23

# Deception: A Tool and Curse for Security Management

M Warren[1] and W Hutchinson[2]
*[1]Dept of Computing & Mathematics, Deakin University, Geelong, Victoria, Australia 3216.*

*[2]School of Management Information System, Edith Cowan University Churchlands Western Australia, Australia, 6018.*

**Key words:** Deception, Information Security, Security Management.

**Abstract:** With the proliferation of electronic information systems over the last two decades, the integrity of the stored data and its uses have become an essential component of effective organisational functioning. This digitised format, used in input, output, processing, storage, and communication, has given those wishing to deceive new opportunities. This paper examines the nature of deception, and its potential as a new security risk in the information age.

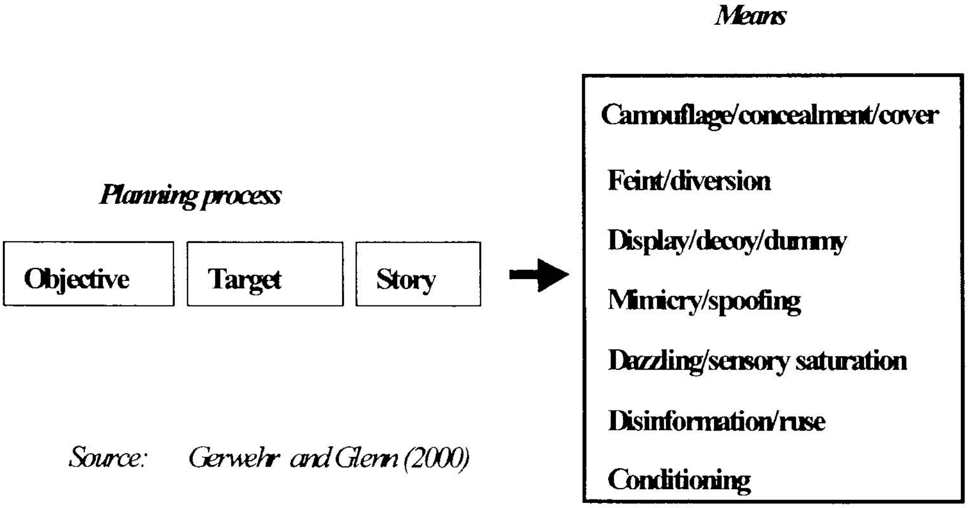
## 1. INTRODUCTION

One major advantage of the digital media is the ability to easily manipulate the bits that constitute its messages. It is also one of its major disadvantages. For instance, Roberts and Webber (1999) trace the history of photographic manipulation and clearly show the ease with which images can be changed to give a totally different perspective. In the digital realm, this is sold as one of the major advantages of computerised imagery. Photographic images, which were always slanted versions of reality, cannot even be taken to be that in today's digitised world. Any component of the image can be changed to reflect whatever is required. Barry (1997) demonstrates the power of visual imagery and how subtle changes can disproportionately change the meaning of an image. Brugioni (1999) illustrates that there is no shortage of government and private organisations as well as individuals only to willing to apply photo-fakery. This is just as appropriate with simpler, conventional text messages. It can be imagined the damage caused to an organisation if a Web based employment advertisement phrase was changed from "Applications from all ethnic groups welcome", to "Applications from all ethnic groups not welcome". This, not so subtle change, could easily cause the organisation involved an enormous amount of embarrassment with its inherent use resources to rectify the situation. Contemporary organisations with their reliance on information technology are vulnerable to deception. Of course, this technology also provides an opportunity. Each person or group can become a deceiver as well as being a victim of deception. Any management regime needs to be fully aware of the potential for deception, and its potential impacts on organisation decision making and operations. Manipulating data to produce desired outcomes has been routinely practiced since the dawn of history. Individuals and organisations choose data which suits the image they want to be portrayed, soldiers camouflage weapons to avoid detection, or disperse false information to conceal intentions. In simple terms, the function of security is both to protect assets and avoid deception from manipulated data.

