. Protecting this information is key and must begin with policies and frequent audits, but all threats need to be identified and plans formulated for counteracting these threats. Let us now take a look at ten threats to your valuable information that you probably didn't make any plans for.

1. Shoulder Surfing

Have you ever been on a train or in a hospital waiting room reading a newspaper and someone is peering over your shoulder to read the comics whilst you are looking at the weather report? Whilst this is quite rude it is quite harmless compared to someone looking over your shoulder whilst you are reading up on a new product launch to be unveiled next month that will make your company millions of dollars over the proceeding year. That very course of events could change if the shoulder surfer was to gain enough information to either sabotage the product launch or set up a competitive operation. Shoulder surfing typically takes place in public venues and involves an "attacker" watching what you read, type or even what keystrokes you make in order to capture information that could enable the attacker to use that information against you. I use the term attacker here



because this is essentially a type of theft known as information theft. Shoulder surfing is on the increase as remote access increases. Many organizations provide mobile computing platforms such as notebook computers and PDAs in order to allow employees to establish a connection back to the corporate network whilst at a hotel, Internet café or airport lounge. Shoulder surfing can happen anywhere

including observing one's PIN at the ATM.

The best defense against this type of attack is to educate users to look around every so often to ensure that unwanted eyes are not being cast upon their every action.

2. Observation

Observation is similar to shoulder surfing but typically involves making observations from a greater distance and occurs when a physical attack is going to be launched. Knowing exactly where a particular server may be located or piece of media that could have that all-important trade secret on it is key to any attacker who wants to perform a clean break in and theft. Observation also allows patterns to be obtained such as: when security patrols occur, when the last person leaves the office for the day, whether any surveillance equipment exists, whether intrusion alarms are installed and whether there are any weaknesses that could allow easy entry. The key objective though is for an attacker to be able to identify what target he/she requires and what obstacles may be in the way of obtaining that target.

The best defense against attackers making observations is to ensure that anything of value is not visible. Notebook computers should be locked away when not in use, servers should be in a secured computing room, preferably without any windows, pertinent information should not be left on sheets of paper easily accessible on desks, windows and doors should be locked after hours and perhaps the best deterrent is to close curtains and/or blinds and turn off lights. If it can't be seen then it is likely that the attacker will look elsewhere where items of value are clearly visible.



3. Eavesdropping

Eavesdropping is the aural equivalent to observation and shoulder surfing information gathering techniques. I recall the time I heard the IP address of a web server, its operating system type and how to remotely access it, including a valid username and password simply by being on an overcrowded



train and overhearing a conversation between two IT system engineers. Eavesdropping is listening into conversations in the hope of gaining something that may be of value. A lot of information gets exchanged in pubs, cafes, on public transport or even at sports events. Considering we do not know who is listening and the intentions of anyone who is listening, this is a common way of leaking information inadvertently.

The best defense against eavesdropping is to ensure that any topics containing sensitive information be kept discussed at lower volume levels or, safer still, should not be discussed in public places.

4. Dumpster Diving

One person's trash may be another person's treasure. Literally this is what dumpster diving is. An attacker may go rummaging through waste in order to locate anything of value from media to documents. It is astounding what may be found in the waste: network diagrams, asset inventories, company financial information, employee records, employee contact lists, customer contact lists, corporate policies, medical records and confidential intellectual property. Probably the most disturbing is those post it notes that were attached to the monitor with a password written on them may very well still contain valid passwords.

The best defense against dumpster diving is to educate users on the importance of destroying any sensitive documents and/or media properly. Documents should be shredded and media must be erased seven times in order to be destroyed. For organizations with high security requirements, media should be physically destroyed, as erasure is not a guaranteed way of preventing any sort of data recovery.



5. Lost Mobile Devices

With the advent of processors becoming smaller and faster, a cellular telephone now has more power than a room sized computer of thirty years ago. Whilst this is great for making users much more mobile and providing applications on demand such as e-mail and file access, the problem is that small devices tend to be more easily lost or stolen. Cellular telephones, PDAs and even notebook computers may all be storing sensitive information.



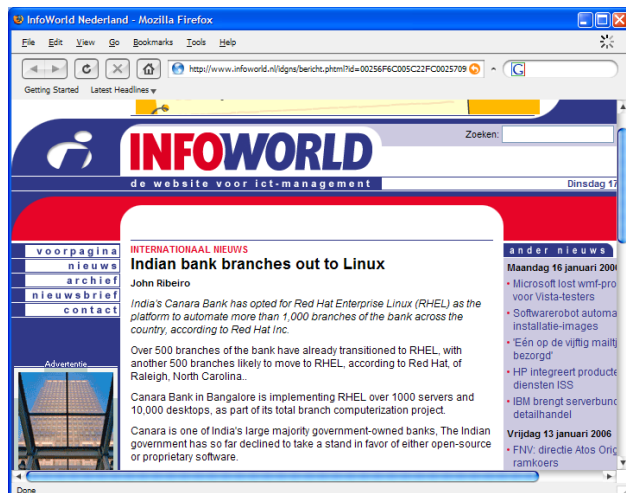
information or even a free pass into the corporate network if remote access software is installed and configured for automated connectivity to the corporate network.

