

# *The Nature of Cyber-attacks in the Future: A Position Paper*

Sumit Ghosh, Ph.D.

**G**iven society's increasing dependence on networked systems, it is clear from their past occurrences that cybercrimes pose a serious threat to our long-term welfare. This article focuses on the current relationship between networked systems and cybercrimes, analyzes the nature of the relationship from a fundamental engineering perspective, and systematically explores where and how future advances in networked systems might influence the evolution of cyber-attacks, even inadvertently giving rise to new forms of cybercrimes. Historical data reveals that technological advances in engineering systems design, including communications and transportation, were often accompanied by lack of foresight, thereby inadvertently opening doors to new forms of vulnerabilities following deployment. The greater the extent of the advancement, the deeper the potential chasm and more severe the damage incurred when a clever perpetrator successfully exploits the weaknesses. For example, when the Bell Telephone System employed human operators to switch telephone calls in the early 1900s, anonymous and unauthorized long-distance calls were a

rarity. As soon as automatic switching equipment replaced human operators, "phone phreaks"<sup>1</sup> discovered a serious flaw in the system. First by simply whistling or using a toy whistle and later through utilizing a tone-generating bluebox, one could break into the signaling control and make unauthorized long-distance calls.

## **THE ENGINEERING FUNDAMENTALS OF NETWORKED SYSTEMS**

To facilitate understanding, this article begins with a simple yet fundamental and complete picture of networked systems. Any networked system consists of three basic elements: nodes, transport links, and control algorithms. While the nodes appear in the public in the form of terminal devices such as the telephone handset for voice communication, computer terminals on which electronic messages are typed and received, or automated teller machines where financial transactions are initiated, their more complete and powerful form consists of the high-performance telephone switching systems housed in telephone stations; powerful routers located in back-office

---

*SUMIT GHOSH, PH.D., is at the Secure Network Design Laboratory (SENDLAB) in the Department of Electrical and Computer Engineering at the Stevens Institute of Technology in Hoboken, New Jersey. He can be reached at [sghosh2@stevens-tech.edu](mailto:sghosh2@stevens-tech.edu).*

closets; control centers that govern the operations of trains, planes, and nuclear reactors; and highly reliable servers in the financial institutions and the Federal Reserve banks. Although the copper cables belonging to telephone and telegraph companies, and the line-of-sight microwave and wireless towers of the cell phone industries, are visible in the open, the optical fibers and line-of-sight laser links employed by Internet service providers (ISPs) are generally out of sight of the ordinary public. The control algorithms constitute the invisible force, are the least tangible of the three elements, and reside in the hardware and software programs of the entire system.

Conceptually, the nodes represent computing engines that encapsulate the ability to execute computationally intelligent software programs. Throughout history, computing needs were supplied by the human brain. This extended into the early 1900s when human operators supplied the intelligence required for telephone switching. Since their conception in the mid-1900s, computers have continued to supply computing power, faster and more reliably and precisely than the average human brain. Because any two communicating devices must be separated by a finite geographical space, regardless of how small or large the actual distance, the energy representing the communication must cross this space, thereby requiring a transmission medium. The forms currently in use include copper cable, optical fiber, wireless, laser-link, etc. The control algorithms constitute the underlying decision making and help realize the overall intent and functions of the system.

In its true form, a control algorithm is an abstract idea that is realized utilizing the tangible resources of the system. Thus, in a simple telephone system, the control algorithm finds and establishes, where possible, a path from the caller to the callee, while in a complex financial network, the system ensures that the correct payer account is debited and the exact same amount credited to the payee account.

In general, every node performs two distinct functions: route packet traffic and provide computing power for executing the underlying control algorithms. Over the past decades, while nodes and links have experienced phenomenal growth, our understanding of control algorithms has evolved the most and this holds the key to immense innovation in the future.

In the future, control algorithms will be increasingly distributed, fast executing, and more powerful. As an example of the subtle power of control algorithms, consider the following real-world example. Authorities would like automobile drivers to slow down in front of a school while it is in session, to prevent children from getting hurt when they accidentally run into the street and the oncoming vehicle's high speed precludes that vehicle from stopping in time. One child has been hurt and there have been a number of near-misses. The authorities first try posting speed limits on the side of the street but they are ignored. They then try to place the signs in the middle of the pavement but to no avail. The authorities seek assistance from the police department and a police officer patrols the area for a limited time, giving out a few tickets; but as soon as the police officer leaves, the situation is back to square one. The authorities also realize that while the event has strained their relationship with the residents of the neighborhood, the cost to permanently station the police officer at the school is prohibitive.

At this time, an individual, say A, comes up with an idea, one whose constituent components involve different elements of the system. Person A reasons that current automobile suspension systems are not designed to react well under abrupt discontinuities in the pavement. The car and the driver would receive a medium jolt, causing a highly unpleasant experience but no serious damage. Person A reasons that the pavement in front of the school could be reengineered: a set of two or three discontinuities, of increasing width, inserted into the pavement, and metallic strips placed into these discontinuities such that can be raised or

*The control algorithms constitute the underlying decision making and help realize the overall intent and functions of the system.*

*The success of the control algorithm stems from a solid understanding of the properties of automobiles and pavement systems, a knowledge of driver behaviors, and the conception of a mechanism that successfully exploits these knowledge pieces to achieve the objective.*

lowered electrically. The strips are lowered to open up the gaps in the pavement while the school is in session and raised to make the pavement uniform when school is not in session. The technology is mature and has been used for decades in drawbridges and elsewhere. Under these circumstances, speeding drivers would be compelled to slow down on their own to avoid the discomfort, and the authorities would achieve their safety goals, both economically and without confrontation. Thus, the success of the control algorithm stems from a solid understanding of the properties of automobiles and pavement systems, a knowledge of driver behaviors, and the conception of a mechanism that successfully exploits these knowledge pieces to achieve the objective.

#### **POTENTIAL ADVANCES IN NETWORKED SYSTEM STEMMING FROM ITS FUNDAMENTAL NATURE**

From the previous discussion, it follows that any networked system is fallible to the extent that one or more of its three fundamental elements are vulnerable. Clearly, improvements in networking will also center around these three elements and the most logical enhancements include the following.

