Abstract

Malware is the intrusive program that affects computer operation and sensitive information of the host system. The objective is to protect such data and prevent malware from injecting fake keystroke into host network stack. The new technique cryptographic provenance verification [CPV] uses a property known as data provenance integrity which improves the trustiness of the system and its data. The system security is enhanced at kernel level. CPV makes use of trusted platform module for detection of fake key stroke. With TPM operating system can identify malware initiated network calls. The propose system consist of two modules sign and verify which prevent tampering of data. Sign module generates signature for outgoing packets from application layer. The packets are encrypted with advanced cryptography algorithm at transport layer and send to verify module along with communication key. Verify module decrypts the received packets and verify them for being malicious. TMP is used for secure key storage which prevents malware from injecting fake keystrokes.
Data Provenance Verification for Secure Hosts using Advanced Cryptography Algorithm

- D. Stefan, C. Wu, D. Yao and G. Xu. Ensuring host integrity with cryptographic provenance verification. In CCSS 09, poster, November 10-12, Chicago, IL, USA, 2009.

Index Terms

Computer Science  
Security
Keywords

Data provenance  keystroke integrity  message authentication  malware attacks
advanced cryptography
universal hashing
trust platform computing.