The best defense against mobile device loss/theft is to ensure that the device is not left in a public area or in plain visibility when not in use. Whilst it may not be easy to prevent loss of such

devices, it is advisable to password protect these devices if possible to make the data much more difficult to retrieve. Also consider using disk and file encryption systems so that information is much more difficult to retrieve should all other security measures be broken.

6. News Stories

Many of us would have heard the line “don’t trust everything you hear on the news”. Sometimes, though, the news provides the truth so vividly one can hardly believe one’s eyes. So many times I have read stories that provide detailed information such as “Government has adopted Debian Linux for servers” and “Bank rolls out Cyberguard Firewalls and ISS Proventia IDS solution”. Media coverage like this provides attackers with some useful information on a silver platter. This immediately provides an attacker with information about an organization’s IT systems that would otherwise need to be obtained via probing. Good publicity for the vendors may not necessarily be good publicity for the organizations in this case. News Stories may also provide information about the loss of key staff members or new staff members being recruited. These stories alert attackers to potential times of weakness where staff may be adapting to new management or policy changes and attacks may go unnoticed. Other News Stories may cover other



organization successes or failures, which could also be used as a basis for attack.

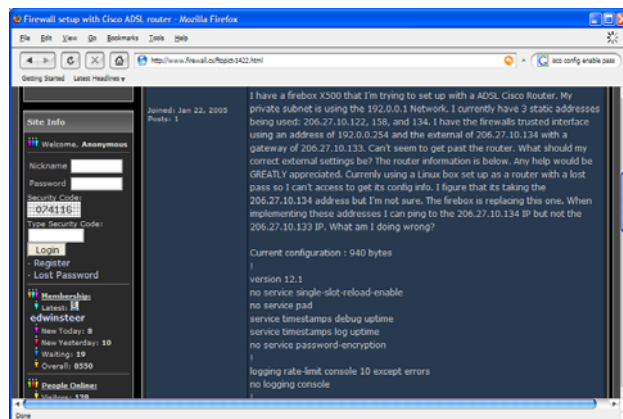
The best defense against information leakage through media is to ensure that media coverage does not contain anything that could be sensitive. Where possible it is best to keep a low profile.

7. Online Forums

Online forums and newsgroups are a great way to communicate with the rest of the world about a common theme. Some forums specialise in providing support for computing resources and also pose a similar threat to any media releases, but probably more so as posts on forums tend to go into a lot more detail. For example I have seen: “Can anyone help me? I just installed Apache 1.39 on my RedHat Linux 7.2 system and I can’t get SSL to work. I created a self signed certificate for www.mysite.com but apache gives an invalid option when I start the apache daemon”. I have seen numerous examples whereby entire Cisco router configurations have been pasted online and the password has been available to crack or sometimes visible in clear text. As can be seen from the above forum posing example we now have a domain name, OS version and Apache version. This alleviates the need for a web-based attacker to have to scan for a target, perform OS fingerprinting and enumerate the application version. This is one of thousands of examples showing information leakage. Many forums provide post with more details than are required to troubleshoot problems and these

details can be dangerous when an attacker gains this information.

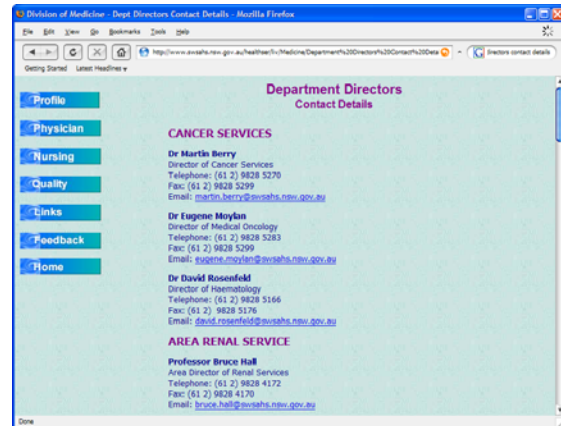
The best defense against information leakage through online forums and/or newsgroups is to ensure that sensitive material is not posted. Where possible it is best to keep a low profile.



