Safe Computing in the Age of Ubiquitous Connectivity

Robert Gezelter, *Senior Member, IEEE*

***Abstract*—The emergence of ubiquitous broadband connectivity has transformed the computing landscape. Telecommuting is no longer limited to those whose work can be done from a fixed home office. Telecommuting has embraced the hundreds of thousands of workers whose day is spent in the field visiting clients and customers. The worker's umbilical to the office is a mobile device with a secure connection provisioned using a fluid, ad-hoc combination of customer accommodations, public Wi-Fi hot-spots, and cellular modems.**

Ubiquitous high-speed networking brings a new dimension to security and privacy for both parties. There is a need to provide privacy for the telecommuter, wherever they are, and a need for the host to accommodate communications. At the same time, the host must maintain the integrity of their internal network or systems.

The well-known Internet standards provide a foundation and a springboard for properly providing robust security in this fluid environment.

***Index Terms*—Wi-Fi, telecommuting, security, privacy**

I. Introduction

The emergence of ubiquitous high-speed connectivity has transformed the computing landscape. It has opened up expansive new vistas on telecommuting. Telecommuting was formerly focused on workers who worked from fixed home offices. Now, hundreds of thousands of individuals whose routine business needs require them to travel have become de-facto telecommuters. This revolution affects a wide spectrum of workers, from low-level field service representatives to globe-trotting senior managers. In the past, communications with people out of the office were extremely limited. Today, the electronic broadband umbilical is a vital part of business life. Insurance checks cannot be written, orders not taken, deliveries of vital components not expedited, and court documents not filed, without network communications. Coffee shops, copy centers, and hotel rooms have become ad-hoc temporary offices. It is common to visit a coffee shop with a Wi-Fi hotspot, and find every table occupied by laptop. Many, if not most of those are connected to internal networks using secure connections. The first leg of those vital connections through the Internet is the coffee shop Wi-Fi hot-spot.

In the past, internal information systems have been protected by physical barriers. Access to the network required presence within the company's physical security domain. The emergence of a mobile workforce enabled by readily available broadband-class connectivity has rendered that presumption invalid. This reality creates a double-edged set of hazards: hazards for the telecommuter and hazards for the host.

II. Trends in Information Access and Availabilitty

Not much more than a decade ago, the business reality was obsolete information. It took days or weeks for information to percolate from one part of an organization to another. Printouts were generated on a regular basis, but they were out of date long before the last page emerged from the printer. It was impossible to obtain up-to-date data about en-route shipments, balances, and inventories. Working with obsolete information was a fact of life.

Business endured this reality. The emergence of internal, online systems that provided employees with access to up-to-the-minute information on inventory, balances, and order status was a major breakthrough.

During the past 15 years, information availability and

Manuscript received March 13, 2007

This article is derived from a series of presentations to IEEE Computer Society chapters throughout North America, the majority of which were sponsored under the IEEE Computer Society's Distinguished Visitor Program for North America.

Support for the real-life exemplar of the utility was provided by ARC XVI Ft. Washington, Inc,. at its senior center, as part of its work with senior citizens, visiting professionals, and professional students under contracts from the New York City Department for the Aging; the New York State Office for the Aging, and other contracts.

R. Gezelter is in private practice with offices in Flushing, NY (phone: +1 (718) 463 1079; e-mail: gezelter@removethis.rlgsc.com; WWW: www: http://www.rlgsc.com).

timeliness has become a self-feeding cycle. In the public sphere, we no longer deal with a daily newspaper, or indeed even morning and afternoon newspapers. Now, up-to-the-minute information is available on TV (e.g., CNN) and via the World Wide Web from our choice of providers (e.g., cnn.com, nytimes.com).

The widespread adoption and availability of Internet technologies has made obtaining current information as simple as opening a web browser window [1]. No longer is it necessary to place a telephone call, write a letter, or purchase a newspaper. For the end-user, this step increased the timeliness and accuracy of the information. Simultaneously, information providers realized a dramatic drop in the costs associated with providing information to their customers. Put simply, the cost of providing information dropped by orders of magnitude. The relevant metric became “How many queries can a server answer per second?” not “How many minutes of staff time are required per query?” This change made information available in seconds; a far cry from minutes, hours, or days.

III. HIGH SPEED ACCESS HAS BECOME EXPECTED

There has been an explosion of broadband access in recent years. Not so long ago, companies with high-speed access to the Internet were the exception. Today, in large areas of North America it is the norm [2].

