Discussion

Paul Barford

Q: How diverse are cyber attack targets and does this diversity have an impact on corresponding defense mechanisms?
A: The primary targets for attacks today are MS Windows hosts. This is due primarily to their prevalence and also to the number of reported vulnerabilities. However, there are an increasing number of alternative devices that are end hosts (e.g. cell phones and other mobile devices), and these pose a formidable challenge for security analysts in terms of developing countermeasures.

Q: Once a malicious host has been identified, can active defenses (i.e. attacking the attacker) be used effectively?
A: There are two separate schools of thought on this issue - one that attacking *is* a good idea and the other that it *is not*. I do not believe that active attacks are a good idea since they can introduce a large amount of additional traffic into the Internet, and I do not believe that they will ultimately be effective since in general, systems used in attacks are used without the owner's knowledge.

Q: Much of what appears to be done in terms of network security and defense against cyber attacks appears to be ad-hoc. Are there possibilities for establishing more of a theoretical basis for cyber security?
A: This is exactly what we have been thinking about recently. I think that our game-theoretic formulation of honeynet mapping is a step in this direction. But, I think that considering this problem from first principles is a good idea, and we are currently considering multiple possible approaches.

Q: Are there possibilities for applying defense mechanisms borrowed from micro-biology/virology/immunology to the problem of cyber security?
A: It turns out that this has been an idea that has been around for some time, and the reason for the term "computer virus." The seminal paper on this idea was written by a group from New Mexico in the mid 1990's, and it treats the problem of determining self versus non-self. While it is unclear to me that this approach has led to any significant improvements in cyber security to date, I believe that this model is powerful and needs to be revisited, e.g,. within the context of our Malcode Genome Project.

Brian Witten

Q: What percentage of resources on a computer are devoted to security?
A: Customers generally prefer that anti-virus and other security software consume less than 5% of CPU cycles.

Q: What do you think is the current state of financial risk analysis in computer security?
A: Most organizations have not calculated the kinds of financial harm that can be done to them through their network. When organizations do identify ways that financial harm can be done to them through their network, calculate the potential level of harm in financial terms, and project the likelihood that someone might attempt and succeed in

doing such harm to them, they often make very substantial investments to protect against such harm

Q: Which vector(s) of computer security research do you think will make the biggest difference in the five-year time frame?
A: I think the "move/counter-move" evolution will continue producing increasingly effective anti-virus, anti-spyware, anti-spam, and anti-phishing technologies as threats continue increasing in sophistication, but I also think that many of the new foundations such as trusted computing hardware and virtualized security systems will be making tremendous contributions within five years as well.

Q: Will we need new systems for more effective protection of healthcare data, such as human genome data and personal genetic profiles, or will the current systems be good enough?
A: Healthcare data has very important privacy and accuracy concerns. People have died from tampering of computerized pharmaceutical records. There has been legislation passed recently which helps address some of these concerns. Fortunately, such legislation has taken a very constructive approach by identifying the information that needs to be protected and providing context for the levels of protection that are needed without prescribing technologies since both the technologies and threats will continue to evolve. Such legislation helps by motivating both deployment of existing stronger technologies and development of technologies to fill critical gaps. Existing technologies that could be deployed more broadly to continue increasing accuracy and privacy of medical information include encryption, strong authentication, stronger operating systems, and larger scale storage systems to facilitate greater record retention for greater accountability.

Q: Is it useful to design computer systems that may have many purposely created "security holes" that can be used to fool attackers?
A: Most systems have more than enough holes already, and sometimes it's possible to start watching the holes as soon as they're found, even if creating the "patch" to fill the hole takes a bit longer. By using this approach of watching unfilled holes right away, it's possible to detect previously unseen threats on a large scale. Generally, fooling an attacker to trap them or learn more about them does not have much value unless the number of attackers can be limited in some sense. As operating systems become increasingly secure, virtual security systems increasingly effective, and hardware supported cryptography grows in use, this may make it harder for many adversaries to continue breaking systems. If so, that might reduce the number of potential attackers such that such strategies become increasingly effective. However, leaving legitimate systems vulnerable would be far more dangerous than introducing intentionally vulnerable decoys that are not operationally needed except for security purposes.

Youki Kadobayashi

Q: Do you have any approaches against phising threats?
A: We have several approaches toward a trusted Internet, such as identification of malicious activities, which will be good for phishing as well.

Q: Some detection schemes require some time to compute. Is real-time detection significant?
A: We have some monitoring systems with a very quick response.

Q: If malicious people learn the logic for identification, is it possible they may spoof the way to perform port-scans? How do you address the “arms-race” of tricks?
A: We have some ideas, which we are not ready to make public.

Keisuke Takemori

Q: How do you determine legitimate access from malicious access?
A: The addresses of our sensors are not available on the Internet, thus all access to our sensors may be malicious.

Q: There are many virus-infected PCs on the Internet. Can an ISP isolate the infected PCs?
A: Japanese ISPs can not isolate infected PCs automatically because of a communication law that restricts ISP operations. The isolation technique is called quarantine service. The users need to apply for quarantine service for their PCs or detect anomalous status themselves.

Q: The rate of correctly predicting attacks is low. How do you improve this rate?
A: Conventional techniques monitor only two attack parameters – those that suggest a cyclic and an expansive pattern. We should collect vulnerability information and put proven ones on many networks.

Q: The ISPs collect incidents and share these among themselves. How do you plan to construct an incident-handling system for users?
A: The telecom-ISAC Japan has an incident-handling scheme for ISPs, but the information is only available for network operations. We should modify incident formats and make them available to users.

Q: The users and the ISPs should cooperate with each other to guard network systems. Please talk about ISP plans to make the Internet secure.
A: It is necessary for users and ISPs to cooperate. The ISPs have some plans to protect both user PCs and network systems. For example, ISPs research and develop user-based defense tools and release them, and people need to use those tools to protect their PCs.