**Bandwidth Increase.** The speed at which information is carried by the transport links is captured by the notion of bandwidth. Clearly, the ability to transport a greater volume of information and faster, increased bandwidth are desirable. To meet the increasing demand, a greater number of optical fibers may need to be installed along existing conduits or higher-capacity blue and UV laser may be deployed. Future technologies might even include lasers operating at x-ray,  $\alpha$ -particle, and  $\gamma$ -ray frequencies, pushing the carrier frequencies to even higher limits. Although necessary and useful, increased bandwidth incurs an inherent weakness. Under attack and during the phases of detection and recovery, a very large number of packets may be lost in a short time, thereby posing a significant challenge. While highly sophisticated

attacks may cause unprecedented damage, even a simple, hit-and-run type attack, capable of disrupting the systems for a very short period, can cause appreciable damage while eluding detection.

**Geographic Proliferation of Networking.** Because sharing constitutes a fundamental attribute of networking<sup>2</sup> and because it holds the potential to facilitate innovation among the citizens of the world,<sup>3</sup> it is both logical and inevitable that networking will undergo extensive proliferation, touching individuals in every corner of the world, transcending even into deep space. Under these conditions, network vulnerability will increase sharply. Attacks may now be launched from anywhere in the vast network, even far-away, remote locations. Also, the difficulties associated with controlling and managing such widely dispersed networks may serve as encouragement for the perpetrators. Furthermore, if hackers are able to design lightning-fast attacks, a topic that will be discussed subsequently, the implications on our current ability to detect, identify, and contain such attacks are grim.

**Increase in the Number of Network Users.** Spurred by the attribute of “sharing,” the future will very likely witness a large increase in the number of network users. Under these circumstances, networks will require a sharp increase in the level of personnel support for management functions, thereby increasing the risk from insiders. The sheer numbers of personnel and users will imply significant challenges to authentication and non-repudiation.

**Innovation in Service Types.** As a consequence of proliferation, future networks are likely to witness new and highly sophisticated types of services, beyond the current schemes that are based on bandwidth reservation, quality-of-service (QoS) attributes, etc. The new services are likely to constitute attractive targets because they tend to utilize specialized knowledge of the network’s

resources and perpetrators may exploit such knowledge to synthesize attacks tailored to specific services and users,<sup>4</sup> causing significant harm while rendering the attacks difficult to detect and their origins hard to locate.

**Transfer of Executable Code.** The idea of transporting executable code through the network has recently experienced rapid proliferation, bringing with it tremendous advantages. In essence, an executable code containing elements specifically designed and incorporated at node A is transported from node A to node B where it is subsequently and immediately executed. Upon execution, node B perceives an image and interacts with this interface, as intended by node A, without possessing any *a priori*, detailed knowledge of node A's design. Presently, network manufacturers and researchers<sup>5</sup> are pursuing this concept in the context of remote network configuration and management, and it is likely that the level of interest will continue to remain high. Underlying this promise, however, is a serious vulnerability with far-reaching adverse consequences. The threat stems from the fact that computer viruses consist of a string of 1s and 0s, are indistinguishable from any highly useful executable code segment, and there are virtually no known scientific principles that can guarantee any system protection from their first attack.<sup>6</sup> As in nature, where in a conflict between a venomous snake and a scorpion, the first one that successfully strikes deals a fatal blow to the other, a carefully designed computer virus can completely wipe out a system during its first attack, denying the system any second chance to recover.

**Continued Use of IP Networking Principles.** Notwithstanding the technologies of classic telephony, ISDN, and the more recent ATM, TCP/IP networking has continued to dominate the evolution of networks over the past three decades. It also underscores the bulk of today's Internet. The recent request for information (RFI) for the design and deployment of GOVNET,<sup>7</sup>

which is intended to provide critical government functions, clearly mandates it to be a private IP network.

Careful analysis reveals two key properties of TCP/IP networking that underlie current networking products as well as the thinking among industry practitioners. The first property is the store-and-forward concept, the advantages of which include the fact that the exact route for any packet is dynamic (i.e., unknown *a priori*) and that different packets, even corresponding to the same message, can assume different routes, thereby enhancing security. In many of the current IP routers, to save on computation, the routing tables are deliberately left unchanged for long periods of time. As a result, many if not all packets of any given message can adopt the same route, thereby sacrificing a basic, security-enhancing premise of the IP protocol.

The second key characteristic is the classic end-to-end reasoning,<sup>8</sup> which argues that regardless of a specific weakness of the intermediate nodes, reliable communication between two end points A and B can be achieved by executing high-level protocols. Thus, where the intermediate nodes suffer from transmission-related errors, the high-level protocol TCP solves the problem by repeated transmissions, initiated and controlled by the end points. Also, where the intermediate nodes are untrustworthy, secure communication between nodes A and B can be achieved through encryption. A key difficulty with TCP is that its inherent retransmission capability also constitutes a potential weakness, and perpetrators have successfully flooded the network, causing buffer overflow, severe congestion, and ultimately network failure. Furthermore, TCP's consumption of the valuable computational resource is an inherent performance limiter. Should TCP continue to be employed in future networks, hackers may exploit this weakness even more. Difficulties with sole reliance on encryption have been documented.<sup>4</sup> To ensure security, the GOVNET RFI further requires that the network features limited connectivity and

*Many if not all packets of any given message may adopt the same route, thereby sacrificing a basic, security enhancing premise of the IP protocol.*

Given the relatively slow speed of space travel, a deep space network (DSN) will play a crucial role in space colonization.

prohibits any interconnection or gateways to the Internet or any other private or public network. A serious concern with this requirement is that it contradicts a fundamental attribute of networking, namely, sharing,<sup>2</sup> and, as a result, GOVNET can quickly become obsolete and abandoned, even by the very users it is expected to serve.

The following is a related scenario described by a security firm at the Management of Technologies (MOT) Symposium.<sup>9</sup> To enhance its computer security, a high-tech company attempted to discourage its employees from using modems on company phone lines by converting its entire telephone system to digital. At the same time, the number of requests for fax lines increased dramatically and it was later revealed that employees had connected their modems to the analog fax lines to get their “job done.” While users rely on information accessed through the network in order to complete their tasks, the exact location of an information source may never be predicted with absolute certainty, *a priori*.

Internet II and Next Generation Internet (NGI) had been launched to compete with one another and succeed the current Internet.<sup>10</sup> Both Internet II and NGI were designed to be identical to the Internet except for employing faster fiber links. The list of expectations included no congestion and unlimited bandwidth for all users. Except for increasing the address space, adding a “scope” field for multicast addressing, and providing support for encryption-based authentication, integrity, and confidentiality, the latest version of the Internet protocol (IPv6) is identical to the traditional Internet protocol (IPv4). The NSF-sponsored workshop on Ultra Large Networks<sup>11</sup> noted the disarray into which Internet II had fallen, stemming from lack of use, and it was the majority feeling that Internet III is not needed as Internet II proved that it is not necessary. The most recent IETF security specification<sup>12</sup> states that “solutions need to work end-to-end without depending on services in the middle,” thereby confirming the IETF belief in the end-to-end reasoning, and

advocates the use of ciphers and public-private key system — Diffie-Hellman or RSA — to achieve security on the Internet.