Only a few short years ago, it was common for home users and non-IT related businesses to use low-speed dialup modems to reach the Internet.

Today, broadband services have become ubiquitous, in cities and reaching into surprisingly remote areas far from major metropolitan areas.

This access explosion has occurred in several parallel streams. There has been a dramatic increase in businesses and homes that have Internet access via DSL, cable, and direct fiber technologies [2,3]. There has been an even faster growth in the availability of hot-spots providing access to the underlying Internet via local wireless connections using the IEEE 802.11 a/b/g protocol suite. Most recently, high speed data services are being offered over the various cellular networks.

Hot-spots have appeared all over the map. Some of these are supported by municipal funding (e.g., New York City’s Bryant Park), others are operated by public spirited individuals, others are provided as an accommodation by businesses for their customers, and still others are available on a pay-per-use or subscription basis (e.g., T-Mobile, or Boingo).

Many major airports are equipped with hot-spots for as a public convenience. Some are provided as a no charge accommodation for travelers (e.g., Pittsburgh), while others are part of for-profit networks (e.g., New York’s LaGuardia).

It is now increasingly common to see business travelers in their airline seats while an airliner is parked at the gate, happily tapping away on mobile computers, using cellular data services to access the Internet.

Hot-spots have appeared in all manner of businesses, car dealers, laundromats, Native American trading posts, restaurants, coffee shops, book stores, and copy centers.

Beginning in 2003, Verizon made use of their existing hard-wired telephone circuits to telephone booths to install hot-spots for their subscribers located in some metropolitan areas. [4]. This service was subsequently discontinued as part of the roll-out of the cellular-based data services.

In short, major parts of North America are, at least in a theory, awash in high speed connectivity. In the past, high-speed access was merely a dream. Now it is presumed to be available 24 hours a day, every day of the year.

IV. AN ISSUE OF TRUST

Whom you trust used to be a simple, straightforward question. In a social sense, trust is often spoken of as a binary proposition. Someone is either trusted or not. This may be desirable and often workable model in the context of a relationship (e.g., a long-term marriage), but it does not take into account the nuances of commerce or law.

Trust is not simply a personal or internal matter. Information is subject to a veritable web of obligations and responsibilities. Some obligations are legal, imposed by acts of Congress or other law making bodies. Other rules are imposed by various regulatory authorities. Beyond the government, there are obligations based on contracts with other individuals and organizations.

Traditionally, people have been given access to different areas within the organization based on an assessment of who they were and what information they needed to perform their work.

In the most stringent cases, in both the national security and commercial worlds, information was restricted to a room, and physical access to the room restricted by a combination of locks, identity checks and guards (who were, often, armed). It is not uncommon for such rooms to be, in all senses of the word, vaults.

V. DATA AND LIABILITY

The question of access and accountability for information is not purely of theoretical interest.

Organizations have responsibilities to protect and penalties associated with the inappropriate use or distribution of information. Negligence in controlling access to restricted information may expose the firm to substantial monetary risk.

Examples of these obligations are easily found.

- HIPAA [5]
- Personnel records
- Tax Returns
- Third party proprietary data, documents, and drawings

The damage resulting from accidental or deliberate breach of the responsibility is often irreparable. The information distribution capabilities of the Internet, together with the widespread use of search engine technologies (e.g., Google) make it all but impossible to recapture all copies of leaked information.

VI. Internet History

The protocols and architecture of the Internet and its predecessor, the ARPAnet, were designed to provide redundancy of routing, not security against misuse and abuse. At that time (1968), computers and data communications equipment were expensive and difficult to use. The original Internet consisted of a small number of computers at major universities, government laboratories, and government agencies [6].

The growing number of colleges on the network increased network traffic and applications tremendously. Electronic mail, file transfer, and other network operations became critical enabling technologies for academic research throughout the ARPAnet connected world. The 1995 advent of the World Wide Web only served to accelerate this trend exponentially.

The widespread availability of smaller computers, and inexpensive high-speed campus spanning local area networks made the use of gateways between the campus networks and the Internet backbone a necessity [7].

This need was demonstrated by the 1988 Morris Worm episode [8], which underscored the vulnerability of many Internet-connected systems to rogue programs [9]. An episode similar in effect, albeit caused by a design flaw in the network routing algorithms used by the IMPs comprising the actual ARPAnet, had previously occurred in 1981. In that case, a single dropped bit in one IMP caused a total network crash [10].

