Communications of the Association for Information Systems

Volume 12 Paper

December 2003

# Defense Mechanisms of Biological Cells: A Framework for Network Security Thinking

Kenneth Knapp
*Auburn University*, knappkj@auburn.edu

Frank Morris
*Auburn University*, Morrij3@auburn.edu

R. Kelly Rainer Jr.
*Auburn University*, rainer@business.auburn.edu

Terry Anthony Byrd
*Auburn University*, tbyrd@business.auburn.edu



## Recommended Citation

Knapp, K., Morris, F., Rainer Jr., R., & Byrd, T. (2003). Defense Mechanisms of Biological Cells: A Framework for Network Security Thinking. Communications of the Association for Information Systems, 12, pp-pp. https://doi.org/10.17705/1CAIS.01247

Communications of the Association for Information Systems

# DEFENSE MECHANISMS OF BIOLOGICAL CELLS: A FRAMEWORK FOR NETWORK SECURITY THINKING

Kenneth Knapp
Frank Morris
R. Kelly Rainer, Jr.
Terry Anthony Byrd
*College of Business*
*Auburn University*
rainer@business.auburn.edu

**ABSTRACT**

Computer and network security are central issues confronting organizations and individuals. This paper explores the use of biology as a reference discipline that can provide meaningful insight and innovation in the area of network security. Specifically, we propose a framework for thinking about network security by examining the similarities between the defense mechanisms of a cell, and the security processes and methodologies of networked computer systems that defend an organization's information resources. Researchers and commercial developers can use this framework to help spark ideas that lead to further research and development in network security. The framework also provides a platform for educators in teaching students about the functions of computer network concepts. Our analysis of defense mechanisms in biological cells showed that security in cells is integrated, ubiquitous, and continuous. An example illustrates how the framework can generate ideas for improving network security.

**Keywords:** cell biology, information security, computer network systems, cellular defense mechanisms, security framework, security paradigm.

## I. INTRODUCTION

Computer and network security are central issues confronting organizations and individuals [Loch et al., 1992; Mehta and George, 2001; Zviran and Haga, 1999]. Network security is a challenge as organizations and individuals become more dependent on computers for information processing and exchange. As the number of computers in use continues to rise and network complexity continues to increase, maintaining secure systems is becoming an overwhelming task.

In modern business environments, networks are essential tools for survival. Typically, the more people who use a network, the more valuable the network becomes. Therefore, securing networks by keeping more people out may do more harm than good. At the same time, however, an increase in network users can result in an increase in security risk, especially because attack is easier than defense [Bruno, 2003].

An additional challenge exists as organizations connect business networks to the Internet. While connecting a network to the Internet greatly increases a company's connectivity, it also further increases the number of potential intruders from which the company must defend itself. The challenge is daunting. Security must protect the critical information of the business while allowing for open communication and commerce [Bruno, 2003].

Security experts indicate that many large companies do not realize how vulnerable they are [Economist, 2002; Straub, 1990]. Not unlike the castles of the Middle Ages that used walls and moats as their primary defense, many businesses today employ firewalls as a primary barrier defense and thus conclude that their networks are secure. However, with the advent of the cannon, castle defenders realized that they needed more defense than just their wall and moat. Likewise, businesses today realize that a barrier defense alone is no longer enough. Even the best defenses must adapt or be defeated by novel technologies and tactics [Bruno, 2003]. While no one is suggesting an end to firewalls, there is a need to develop more efficient ways of securing the network. Industry is moving out of the fortress model of information security to a more sophisticated early-detection system that spots symptoms. However, as security is heightened, accessibility and operational efficiency are often sacrificed. What is needed is a rethinking of how to allow users easier access to data without obstructing the efficient flow of information because of enhanced security [Bruno, 2003].

The purpose of this article is to explore the use of biology as a reference discipline that can provide meaningful insight and innovation in network security. More specifically, we propose a framework for thinking about network security by examining the similarities between the defense mechanisms of a cell (i.e. the defense of an organism), and the security processes and methodologies of networked computer systems that defend an organization's information resources. Such a framework and exploration can provide benefits, not only to the research community, but to a much broader community as well.

Researchers can use this model as a security framework that can help spark ideas and lead to further research on the subject of network security. In the area of education, cell biology provides an interesting analogy for teaching students about numerous areas of information system security. Commercial developers of computer security technologies can use this framework to gain insights, which may lead to the development of innovative new products and/or the improvement of existing products. Those responsible for implementing network security in organizations can use this model for thinking about ways to configure and deploy their networks and defenses to protect their IS resources better.

In Section II we first introduce the framework and then provide fundamental information about network defense mechanisms and cellular biology. Next, we present our framework and introduce relevant analogies for illustration and validation (Section III). Based on the analogies, we then offer five central themes for cellular defense followed by an example of using the framework. Finally, we discuss implications (Section IV) and provide our conclusions (Section V).

## II. THE FRAMEWORK

### USING BIOLOGY TO THINK ABOUT COMPUTING

Using biology as an analogy for computing is not new [ e.g., Kurzweil, 2000]. In general, such references are informal and use different facets of the biology of the human body as analogies for various computing technologies, systems, or networks (e.g. the computer virus, the Internet as the digital nervous system). We focus specifically on the area of the defense mechanisms of a cell (a subset of the domain of biology) as a framework for thinking more formally about methods for the defense of a computer network (a subset of the domain of computer technology).

Figure 1 illustrates some of the more significant cellular defense mechanisms and how they relate to network defense mechanisms.