There is yet another potentially serious problem with GOVNET. When a system that has been completely closed and isolated for maximal security is attacked from within, often the result may be unimaginable damage. As an analogy, consider the recent flooding of the Mississippi River in the midwestern states of the United States, when volunteers frantically piled sandbags to raise the height of the levies on both banks. However, as the weather worsened, rainfall inland continued to accumulate because the levies blocked their drainage into the river. As a result, all homes in numerous towns were flooded. The same levies that were being faithfully raised to secure the towns from the rising waters of the Mississippi River ironically turned into seeds of destruction.

As a second analogy, the most prestigious and fastest train in India, the Rajdhani Express, had an unprecedented record of security. For each of the air-conditioned compartments, the conductors dutifully locked every window and door shut, not just to keep the inside cool but to shut out dust, bandits, and unauthorized people. However, on September 9, 2002, when the “up” train fell into the river Dhawe,<sup>13</sup> the same locked windows and doors turned into death traps for the passengers inside because they could not be opened by rescuers from the outside.

There is widespread optimism in the scientific community<sup>14</sup> that the solar system will be richly colonized within the next 100 years. Given the relatively slow speed of space travel, a deep space network (DSN) will play a crucial role in space colonization. In discussing the NASA Interplanetary Network (IPN) project, Charles<sup>15</sup> notes that future plans for the IPN are to integrate local networks on Earth, other planets or moons, or even a space station or spacecraft, using traditional Internet protocols with a network that uses special long-haul, deep-space protocols.<sup>15</sup> Robert Durst and others at the MITRE Corporation have been working on

a communication protocol to extend Internet communications into space. They present extensions to TCP for space communications.<sup>16</sup>

However, DSNs are characterized by extreme latencies. For example, despite the potential for minor errors in store-and-forward routing in IP networks, the consequence is slight because since message transport times on earth range in the milliseconds. In contrast, the propagation delay from Earth to Mars ranges from 3 to 20 minutes, and a minor error in forwarding a packet may have severe consequences, especially for remote control. Thus, if DSNs are based on TCP/IP in the future, they will be highly susceptible to attacks.

**The Role of Control Algorithms in the Evolution of Networked Systems.** A key attribute of networked systems is the complex set of interactions between the constituent entities that are encapsulated by the underlying control algorithm. While the absolute timing of the interactions is very important, the relative timings are far more critical and challenging. Historical analysis of the evolution of networking and networked systems reveals the lack of a comprehensive set of principles and systematic experimental techniques to guide the synthesis of accurate control algorithms.

Leading researchers from the top telecommunications companies<sup>17</sup> have expressed serious concern regarding the occurrence of inconsistencies and failures in the context of “feature interactions” and the present inability to understand and reason about these events. For example, while private telephone numbers are successfully blocked from appearing on the destination caller-id screens under normal operation, as they should, these private numbers are often unwittingly revealed during toll-free 800 calls.<sup>18</sup> As a second example, despite the telephone subscriber paying a monthly fee for the “caller-id” service, incoming phone calls from the outside, including even those initiated by the local telephone service provider, often show up as “out of area” on

the consumer’s caller-id display. At the NSF-sponsored workshop on Ultra Large-Networks,<sup>17</sup> the general consensus among the leading experts on networking was that the Internet is not truly understood and its successful growth remains a mystery.

Other experts have started to comment, both privately and publicly, that the “Internet is far too complex to secure.”<sup>19</sup> At the MOT Symposium,<sup>9</sup> it was observed<sup>20</sup> that “buggy” code is responsible for security holes. While it is true, it only reflects the tip of the iceberg. A far deeper cause is little or no understanding of the interactions between high-level software and the underlying hardware at their interface. Moreover, any number of software patches, layered on top on an ill-defined interface will not only fail to address the problem, but worse, the additional layers will unnecessarily increase the computational burden and severely diminish system performance. For example, on a university campus, the use of firewalls and intrusion detection is extensive, resulting in e-mails typically requiring up to three hours to reach building B from building A even though they are a mere 400 feet apart. Clearly, it is faster to walk for five minutes and deliver the message in person.

In the sub-discipline of buffer management, an important area in network design and research, virtually all publications represent studies, either based on analytic modeling or simulation, of the behavior of proposed techniques for a single switch.<sup>21</sup> Clearly, a single switch network is not realistic. Lawson<sup>22</sup> traces the origin of the complexity in the computer industry to the deployment of “compromised” hardware design for all types of computing leading to the demand for unprecedentedly complex system software which, despite involving thousands of code developers, was never completely understood. To meet the increasing demand for sophisticated services, future systems must employ even more complex control algorithms. Thus, a complete understanding is imperative to harden systems from potential attacks and prevent serious failures.

*On a university campus, the use of firewalls and intrusion detection is extensive, resulting in e-mails typically requiring up to three hours to reach building B from building A that are a mere 400 feet apart. Clearly, it is faster to walk for five minutes and deliver the message in person.*

## **Attacks Directed against Networking Elements**

In contrast to the past and current virus attacks against computer installations and user machines, perpetrators in the future are likely to direct their attacks against the networking elements. Potential reasons for this shift in focus are threefold. First, given the growing sophistication, range, and operational speed of the switches and routers, any disruption of the networking elements will cause far more widespread damage than attacking user machines individually. Second, given that the network providers are increasingly attracted to transferring executable code from network management centers to remote network switches for dynamic node reconfiguration or dynamic services deployment, perpetrators will find it irresistible to design viruses to attack the switches. Third, current practice and thinking in the industry is that network management centers can safely exchange control and status signals with the remote nodes through the same channels that carry user traffic. This greatly increases the vulnerability and, if the present thinking persists, widespread network disruption is likely in the future.

