GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

The Biological Analogy and the Future of Information Security

GSEC Practical Assignment

Version 1.2f

Randy Buttram

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

GSEC Practical Assignment
Version 1.2f
Randy Buttram

The Biological Analogy and the Future of Information Security

Historically, computer systems and networks have been described using biological analogies, likening computing systems to living organisms. This analogy stems at least partially from the view of computing as artificial intelligence, the recreation of biological intelligence and mental processes in a manufactured form, whether mechanical (Charles Babbage's Difference and Analytical Engines), electronic (vacuum tubes through transistors), optical (current projects in photonic computers) or subatomic (quantum computing). This analogy is used within the field of information security not only by historical precedent, but due to the validity of the analogy and the utility with which it can help information security professionals understand the increasingly complex systems for which they are responsible. Like any analogy, however, there is a breakdown point at which the analogy no longer applies.

However, parallels can be drawn between the medical sciences and information security, as both are concerned with maintaining the health of their respective systems. To be specific, historical events from the medical profession can, I believe, yield insights as to the possible future of the information security profession. Additionally, the biological analogy may well become more accurate, and the 'breakpoint' at which the analogy no longer applies may extend farther. In the extreme case, there may be a merger of the medical and information security professions, to a greater or lesser degree. Indeed, this has already happened in at least one case![1]

The Biological Analogy

In the general biological analogy of computing, computer systems and networks are often described as being comparable to a biological system such as the human body. In one such model, systems can be described as organs, and networks considered to be simultaneously the circulatory system interconnecting them and the nervous system through which they interchange control information. Continuing further, intrusion detection (including antivirus) can be viewed as analogous to the infection-fighting systems, while firewalls represent various filtering systems which prevent the ingestion of hazardous substances (skin, respiratory, stomach, etc.).

In this analogy, malicious code (e.g. viruses, Trojans, worms) is often represented as medically infectious organisms. Viruses in particular take their name from the medical microorganism whose behavior they imitate. And hostile behavior (e.g. unauthorized access, denial of service) is viewed as a malicious injury or attack, much like a medical trauma.

The Analogy Detailed

In a well-architected and deployed environment, computer systems share a number of common characteristics with bodily organs. In each case, an individual component (computer system or organ) is purpose-specific – a clear case of 'form-follows-function'. Similarly, networks can be viewed as combination circulatory and nervous systems, interconnecting components and carrying control and support signals. In this view, control signals between computer systems are analogous to nervous impulses, and data is analogous to red blood cells.

Information security can be described in this framework as well. Intrusion detection systems (which include antivirus systems in this model) are analogous to the white blood cells and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

antibodies which work to detect and eliminate intrusions; like intrusion detection systems, which are (currently) dependent on signatures of known exploits, antibodies are attacker-specific. Firewalls are the input filters, which work to prevent harmful intrusions from occurring, such as the skin and the filtering capabilities of the respiratory system. And, continuing the analogy further, when an intrusion does occur, the response may 'clog up the system', with a firewall slowing (or even stopping) network traffic in a manner analogous to the sinuses congesting in the presence of an allergen or infection.

The analogy between malicious code and hostile behavior and medical issues is more direct. Viruses, and to a lesser extent worms, are named because their behavior specifically resembles the behavior of their medical analogue: self-replicating, infectious through casual and/or intimate contact, and damaging to the infected target. While there is no direct biological equivalent to an externally-introduced Trojan, a very rough analogy can be drawn between a Trojan (a malicious program which masquerades as a legitimate program) and a cancer (normal cells which are behaving in a 'malicious' manner). Similarly, active malicious activity (unauthorized access attempts, denial of service attacks, etc.) shows some similarity to medical trauma incidents, in that there is usually an active assailant involved, and the target is more directed, while handling of such incidents more closely resembles triage and trauma care.

Limitations of the Analogy

Quite obviously, there are limitations to the model described above. In poorly architected and deployed environments, computer systems are installed willy-nilly, without regard for robust and secure configuration, and are often called upon to perform multiple distinct functions, a situation which is only found in the simplest of biological organisms (and is often a legacy of simpler computing environments which have grown larger than planned without robust configuration and change management). Computer systems can be deployed with redundancies and failover capabilities that biological systems do not have available, though biological systems are often more robust and fault tolerant than computer systems. Plus, there are computer system components which lack any kind of biological analogue.

