Risk analysis on Internet connection

Marcel E.M. Spruit and Paul H. Samwel

Delft University of Technology, Department of Information Systems, P.O. Box 356, 2600 AJ Delft, The Netherlands, E-mail: spruit@is.twi.tudelft.nl

Rabofacet, ZL-R-142, P.O. Box 17100, 3500 HG Utrecht, The Netherlands, E-mail: P.H.Samwel@rf.rabobank.nl

Key words: Security, Internet, threats, risks, risk analysis, countermeasures, IT audit, EDP audit

Abstract: Many organisations use risk analysis to analyse the vulnerability of their information technology. However, the majority of existing risk analysis methods and tools cannot deal adequately with the variable complex of measures against Internet threats, depending on Internet services rather than installed equipment or information systems. This paper describes a structured approach of a limited risk analysis on an Internet connection, in order to assess the threats which will be encountered if the organisation decides to connect to the Internet, and to determine which measures are necessary to protect against the relevant threats. This is useful in both the design phase for selecting a suitable set of security measures, as well as the testing phase to audit the adequacy of a chosen set of measures.

1. INTRODUCTION

More and more organisations connect their internal infrastructure to the Internet, or they have plans to connect in the short term. Many organisations, especially those which are not connected yet, consider the Internet to be the ideal communication medium which fits every organisation. In practice the Internet is far from ideal and quite a lot of threats are encountered. Many of the relatively large organisations have specific knowledge on how to protect against Internet threats, or they hire this knowledge from specialised companies. Smaller organisations probably would like to perform a risk analysis themselves in order to select the Internet services which are useful and feasible, and the security measures which are required to protect the business processes against Internet threats. For that they need a relatively simple and straightforward risk analysis approach that supports the analysis of Internet threats.

However, the majority of existing risk analysis methods and tools (for example CRAMM [CCTA]) does not support the analysis of Internet threats adequately. Besides, publicly known security baselines [COP95, Fras97, GuBa99] only address security measures against Internet threats by means of general guidelines. This probably is caused by the fact that connecting a local network to the Internet requires a variable complex of measures against Internet threats. The problem is that a large part of the security measures depends on the Internet services that will be used, rather than on the installed equipment or information systems.

This paper describes a structured approach of a limited risk analysis on an Internet connection which can be incorporated into existing risk analysis methods and tools. The approach can on the one hand be used to assess the threats which will be encountered if the organisation decides to connect to the Internet, and on the other hand to determine which measures are necessary to protect against the relevant threats.

2. THREATS

Organisations which connect their local network to the Internet can use Internet services. Before connecting to the Internet one should select the Internet services which are useful to the organisation. Often the following services are used:

- E-mail: The digital equivalent of ordinary mail. This is currently the mostly used Internet service.
- Usenet News (News): The digital equivalent of discussion groups, grouped per topic.
- World Wide Web (WWW): Gathering information using ‘hyperlinks’ between documents which can be distributed over several different computer systems.
- Terminal emulation (Telnet): Making a remote access connection to a specific computer system, while simulating an ordinary terminal.
- File transfer (FTP): Transfer of files from one computer system to another.
- Domain Name System (DNS): The address service of the Internet, which translates Internet names into IP addresses, and vice versa. This service is used in combination with many other services like e-mail, WWW, etcetera.

Many more services are available on the Internet and the number of services is still increasing [IETF99].

To exploit Internet services one has to be connected to the Internet. There are several alternatives. The usual choice is to connect the existing local network to the Internet. If this is the case one can use existing Internet services, but at the same time one is susceptible to Internet threats. Another alternative is to connect only a stand-alone workstation to the Internet. In such a situation the Internet threats focus on the workstation instead of the local network, but Internet services are available on the workstation only. Last but not least one can consider not to connect to the Internet at all. This offers of course the best prevention against Internet threats, but none of the Internet services are available. In practice the latter choice may be less secure than expected due to end users creating their own, unsecure, connection to the Internet.

As shown in Table 1 one can deduce the relevant Internet threats from the information security services, subdivided into information security aspects.

Table 1. Internet threats distinguished by information security services and aspects.

