**Cloudproxy Nuts and Bolts**

manferdelli@, tmroeder@

**Overview**

Cloudproxy is a software system provide *remotely authenticated* isolation, confidentiality and integrity of code and data for Hosted Systems preventing attacks from co-tenants and (under modest assumptions) insiders in a remote data center. Cloudproxy operated on two components to achieve this, a Host System (raw hardware, Virtual Machine Manager, Operating System) which provides capabilities described below to a Hosted System (VM, Application, Container).

Cloudproxy provides a mechanism at each level of the software stack to isolate Hosted Systems, measure and remotely verify the exact software and configuration information constituting the Hosted System and provide security services like sealing that ensures that information (like keys) can be securely provisioned and retrieved only by the correct Hosted System, while isolated, on a supported platform.

A key concept is that of Code Identity and Measurement. Readers can consult [1] for a fuller description. This document is intended as a brief but relatively comprehensive for programmers who want to build secure Hosted Systems. We cover the critical ideas, installation, programming model and critical key management techniques

**The Tao**

StartHostedProgram

Seal

Unseal

Attest

GetRandom

OpenTaoChannel

Authorization Guard

Crypto Support

Program certificates

**Hardware roots of Trust**

Cloudproxy supports TPM 1.2 and TPM 2.0 as hardware roots of Trust for Host Systems booted on raw hardware. We have implemented support for other mechanisms and adding a new hardware mechanism is relatively straightforward provided the new hardware supports accurate measurement of booted images, isolation for Hosted Systems and attestation which is used to initialize the key hierarchy.

Once the base Host System is safely booted on a supported hardware, Cloudproxy implements software support for recursive Host systems at almost every layer of software including:

1. A Host System running under a VMM which isolates each Hosted Virtual Machines.
2. A Host System running in an operating system which isolates Hosted Processes (or applications).
3. A Host System running in an operating system which isolates Hosted Operating Systems or Containers.
4. A Host System running in an application (like a browser) which isolates Hosted sub-applications, like plug-ins.

In all cases, Hosted Systems have the same interface to the Host System and can use any Host Service (for example, any system call on Linux) so the programming model at each Hosted layer is essentially unchanged from the non-Cloudproxy case.

**Principal Names**

Principal names are hierarchical. The root name for a hosted program, in the development case, might look something like

key([080110011801224508011241046cdc82f70552eb...]).Program([25fac93bd4cc868352c78f4d34df6d2747a17f85...])

Here, key([080110011801224508011…]) represents the signing key of the host and Program([25fac93bd4cc868352c78f4d34df6d2747a17f85...]) extends the host name with the hash of the hosted program (25fac93bd4cc868352c78f4d34df6d2747a17f85...). If the host were a real linux\_host rooted in a TPM boot, its name would name the AIK and the PCRs of the booted linux systems which incorporate the hash of the Authenticated Code Module (“ACM”) that the bios called to start the authenticated boot and the hash of the linux image and it’s initramfs.

**Authorization**

Guards make authorization decisions. Current guards include:

* the liberal guard: this guard returns true for every authorization query
* the conservative guard: this guard returns false for every authorization query
* the ACL guard: this guard provides a list of statements that must return true when the guard is queried for these statements.
* the datalog guard: this guard translates statements in the CloudProxy auth language (see tao/auth/doc.go for details) to datalog statements and uses the Go datalog engine from github.com/kevinawalsh/datalog to answer authorization queries. See tao/datalog\_guard.go for the translation from the CloudProxy auth language to datalog. And see install.sh for an example policy.

**Tao channel**

SSL like, uses Program Certificate

**Workflow**

A fairly complete example is in go/apps/fileproxy. We will focus our description at the Linux process level. For that, the Tao enabled Linux, has been measured and is running a Tao service that your application can communicate with using the Tao library (either in Go or C++). This Linux Tao is the Host System and your application is the Hosted System. You can assume the Linux Tao service is already provisioned with an attestation key and supporting certificates naming the measurement of the Linux instance. As a result, the Linux service can start measured Cloudproxy services given an executable image. When your Cloudproxy application starts in main, someone has already interacted with the Linux level Tao to measure and start your image. Most application development is identical with writing (a safe!) Linux application and all Linux system calls are available to your Cloudproxy application. There are two workflows, one for when you run your program for the first time on the target hardware/OS (“Initialization Phase”) and a second for “post initialization” activation of the Cloudproxy application (“Normal Processing Phase”). During the first phase, your application will produce several files (sealed data, Program Certificate); if these files are present and your application can successfully unseal the sealed data, you do not need to do any further initialization.

