GAME THEORY AND NETWORK SECURITY

POSITION PAPER FOR DARPA WORKSHOP ON GAMBIT (GAME THEORY INFORMATION TECHNOLOGY)

João P. Hespanha

University of California at Santa Barbara

The basic principle behind the design of the Internet was to utilize massive redundancy to achieve fault tolerance. With this, one expected to achieve *network security*, i.e., robustness with respect to attacks to its infrastructure. With several decades of hindsight, it is now clear that fault tolerance and security are quite different concepts and, although fault tolerance has been largely achieved, we are a long way from making such a claim in the network security area. In fact, there is a pervasive feeling that, as they grow, computer networks are increasingly more vulnerable to attacks.

The distinction between fault-tolerance and security is well understood in the context of mathematical games: The former can be viewed as a game against chance (usually a benevolent player), whereas the latter can be viewed as a game against an adversary with a private agenda. Unfortunately, an adversary is often able to explore weaknesses that chance would not easily find. In other words, a complex sequence of faults would almost certainly not occur by accident but can often occur if prompted by an attacker.

We believe that network security is potentially one of the next "Killer Apps" for game theory in the context of information technology. We support this by the following two observations:

1. Communication networks are extremely vulnerable components to any critical system. This vulnerability stems from the fact that they are composed of a multitude of individual components, inherently spatially distributed and therefore difficult to protect. This is particularly extreme in the case of wireless networks where the communication medium cannot be contained and is especially susceptible to jamming, eavesdropping, battery drainage due to overuse, etc. Note that, although the war-fighter could greatly benefit from ad-hoc wireless networks, they are highly susceptible to attacks and currently are not sufficiently reliable to be trusted in life threatening situations. As argued above, by itself, redundancy does not solve these problems, as one can infer from the large number of successful attacks that almost routinely occur in (highly redundant) public (and even some private) communication networks.

2. Game theory is a natural framework for network security. In the context of network security, it would be naïve to regard faults as random events. Moreover, when prompted by an attacker, very unlikely events can occur. E.g., the Internet was designed to reconfigure itself when a network switch "dies," and automatically route packets around the faulted computer. This reconfiguration occurs at the network layer of the protocol stack and is triggered because the switch stops responding to its immediate neighbors. However, if the switch actually does not "die" but instead is infiltrated by an attacker, it may still respond to its neighbors (to prevent being excluded from routing) and yet not forward data packets.

In the context of fault-tolerance, it would seem extremely unlikely that a switch would stop transmitting data packets and yet consistently reply to routing packets, so nothing was done to account for this possibility. The result is that currently in most networks this needs to be manually detected and corrected. See references below for a game-theoretic approach to address this and other shortcomings of current routing algorithms.

Once a potential “Killer App” was identified, one should ask what the critical challenges that need to be overcome are to make it emerge. We see three critical issues:

1. Scalability: The vulnerability in a communication network arises from its size. Therefore, any solution to network security is only useful if scalable.
2. Speed: Attacks to computer networks take place in “machine-time.” This calls for proactive defense mechanisms, where the possible actions of an attacker need to be taken in consideration ahead of time
3. Legacy/backward compatibility: This is perhaps the most difficult challenge that the designer of new secure network protocols must face. In some cases one may need to “bite the bullet” and replace the protocols in networks that one wants to make secure.

One should also note that many of the observations made here can be applied to other networks where security is a major concern. These include, e.g., power distribution networks, supply networks, transportation networks, etc.

References

[1] Stephan Bohacek, João Hespanha, Katia Obraczka. Saddle Policies for Secure Routing in Communication Networks. Feb. 2002. Submitted to the 41th Conf. on Decision and Control.

[2] João Hespanha, Stephan Bohacek. Preliminary Results in Routing Games. In *Proc. of the 2001 Amer. Contr. Conf.*, June 2001.

[3] Stephan Bohacek, João Hespanha, Junsoo Lee, Chansook Lim, Katia Obraczka. NS-Evaluation of Secure Stochastic Routing. Technical Report, University of California, Mar. 2002.

These and related references are available at:

http://www.ece.ucsb.edu/~hespanha/published.html#3.CommunicationNetworks

http://www.ece.ucsb.edu/~hespanha/techreps.html#3.CommunicationNetworks