## **Electric Power Line as a Serious Vulnerability**

Because electric power constitutes the life-support of all computers today and as this trend is likely to continue into the future, the power line constitutes a serious vulnerability. The ability of current operating systems to shut down power to the underlying hardware, under user directive, has proved highly useful, especially when it comes to an uninterruptible power supply initiating a safe shutdown following a power outage. However, this feature also underscores serious threats. First, perpetrators can design viruses to initiate shutdown during critical activities and camouflage them to appear as a system crash, thereby eluding detection. Second, attacks may target and corrupt the system BIOS, thereby rendering the node

temporarily unusable. Serious attacks may consist of reprogramming the BIOS, recovery from which will require the motherboard to be repaired or the BIOS replaced, implying a complete and prolonged shutdown. Third, viruses can initiate repeated shutdowns, even improper transient shutdowns, throwing the underlying hardware into a meta-stable state and causing damage to its internal components. Fourth, it is conceivable for a clever perpetrator to design a virus that will systematically shut down a node following every effort to turn it back on. Fifth, it is not entirely inconceivable for a team of determined perpetrators to transmit a virus-infected signal, disguised in the form of a traditional power surge, over the power line into the nodes at homes and business offices. The attackers may get help from tapping into the control signals that are also sent over the power lines by the power-generating companies to dynamically divert power to different power-consuming substations. The great number of nodes that are likely to succumb to this attack renders the threat very severe.

## **Blindingly Fast Viruses**

To date, most virus designs have targeted high-level application programs that execute slowly due to their significant code lengths. Because viruses piggyback on the host program and execute every time the host program is executed, current viruses execute relatively slowly. Thus, when the Minda virus would attack a node, one could observe the folders being steadily stripped off their constituent files, in real-time. In the future, sophisticated viruses designed to “jump” from the host application program to the core operating system will be entirely conceivable. In biology, the notion of a virus jumping from one animal species to another has been confirmed. Because the core functions are highly efficient compact code fragments that execute frequently and quickly, the virus will execute blindingly fast.

## **LONG-TERM INNOVATIONS IN NETWORKED SYSTEMS**

Networked systems are here to stay; the underlying reasoning is simple and profound. Networked systems reflect human civilization's core objectives: (1) acquire information on appropriate channels through interaction with other individuals on a need-to-know basis, and (2) execute decisions on an individual or collective basis to (3) accomplish a desired goal or purpose. These objectives bear a direct one-to-one correspondence with the three basic elements of networked systems stated earlier. Thus, as the discipline of networked systems matures and increasingly becomes integrated into society, demand for greater efficiency and widespread benefit will spur revolutionary innovations. This section focuses on a few conceptual ideas that are original and possibly revolutionary but as yet untested.

### **Generalized Networks**

Increasingly in the future, networks will include both stationary and mobile nodes. In the resulting generalized network, while a few nodes may constitute the core, a set of nodes may aperiodically join and leave the network. For greater cooperation and efficiency, every node may even participate in route computation, discovery, and other important networking functions. A generalized network of the future may span terrestrial nodes as well as nodes orbiting the Earth, space stations, switches on other planets, and even spaceships en-route in deep space. This desire for great efficiency and usefulness also renders such networks vulnerable to impersonation by perpetrators, leading to a potential breakdown in privacy and accountability. To eliminate the weaknesses, designers must carefully synthesize the underlying control algorithms. A thorough understanding of the principles of asynchronous distributed algorithms,<sup>23</sup> followed by insights into the proposed algorithms obtained through modeling and asynchronous distributed simulation,<sup>24</sup> may be of immense help.

Because wireless communication can either be radio based or employ direct line-of-sight microwave or laser, generalized networks are susceptible to computer viruses forcibly injected from the outside. A remote perpetrator can direct a strong beam at a target, overwhelm the local signal, and force a virus-infected signal that may eventually disrupt the system. Current versions of cellular phones, for example, are susceptible to severe damage by viruses transported over the ether. It is pointed out that, unlike a biological virus that is tiny yet based on matter and must necessarily reach the target physically (i.e., either through direct contact or airborne), a computer virus can assume the form of pure electromagnetic energy and is not subject to the same restrictions.

The U.S. military is increasingly embracing the concept of precision weapons such as the recently tested massive ordnance air blast (MOAB) bomb, and the intelligent hovering missiles, drones, and robotic tanks of the future that focus on intercepting wireless signals from the global positioning satellites to calibrate their present positions and guide themselves to the target precisely. Such weapons are highly susceptible to directed viruses that can not only cause the weapon's programming to be severely disrupted, but even reprogrammed, en-route, to force it to turn back to the launch site and detonate.

### **Strictly Inanimate Networked Systems**

Although any network must ultimately be in the service of mankind, the concept of a "strictly inanimate networked system" has been motivated by the observation that most system break-ins, approximately 90 percent, are caused by insiders. Then there are human errors, stemming from fatigue and lack of understanding, and unintentional leakage of critical system information resulting from employees succumbing to "social engineering" tactics by clever perpetrators. There is yet another reason cited to keep human beings away from networks — namely, operational speed.

*A generalized network of the future may span terrestrial nodes as well as nodes orbiting the Earth, space stations, switches on other planets, and even space ships en-route in deep space.*

*All valuable data, information, and procedures — whether related to medical, financial, trade secrets, etc. — are maintained by inanimate entities, beyond direct access and manipulation by human operators.*

Given that human beings are slow and impatient, their reaction times around 0.25 second to 0.5 second, in contrast to computer operational speeds governed by GHz clock rates (i.e., execution cycle time of one-billionth of a second) any interaction invariably slows down networks dramatically. Therefore, whenever possible, network functions must be handled entirely by inanimate robots and computers, and kept off-limits to human operators. Clearly, while human beings may not be removed entirely from the process of network design, network operation and management constitute ideal candidates for automation.

Conceivably, one can envision a future where networks, upon design and deployment, permit no direct interface with human beings. The network itself schedules tasks, allocates resources, analyzes its integrity, checks connectivity, initiates self-healing<sup>25</sup> in the event of failures, etc. All interactions with such networks occur through inanimate robots and computers that serve as the controlling gates, task schedulers, and watchdogs. All valuable data, information, and procedures — whether related to medical, financial, trade secrets, etc. — are maintained by inanimate entities, beyond direct access and manipulation by human operators. When an individual or organization with the proper authorization requires access to specific information, the request is submitted to a computer or robot, which first verifies the authorization, analyzes any potential conflicts, and then schedules the request to be processed. For high efficiency, the computational and network resource requirements of the request must be substantial.

Despite their obvious advantages from the perspective of security, strictly inanimate networked systems underlie serious potential problems. First, while an inadvertent system design flaw is clearly conceivable, during operation, the defect may interact with other system characteristics in unknown ways. Under a fully automated operational mode, before the error is detected, user data and information can be

irreparably damaged and the network elements rendered uncontrollably haywire.