## 2. PRINCIPLES OF DECEPTION

In this paper, deception is defined as *the deliberate alteration of data or a situation's context to promote a desired outcome.* Therefore, it does not include self-delusion, or a person's natural tendency to use mental model to interpret things in an individual way. The definition places emphasis on a second party being involved, where that person or organisation is consciously trying to create deception.

To understand the fundamental of deception, it is necessary to define data, information, and knowledge. Boisot's (1998) model defines data as the attribute of a 'thing' such as, its colour, shape, or its value. Knowledge is an attribute of an 'agent' (usually this means a human, although it can be argued that intelligent machines can have knowledge). Knowledge is a product of experiences, education, age, gender, culture, and many of the other factors that make up individuals. Thus, humans derive information by using their knowledge to select appropriate data to provide them with information. Hence to deceive, it is necessary to alter data by addition, deletion, or modification and/or alter the context in which the data is interpreted.



*Source:* Gerwehr and Glenn (2000)

*Figure 1.* Types of Deception

Bowyer (1982) classifies deception into two main types that of Level 1: Hiding the real and Level 2: Showing the false. It should be pointed out that 'showing the false' also involves 'hiding the real'. Figure 1 details the types of deception. Whilst this paper is too short to go into each method of creating an illusion by 'feeding' data to an unsuspecting person, the variety of techniques to do can be left to the imagination. Also, there is the potential to manipulate the context by which data is interpreted. Deception is an option for both attacker and defender alike. This paper will consider both but further discussion of Web based deception can be found in Hutchinson and Warren (2000a, 2000b). It can be seen from figure 1 that for effective deception an objective, a target, and a story are required. A method of achieving the objective needs to be decided. As mentioned before, these can be used by the security function or against it.

## 3. USING DECEPTION TO AID THE SECURITY FUNCTION

Many technical deception systems are used by the security function to deceive individuals in order to obtain information about their actions. These on-line tools are used to deceive hackers into thinking they are attacking an actual system, instead all their activities are being recorded. Some commonly used approaches are:

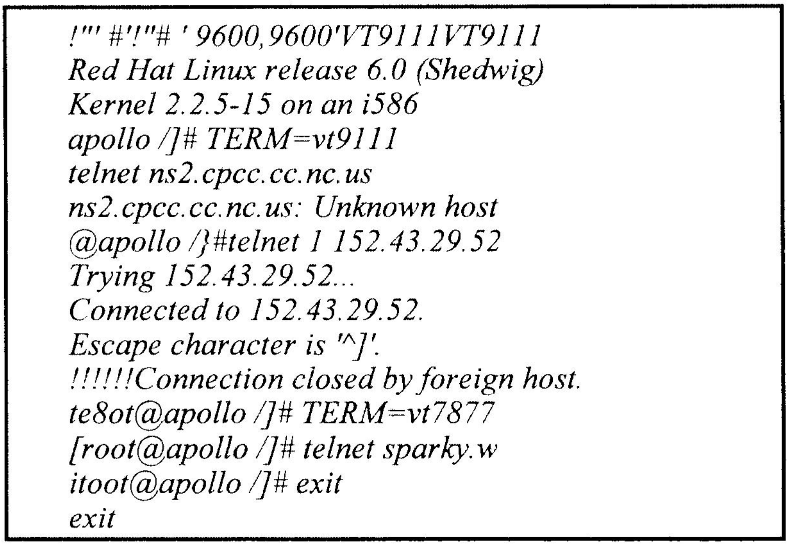
## 3.1 Honeypots

A *honeypot* is a 'pretend' server with the aim of tracking *black-hats* (an unauthorized person trying to get access to a system (Spitzner, 2000a) in the act of probing and compromising a system. The aim is to deceive the black-hat into thinking they are attacking an actual real life server (software examples include systems by Cohen (2000), and Network Associates (2000)). The aim of the honeypot is to monitor the black hats by a number of means (Spitzner, 2000a), they are:

- Tracking the honeypot firewall logs
- Analysis of honeyPot system logs to determine what the kernel and user processes are doing.
- Using a *sniffer* on the firewall that 'sniffs' any traffic going to or from the honeypot. The advantage of a sniffer is that it picks up all keystrokes and screen captures.
- Using a *tripwire* on the honeypot. A tripwire tells the system administrator what binaries have been altered on a compromised system (such as a new account added to: /etc/passwd, or a trojaned binary).

