Cryptographically Protected Objects

Uwe G Wilhelm
Presented by : Mohan Rajagopalan

October 13,1999

1 Abstract

Cryptographically protected Objects describes a mechanism that guarantees the integrity of Mobile Objects during transit and within a given execution environment. The mechanism is based on the usage of the CryPO protocol which is an application of Public Key Cryptography to Tamper proof environments(TPE) . A Tamper Proof environment is based on the notion of a blackbox system, which can neither be inspected not tampered with. The notion of trust relationships is introduced and Certification is the selected as the mechanism for conveying trust.

An extension of this article highlights the notion of trust in Mobile and Distributed Computing environments. This technique has found industrial application in smart cards using the JAVA CARD API.

2 Introduction and Problem Definition

This paper is motivated by pervasive influx of new technologies (with a highlight on Mobile and Distributed computing solutions) which bear important economic implications. It tries to provide a generic solution which may be applied to the whole domain of mobile computing including Java Applets , Activex Controls etc.

In the mobile scenario we are repeatedly faced with a scenario where the users of an object are different from the producers. This implies the objects are expected to leave the (hopefully!!) secure domains of their manufacturers and venture into the (big bad!!) world. This very notion of entry into a unsure / insecure domain introduces a range of hazards. Code tampering, reverse and re-engineering, code piracy which lead to loss of proprietary algorithms, secure & resticted data, copyright violations etc. are now evils that can not be neglected.

The paper explores a soution that is aimed at maintaining the integrity of Object code during transit and within the execution environment. The paper aims at developing a solution that is not necessarily fool-proof but a soution that deters the "hacker" enough. In the following technique we try to restrict the object in a secure environment throughout its lifetime. The paper discusses the provision of this secure transmission and exectuion environment.

3 Protected Objects

The solution to the above mentioned problem lies in providing an environment which can neither be tampered with nor be inspected.This is similar to the notion of a *blackbox*. We need to devise these blackboxes which will transparently be host to the objects. We also need a protocol that ensures secure movement of the objects in the given environment.

3.1 Tamper Proof Environment

A Tamper Proof Environment (TPE) is an attempt to implement the blackbox. All Objects within the system are expected to reside within the TPE. Each Host / user is provided with a TPE which controls the execution of objects through a limited interface to the local environment. These interactions are checked and reguleted by the TPE.

The TPE uses public Key cryptography to ensure secure transactions among objects and message passing. The underlying assumption of the whole system will be : *the private key of the TPE never known to anyone but the user.* Even the user / host on which the TPE resides is never allowed to know the private key of the TPE. Messages may be passed to the TPE encrypted using the published public key.

The concept of *Certification* is used to establish trust relationships amongst the TPE's in the system. A certificate contains data which identifies the manufacturer, guarantees provided & public key of the TPE. The TPE manufacturer is expected to play the role of the certifcate store and is handed the responsibility of public key distribution. The TPE manufacturer is assumed to be a trusted entity i.e. it is always on the good side.

3.2 CryPO protocol

The CryPO protocol is a 2 phase protocol which ensures secure transmission of Objects and messages within the system. The first phase is the "Certification Phase" which preceedes the actual usage of CryPO protocol. The TPE manufacturer publishes its public key, which is in turn used to provide each TPE with its Public Key through the published certificates.

The "Usage Phase" of the protocol is fairly simple. Object users request for an object based on its name and their certificates. The Object provider validates the certificate to check if it satisfies all required guaratees. If it does the Object is then encrypted using the public key (derived from the certificate) and packaged to the TPE. The TPE then decrypts it using its personal private key and then executes it.

4 Conclusion

The paper introduces a system whereby a blackbox environment is provided to Objects within the system. This mechanism ensures that the integrity of Object Code is preserved throughtout. The mechanism also ensures that even though objects may flow freely and through hosts and other users they are understandable only within the TPE. All damage that may be caused by / to the Object is restricted within the internal bounds of the TPE which is the Objects window to the outside world. Incase an Object is tampered with the TPE can be found and it will lose the trust it has to have to be a part of the system.

This paper does not introduce any flashy new ideas but is an impressive compilation and application of known principles of cryptography. The paper introduces several new (and abstarct) concepts like the "Notion of trust". many of these have found acceptance in the Distributed Computing and Communications communities who are major users of Mobile Technology. This technology has found industrial application through smart cards developed using the Java Card API (Schlumberger and Gemplus).