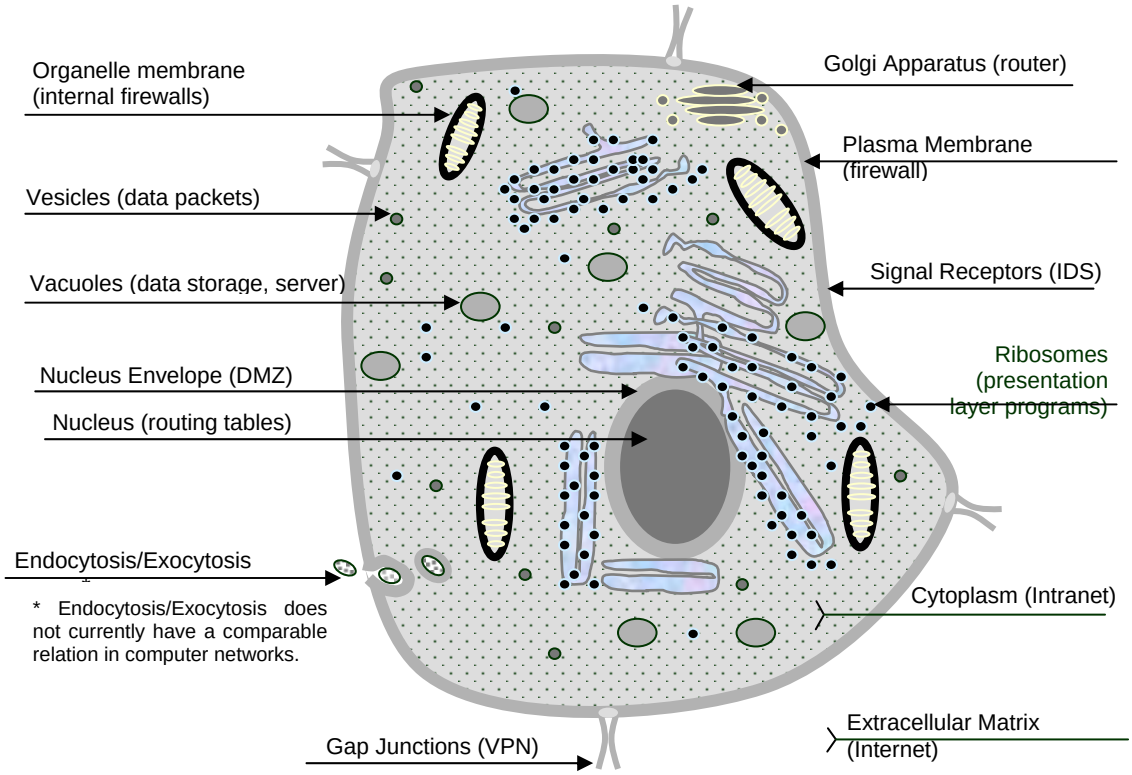


Figure 1: The Framework

The next two subsections provide basic information concerning computer networks and cell biology. These sections provide definitions and concepts that we use to draw analogies between cellular defenses and network defenses.

## COMPUTER NETWORKS: BACKGROUND AND BASICS

The electronic transmission of data across global networks is essential for 21st century commerce. Global network integration, the merging of local and wide area networks with the Internet, provides many business opportunities. However, increased global connectivity gives outsiders greater potential to access the internal network of organizations thus putting corporate information resources at greater risk to malicious destruction or manipulation [Stallings, 2001]. As a result, modern network architectures became more complex as they defend against attacks that originate from the public Internet. Over the past twenty years, defenses evolved into a complex configuration of firewalls, intrusion detection systems, and 'demilitarized zones' [Frolick, 2003]. Figure 2 illustrates a representative network architecture.

Some of the earliest defensive mechanisms were choke routers. These routers blocked certain addresses, ports, and protocols at the external point of presence of an organization's network. As the frequency of cyber attacks increased during the 1990s, these routers no longer provided the necessary protection needed to defend against attacks.

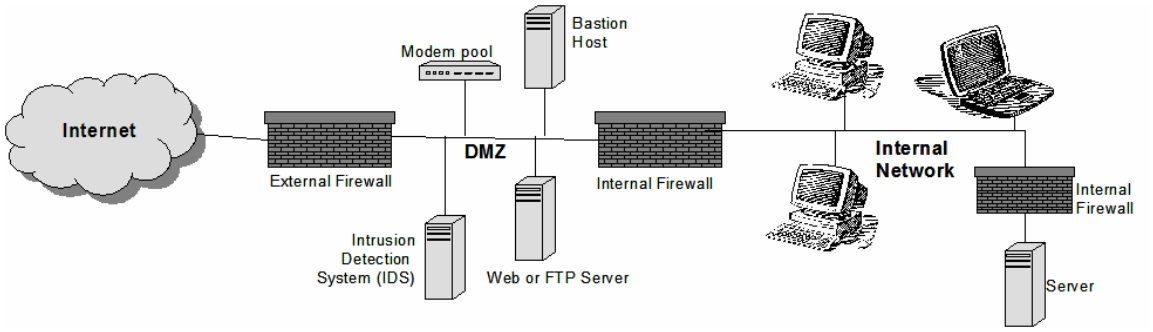


Figure 2: Representative Network Architecture

The implementation of firewalls as dedicated network devices addressed security more effectively. Firewalls advanced greatly and are now classified into several types, including:

- packet-filter firewalls, which inspect every data packet entering or leaving the network,
- application-level firewalls (often called bastion hosts), which apply security mechanisms to specific applications, and
- stateful-inspection firewalls, which 'remember' exiting data and allow or reject packets based on what the firewall anticipates [Carr and Snyder, 2003].

Other firewall varieties emerged including internal network firewalls and home or office personal firewalls.

Intrusion Detection Systems (IDSs) work with firewalls to detect and prevent suspect data traffic from entering an organization's network. Advanced IDSs contain sophisticated pattern analysis and rating systems to identify and flag suspicious and dangerous data patterns. Modem pools help organizations consolidate their network access points by centralizing modems, thus eliminating dangerous 'back doors' into the network. These modem pools and devices like Web or FTP servers can now be located in demilitarized zones (DMZs), a type of buffer zone between an organization's internal network and the public Internet. DMZs allow an organization's customers and suppliers access to important network-based information without them needing to penetrate the internal network.

Evolving non-perimeter defensive mechanisms include anti-virus software, encryption systems, and virtual private networks. For example, anti-virus software now automatically updates itself according to a central configuration. In addition, popular antivirus packages now perform heuristic scanning to help identify new viruses based on their resemblance to other known viruses. Security configurations for network devices such as servers are a top concern. Servers must maintain robust passwords, up-to-date security patches, and proper administrative settings to deliver necessary security. Secure sockets layer is an example of a communication mechanism with security built into its functionality. Other popular network communication services like virtual private networks create a secure tunnel between multiple organizations over insecure networks, typically the public Internet.

Information security threats will continue to provide challenges into the future. Organizations will pay increased attention to network architectures and defensive mechanisms to protect their information resources.

## CELL BIOLOGY: BACKGROUND AND BASICS

In 1858, Rudolf Virchow formulated Cell Theory. The basic premise of his theory is that the cell is the fundamental unit of function in all organisms. Corollaries to the theory state that the chemical composition of all cells is fundamentally alike; and, that all cells arise from preexisting cells through cell division [Farabee, 2003].

