Just Sick About Security

Jeff Williams
williams@arca.com

Arca Systems, Inc.
8229 Boone Blvd., Suite 750
Vienna, VA 22182

This paper explores the similarities between people's health and the security of complex computer systems. The endless battle between threats to human health and our defense mechanisms has been going on for hundreds of thousands of years and has resulted in an extremely flexible set of protections. Our intrusion detection and immune systems are so good that most attacks go unnoticed. In other disciplines, looking to nature has proven extremely valuable. For example, in aviation, we have found many of the most efficient wing designs in birds and even whales. Perhaps we can look to nature for help understanding the threats to computer systems and even find strategies for protecting against them.

In addition to the defenses we have evolved, humans also practice medicine. Advances in nutrition and health care have greatly improved the quality and length of human life. While we have been practicing medicine for almost as long as we have been human, we have only a few decades of experience with protecting computer systems. This is another area to search for help in computer security.

COMPARISON

From a security point of view, the similarities between computer systems and people are striking. A quick examination of the architecture, external and internal interfaces, and communications system shows a number of these similarities.

First, people are made up of many distinct, but tightly integrated systems. The critical functions are distributed among the nervous, digestive, immune, circulatory, respiratory, skeletal, muscular, urinary, endocrine, exocrine, and reproductive systems. Each of these systems is created from smaller systems all the way down to the cellular and molecular level.

Real human interfaces cover a wide range of signals. We can receive a large portion of the ultraviolet spectrum, can eat and breathe, perform chemical analysis, can sense temperature, and can perform sophisticated pre-processing and selection of input. These interfaces reflect a careful balance between security and functionality. Eyes have eyelids, skin is tough and heals quickly, the excretory system is one-way, and

the mouth even supports specialized bacteria.

People's internal interfaces also have protection mechanisms. For example, blood supplied to the brain passes through a filter to ensure that it doesn't have any harmful contents. Unfortunately, as we well know, filtering based on content is never perfect. Alcohol and cocaine are two examples of substances that can penetrate the blood-brain barrier with unexpected results. Similarly, the stomach doesn't digest itself because a special type of cell has evolved that is resistant to stomach acid which protects the rest of the body.

These internal interfaces can prioritize communications between people's internal systems. Slower messages are handled chemically and faster messages are sent electrically. However, these systems are not perfect. Sometimes the communications system is affected by spoofed or blocked signals. Prozac, for example, tends to stabilize human behavior by blocking the reuptake of serotonin, a chemical similar to LSD, in the brain. In epileptic seizures, the synchronized firing of neurons can cause a significant disruption in brain activity.

In order to talk about a person's resistance to injury and illness, you have to consider their environment. If people could be isolated from threats, there wouldn't be much need for defenses, but we must interact with our environment by eating, communicating, drinking, excreting, and sensing in order to survive. For example, Native Americans were probably considered extremely healthy before the arrival of European diseases. Similarly, the products and components that make up systems of computers must also interact with their environment, sometimes endangering the system. For example, UNIX computers might be considered secure in a small closed network, but are extremely vulnerable to the threats of the Internet environment.

One of the most telling similarities between human health and computer security is the impossibility of accurate measurement. How do you ever know that you are healthy? Or secure? In either case, you can identify possible threats and vulnerabilities forever.

BASIC PROTECTIONS

The most obvious protection in the human body is our amazing ability to detect conditions that are likely to lead to injury. Our reaction to pain is innate and keeps us out of trouble much of the time. If a computer receives an unexpected input, maybe it should say "ouch" and focus attention on the possible attack.

Our skin provides a flexible, waterproof barrier that keeps in body fluids and keeps out bacteria and harmful rays from the sun. Generally, the skin defines the boundary between the outside world and our body. However, we compromise this boundary by eating, breathing, kissing, and having intercourse. Sometimes, the skin gets cut or torn. In this case, the bleeding and clotting process cleans and seals the wound. Other times, the skin can't do its job properly. For example, hydrofluoric

acid goes right through skin and kills cells beneath the surface. In general, however, the skin protects the body from most outside attacks.

Setting up a virtual "skin" around a computer system is often achieved with physical protection or encrypted private networks. Like real skin, these boundaries also have holes, or interfaces, for exchanging data. They may also be penetrated by threats that they were not intended to stop. Identifying this boundary can help to focus attention on problems that are likely to penetrate the system, as opposed to the entire spectrum of threats.

Eyes reflect a good balance between health and performance. They are protected by eyelashes and eyelids, yet still provide uninterrupted vision and amazing reaction time. This is a good model for keeping the overall goal in mind when working on security. Eyes would be better protected if they were deep set and had a tough covering, but they probably wouldn't be able to do their job as well. Similarly, workstations might be more secure if they had mandatory controls, but they would be more difficult to use.

Women have developed some remarkable protection mechanisms to ensure a healthy fetus. Many pregnant women experience cravings for unusual foods, like pickles and ice cream, or morning sickness. Both of these effects have been linked to the nutritional needs of the unborn child. In computer systems, configurations change all the time, and the protection mechanisms should support all the possibilities.