While the basic architectural specifications underlying the Internet were not designed with security as an emphasis, there are long accepted standards that provide a framework for constructing networks that enable privacy, security, and integrity without undermining the ease of use that has been the hallmark of the Internet's acceptance. The private intranet address spaces specification, RFC 1597 [11] and its successor, RFC 1981 [12] are important building blocks for such networks.

VII. Canonical Internet Security

Long before the advent of the World Wide Web, it was recognized that not all traffic on the Internet was legitimate [13]. The transformation of these gateways from uninterested proxies for indirectly connected machines to firewalls, gateways with policy and authentication mechanisms is unsurprising. Hardening the access of individual machines within a campus or corporate network is an exhausting task, and never ending. It also defuses accountability.

The canonical firewall architecture, with one or more firewalls creating a choke point for entry to or exit from the internal network was obvious (Fig.1). It was also straightforward to realize that in the context of protection, all systems are not, nor should they be, created equal.

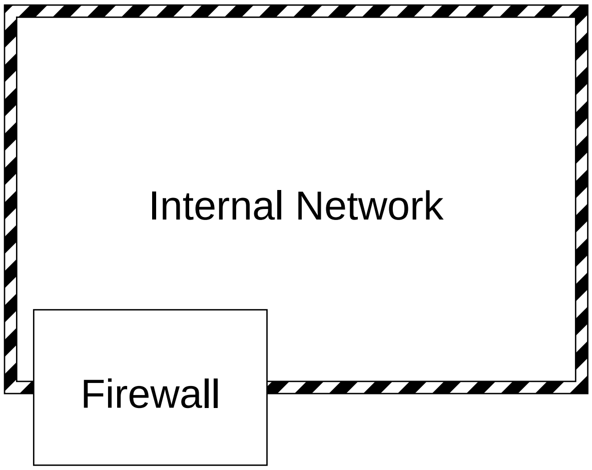

Fig 1. The Canonical Firewall architecture guarantees a conceptual monopoly on communications between systems located within the security perimeter and the outside world (reprinted from [19]).

It is clear that publicly accessible resources need to be protected from malicious traffic, but at the same time need to be accessible for their primary purpose. It is equallyclear that internal systems will have a different set of limitations.

Thus, the canonical DMZ configuration (Fig. 2) achieved its goals. WWW servers, FTP servers, DNS servers and others were placed behind an outer firewall, which protected against the most severe forms of malicious traffic. Internal corporate systems that were not intended to be publicly accessible were placed behind an inner firewall, which limited their access even more strictly.

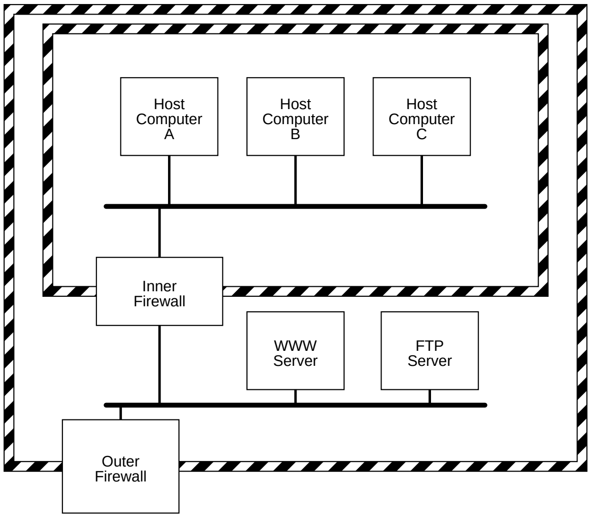

Fig. 2. A Demilitarized Zone (DMZ) allows WWW servers, FTP servers, and other publicly accessible resources to have a different set of access policies than the general internal network (reprinted from [19]).

VIII. The Threat Environment

Computer networks were originally protected by equipment in-availability and expense. The equipment to compromise the network was not easily or inexpensively available.

The first spam incident, on May 1, 1978, on the original ARPAnet is illustrative. A salesman for DIGITAL Equipment Corporation sent a piece of sales-related (non-technical, a violation of the “no commercialism” policy on network use) to a large number of users via electronic mail. The solution was simple. The program manager for the network simply contacted the relevant manager and told them “DO NOT do this again”. This is a naively quaint response for a far simpler time [14].

