

Digital Security White Paper

**Version 10.0
Last Updated: 08-12-2002**

**by
Frederic V. Farcy**

of



Table of contents

| | |
|--|-----------|
| Technology and Security by Frederic V. Farcy..... | 7 |
| Hacker vs. Cracker | 7 |
| <i>From the Hacker Dictionary</i> | <i>7</i> |
| Security Facts about Crackers..... | 8 |
| Enterprise Security by Jupiter Media Metrix | 9 |
| Introduction | 10 |
| What is your “Security Awareness IQ” | 11 |
| <i>SAIQ Questionnaire.....</i> | <i>12</i> |
| <i>SAIQ Questionnaire Answer</i> | <i>16</i> |
| TNTmax Security..... | 17 |
| Definition | 17 |
| Security Environment..... | 18 |
| <i>Individual Security</i> | <i>18</i> |
| <i>Company Security.....</i> | <i>18</i> |
| <i>External Security.....</i> | <i>18</i> |
| Security Layers | 19 |
| <i>Figure 1 - Fundamental Security Components.....</i> | <i>19</i> |
| <i>Figure 2 Example of Security Layers</i> | <i>20</i> |
| Passwords | 20 |
| <i>Password Theoretical Understanding</i> | <i>21</i> |
| <i>Password Structure Rule.....</i> | <i>22</i> |
| <i>TNTmax Password Strength Scale</i> | <i>22</i> |
| <i>Password Crack Understanding</i> | <i>23</i> |
| <i>Changing your Passwords.....</i> | <i>23</i> |
| <i>Password Hints.....</i> | <i>24</i> |
| <i>Password Selecting Hints.....</i> | <i>26</i> |
| <i>Password Safe.....</i> | <i>26</i> |
| E-Mail | 27 |
| <i>Introduction</i> | <i>27</i> |
| <i>What you need to know about E-Mail</i> | <i>27</i> |
| <i>Simple E-Mail Security Rules</i> | <i>28</i> |
| <i>E-Mail Security Tools.....</i> | <i>29</i> |
| TNTmax maxGUARD – Security Solution | 30 |
| VPN – Virtual Private Network..... | 32 |
| <i>VPN Client.....</i> | <i>32</i> |
| <i>VPN Gateway</i> | <i>32</i> |
| <i>VPN Extranet.....</i> | <i>32</i> |
| <i>VPN intranet.....</i> | <i>33</i> |

| | |
|---|-----------|
| <i>VPN Benefits</i> | 33 |
| WIRELESS Network | 34 |
| <i>Brief Introduction to 802.11b</i> | 34 |
| <i>Wireless Security Need to Know</i> | 35 |
| <i>WAR Driving</i> | 35 |
| Security fatcs you should know | 36 |
| Top Hackers/Crackers List | 37 |
| TNTmax Security Resources | 38 |
| Governmental Resources | 38 |
| <i>CIA – The Central Intelligence Agency</i> | 38 |
| <i>FBI – The Federal Bureau of Investigation</i> | 38 |
| <i>NSA – The National Security Agency</i> | 38 |
| <i>CIAC – Computer Incident Advisory Capability</i> | 38 |
| Military Resources | 39 |
| <i>DARPA – Defense Advanced Research Project Agency</i> | 39 |
| <i>DTIC – Defense Technical Information Center</i> | 39 |
| Telecommunication Resources | 40 |
| <i>AT&T</i> | 40 |
| <i>Exodus</i> | 40 |
| <i>Globix</i> http://www.globix.com/services_security_beyond.html | 40 |
| <i>UUNET – MCI WorldCom</i> | 40 |
| <i>Verizon</i> | 40 |
| Organization Resources | 41 |
| <i>CERT – Carnegie Mellon Software Engineering Institute</i> | 41 |
| <i>SANS Institute Online</i> http://www.sans.org/newlook/home.htm | 41 |
| Software Vendors | 42 |
| <i>Microsoft – Microsoft Security Advisor</i> | 42 |
| <i>MyCIO</i> | 42 |
| <i>Network Associates - Mcafee</i> | 42 |
| <i>eEye – Digital Security</i> | 42 |
| <i>Debian</i> | 42 |
| Security Industry | 43 |
| <i>Trusted System Service Inc.</i> | 43 |
| <i>ICSA.net</i> | 43 |
| <i>Security Focus</i> | 43 |
| <i>AntiOnline</i> | 43 |
| <i>AntiCode</i> | 43 |
| <i>HackerWhacker</i> | 43 |
| Cracker/Hackers | 44 |
| <i>2600</i> | 44 |
| <i>Blacklisted411</i> | 44 |
| <i>DEFCON</i> | 44 |

| | |
|--|-----------|
| <i>Hacker News Network</i> | 44 |
| <i>L0pht.com</i> | 44 |
| <i>Rootkit.com</i> | 44 |
| <i>Root Shell</i> | 44 |
| Book and Magazine Resources..... | 45 |
| <i>Computer Security Handbook Third Edition</i> | 45 |
| <i>The Lubrinco Group</i> | 45 |
| <i>Information Security Magazine</i> | 45 |
| <i>Hacking Exposed Book</i> | 45 |
| <i>Linux Firewall Second Edition</i> | 45 |
| <i>Network Intrusion Detection an Analyst's Handbook</i> | 45 |
| Hardware Vendors..... | 46 |
| <i>CISCO</i> | 46 |
| <i>EESCOM - Electronic Engineering Systems, Inc</i> | 46 |
| Reference Resources..... | 47 |
| <i>Acronym Finder</i> | 47 |
| <i>PC Webopaedia</i> | 47 |
| <i>Tech Web TechEncyclopedia</i> | 47 |
| <i>CNET</i> | 47 |
| <i>WHATIS</i> | 47 |
| <i>Internet Traffic Report</i> | 47 |
| TNTmax Security Glossary of Terms | 48 |
| A..... | 48 |
| <i>Argus</i> | 48 |
| B..... | 48 |
| <i>Bomb</i> | 48 |
| <i>BUG</i> | 48 |
| C..... | 48 |
| <i>COPS (Computer Oracle and Password System)</i> | 48 |
| D..... | 49 |
| <i>DDoS or DoS</i> | 49 |
| <i>DES and 3DES</i> | 49 |
| E..... | 49 |
| <i>Encryption</i> | 49 |
| F..... | 50 |
| <i>Firewall</i> | 50 |
| H..... | 50 |
| <i>Hacker</i> | 50 |
| I..... | 50 |
| <i>IDIOT</i> | 50 |

| | |
|---|----|
| <i>IDS (Intrusion Detection System)</i> | 50 |
| <i>ISS (Internet Security Scanner)</i> | 50 |
| J..... | 50 |
| <i>JOHN the RIPPER</i> | 50 |
| K..... | 51 |
| <i>Key</i> | 51 |
| L..... | 51 |
| <i>LeapFrog Attack</i> | 51 |
| M..... | 51 |
| <i>MD5</i> | 51 |
| <i>mail.local</i> | 51 |
| N..... | 51 |
| <i>Nak Attack</i> | 51 |
| <i>National Information Infrastructure (NII)</i> | 51 |
| <i>NetSaint – (new name Nagios)</i> | 52 |
| <i>Ntop</i> | 52 |
| O..... | 52 |
| <i>Open Security</i> | 52 |
| P..... | 52 |
| <i>Phreaking</i> | 52 |
| Q..... | 52 |
| <i>Queso</i> | 52 |
| R..... | 52 |
| <i>Retro-Virus</i> | 52 |
| S..... | 53 |
| <i>SATAN (Security Administrator Tool for Analyzing Networks)</i> | 53 |
| <i>Shadow passwords</i> | 53 |
| <i>Swatch</i> | 53 |
| <i>SSH</i> | 53 |
| <i>SNORT</i> | 53 |
| T..... | 54 |
| <i>TCP/IP wrapper program</i> | 54 |
| <i>Tripwire</i> | 54 |
| U..... | 54 |
| <i>UDP</i> | 54 |
| V..... | 54 |
| <i>Virus</i> | 54 |
| <i>VPN</i> | 54 |
| W..... | 54 |

| | |
|----------------------|----|
| <i>Worm</i> | 54 |
| <i>WiFi</i> | 55 |
| <i>WEP</i> | 55 |
| X..... | 55 |
| <i>X.25</i> | 55 |
| <i>Xenix</i> | 55 |
| Y..... | 55 |
| <i>Y2K</i> | 55 |
| Z..... | 55 |
| <i>Zombies</i> | 55 |

Digital Security by Frederic V. Farcy "ThefRog"

Hacker vs. Cracker

I will start by providing you with the correct definition of the term HACKER.

"Hacker: [originally, someone who makes furniture with an axe] n. 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating hack value. 4. A person who is good at programming quickly. 5. An expert at a particular program, or one who frequently does work using it or on it; as in `a UNIX hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) 6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example. 7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. 8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. See cracker."

From the [Hacker Dictionary](#)

A malicious meddler who tries to discover sensitive information by poking around. Hence `password hacker', `network hacker'. The correct term for this sense is cracker. "As far as my terminology serves, crackers are those who give hackers a bad name (because most people cannot distinguish the two). Somebody who breaks into other's computer systems, or digs into their code (in order to make a copy-protected program run free, or access networks illegally for example) is a cracker. Then, someone who's really good at what he does with computers is called a hacker. A hack, in software circles, is a quickly written short piece of code that makes something work. It may not be beautiful to look at, but it makes things function." Ari Lukumies wrote: Hackers are very smart programmers like Linus Trovalds the father of the Linux operating system who utilize their programming skills for good purposes.

DO NOT CONFUSE a **HACKER** and a **CRACKER**.

The term Hacker can be traced back to MIT where it was born from student jargon in the early 1950s.

"A great operating system hacker that has converted to a cracker forms the most lethal and dangerous combination. These elite crackers that can read assembly language code straight from an hexadecimal tcpdump represent 0.001% of the crackers out there and they keep us awake at night" Frederic V. Farcy

The term "Master Hacker" is given by hacker to another hacker that they consider has superior hacking skills. Example of a Master Hacker is Richard Stallman founder of the Free Software Foundation.

Security Facts about Crackers

Today a great deal of companies and individuals are taking security more seriously and use encrypted e-mail, SSL, VPN, Firewall, IDS and more in order to keep their information private and secure. Crackers always look for the easy target unless they have a mission. Using the right security and constant monitoring give you a better chance to keep your information secure from the outside world.

Note from a Cracker to Another about the status of the increasing use of encryption and security.

```
\=====/  
FADE TO HACK  
/=====\  
by Erik Bloodaxe
```

[Sung to the tune of "Fade to Black" by Metallica]

Accounts just seem to fade away
Losing access every day
Getting lost within some shell
I have lost the will to hack
No more passwords left to crack
There are no more nets for me
I need virtual reality

Nets aren't what they used to be
Someone's always logging me
Access Barred, this can't be real
No more packets left to steal
Now they've installed public key
And they're using Secure ID
Security awareness taking dawn
I was root, but now root's gone

Rerouted my call to save myself, but it's too late
Now I can't think, think why I should even try

Yesterday seems as though it never existed
The SS greet me warm, now I will just say goodbye

Most common security threats a company will face will come from within its own network (Employee and staff). According to Jupiter research, companies need to team up with an outside security partner. TNTmax has introduced maxGUARD combination of hardware, software and human security specialists to answer the security needs of Small to Medium size Enterprise SME worldwide.

Having a security system in place should not give you a false sense of invulnerability. It should provide you with the right tools to monitor, block, and record all traffics in and out of

your network. Expert diligent monitoring can provide you with the ability to anticipate a cracker's next move and stay one step ahead. All companies need to define a security policy as well as an incidence response plan.

Enterprise Security by Jupiter Media Metrix

Enterprise Security
Managing Services for Maximum Coverage
Volume 3 / October 9, 2001
<http://www.jup.com/>

"It is financially and operationally impossible for companies to manage their response to network security breaches in-house. Businesses must outsource at least the execution of incident response to a managed security service provider to assure that adequately trained staff and proper tools are on hand when needed; anything less will leave a company exposed.

What systems and processes does a security policy need to cover? Who should make decisions about policy within the organization? Where does outsourcing make sense? How can businesses manage security internally?