Similarly, networks differ greatly from the biological circulatory and nervous systems. A key difference is the commonality of the physical pathways of a network, and the general indistinguishability between control signals (such as the TCP/IP handshake) and data (indeed, some exploits place data in the TCP/IP handshake to take advantage of this), while there is a clear delineation between the circulatory and nervous systems. Similarly, the organs which support the biological systems are themselves specialized (and centralized, i.e. the heart and the brain), while the systems which support networks (network devices, e.g. switches and routers), while specialized, are not exclusively centralized.

The differences between intrusion detection and perimeter systems and biological immune systems are significant. The biological immune system includes an automatic response to a detected intrusion, while such capabilities are sometimes difficult to implement, especially in general-purpose host-based or in network-based intrusion detection systems. Likewise, firewalls have a hit-or-miss track record with regards to perimeter protection, as many intrusions involve spoofing the perimeter firewall, while the respiratory filters miss little if anything; most of the symptoms of minor respiratory illness (congestion and associated effects) are the result of the filtering system doing its job properly!

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

As noted above, while viruses are defined based on their resemblance to their biological analogue, Trojans are only roughly analogous to any biological malady. Additionally, infection vectors are more constant on computer networks, due to the 'always-on' nature of network interconnections, with only perimeter systems and intrusion detection to combat infections, rendering the application of quarantine and other proven public health measures impractical at best, often contributing to the damage of an attack

Lastly, one of the key 'prizes' of the information security environment is the datastore. There is no obvious biological analogue to the datastore and the issues involved in protecting it. Similarly, while there are preventative immunizations which can be introduced into a biological system to prevent an infection from damaging the system, no such ready analogue has been developed for information systems.

Utility of the Analogy

The biological analogy most readily fails when a high level of granularity is used in constructing the model. However, the model remains generally valid at such levels. When the level of granularity is reduced, and whole systems are compared, the analogy strengthens. And, as computing systems become more complex and their capabilities more closely approximate the capabilities of biological systems, the analogy may become even less susceptible to breakdown. As Martin Libicki observes, "the increasing power of hardware and the growing sophistication of software suggests a future in which silicon starts to act more like carbon…."[2] Such a likely future will present systems interconnected by networks which attain the complexity of biological systems; on an aggregate level, biological analogy will increase in accuracy, and an understanding of basic medical practice and theory may well be useful for the information security professional.

The Future of Information Security

Predictive analysis is a much art as science when dealing with real-world systems. Accuracy of prediction is highest when the system under analysis is an aggregate system (macro-scale physical mechanics), the predictive term is large compared to the period of fluctuation (long-term stock market performance, climatological trends), or the projection is for an immediate time frame and the discussion is limited to general trends. The last of these is the context of this projection of the information security profession.

Short-term projections are typically based on extrapolations of current behavior, with influencing factors taken into account. Additionally, the past behavior of analogous systems can often yield insight into the likely future behavior of a system under analysis. Using the biological analogy above, examination of recent medical issues can be useful in anticipating the near-term direction of the information security profession.

The Rush to Interconnect

The key development in information systems in the 1990s was internetworking, the interconnection of individual networks for the interchange of information. However, this opened the individual networks to hostile or malicious activity and data. Thus, the challenges faced by information security professionals are focused on managing data traffic; permitting what is 'good' while denying what is 'bad'.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Using the biological analogy, this frenzy of internetworking can be likened to an environment where the likelihood of the spread of an infection is higher because of greater contact along infectious vectors. While there are a number of historical cases where such conditions have occurred, one of the most recent, and thus more familiar to the modern information security professional, is the spread of the HIV virus.

The decade of the 1970s saw a drastic increase in the number and frequency of sexual encounters among a significant demographic within Western society. Known medical issues of the time were typically treatable with then-current medical procedures (antibiotics for most STDs), or were 'live-withable' (genital warts, herpes) without significant impact on the 'interconnective' lifestyle.

This is analogous to the internetworking boom of the 1990s, as previously private systems were directly and intimately connected to a large number of other such systems with great frequency, and direct transferral of 'data' occurred. Like the Sexual Revolution of the 1970s, the Internet Revolution of the 1990s had its threats (e.g. the Internet worm, the Melissa virus), but the threats were perceived to be such that they could be 'treated' (by antivirus systems), or that the threat was low enough compared to the potential gains that the risk was absorbed, by conscious choice or by 'default by denial'.