The aim of the honeypot is to attract the black-hats, monitor them, let them gain root access to the system, and then eventually log them off the system, all without any suspicion being aroused. Once black-hats gain root access, they are monitored for several days in order for the system administrator to learn what they were doing. The biggest problem is how to limit the black-hats offensive actions (Spitzner, 2000b).

This is done by using the honeypot firewall, and implementing a rule base schema that allows access from the Internet to a honeypot's firewall, but limits outbound network traffic. It is important that the black-hat is allowed enough outbound traffic so as not to arouse suspicion. The results of these honeypot assessments are made public (http://project.honeynet.org/) so that network administrators can access the information and ensure that they are protected against common hacker attacks and techniques. The following figure illustrates the output recorded by a hacker trying to attack a Honeypot. (*ibid*).



```
!'" #'!"# ' 9600,9600'VT9111VT9111
Red Hat Linux release 6.0 (Shedwig)
Kernel 2.2.5-15 on an i586
apollo /]# TERM=vt9111
telnet ns2.cpcc.cc.nc.us
ns2.cpcc.cc.nc.us: Unknown host
@apollo /}#telnet 1 152.43.29.52
Trying 152.43.29.52...
Connected to 152.43.29.52.
Escape character is '^]'.
!!!!!!Connection closed by foreign host.
te8ot@apollo /]# TERM=vt7877
[root@apollo /]# telnet sparky.w
itoot@apollo /]# exit
exit
```

*Figure 2:* The output from a honeypot of a Hacker's attack

The information obtained from the honeypot audits are forwarded to CERT (http://www.cert.org/) for their assessment and also the system administrators of the systems involved in the attack.

## 3.2 Honeynets

The work by Spiztner developed into expanding the honeypots into *honeynets*. Spitzner (2000c) identified that the honeypots needed to be expanded for the following reasons:

- to be able to determine attacks upon switches, routers and different operating systems of a network
- generate information from several sources (for example, honeypots) in order to provide information in greater detail.
- detect new attack patterns such as vulnerability scanning and how black-hats progress from one system to another.

The result was grouping a number of honeypots together to form a honeynet, so a black-hat would feel that they were gaining access to a much large networked system. When in reality more of their actions and attack strategies will be recorded.

## 4. SPOOFING ATTACKS

Attackers also use deception. For instance, in a web *spoofing attack,* the attacker creates an on-line environment within which a victim will be deceived and disclose information such as passwords. The secret of web-spoofing attacks is to create an environment in which the victim is misled into thinking they are actually at the correct web-site and undertaking actual transactions. To start an attack, the attacker must somehow lure the victim into the attacker's false on-line web site.

There are several ways to do this. An attacker could put a link from a popular web page to a false web page. If the victim is using web-enabled email, the attacker could email the victim a pointer to a false web site, or even the contents of a page in a false web site. Also, the attacker could trick a web search engine into indexing part of a false web site. The key to this attack is for the attacker's Web server to sit between the victim and the rest of the web (Felten et al, 1997).

The attacker's first trick is to rewrite all of the URL (Uniform Resource Locators) on a web page so that they point to the attacker's server rather than to some real server. "Assuming the attacker's server is on the machine www.attacker.org, the attacker rewrites a URL by adding http://www.attacker.org to the front of the URL. For example, http://www.home.netscape.com becomes http://www.attacker.org/http://home.netscape.com." (from Felten et al, 1997, p.3).