Security Is More Than Just a Firewall. *Firewalls, virtual private networks (VPNs), public key infrastructure (PKI), and other technologies are merely elements of a master plan that must be orchestrated across an entire enterprise to secure its assets. Focusing solely on intrusion detection, authentication, or any other components of a full security solution will ultimately guarantee an insecure system.*

Soft Concerns Will Limit Security Spending. *More than 46 percent of security budgets will shrink or remain the same over the next 18 months, and only 6.4 percent will grow more than 50 percent. While threats will increase, businesses coping with stagnant budgets will be hard-pressed to defend themselves. Unprepared businesses may not be able to secure qualified consultants within budget.*

Manage Corporate Security at the Executive Level. *A security policy must encompass more than the Web or it will ultimately fail. One person at the executive level of the organization must be responsible for all security policy, including client-facing applications, physical security, and human resources and IT processes for managing current and past employees."* Copyright © 1998-2002 Jupiter Media Metrix, Inc./Jupiter MMXI. All rights reserved.

Introduction

This document has been compiled as an ongoing tool to protect our customers and educate our employees on the various electronic threats brought on by the Internet. Several issues are discussed, including security policies, encryption, virus, Trojan horse, worm, zombie's agents, hacking, phreaking, physiological hack, DDoS attack (Distributed Denial of Service), security standards, the NSA, and much more. The goal of this white paper is to educate our company's staff and clients on these threats in order to ensure the highest level of awareness regarding SECURITY.

This paper is not intended for security expert but rather directed to everyone else interested in understanding digital security.

The Internet is the best source of information on this subject. We will point out some important resources available today, organized by categories, to help in your personal research.

"Absolute Security is a never-ending quest, therefore incessant learning, awareness and understanding of its mechanics is your only weapon," says Frederic V. Farcy, CTO of TNTmax.

Security has never been more complex, especially today with Internet telecommunications infrastructures crossing ground, air, ocean, and space. Unlimited new types of crimes are possible. It is important to bear in mind that it is people that commit crimes, not computers or software. The Internet is a playground for CYBER HIJACKERS, CRACKERS, CYBER TERRORIST, ELECTRONIC VANDALES, COMPUTER ESPIONAGE, and PERSONALITY THIEFT.

The Internet is the ultimate network for crime:

- Over 8 million websites
- 1 billions users
- Over 10,000 ISP worldwide (Internet Service Providers)
- No global regulation.
- No "finger prints" or traceable unique digital IDs that are always ON and non removable on computers today.
- A general lack of experienced security IT personnel.
- Errors/bugs created by software vendor: create security holes.
- Lack of technology understanding on the part of the average user who is easy prey.
- Easy access to the Internet from anywhere makes it harder to control.
- Availability of more and more shared processing power on the Internet allows for "Distributed Factoring", making encryption key length obsolete faster and faster.
- And much more...

Facts: Hackers are people with a superior understanding of computer kinetics, from the operating environment to its communication mechanisms. They have a great deal of patience for learning and understanding new technology behaviors. Acquiring FREE access to closed computer systems, which, at the time, were only available to large corporations, initially motivated hackers.

Hackers break the LAW to obtain information or access systems they want to understand and exploit. Hackers have different moral values than the average law-abiding citizen. That is why we separate them into two categories: "Friendly Hackers" and "Hacker Foes". Friendly hackers are just out there to have fun; they are not trying to cause harm to systems. Hacker foes maliciously attack systems to cause harm and gain certain benefits, monetary or other.

Hackers are young and old, male and female, of all nationalities and religions. They could be the coworker sitting next to you, your daughter or your neighbor.

This is not a document on the make-up and profile of a hacker, but rather an introduction. "Understanding your enemy will make you stronger" (Sun Tzu, the Art of War).

Does this security document still relate to you if you are not in charge of technology? YES, it does. As a company employee, you are part of a team and security touches everyone in a team from the physical to the digital level:

- Making sure the doors are locked properly.
- Supervising confidential material around the office environment.
- Restricting access to confidential material to non-company employees.
- Not giving sensitive or confidential information over the phone.
- Assuming responsibilities.
- Defining and enforcing policies.
- Not spreading potentially damaging viruses in your network.
- Preventing theft of company property, both intellectual and physical.
- Being AWARE of security.
- Educating other employees around you.

Today the average individual has a great deal of exposure to technology in his/her daily life. It is vital that user

What is your "Security Awareness IQ"

This is a simple test, put together by Frederic V. Farcy, CTO of TNTmax to test your security awareness IQ. Simply fill in the questionnaire below and compute your total SAIQ (Security Awareness IQ). The result will give you a sense of how aware you are of security issues. It is important you do not make up the answer. The questions have been designed to test several categories of human behavior and understanding in order to give the user an accurate "Security Awareness IQ" SAIQ.

No matter what you score on the SAIQ test, this document will help you further your awareness and understanding of security on the Internet.

It is very important that every employee of TNTmax develop an EXPERT SAIQ in order to better serve our clients' e-business needs.

SAIQ Questionnaire

Individual Related

- 1) Do you lend the key of your apartment/house/car to friends?
 - a. Yes
 - b. In special cases
 - c. In an emergency only
 - d. Never

- 2) Do you wear your seat belt while seating in a car as passenger or driver?
 - a. Never
 - b. Sometimes
 - c. Frequently
 - d. Always

- 3) How many locks do you have on your front door and how many do you lock when you leave your dwelling?
 - a. I have one and I lock it
 - b. I have two and lock only one
 - c. I have two and lock them both
 - d. I have more than two and lock them all

- 4) Once in your car/rental car, do you lock the door of the vehicles while driving or verify that the doors are locked?
 - a. Never
 - b. Rarely
 - c. Sometimes, depending of neighborhood
 - d. All the time

- 5) Do you carry a self-defense legal weapon on you when going out at night?
 - a. No, Never
 - b. Once
 - c. Occasionally
 - d. Always

- 6) When someone from the phone/cable/newspaper/other company calls you at home?
 - a. I answer all their questions if I am interested in the offer
 - b. I answer some of their questions and ask to see the offer in writing
 - c. I ask for their name and extension number and call them back on a trusted number I know
 - d. I never give information on the phone to people I do not know

- 7) Do you make purchases on the Internet using your personal credit cards?
 - a. Yes, all the time
 - b. Only on sites I trust
 - c. Only on secure sites I trust
 - d. Never, I do not trust the Internet

Work Related

- 8) Do you know what is the difference between HTTP and HTTPS and could you explain to a customer/friend why one is secure and the other is not?
 - a. I do not understand the question
 - b. I forgot what HTTPS is
 - c. I think I could explain it
 - d. I could explain it easily

- 9) Do you know and understand any of these terms? (Phreaking, warz, spoofing, zombies agents, viruses, Trojan horse, worm, DDoS, Port Scanning, Ping of Death, BackOrifice, Bok, NetBus)
 - a. None of them, but I know they are related to hackers
 - b. Some of them
 - c. All of them
 - d. Please, I am a security expert

- 10) What is the total length of your password?
 - a. 1 to 4 characters in lengths
 - b. 5 to 8 characters in lengths
 - c. 9 to 15 characters in lengths
 - d. 16+ characters in lengths

- 11) What kind of password do you use?
 - a. Characters only
 - b. Upper/Lower characters only
 - c. Upper/Lower characters mix with numbers
 - d. Upper/Lower characters mix with numbers and special characters

- 12) Do you give your password to friend/other employee in your office?
 - a. Yes
 - b. Sometimes
 - c. If I am asked by upper management
 - d. Never, unless forced

- 13) Do you keep confidential/sensitive information in a secure locked place?
 - a. No, I do not have a safe place to store it
 - b. No, I do not deal with confidential/sensitive information
 - c. Yes, sometimes
 - d. Always

- 14) Do you protect your company's Intellectual Property?
 - a. I do not know, I do not understand the question
 - b. No, it does not relate to me
 - c. Yes, I think so
 - d. Yes

Technology Related

- 15) Do you consider ATMs to be a secure way to do banking?
 - a. Yes, Always
 - b. Yes, Sometimes
 - c. Only when located indoor
 - d. Only when located indoor and with a security guard present

- 16) Do you give your mother's maiden name to Credit Card/Banking companies as a security word?
 - a. Always
 - b. Yes, because it is easy to remember
 - c. No, I make up a different name that I use for all credit/ATM cards
 - d. No, I make up different names for every credit/ATM card

- 17) Do you mind having to remember passwords and user IDs?
 - a. Yes, very much
 - b. Yes
 - c. Somewhat
 - d. Not at all

- 18) Do you use the same password/PIN code?
 - a. Yes
 - b. No, I use one PIN code and one password for everything
 - c. No, I use two PIN codes and two passwords for everything
 - d. No, I use different PIN codes and different passwords for everything

- 19) Do you use easy to remember PIN codes and passwords? (Example zip code, DOB, pet name, place, color, words, birthplace, girlfriend/boyfriend/family member name, or any combination of the above)
 - a. Yes, always
 - b. Most of the time
 - c. Sometimes, if not very important
 - d. Never

- 20) How often do you change your user IDs and passwords?
 - a. Never
 - b. Only when I am forced to
 - c. Once a year
 - d. Every three months

- 21) Do you use Encryption when sending sensitive information over the Internet?
 - a. Never, I feel e-mail is secure
 - b. I do not know how to encrypt my e-mail
 - c. Sometimes
 - d. All the time

- 22) Do you have an anti-virus scanner running on your computer at home?
- a. No
 - b. I do not know
 - c. Yes, and I update my virus data file and engine once a year
 - d. Yes, and I update my virus data file and engine once a month
- 23) Do you keep yourself informed of Internet security issues?
- a. Never
 - b. No, that is not my job
 - c. I read head lines and related e-mail
 - d. I keep up to date with Internet security issues
- 24) Do you open e-mail attachments sent to you?
- a. Always
 - b. Only if it looks fun or important
 - c. Only if I know what it is
 - d. Only if it comes from a trusted source and it has been scanned

SAIQ Questionnaire Answer

To rate your SAIQ simply total your points as follows:

If you answered (A) for any question you score 1 point
If you answered (B) for any question you score 3 points
If you answered (C) for any question you score 6 points
If you answered (D) for any question you score 10 points

If your total amount of points is:

Between 23-68: You have a LOW SAIQ and you MUST enhance your security IQ. Thus, read this document carefully and change your security habits.

Between 69-137: You have a MEDIUM SAIQ and you need to read this document carefully and change your security habits.

Between 138-192: You have a HIGH SAIQ and you should continue reading this document to keep your rating up.

Between 193-Above: You have an EXPERT SAIQ and you know you need to keep up with security issues to keep your EXPERT rating.

TNTmax requires all its employees to have a HIGH to EXPERT SAIQ, depending of their position, in order to better serve our clients' e-business needs.

TNTmax Security

Definition

The biggest challenge of Internet security today is educating users and keeping them up-to-date with the latest security issues. For this reason, TNTmax developed this white paper to educate employees, clients, and partners on an ongoing basis.

"Understanding security needs and requirements is our best defense; keeping up with the latest security developments and issues is our best offense." Frederic V. Farcy of TNTmax.

Lets start by looking at the traditional dictionary definition of the word "security" and "secure" from "The American Heritage Dictionary of the English Language":

se.cu.ri.ty 1. Freedom from risk or danger; safety. 2. Freedom from doubt, anxiety, or fear; confidence. 3. Anything that gives or assures safety. 4. Something deposited or given or assures safety. 4. Something deposited or given assurance of the fulfillment of an obligation; a pledge. 5. One who under take to fulfill the obligation of another; surety. 6. Plural. Written evidence of ownership or creditorship; especially a stock certificate. 7. Measures adopted to guarantee freedom or secrecy of action, communication, or the like, as in wartime.

Se.cure 1. Free from danger or risk of loss; safe. 2. Free from fear or doubt; not anxious or unsure. 3. a. Not likely to fail or give way; stable; strong. B. Well-fastened. 4. Assured; certain; guarantee. 5. Archaic Careless or overconfident. - tr.v. secured, -curing, -cures. 1. To guard from danger or risk of loss. 2. To make firm or tight; to fasten. 3. To make certain; guarantee; ensure. 4. To make a pledge on, as a loan. 5. To get possession of; acquire; procure. 6. To bring about; effect.