Cells are the smallest structural units of living matter capable of functioning independently. A single cell can be a complete organism in itself, such as a bacterium or yeast; or cells can work together to become the building blocks of large multicellular organisms as complex as the human being [Britannica, 2003].

### Basic Cell Structure

Cells are enclosed by the *plasma membrane*, which forms a selective barrier allowing nutrients to enter and waste products to leave[1]. The plasma membrane of the cell is the primary barrier between the cytoplasm and the extracellular environment [Friedman, 1986]. Channels called *gap junctions* allow the passage of molecules through the plasma membranes between pairs of cells [Britannica, 2003]. The *cytoplasm* is the material that fills the inside of a cell between the plasma membrane (cell membrane) and the membrane of the nucleus. The interior of the cell is organized into many specialized compartments, or *organelles*, each surrounded by a separate membrane. [Farabee, 2003].

The *nucleus,* the largest and most prominent organelle, is enclosed by the double-membrane nuclear envelope. The outer membrane of the nucleus is continuous with a system of membranes within the cytoplasm [Barrett et al., 1986]. The *nucleolus* is an area of the nucleus where ribosomes are constructed [Farabee, 2003]. *Ribosomes* provide sites for protein synthesis and are not membrane bound.

Another group of organelles, the *mitochondria,* are bounded by a double membrane that folds to form inward projections. The *golgi apparatus (or golgi complex)* is an organelle in the cytoplasm that packages newly synthesized proteins and carbohydrates into membrane-bound vesicles for transport to their final destination inside or outside of the cell [Barrett et al., 1986]. *Vesicles* are small membrane-bound spaces in most cells that transport macromolecules into and out of the cell and carry materials between organelles in the cell. Much larger than vesicles are the *vacuoles*. Vacuoles are membrane-bound fluid-filled spaces in cells that remove waste products and store ingested food [Farabee, 2003].

In this section we briefly described fundamental network and cellular terms and functions that can serve as a useful reference for the remainder of this paper. In the next section, we discuss five categories of analogies that provide examples of the numerous similarities between computer network defenses and the defense mechanisms of a cell.

## III. FIVE CATEGORIES OF ANALOGIES

Table 1 lists computer network terminologies or actions in the center column, with the analogous cell biology terminology or action on the right side. The left side lists the functions common to both computer networks and cell biology. These analogous functions are grouped into five major categories that exhibit similarities.

### 1. BARRIER DEFENSE ANALOGY

During the 1990s, computer network architectures evolved to contain perimeter defenses designed to protect internal information resources. As these perimeter architectures increase in

[1] Plant cells also have a rigid cell wall in addition to a plasma membrane. For the purposes of this paper, however, we discuss cells in general without distinguishing between plant and animal cells.

complexity, they become more comparable to the cell's plasma membrane. First, the cell membrane acts as a barrier separating the cell's external and internal environments. Second, it acts as a filter allowing the entry of wanted elements while keeping out unwanted elements [Barrett et al., 1986]. In comparison, network perimeter architectures consist of external routers, intrusion detection systems and firewalls that together define the organization's "point of presence" demarking the internal network from the public Internet. Like cell membranes, firewalls also filter out unwanted data communications while permitting wanted data to enter. Furthermore, analogies concerning threats exist between firewalls and plasma membranes. Any transport channel that circumvents the plasma membrane endangers the cell [Friedman, 1986] just as an unauthorized modem or a faulty firewall logic rule can endanger an entire organizational network.

Table 1: Framework for Network Security Thinking

| **Function** | **IT Infrastructure Term or Action** | **Cell Biology Term or Action** |
|---|---|---|
| Barrier Defense | Exterior Router<br>Packet Filter/Stateful Inspection Firewalls<br>Intrusion Detection Systems | Plasma Membrane / Plant cell wall<br>Oligosaccharins: "oxidative burst" |
| Barrier Transmission and Communication | Tunneling protocols<br>Secure Sockets Layer<br>Virtual Private Networks<br>Advanced Encryption Mechanisms<br>Network Ports | Variety of Membrane Channels<br>Gap Junctions<br>Facilitated Diffusion & Transporters (i.e. Glucose)<br>Extracellular matrix signaling |
| Internal Organization | Internal Firewalls;<br>Network DMZ (Buffer Zones) | Membrane-bound organelles, mitochondria<br>Nuclear pore complex, double membrane envelope |
| Internal Routing and Sorting | Email, standard mail<br>Fax, telephone<br>IPv6<br>Routers, routing Tables | Endocytosis, Exocytosis<br>Golgi Apparatus<br>Cell Nucleus |
| Virus Defense and Response | 1.Infection Carrier<br>2.System Cleansing (anti-virus s/w)<br>3.System Isolation<br>4.System Corruption | 1.Infection Carrier<br>2.Intracelluar digestion, endocytosis<br>3.Cell Division<br>4.Cell Death |

In general, cell membranes provide three main functions:

1. mechanical protection and a chemically buffered environment,
2. a porous medium for the distribution of water and other small molecules, and
3. a storage site of regulatory molecules that sense the presence of pathogenic microbes [Britannica, 2003].

These three cell functions are comparable to network perimeter functionality. Computer network devices such as firewalls and intrusion detection systems provide:

1. electronic protection through a buffered environment,
2. a "porous" medium for the distribution of packets, and
3. a regulatory listing to detect the presence of electronic intrusions.

### The Role of Oligosaccharins

One of the more versatile cell defense mechanisms involves oligosaccharins. Among its multiple roles, oligosaccharins provide a signaling function that can develop when a pathogen attacks a cell triggering an "oxidative burst" near the cell membrane. This burst produces hydrogen peroxide, superoxide, and other active oxygen types that directly attack a pathogen and can trigger a hardening of the cell membrane. In addition, oligosaccharins stimulate the production of other chemicals released outside the cell to help digest the pathogen's wall [Saupe, 2002] in a type of cellular counterattack.

A desired quality of computer network architectures is to provide an active, coordinated defense against attacks of an adversary rather than a passive, reactive one [Tiboni, 2002]. The multiple roles of oligosaccharins serve as an interesting example of what cells do to provide an 'active defense.' For example, compared to computer networks, the hardening of the cell membrane upon detection of a threat is comparable to switching a firewall's logical rulebase to a more secure configuration upon detection of certain predetermined threat conditions, thus making the firewall more difficult to penetrate.