Security service	Security aspect	Generic threat	Internet threat
Confidentiality	Exclusiveness	Disclosure	– Disclosure of confidential data – Sniffing on local network or Internet
		Abuse	– Hacking on local network
Integrity	Correctness, Completeness	Change, Removal, Addition	– Change/delete/add data – Infection by virus/worm/Trojan horse
	Validity	Repudiation	– Repudiate transaction/message
	Authenticity	Forgery	– Forge transaction/message
Availability	Timeliness	Delay	– Long response time
	Continuity	Denial of service	– Internal resources not available – Wrong routing

Implementation of a specific Internet service can introduce some of the threats mentioned in Table 1. For example, the use of e-mail may result in disclosure of confidential data by an employee in an e-mail message. Different services introduce different threats. Table 2 shows the extent to which different threats can be introduced by each service.

Table 2. The extent to which threats can be introduced by Internet services.

Internet threats	E-mail	News	WWW	Telnet	FTP	DNS
Disclosure of confidential data	ooo$^{\#out}$	x	ooo	ooo	ooo	ooo$^{\#in}$
Sniffing on local network or Internet	oo	x	oo	oo	oo	oo
Hacking on local network	ooo$^{\#in}$	x	oo	ooo$^{\#in}$	oo$^{\#in}$	oo$^{\#in}$
Change/delete/add data	x	x	o$^{\#in}$	ooo$^{\#in}$	ooo	x
Infection by virus/worm/Trojan horse	ooo$^{\#in}$	ooo$^{\#out}$	ooo$^{\#out}$	x	ooo	x
Repudiate transaction/message	ooo$^{\#in}$	x	ooo	oo	ooo	x
Forge transaction/message	ooo	x	ooo	oo	ooo	oo
Long response time	x	x	ooo	ooo	ooo	oo
Internal resources not available	oo$^{\#in}$	oo$^{\#out}$	oo	oo$^{\#in}$	oo	o
Wrong routing	x	x	x	x	x	ooo

Note: #in Inbound (external user/initiator) Legend: ooo = likely o = unlikely
#out Outbound (local user/initiator) oo = possible x = not possible

Countermeasures can be taken to protect against relevant threats. Some threats however, in particular 'long response time', cannot be prevented because the origin is somewhere in the Internet networks.

3. COUNTERMEASURES

If the local network is connected to the Internet measures have to be taken to protect against Internet threats (see Table 2). The measures can be divided into generic measures and service specific measures.

3.1 Generic measures

Generic security measures act as a first line protection. They are independent of the Internet services, but usually relate to the type of infrastructure between the internal network and the Internet. Each generic measure protects against one or more Internet threats (see Table 3) [ChBe94, ChZw95, GuBa99, ISO99, PoBa92, Schn96].

Table 3. General security measures.

Threats→ Measures↓	Disclosure of confidential data	Sniffing on local network or Internet	Hacking on local network	Change/delete/add data	Infection by virus/worm/Trojan horse	Repudiate transaction/message	Forge transaction/message	Long response time	Internal resources not available	Wrong routing
Authentication on all computers in local network	o	–	o	o	–	–	–	–	o	–
Strong authentication techniques	o	–	oo	ooo	–	–	–	–	oo	–
Single connection to Internet with ‘packet filtering firewall’	o	–	o	o	–	–	–	–	o	–
Idem, but ‘application/proxy firewall’	o	–	oo	oo	–	–	–	–	oo	–
Idem, but ‘screened subnet firewall’	o	–	ooo	oo	–	–	–	–	ooo	–
Intrusion detection	o	–	o	o	–	–	–	–	o	–
Encryption on transported data	–	ooo	–	o	–	o	ooo	–	–	–
Encryption on stored data	o	–	–	oo	o	–	–	–	–	–
Tunnel techniques in firewall	–	oo	o	o	o	o	oo	–	o	–
Local anti-virus software	–	–	–	–	o	–	–	–	–	–
Central virus check on incoming data	–	–	–	–	ooo	–	–	–	o	–
Educate users of local network	o	–	o	o	o	–	–	–	o	–

Legend: ooo = adequate protection o = some protection x = not applicable
oo = reasonable protection – = no protection

3.2 Service specific measures

Apart from the generic security measures there is a need for additional measures which depend on the services used. For example, the threat ‘disclosure of confidential data’ (see Table 1) is not effectively nullified by the generic measures mentioned in Table 3. If e-mail is used, an additional measure like ‘the use of digital signatures’ may be necessary. Different services require different measures.

