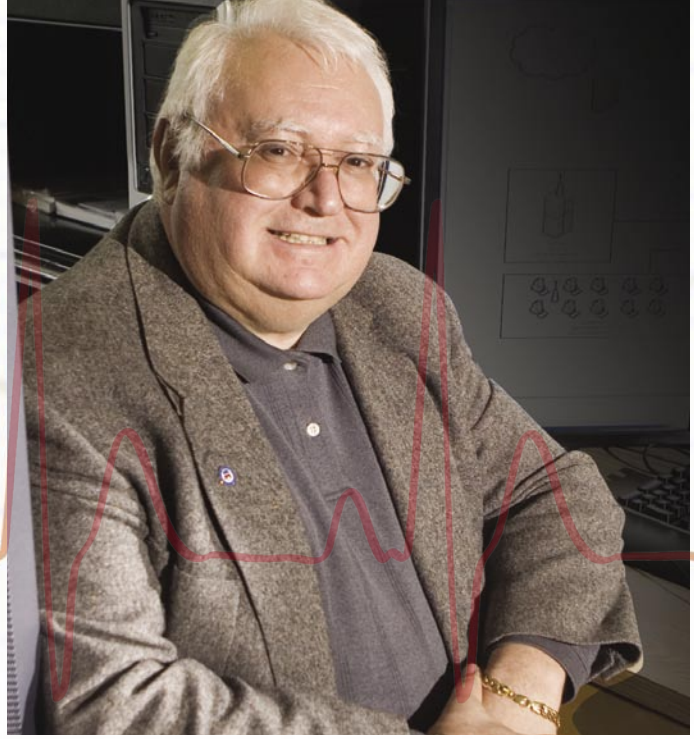
"When it comes to computer security, it's an arms race. Each time you come up with a new way to defend a computer network, the bad guys come up with a new way to attack it. This could go on forever."

— Victor Skormin



By exploiting the ability to self-replicate — generally a signal that software is up to no good — the new technique mimics the human body's response to a biological intruder and detects even previously unknown malicious software — or "malware."

Malware is an area of intense interest to the computing community worldwide, and for good reason. According to *Consumer Reports*, computer viruses did at least $5.2 billion in damage last year, or about $109 per individual victim.

The immune system-simulating malware-detection technique is the second spin-off of ongoing Binghamton research investigating biologically inspired methods in computer security. The first spin-off, a book titled *Immunocomputing*, won widespread acclaim for laying the mathematical foundation for applying immune methods in computing.

The Binghamton team is led by Distinguished Service Professor Victor Skormin, director of the Center for Advanced Information Technologies and a co-author of the book. It includes Associate Professor Douglas Summerville and doctoral students Alexander Volynkin and James Moronski.

"Victor is an innovator. He's very creative," said Joseph Giordano, computer scientist at the Air Force Research Laboratory in Rome, N.Y. "He's pushed this biologically inspired network defense thinking — and when you really come down to it, it's a new way of thinking."

The U.S. Air Force has already invested about $1.5 million in this research, and Skormin expects that figure will surpass $2 million in the near future. His long-standing relationships with the Air Force Office of Scientific Research and the Rome laboratory have laid the foundation for the partnership and helped boost Binghamton's profile in the area of information assurance.

"Malicious biological tissue has very specific malicious genes," Skormin explained. "A gigantic percentage of the genetic material in this tissue is the same as in healthy tissue, but it has some specific genes that make it malicious. This way of thinking led me to the concept of detecting the gene of self-replication in computer programs. It is very unlikely for a legitimate program to self-replicate. But a virus or computer worm self-replicates because it's the only way to create an epidemic that would maximize its destructive impact."

The functionality of legitimate software can be traced through so-called "system calls, " which enable different parts of

the computer system to communicate. Each system call has 40 attributes. Malware invokes the same system calls, but with different sequencing. Skormin sees amino acids as a parallel, in that typical cells and biological intruders have the same basic composition but are sequenced differently.

The Binghamton researchers looked at the combination of attributes to identify signatures that indicate the incontrovertible mark of malware: self-replication. They then created a program to monitor system calls and their attributes and alert the user if there are signs of self-replication. The user can decide to delete the program — or, if it's believed to be legitimate, to let it run.

The Binghamton team intends next to apply this idea to a network of computers. They are in the process of building a testbed that will emulate a large computer network with up to 2,000 hosts and a number of servers. They'll be able to deploy malware and other information attacks to investigate the proliferation of self-replicating software and assess its impact on the network. They'll also evaluate possible defensive mechanisms.

In essence, the Binghamton software will try to detect problems in individual machines and then report them to the server. "From the server level we will see the big picture, "Skormin said. "When you see the whole network reporting on attempts to self-replicate, this means that you will know if a distributed, evolving attack takes place."

The immune system provides an example of a distributed defense mechanism relying on highly specialized self-replicating "anti-viruses." Skormin and his team intend to replicate this approach in a computer network.

The immune system provides an example of a distributed defense mechanism relying on highly specialized self-replicating "anti-viruses." Skormin and his team intend to replicate this approach in a computer network. The trick at such a large scale will be spreading an anti-virus without exhausting the network resources; therefore, the key issue is the definition of a complex negative feedback mechanism governing this process.

Skormin and his team will begin with a limited-size network, but he's confident the approach has far wider applications.

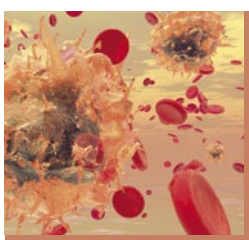
"Even the Internet could rely on this," he said.

Binghamton's researchers hope to find a corporate partner to help commercialize the technique. Skormin has also begun talks with Wall Street representatives who envision applications for the banking industry.

"The advantage of what we do is that we're not looking back into the history of known attacks," he said. "We're developing techniques that will help to oppose previously unknown viruses."

Giordano noted that the Air Force appreciates each of these innovations. "The way we are today in an information society, ideas get generated rapidly and we have the tools to experiment," he said. "Things like this may make it to the market sooner than we all think."

Skormin likes to joke that he and his team have excellent job security because there's such creativity on each side of the information assurance battle. "When it comes to computer security, it's an arms race," he said. "Each time you come up with a new way to defend a computer network, the bad guys come up with a new way to attack it. This could go on forever."■



In computer security, a computer virus is a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of a virus into the program is termed an "infection," and the infected file, or executable code that is not part of a file, is called a "host." Viruses are one of the several types of malicious software or malware. In common parlance, the term virus is often extended to refer to worms, trojan horses and other sorts of malware; viruses in the narrow sense of the word are less common than they used to be, compared to other forms of malware.

While viruses can be intentionally destructive, for example, by destroying data, many other viruses are fairly benign or merely annoying. Some viruses have a delayed payload, which is sometimes called a bomb. For example, a virus might display a message on a specific day or wait until it has infected a certain number of hosts. A time root occurs during a particular date or time, and a logic bomb occurs when the user of a computer takes an action that triggers the bomb. The predominant negative effect of viruses is their uncontrolled self-reproduction, which wastes or overwhelms computer resources. — From *Wikipedia*