Editorial: *From Editor-in-Chief*
Tackling the Threats of Internet Worms

Computer Worm is a kind of malicious program that self-replicates automatically within a computer network. Again, Internet is defined as a network of networks. This is the reason why computer worms do not reside only within one computer or a single network but rather get spread all over the Internet whenever it is possible during computer-to-computer communications. The reality of today's Internet is that the worms pose a major threat to the Internet infrastructure security. This is also understood that destruction of worms is not an easy task either and often very expensive. Multiple network devices and preventive mechanisms should be in place to hold appropriate defense at each step the communications are done through.

There are various ways how the worms can spread over the Internet. They can exploit low-level software defects, operating system weaknesses, improperly configured servers, can use their victims for illegitimate activities; such as corrupting data, sending unsolicited electronic mail (i.e., email) messages, generating traffic for distributed Denial of Service (DoS) attacks, or stealing information, and so on. Today, the speed at which the worms propagate poses a serious security threat to the Internet.

Among various types of worms, polymorphic worm is considered the worst. Polymorphic worm is a kind of worm that is able to change its payload in every infection attempt. This deceptive quality of the worm makes it capable of evading many of the existing Intrusion Detection Systems (IDSs), and damage data, delay the network, cause information theft, and other illegal activities that lead to even for example, high financial loss. If a government network or military network infrastructure is affected by worms, this can cause real havoc to the nation's interest and national security.

To defend the networks against the worms, Intrusion Detection Systems (IDSs) such as Bro and Snort are commonly deployed at the edge of network and the Internet. The main principle of these IDSs is to analyze the traffic to compare it against the signatures stored in their databases. A signature in this case is defined by a pattern (or, the most frequently occurring byte patterns in multiple instances of the worm) that an IDS looks for when scanning files or network traffic.

Whenever a novel worm is detected in the Internet, the common approach is that the experts from security community analyze the worm code manually and produce a signature. The signature is then distributed and each IDS updates its database with this new signature. For detecting future worm attacks, this stored signature is usually used. Such approach of manually creating signature is time consuming, requires huge efforts, often very slow and when we have threats of very fast replicating worms (that take as small as few seconds to bring down the entire network) like zero-day polymorphic worms (*zero-day* means never seen before!), the need of an alternative is recognized. The alternative approach is to find a way to automatically generate signatures that are relatively faster to generate and are of acceptable good quality.

Very little works have been done in this particular area. In fact, due to the nature of "*unpredictability*" and "*unknown event*", designing a robust mechanism to handle zero-day polymorphic worms automatically is a very challenging task. As long as the concepts of network and associated software vulnerabilities remain with current infrastructure, it is possible to get affected by worms; be it polymorphic or not. The next generation networks (NGN), Future Internet (FI), Internet of Things (IoT), Cloud computing, Pervasive or Ubiquitous computing, all these technologies may face the same challenges from worms. In fact, the companies relying on Cloud concepts to provide various computing resources as services, may face serious damage if worms infect the Cloud servers and bring them down. Like the past and the present, future would also be seeing the spread of different kinds of Internet worms.

This is an open area of research. Numerous aspects of various kinds of worms and their impact on today's and future networks should be more thoroughly investigated. No matter what is available to the research world or as solution from the software or network solution providers, the threats of innovative kinds of worms would exist as long as malicious programs are written either for fun, challenge, adventure, or criminal purposes. The best defense against such threats is awareness and constant engagement with the network's security mechanisms that may need up-gradation on a regular basis.

Al-Sakib Khan Pathan
Department of Computer Science
International Islamic University Malaysia
Kuala Lumpur, Malaysia
sakib.pathan@gmail.com , sakib@iium.edu.my