Furthermore, there may exist additional threats which are only relevant in the presence of a certain Internet service. For example, the threat ‘employee violates netiquette’ is only relevant while using e-mail. Such threats obviously require additional security measures. These additional measures also depend on the services used.

It is possible to draw up a table with specific security measures for each Internet service. Such a table contains security measures protecting against generic Internet threats as well as additional threats which are relevant for the given service. This is illustrated for the following services: e-mail (Table 4), WWW (Table 5), FTP (Table 6) and DNS (Table 7).

3.2.1 E-mail

E-mail aims at sending and receiving electronic mail messages between the local network and the Internet. The main protocol is SMTP. Other protocols are MIME for attachments, POP for transfer of message between mail server and user, and IMAP for manipulation of messages on mail server [IETF99].

Apart from the generic Internet threats (see Table 4) there are some specific threats:

- Employees violating netiquette, good manners, or business image.
- Receiving unwanted e-mail (flooding, spamming).
- Vulnerability of Sendmail software.

Table 4. Specific e-mail security measures

Specific threats→ Generic threats→ Measures↓	Disclosure of confidential data	Sniffing on local network or Internet	Hacking on local network	Change/delete/add data	Infection by virus/worm/Trojan horse	Repudiate transaction/message	Forge transaction/message	Long response time	Internal resources not available	Wrong routing	Employees violating netiquette, good manners, or business image	Receiving unwanted e-mail (flooding, spamming)	Vulnerability of Sendmail software
Use strongly protected external mail relay host and an internal mail server	–	–	ooo	x	–	–	–	x	oo	x	–	–	ooo
and configure DNS such that all e-mail goes to external server													
and mask internal addresses													
and use protocols with strong authentication instead of POP between internal and external mail server													
and do not allow the use of POP on Internet (e.g. from home)													
and use dial-up server with strong authentication between workplace at home and internal mail server													
and maintain e-mail software regularly													
Encrypt e-mail messages	–	ooo	–	x	–	–	oo	x	–	x	–	–	–
Use digital signature on e-mail messages	o	–	–	x	–	ooo	ooo	x	–	x	o	–	–
Scan attachments on viruses	–	–	–	x	ooo	–	–	x	o	x	–	–	–
Update antivirus software regularly													
Limit entry of sizeable e-mail messages	–	–	–	x	–	–	–	x	o	x	–	o	–
Validate messages via other media	–	–	–	x	–	ooo	ooo	x	–	x	–	–	–
Educate e-mail users	o	o	o	x	o	–	–	x	o	x	oo	o	–
Use mail filter techniques	–	–	–	x	o	–	–	x	o	x	–	oo	–

3.2.2 WWW

World Wide Web aims at gathering information while using ‘hyperlinks’ between documents distributed over several computer systems. The contents of such a document is based on the HyperText Markup Language, HTML, and the location is indicated by a Uniform Resource Locator, URL. The main communication protocols are HTTP and HTTPS (secure HTTP for SSL) [IETF99].

WWW-documents can contain subdocuments written in a dynamic web-language like Java, Javascript, or ActiveX [GrFe97]. Such subdocuments offer comprehensive functionality, but bring along additional risks. This is in particular the case when a compiler or interpreter contains vulnerabilities [DFW96].

Apart from the generic Internet threats (see Table 5) there are some specific threats:

- Vulnerability in browser software.
- Vulnerability in server software.
- Vulnerability of dynamic language compiler/interpreter.
- Excessive private WWW use.
- Employees violating netiquette, good manners, or business image.

Table 5. Specific WWW security measures.