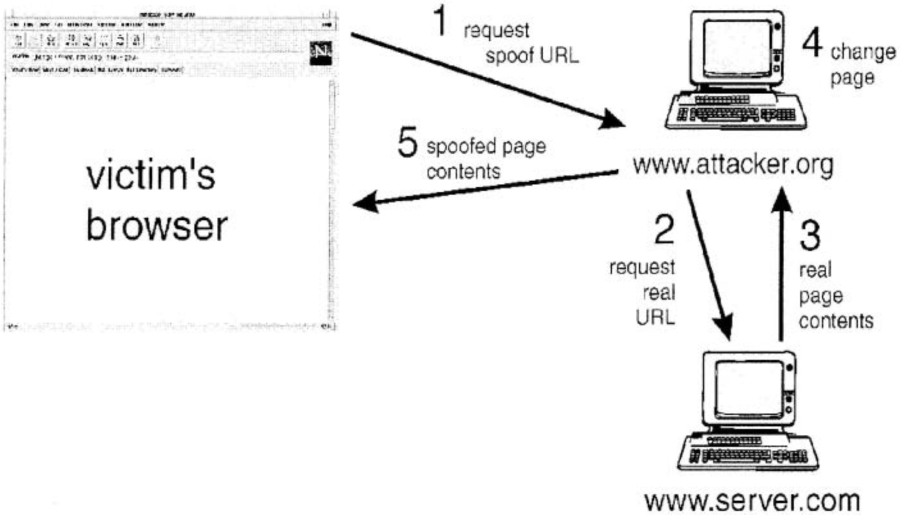
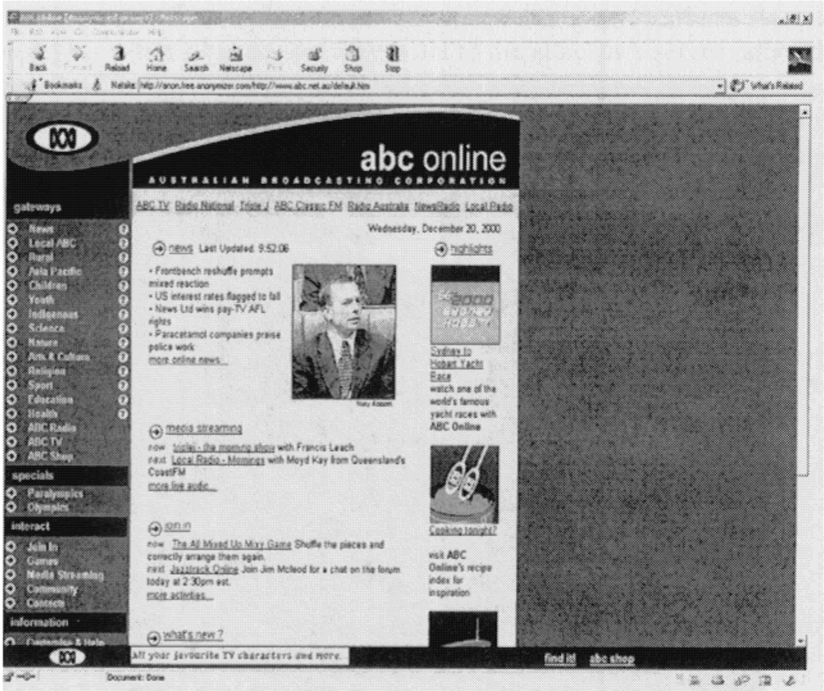


*Figure 3:* Examples of Web Spoofing Attack (from Felten et al, 1997)

Figure 3 shows an example Web transaction during a Web spoofing attack. The victim requests a Web page. The following steps occur: (1) the victim's browser requests the page from the attacker's server; (2) the attacker's server requests the page from the real server; (3) the real server provides the page to the attacker's server; (4) the attacker's server rewrites the page; (5) the attacker's server provides the rewritten version to the victim.

Figure 4 illustrates a real life example of web-spoofing. This service is offered by Anonymizer (http://www.anonymizer.com/) and offers anonymous viewing of web pages by the use of web spoofing, in this example the Web page of the Australian Broadcasting Corporation is viewed by the Anonymizer server, the implication of this is that any IP (Internet Protocol) logging tools would track http://www.anonymizer.com/ but not http://www.abc.net.au which would protect the privacy of a user.



