SC MEDIA THE CYBER-SECURITY SOURCE

by Stephanie Forrest
February 23, 2017

Biology and computers: drawing parallels between immunology and cyber-security

Stephanie Forrest discusses the parallels between computer viruses and biology and how our understanding of them is informing cyber-security.

Malicious behaviour arises spontaneously in a wide variety of complex systems, ranging from diseases in humans to bullying in social systems to cyber-security attacks. It is likely that there are common principles underlying the role of attacks and defence across these different systems.

Focusing on biology, it is relatively easy to make generalisations about the similarities of computer viruses and the viruses that infect our bodies, but many of us don't recognise just how much we can learn by thinking more deeply about the biology. Let's explore some of the parallels between these two systems and how our understanding of these parallels is informing cyber-security. The vertebrate immune system – possibly the most complex defence system ever devised – provides many important clues about how to design a successful defence system for computers.

Behaviour-based intrusion detection

A key capability of the immune system is its ability to recognise dangerous novel foreign pathogens and control their damage. At the same time, it must also avoid attacking the body, known as "self," in what is known as autoimmunity. This process serves a function remarkably similar to intrusion detection and response systems in computers. In order to succeed, nature needed to discover how to define self – the normally occurring cells and molecules in the body in such a way that self can be distinguished from outside infiltrators. Similarly, in a computational setting, programmers face the challenge of identifying an appropriate data stream to distinguish normal from abnormal behaviour.

Defining self in computation is challenging. We require that the monitored data be stable under normal behaviour and routine changes, eg, software patches, while being unstable during attacks. Stable behaviour provides a model for normal operative function, and a common choice is short sequences of system calls that are issued or requested by executing programs.

In biology, short sequences of amino acids, known as peptides, play the role of system calls in a computer security system.

Managing false positives

There are two common flavours of intrusion-detection systems: anomaly or behaviour-based systems, and signature-based systems. As it happens, the vertebrate immune system uses both strategies, relying on anomaly detection to identify novel pathogens (zero-day attacks), and on signature detection to respond quickly and aggressively to previously seen threats. This second system is known as the secondary response, and it is the reason that we only become ill from diseases like measles once, regardless of how many times we are exposed.

Not all anomalies correspond to attacks, and this is a challenge for both biological and computational systems. These are referred to as ”false positives” in computer security and autoimmunity in biology.

Controlling autoimmunity appears as a major challenge for immunology, and there are many mechanisms that reduce the risk that the immune system will accidentally attack its own body. Of these, one of the most interesting are second signals. In many cases a single immune detector cannot be activated if it notices a foreign pattern, unless it receives a second confirming ”this is real” signal, say from a helper T-cell. This provides an important check on the immune system. Finally, immune responses are not completely binary go/no go decisions, but rather, they use a graduated approach, stepping up the response as the threat increases.

As an example of how this can be implemented computationally, a security monitoring system notices an anomaly, so it delays the subsequent system calls from that same program, slowing down the computational process and alerting the system administrator to the issue. The system admin acts as the second signal, either confirming or ignoring the alert before the system can make any dramatic changes.

Future challenges

All systems, be they natural or technological, can fall prey to malicious behaviour. And as systems become more complex, it is more likely that malicious behaviour will evolve inadvertently. Just look at antibiotic-resistant bacteria: large populations of bacteria have evolved to evade the protection of antibiotics. Taking cues from biological defence systems now can help us understand and anticipate the problems we will likely face in the future.

Moving forward, we need to look at natural systems that have successfully evolved defences and restraints on malicious behaviour. By understanding how those defences developed, we can then apply those valuable insights to build better defences in our computing systems.

Contributed by Stephanie Forrest, professor, University of New Mexico, and member, Association for Computing Machinery (ACM)

Topics:

- Behaviour
- Defence

- Threat