	Generic threats→										Specific threats→				
Measures↓	Disclosure of data	Sniffing local or on Internet	Hacking on local network	Change/delete/add data	Infection by virus/worm/Trojan horse	Repudiate transaction/message	Forge transaction/message	Long response time	Internal resources not available	Wrong routing	Vulnerability in browser software	Vulnerability in server software	Vulnerability of dynamic language compiler/interpreter	Excessive private WWW use	Employees violating netiquette, good manners, or business image
Use dedicated and secure WWW server and disable external uploads to WWW server and restrict internal uploads to WWW server and maintain WWW software regularly	–	–	oo	oo	–	–	–	–	oo	x	–	oo	–	–	–
Disable inbound WWW at firewall	oo	–	ooo	–	–	–	–	–	o	x	–	ooo	–	–	oo
Outsource inbound WWW to ISP	o	–	ooo	–	–	–	–	–	o	x	–	ooo	–	–	oo
Restrict use of CGI	–	–	o	–	–	–	–	–	–	x	–	o	–	–	–
Put public information on read-only device	–	–	oo	oo	–	–	–	–	o	x	–	o	o	–	–
Disable outbound WWW at firewall	o	–	–	–	ooo	–	–	–	–	x	ooo	–	ooo	ooo	o
Use HTTPS (SSL) instead of HTTP	–	ooo	–	–	–	–	ooo	–	–	x	–	–	–	–	–
Validate important information via other media	–	–	–	–	–	ooo	ooo	–	–	x	–	–	–	–	–
Disable cookies	o	–	–	–	–	–	–	–	–	x	–	–	–	–	–
Scan HTML pages on hazardous applets/viruses and update scanning software regularly and restrict automatic startup of applications	–	–	o	oo	ooo	–	–	–	o	x	o	o	o	–	–
Disable dynamic languages, like Java	–	–	o	oo	ooo	–	–	–	o	x	o	o	o	–	–
Restrict dynamic languages, like Java	–	–	o	o	oo	–	–	–	o	x	o	o	o	–	–
Educate WWW users	o	–	o	–	o	–	–	–	o	x	–	–	–	o	oo

3.2.3 FTP

File transfer aims at transfer of files from one computer system to another. The main protocol is FTP [IETF99].

Apart from the generic Internet threats (see Table 6) there are some specific threats:

- Receiving unwanted FTP (flooding).
- Vulnerability of FTP software.

Table 6. Specific FTP security measures.

	Generic threats→										Specific threats→	
Measures↓	Disclosure of confidential data	Sniffing on local network or Internet	Hacking on local network	Change/delete/add data	Infection by virus/worm/Trojan horse	Repudiate transaction/message	Forge transaction/message	Long response time	Internal resources not available	Wrong routing	Receiving unwanted FTP (flooding)	Vulnerability of FTP software
Disable inbound FTP at firewall	oo	–	ooo	oo	o	–	–	–	oo	x	ooo	ooo
Disable outbound FTP at firewall	oo	–	–	oo	o	–	–	–	o	x	–	–
Do not allow inbound FTP to upload	–	–	oo	oo	o	o	–	–	oo	x	oo	o
Do not allow outbound FTP to download	–	–	–	o	o	o	–	–	o	x	–	–
Do not allow anonymous FTP	oo	–	oo	oo	o	o	–	–	o	x	oo	o
Do not allow anonymous FTP to upload	–	–	o	o	o	o	–	–	o	x	oo	o
Encrypt transferred files	–	ooo	–	o	–	–	oo	–	–	x	–	–
Use digital signatures	–	–	–	–	–	ooo	ooo	–	–	x	–	–
Educate FTP users	o	o	o	–	o	–	–	–	o	x	–	–
Scan input files on viruses	–	–	–	–	ooo	–	–	–	o	x	–	–
Update antivirus software regularly												
Maintain FTP software regularly	–	–	o	–	–	–	–	–	o	x	–	oo

3.2.4 DNS

Domain Name System aims at translating Internet names into IP addresses, and vice versa [IETF99].

Apart from the generic Internet threats (see Table 7) there are no additional specific threats.

Table 7. Specific DNS security measures.