Second, given the huge complexity of networked systems, an unscrupulous network designer can easily and surreptitiously leave behind backdoor traps and subtle susceptibilities that can be enabled and disengaged at will, years later. Third, the probability is very high that such systems will completely defy any attempt to develop a reasonably accurate analytic model. Assuming today's design techniques are translated into the future unchanged, any serious malfunction or catastrophic failure of the automated network will provide very little insight into the causes of the failure.

Fourth and most severe, if and when a perpetrator launches a virus, its interactions with the automated network may take on a new life, unknown even to the virus designer. Worse, if multiple viruses are launched, their convoluted interactions may yield a behavior that is unprecedented and beyond imagination. Without human beings to slow down the network, the unplanned and undesirable interactions will operate blindingly fast. The resulting damage can either be very extensive or the attack can be sustained over such long periods of time that it permanently alters the nature of information and brings about unforeseen societal changes.

Finally, in the event that portions of the networked system are detected to have gone berserk and it has been decided to shut down those units for repair, one might encounter severe difficulty in attempting to disable the illegal activities. During operation, the system may have autonomously modified the connectivity and routing algorithms through self-healing, making it difficult to determine the true source of the problem. In essence, the source of the attack is internal although it may be triggered by an external event or attack. Conceivably, in the future, the notion of self-healing may be extended to the network autonomously "reaching out" and choosing power receptacles or turning on backup power generators for most efficient, uninterrupted operation. Under these circumstances,

turning off suspected network components may pose an enormous challenge.

### **Highly Interlinked Networked Systems**

To provide for the growing need for highly sophisticated services and for efficiency in our daily activities, networks from different areas will be increasingly integrated in the future. As an example, a giant intelligent transportation network is clearly conceivable in the future, one that integrates the airline network, railway network, public transit system network, and taxi network. The thinking is that, while en-route, any traveler can continuously replan the route to the destination, taking into account current information on any expected delays stemming from accidents and incidents, etc., or unexpected changes in personal matters.

As a second example, the benefits of integrating the cell phone network with a home automation network and the national power grid are immense. An Arizona resident returning home ahead of schedule from New York might utilize the cell phone to remotely turn on the home A/C a few hours prior to his expected arrival, turn on the swimming pool pump having recently learned of a dust storm in Phoenix, and instruct the computer to turn itself on after the house has cooled down below 74 degrees. Already, in parts of the United States, the water company utilizes unused telephone lines in homes to remotely read the water meter, thereby interconnecting the telephone and water services network. Also, electric power-generating companies transmit control signals to dynamically divert power to different cities over the same high-tension lines that carry the high-voltage electricity. In the post 9/11 era, there is an increasing desire to develop a homeland security networked system that will coordinate the different federal, state, and local agencies to meet any future threat to the nation.

While the benefits of increased connectivity are limited only by our imagination, so are the threats and attacks that a perpetrator might conceive and develop. For a

highly interlinked networked system to be successful, the underlying control and coordination algorithm must be accurate; that is, it must generate correct results under every conceivable interaction between the elements of the interacting networks. Where the algorithm is less than sound, a perpetrator might cause a disproportionately high degree of damage by exploiting the tremendous resources of all of the networks combined.

In the homeland defense scenario, a weak control and coordination algorithm might enable a smart perpetrator not only to cause confusion and panic, but also to turn the networks' resources into a self-destructive weapon. To understand whether and how this is at all possible, consider the following example<sup>27</sup> from biology. The human immune system has evolved into a highly sophisticated defense mechanism — in essence, an algorithm against foreign microbes over hundreds of thousands of years. A number of different types of specialized cells, T-cells, white blood corpuscles, etc., numbering in the hundreds of thousands, constantly patrol up and down the bloodstream, searching out and attacking foreign microbes and destroying them whenever possible. By most measures, the algorithm is exceptionally successful, for it has continued to successfully defend billions of human beings against millions of different types of microbes over the last hundreds of thousands of years.

However, it has recently come to light that a tiny humble hantavirus has learned not only how to penetrate the defense mechanism, but also to bring about complete self-destruction. The mechanism it employs is fascinating. The tiny hantavirus enters the human body through the skin and propagates toward the lungs, easily slipping through the thin walls of the blood vessels lining the air sacs. Before the virus can do any discernible damage, the antibodies have detected the invader and quickly give chase, forcing their way through the blood vessels in the lungs. In the process, however, their much bigger size forces the blood vessels to

*In the post 9/11 era, there is an increasing desire to develop a homeland security networked system that will coordinate the different federal, state, and local agencies to meet any future threat to the nation.*

*The phenomenon of timing discrepancies with seriously adverse consequences is not new; there have been numerous inadvertent occurrences in the past.*

rupture, and plasma leaks into the air sacs, causing death within hours from respiratory failure.

The importance of a carefully synthesized coordination and control algorithm was recently underscored in a simulated attack carried out in Denver<sup>28</sup> to measure the country's level of preparedness against a bioterrorism attack. To mobilize the maximum resources under an attack, all relevant federal, state, and local agencies were involved. As the exercise unfolded, while the communication between members of the same agency intensified, as expected, the overall decision-making process broke down, causing tremendous casualties and widespread panic. For every major decision, more than a hundred people from the different agencies had to be brought into a massive conference call for consultation. While some of the workers were on the surface with wired telephones, others used cordless or satellite phones, and yet others used cell phones while in underground bunkers. The conference call frequently broke down, resulting in the lack of correct decisions and, ultimately, confusion.

Furthermore, a highly intelligent and dedicated perpetrator of the future might carefully analyze the coordination and control approach of a massively interlinked system and develop a sophisticated attack by utilizing (1) enormous computing power from distributed processors, (2) knowledge of asynchronous distributed algorithms, and (3) testing and refining the attack through modeling and simulation.

The most serious threat to the highly interlinked networked systems in the future may come from coordinated attacks that are likely to be extremely effective while remaining elusive. For quick response in an emergency in the future, the railway, telephone, intelligent transportation system, FAA, FBI, immigration and naturalization, air defense, Coast Guard, police, and hospital networks, are more than likely to be all interlinked. Underlying every timely interaction between the networks is the concept of an event, a key attribute of which is the

notion of time. Given that the networks are dispersed over a wide geographical area, algorithms must be put in place to ensure proper time synchronization for consistent and accurate results. A coordinated attack on the clocks through the use of high-energy electromagnetic pulses (EMPs) might cause disruption, even for a short period of time, causing unexpected, possibly unthinkable losses. The phenomenon of timing discrepancies with seriously adverse consequences is not new; there have been numerous inadvertent occurrences in the past. In the accidental downing of two U.S. military helicopters during the Gulf War by a U.S. fighter plane,<sup>29</sup> timing discrepancy caused two critical pieces of information to be flipped erroneously: (1) the radar image is a friend, and (2) the radar image is unknown, possibly an enemy.