From these two traditional definitions, we can see that the words "security" and "secure" are very contextual, and therefore must be treated in relation to a very specific environment.

For the purpose of this paper, I will focus on technology-related security and the Internet. Now, let's take a look at the definition of security in relation to technology and the Internet from "Webopedia":

Security: Refers to techniques for ensuring that data stored in a computer cannot be read or compromised. Most security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

Every individual's personal evaluation of a secure situation is based on his/her own interpretation of security. This creates situations where one person's actions are un-secure for another one. For instance, one person may consider that crossing a street outside the specified crossing area is secure, while another may consider that action un-secure and dangerous. This specific case will force me to discuss security in relation to the environment of the "individual" or the "company". There are many other environments that I will not discuss in this paper in order to stay focused on security issues as related to technology.

Security Environment

It is important for any one individual to understand security in relation to his/her environment. I will look at security from the simple to the more complex environments in relation to the company and its individual requirements.

"Information system security, like all aspects of security, is far more than just a technical issue. Security depends on human beings to understand and carry out procedures. Security must become part of the corporate culture – a consistent way of approaching all aspects of one's work."ⁱⁱⁱ

Individual Security

For the purpose of this paper, I will refer to "Individual Security" as security dealing directly with a person. For example, fastening your own seat belt is an individual security response. Selecting a Personal Identification Number (PIN) for your personal bankcard is an individual security action. Each individual must consider secure or un-secure based on his/her own personal action and reaction. Individuals build relationships of trust between themselves based on a variety of factors, one of them being security. Each individual evaluates his/her own requirement for security and builds trust relationships based on these criteria. Some individual security action/responses are based on the older part of the brain, which trigger-reflex responses to threat. Example: putting your hand in front of your face to protect yourself from a ball coming at you.

Company Security

For the purpose of this paper we will refer to "Company Security" as security dealing directly with a group of people working together. Example: locking the office door if you are the last person leaving the office is a company security response. Not smoking in the office to prevent possible fire is a company security action. As with individuals, companies build trust relationships between themselves based on a variety of factors, one being security. As a company building e-business solutions for our customers, it is important to build strong security measures and procedures in order to be trusted by our clients and partners. [maxGUARD]

External Security

For the purpose of this paper we will refer to "External Security" as security dealing with everything outside the company employees and the company security policies: governmental, legal, partners' requirements, third party requirements, and more. External security requirements will dictate some of the Internal Company Security policy requirements. In turn, company security requirements will dictate individual security requirements for each employee.

Security Layers

Both individual and companies build security layers around sensitive areas to protect themselves from harm, fraud, failure, and more. I will outline these security layers and their respective level of strength and weakness as well as their roles.

The most basic layers are the secure layers versus the un-secure layers; a corporation builds a series of security layers in order to protect it from the un-secure outer layers. All information within the company belongs to the company and must be protected from the un-secure layer.

Figure 1 - Fundamental Security Components

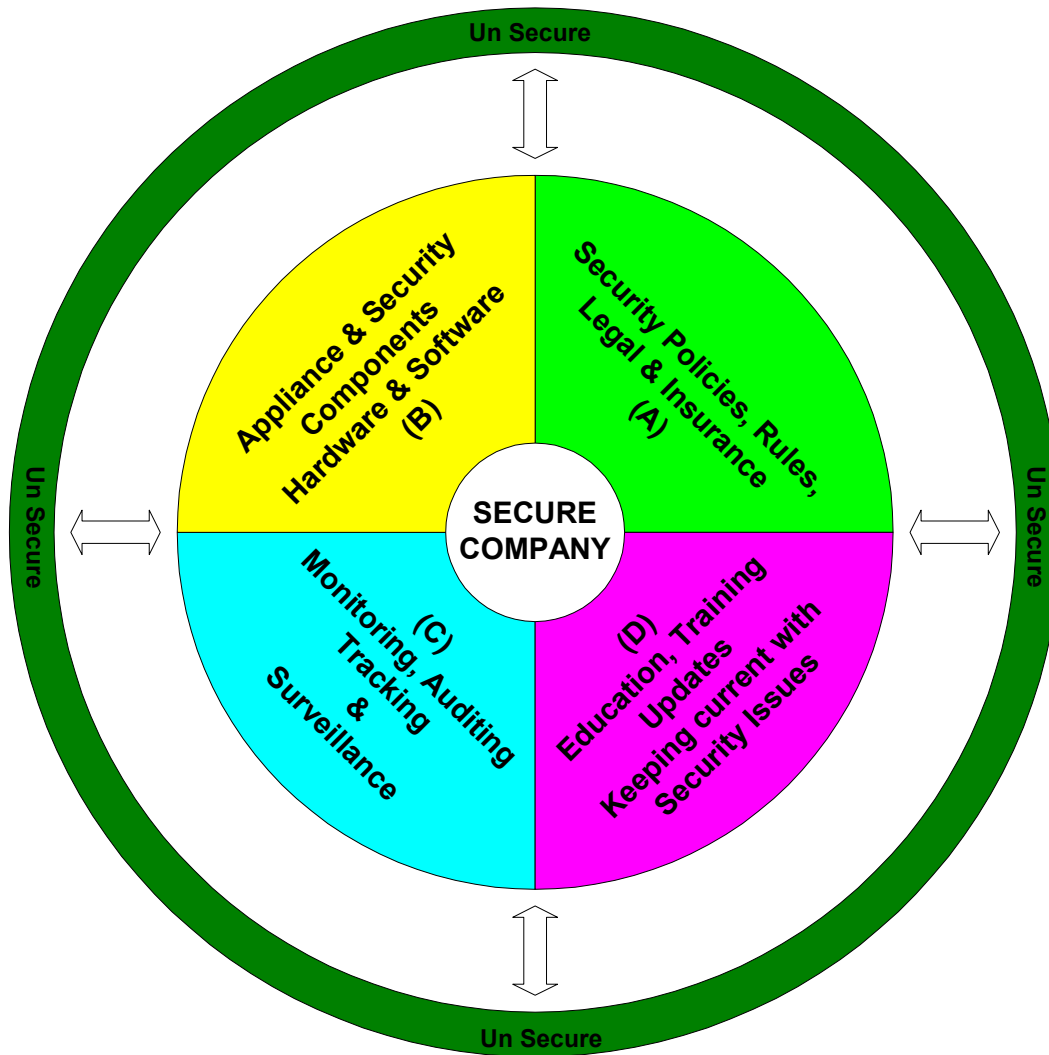
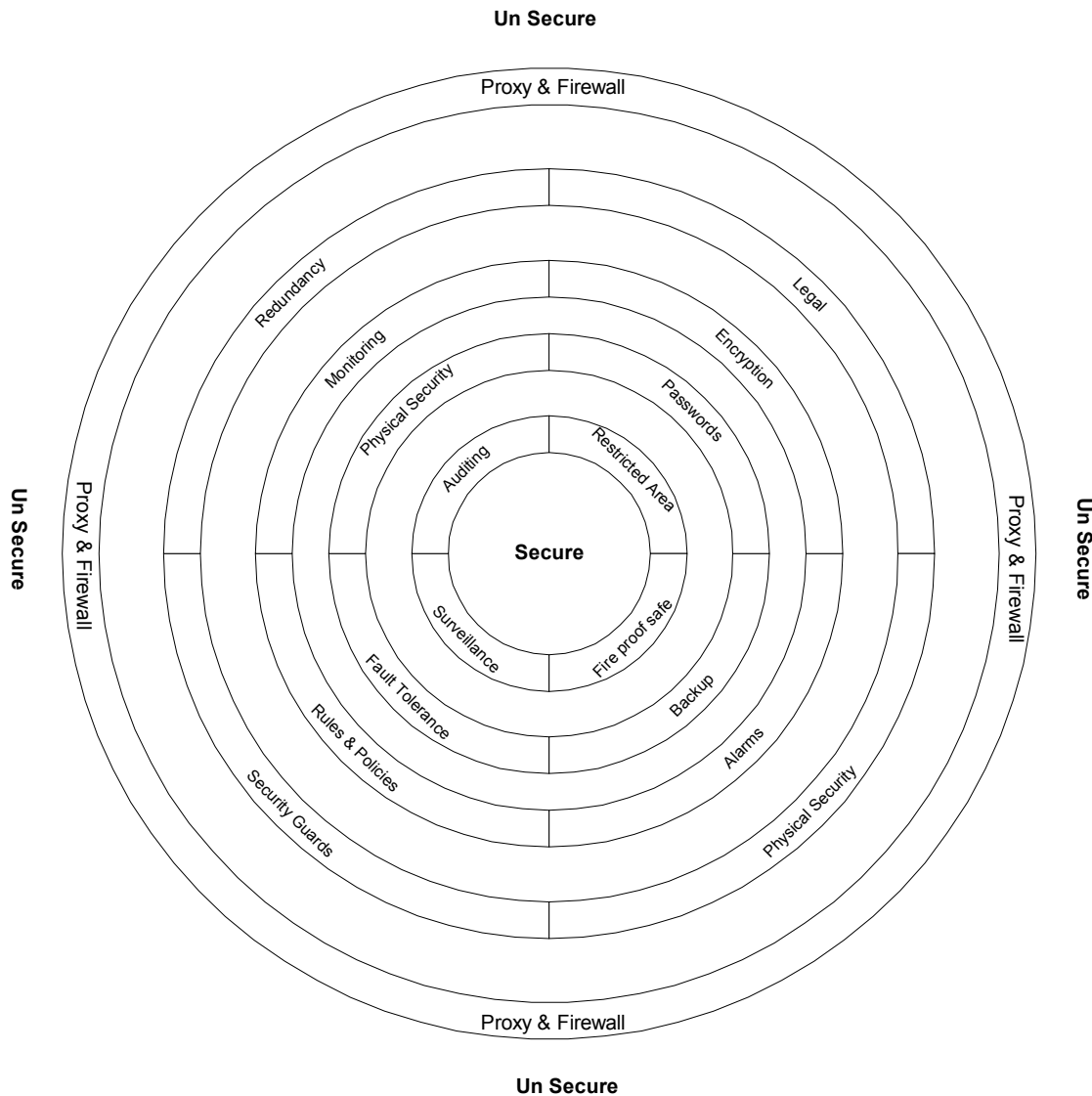


Figure 2 Example of Security Layers



Passwords

The password is a secret series of characters, digits, and other printable characters secretly selected by one user or organization. The password and a user identification (user ID) combination will grant the user or the organization access to secure computer/banking information, that recognizes and trusts them.

Understanding the strength and weakness of your password is very critical to the organization/company. Any individual who selects a weak password is putting the company at risk by creating a weakness in the security layers implemented by the company.

Password Theoretical Understanding

The amount of password variants available with a given character set can be calculated using the following formula:

Total quantity of passwords variants = Total "Key space" RAISED TO the maximum length of the password.

"Key space" is the total number of characters in the set. Character sets consist of alphabetic characters, digits, and other special characters (ex: +, -, *, &, \$, #, @, ! etc...). Character sets depend on the country of origin of the alphabet (Latin character set is different from Japanese character set and so forth). For this example we will use the U.S. character set (Latin set).

Character Set Example

| Character Set description | Example | Key space total length |
|--|-----------------------|------------------------|
| Digits only | 0-9 | 10 |
| All lower case or all UPPER case letters only | a-z or A-Z | 26 |
| Special printable characters sets only | ~-> | 34 |
| All lower case or all UPPER case letters with digits | a-z+0-9 or A-Z+0-9 | 36 |
| Mixed case letters | a-z and A-Z | 52 |
| Mixed case letters with digits | a-z + A-Z + 0-9 | 62 |
| Mixed case all printable characters | a-z + A-Z + 0-9 + ~-> | 96 |

We have compiled a table underneath that shows the time for a complete search (on a single Pentium 600Mhz), that is, in the 'worst case', the time necessary to crack a password using brute force password cracking. In the 'best case', the very first password will be the right one. The probability of finding the password in half the maximum time is 50%. Search time can be reduced using multiple and more powerful computers.