## 2. BARRIER TRANSMISSION AND COMMUNICATION ANALOGY

Today, concerns such as privacy and computer crime mandate that electronic communication between organizations must be secure. To meet this need, numerous secure communication services such as virtual private networks, secure sockets layer, tunneling protocols, advanced encryption techniques, and others have emerged. Similarly, a rich variety of specialized communication mechanisms in cells incorporate security concerns. In this subsection, we address four such cellular mechanisms: channels, tunnels, transporters, and signaling in the extracellular matrix.

### Membrane Channels

Computer firewalls and routers manage electronic communications by opening and closing thousands of ports that allow or block the various types of communication flows across a network. At the biological level, a similar structure exists. Cells can communicate via electrical current flowing across the cell's membrane. This current appears as bursts traveling through open channels, or holes, formed by proteins intrinsic to the membrane. If no hole is open, no significant current flows. These channel openings can occur spontaneously. Channels can also be opened by signals sent from substances such as calcium wanting to enter the cell or from changes in electrical potential across the membrane. Like some network firewalls that can restrict the passage of certain protocols or packets through certain ports, cell membrane channels permit passage of limited substances while other channels pass only ions with a particular positive or negative charge.

### Gap Junctions

Similar to virtual private networks that provide interorganizational communications using protocols such as point-to-point tunneling, some cells contain tunnels called gap junctions that allow passage of small molecules between cells [Encyclopedia, 2003]. Gap junctions offer similar functionality to virtual private networks in organizations in that they provide a tunnel that enables protected communications between organisms or organizations.

### Facilitated Diffusion

Contrasted with channels, facilitated diffusion is a transporter mechanism in which molecules create binding sites on one side of the membrane that allow molecules to bind to the membrane through chemical attraction. The binding site is highly specific, often fitting the atomic structure of only one type of molecule. When the molecule has attached to the binding site, the transporter, in a process not fully understood, brings the molecule through the membrane and releases it on the

other side [Britannica, 2003]. This mechanism allows desired molecules to diffuse the cell's barrier without creating unnecessary and insecure holes.

In a process similar to facilitated diffusion in cell membranes, computer and network firewalls allow desired elements to pass while blocking unwanted elements by eliminating possible entry channels. Firewalls, however, do not yet provide the same degree of facilitated diffusion as cells. Packet-filter firewalls, for instance, look at each packet entering and leaving the network based on predefined user rules, but often leave open holes or ports allowing potentially dangerous communications to pass through the firewall [Carr and Snyder, 2003]. Stateful inspection firewalls more closely accomplish a "facilitated diffusion" by monitoring active connections over time and recording information such as IP address and port numbers of all outgoing packets that request return packets from an external information system. Open ports remain so only if requested by an outgoing packet [TechTarget, 2003] thus reducing the opportunity of passing dangerous packets into the organization's network.

### The Glucose Transporter

Numerous specialized 'facilitated diffusion' transporters in cells help certain types of molecules cross the cell membrane. Some of the major types of membrane transporters include active, passive, primary-active, secondary-active, bulk, anion, sugar, and the glucose transporter. Since each transporter varies in how it passes molecules across the membrane, we will limit our discussion to one specific example, the glucose transporter.

Unlike most membrane channels, the glucose transporter does not select molecules to transport by size. Instead, this transporter makes a conformational change and "flips" the glucose from one side of the membrane to the other. This flipping occurs at a rate of 1,000 molecules per second compared to the 1,000,000 ions per second rate of most channels. The movement of glucose across the membrane ceases once equilibrium is reached [Encyclopedia, 2003]. This conformational change and flipping of molecules provides an example for computer networks in that the transporter appears highly secure leaving no open holes in the membrane.

While firewalls do provide a level of security in computer and network systems and serve a function similar to the cell's outer membrane, the degree of specialization in cells appears far more advanced and inherently more secure. As mentioned, the glucose transporter is just one of many specialized cellular membrane transport mechanisms. The method that molecules use to cross the membrane depends on factors such as molecule size, substance, and cell need (i.e. glucose equilibrium). Other details remain a topic of research for cell biologists as knowledge of cell membranes continues to grow [Doms and Trono, 2000]. Therefore, when considering the multiple ways that elements cross the cell membrane, it becomes clear that cells contain a large repertoire of highly secure communication mechanisms that is more specialized than the communication mechanisms in computer network firewalls.

### Cell-to-Cell Communications via the Extracellular Matrix

Modern electronic communications between organizations uses terms that are similar to those used in cellular biology. Terms like cyberspace, extranet, and matrix computing are part of the information technology lexicon. In multi-cell organisms, communications that occur outside the cell do so in extracellular space, which consists of a gel material known as the extracellular matrix. The gel is composed of complex sugar molecules in a water-based solution filled with salts, proteins, other nutrients, and waste products. Molecules called receptors that are associated with the cell's membrane provide the links from the cell to the extracellular matrix. These receptors interact with protein fibers that influence cell behaviors often leading to changes in cell shape, movement, and development. A cell can secrete or expel molecules through its membrane to transverse the extracellular space to another cell's receptor. In addition to using receptors, cell behavior can be impacted by the passing of chemical or electrical signals across

extracellular space using communication mechanisms such as the gap junctions, discussed previously.

In computer networks, intrusion detection systems (IDS) attempt to identify intrusions by flagging suspicious communications. An IDS is typically configured as a reactive system [Sequeira, 2003] often identifying dangerous communications too late. Cells, however, take a proactive approach to intrusion detection by deploying an array of different receptors that respond to extracellular signals in what may be called a signal detection system. Once detected by an associated receptor, an "approved" chemical signal triggers an event that changes a cell's behavior. Depending on the type of cell with which it is communicating, a particular chemical signal can cause different cellular reactions. In one example, a receptor will trigger the opening of a membrane channel allowing a flow of ions into the cell which can impact the electrical properties of the cell's membrane or cytoplasm [Britannica, 2003].

Although complex, we can divide communication between cells into four basic steps:

1. A cell sends a signal to another cell.

2. A cell receives the signal.

3. The cell analyzes the request and "decides" to deny or allow the element to cross the membrane.

4. If allowed, the cell changes its behavior, such as opening a channel in its membrane to allow the specified molecule to pass into the cell.

Computer network defense mechanisms work in similar ways.

1. A requestor sends a message asking for an opening in the firewall.

2. The organization receives the communication.

3. A network administrator analyzes the request and decides to deny or allow the communication to pass.

4. If allowed, the administrator takes some action such as writing a rule to the firewall stating the time interlude, source internet address, and required protocol of the expected communication.