Wednesday, December 20, 2000

news Last Updated: 9:52:06

- Frontbench reshuffle prompts mixed reaction
- US interest rates flagged to fall
- News Ltd wins pay-TV AFL rights
- Paracetamol companies praise police work

more online news...

highlights

Sydney to Hobart Yacht Race watch one of the world's famous yacht races with ABC Online

Cooking tonight? visit ABC Online's recipe index for inspiration

media streaming

now triple j - the morning show with Francis Leach
next Local Radio - Mornings with Moyd Kay from Queensland's CoastFM
more live audio...

join in

now The All Mixed Up Mixy Game Shuffle the pieces and correctly arrange them again.
next Jazztrack Online Join Jim Mcleod for a chat on the forum today at 2:30pm est.
more activities...

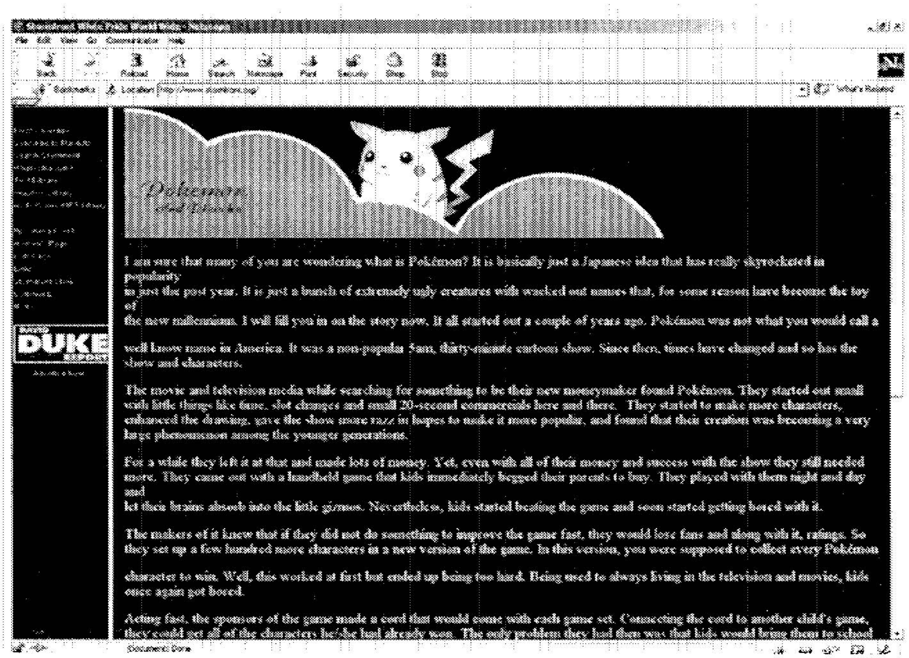
what's new ?

All your favourite TV characters and more.

*Figure 4:* Real Life Example of Web Spoofing

## 5. BASIC DECEPTION

The basic way to mislead is to give false information as if it was true information. With web-pages the most common method is to include META Tags. These are comments lines within web-pages that represent the content of the web pages such as 'Research', 'University A', teaching or they could include META tags such as 'Pokemon', 'Britney Spears', or 'Buffy the Vampire Hunter'. This means that a search engine would wrongly list a web-page as being about a particular subject when in fact it is not. The majority of search engines rank web-sites by sending out a program called a spider, to inspect a particular site. The spider reads the META tags, determines the relevance of the web-pages information and keywords, and then ranks the site according (Deitel et al, 2001). Because of the misuse of META tags there is a growing trend among many search engines to scale down or eliminate indexing META tags (Deitel et al, 2001). Figure 5 gives an example of this where supposed information about 'Pokemon' is found in the children's pages of a white extremists web-site.


File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Location
What's Related
Pokemon
DUKE
Document: Done

I am sure that many of you are wondering what is Pokémon? It is basically just a Japanese idea that has really skyrocketed in popularity
in just the past year. It is just a bunch of extremely ugly creatures with wacked out names that, for some reason have become the toy of
the new millennium. I will fill you in on the story now. It all started out a couple of years ago. Pokémon was not what you would call a
well know name in America. It was a non-popular 5am, thirty-minute cartoon show. Since then, times have changed and so has the show and characters.