Time to Crack a Password using Brute Force

| Char sets Password length | 26 (no case, letters only) | 36 (no case, letters and digits) | 52 (case sensitive, letters no digits) | 96 (all printable characters) |
|---------------------------|----------------------------|----------------------------------|--|-------------------------------|
| 4 | Instantly | < 1 minute | 4 minutes | 59 minutes |
| 5 | 7 minutes | 38 minutes | 4 hours | 4 days |
| 6 | 3 hours | 25 hours | 8 days | 12 months |
| 7 | 4 days | 38 days | 17 months | 108 years |
| 8 | 3 months | 4 years | 69 years | 10900 years |
| 9 | 8 years | 127 years | 4087 years | > 1M years |

* Base on PIII 600mhz single CPU using John the Ripper.

Password Structure Rule

All individual TNTmax employee passwords must be 8 characters or greater and must use a combination of upper and lower characters + digits + special characters. TNTmax requires a minimum length and character set type for individual passwords, but it is important that each individual employee understand the strength and weakness of a password.

Example of a password following TNTmax minimum requirements: **FreD57&58**

TNTmax Password Strength Scale

TNTmax has established a strength scale to help individual employees identify weak passwords. All passwords in **BOLD** are considered by TNTmax as weak and must never be used by individual employees of the company. TNTmax considers all passwords in *Italics* to be acceptable as long as individual employees change them every three months. TNTmax considers all passwords underlined as strong passwords as long as individual employee changes them every year.

| Char sets PSW Length | 26 (no case, letters only) | 36 (no case, letters and digits) | 52 (case sensitive, letters no digits) | 96 (all printable characters) |
|-------------------------|-------------------------------|--|---|-------------------------------------|
| 4 | 456976 | 1679616 | 7311616 | 84934656 |
| 5 | 11881376 | 60466176 | 380204032 | 8153726976 |
| 6 | 308915776 | 2176782336 | 19770609664 | 782757789696 |
| 7 | 8031810176 | 78364164096 | 1028071702528 | 75144747810816 |
| 8 | 2.09e+11 | 2.82e+12 | 5.35e+13 | <i>7.21e+15</i> |
| 9 | 5.43e+12 | 1.02e+14 | <i>2.78e+15</i> | <i>6.93e+17</i> |
| 10 | 1.41e+14 | <i>3.66e+15</i> | <i>1.45e+17</i> | <u>6.65e+19</u> |
| <i>11</i> | <i>3.67e+15</i> | <i>1.32e+17</i> | <i>7.52e+18</i> | <u>6.38e+21</u> |
| <i>12</i> | <i>9.54e+16</i> | <i>4.74e+18</i> | <u>3.91e+20</u> | <u>6.13e+23</u> |
| <i>13</i> | <i>2.48e+18</i> | <u>1.71e+20</u> | <u>2.03e+22</u> | <u>5.88e+25</u> |
| <u>14</u> | <u>6.45e+19</u> | <u>6.14e+21</u> | <u>1.06e+24</u> | <u>5.65e+27</u> |
| <u>15</u> | <u>1.68e+21</u> | <u>2.21e+23</u> | <u>5.50e+25</u> | <u>5.42e+29</u> |

NOTE: Important sometime the password algorithm is flawed making the length of a very long password crack able in relative short time (Example: WEP encryption flaw).

Password Crack Understanding

It is important to understand how a password can be cracked in order to better understand what type of password to use and when. Many techniques are used to crack/hack passwords:

- Guessing (Bad passwords are easily guessed by Hackers)
- Shoulder Surfing (Hackers watch your fingers as you enter the password)
- Brute force attack (Software)
- Psychological Hack (Hackers can obtain valuable information by lying, on the phone, for example)
- Running a large Dictionary of man made passwords against your passwords
- Bribery
- Seduction
- Extortion
- Blackmail
- Impersonation
- More

ATM card PIN codes can have as little as 4 digits ($9^4 = 6561$ possibilities or $10^4 - 10,000$). To protect consumers, banks allow a total of three wrong PIN code entries before locking the customer's account from any further access.

However, Microsoft Word, Excel, and Access passwords can be cracked using dictionary and brute force and other software-cracking algorithms. However, the perpetrator must first gain access to a file in order to run software against it.

User Logins, e-mail, and other passwords can also be cracked using dictionaries, brute force, and other software-cracking algorithm. But again, the perpetrator must gain access to the password file in order to run software against it. Password files are usually stored in a secure directory on the server, but operating system bugs and other software security weaknesses can make these files accessible to any knowledgeable hacker.

Changing your Passwords

It is very important to understand that changing your passwords periodically is not only crucial but also necessary. The right combination of password length complexity with periodic change gives every individual user a higher chance of keeping his/her password secure.

Company policy requires all of our employees to change their passwords every three months and does not let our employees use the same password twice. The company's goal is to minimize the possibility of a security breach.

Password Hints

- Password hints are structured as follows:
- Password updating hints
- Minimum number of passwords on your digital key chain required hints
- Password selecting hints

Updates Hints

- Change your passwords often and keep strict rules.
- Always change all your passwords at the same time
- Use your own method to remember your passwords
- Learn all your password(s) at your own speed, one at a time or all at once, but avoid writing them down on paper
- Change all passwords at least every three months
- Put all your user id and passwords in a safe or safety deposit boxes with detail instruction for your family and spouse in the even of death.

Digital Key Ring Minimum Password Hints

Your digital key ring will depend greatly on your individual requirements. I will break down the categories in order to let the reader select the best match for their personal profile.

The following categories are broken down into:

- Home user only
- At work users only
- Both home and at work users

Simple profile categories break down:

| Digital Key Ring | | Categories | | | | | |
|------------------|---------------------------|------------|------|------|------|------|------|
| | | A | | B | | C | |
| | | Work | Home | Work | Home | Work | Home |
| 1 | E-Mail account(s) | NO | YES | YES | NO | YES | YES |
| 2 | Internet Dial-Up Account | NO | YES | YES | NO | YES | YES |
| 3 | Login PC/Workstations | NO | YES | YES | NO | YES | YES |
| 4 | Login Database (Info) | NO | YES | YES | NO | YES | YES |
| 5 | Login Accounting/Banking | NO | YES | YES | NO | YES | YES |
| 6 | Login Trading/Financial | NO | YES | YES | NO | YES | YES |
| 7 | Password Word Document | NO | YES | YES | NO | YES | YES |
| 8 | Password Spreadsheet | NO | YES | YES | NO | YES | YES |
| 9 | Password Project/Others | NO | YES | YES | NO | YES | YES |
| 10 | Password Project/Others | NO | YES | YES | NO | YES | YES |
| 11 | Credit Cards Phrase/Word | NO | YES | YES | NO | YES | YES |
| 12 | E-Commerce Registration | NO | YES | YES | NO | YES | YES |
| 13 | Other E-Registration | NO | YES | YES | NO | YES | YES |
| 14 | Chat, mIRC, e-Boards, etc | NO | YES | YES | NO | YES | YES |
| 15 | FTP, Telnet, VPN, Other | NO | YES | YES | NO | YES | YES |

You should NEVER HAVE ONE PASSWORD FOR ALL YOUR PASSWORD REQUIREMENTS. Minimum requirements are:

If you have a total of 1-5 Digital Key Ring Requirements you need to have a minimum of five different user IDs and five different passwords.

If you have a total of 6-10 Digital Key Ring Requirements you need to have a minimum of six different user IDs and six different passwords.

If you have a total of 11-15 Digital Key Ring Requirements you need to have a minimum of seven different user IDs and seven different passwords.

If you have a total of 16+ Digital Key Ring Requirements then follow the same rule of adding a minimum of one user ID and password per every five digital key ring requirements.

Password Selecting Hints

One simple hint: your password must be as random as possible. Use the proper length as described above (TNTmax Password Strength Scale). Use a good combination of mixed upper and lower case, with digits, special characters and regular characters. Stay informed about security issues. Electronic security is a new requirement; not everyone is pleased by this requirement, but you should use all secure means to protect your own privacy.

Password Safe

Use password safe to store all your passwords, user id, credit card information and other sensitive information. A password safe is a software program that provides a user with the ability to store his/her password, user id and other sensitive information in a secure file requiring one password to access.

Password safe program are not all created equal and make sure that you get one that use strong encryption for the password database file. Use a very long and complex password for this one software.

Example: "passwordsafe" program is small and use blowfish strong encryption, it can fit on a floppy disk <http://www.counterpane.com/passsafe.html>.

Backup your safe password database and software on a CD-ROM and put it in a safe or safety deposit box.

E-Mail

Introduction

E-mail is by far the most popular tool on the Internet. Although it is difficult to put a number on the fast-growing number of people, machines, appliances and other devices connected to date, a close estimate of the Internet user population would be 200 million worldwide. If every user sends and receives a low average of 5 e-mails per day, this represents 1 billion e-mails going around the planet every day.

Besides being one of the greatest communication tools, e-mail is also the number one target for:

- Virus distribution and attack
- Information and data theft
- Harassment
- Spamming
- Other

The recent "Love Letter" and copycat viruses illustrate the power of e-mail. A single virus that utilized a simple Windows 9.x and 2000 scripting language and a re-mailer distribution scheme, using each target user e-mail account(s) and address book(s), was able to spread across the planet within a few hours.

The virus was very effective for three simple reasons:

- The virus attacked directly upon activation; that is, the virus needed to be activated by opening its attachment in order to harm computers.
- The virus used a trusted e-mail address scheme distribution to guarantee high click-rate (recipients got the virus e-mail from a friend or trusted e-mail source)

No VIRUS DATA and CURE were available for the first 3 hours -- from initial detection and before widespread warning hit the Internet.

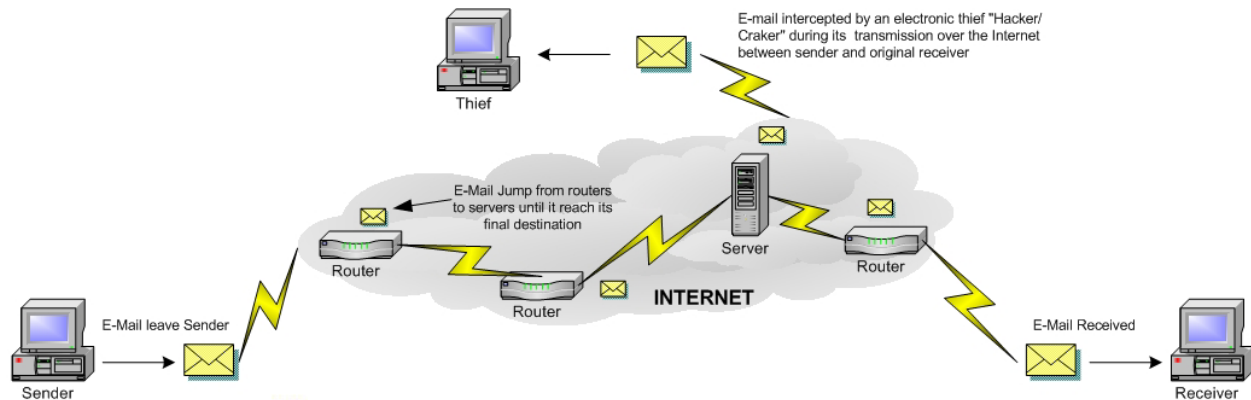
The virus code is easily modifiable by anyone; therefore beware of any attachment sent to you. There are already several copycat versions of the "Love-Letter" virus circulating over the Internet with such new names as "Very Funny".

How the spreading of the virus could have been prevented? How can data be protected from replacement or deletion? **maxGUARD**

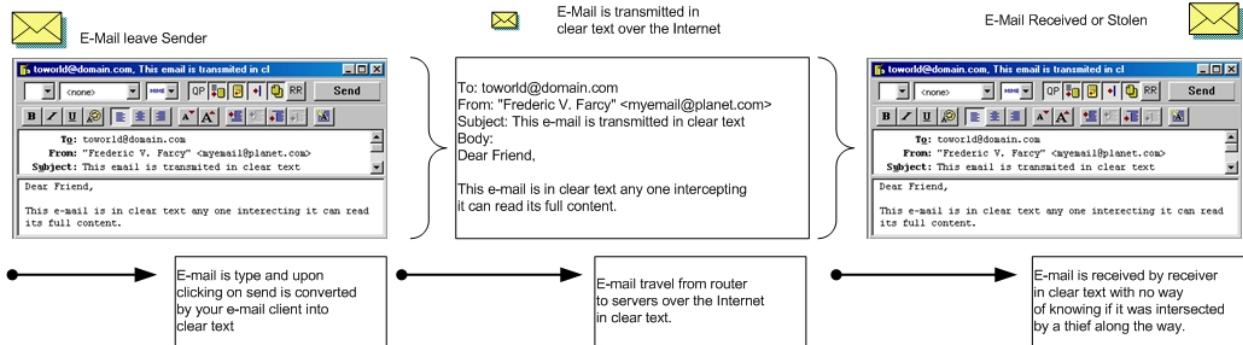
What you need to know about E-Mail

E-mail is a revolutionary communication tool. It is simple to use, fun, and powerful (allowing us to send pictures, video, sound, and text around the world for a fraction of the cost, almost instantaneously). Yet, we need to understand a few important facts about e-mail.