End of the Revolution

The emergence of the HIV virus[3] halted the Sexual Revolution virtually overnight. As the facts about the infectious vectors became known, a variety of lifestyle changes took place among a significant majority of the demographic in question, as well as among society in general, as processes involving the infectious vectors were adjusted to screen for the infection. (It is important to examining the history to note that many conventional public health measures, e.g. quarantining infected patients, were not implemented.) Additionally, significant resources were allocated to medical research into the virus and the search for a vaccination or cure.

One effect of these events has been an increased awareness of personal medical safety, especially in situations involving intimate physical contact, or contact with bodily secretions. Individuals, organizations, and entire industries have changed their processes to account for and mitigate the risk of HIV infection. While some members of heavily-affected demographic groups have made accusations of deliberate unresponsiveness by public health officials, those same persons have acted to prevent some public health measures from being applied, as noted above.

History Repeats Across the Analogy

As noted above, the internetworking boom led to greater electronic intercourse between previously private networks. Additionally, some networks were created for the specific purpose of joining in the 'interconnective' marketplace and taking advantage of the opportunities it offered. However, as interconnection increased, so did the threat level. One after another, successive infections took advantage of the interconnections, the casualness with which many of the interconnections were set up, and the lack of diligence in planning, design, and deployment of systems which were intended for interconnection, whether by primary systems vendors or by end users.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

However, recent events may prove to be the watershed for internetworking that the HIV virus proved to be for the Sexual Revolution. The Code Red (I&II) and Nimda (-A&-E) worms have greatly increased information security awareness among organizations and individuals alike. World events raise the spectre of organized cyberwarfare, as well as illustrating the value of disaster recovery and business continuity. And a worsening economy, with accompanying corporate downsizing, has brought the disgruntled insider to the attention of the collective consciousness. And a certain demographic assigns blame to certain primary vendors while insisting on processes that permit the continued dissemination of information which facilitates the creation and spread of infections.

While the late 1980s and 1990s were replete with system-crippling malware (e.g. the Internet worm[4], Michelangelo, Melissa), the level of connectivity and criticality of connected systems was not sufficient to significantly increase the perceived threat, particularly as compared to the Y2K issue.

The Y2K issue was an unacknowledged information security issue in the area of availability and, to a lesser degree, integrity. Systems which did not 'roll over' correctly and handle dates properly would likely have shut down completely, rendering those systems and the data stored on them unavailable. Where the systems did not shut down completely, the corruption of time-stamped and date-sensitive data was a real risk as well. The remediation of the Y2K issue is a real example of the kind of investment that information security can require, with the return on the investment literally being the continued existence and operations of the organization!

With Y2K successfully resolved, businesses entered into an even more extensive (and intensive) round of interconnectivity, as vendor, partner, and customer systems were deemed 'trustworthy' by virtue of having survived the date rollover. With the increased interconnectivity came an increased dependence on the security of not only one's own systems, but of one's connected partners as well. Additionally, the increasing deployment of computers to workers at all levels of organizations left networks vulnerable to errors by the technologically unsophisticated. Furthermore, the crushing schedule requirements placed on implementers militated against thorough planning and configuration management.

The Code Red[5], Code Red II[6], Nimda-A[7], and Nimda-E[8] worms, all of which struck in the second half of 2001, brought these realities home to the computing public. As these infections spread due to naïve users opening email attachments, insecurely configured systems serving as active infection propagators, and open, trusted interconnections between organizations providing pathways for these infections to spread, entire organizations were unable to conduct normal business, and potentially billions of dollars were lost.

To the information security community, the events of September 11, 2001 demonstrated a worst-case disaster recovery/business continuity scenario. Additionally, while the military information systems community has been evaluating and monitoring the cyberwarfare threat for over a decade, the prospect of 'terrorist hacking' has also increased information security awareness at the corporate executive level.[9] Fortunately, those lessons were not lost on executive management. As worsening economic conditions cause organizations to rein in their spending, particularly in IT, information security budgets are increasing.[10]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

While the information security community has long considered the insider threat to be the area of greatest risk, many organizations still do not perceive the insider threat as significant, despite statistics that indicate that "the majority of security breaches are caused by members of staff."[11] Nevertheless, as companies downsize in response to changing economic conditions, released employees and non-employee workers (contractors and consultants), in critical IT positions especially, are in a position to do large amounts of damage to the companies they leave behind.[12]

Projecting the Future

It is becoming rapidly apparent that well-operated organizations are increasingly recognizing the value of information security to their operations. While information security remains a cost center for most organizations, the first ROI (Return on Investment) calculations are now becoming available which quantify the value of information security to the organization.[13] Information security companies are a clear counter-trend to the overall slowdown of the technology sector.[14]

The key indicator for the future of information security seems to be the recognition of the importance of information security by executive management. Security issues are increasingly becoming recognized as vital to the overall economic health of an organization. From work stoppages due to one of the myriad of malware infections to losses due to theft of equipment by released employees[15] to lost corporate image and market value due to a public Web site defacement, security breaches are beginning to cost their victims in amounts visible to executive management.