Once opened, packets flow through the firewall port to the destination computer system. Here, cellular communications in organisms share a similar model to electronic communications in organizations.

## 3. INTERNAL ORGANIZATION ANALOGY

In recent years, various types of network appliances from routers to operating systems started integrating firewall functionality into their services. In addition to these hybrid firewall devices, dedicated firewalls internal to the network are appearing, especially in organizations with large networks. These internal firewalls can segment functional departments electronically within an organization or provide dedicated protection for high-value information systems or subnets. Internal firewalls not only provide an additional layer of protection from external intruders, but also protect information resources from internal threats. Similarly, cells are compartmentalized into organelles. Each organelle has something of an internal firewall, an internal membrane structure with a distinct composition of proteins and lipids enabling a membrane to carry out its unique function. Like the external plasma membrane, internal organelle membranes contain transport proteins that facilitate chemical communication between organelles.

The most prominent organelle, the nucleus, is a highly protected resource. A double-membrane envelope separated by a perinuclear space encloses the nucleus. The perinuclear space is like a

buffer zone or network DMZ, which forms nuclear pores through which the nucleus and cytoplasm communicate. Proteinaceous granules often guard these pores to help regulate the passage of small ions and macromolecules into the nucleus [Barrett et al., 1986]. Another organelle, the mitochondria, is responsible for the energy transactions necessary for cell survival. Like the nucleus, mitochondria also have a protective double membrane.

The lesson that cells teach is that security is a multi-layered process. While the plasma membrane provides the initial protection, the organelles provide their own protection with unique and specialized membranes. The more valuable the organelle is to the cell, the more robust its membrane seems to be.

Similarly, based on the increased use of hybrid and internal firewalls in organizational networks, it appears that network architectures are beginning to resemble the security architecture of cells. The concept of *defense in depth*, which stipulates that information security processes should penetrate much deeper into an organization than provided by perimeter defenses, is consistent with the multi-layered approach that cells take [Panko, 2004].

## 4. INTERNAL ROUTING AND SORTING ANALOGY

Just as organizations use numerous internal systems of communication, such as electronic mail and instant messaging, cells too use numerous internal delivery systems. One “full-service” system that facilitates cell transport and routing between organelles is endocytosis and exocytosis. In the process of endocytosis, cells—and some organelles—engulf material by forming an invagination, or inward depression, of their outer plasma membrane. The inward depression continues to bulge further into the cell’s cytoplasm until it finally pinches off as a vesicle. Later, a transport process called exocytosis discharges unwanted materials by performing endocytosis in reverse. Together, the endocytosis and exocytosis mechanisms serve as a security escort service directing and delivering material to the place it needs to go and safely escorting unwanted waste to the outside of the organelle or cell membrane. [Barrett et al., 1986]. This close-knit approach between cell security and routing represents a similar approach that is evident in some of the new Internet standards. The latest internet address protocol now being implemented, IP version 6 (IPv6), adds security and privacy values into a packet’s header field. IPv6 also will require the use of certain security protocols in the Internet Protocol Security (IPsec) framework that will enhance security capabilities at the packet level [TechTarget, 2003]. Improvements such as IPsec and IPv6 can make the Internet inherently more secure because security is designed into the core functionality of these newer protocols. The security architecture of the newer Internet standards is closer architecturally to the framework used in cells in that the newer standards now integrate security tightly into the functionality of the communication mechanism.

Like organizational computer networks, an extensive routing system moves macromolecules to their proper functional compartment in cells. These ‘routers’ are membrane-bound systems devoted to keeping intracellular order by delivering newly synthesized macromolecules to their proper home. Although not well understood, the Golgi Apparatus handles many of these operations as the principal router of protein traffic in the cell [Britannica, 2003]. Other sorting operation details are unknown and the subject of current biological research. The internal ‘routing tables’ in a cell are contained in the nucleus. As the highly protected information hub of the cell, the nucleus provides details about the transportation of proteins into different compartments. It contains most of the cell’s genetic information and houses the DNA molecules, which contain the information a cell needs to retain its unique character.

Internal routing and sorting in cells is not unlike that in computer networks. While such features as IPv6 and the inclusion of firewall functionality in routers are improving security in computer networks, no network mechanism yet reaches the level of encapsulated protection provided in cell processes such as endocytosis and exocytosis.

## 5. THE VIRUS ANALOGY

Many similarities exist between computer viruses and biological viruses. Both domains use similar terminology to describe the phenomenon of a virus. In addition, the general function of a biological virus closely parallels that of a computer virus.

### Virus Infection and Reproduction

In both the domains of biology and computing, viruses exist in numerous varieties, with many different means of creating problems for their hosts. Like biological viruses that can only reproduce inside host cells, most computer viruses reproduce only within another computer. Also like biological viruses, many computer viruses are capable of mutation and recombination. Some computer viruses can therefore evolve and adapt to their changing environments just as biological viruses are capable of doing. An example of such a computer virus is the encrypted virus.

> *"An encrypted virus's code begins with a decryption algorithm and continues with scrambled or encrypted code for the remainder of the virus. Each time it infects, it automatically encodes itself differently, so its code is never the same. Through this method, the virus tries to avoid detection by anti-virus software* [McAfee, 2003]."

Three main types of reproductive cycles, or "life histories," occur among animal viruses. Each of these three types of reproductive cycles is analogous to computer viruses.

1. The first is the lytic cycle that occurs when a virus invades a cell, reproduces, and then disperses when the cell membrane breaks, or lyses. Certain computer viruses are also designed to enter a host system and perform some operation that results in a catastrophic, unrecoverable shut down or loss of data.

2. Animal viruses called temperate viruses use a second type of reproductive cycle. These viruses may either go through a lytic cycle and destroy the cell they invade, or may instead enter a dormant phase in which the virus DNA is joined to that of the host cell and replicated with it over many cell generations. A host cell containing such a temperate virus is called a lysogenic cell. Certain external stimuli can cause a lysogenic cell's virus DNA to enter the lytic cycle, bursting the cell and releasing intact viruses. An important consequence of the lysogenic relationship is that viruses released when a cell lyses may carry with them a portion of the host's DNA. Host DNA may then be introduced into a new host cell when the virus infects another cell. This process is called transduction (carrying across), and it produces genetic recombination in the new host cell [Arms and Camp, 1987].