Most e-mail servers use a method of transmission over the Internet called clear text (see diagram below – CLEAR Text Email Transmission Diagram). This means that the content of your e-mail is fully readable by any person stealing it along the way, before it reaches its destination. We will not detail how electronic thieves are able to steal or modify your clear text e-mail, but it is important to be aware of that possibility.



CLEAR Text E-Mail Transmission Diagram



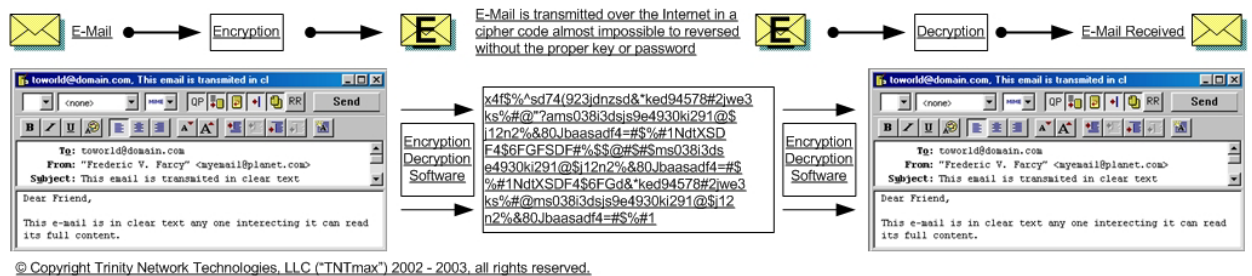
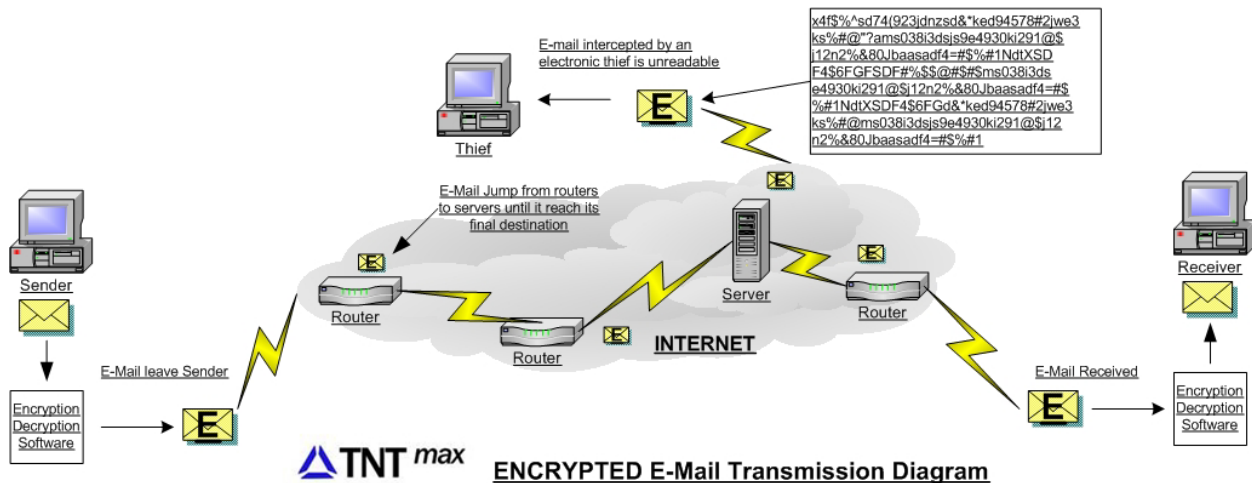
© Copyright Trinity Network Technologies, LLC ("TNTmax") 2002 - 2003, all rights reserved.

Simple E-Mail Security Rules

- Always assume that your e-mails are sent in clear text, unless you know otherwise or have been instructed otherwise by your computer specialist.
- Review the type of information/data you are about to transmit via e-mail and select the appropriate security measures (see below for e-mail security measures).
- Use virus scanner software on all your incoming and outgoing e-mail using the latest "Virus Definition Data" file.
- Do not click open on any unexpected attachments, especially executable software, scripts, ActiveX, Java, bizarre links, and other unrecognized items.
- Make sure you identify the sender's e-mail address and the name of the attachment. If you can only identify the e-mail address and do not recognize the attachment or are not expecting an attachment, inquire about the content of the attachment by contacting the sender directly, BEFORE opening the attachment.
- Use encryption protection when sending sensitive information via e-mail (see Diagram below - ENCRYPTED e-mail Transmission Diagram). Encryption software ciphers the content of your message before sending it. For the encryption to work, both the sender and receiver must use the same encryption/decryption software. A

prior password or key received by the sender enables him/her to de-cipher the content of e-mail.

- Use password protection when sending sensitive attachment information. Some software allows the sender to add a password to attachments. Call the recipient to give him/her the password or send the password through an encrypted e-mail.
- Restrict access to your personal computer or office workstation.
- Stay informed of new Viruses and Security problems and issues.



E-Mail Security Tools

Today you use e-mail to create, send, and receive your e-mails. In addition to staying informed on security issues, you will need the following software:

- A virus scanner active on your personal computer and/or office workstation (example McAfee, Norton Anti Virus, or Others).
- A key base encryption/decryption software package (example PGP or others).
- Stay informed of new software tools. [maxGUARD]

TNTmax maxGUARD – Security Solution

Even the most security savvy companies will have vulnerabilities on their network and, because of this, must remain diligent to minimize risk. The first step is knowledge and with knowledge comes the opportunity to mature and improve.

TNTmax maxGUARD is a firewall, Intruder Detection System, Virtual Private Network VPN, Content Filtering, Anti-Virus Filtering, Content Monitoring, Cache Server combine with the daily monitoring, management and support of our Security team of experts.

maxGUARD combines the strength of Linux base open source software tools with the TNTmax security team. We believe that the combination of constant update, management and monitoring of our client network provide the strongest defense.

Monitoring a cracker during a network discovery enable us to anticipate his/her next move and counter before the fact, while constantly learning from our enemies.

TNTmax + maxGUARD = TNTGUARD^{max} (Winning combination for your security requirements.)

maxGUARD is built using open source ONLY components, any component we modify or create follow the open source GPL. The software is built around Linux Debian Distribution customized and harden for maxGUARD, we use, IPTABLES, SNORT, SQUID, OPEN SSH, FREE SWAN and more.

Today security is not simply an appliance you plug in front of your network and hope, will provide you with the protection you need. Today technologies security need to utilize the best software available as well as the best knowledge from security experts. Only that combination of the latest technologies and human expert knowledge can anticipate and best react to secure your business against security threats.

Example of Security Problem and Solutions:

- **Problem:** Employee inside the network decides to download and install on his Machine a P2P software Example KazaA – Morpheus to download music and other items from the Internet. This creates a great security threat, since the user is opening a hole from the inside for crackers to exploit.
- **Solution:** maxGUARD can prevent these P2P software from communicating with the outside world rendering them useless. Also maxGUARD can monitor known ports. Example: 1241 for KazaA.
- **Problem:** User uses IM Instant Messaging protocol to talk to friends and co-workers Example: AOL IM, MSN, Yahoo and others.
- **Solution:** IM can be banned from use during office hours 9:00am to 5:00pm by applying a content filter from within the network using maxGUARD, that prevent all or selected users from using IM Instant messaging.
- **Problem:** User introduces virus into the network by downloading personal attachments from their personal online e-mail (example : Yahoo mail, Hot mail, etc).
- **Solution:** Personal E-mail can be banned from use during office hours 9:00am to 5:00pm by applying a content filter from within the network using maxGUARD, that

VPN – Virtual Private Network

Virtual private network "VPN" is a method that establishes a secure "private network" to a computer at another location through the public Internet. This is frequently used by businesses to allow employees to telecommute and establish a connection to their private company network. Companies with offices in various geographical locations can now connect to the Internet at each of their geographical locations and establish a VPN secure private network between each site to create a Wide Area Network (WAN) using the existing Internet network instead of an expensive dedicated private network.

Virtual Private Networking (VPN) has become one of the new buzzwords in the networking industry. Unfortunately, the term VPN can mean different things to different people. Following are some definitions.

VPN Client

A few years ago, employees working from home, traveling, or working in small offices would connect to a corporate network via dial-up sessions into their corporate Remote Access Server (RAS). This would require long distance calls in some cases plus required the corporation to support modems and dial-in lines, similar to what Internet Service Providers have to do. Since most employees have Internet connections from home, it made sense to be able to connect to the corporate site over their dial-up Internet connection. This also allows employees to use their local ISP's fastest connection such as cable modems, DSL, and ISDN. For traveling users, all they would need to do is dial into their ISPs local phone number.

To enable this connection to be encrypted, protocols needed to be developed. The first remote user VPN protocol to be widely distributed is the Point to Point Tunneling Protocol (PPTP) from Microsoft. Windows NT 4.0 includes PPTP for free so it's become the popular VPN protocol for NT networks, even though it doesn't have the strongest security. Today, the IP Security (IPSec) protocol has emerged as an industry standard protocol. While the IPSec protocol provides strong security, you'll also see it used with the Layer 2 Tunneling Protocol (L2TP used by Microsoft) to help out with IP addressing management on the VPN clients.

VPN Gateway

Before VPN, companies would connect their offices together via expensive point-to-point leased lines. With the Internet explosion, companies wanted to utilize the Internet as their Wide Area Network (WAN) link to save cost. For security, the data being transmitted over the Internet must be encrypted. The IPSec protocol is being used for site-to-site VPN creating a secure network gateway between the two sites.

VPN Extranet

Extranet describes one application using VPN technology. The concept is that a company and a vendor/supplier can access network resources at each site. Before Extranets, some companies connected to their suppliers via leased-lines and built separate supplier

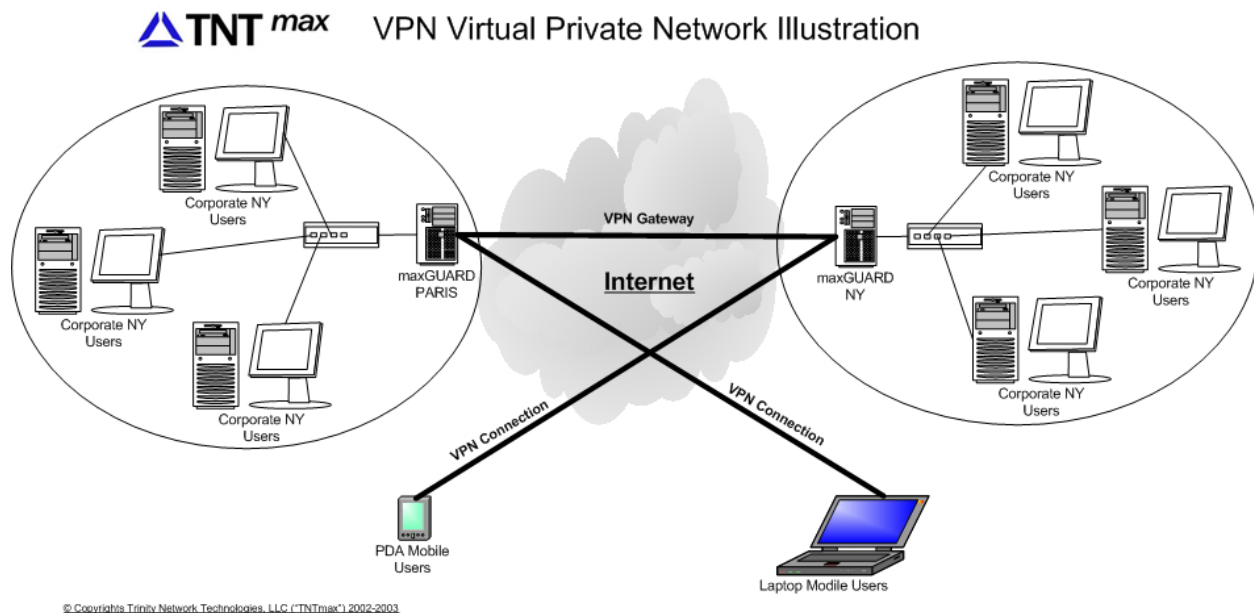
networks, isolated from their internal corporate network. Going forward, IPSec is the protocol for Extranet applications. Extranet equipment must also enforce authentication and authorization policies in addition to encryption.