Today, the problem is far more complex. Simple solutions do not begin to address the problem. Today, the security problem has transformed by pervasiveness of technology. Today, the low-cost and easy access to technology has reduced the costs associated with an attack into the realm of the tens of dollars, increasing the problem by several orders of magnitude. Today, there are more computers on many desktops than there were in the 1969 ARPAnet [6]. The present Internet capacity of most companies today dwarfs what was available on the early ARPAnet backbone.

This mass enabling has transformed the threat environment. In the past, the costs and proficiency required to mount an attack severely limited the potentials for attack.

Today, the basic hardware required to mount an attack is available for a pittance in the corner store. Apple’s iPod is one of the most successful products of the last decade. An iPod contains all of the basic technology elements needed for a sniffing attack on a network. Such mobile devices are small, innocuous, and inexpensive.

The software technology for attacks has also benefited from the connectivity provided by the Internet. There are widespread reports of www sites in various parts of the world where malware may be constructed using a series of menus, with no underlying technical expertise required.

These developments put network attacks within the capability and budget of any individual or company with a motive. The motive may be commercial, criminal, or plain and simple revenge.

IX. Security for a Nuanced Community

Communities within organizations are complex. It has been well understood for many years that it is not possible to express the security requirements in an all or nothing way [15]. The use of multiple security identifiers and differing access rights to information has been a long standing requirement of security implementations.

It should come as no surprise that a simple red (untrusted)/black (trusted) dichotomy in network access does not satisfy the need to accurately express the nuances of all but the most simplistic security requirements.

It does not take an organization the size of a Fortune 10 to illustrate a need for multiple security zones with differing degrees of access (see Fig. 3).

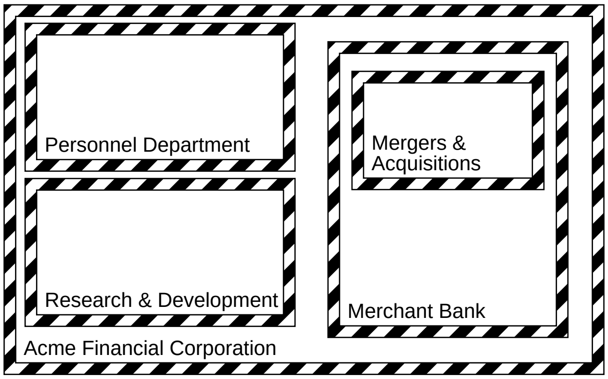

Fig. 3. Nested Domains with internal firewalls provide a basis for implementing different access and communications policies for different groups within the organization. These requirements may be externally required, internal, or some combination (reprinted from [19]).

The simplest example is a small retail establishment that wishes to provide a Wi-Fi hot-spot for its customers. The store also has an internal network to connect its cash registers to the server in the office, which in turn needs Internet access to perform its tasks.

It is clear that there are at least two levels of security required. Customers should not have access to the streams of transaction data flowing from the cash registers to the store computer. This transaction data streams can be expected to include account numbers and validation information for customer credit cards. Compromising one or more of these data streams could quickly lead to multiple cases of identity theft. Most merchant agreements include provisions that require merchants to secure data streams that include this information.

This same scenario may be affected by legal requirements. New York's Westchester County is acknowledged to have the first law requiring merchants to take basic security measures to protect customer personal data [16]. These precautions are basic, and do not require expensive steps to achieve compliance [17].

X. Case Study – A Senior center

Founded in 1973, ARC XVI Ft. Washington, Inc. operates a senior citizens' center in New York City's Washington Heights neighborhood. Each weekday, over 150 seniors visit the center to share lunch, take classes, attend lectures, and socialize. The center also has a staff of social workers to assist seniors with access to programs and navigating the bureaucracy.

In addition to its direct efforts on behalf of seniors, ARC XVI also has extensive relationships with major hospitals including New York-Presbyterian Hospital and Columbia University Medical Center, its medical and dental schools, and other colleges that have programs for students focused on areas that serve the elderly. It is common for students from Yeshiva University's Wurzweiler School of Social Work, as well as undergraduate social work students from City University's Lehman College to do fieldwork or internships at the center.

In addition to staff computers used for administrative work, there are also computers for personal use by seniors. These are used for web browsing, electronic mail, and instant messaging.

Students and their supervising faculty members often arrive at the center toting notebook computers, and need Internet access, or access to external systems via the Internet, to accomplish their projects..