CHECKING INPUT

At almost every stage, humans have evolved mechanisms to deal with bad input. For example, the majority of input to the human body comes through the nose and mouth. Air is closely examined in the nose. Ammonia, for example, causes an extremely fast reaction. Air is then filtered through the nose and sinuses, the cilia in the throat, and the alveoli in the lungs. If foreign particles are detected, the body can respond with sneezing or coughing. For food, the first check is the conscious choice of healthy food over junk. The nose and tongue detect spoiled or bad tasting food and the teeth ensure digestibility. If these checks fail, the body can respond with vomiting or diarrhea to purge the attack from the system.

Computer systems also need a series of checks on input, but unfortunately, many systems rely on a single point of failure. An attacker that successfully breaches the single security check is not likely to be detected. There are actually many types of checks available, including input validation, content analysis, and consistency checking. Checking input is very hard and needs to occur at many levels if it is to work properly.

In addition to physical input, people can be seriously affected by the information they receive. Everything from teasing to psychological torture can lead to serious mental problems later in life, such as schizophrenia or depression. Similarly, if a computer system receives bad information, serious vulnerabilities may

be introduced. For examples, see the Risks Digest, which contains descriptions of the effects of bad input in almost every issue.

INTRUSION DETECTION

People are not born with defenses against most sicknesses. Our immune systems deal with these recurring threats by identifying and remembering them, so that they are easily handled the next time around. Viruses are common examples of these recurring threats. When a virus tries to invade the human body, it encounters the immune system. In most cases, the intruder is identified and a defense is constructed. In other cases, like cancer, the immune system is blind to the intrusion. If an identification is made, the intruder and the appropriate defense are remembered. From this point forward, the intruder is no longer a threat. This strategy is exactly the one that works for computer viruses. We identify viruses, develop a defense, remember an identification sequence, and start scanning. Like the human process, the creative work is identifying and developing defenses for new viruses and the ongoing work is scanning and defending known viruses.

Sometimes several different attacks work together to harm an individual. This is the case with AIDS. First, the HIV wears out the immune system by mutating so fast that the body cannot keep up. Then an opportunistic infection takes advantage of the weakened immune system and kills the patient. This attack is in some ways similar to the IP spoofing attacks that have become popular on the Internet, where an authorized host is overwhelmed while the attacker can guess the response needed to be mistaken for that host.

The human immune system is advanced enough to recognize cells and organs that don't belong. This differentiation between self and non-self allows the body to reject things that are likely to cause harm. Unfortunately, sometimes the body rejects an organ that could prolong survival. Computer systems don't have this problem because they don't have any sense of identity. The closest approximation is probably the digital signing of Java applets. Perhaps someday, computer systems will have a sense of self and will not execute foreign software.

Parasites also invade the human body. Some are harmful and others are normal. A tapeworm, for instance, may live in a human for some time without being detected. Only when the effects become noticeable is the tapeworm likely to be found. Computer systems have parasites too. They are usually called worms or Trojan horses. The same detection problem applies too. Even with access to the source code, it is extremely difficult to determine whether or not there is any malicious code in a piece of software. Just as in people, no amount of input checking will totally prevent the parasite threat.

OTHER THREATS

Staying healthy requires a constant effort throughout one's life. Strangely, though, people expect that once a

computer system is set up, it will stay secure forever. Cumulative threats may go undetected for a long time. People who live under power lines, have lead in their water, or have high blood pressure may feel great while slowly their health is slipping away. In computer systems, users may allow so much mail to accumulate in their mailbox that the server becomes unwieldy. Perhaps the administrator does not do a good job of removing old versions of software or unused user accounts. Slowly but surely, these systems become more and more likely to have security problems.

Humans are extremely susceptible to threats that promise a quick reward for dangerous behavior. In computer systems, these problems occur all the time too. Some people abuse drugs in order to satisfy a short-term need and some computer users use questionable software to get a quick technology fix. Also, while some people engage in sexual activity without the protection of a condom, computer users have a strong tendency to connect to untrusted networks without a firewall. Of course, neither condoms nor firewalls are perfect, and abstention is always an option.

A person's genetic code completely specifies a person, and may be the ultimate in correctness with a perfect mapping from the DNA formal model to the implementation. But some people are born with genetic disorders that can cause severe health problems. Cystic fibrosis eventually causes the lungs to become so clogged that the person can no longer breathe. So even a model that is perfectly consistent internally can have security holes. Can these computer security flaws be eliminated through natural selection? Perhaps someday we will figure out how to unleash the power of evolution to create self-protecting software, but that day is probably a long way off.

The current human design even has lots of error-correction and runtime error detection/termination built in. When genetic material is damaged, cells generally die, and there are mechanisms built in to perform active defense against error conditions. However, the defenses and mechanisms occasionally make mistakes and fail. Mainframe computers used to have extensive error detection and correction, and modern computers still have error correcting memory, but this type of mechanism is not as prevalent as it once was.