VPN intranet

Now that the IPSec protocol is becoming the de facto standard, the next logical application is to extend IPSec within the intranet. This allows data throughout the intranet to be encrypted. This application is also being called Virtual Private LAN (VPLAN). Microsoft's upcoming Windows 2000 O/S includes IPSec which will allow encryption all the way down to the server (or client).

VPN Benefits

VPN utilizes the inexpensive worldwide INTERNET network backbone to build a virtual private network on top of it at low cost rather than using expensive private network "Packet Switching Network". It provides employees with easy secure remote access to the company network over the INTERNET.



WIRELESS Network

Wireless networks enable users to interconnect their computer system using broadcast wireless airwave. This is rapidly becoming a very popular way for users everywhere to connect their computer to a network. IEEE 802.11b wireless network can be found in most Starbucks coffee stores as well as some parks, campuses and many other areas.

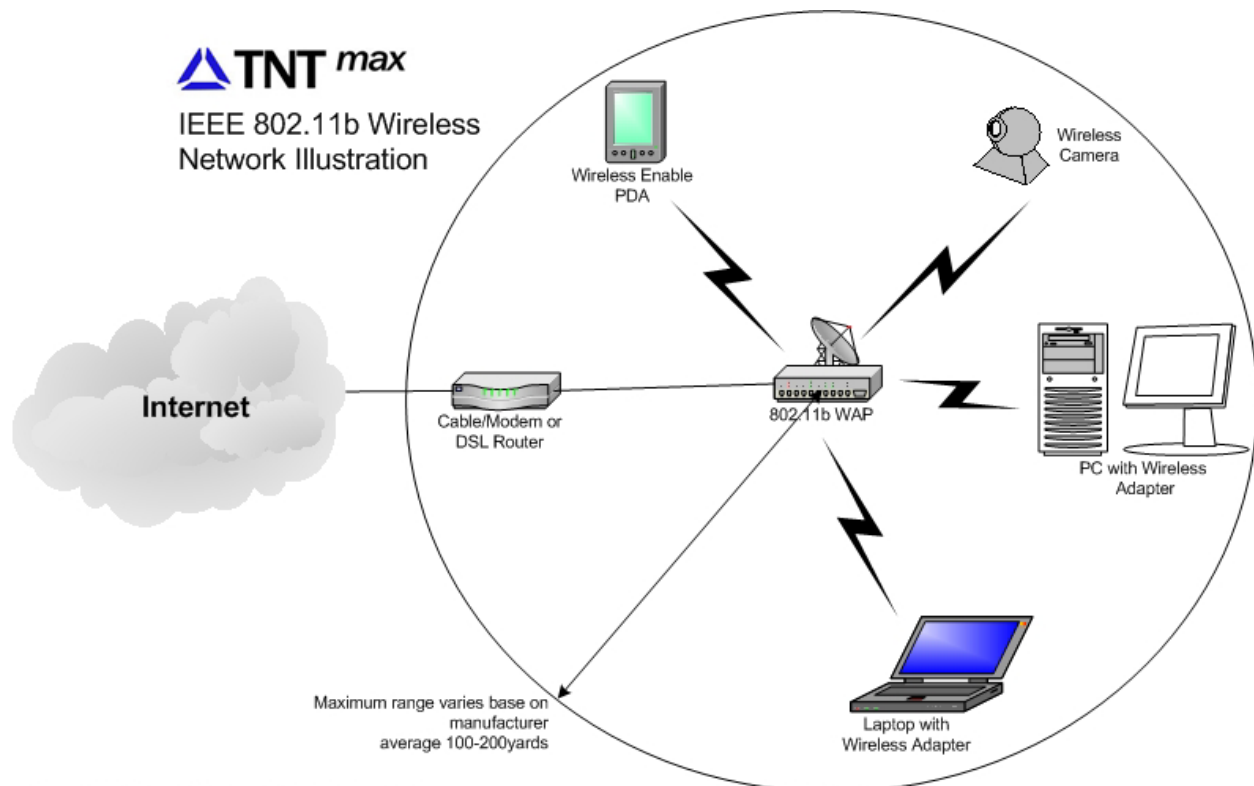
Brief Introduction to 802.11b

Wireless 802.11b technology lets a home user create a simple network to connect to his/her Cable Modem or DSL Internet connection without using any wiring.

It is important to understand that there are a great deal of wireless technologies in existence today but for the purpose of this paper I will focus on 802.11b which is the most popular today. Other wireless technology examples are: 802.11a, BlueTooth, GSM etc).

802.11 use DSSS (Direct Sequence Spread Spectrum) to generate the bit streams to be transferred in the 2.45-GHz ISM band with a speed up to 11Mbps base on distance, climate and physical obstacles.

Wireless networks are very simple to install and get going fast. They require the installation of a wireless access point WAP connected with a wire to the network and the installation of a wireless network adapter in the client portable computer or PDA.



© Copyrights Trinity Network Technologies, LLC ("TNTmax") 2002-2003

Wireless Security Need to Know

Wireless technology utilized broadcasting as main vehicle to communicate with devices locate in its perimeter range. It is possible to pickup wireless network utilizing professional antenna up to 1 mile from the broadcasting WAP. The average wireless network adapter does not support that range (see your manufacturer manual for maximum range).

Wireless network configured with no encryption send information over the airwave in clear text (everyone can read the information being transmitted/received).

Most important to know is WEP (Wired Equivalent Privacy) used to encrypt the information traveling in the airwave is flawed and can be broken quite easily and almost in real time. Similar WEP2 revision of the WEP contains similar weaknesses making the protocol not secure and not to be trusted by the user.

WAR Driving

War driving also called net-stumbling and parking-lot attack is the most trivial method to compromise a wireless network with or without the notice of the user. All the perpetrator requires to perform such attacks are:

- Laptop Computer
- Wireless network adapter
- Extra Antenna with boost up range capability (not required)
- Wireless network sniffing programs (AirSnort, Sniffer Wireless, Airosniff and more)
- WEP Encryption cracking program (WEPCrack, Kismet and more)
- Other network software tools (TCPDump, Prism2Dump)
- Wheel to drive around in high populated area looking for active networks

Wireless protection and countermeasure

Do not wait for WEP security updates, instead use a firewall and VPN connection; example: maxGUARD. Implement SSID and MAC Address restriction and use secure protocol such as IPSec, VPN, SSH, SSL to communicate.

Security facts you should know

- 1) **Deleted Files.** When you delete a file from your computer by pressing Delete or by dragging it into the recycle bin. The file is not actually deleted from your computer, but made available for overwrite by the operating system.
- 2) **P2P – Peer to Peer.** Do not install Peer to Peer software on your machine, they are a great security threat, used in large extent by cracker/hacker that upload worms and viruses as well as remote control software. They also create many other problems that can give cracker and hacker full access to your computer. (Example: KazaA, Morpheus, etc..)
- 3) **IM – Instant Messenger.** Be aware that IM has many security flaws that enable cracker/hacker to listen in on your conversation, have access to your hard drive. Keep up to date with the latest security patch for your IM and disable file sharing, and all other options you do not need (Example: AOL IM, Yahoo IM, MSN IM, etc...)
- 4) **IRC – Internet Chat Relay.** Be aware that IRC are full of cracker/hacker that pretend to offer free software/music and send their target infected WORM file with backdoor to provide them access to your computer. IRC are very big for Social Engineering, be aware of what info you provide strangers (Never give any info to strangers that may harm you).
- 5) **Outlook Attachment.** Microsoft Outlook keeps your attachments in a hidden folder in the "Documents and Settings" folder. You will need a third party tool to force Outlook to accept all extension files sent to you or access that folder directly. When deleting an e-mail, it is stored in the delete folder of Outlook, when you empty the delete folder in Outlook, your e-mail is still stored in the PST file until you run the COMPACT folder option.
- 6) **Social Engineering.** Is the most common tactic used by an individual or group of cracker/hacker to make the target feel comfortable and secure to divulge key information that will enable them to break into a company's computer system. Always know the source that is contacting you. See example of real life social engineering: <http://online.securityfocus.com/infocus/1527>
- 7) **Knowledge is your best defense...**

Top Hackers/Crackers List

The top Hackers/Crackers list found below is a partial small list in alphabetic order. The list has group and individual that are listed using their online HANDEL.

| | | |
|------------------------------|--------------------------|---------------------|
| AX1S | LmT | The Pull |
| Bronc Buster | Lone Star Hellion | Vladimir Levin |
| Captain Zap: Ian Murphy | MafiaBoy DDOS | |
| cDc CULT OF THE DEAD COW | MAYHEM | Many Many More..... |
| Code Sifu | Merlot Soak | |
| David Smith – Mellissa Virus | MOD Masters Of Deception | |
| DEBIAN | Moonlight Maze | |
| Drunken Master | Zilterio | |
| EVILZ | Network Wrangler | |
| Gravy Maven | NICK1 | |
| Hacktivismo | Oxblood Ruffin | |
| Haxx0ring | poizonB0x | |
| Hole Poker | Pr0phet | |
| Jon Messner | r00tcrew | |
| John T. Draper | Research Beast | |
| Kevin Mitnick | Robert Tappan Morris | |
| Lederhosen Enthusiast | The Mixer | |

TNTmax Security Resources

This is an ongoing reference list intended to be refined with every revision of this White Paper. Feel free to communicate to me your suggestions for additions/corrections to this document at ffarcy@TNTmax.com

Governmental Resources

CIA – The Central Intelligence Agency

<http://www.cia.gov/>

The Central Intelligence Agency was created in 1947 with the signing of the National Security Act by President Truman. The National Security Act put in charge the Director of Central Intelligence (DCI) with coordinating the nation's intelligence activities and correlating, evaluating, and disseminating intelligence, which affects national security.

FBI – The Federal Bureau of Investigation

<http://www.fbi.gov/>

The Federal Bureau of Investigation (FBI) is the principal investigative arm of the United States Department of Justice (DOJ). Title 28, United States Code (U.S. Code), Section 533, which authorizes the Attorney General to "appoint officials to detect...crimes against the United States," and other federal statutes, gives the FBI the authority and responsibility to investigate specific crimes. At present, the FBI has investigative jurisdiction over violations of more than 200 categories of federal crimes.

NSA – The National Security Agency

<http://www.nsa.gov/>

"Fear the network of the gods, because it does not fear you". The National Security Agency is the Nation's crypto logic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. A high technology organization, the NSA is on the frontiers of communications and data processing. It is also one of the most important centers of foreign language analysis and research within the Government.

CIAC – Computer Incident Advisory Capability

<http://ciac.llnl.gov/>

CIAC provides on-call technical assistance and information to [Department of Energy \(DOE\)](#) sites facing computer security incidents. This central incident handling capability is one component of all encompassing service provided to the DOE community. The other services CIAC provides are: awareness, training, and education; trend, threat, vulnerability data collection and analysis; and technology watch. This comprehensive service is made possible by a motivated staff with outstanding technical skills and a customer service orientation. CIAC is an element of the [Computer Security Technology Center \(CSTC\)](#) which supports the [Lawrence Livermore National Laboratory \(LLNL\)](#).

Military Resources

DARPA – Defense Advanced Research Project Agency

<http://www.darpa.mil/>

The Defense Advanced Research Project Agency (DARPA) is the central research and development organization for the [Department of Defense \(DoD\)](#). It manages and directs selected basic and applied research and development projects for DoD. It pursues research and technology where risk and payoff are both very high and where success may provide substantial advances for traditional military roles and missions and dual-use applications.