It goes without saying that these different constituencies have differing security and confidentiality requirements:

- The center requires that its network be secure to protect its client and internal administrative systems
- The students and faculty advisors require access to the Internet and, in some cases external private systems to accomplish their projects
- The members of the senior center need to be able to use the classroom computers without impacting the staff administrative network

To date, personal notebook computers belonging to seniors have not been an issue, but this could change in the future. When that case arises, a more public accommodation for wireless access (a "public Wi-Fi hot-spot") may become necessary.

Each of these communities (e.g., members, staff, and students) needs network access. That they must share a connection for economic and infrastructure reasons goes without saying.

The solution is to implement the methodology described in the previous section.

The most secure configuration would be to isolate each of the communities in a separate security domain, within a common network security domain which is in turn connected to the high-speed Internet connection (Fig. 4).

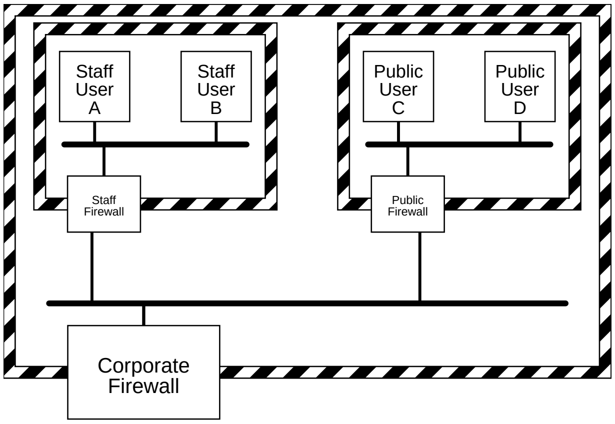

Fig. 4. Separate public and administrative networks, each protected by their respective firewalls can share a common Internet connection. This provides the same structure as that provided by an ISP with a LAN-type service.

A first step in enabling access and providing the necessary security precautions was implemented quite simply with off-the-shelf networking hardware. A small office wireless gateway provided the infrastructure for wireless access for roaming systems. The outside of the wireless access zone was within the administrative network.

Thus, while the wireless users could see the Internet, and connect to systems on the Internet, they could not communicate directly with the systems on the administrative network.

Similarly, the computers used by seniors for personal use were isolated in their own sub-network, behind a small office gateway. This gateway separated their network segment from the administrative systems in the same manner as the wireless router. The personal systems can reach the Internet, but network traffic from their network segment can only access the Internet, not the administrative network (Fig. 5).

The administrative network is protected from being addressed from either of the two lower-security (less trusted) networks. Traffic transits the administrative network en-route to the shared Internet connection.

XI. Summary

This structured approach to the logical topology of the network provides high-speed access to each community while maintaining the privacy concerns of each of the constituent communities and the security concerns of the local site for its internal systems.

This approach, by leveraging standard Internet technologies including private IP addresses, firewalls, and virtual private networks, allows a company to enable high-speed access for visitors and different groups within the organization, without compromising requirements for privacy of each of the groups, while providing transparent access to a common high-speed Internet connection.

