Multi-level Information Security in Information Flow Tracking

Tech ID: 23222 / UC Case 2013-209-0

BACKGROUND

Information flow tracking (IFT) is a frequently used technique for enforcing IFC. IFT associates a label with data, and monitors the propagation of this label through the system to check if sensitive data leaks to an unclassified domain or if integrity-critical components are affected by untrusted data. With more functional units, such as security primitives, being built into hardware to meet performance and power constraints, it is required that embedded security be enforced from the underlying hardware up. In this process, hardware assisted IFT methods have been deployed to capture harmful flows of information including those through hardware specific timing channels. Implicit flows resulting from these timing channels have been shown to leak secret keys in stateful elements such as caches and branch predictors. In addition, such timing flows can cause violations in real-time constraints, hindering real-time operations of a system or even rendering the critical system useless. Further, these channels are so hard to detect that they are usually identified only after operational critical security policies have been violated.

Critical embedded systems such as those found in the military, industrial infrastructures and medical devices all require strict guarantees on information flow security because of the extremely high cost of a failure. These systems require rigorous design and testing to ensure that untrusted information never affects trusted computation or that secret information never leaks to unclassified domains. The requirements, for both integrity and confidentiality, can be captured by the formal model of information flow security.

TECHNOLOGY DESCRIPTION

To allow full account for information flow security in critical systems, researchers have proposed Gate-Level Information Flow Tracking (GLIFT). GLIFT monitors all digital information flows by tracking individual bits through Boolean gates. At such a low level of abstraction, GLIFT is able to capture all transition activities including register to register timing. As a result, all digital information flows are made explicit, including timing channels that are inherent in the underlying hardware implementation but invisible to programmers.

Previous work has illustrated the employment of GLIFT for building verifiably information flow secure high-assurance systems. GLIFT has been shown to be effective in detecting timing channels in bus protocols such as I2C and USB.

Although GLIFT provides an effective approach for enforcing information flow security, the existing GLIFT method targets a two-level linear security lattice and thus only considers two-level security labels, e.g., trusted < untrusted or, the dual, unclassified < confidential. However, most systems benefit from or require multi-level security (MLS). For example, data objects are usually classified into at least four security levels, namely Top secret, secret, confidential and unclassified in military systems. A two-level linear security lattice simply cannot be used for modeling such a policy. In addition, many systems tend to be interested in non-linear lattices for modeling security policies.

For example, it is often desirable to have a policy which requires isolation of the highest security level (Top Secret) from several incomparable entities (e.g., Secret US and Secret UK). That is, the model specifies that Secret US and Secret UK are at the same level but represent two different objects. More specifically, Top Secret might be the label for a data encryption process which requires that Secret US and Secret UK learn nothing other than the cipher-text while it is perfectly secure for processes Secret
US and Secret UK to learn information about one another. Thus, there is a need to expand GLIFT to more general security lattices in order to adapt to a wider range of systems.

CONTACT
University of California, San Diego
Office of Innovation and Commercialization
innovation@ucsd.edu
tel: 858.534.5815.

OTHER INFORMATION

CATEGORIZED AS
- Computer
  - Security

RELATED CASES
2013-209-0

Given here is an advancement of the GLIFT binary security model, enabling multi-level security for information flow tracking systems built into the hardware level.

This model classifies data objects in a system into different security levels, tracks the flow of information between security domains, and enforces a specific security policy such as non-interference. While non-interference is a strong and useful security policy, it requires tight information flow control (IFC) to prevent unintended interactions between different system components resulting from harmful flows of information.

APPLICATIONS

Industries that require security (trusted platforms, secure storage, network devices, etc.) and/or integrity (real-time operating systems, critical embedded system controllers, etc.) stand to gain the most from this technology. Even automobile OEMs will require secure systems, now that all new vehicles are controlled by dozens of embedded microcontrollers. A very high demand for this technology is anticipated, as it is the first tool in the industry to formally validate security and integrity properties spanning across hardware and software, enabling more efficient solutions while maintaining system integrity.

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	10,083,305	09/25/2018	2013-209

University of California, San Diego
Office of Innovation and Commercialization
9500 Gilman Drive, MC 0910, ,
La Jolla,CA 92093-0910

Tel: 858.534.5815
innovation@ucsd.edu
https://innovation.ucsd.edu
Fax: 858.534.7345