Consider a hypothetical coordinated attack within the financial industry. A team of perpetrators design and launch a virus that recognizes files with financial records in them, surreptitiously changes a few of the facts and figures at random just prior to the initiation of the backup process, and then restores the figures to their original values at the conclusion of the backup routine. Because the backup routine handles thousands of files, it cannot possibly check the integrity of every individual file prior to saving it on the backup media. Because the online records are unaffected, regular audit checks do not detect the anomaly. By design, the virus executes surreptitiously over a very long period of time, thereby adversely affecting the backup records at several levels and destroying any chance of the correct figures from ever being reconstructed later through correlation. The viruses may even be customized for each bank and financial institution so as to defeat any attempt to recognize a discernible pattern, thereby diffusing any suspicion of a coordinated attack. The last phase of the coordinated attack consists of an assault on the main online computer system and every concurrently running secondary unit, either through an explosive device or by manipulating the

grid that provides electric power to the machines. Thus, not only are the online records destroyed, but the backups, at every level, have been corrupted, causing confusion, panic, and unforeseen difficulties.

To test the protection of the nation's critical infrastructure, two exercises — the first, code-named Black Ice held in Salt Lake City in November 2000 and the second, code-named Blue Cascades held on June 12, 2002 in Portland, Oregon — revealed the following. The effects of a major terrorist attack or natural disaster could be made significantly worse by a simultaneous cyber-attack.<sup>30</sup>

The October 14, 2002, terrorist attack in Bali, Indonesia, may have been planned as a coordinated attack. Immediately following the disaster, it was reported that the cause was a single powerful bomb. Soon thereafter, it was revealed that there were two explosions. The first, a small one, was detonated inside the club and caused the panicked patrons to huddle outside in an alley behind the building. With a high concentration of people in the alley, a much more powerful bomb was then exploded by the terrorists, causing extensive death and damage.

### **Quantum Entanglement Technology for Packet Transport?**

The notion of “entanglement”<sup>31</sup> in quantum mechanics refers to the fact that when two quantum particles — A and B — in our universe are entangled, they share the same destiny, regardless of the physical distance between them. That is, whatever occurs to A will happen to B simultaneously. This phenomenon has already been experimentally verified. Clearly, entanglement occurs at speeds in excess of the speed of light, transcending the limits set by the special theory of relativity. However, although B undergoes a change at time  $t$ , for example, corresponding to the change experienced by A at that instant, an observer  $O_B$  located near particle B may not possess instantaneous knowledge of the fact that the cause of B's transformation is indeed particle A. For this,

another observer,  $O_A$ , near particle A must send a message by any conventional means to  $O_B$ . Thus, although particles A and B may experience exact changes instantaneously, information flow between A and B is still bound by the speed of light.

From the perspective of information security, quantum entanglement offers an unprecedented new capability. We can subject particle A to a transformation locally and upon successful completion of the transformation of A, observer  $O_A$  sends a conventional message to observer  $O_B$ . The actual change experienced by A can be viewed as an important message. This message, however, is never propagated by conventional means. Only a simple communication from observer  $O_A$  to  $O_B$  asking the latter to read the state of particle B is propagated over a copper cable, optical fiber, wireless, direct laser, etc. Upon reading the state of B, observer  $O_B$  can extract the degree of change experienced by B and determine its meaning by referring to a table, jointly developed between  $O_A$  and  $O_B$  earlier. Thus, given that the actual message is manifest in the form of a transformation of A, strictly performed locally, the need for encrypting a packet in transit is eliminated. Furthermore, even if a perpetrator were to steal the table or intercept and read the simple communication from  $O_A$  to  $O_B$ , little harm would come from it. However, there is a serious difficulty with this approach. A perpetrator can easily cause complete disruption by intercepting and destroying the simple communication. Observer  $O_B$  would be denied knowledge that observer  $O_A$  had been attempting to communicate with it. Other forms of attacks are also conceivable.

In the teleportation experiment that validated quantum entanglement, the research team led by Zeilinger<sup>31</sup> had obtained entangled photons by splitting a UV laser pulse through a parametric down-converter crystal and then directed the photons to  $O_A$  and  $O_B$ . Clearly, a perpetrator can hijack photon B and masquerade as observer  $O_B$ . Worse, by performing manipulations and measurements on photon B, prior to those conducted by

*A perpetrator can easily cause complete disruption by intercepting and destroying the simple communication.*

Even the consensus report from the National Research Council on networking research recommends the aggressive pursuit of new ideas under the three M's — measurement of the Internet, modeling of the Internet, and making disruptive prototypes.

observer  $O_A$ , the perpetrator may surreptitiously affect observer  $O_A$ 's observations and measurements. The perpetrator can also duplicate the experimental setup, masquerade as  $O_B$ , and send a bogus entangled photon to  $O_A$ .

### **Fundamental Insight into the Nature of Security**

Careful analysis reveals that, from theoretical principles and practical considerations, 100 percent security in any networked system may not be achievable. The underlying reasoning can be traced to the inherent characteristics of human nature, namely, limited memory, impatience, susceptibility to fatigue, boredom during repetitive tasks, and the desire to maintain full control over every system design.

Consider, for example, the issue of password-based access control. For obvious reasons, a password must consist of a finite number of characters, presumably between five and nine, so that one may commit it to memory. Any longer sequence of characters might be easily forgotten and would require writing it down, implying a vulnerability. Given today's fast computers, even a brute-force approach to breaking a password would yield quick results. Thus, one precautionary measure, used in practice, limits the number of password attempts for a given user account to three or four, after which the user account is locked out and must be reset by the systems manager with access to the root account.

This measure, however, cannot be extended to the root account; for then, a perpetrator will repeatedly attempt to log on to the root account, making sure that the bogus passwords fail, and lock out the root account, from which the system may not ever be recovered. Therefore, by design, the system must tolerate an indefinite number of log-on attempts to the root account. This constitutes a fundamental vulnerability because, in time, any password cracking program will invariably break the system.

Although the discipline of mathematics categorically denies a network from ever gaining a 100 percent security status, the situation is far from bleak. Through engineering principles, a pragmatic secure network to carry out society's critical functions is realizable.