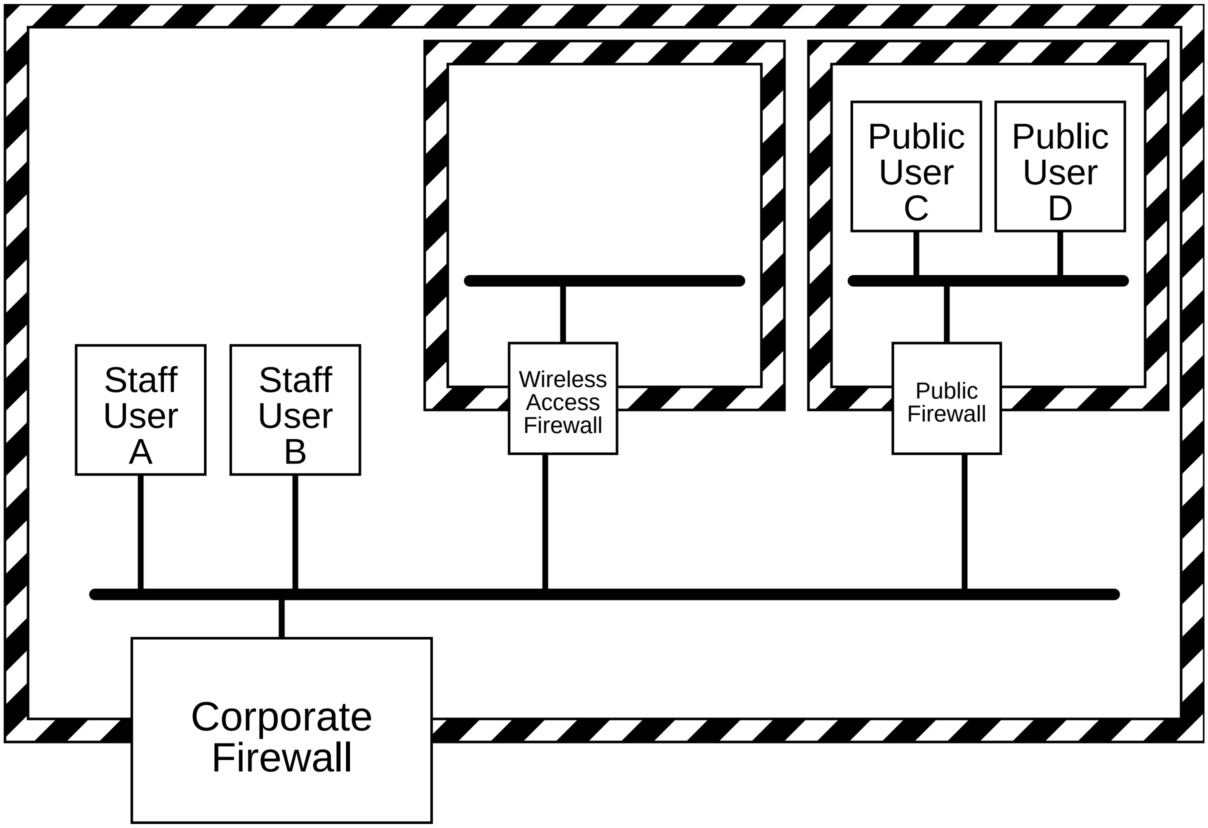

Fig. 5. The actual implementation of the network at ARC XVI Ft. Washington allows the public Internet traffic to traverse the administrative network. This is acceptable since all of the public traffic is limited to an internal RFC 1918 Intranet, that cannot address any of the systems on the administrative network. The traffic is forwarded from the public firewall or Wi-Fi Firewall to the main firewall.

Acknowledgment

I thank Ms. Fern Hertzberg, the Executive Director of ARC XVI Ft. Washington, and the staff and members of the ARC XVI Ft. Washington Senior Center for permitting the use of their organization as an exemplar of providing electronic hospitality, including Internet connectivity, to a diverse community with differing needs and obligations without endangering the security of the organizational network as a whole.

References

[1] R Gezelter, “Plain Talk that Management Needs to Hear from their Technical Support Staff”, Commerce in Cyberspace, February 6, 1996, The Conference Board; retrieved from http://www.rlgsc.com/tcb/plaintalk.html on March 11, 2007

[2] “Home Connectivity in the US”; retrieved from http://www.websiteoptimization.com/bw/0701 on March 6, 2007.

[3] J. Horrigan, “55% of Adult Internet Users have Broadband at Home or Work”, Pew Internet & American Life Project, April 2004, retrieved from http://www.pewtrusts.com/pdf/pew_internet_broadband_0404.pdf on March 11, 2007

[4] D. Jones, “Verizon: WLAN: Phone Home”, Unstrung, May 13, 2003, retrieved from http://www.unstrung.com/document.asp?doc_id=33682 on March 6, 2007

[5] Health Insurance Portability and Accountability Act of 1996, Public Law 104-191

[6] J. Reynolds, J. Postel, "RFC 1000 -- The Request for Comments Reference Guide", retrieved from http://www.ietf.org/rfc/rfc1000.txt on March 11, 2007

[7] J. Postel "RFC 760 – DOD Standard Internet Protocol", January 1980, retrieved from http://www.ietf.org/rfc/rfc760.txt on March 11, 2007

[8] E. Spafford, "The Internet Worm Program: An Analysis", Department of Computer Sciences, Purdue University, West Lafayette, Indiana, CSD-TR-823, November 1988, http://homes.cerias.purdue.edu/~spaf/tech-reps/823.pdf on March 11, 2007