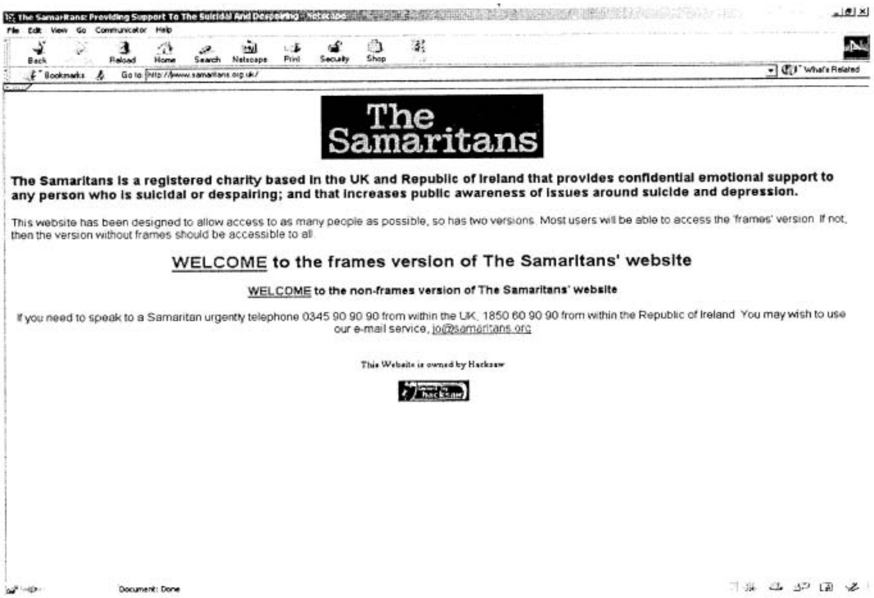
The movie and television media while searching for something to be their new moneymaker found Pokémon. They started out small with little things like time, slot changes and small 20-second commercials here and there. They started to make more characters, enhanced the drawing, gave the show more razz in hopes to make it more popular, and found that their creation was becoming a very large phenomenon among the younger generations.

For a while they left it at that and made lots of money. Yet, even with all of their money and success with the show they still needed more. They came out with a handheld game that kids immediately begged their parents to buy. They played with them night and day and
let their brains absorb into the little games. Nevertheless, kids started beating the game and soon started getting bored with it.

The makers of it knew that if they did not do something to improve the game fast, they would lose fans and along with it, ratings. So they set up a few hundred more characters in a new version of the game. In this version, you were supposed to collect every Pokémon
character to win. Well, this worked at first but ended up being too hard. Being used to always living in the television and movies, kids once again got bored.

Acting fast, the sponsors of the game made a cord that would come with each game set. Connecting the cord to another child's game, they could get all of the characters he/she had already won. The only problem they had then was that kids would bring them to school

*Figure 5:* Pokemon Information found in a White Extremist Web-Site


The Samaritans: Providing Support To The Suicidal And Despairing - Netscape
File Edit View Go Communicator Help
Back
Reload
Home
Search
Netscape
Print
Security
Shop
Bookmarks
Go to: http://www.samaritans.org.uk/
What's Related
Document: Done

The Samaritans

**The Samaritans is a registered charity based in the UK and Republic of Ireland that provides confidential emotional support to any person who is suicidal or despairing; and that increases public awareness of issues around suicide and depression.**

This website has been designed to allow access to as many people as possible, so has two versions. Most users will be able to access the 'frames' version. If not, then the version without frames should be accessible to all.

**WELCOME to the frames version of The Samaritans' website**

**WELCOME to the non-frames version of The Samaritans' website**

If you need to speak to a Samaritan urgently telephone 0345 90 90 90 from within the UK, 1850 60 90 90 from within the Republic of Ireland. You may wish to use our e-mail service, jo@samaritans.org

This Website is owned by Hacksaw

***Figure 6:*** A successful hack of The Samaritans Web-site?

We are now facing a situation that web sites are very vulnerable to attack. Of course to deceive, attacks must not be discovered. For example, the site displayed Figure 6 has not obviously been attacked. The hack can only be identified by the *hack tag* at the bottom of the web-site. In this example the hacker has left the original web-site but only added a calling card. The hacker could easily have changed some of the context of the web-site such as the telephone number displayed or the web site links.