Measures↓ \ Generic threats→	Disclosure of confidential data	Sniffing on local network or Internet	Hacking on local network	Change/delete/add data	Infection by virus/worm/Trojan horse	Repudiate transaction/message	Forge transaction/message	Long response time	Internal resources not available	Wrong routing
Use a public external DNS server and a screened internal DNS server	oo	–	oo	x	x	x	o	–	oo	–
and remove internal address information from outgoing messages										
and prevent the use of ‘forwarding’ of external DNS to internal DNS										
and prevent the disclosure of information with respect to the local network										
Check consistency of addresses (by ‘forward and backward’ translation between Internet name and IP address)	–	–	o	x	x	x	oo	–	o	o
Prevent the use of ‘zone transfers’	o	–	o	x	x	x	–	–	–	–

4. DISCUSSION

Complex software generally contains bugs. This is also applicable to software that is necessary to use Internet services. Moreover, this software often is the object of attack by hackers. As a result the hacking community causes a more or less continuous stream of security alerts based on software bugs or organisational errors. The use of software to implement Internet services therefore requires a continuous attention to find potential problems in equipment and organisation. When a problem is found it should be solved as soon as possible. Therefore an adequate incident, configuration and change management is necessary.

Not only deficiencies in equipment can cause problems, but also human errors. Administrators, as well as users can make errors and will make errors. For example, the use of weak passwords is a notorious error, often exploited by hackers. It is important that there is sufficient administrating capacity. Moreover both users and administrators should be sufficiently skilled. Adequate procedures can also help preventing problems.

For the tables given above it is implicitly assumed that the implementation of measures and the maintenance of equipment is adequate, as well as the organisation of users and administrators. If that is not the case the susceptibility for threats and the effectiveness of measures generally becomes worse.

If the approach described in this paper is implemented in a specific tool which supports the risk analysis on Internet connections, it is useful to include the possibility to mark in the tables (e.g., by notes or links) the security measures which have been broken through, for example by hackers, and how such a breach could be solved.

Both audit [MuPa90] and penetration testing [MoSc96] can be used to evaluate whether security measures have been implemented adequately. Auditing generally is more effective to evaluate the completeness of the set of security measures and the correctness of the configuration of relevant components. However, an audit is less useful to evaluate whether the hardware and software components are free of known bugs. A penetration test can fill this gap by running an up to date set of attack techniques against the infrastructure. Because audits and penetration tests require particular skills, it is usually done by experts.

5. CONCLUSION

More and more organisations give in to Internet. However, connecting to the Internet, and using Internet services, induces additional threats. One needs to know which threats are relevant before on can set up security measures. This paper describes an approach which supports the analysis of Internet threats and countermeasures beforehand. The approach is meant to be incorporated into existing risk analysis methods and tools. To completely evaluate the adequacy of security measures with respect to an Internet connection afterwards, one should make use of audits and penetration testing techniques.

6. ACKNOWLEDGMENT

The authors would like to thank Mesut Ates for his valuable inputs to this paper.

7. REFERENCES

[CCTA] CCTA Risk Analysis and Management Methodology (CRAMM), Central Computer and Telecommunications Agency (CCTA), UK

[ChBe94] W.R. Cheswick and S.M. Bellovin (1994), *Firewalls and Internet security*, Addison Wesley

[ChZw95] D.B. Chapman and E.D. Zwicky (1995), *Building Internet Firewalls*, O'Reilly&Associates

[COP95] Code of Practice for Information Security Management, British Standard BS7799, 1995

[DFW96] D. Dean, E.W. Felten and D.S. Wallach (1996), *Java security: from HotJava to Netscape and beyond*, IEEE Symposium on security and privacy

[GrFe97] G. McGraw and E. W. Felten (1997), *Java Security, Hostile Applets, Holes and Antidotes*, Wiley Computer Publishing

[GuBa99] B. Guttman and R. Bagwill (1999), *Internet Security Policy: A Technical Guide*, NIST Special Publication 800-XX Draft

[Fras97] B. Fraser (1997), *Site Security Handbook*, RFC-2196

[IETF99] IETF (1999), *Requests For Comments (RFCs)*, http://www.ietf.org/rfc/

[ISO99] ISO (1999), Standards for Information Security Services, http://www.iso.ch/cate/cat.html

[MuPa90] M.A. Murphy, X.L. Parker (1990), *Handbook of EDP auditing*, Warren, Gorham & Lamont

[MoSc96] P.R. Moyer and E.E. Schultz (1996), *A systematic methodology for firewall penetration testing*, Network Security, March

[PoBa92] W. T. Polk and L. E. Bassham (1992), *Guide to the Selection of Anti-Virus Tools and Techniques*, NIST Special Publication 800-5

[Schn96] B. Schneier (1996), *Applied Cryptography*, John Wiley