[9] J. Reynolds, "RFC 1135 The Helmintiasis of the Internet, December 1989"; retrieved from http://www.ietf.org/rfc/rfc1135.txt on March 6, 2007

[10] E. Rosen "Vulnerabilities of Network Control Protocols: An Example", *ACM Software Engineering Notes*, Volume 6, Number 1, pp 6 – 8, January 1981

[11] Y. Reckhter, B. Moskowitz, D. Karrenberg, GJ deGroot, "RFC 1597 – Address Allocation for Private Internets", retrieved from http://www.ietf.org/rfc/rfc1597.txt on March 11, 2007

[12] Y. Reckhter, B. Moskowitz, D. Karrenberg, GJ deGroot, E. Lear, "RFC 1918 – Address Allocation for Private Intranets", retrieved from http://www.ietf.org/rfc/rfc1918.txt on March 11, 2007

[13] S. Bellovin, "There Be Dragons", Proceedings of the Third USENIX Security Symposium, Baltimore, Maryland, September 1992

[14] M. Doehrman "Colorado Springs Businessman Gary Thurek was the first to send spam e—mail", The Colorado Springs Business Journal, February 10, 2006; retrieved from http://www.allbusiness.com/north-america/united-states-colorado/1105241-1.html on March 11, 2007

[15] R. Gezelter, "Internet Security", Chapter 23 in *Computer Security Handbook, 3rd Edition,* A. Hutt, S. Bosworth, and D. Hoyt (Eds.) New York, John Wiley & Sons, 1995, pp 23-1 – 23-25

[16] Local Law 4-2006, Westchester County, State of New York

[17] R. Gezelter, *Wireless Security: What Every Business Must Know*, presented on October 6, 2006, County Center, White Plains, New York. Slides available from http://www.rlgsc.com/westchester/2006-10/wirelesssecurity.html

[18] E. Lear, E. Fair, D. Crocker, T. Kessler "RFC 1627 -- Network 10 Considered Harmful (Some Practices Shouldn't be Codified", July 1994, retrieved from http://www.ietf.org/rfc/rfc/1627.txt on March 11, 2007

[19] Ibid, "Internet Dial-Tones and Firewalls: One Policy Does Not Fit All", IEEE Computer Society, Charleston, South Carolina chapter, June 10, 2003. Slides available from http://www.rlgsc.com/ieee/charleston/2003-6/internetdial.html

[20] Ibid, "Safe Computing in the Age of Ubiquitous Connectivity", IEEE Computer Society Distinguished Visitor lecture on April 1, 2005, Slides available from http://www.rlgsc.com/ieee/Binghamton/2005-04/ubiquitous.html

[21] Ibid, "Protecting Internet Visible Assets" Chapter 21 in *Computer Security Handbook, 4th Edition,* S. Bosworth, M. Kabay (Eds.), New York, John Wiley & Sons, 2002

[22] Ibid, "Protecting WWW Sites", Chapter 22

[23] E. Alderman, C. Kennedy *The Right to Privacy* Alfred Knopf, New York, 1995

[24] C. Stoll, *The Cuckoo's Egg,* Bantam Doubleday Dell Publishing Group, 1989

[25] W. Cheswick, S. Bellovin *Firewalls and Internet Security: Repelling The Wily Hacker, 1st Edition* Addison Wesley, New York 1994

[26] R. Gezelter "Better Invisible than Agile: Applications of RFC 1597", Fall 1995 US DECUS Symposium, San Francisco, California, December 7, 1995. Slides available from http://www.rlgsc.com/decus/usf95/index.html

[27] A.Tannenbaum, *Computer Networks,* Prentice-Hall

Robert Gezelter (M'81–SM'2001) is a native New Yorker. He has made his home in Flushing since 1967. Mr. Gezelter holds BA (1981) and MS (1983) degrees from New York University in computer science.

He has been in private practice since he left the Courant Institute's research staff in 1982. He is a Contributing Editor for the *Computer Security Handbook, 4th Edition* (New York, New York, Wiley, 2003) and a contributor to the *Handbook of Information Security* (New York, New York, Wiley, 2005). He has written numerous articles in various publications and spoken throughout the United States and internationally. His work involves the design, implementation, and use of operating systems and their internals, networks, software architectures, and related matters.

Mr. Gezelter is also an active member of Encompass (formerly DECUS). In 2003, the IEEE Computer Society appointed him to its Distinguished Visitor Program for North America.