Similar to the biological temperate virus, some computer viruses also enter a host system and lie dormant until some stimulus event brings them to action to perform whatever act they were designed to perform. Also, just as with the biological virus, such computer viruses can reveal, carry away, or at least utilize, some portion of information from the host computer as they replicate and move to other systems. An example of this type of computer virus is the "Trojan Horse" class of computer viruses. Trojan Horse viruses camouflage themselves as harmless pieces of software and lie dormant in the network, examining the keystrokes pressed by people as they use computer programs, accessing data in the system's memory and stealing passwords and files [Economist, 2002].

3. Many animal viruses are known to be replicated and released continuously from intact host cells. In this third type of reproductive cycle, the virus enters its host cell by endocytosis. In the endocytosis process, certain proteins in the viral membrane bind to receptor proteins in the host cell's plasma membrane. The host cell's membrane eventually engulfs the virus into a vesicle within the cytoplasm. Once inside the cell, the virus can release its viral RNA, which directs the host cell to replicate the RNA genome and produce proteins for the viral capsid and envelope. New copies of the viral genome and capsid combine in the cytoplasm. These newly formed

viruses, or nucleocapsids, move to the host's plasma membrane where the outer coating of the new virus and the new envelope proteins on the host's outer wall attach to each other. The host cell's plasma membrane bulges out around the forming virus particle. Eventually, the virus is fully surrounded by its new envelope and pinches off, or buds, from the host cell. Animal viruses that bud this way include influenza, measles, mumps, and rabies [Arms and Camp, 1987].

Some computer viruses are designed to perform a function similar to the animal virus' nucleocapsid approach. The computer virus enters the host system embedded or attached to an email or other document. Once inside the host system, the computer virus begins replicating new copies of itself, attaching to or "wrapping" these new virus copies in outgoing email or perhaps in other documents. As the email or other documents travel to another computer system, the new copies of the virus invade the new host system and the process is repeated. Examples of this type of computer virus include the Code Red, Nimda, and Klez viruses [McAfee, 2003].

### Virus Detection and Response

Nonspecific defense mechanisms protect all animals from diseases and viruses. Examples of nonspecific mechanisms in animals include skin, interferon, phagocytes, and bacterial fluids [Arms and Camp, 1987]. Computer networks also use nonspecific defense mechanisms. Examples of nonspecific defense mechanisms in computer networks include firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS) and antivirus software. Like nonspecific defense mechanisms, the immune system refers to a general system that provides for the defense of an organism from diseases, including viruses. Taken together, we can envision the group of nonspecific defense mechanisms for the network as its immune system.

The biological immune system protects the body against viruses, as well as against other invaders, frequently destroying them in the bloodstream so that they never reach the cells of vital organs such as the brain or liver. Just as in the body, some computer viruses and/or other "invaders" are stopped by a firewall or other defenses and never reach a network computer. However, if viruses elude the body's immune system and invade a cell, the infected cell releases interferons, proteins that help to protect healthy neighboring cells from the virus. Interferons stimulate these cells to produce substances that interfere with viral replication, a process that serves to isolate the neighboring cells from the virus. Intrusion detection systems and antivirus software are examples of systems that can serve a similar function in a computer network. When a virus is detected in a network, intrusion detection systems can notify administrators, send messages to other computers, and in some systems, isolate the infected computer from the other computers on the network. Similarly, when antivirus software detects a virus on a computer, it typically notifies the administrator and quarantines the virus. Quarantining a virus isolates the virus on the system and prevents it from doing any damage to the computer. The virus is held in quarantine until it is destroyed or otherwise removed from the system.

## FIVE CENTRAL THEMES FOR CELLULAR DEFENSE

Five common threads or central themes emerged from this discussion, as presented in Table 2.

Table 2. Five Central Themes of Cellular Defense Mechanisms

| |
|---|
| 1. Seamless integration of communication and security functionality |
| 2. Proactive approach to membrane defense and crossing |
| 3. High level of specialization of communication methods |
| 4. Standard use of internal membrane protection of high value resources |
| 5. Overall, security is integrated, ubiquitous, and continuous |

*1. Security functionality is highly integrated into cellular communication mechanisms.*

That is, the security is not separate from the communication mechanism, but is rather an integral part of the communication system itself. In general, we do not see dedicated security mechanisms in cells. What we do see is security built directly into the various communication mechanisms. Examples of such integration in cellular communication systems include facilitated diffusion, membrane channels, and the numerous transporters, all of which are also inherently secure mechanisms.

*2. Cells take a proactive approach to identification and passage of items through the outer cell membrane.*

Instead of taking the approach of identifying unwanted elements, which is the common method with intrusion detection systems in computer networks, cells take an opposite approach. By focusing on the 'friendly' chemical or electrical signals provided by a visitor at the outer wall of the cell membrane, cells provide an active defense by identifying desired elements prior to allowing their passage through the external membrane[2].

*3. Cells developed a rich variety of highly specialized mechanisms for moving molecules across or through the outer membrane.*

There appears to be a tailored mechanism for each type of molecule. In fact, there are numerous other transporters and membrane channels, with each designed for specific types or groups of molecules.

*4. Cells make liberal use of internal membranes to protect their more valuable assets or resources.*

Mitochondria, vesicles, and the nucleus, for example, all contain their own protective membrane—or multiple membranes—in addition to the cell's outer membrane.

When considering the full range of mechanisms that inherently provide cellular security, we conclude that cells maintain a high-security orientation. Defensive functionality is present in mechanisms at the cell wall, within organelles, during internal routing, and throughout the entire cell. In addition, the defensive mechanisms of a cell are not intermittently active, but rather are continuously active, or always on.

*5. The overall central theme is that cell security is integrated, ubiquitous, and continuous.*

That is, in biological cells, security is a part of everything, security is everywhere, and security is always functioning. These five themes suggest general implications for network security design, which we discuss in Section V.

## SUMMARY OF THE ANALOGIES

The five categories of analogies presented in the previous sections include:

- The Barrier Defense Analogy,
- The Barrier Transmission and Communication Analogy,
- The Internal Organization Analogy,
- The Internal Routing and Sorting Analogy, and

[2] Cells also respond to threats from unwanted elements like dangerous pathogens, but the primary focus seems to be on the proactive identification of friendly or desired elements.

- The Virus Analogy.

Each of the analogies in these categories suggests similarities between biological cellular functions that defend the organism as compared to computer network systems that defend the organization. However, the value of formally exploring such similarities comes from the stimulation of ones thinking, which helps generate ideas and insights, which in turn can lead to network security improvements. In the next section, we offer two examples of how we used the framework to spark ideas for improving computer network security.