The historical example of the Y2K issue can, if carefully presented, be used as an illustration of the magnitude and impact that information security issues can have on the organization. While Y2K was an application security vulnerability, and required significant amounts of applications work to remediate, that example can be used, separately or in conjunction with the ROI calculations discussed above, to illustrate the value of integrating information security from the planning and architecture phase of a system or network project through deployment into post deployment testing, in addition to the more common operational audit and break-fix information security activities.

For the information security professional, these developments are a positive thing. Qualified information security professionals are in high demand.[16] Security organizations are being represented at increasingly higher levels of the organization, with some organizations creating a Chief Security Officer as a corporate officer reporting directly to the CEO.[17] Other organizations are moving information security from IT to legal, to separate audit and policy from implementation and enforcement.

Coupled with the new tools for measuring the positive impact that security can have on the bottom line, the coming decade may well be a boom era for information security. Many difficult issues remain, from privacy to intellectual property to user awareness; the solution to many of these will not lie entirely within the scope of the information security profession. And the career path available for the information security professional will not always be a technical one, as upper management and executive positions are being created in information security. While there will always be a need for the whitehat hacker to counter the blackhats, information security is maturing into a business profession, not just a technical one.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

---

[1] Dr. Peter Tippet, M.D. is the Vice Chairman and Chief Technologist for TruSecure Corporation, a managed security solutions provider. URL: http://www.trusecure.com/html/about/execbios.shtml#peter (14 November 2001)
[2] Libicki, Martin. "The Future of Information Security." Institute for National Strategic Studies. URL: http://www.ndu.edu/inss/books/infosec/infosec.html. (14 November 2001)
[3] "History of AIDS 1981-1986." AVERT. URL: http://www.avert.org/his81_86.htm (14 November 2001)
[4] Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons, 2001. p. 380-381
[5] CERT® Incident Note IN-2001-08. CERT. 19 July 2001. URL: http://www.cert.org/incident_notes/IN-2001-08.html. (14 November 2001)
[6] CERT® Incident Note IN-2001-09. CERT. 6 August 2001. URL: http://www.cert.org/incident_notes/IN-2001-09.html. (14 November 2001)
[7] CERT Advisory CA-2001-26 Nimda Worm. CERT. 25 September 2001 URL: http://www.cert.org/advisories/CA-2001-26.html. (14 November 2001)
[8]CERT/CC Current Activity. CERT. 12 November 2001 URL: http://www.cert.org/current/current_activity.html#W32/nimda. (14 November 2001)
[9] Scalet, Sarah D. "Cyberterrorism Is Everyone's War." CIO. 11 October 2001. URL: http://www.cio.com/research/security/edit/a101101_cyber.html. (27 November 2001)
[10] Dignan, Lary. "Survey: Attacks prompt IT spending gloom." ZDNet News. 17 October 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,5098417,00.html. (27 November 2001)
[11] IT Analysis. "Security: the enemy within." The Register. 22 November 2001. URL: http://www.theregister.co.uk/content/55/22974.html. (27 November 2001)
[12] Scalet, Sarah D. "The Insiders." CIO. 6 September 2001. URL: http://www.cio.com/security/edit/a0906_trust.html. (27 November 2001)
[13] Berinato, Scott. "Coming Up ROSI." CIO. 26 October 2001. URL: http://www.cio.com/security/edit/a102601_rosi.html. (27 November 2001)
[14] Lemos, Robert. "Report: No Slump For Security Biz." ZDNet News. 22 August 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2806762,00.html. (27 November 2001)
[15] Konrad, Rachel. "Laid-off Tech Workers Strike Back." ZDNet News. 24 September 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,5097371,00.html. (27 November 2001)
[16] Bryce, Robert. "Supply and Demand." Interactive Week. 15 October 2001. URL: http://www.interactiveweek.com/article/0,3658,s%253D619%2526a%253D16396,00.asp. (27 November 2001)
[17] Scalet, Sarah D. "Another Chair at the Table." ZDNet News. 09 August 2001. URL: http://www.cio.com/research/security/edit/a080901_alignment.html. (27 November 2001)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.