STAYING HEALTHY

Keeping healthy is a life-long endeavor, not something that people can do once. People need to exercise, brush their teeth, eat right, and take vacations in order to keep healthy. Keeping computer systems secure is also a continuous effort. We should start talking about computer security as a lifestyle or set of habits. Some good ones include performing preventative maintenance, configuration management, intrusion detection, and incident reporting.

Also, when people buy food, they are presented with a wealth of information about the ingredients, vitamins, minerals, and recommended daily

allowances. There is no similar source of computer information for the consumer. Information on the Internet should be accurately labeled according to its content, and software should come with information about the capabilities and vulnerabilities associated with its use. Warning labels for particularly dangerous products, like cigarettes, alcohol, Java, and Microsoft Word should also be provided to the consumer.

Although many human ailments are not yet curable many have treatments that can help ease the symptoms. For example, herpes infects one in six Americans, but is kept under control with medicines. Computer systems have similar problems. For example, files occasionally get corrupted during the course of normal use, but the problem is treatable with good backup procedures. When problems are found in a dental checkup, ignoring the problem almost always makes it worse. Similarly, we should drill out the problems in our computers and get fillings.

There are inoculations for many dangerous diseases. Many work by introducing an antigen or vaccine into the body so the immune system can learn to defeat it. This would be a good model for improving automated intrusion detection systems, if they were advanced enough to take advantage of it. For now, we can use computer security advisories to make sure that our systems are protected against known vulnerabilities.

HEALTHCARE INDUSTRY

People understand that healthcare is complicated enough that it's necessary to have specialists for particular aspects of medicine. You wouldn't hire an ear, nose, and throat doctors to do brain surgery, for example. This level of specialization is starting to arise in computer security, too. There are firewall experts, INFOWAR specialists, trusted operating system gurus, and certification and accreditation professionals. On the other hand, there are plenty of medicine men and snake oil salesmen with products and services that prey on the fears of people who don't understand the problem and are waiting for a miracle cure.

People have a variety of healthcare options. For minor accidents, a first aid kit or over-the-counter drugs will usually suffice. Often a self-examination can identify problems in time for treatment. For more serious illness or injury, a visit to the doctor is required. When the situation is severe or life-threatening, emergency services like 911, ambulances, and emergency rooms are available. Computer systems do not have a full range of security options.

The World Health Organization and the Center for Disease Control have established emergency response teams to help stop the spread of particularly threatening diseases. There are a few computer emergency response teams, such as CERT and CIAC, to help deal with attacks, but the statistics reveal that there are more incidents than they can handle. There are also a few over-the-counter programs to help diagnose

security, but few treatments. Children are not allowed to go to school unless they have had their shots. Perhaps it would be possible to make inoculation mandatory, so that only healthy computers could attach to the Internet. Or users could decide not to connect with untreated computers.

Medical science is making great progress in developing complex new drugs and therapies. Despite a lengthy testing process for new drugs, sometimes unexpected reactions occur when combined with other treatments. This situation is analogous to problems which occur when software patches are issued to fix problems with existing code. Many times, these patches introduce new unexpected problems when combined with other software. Recently a security advisory had to be released describing a security vulnerability introduced when running SATAN, a program designed to help security administrators find holes. Just as taking experimental or radical treatments is a risky business, so is the process of accepting software patches or using "beta" programs.

The healthcare world is approaching a crisis due to the overuse of antibiotics during the past few decades. The problem is that antibiotic resistant strains of diseases like tuberculosis and pneumonia have evolved. In some cases only a single antibiotic is still effective against these diseases. The threats to computer security are always evolving, changing, and adapting to countermeasures too. Recently, for example, polymorphic viruses have evolved to counter the virus scanners and hacking tools have surfaced to quickly find any chink in our protection mechanisms. We should never be complacent with our countermeasures.

CONCLUSIONS

We can learn a lot about securing complex systems by looking to evolution and medicine. From evolution, we should especially note the complex relationship between threats and protections. Currently, our protections are being overwhelmed by a sort of pre-Cambrian explosion of technological speciation. Many technologies are at risk of dying off due to their extreme vulnerability. We should keep looking for the technologies that are flexible and adaptable to the changing threat environment.

From medicine, we should note the dramatic rise in people's life expectancy in response to better diet and health care. People who were considered healthy 100 years ago could be considered high risk today. Technologies considered secure last year might be extremely weak today. Certainly the 56 bit strength of DES is no longer considered a strong choice. We should promote computer security wellness in addition to looking for new security technologies.

Of course, there are differences between the real world and cyberspace. For one, the physics are different. In cyberspace, objects can be duplicated perfectly and quickly and they can move at the speed of light. Allowing evolution to occur under the physical laws of cyberspace

would have different results than in the real world, where moving around and making copies is difficult and expensive. Nevertheless, it is still instructive to look at people's health and safety for models of security that have withstood the test of time.