## IV. USING THE FRAMEWORK

The first idea came from two processes in biology. The first process is one of the methods the cell membrane uses to move larger molecules into and out of a cell (i.e. endocytosis and exocytosis). The second process is the nucleocapsid approach that some viruses use for replication. These two processes lead to our first network security idea: that data traveling within a computer network should not move through security, and/or from security to security, but rather, the security should move with the data. That is, data should be "wrapped" in the security and the security would move with the data as the data moves through the network.

A second idea came from the active defense mechanisms in cells: first, the oligosaccharins, which signal the 'oxidative burst' at the cell membrane as an offensive counter attack; and second, the reaction of a cell invaded by a virus, that when dying, releases interferons into the system prior to its death to warn and protect other cells. Based on these two active defense mechanisms, each individual computing system should have the capability of identifying an attacker, sounding a system-wide alarm, and sending vital information concerning the attacker to all other systems within the network. Using the vital information concerning the attacker, other systems would release 'hunter-killer' agents, that would scour the entire network to 'search-and-destroy' the previously hidden or unidentifiable attackers.

An additional layer of security could provide for an emergency response when an attacker immediately and catastrophically eliminates an individual system. Under this circumstance, the infected system would not be able to send out a warning or other information to allow identifying of its attacker. However, in such a case, a network monitoring system would detect the elimination of the attacked system and automatically raise the security level of the entire network, effectively insulating each individual system until an investigation could reveal the problem with the 'dead' system.

An extension of the second idea would include a full-time active defense mechanism. In a cell's external environment, the cell receives full-time protection from the body's immune system. Many potential threats are eliminated before they can attack an individual cell. In a similar manner, an extension of the second idea proposes intelligent 'hunter-killer' agents that would continually roam the network in search of intruders. Anytime a new threat was identified, all agents would have their memories or knowledge bases updated to add to their list of known intruders. Each agent would also have the capability of using its knowledge base to identify potential attackers and make a temporary 'arrest.' Temporary detainment allows the suspect to be isolated for a quick 'background-check' before facing either release back into the network or permanent deletion. Regular communication would be maintained among all of the agents so that each such encounter would also update the other active agents in the system.

## V. IMPLICATIONS

### GENERAL IMPLICATIONS FOR USING THE FRAMEWORK

We believe that our framework and exploration can provide benefits, not only to the research community, but to a much broader community as well. In the area of education, cell biology and

the framework presented in this article can provide interesting analogies for teaching students about the functions of firewalls, intrusion detection systems, exterior/interior routers, proxy servers, network DMZs, access control lists, anti-virus software, and numerous other areas of information system security. Since biology is part of a basic high school curriculum, biological analogies provide a natural reinforcement and cross-training tool when discussing computer technologies in the classroom. In addition, because analogies between computing and biology have been used for some time (e.g. computer viruses, computer memory, neural networks) using such relationships in teaching are natural extensions of analogies that many students already know something about.

In addition to being useful within education, we also feel the framework can be helpful to practitioners and consultants in a number of different ways. For example, those who are responsible for implementing network security in organizations can use this model for thinking about ways to configure and deploy their networks and its defenses to protect their IS resources. Commercial developers of information security technologies can use this framework in thinking about and developing innovative new products and improvements to existing products.

The framework can be used as a guide to spark ideas and lead to new research on network security. However, while we feel there can be significant value in using the framework in research, we did not find a single reference to such an approach in the extant MIS literature. In our search of the literature, we found only two references to any similar approach and these were both in Computer Science. Consider the value of an approach similar to our framework as quoted in a reference from MIT's Journal of Evolutionary Computation. Here the authors describe the use of the biological immune system as a basis for designing artificial systems:

> *We believe that the biological immune system provides a compelling example of a massively-parallel, adaptive, information-processing system, which we can study for the purpose of designing better artificial systems. The biological immune system is compelling because it exhibits many properties that we would like to incorporate into artificial systems: it is diverse, distributed, error tolerant, dynamic, self-monitoring (or self-aware), and adaptable. These properties give the biological immune system certain key characteristics that most artificial systems today lack: robustness, adaptivity, and autonomy* [Hofmeyr and Forrest, 2000, pg. 443].

## GENERAL IMPLICATIONS FOR NETWORK SECURITY DESIGN

The five central themes discussed in Table 2 suggest specific implications for computer network design, as summarized in Table 3.

Table 3. Implications of the Five Central Themes for Network Security Design

| **FIVE CENTRAL THEMES:** | **IMPLICATIONS FOR NETWORK DESIGN:** |
|---|---|
| Integration of communications and security | Integrated or embedded security functionality |
| Proactive membrane defense and crossing | Focus on active detection of friendly communications |
| Specialization of communication methods | Specific and specialized communication mechanism |
| Internal protection of valued resources | Widespread use of internal firewalls |
| Security is integrated, ubiquitous, and continuous | Security is integrated, ubiquitous, and continuous |

1. We should see fewer security-dedicated processes and more communication processes with embedded or integrated security functionality (e.g. virtual private networks).

2. Instead of focusing on the detection of unwanted or dangerous data communications, firewalls and intrusion detection systems should evolve to focus primarily on actively detecting desired or 'friendly' communications.

3. We should see a proliferation of specialized network communication processes designed specifically for the various types or groups of network transmissions.

4. Within organizational networks, we should see an increase in the use of internal firewalls providing increased protection for the organization's important assets or resources.

5. Finally, as an overarching network design theme, we should expect to see a proliferation of network security mechanisms and devices based on security that is integrated, ubiquitous, and continuous.

## VI. CONCLUSIONS

The growing need and projected demand for better network security coupled with a general absence of related articles in MIS academic journals suggests that the area of computer network security is a fruitful subject for scholarly research attention. More specifically, within the domain of MIS, the area of computer network security offers a topic that is both appropriate to the MIS discipline's core properties [Benbasat and Zmud, 2003] and ready for innovative study, research, and exploration.

The general approach represented in our framework is described in the following quote:

> *The latest thinking draws on lessons learned from the body's immune system. Besides being one of the wonders of biology, the immune system is also a marvel of parallel and distributed computing--and one that offers insight into how networks can be made to resist attacks naturally* [Economist, 2002, pg. 32].