DTIC – Defense Technical Information Center

<http://www.dtic.mil/>

A key element of the DoD Scientific and Technical Information Program, the DTIC is the central Department of Defense facility for providing access to and facilitating the exchange of scientific and technical information. The DTIC's Homepage describes the wide variety of products and services available from DTIC, which are designed to assist our users in obtaining the information they need easily and quickly. DTIC is part of the Defense Information Systems Agency ([DISA](#)).

Telecommunication Resources

AT&T

<http://www.att.com/isc/>

AT&T has a long history of ensuring the security of their customers' communications. The success of e-commerce has led to a proportional increase in computer-aided crimes. The AT&T Information Security Center can help protect your network.

Exodus

<http://www.exodus.net/security/>

Exodus Communications has developed a series of security products and support services to meet the challenges of both physical and electronic security.

Globix

http://www.globix.com/services_security_beyond.html

Security does not end at the firewall. Globix partners, with the most sophisticated companies in the industry, offers enhanced security services.

UUNET – MCI WorldCom

<http://www.uu.net/products/uusecure/>

UUNET® understands that security is vital to organizations using the Internet. UUNET® is able to supply leading security products, designed to protect your Internet-connected network against intrusion and help you use the IP infrastructure as a private communications platform.

Verizon

<http://www.vzmultimedia.com/customersupport/areacodes/seccheck.html>

Verizon Communications.

Organization Resources

CERT – Carnegie Mellon Software Engineering Institute

<http://www.cert.org/>

The CERT Coordination Center is part of the [Survivable Systems Initiative](#) at the [Software Engineering Institute](#), a federally funded research and development center at [Carnegie Mellon University](#). They were started by DARPA (the Defense Advanced Research Projects Agency, part of the U.S. Department of Defense) in December 1988, after the Morris Worm incident crippled approximately 10% of all computers connected to the Internet.

Originally, their work was almost exclusively incident response. Since then, they have worked to help start other incident response teams, coordinate the efforts of teams when responding to large-scale incidents, provide training to incident response professionals, and research the causes of security vulnerabilities, prevention of vulnerabilities, system security improvement, and survivability of large-scale networks.

SANS Institute Online

<http://www.sans.org/newlook/home.htm>

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 62,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions for the challenges they face. As part of this effort, SANS offers a series of exceptional educational conferences featuring up to eight days of in-depth courses and multi-track technical conferences focusing on user experiences and problem solving. SANS also produces a series of cooperative research reports, electronic digests, posters of authoritative answers to current questions, and cooperatively created software

Software Vendors

Microsoft – Microsoft Security Advisor

<http://www.microsoft.com/security/>

Microsoft security issues regarding all their products line, from Internet, applications, operating systems and more.

MyCIO

<http://mycio.com/>

MyCIO.com is the world's first infrastructure application service provider (ASP) to deliver managed network security and availability services via the Internet. MyCIO.com provides simple, quick, and cost-effective application services that free companies from managing complicated enterprise security and availability software.

Built around the leading names in security and availability-McAfee, PGP and Sniffer-myCIO.com services ensure continuous, uninterrupted protection against the growing number of security threats to critical e-business applications networks.

Network Associates - McAfee

<http://www.networkassociate.com/> or <http://www.nai.com/>

With headquarters in Santa Clara, Calif., Network Associates (Nasdaq: NETA) is the world's largest independent network security and management software company and the eighth largest independent software company overall. Network Associates is the culmination of best-of-breed technologies from the world's leading software developers. These leading brands are used by Network Associates' more than 60 million customers around the globe and include McAfee anti-virus, PGP encryption, Gauntlet firewall, Magic Help Desk applications, and the Sniffer family of network analyzers.

eEye – Digital Security

<http://www.eeye.com/html/>

eEye is your security partner, watching over networks. They provide consulting and security services to help secure networks and the vital corporate data that reside on servers.

Debian

<http://www.debian.org/>

Open source distribution of Linux. One of the largest and most stable distribution of Linux, for the system administrators.

Security Industry

Trusted System Service Inc.

<http://www.trustedsystems.com/>

Trusted Systems Services has been in business since 1986. In the early days, they architected several high-end "B-level" versions of secure UNIX. Trusted System Service was one of the first companies to dedicate to Windows NT security -- back when it was 3.1! Their textbook *Windows NT Security Guide* (Addison-Wesley) was the second one on the subject.

Trusted System Service Inc. has done much security consulting, government projects, training, and software, mostly Windows NT. Today their primary business is creating, selling and supporting their own security software for Windows NT/2000. While they still do some security consulting, most of this work is custom installation of their AdvancedChecker product.

ICSA.net

<http://www.icsa.net>

ICSA.net is the worldwide leader in security assurance services for Internet-connected companies. ICSA.net's services reduce risk and improve the quality of Internet security implementations, enabling the safe deployment of new Internet technologies and applications. ICSA.net supports both corporate-user and the vendor/supplier communities with critical industry data and analysis from ICSA Labs, the industry's leading product research and certification facility, and with the industry leading publication for security professionals, Information Security Magazine.

Security Focus

<http://www.securityfocus.com/>

SecurityFocus.com is designed to facilitate discussion on security related topics, create security awareness, and to provide the Internet's largest and most comprehensive database of security knowledge and resources to the public.

SecurityFocus.com is a single place, or community, on the Internet where people and corporations can find security information and have security questions answered by leading authorities in the industry. This site provides access to security links and resources including news, books, mailing lists, tools and products, and security services. In addition to this knowledge, SecurityFocus.com features one of the strongest collections of security advisories, vulnerabilities and solutions available on the Internet.

AntiOnline

<http://www.antionline.com/>

Security resources site – very useful.

AntiCode

<http://www.anticode.com/>

Security resources site – very useful.

HackerWhacker

<http://www.hackyourself.com/>

Security resources site – very useful.

Cracker/Hackers

Important Notice: Do not try to contact people or parties from the sites listed below. The information listed below has been compiled for research purpose ONLY.

2600

<http://www.2600.com/>

Hacker and cracker magazine.

Blacklisted411

<http://www.blacklisted411.com/>

Official Hackers Magazine.

DEFCON

<http://www.defcon.org/>

DEF CON is made up of many people, who all know kung-fu and networking. Once a year, much like the quickening, they gather in Las Vegas to practice the arcane arts of drinking, socializing, debugging, and crowd control. Without these core Goonstm, DEF CON would not happen. It is due to their hard work and innate ability to survive on caffeine that allows the attendees to enjoy the con in a state of bliss.

Hackers.com

<http://www.hackers.com>

This is run by a group of hackers, whose intents are to clear the name of these explorers of the web. Good inside source of security tips and more.

Hacker News Network

<http://www.hackernews.com/>

The Hacker News Network's mission is twofold. Their prime mission is to deliver the real news from the computer underground for the computer underground. The reporting will not be dumbed down to match the computer illiteracy of the average TV viewer.

Their second mission is to report the activities of the underground without the biases of the mainstream media.

L0pht.com

<http://www.l0pht.com/>

A group of hackers who got together and started working on projects together. One of the projects turned out to be L0pht.com. There are remnants of different groups that make up L0pht, such as RDT, cDc, RL, etc. Merge with a Security company

Rootkit.com

<http://www.rootkit.com/>

Crackers' site

Root Shell

<http://www.rootshell.com/beta/news.html>

Good web site with interesting information about various cracks, viruses, attacks etc...

Book and Magazine Resources

Computer Security Handbook Third Edition

More than twenty years ago the first edition of this book was published. Today it is referred to as the blue book of security. A must read for computer security specialists and analysts. This is a great source of procedure analysis, policies deployment, and security framework for any company. Recommended reading by Frederic V. Farcy of TNTmax, Inc.

The Lubrinco Group

<http://www.lubrinco.com>

The LUBRINCO Group deals with high-risk threats to individuals and organizations. Their primary focus is on three areas of specialty: [High-risk protective services](#); [Economic espionage investigations](#) / [counter-CI \(competitive intelligence\) consulting](#); and [International and domestic due diligence and financial investigations / strategic partner location](#).

LUBRINCO's clients range from private citizens to government agencies or large corporations. Because of their experience, you will get highly professional service in their areas of specialty. Perhaps even more important, you will also get personal service from their management.

Information Security Magazine

<http://www.infosecuritymag.com/>

Great source for Linux and NT security tips and prevention. Recommended reading by Frederic V. Farcy of TNTmax, Inc.

Hacking Exposed Book

<http://www.hackingexposed.com/>

Great series of books a must read for anyone in charge of security for a network.

Linux Firewall Second Edition

<http://www.newriders.com/>

A Detail book about Linux IPTABLES firewall.

Network Intrusion Detection an Analyst's Handbook

<http://www.newriders.com/>

Great book about Intrusion Detection a most critical part of security.

Hardware Vendors

CISCO

http://www.cisco.com/warp/public/779/largeent/learn/technologies/network_security.html

The Cisco white paper, Delivering End-to-End Security in Policy-Based Networks, explains end-to-end security policy management through the CiscoAssure policy networking initiative.

EESCOM - Electronic Engineering Systems, Inc

<http://www.eescom.com/>

Electronic Engineering Systems, Inc. T/A EES Computers, was founded in 1996 to develop and provide turnkey secure computer systems for the local military. Today, EES designs, develops, markets, and supports a family of PC computers and secure computer products for the military, business, and civilian sectors. These products focus on preventing data access by unauthorized insiders and outside unauthorized attempts or attacks by hackers. In March 24 1999, EES Inc. signed a Distributor Agreement with SAIC-AMSEC (Science Applications International Corporation), for promoting their products worldwide. All their secure computers are now listed on [SAIC-GSA IT](#) schedule.

Reference Resources

Acronym Finder

<http://www.acronymfinder.com/>

The Acronym Finder is a World Wide Web (WWW) searchable database of more than 128,000 common abbreviations and [acronyms](#) about computers, technology, telecommunications, and the military, including the [Department of Defense](#) (DoD), [Air Force](#), [Army](#), [Navy](#), [Marine Corps](#), [National Guard](#), and [Coast Guard](#) acronyms and abbreviations. The Acronym Finder is not a glossary of terms, web search engine, dictionary, or a thesaurus -- it is only designed to search for and expand acronyms and abbreviations.

PC Webopaedia

<http://www.pcwebopaedia.com/>

The only online dictionary and search engine you need for computer and Internet technology.

Tech Web TechEncyclopedia

<http://www.techweb.com/encyclopedia/>

Source for technology oriented search engine and encyclopedia.

CNET

<http://www.techweb.com/encyclopedia/>

CNET is one of the world's leading new-media companies. Since 1995, their award-winning web sites and television series have become the definitive source of information about computers, the Internet, and digital technologies.

The company's information center is designed to help you easily understand what CNET is and does. You'll find information ranging from "what's new" at CNET, to a complete resource for investors, or how to advertise on our network.

WHATIS

<http://whatis.com/>

whatis® is a knowledge exploration tool about information technology, especially about the Internet and computers. It contains over 2,000 individual encyclopedic definition/topics and a number of quick-reference pages. The topics contain about 12,000 hyper-linked cross-references between definition-topics and other sites for further information.

Internet Traffic Report

<http://www.internettrafficreport.com/>

The Internet Traffic Report monitors the flow of data around the world. It then displays a value between zero and 100. Higher values indicate faster and more reliable connections.

TNTmax Security Glossary of Terms

This is an on going glossary of terms indented to be refined with every revision of this white paper. Feel free to communicate to me your suggestions for additions to this document at ffarcy@TNTmax.com

A

Argus

Argus is a network-monitoring tool that uses a client-server model to capture data and associate it into "transactions." The tool provides network-level auditing; it can verify compliance to a router configuration file, and information can be easily adapted to protocol analysis, intrusion detections, and other security needs. Argus is available from many sites, including

<ftp://ftp.net.cmu.edu/pub/old/argus-1.5/>

B

Bomb

A general synonym for crash, normally of software or operating system failures

BUG

One day in the 1940s, Harvard's famed Mark II, the precursor to today's computers, failed. When the problem was investigated, Grace Hopper and her colleagues found that a moth had lodged itself in the circuits, causing the machine to malfunction. The moth was removed with a pair of tweezers (and later was preserved at the Naval Museum in Dahlgren, along with Homer's logs). Apparently, on discovering the moth, Hopper exclaimed, "There is a bug in the computer". From then on, whenever there was a problem with the computer, scientist said they were looking for bugs. Even today, any software mistake is called a BUG.

