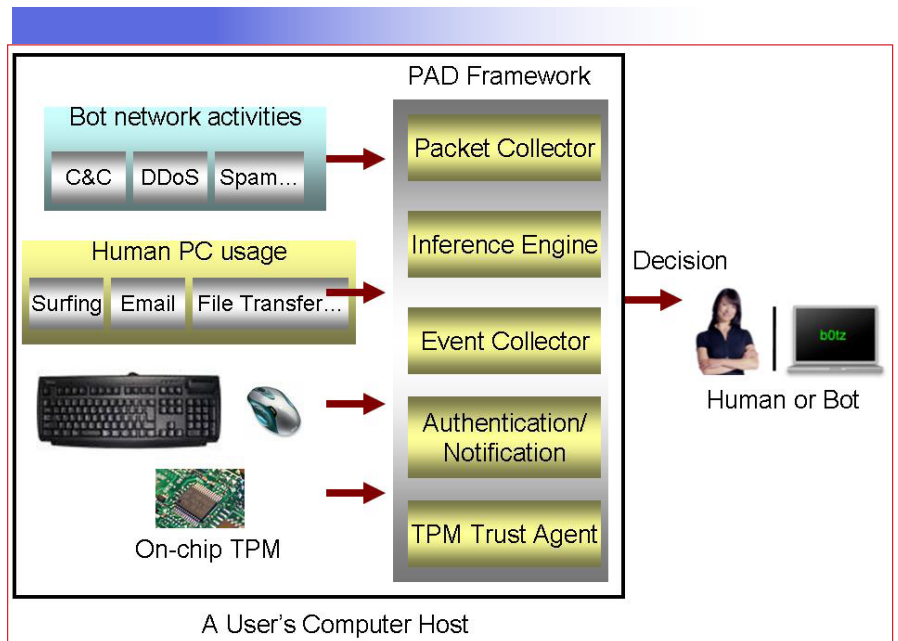


Contact: Robert Gruetzmacher, Ph.D, CLP
Office of Technology Commercialization
Rutgers, The State University of New Jersey
3 Rutgers Plaza, ASB III, 3rd Floor
New Brunswick, NJ 08901
Cook Campus: 732.932.0115 x3010
email: gruetzrr@oct.rutgers.edu

Rutgers Inventor:
Danfeng Yao, Ph.D.
Department of Computer Science

Rutgers Technology #: 09-046



Robust Keystroke Authentication and Input-Traffic Correlation Analysis for Accurate Bot Detection

Invention Summary: Our security technology aims to detect a compromised personal computer by monitoring and analyzing the characteristic human behavior patterns of the PC owner. A Personalized Anomaly Detection (PAD) system was developed that is able to adapt to future generations of malware and provides a robust security shield for networked computers.

PAD extracts and learns the PC owner's web activities and input behaviors. Main features include: (1) collecting and analyzing keystroke dynamics of the human user in a client-server architecture, and using the typing patterns as a biometric for detecting anomalies including bot infection; (2) providing a lightweight cryptographic verification mechanism to ensure the integrity of PAD detection operations and prevent the injection of fake input events; (3) providing a technique for detecting backdoor bot traffic through the correlation analysis between the input events and network packets; (4) providing a lightweight cryptographic detection method that identifies abnormal execution of network stack calls (these types of calls are typically used by bots and rootkits).

Market Application: Our technology realizes an advanced and robust firewall. It can be deployed to

remotely monitor computers in an organizational network. It can also be sold as stand-alone security software to individuals.

Advantages: Virtually all the state-of-the-art bot solutions are based on finding botnet communication characteristics, which fail to be effective when botnet patterns are even slightly altered. The advantage of our technique is that it focuses on human-user characteristics, versus those of malware, allowing computer security to be realized without the need for continually monitoring ever-changing malware patterns. This approach complements conventional malware-detecting techniques based on code analysis, data mining, or network trace filtering. Our design involves a unique and tamper-resistant traffic-enforcement framework that cryptographically verify the provenance information of both system and application-level data utilizing on-chip hardware support.

Intellectual Property & Development Status: A provisional patent application has been filed.