FLAIRS-30 Poster Abstracts

Zdravko Markov and **Vasile Rus**

Editors

Distributed Trust for Intrusion Detection

Timothy Atkinson, Marius C. Silaghi
(Florida Institute of Technology, USA)

When we consider the typical approach to how a computer trusts another computer, the trust is either complete for the given action, or there exists no trust at all. Namely, either an authentication process based on passwords, keys or some other cryptographic mechanism succeeds, and all the corresponding service is provided for as long as the client is connected; or no information is provided and the client/attacker can try again, until some hard-coded rules are met and the peer is black-listed. If the computer at the remote end has been compromised, no amount of certainty given by the authentication protocol can protect the local machine. Further, if the local machine has some critical resource the hacker is trying to gain access to, then disconnecting the remote machine may be the only mechanism available to prevent it from identifying a vulnerability in the local machine. The question we address is to dynamically evaluate reliability as a probability of trustworthiness for a computer's communication channels and hypothesize if that communication channel has been compromised in a network unknown to the agent. A computer can decide to offer services and information according to the probabilities assessed. Namely, one can restrict dynamically the channel to block or disconnect it when the value of the information provided is lower than the perceived risk to the local machine. To that end we develop dynamic trust re-evaluators based on belief networks, and linked in a network of probabilistic measurements, that do not fully trust each other.