International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Survey on Integrity Protection Mechanisms for Open Mobile Platform

Alankrita Ladage[1], Prof. T. H. Gurav[2]

[1]Computer Engineering Department & Pune University, India
[2]Computer Engineering Department & Pune University, India

***Abstract**: To effectively achieve integrity protections goals while respects the constraints of mobile computing environment, A Simple and Efficient but yet effective solutions for integrity of real world cellular phone platforms. Our mechanism is based upon information flow control. Our goal is to prevent software-based attacks from application level. Our major objective is to prevent platform integrity compromising from user installed applications. We can prevent major types of attacks towards system integrity through mobile malware.*

Keywords: Integrity protection, SEIP, Mobile computing

1. Introduction

As in these days' mobiles are handy devices to use for computer application like internet surfing, downloading songs, video etc. Mainly computer security is concerned with three aspects: confidentiality, integrity, and availability.

1. **Confidentiality:** Preventing unauthorized users from gaining access to critical information of any particular user.
2. **Integrity**: Ensures unauthorized modification, destruction or creation of information cannot take place.
3. **Availability:** Ensuring authorized users getting the access they require

Organizations implement security in accordance with their needs. An organization creates a security policy and uses security mechanisms to enforce the policy. A security policy is a statement that partitions the states of the system into a set of authorized or secure states and a set of unauthorized or unsecured states. The goal of an information system is to control access to the subjects and objects in the system. A security policy governs a set of rules and objectives needed by an organization .Like this person using mobile also needs a security. With the increasing computing capability and network connectivity of mobile devices such as cellular phones and smartphones, security of these devices has gained extensive attention due to their increasing usage in people's daily life.

Existing research on mobile device security mainly focuses on porting PC counterpart technologies to mobile devices, such as signature- and anomaly-based analysis. Anomaly based detects the abnormal behavior in the computer systems and computer networks. The deviation from the normal behavior is considered as attack. Signature based matches the signatures of already known attacks that are stored into the database to detect the attacks in the computer system. The integrity of a process is determined simply by where it gets its input. If a process reads user data, or data off of an untrusted network it is considered low integrity.

2. Literature Survey

This section provides a description of some of the integrity protection approaches followed in both the enterprises and the research community.

A. BIBA

Biba [5] is a hierarchical integrity policy, similar to Bell LaPadula but, interestingly, the exact opposite. It allows processes to both read and write to objects of the same integrity, no surprises there. Next it allows high integrity processes to write to low integrity objects, but not read them and last it allows low integrity processes to read high integrity objects but not write them. Though the use of Biba is very limited and has never hit a mainstream operating system it is a very good practice, if implemented in a usable way. The standard SELinux policies implement something between Biba and 'least privilege', with a nice balance to ensure system integrity without making the system completely unusable. Biba, for example, isn't very flexible. Since processes and objects are simply labelled with their integrity there is no way to make practical changes to the policy. You either fall within the constraints of Biba or you are entirely MAC exempt.

The SELinux Apache policy doesn't allow Apache to write to the high integrity files we talked about above (/usr, /lib, /bin, etc) while allowing it to write to its logs, its cache, etc. Since objects in SELinux have fine grained labelling we can restrict access to apache high integrity objects, such as apache modules, the apache configuration and so on. In many ways SELinux lets us constrain applications more than Biba while at the same time making practical exceptions when necessary. This brings me to my next kind of security.

B. CW-LITE

The Clark-Wilson integrity model provides a different view of dependence [7]. Security-critical processes may accept low integrity information flows, but the program must either discard or upgrade all the low integrity data from all input interfaces. The key to eliminating dependence on low integrity information flows is the presence of filtering interfaces that implement the discarding or upgrading flow integrity data. The Clark-Wilson integrity model does not

distinguish among program interfaces, but treats the entire security- critical program as a highly assured blackbox. As a result, all interfaces must be filtering interfaces.

C. CLARK –WILSON

The Clark-Wilson model[3], published in 1987 and updated in 1989, involves two primary elements for achieving data integrity the well-formed transaction and separation of duties. Well-formed transactions, as previously mentioned, prevent users from manipulating data, thus ensuring the internal consistency of data. Separation of duties prevents authorized users from making improper modifications, thus preserving the external consistency of data by ensuring that data in the system reflects the real-world data it represents.

The Clark-Wilson model differs from the other models that are subject and object oriented by introducing a third access element programs resulting in what is called an access triple, which prevents unauthorized users from modifying data or programs. In addition, this model uses integrity verification and transformation procedures to maintain internal and external consistency of data. The verification procedures confirm that the data conforms to the integrity specifications at the time the verification is performed. The transformation procedures are designed to take the system from one valid state to the next. The Clark-Wilson model is believed to address all three goals of integrity

D. LOMAC

Low Water-Mark Mandatory Access Control (LOMAC) [4] is a Mandatory Access Control model which protects the integrity of system objects and subjects by means of an information flow policy coupled with the subject demotion via floating labels. In LOMAC, all system subjects and objects are assigned integrity labels, made up of one or more hierarchical grades, depending on their types. Together, these label elements permit all labels to be placed in a partial order, with information flow protections and demotion decisions based on a dominance operator describing the orders.

