GW | Office of Technology Transfer

Novel Technology Opportunity Available
Non-confidential summary

CC-Hunter: Microarchitecture-Level Framework and Method for Covert Timing Channel Detection

Inventors: Prof. Guru Venkataramani, Jie Chen, PhD candidate, Department of Electrical Engineering and Computer Engineering, The George Washington University

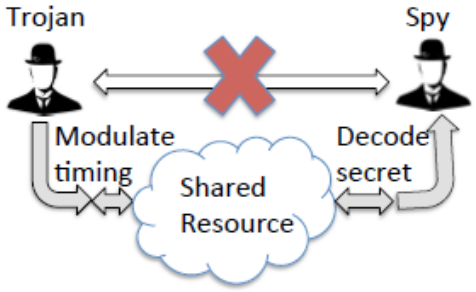
Field
Computer Science, Information Security

Objective
Seeking development and licensing partners

Keywords
Cyber security, Covert timing channels, Shared hardware, Cloud computing, Hacking, Trojan, Spy, Information Security

Researchers at The George Washington University have created a microarchitecture-level framework, which implements novel methods and algorithms developed for the detection of hacking covert timing channels that are used by Trojan/spy processes in order to leak confidential information from computing environments relying on shared hardware.

Information leakage from shared hardware is a rapidly growing problem. Cloud computing is highly vulnerable to covert timing channels, which are "insider threats", i.e. illegitimate communication channels established between a Trojan and a spy process via timing modulation to leak information undetected. Trojan processes with higher privileges intentionally subvert system security policies to illegitimately transmit confidential information to a spy process with lower access privileges. Covert timing channels are notoriously hard to detect because they leave no physical trace of an attack having taken place. CC-Hunter is designed to limit damage arising from such extremely stealthy, insider attacks where sensitive user information could be exposed to malicious parties. CC-Hunter can detect those covert channels by tracking conflict patterns dynamically on shared hardware during program execution. This novel conflict pattern detection allows the recognition of illegitimate communication channels even if the Trojan and spy programs change their communication protocols dynamically to avoid detection.



The existing technologies try to reduce the risk of timing channel attacks by constraining data bandwidth or minimizing resource sharing, which is quite inefficient because these techniques affect the overall system performance dramatically. CC-Hunter overcomes this issue by detecting covert channels without limiting resources. It also includes a novel pattern clustering algorithm to detect covert timing channels even at low bandwidths or in presence of noise signals. Experiments have demonstrated that CC-Hunter is able to efficiently detect many types of covert timing attacks at varying bandwidths and message patterns, with zero false alarms.

The CC-Hunter framework is a powerful innovation in the field of Cyber Security with an enormous commercial potential in a growing number of computing environments based on shared hardware, such as cloud computing. It safeguards sensitive information and communications from malicious hackers.

Applications:

- Cyber-security in cloud computing
- Covert timing channel attack detection
- Improved security on servers shared by multiple user and processes
- New cloud-based systems and online services relying in confidentiality such as e-commerce

Advantages:

- Implementation of a groundbreaking method for a dynamic detection of covert timing channels, Trojans and spy processes communications
- System performance, it avoids interfering with system performance as existing technologies do
- It provides capability to detect illegitimate communication at varying bandwidths

Patent Status: Provisional Patent Application Filed

Contact:
Gus Williamson, Licensing Associate
Tel: +1-202-994-8975
Email: gwilliamson@gwu.edu