

Title: A Trust-based model for Collaborative Intrusion Response

Name: Kapil Singh and Norman C. Hutchinson

Abstract

Intrusion detection systems (IDS) are quickly becoming a standard component of a network security infrastructure. Most IDS developed to date emphasize detection; response is mainly concentrated on blocking a part of the network after an intrusion has been detected. This mechanism can help in temporarily stopping the intrusion, but such a limited response means that attacking is free for the attacker. The idea behind our approach is to frustrate the intruder by attacking back. This requires developing a sense of trust in the network for the attacked host and establishing proof of the attack so the attack-back action can be justified.

To develop this trust model, we propose a protocol that makes use of encryption and digital signatures over the network logs. The protocol allows the attacked host to prove to the attacker's edge router that it has been attacked. The model is quite flexible and based on the level of trust developed for the host, an appropriate countermeasure is taken. Besides attack-back, other possible responses could be blocking a part of the network and use of network puzzles to limit the attacker's access to network resources.

Once the host is suspicious that it is being attacked, it uses the Sleepy Watermarking technique to trace the intrusion connection chain back to its origin and informs the routers to start monitoring this traffic chain. When the host is convinced that it is under attack, it sends its enriched logs in an encrypted form to the attacker's edge router. The router, in turn, compares its own logs against the received logs to decide on the appropriate response. The logs of the attacked host's edge router can also be used to improve the trust level.

We believe that the attack-back approach would certainly demoralize novice attackers, and even expert attackers will think twice before attacking again. Also, the protocol prevents a host from faking that it has been attacked. We are building a system that can handle a majority of already known attacks (signature-based). We are also exploring the idea of adding a third trusted party into the system in order to provide countermeasure action for novel attacks (anomaly-based).