8. Web Site

Almost every organization has a web site whether it is a simplistic online brochure or a sophisticated fully interactive home shopping portal. Web sites are convenient and can provide vast amounts of information that may be difficult to otherwise source, but the problem with web sites is not what we know they contain but what we don’t know they contain; simply put - what can be of use to an attacker. Customer information, contact lists, e-mail addresses are all of value to marketing companies for example. In fact, a number of documents that should only be published on intranet sites may accidentally be published to an Internet site. Things like password lists, asset inventories, financial records and a host of other information. There is

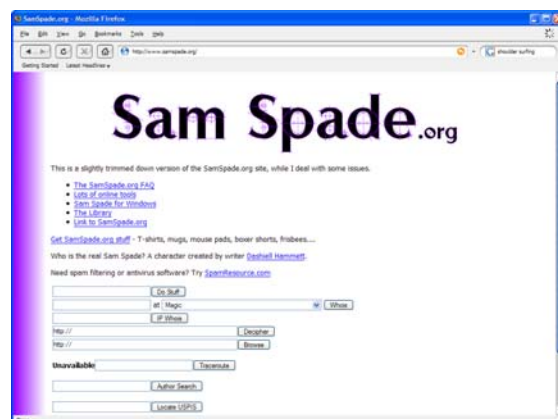
a term used to describe the searching for documents that have been made publicly available by mistake on Internet web sites: Google Hacking. All it takes is a specially crafted search string and countless numbers of results are displayed providing sensitive information about an organization. Be aware that your organization's web site could provide a plethora of information that could make an attacker's life easier.



The best defense against sensitive material being published to the web is to have a review and approval process prior to any publishing. The content needs to be checked for links to any other files that contain sensitive data and should also be scanned to ensure that contact details are not going to be placed online. Although the web site provides a popular means for allowing contact to be made with an organization, consider using a web-based form for collecting information rather than disclosing an e-mail address. This way what happens to the data after entry is not obvious.

9. Online Tools

Besides providing the ability to search forums and corporate web sites for sensitive information, the web also provides a host of online tools, which can be used to obtain IP addressing details, mail server details, DNS information and contact information. Information such as this becomes publicly available when an organization establishes contact with a network registry and requests a block of IP addresses or registers a domain name. A tool known as "whois" allows a search to be carried out on an IP address, IP address range, host name or domain name and find out who the owner is. Often contact details for the owner are provided including an address, e-mail address and telephone number. Network registries include ARIN (North America), RIPE (Europe), LACNIC (South America), APNIC (Asia Pacific) and AFRINIC (Africa). Another automated tool available online for finding out



this sort of information is Sam Spade (www.samspade.org) which allows a number of interesting pieces of information about an IP address or host name to be returned. These tools form an important first step in the reconnaissance phase of a targeted attack and their power should not be underestimated.

The best defense against online tools is to limit the amount of

information provided to network registries. Having “whois” records available publicly is unavoidable but it is possible to have these records created without a whole host of details such as mail address, telephone number and e-mail address.

10. Social Engineering

Social engineers are those who prey on and exploit human weaknesses. Humans are naturally optimistic, helpful, fear getting into trouble and usually sympathetic to someone caught in a crisis, so if a social engineer can demonstrate that he/she is indeed in a crisis and must have a password reset in order to regain access and meet a deadline, chances are that the victim will fall prey and the social engineer’s wishes will be granted. Social engineering requires some background work, however, such as learning who to contact to ask for information and what is the right question to ask in order to get the desired response. This background information comes from several of the previously discussed threats including, but not limited to, observation, eavesdropping and dumpster diving. A social engineer may use face-to-face communications, e-mail, telephone or a number of other communications methods to perform the social engineering attack. A daring social engineer may even do a lot of research on the personal life of a victim to create a pseudo friendship and form a level of trust so as to make obtaining the necessary information easier. It all depends on how much patience and skill is involved in conning the victim in to divulging sensitive information. Depending on how susceptible a victim is to social engineering, a social engineer may go beyond asking for a password to be reset, and may be successful in obtaining an actual password or having a new user account created. Some victims may be as easy to manipulate as puppets.

The best defense against social engineering is user education. Educate users on the type of information that is sensitive to the organization: what can be divulged; what can’t be divulged and the sorts of things that can be asked in order to help determine the identity of a requester before responding to the request. If in doubt ensure that information is only available on a “need to know basis”. Requiring personal information such as date of birth before resetting passwords is a good first step to establishing identity. Obtaining a telephone number with which to call back the requester is also a good means of establishing identity. Most social engineers will not want to leave any paths, which may be traced, back to them.



Conclusion

Many of these threats may occur without any electronic attacking skills and often will have very low visibility, most likely being lost in the daily routines of a working organization. All of these threats are difficult to protect against with technology so it must, therefore, come down to regular policy updates, ongoing policy enforcement and user education to help prevent some of these threats from taking effect. To help create awareness, all users including casual and contract workers should sign off to indicate that the content was understood and reasonable. This should occur should after commencing employment with the organization and once every six to nine months thereafter. It is also highly recommended that an audit from a trusted third party security specialist be carried out on a frequent basis to confirm that the policy is up to date, aligned with organization security practices and effective, An audit is essential to help identify all threats, regardless of magnitude, including those which you, until now, have not been aware of and/or have not made any plans for.