### **NEW APPROACHES TO SECURE NETWORKED SYSTEM DESIGN FOR THE FUTURE**

This section briefly presents a few key suggestions and new approaches that can assist in secure network design in the future. It is pointed out that even the consensus report from the National Research Council on networking research<sup>32</sup> recommends the aggressive pursuit of new ideas under the three M's — measurement of the Internet, modeling of the Internet, and making disruptive prototypes.

**Eliminate Transfer of Executable Code.** Where security is of primary concern, eliminating the transfer of executable code constitutes a fundamental requirement. A logical and equivalent replacement<sup>6</sup> consists of transporting data across a network, which is then executed locally. Conceptually, any activity achievable through the transfer of executable code and its subsequent execution on the receiver's machine may be equally accomplished by the propagation of data, followed by its use in the course of execution of a local program executing on the receiver's computing engine.

**Augment the Concepts of Store-and-Forward and End-to-End Reasoning with Other Networking Principles Currently under Investigation.** It is pointed out that the recent breakthrough — a deterministic  $O((\log n)^{12})$  time algorithm for testing if a number is prime<sup>33</sup> — poses a fundamental challenge to the computational intractability that had constituted the main defense of cryptography.

### **Utilize the Principles of Asynchronous Distributed Decision-Making Algorithms<sup>23</sup>.**

This is done to develop accurate control and coordination algorithms for complex networked systems.

### **Test, Refine, and Experimentally Study a Proposed Networked System Design through Modeling and Simulation prior to Developing and Deploying a Complete Prototype.**

Specifically, develop accurate behavior-level models of proposed networked system designs, synthesize a simulation employing asynchronous distributed event-driven techniques, and then execute the simulation on a testbed of loosely coupled parallel processors that closely resembles reality. While the approach is scientific and unquestionably economical, it has the potential to eliminate serious design errors, possibly preventing catastrophic failure and irreparable damage during the network's operational life.

**Develop an Accurate Solution.** The designers of a secure networked system must be fully committed and determined to develop an accurate solution, not a good enough one, even if that means falling behind schedule or incurring cost overruns within reason. For not only will a well-designed system last 100 to 200 years, but any compromise or imprecision may imply irreparable loss in the future or the failure to prove the guilt of perpetrators beyond a reasonable doubt.

### **Take a Note from History**

An examination of history reveals that courageous individuals as well as perpetrators were able to discover fatal weaknesses in otherwise highly fortified systems through comprehensive analysis. Often, the attacks that had successfully exploited these vulnerabilities were blatantly simple. For example, in ancient Asia Minor, Alexander of Macedonia clashed with Darius, emperor of the mighty Persian Empire. In their first battle, Alexander and his army of 15,000 faced Darius with his army of over 45,000. According to the prevailing rules of military

engagement, Alexander should have withdrawn in the face of superior numbers to avoid a crushing defeat. However, brash, in his early twenties, a novice, and bent on revenge for earlier humiliating Greek defeats, Alexander decided to engage in battle. He noticed that Darius had employed a number of archers, a sign of weakness in that era, and embarked on an unprecedented strategy. Leaving behind the bulk of his army in charge of his generals, Alexander charged at the head of an elite group of 5000 Macedonian Republican Guards, focusing straight at Darius. Observing the battle from his location in the middle of his own army, the seasoned veteran Darius quickly recognized Alexander's single-minded focus on capturing him. Fearing for his life, Darius fled the battlefield, leaving the Persian army in complete disarray and eventual defeat.

Now consider a second example. Fast-forwarding to the last century, in the late 1960s, despite employing thousands of engineers and scientists to develop a highly sophisticated telephone system, phone phreaks<sup>1</sup> were able to use a simple toy whistle found in Captain Crunch cereal boxes to break into the system and initiate unauthorized long-distance calls. At the time, Ma Bell employed in-band signaling, wherein the control signals were transported along the same wire that carried voice. From a security perspective, this was a fundamental design flaw, one that had to be corrected later by installing a physically distinct signaling network.

Consider a more recent occurrence as a third example. In the mid to late 1990s, a major oil company stated publicly that it was developing a secure wireless network at an enormous cost rated at Gbps (gigabits per second), to transfer billions of bits of data obtained from the ocean-bed exploration for oil from ship to shore. Lacking a holistic approach, the planners had overlooked a simple fact that these billions of bits would be subsequently processed down to a few hundred bytes and ultimately expressed in the form of maps and charts of the ocean floor that, in turn, would help engineers

It may help to maintain a fine line of distinction between individual hackers who are tempted by the challenge to discover vulnerabilities in highly fortified system and organized perpetrators motivated to cause meaningless harm to others.

decide whether or not to drill the ocean floor. Clearly, the processing could be carried out locally on the ship, using desktop or laptop computers and the few hundred bytes of processed information easily sent to the corporate laboratory through inexpensive and existing secure wireless links.

Clearly, the greatest threat to any networked system comes from an intelligent individual or a team dedicated to harming the system. The most logical and perhaps the only recourse lies in the designers expending serious effort to uncover any flaws and errors in the system design before the perpetrators find them, through holistic thinking and simulation, both prior to developing the prototype and after the system is deployed. Furthermore, it may help to maintain a fine line of distinction between individual hackers who are tempted by the challenge to discover vulnerabilities in highly fortified system and organized perpetrators motivated to cause meaningless harm to others. Should individual hackers, who tend to draw a line when it comes to causing real harm to people, be severely prosecuted, we may never find out system vulnerabilities until a perpetrator strikes a severe blow and it is too late to prevent a catastrophic meltdown. In a strange sort of way, without clever hackers earnestly at work, the discipline of networked systems may quickly suffer from complacency, arrested progress, and become unexciting and lifeless. ■

#### Notes

1. The Learning Channel. Hackers: Computer Outlaws. Cable Television, July 25, 2001.
2. Seshasayi Pillalamarri and Sumit Ghosh. The Impact of Source Traffic Distribution on Quality of Service (QoS) in ATM Networks. In *Proceedings of the IEEE International Conference on Communications*, pp. 2855–2859, June 11–15, 2001.
3. Walter Lessig. *The Future of Ideas: The Fate of the Commons in the Connected World*. Random House, New York, 2001.
4. Sumit Ghosh. *Principles of Secure Network Systems Design*. Springer-Verlag, New York, April 2002.
5. In *Annual International Working Conference on Active Networks*, <http://www.iwan2002.org>, December 4–6, 2002.