The key point of this "latest thinking" approach is that the biology-computer analogy can offer insights that may otherwise be overlooked. That is, as networks continue to grow in their connectivity, number of users, and overall complexity, the more the design of network security should perhaps follow the example of the cell—that network security should also be integrated, ubiquitous, and continuous.

In summary, the framework presented in this paper and its approach to using cellular biology as a reference for thinking about network security is a timely idea that can offer important implications within a broad community. It is our belief that as computing technology continues to expand its role as an enabling necessity in organizations, network security will also continue to grow in its need for new ideas and creative solutions for securing the information and resources of the modern business. We extend a call to researchers in MIS and related domains to become a part of the creative process of developing insightful solutions in response to the growing challenge of providing innovative and viable network security.

*Editor's Note:* This article was received on November 18, 2003 and was published on December 31, 2003

## REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the

paper on the Web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. the authors of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Arms, K. and P. S. Camp (1987), *Biology* (3rd ed.) Philadelphia, PA: Saunders College Publishing.

Barrett, J. M., Abramoff, Kumaran, et al. (1986), *Biology*. Englewood Cliffs, N.J.: Prentice-Hall.

Benbasat, I. and R. W. Zmud (2003), "The Identity Crisis Within the IS Discipline: Defining and Communicating the Discipline's Core Properties," *MIS Quarterly*, 27 (2), 183-194.

Britannica (2003), "Encyclopedia Britannica Online," http://search.eb.com/eb/ article?eu=108758 (current March 15, 2003).

Bruno, L. (2003), "Digital Defenses: A Business's Network Is Its Castle," *Red Herring*, 52-53, January

Carr, H. H. and C. A. Snyder (2003), *The Management of Telecommunications* (2nd ed.) New York: McGraw-Hill Primis Custom Publishing.

Doms, R. W. and D. Trono (2000), "The Plasma Membrane as a Combat Zone in the HIV Battlefield," *Genes & Development*, (14), 2677-2688.

Economist (2002), "Inoculating the Network," *The Economist*, 363 (8278), 30-33, June 22.

Encyclopedia (2003), "Encyclopedia Britannica Online," http://search.eb.com/eb/ article?eu=108758 (current March 15, 2003).

Farabee, M. J. (2003), "On-Line Biology Book," http://www.emc.maricopa.edu/ faculty/farabee/BIOBK/BioBookTOC.html (current May 5, 2003).

Friedman, M. H. (1986), *Principles and Models of Biological Transport*. Berlin and New York: Springer-Verlag.

Frolick, M. N. (2003), "A New Webmaster's Guide to Firewalls and Security," *Information Systems Management*, 20 (1), 29-34.

Hofmeyr, S. and S. Forrest (2000), "Architecture for an Artificial Immune System," *Evolutionary Computation*, 8 (4), 443-474.

Kurzweil, R. (2000), *The Age of Spiritual Machines: When Computers Exceed Human Intelligence*. New York: Penguin Putnam Inc.

Loch, K. D., H. H. Carr, and M. E. Warkentin (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *Management Information Systems Quarterly*, 16 (2), 173-184.

McAfee (2003), "Virus Information Library," http://www.mcafee.com/anti-virus/ default.asp (current May 22, 2003).

Mehta, M. and B. George (2001), "Security in Today's E-World," Proceedings of the *Seventh Americas Conference on Information Systems*, Atlanta, GA: Association for Information Systems, 1219-1226.

Panko, R. (2004), *Corporate Computer and Network Security*. Upper Saddle river, NJ Prentice Hall.

Saupe, S. G. (2002), "Plant Physiology," http://www.employees.csbsju.edu/ ssaupe/index.html (current March 23, 2003).

Sequeira, D. (March, 2003), "Intrusion Prevention Systems: Security's Sliver Bullet?," *Business Communications Review*, 36-41.

Stallings, W. (2001), *Business Data Communications* (4th ed.):Upper Saddle River, NJO Prentice-Hall

Straub, D. W. (1990), "Effective IS Security: An Empirical Study," *Information Systems Research*, 1 (3), 255-276.

TechTarget (2003), "Whatis.com," http://whatis.techtarget.com/ (current March, 2003).

Tiboni, F. (April 15, 2002), "Pentagon Decides Best Defense is Active Defense in Cyberattacks," *Federal Times*, 38 (11), 6-8.

Zviran, M. and W. J. Haga (1999), "Password Security: An Empirical Study," *Journal of Management Information Systems*, 15 (4), 161-185.

## LIST OF ACRONYMS

| | |
|---|---|
| DMZ | Demilitarized Zone |
| DNA | Deoxyribonucleic acid |
| FTP | File Transfer Protocol |
| IDS | Intrusion detection systems |
| IP | Internet Protocol |
| IPS | Intrusion prevention systems |
| IPsec | Internet Protocol Security |
| IPv6 | Internet Protocol version 6 |
| RNA | Ribonucleic acid |

## ABOUT THE AUTHORS

**Kenneth J. Knapp** is a doctoral candidate in Management Information Systems at Auburn University. He is an active duty Lieutenant Colonel (select) in the United States Air Force specializing in information management and security. He has a B.S. in Computer Science from DeSales University and an MBA from Auburn University. He served as Assistant Professor and Director of Curriculum at the United States Air Force Academy's Department of Management from 2001 to 2002. He is a member of AIS and the Armed Forces Communications and Electronics Association.

**R. Frank Morris, Jr.** is a Ph.D. student in Management Information Systems at Auburn University. His research interests include computer and network security, information systems strategy, computer/technology acceptance and use, and information systems value and success. He holds a bachelor's degree in Aerospace Engineering from Georgia Institute of Technology and an MBA from Georgia Southern University. Mr. Morris has more than twenty years of experience working in private industry.

**R. Kelly Rainer, Jr.** is George Phillips Privett Professor of Management Information Systems at Auburn University. He is co-author, with Efraim Turban and Richard Potter, of *Introduction to Information Technology* (3rd edition), Wiley and Sons, 2004.

**Terry Anthony Byrd** is Professor of Management Information Systems at Auburn University, Auburn, Alabama. He holds a B.S. in Electrical Engineering from the University of Massachusetts at Amherst and a Ph.D. in Management Information Systems from the University of South Carolina. His research appears in the *Journal of Management Information Systems*, *MIS*

*Quarterly*, *Decision Sciences*, *OMEGA*, *Interfaces*, and other leading journals. His current research interests include the strategic management of information technology, information technology architecture and infrastructure, and information technology integration.

Communications of the Association for Information Systems

ISSN: 1529-3181