C

COPS (Computer Oracle and Password System)

COPS is a publicly available collection of programs that attempts to identify security problems in a UNIX system. COPS does not attempt to correct any discrepancies found; it simply produces a report of its findings. COPS is available from <ftp://info.cert.org/pub/tools/cops/> and by uucp from uunet.uu.net.

Crack

D

DDoS or DoS

Distributed Denial of Service Attack is flooding attacks. Tribe and Trinoo are examples of so-called denial-of-service attacks, a method that's been around as long as there have been networks to inundate. Launching attacks from several computers too has been tried before, for example, with the "[Smurf](#)" attacks of last year.

"But Tribe and Trinoo give a new level of control to the attacker, and they are being improved," Dittrich said. Moreover, because the origin of the program is obscure, it's hard to counteract, said Quinn Peyton of the [Computer Emergency Response Team](#) (CERT) at Carnegie Mellon University.

"There are machines now sitting there, prepared to attack somebody else," Peyton said.

"Now one person can do a massive denial-of-service."

CERT warns that the Trinoo and Tribe attack tools "appear to be undergoing active development, testing and deployment on the Internet."

Tribe Flood Network and Trinoo launch their attacks from a host of innocent computers that already have been broken into. Then, on a signal from a master computer, the computers simultaneously bombard the victim machine with packets of information so fast that it becomes unresponsive. At that point, the target computer will not respond to commands and can't be taken off the network.

Encryption Protocol:

DES and 3DES

The Data Encryption Standard (DES) uses 56-bit symmetric keys to encrypt data in 64-bit blocks. The 56-bit key provides 72,057,594,037,927,900 possible combinations. This sounds impressive, and it would take up to 20 years for typical business computers to run this many combinations. But, more focused, well-funded hacker organizations with a bigger inventory of powerful computers could break it in about 12 seconds. DES has been developed even further with its 3DES ("triple-DES") system that encrypts information multiple times. For example, with 3DES, the data is encrypted once using a 56-bit key. The resulting cipher-text is then decrypted using a second 56-bit key. This results in clear-text that doesn't look anything like what was originally encrypted. Finally, the data is re-encrypted using a third 56-bit key. This technique of encrypting, decrypting, and encrypting (EDE) increases the key length from 56 bits to 168 bits.

E

Encryption

It is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to *decrypt* it. Unencrypted data is called *plain text*; encrypted data is referred to as *cipher text*.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption.

F**Firewall**

A system or combination of systems that enforces a boundary between two or more networks. Gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with many modems and public network ports on it, but just one carefully watched connection back to the rest of the cluster. [maxGUARD]

H**Hacker**

A slang term for a computer enthusiast. Among professional programmers, the term *hacker* implies an amateur or a programmer who lacks formal training. Depending on how it used, the term can be either complimentary or derogatory, although it is developing in an increasingly derogatory connotation. The pejorative sense of *hacker* is becoming more prominent largely because the popular press has co-opted the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker.

I**IDIOT**

Intrusion Detection In Our Time. A system that detects intrusions using pattern-matching.

IDS (Intrusion Detection System)

An intrusion detection system (**IDS**) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system. Example SNORT.

ISS (Internet Security Scanner)

ISS is a program that will interrogate all computers within a specified IP address range, determining the security posture of each with respect to several common system vulnerabilities. ISS is available from many sites, including <ftp://info.cert.org/pub/tools/iss/>
For further information about ISS, see:

ftp://info.cert.org/pub/cert_advisories/CA-93:14.Internet.Security.Scanner

J**JOHN the RIPPER**

John the ripper also call "john" for short is a dictionary-only cracker written by Solar Designer and available at <http://www.false.com/security/john>. It is a command line tool available for many operating system platform including Linux, windows, etc... It is very fast and can crack several different encryption algorithms. John cracks LanMan only and provide case insensitive passwords guess which is a problem in mixed case sensitive password.

K**Key**

A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt.

L**LeapFrog Attack**

Use of userid and password information obtained illicitly from one host to compromise another host. The act of TELNETing through one or more hosts in order to preclude a trace (a standard cracker procedure).

M**MD5**

MD5 is a cryptographic checksum program. MD5 takes as an input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. It is thought to be computationally infeasible to produce two messages having the same message digest or to produce any message having a given pre-specified target message digest. MD5 is found in RFC 1321. See <ftp://info.cert.org/pub/tools/md5/>

mail.local

Some versions of /bin/mail based on BSD 4.3 UNIX are vulnerable, because of timing windows in the way /bin/mail uses publicly writable directories. If you cannot install a patch from your vendor, replace /bin/mail with mail.local. Beginning with sendmail version 8.7.1, mail.local is included in the sendmail distribution, in the subdirectory mail.local. The program is also available from many sites, including <ftp://info.cert.org/pub/tools/mail.local/>. For further information about mail.local, see ftp://info.cert.org/pub/cert_advisories/CA-95:02.binmail.vulnerabilities

N**Nak Attack**

Negative Acknowledgment - A penetration technique, which capitalizes on a potential weakness in an operating system that does not handle asynchronous, interrupts properly. Thus, it leaves the system in an unprotected state during such interruptions.

National Information Infrastructure (NII)

The nation-wide interconnection of communication networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The NII encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tapes, cable, wire, satellites, fiber-optic transmission lines, networks of all types, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component of the NII. (Pending approval in JP 1-02)

NetSaint – (new name Nagios)

NetSaint is a program that will monitor hosts and services on your network. It has the ability to email or page you when a problem arises and when it gets resolved. NetSaint is written in C and is designed to run under [Linux](#), although it should work under most other *NIX variants. It can run either as a normal process or as a daemon, intermittently running checks on various services that you specify. The actual service checks are performed by external "plugins" which return service information to NetSaint. Several CGI programs are included with NetSaint in order to allow you to view the current service status, history, etc. via a web browser.

<http://www.netsaint.org/>

Ntop

ntop is a network traffic probe that shows the network usage, similar to what the popular top Unix command does. ntop is based on [libpcap](#) and it has been written in a portable way in order to virtually run on every Unix platform and on [Win32](#) as well.

<http://ntop.org/>

O

Open Security

Environment that does not provide an environment with sufficient assurance that applications and equipment are protected against the introduction of malicious logic prior to or during the operation of a system.

P

Phreaking

Closely related to hacking, using a computer or other device to trick a phone system. Typically, phreaking is used to make free calls or to have calls charged to a different account.

Q

Queso

Queso is a software tool used by hacker/cracker to determine the target operating system via and open port by default 80. Queso is not a port scanner and is use by hacker/cracker during the scanning and enumeration phase.

R

Retro-Virus

A retrovirus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.

S

SATAN (Security Administrator Tool for Analyzing Networks)

SATAN is a testing and reporting tool that collects a variety of information about networked hosts. SATAN is available from many sites, including <ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.tar.Z> For further information about SATAN, see ftp://info.cert.org/pub/cert_advisories/CA-95:06.satan ftp://info.cert.org/pub/cert_advisories/CA-95:07a.REVISED.satan.vul

Shadow passwords

If your UNIX system has a shadow password capability, you should use it. Under a shadow password system, the /etc/passwd file does not have encrypted passwords in the password field. Instead, the encrypted passwords are held in a shadow file that is not world readable. Consult your system manuals to determine whether a shadow password capability is available on your system and to get details of how to set up and manage it.

Swatch

Swatch, the Simple WATCHer program, is an easily configurable log file filter/monitor. Swatch monitors log files and acts to filter out unwanted data and take one or more user-specified actions based on patterns in the log. Swatch is available from <ftp://ftp.stanford.edu/general/security-tools/swatch/>

SSH

Developed by SSH Communications Security Ltd., Secure [Shell](#) is a program to log into another computer over a [network](#), to execute commands in a [remote](#) machine, and to move files from one machine to another. It provides strong [authentication](#) and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when [encryption](#) is enabled. SSH is available for [Windows](#), [Unix](#), [Macintosh](#), and [OS/2](#), and it also works with [RSA authentication](#).

<http://www.openssh.com/>

<http://www.ssh.com/products/ssh/>

SNORT

Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plugin architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient. Snort has three primary uses. It can be used as a straight packet sniffer like tcpdump(1), a packet logger (useful for network traffic debugging, etc), or as a full blown network intrusion detection system. watch, the Simple WATCHer program, is an easily configurable log file filter/monitor. Swatch monitors log files and acts to filter out unwanted data and take one or more user-specified actions based on patterns in the log. Swatch is available from <http://www.snort.org/about.html>

T

TCP/IP wrapper program

The TCP/IP wrapper program provides additional network logging information and gives a system administrator the ability to deny or allow access from certain systems or domains to the host on which the program is installed. Installation of this software does not require any modification to existing network software. This program is available from ftp://info.cert.org/pub/tools/tcp_wrappers/

Tripwire

Tripwire checks file and directory integrity; it is a utility that compares a designated set of files and directories to information stored in a previously generated database. Any differences are flagged and logged, including added or deleted entries. When running against system files on a regular basis, Tripwire enables you to spot changes in critical system files and to immediately take appropriate damage control measures. Tripwire is available from many sites, including <ftp://info.cert.org/pub/tools/tripwire/>

U

UDP

User Datagram Protocol (UDP) is part of the TCP/IP protocols. The TCP/IP consists of 65,535 UDP Ports and 65,535 TCP Ports totaling 131,070 ports.

V

Virus

A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Most viruses can also replicate themselves. All computer viruses memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Since 1987, when a virus infected ARPANET, a large network used by the Defense Department and many universities, many anti-virus programs have become available. These programs periodically check your computer system for the best-known types of viruses. Some people can distinguish between general viruses and *worms*. A worm is a special type of virus that can replicate itself and use memory, but cannot attach itself to other programs.

VPN

virtual private network *n.* 1. A set of nodes on a public network such as the Internet that communicate among themselves using encryption technology so that their messages are as safe from being intercepted and understood by unauthorized users as if the nodes were connected by private lines. 2. A wide area network formed of permanent virtual circuits (PVCs) on another network, especially a network using technologies such as ATM or frame relay. See *also* ATM (definition 1), frame relay, PVC. *Acronym:* VPN.

<http://openvpn.sourceforge.net/>
<http://www.freeswan.org/>

W

Worm

Independent program that replicates from machine to machine across network connections, often-clogging networks and information systems as it spreads.

WiFi

Acronym used to describe Wireless Network 802.11b standard.

WEP

Wired Equivalent Privacy, encryption mechanism widely used in 802.11b WAP (Wireless Access Point) devices. Both WEP and WEP2 algorithm are flawed and are consider unsecure.

X

X.25

A popular standard for packet-switching networks. The X.25 standard was approved by the CCITT (now the ITU) in 1976. It defines layers 1, 2, and 3 in the OSI Reference Model.

Xenix

A version of UNIX developed by Microsoft for the x 86 platforms that was compatible to AT&T System V Definition.

Y

Y2K

Year 2000 acronym. Was used to describe the date problem found in legacy system that used on two digits to describe the year.

Z

Zombies

Zombies are used to describe a machine that has been compromised by a hacker and are used in DOS Denial of Service attack or DDOS Distributed Denial of Service Attacks (example Trinoo, TNF, Stacheldraht, Zombie Zapper).

A Zombie process in UNIX is used to describe a program/daemon that has not stopped properly and is still loaded into memory gobbling up resources.

ⁱ The American Heritage Dictionary of the English Language, Williams Morris, Editor Publish by Houghton Mifflin Company 1969-1981 page 1173

ⁱⁱ Webopedia is an online encyclopedia of technical terms and definitions. Webopedia can be found at webopedia.internet.com, the definition we used in this white paper was taken from the following web page of the webopedia online site on Feb 2000
<http://webopedia.internet.com/TERM/s/security.html>

ⁱⁱⁱ Computer Security Handbook, third edition, edited by Arthur E. Hutt, Seymour Bosworth, Douglas B. Hoyt, published by John Wiley & Sons, Inc. 1995, chapter 18 page one section 18.1 by M. E. Kabay.