## 6. ETHICAL IMPLICATIONS

The ethical implications of deception are now becoming more important with the growth of the Internet. The advent of the Internet has expanded the amount of data available but has also decreased the reliability of much of it. As Ulfelder (1997, p.75) says: "The are no editors or safeguards to ensure that net information is fair or factual". It is, in fact, a good medium for propaganda because "Nobody is small on the Web" (Rapaport, 1997, p.101) opportunities exist for getting viewpoints across from many. A single person with a grudge against an organisation can weave a damaging image by setting information into a specific context. Of course, organisations can do likewise. Honey pots and honey nets they can be used to capture black hats actions and method and an aid to improving security. On the other hand, the use of web-spoofing, misuse of META tags, and alteration of web-pages could result in a situation that the content of web-pages could not be trusted because there is no assurance that the information is true or false.

## 7. CONCLUSION

It is interesting that in a recent survey of Australian IT managers (Hutchinson and Warren, 1999), 66% did not think there was any threat from competitors attacking their systems in any way. This perception does not bode well for the detection of acts of deception. Data integrity is an extremely important component of information management, but it must not just concentrate on internal processes of access and amendment rights. Strategies to cope with deliberate and organised attacks of a subtle nature need to be developed. Deception is one of these strategies.

## 8. REFERENCES

Barry, A.M.S. (1997). *Visual Intelligence,* State University of New York Press.

Boisot, M.H. (1998) *Knowledge Assets.* Oxford University Press, Oxford.

Bowyer, J.B. (1982). *Cheating,* St.Martin's Press, New York.

Brugioni, D.A. (1999) *Photo Fakery: The History and Techniques of Photographic Deception and Manipulation,* Brasseys Inc., Dulles, Virginia.

Cohen, F (2000). *Deception Tool – kit,* URL: http://all.net/dtk/dtk.html

Deitel H, Deitel P and Nieto T (2001) *e-Business and & e-Commerce: How to Program,* Prentic Hall, New Jersey.

Gerwehr, S.,Glenn, R.S. (2000) *The Art of Darkness: Deception and Urban Operations,* Rand, Santa Monica.

Hutchinson, W.E., Warren, M.J. (2000a) The use of Deception in Systems, *Proceedings of International Conference on Systems Thinking in Management,* eds; G. Altmann, J.Lamp, P.Love, P.Mandal, R. Smith, M.Warren. 8-10 Nov, 2000, Deakin University, Geelong. pp.263-268.

Hutchinson, W and Warren, M.J. (2000b) Deception and the Information Security function, *Proceedings of INC 2000 Second International Network Conference,* 3-6 July 2000, Plymouth, UK. pp.273-280.

Hutchinson, W., Warren, M. (1999). *The attitude and practice of Australian Information Technology managers toward Cyber-Vigilantism,* InfoWarCon99, *Washington, USA, September, 1999.*

Felten, E, Balfanz D, Dean D and Wallach, D (1997). *Web Spoofing: An Internet Con Game, Technical Report 540-97, Princeton University and also presented at* 20th National Information Systems Security Conference, *Baltimore. USA, October, 1999.*

Network Associates (2000) *Cybercop Sting* . URL: http://www.nai.com/asp_set/products/tns/ccsting_intro

Rapaport, R. (I 997). PR finds a new cool tool, *Forbes,* Oct 6, 1997, p. 101-l08.

Roberts, P., Webber, J. (1999). Visual Truth in the Digital Age: Towards a protocol for Image Ethics, *Australian Computer Journal,* **31**:3; 78-82.

Spitzner, L. (2000a) *To Build a Honeypot.* URL: http://project.honeynet.org/papers/honeypot/

Spitzner, L. (2000b). *Know Your Enemy: A Forensic Analysis,* URL: http://www.securityfocus.com/ih/articles/foranalysis.html

Spitzner, L (2000c) To Build a Honeynet, *FIRST (Forum of Incident Response & Security Teams) Conference 2000,* Chicago, USA.