E. SEIP

SEIP [1] is simple and efficient but yet effective solution for the integrity protection of cellular phone platforms. As all above all models have some disadvantages and limitation, the SEIP is now considering for integrity protection which has protection rules based on open mobile platform and application behaviour. It provides a set of rule which control flow of information according to different mobile systems.

3. Comparison between Different Approaches For Integrity Protection

In CW-Lite, some low integrity information flows may be accepted by high integrity subjects. In the laptop example, the some interfaces of the [8] UNIX services and corporate applications may be deemed capable of discarding or upgrading such low integrity inputs. We refer to these interfaces as filtering interfaces.

Table 1

Parameters	*Biba*	*CW-Lite*	*Clark Wilson*	*LOMAC*	*SEIP*
High integrity process can read low integrity Process	No	Yes	No	No	Yes
High integrity process can read low integrity Network Data	No	Yes	No	No	No
Sanitation of low integrity data	Yes	Yes	Yes	Yes	No
Downgrade process integrity level	No	No	Yes	Yes	Yes
Upgrade process integrity level	No	No	No	No	Yes

In CW- Lite, low integrity permissions are only accessible through filtering interfaces via filtering subjects. That is, the permissions of filtering subjects are only available when the code of a filtering interface is run. Otherwise, the process runs with the permissions of a trusted subject and is limited to Biba integrity Information flow-based integrity models have been pro- posed and implemented in many different systems, including the well-known Biba , Clark-Wilson , and LOMAC.[9] Biba integrity property restricts that a high-integrity process cannot read lower integrity data, execute lower integrity programs, or obtain lower integrity data in any other manner.

4. Limitations

Although recent SEIP detect the major threats from user downloaded application or unintentionally installed applications including code and data received form Bluetooth, MMS including browser and it does not based on the information flow system. SEIP implemented in some major services like device status manager, system configuration service it is not a complete list for whole platform

5. Future Scope

In SEIP integrity protection mechanism low integrity application cannot be installed but we can improve this by allowing low integrity application to be installed. Another is in this mechanism is that high integrity level of subject means no vulnerability of its implementation. So we can check that high integrity level of subject can be threat to system or not.

6. Acknowledgment

I would like to express my gratitude and appreciation to all those who gave me the possibility to complete this paper. Special thanks to my final my guide, whose stimulating suggestions and encouragement, helped me in writing this paper

7. Conclusions

SEIP proposes a set of integrity rules to control information flow according to different types of subject in mobile systems. This enables very simple security policy

development. The security policy is less than 20kB and it is lightweight

References

[1] Xinwen Zhang, Jean-Pierre Seifert and OnurAciicmez, "Design and Implementation of Efficient Integrity Protection for Open Mobile Platforms", IEEE Transactions on Mobile Computing, Vol. 13, no. 1, January 2014
[2] Member, IEEE,, Member, IEEE, and, IEEE J. Cheng, S. Wong, H. Yang, and S. Lu, "SmartSiren: Virus Detection and Alert for Smartphones," Proc. ACM Conf. Mobile Systems, Applications, 2007
[3] W. Enck, P. Traynor, P. McDaniel, and T.L. Porta, "Exploiting Open Functionality in SMS-Capable Cellular Networks," Proc.12th ACM Conf. Computer and Comm. Security (CCS), 2005S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[4] C. Heath, Symbian OS Platform Security. Symbian, 2006
[5] T. Jaeger, R. Sailer, and U. Shankar, "PRIMA: Policy-Reduced Integrity Measurement Architecture," Proc. 11th ACM Symp. Access Control Models and Technologies (SACMAT), 2006.
[6] N. Li, Z. Mao, and H. Chen, "Usable Mandatory Integrity Protections for Operating Systems," Proc. IEEE Symp. Security and Privacy, 2007.
[7] P. Loscocco and S. Smalley, "Integrating Flexible Support for Security Policies into the Linux Operating System," Proc. USENIX Ann. Technical Conf., pp. 29-42, June 2001.
[8] D. Muthukumaran, A. Sawani, J. Schiffman, B.M. Jung, and T. Jaeger, "Measuring Integrity on Mobile Phone Systems," Proc. 13th ACMSymp. Access Control Models and Technologies (SACMAT), 2008.
[9] U. Shankar, T. Jaeger, and R. Sailer, "Toward Automated Information-Flow Integrity Verification for Security-Critical Applications," Proc. Network and Distributed Systems Security Symp. (NDSS), 2006.