6. Sumit Ghosh. Computer Virus Attacks on the Rise: Causes, Mitigation, and the Future. *Financial IT Decisions 2002*, Vol. 1, A Bi-Annual Technology Publication of the Wall Street Technology Association, 1:16–17, Feb/Mar 2002.
7. General Services Administration. Request for Information — GOVNET. U.S. Federal Government, November 21, 2001.
8. V.L. Voydock and S.T. Kent. Security Mechanisms in High-Level Network Protocols. *ACM Computing Surveys*, pp. 135–171, June 1983.
9. Management of Technologies Symposium. Guarding Your Business: Enterprise Architectures for Security. <http://attila.stevens-tech.edu/motsymposium>, October 22–24, 2002.
10. Jon Swartz. PAGE ONE — Need for Speed Spawns 2 Internetlets. *San Francisco Chronicle*, <http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/1997/07/28/jMN20332.DTL>, July 28, 1997.
11. In NSF sponsored workshop on Ultra-Large Networks: Challenges and New Research Directions, Nov. 18–20, 2001.
12. Jeffrey I. Schiller. IETF Security Specification — Designing Secure Protocols. <http://www.ietf.org>, 1 July 2002.
13. Editorial. The Rajdhani Disaster. *The Tribune*, Chandigar, India, <http://www.tribuneindia.com/2002/20020911/edit.htm>, September 2002.
14. Larry Lange. The Internet Technology 1999 Analysis and Forecast. *IEEE Spectrum*, 36(1), 35–40, January 1999.
15. John Charles. Technology News: Interplanetary Network Aims for the Stars. *IEEE Computer*, 32(9), 16–19, September 1999.
16. Robert C. Durst, Gregory J. Miller, and Eric J. Travis. TCP Extensions for Space Communications. *Wireless Networks*, 3(5), 389–403, October 1997.
17. Private communications with Dr. Alfred Aho. Vice President of Research. Bell Labs, Lucent Technologies, Murray Hill, NJ, December 2001.
18. Private Communications with Gottfried Luderer. Emeritus ISS Chair Professor. Electrical Engineering Department, Arizona State University, Tempe, AZ 85287, January 2002.
19. Bruce Schneier. Code Red Worm. CRYPTOGRAM, page <http://www.counterpane.com>, August 2001.
20. Steve Bellovin. Realistic Security. In *Guarding Your Business: Enterprise Architectures for Security, Management of Technologies Symposium*, pages <http://attila.stevens-tech.edu/motsymposium>. Stevens Institute of Technology, Hoboken, NJ 07030, October 22–24, 2002.
21. A. Bonde and S. Ghosh. A Comparative Study of Fuzzy versus “Fixed” Thresholds for a Robust Queue Management in Cell-Switching Networks. *IEEE/ACM Transactions on Networking*, 2(4), 337–344, August 1994.
22. Harold W. Lawson. Rebirth of the Computer Industry. *Communications of the ACM*, 45 (6), 25–29, June 2002.
23. Sumit Ghosh. *Algorithm Design for Networked Information Technology Systems: Principles and Applications*. Springer-Verlag, New York, 2003.

24. Sumit Ghosh and Tony Lee. *Modeling and Asynchronous Distributed Simulation: Analyzing Complex Systems*. IEEE Press, New Jersey, 2000.
25. R. Kawamura, K. Sato, and I. Tokizawa. Self-Healing ATM Networks Based on Virtual Path Concept. *IEEE Journal on Selected Areas in Communication*, 12(1), 120–127, January 1994.
26. Anthony Oettinger. Plenary Presentation. In *BRG Symposium on Command and Control Research*, Washington, D.C., 28 June 1993.
27. Public Broadcasting Service, KNME-TV, Albuquerque, New Mexico. Dangerous Friends, Friendly Enemies. In *Intimate Strangers: Unseen Life on Earth*, <http://www.pbs.org/opb/intimatestrangers/>, Aired 26 February 2000.
28. Channel 13, New York City. BIOTERRORIST ATTACK: WHO GETS VACCINATED? Public Broadcasting Service, <http://www.pbs.org/wnet/religionandethics/week511/cover.html>, November 16, 2001, Show 511.
29. CNN Primenews. Defense Department Finding, Pentagon. In Reporter Jamie McIntyre, Cable Network News, Atlanta, GA, August 24, 1994.
30. Dan Verton. Exercise Exposes Vulnerabilities. In *Computerworld*, <http://www.computerworld.com/industrytopics/energy/story/O,10801,72532,00.html>, 8 July 2002.
31. Justin Mullins. The Topsy Turvy World of Quantum Computing. *IEEE Spectrum*, February 2001, 42–49.
32. CSTB: Annual Convening on Research Horizons. Looking over the Fence at Networks: A Neighbor's View of Networking Research. National Research Council Consensus Report, page [http://www7.nationalacademies.org/cstb/pub\\_lookingover.html](http://www7.nationalacademies.org/cstb/pub_lookingover.html). 23-24 January 2001.
33. Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. <http://www.iitk.ac.in/news/primalty.html>, 6 August 2002.

## THE HUB OF INFORMATION SECURITY

**MARCH 22 - 24, 2004** Orlando, FL The Rosen Centre Hotel

**OPTIONAL WORKSHOPS** March 20, 21, 24, 25 & 26

**VENDOR EXPO** March 22 & 23

**80+ SESSIONS TARGETING TOPICS CENTRAL TO YOUR SUCCESS** Web services security, the latest in hack tools and spyware, wireless mapping, network forensics, e-provisioning, DMZ security, Active Directory 2000 and .NET, hacking VPNs, event correlation, implementing an IDS, evaluating your PDA security, and much more!

**THE 2ND ANNUAL CISO EXECUTIVE SUMMIT** This exclusive one-day program for IT security thought leaders features high-profile experts and a special keynote address

**KEYNOTE SPEAKER WILLIAM C. BONI** Vice President and CISO, Motorola

**THE INFOSEC WORLD EXPO™** Get up-to-date on the latest infosec technology at this blockbuster showcase featuring 125+ exhibitors

**CANDID INTERVIEW WITH KEVIN MITNICK** Reformed hacker and President, Defensive Thinking; by G. Mark Hardy, President, National Security Corporation

**THE ULTIMATE HACKER CHALLENGE** See if you can break into our network!



For more info and to register go to  
[www.misti.com/infosecworld](http://www.misti.com/infosecworld)  
 or call 508-879-7999.



#### CISO EXECUTIVE SUMMIT SPONSORS



#### PREMIER MEDIA SPONSOR