*Initialization Phase*

For simplicity, let’s assume all your Cloudproxy applications operate in a single security domain; for example, they may all implement a single coordinated transaction service for an entity which has a public key Ppolicy that is used to authenticate all credentials and service directives.

In this phase, your application generates a public private key pair that will authenticate your program to other Cloudproxy applications. It then asks the the Host System to attest to your newly generated public key. This attestation is transmitted to a trusted security domain service which examines the evidence in the attestation naming your application code measurement and Host System evidence, if this complies with the security domain policy, the security domain service uses the private portion of Ppolicy which we denote by ppolicy to sign a “Program Certificate” for the public key you provided. The security domain service must run in a secure location since the safe use of ppolicy is critical to the overall Cloudproxy security. When you receive the Program Certificate you use the Host System Tao to seal the private key producing an encrypted, integrity protected blob that can be used by your Host System, in subsequent invocations, to give you back this private key. The Host System ensures that your program, and only your program, when running under an isolation guarantee provided by the Host System, can obtain this unsealed information. Often, you will also generate symmetric keys that your program will use to encrypt and integrity protect information (including other keys) and potentially negotiate shared keys with other Cloudproxy services or (to protect data that will be used by your application and other Cloudproxy applications in this security domain on this and other machines can use to encrypt and integrity protect data they should all have access to). Finally, you will seal this additional “private data” along with a monotonic counter available locally or remotely accessible from other Cloudproxy services enabling you to prevent “rollback” attacks on this critical state information. You should store all the resulting “sealed” files and certificates so you can retrieve them on subsequent invocations.

*Normal Processing Phase*

In the Normal Processing Phase, when you first enter main, you will typically retrieve all the sealed blobs produced in the Initialization Phase, unseal them and proceed with your normal processing. You can use your sealed keys to encrypt and integrity protect all data you store or transmit. In the course of normal processing, it is likely you will want to cooperate with other Cloudproxy applications securely. Cloudproxy provides support to open an encrypted, integrity protected channel between Cloudproxy applications (locally or remotely) using your Program Key. These channels *authenticate* the identity of peer Cloudproxy applications you can ensure you share important data and rely on interactions over this channel with security domain authorized, trusted programs that are isolated and protected by a Host System meeting the security requirement of the security domain.

**The API – Go**

Domains represent security contexts; they encapsulate configuration information like names, path to key blobs, path to policy key, and the guard employed for authorization decisions.

CreateDomain initializes a new Domain, writing its configuration files to a directory. This creates the directory and, if needed, a policy key pair encrypted with the given password when stored on disk; it also initializes a default guard. The call is:

func CreateDomain(cfg DomainConfig, configPath string, password []byte) (\*Domain, error)

Any parameters left empty in cfg will be set to reasonable default values.

Domain information is loaded from a text file, typically called tao.config via the call:

LoadDomain(configPath string, password []byte)(\*Domain, error)

which returns a domain object if successful. The password is used to load a key set from disk. If no password is provided, then LoadDomain will attempt to load verification keys only. For example, LoadDomain is called with a configPath and an nil password to load the policy verification key.

A configuration object, type DomainConfig, holds configuration information for the domain between tao activations.

[The](http://github.com/jlmucb/cloudproxy/tao) [API used by](http://github.com/jlmucb/cloudproxy/tao/auth) a Hosted System:

* [GetRandomBytes(chil](http://github.com/jlmucb/cloudproxy/tao/auth)[dSubp](http://github.com/jlmucb/cloudproxy/tao)[rin auth.SubPrin, n int) (bytes []by](http://github.com/jlmucb/cloudproxy/tao/net)[te, err error): returns a slice of n random bytes.](http://github.com/jlmucb/cloudproxy/tao)
* GetSharedSecret(tag string, n int) (bytes []byte, err error): returns a slice of n secret bytes. (This is not currently used in any test programs).
* Attest(childSubprin auth.SubPrin, issuer \*auth.Prin, time, expiration \*int64, message auth.Form) (\*Attestation, error) : requests the Tao host sign a statement on behalf of the caller
* Encrypt(data []byte) (encrypted []byte, err error): seals data.
* Decrypt(encrypted []byte) (data []byte, err error): unseal.
* AddedHostedProgram(childSubprin auth.SubPrin) error: create new program.
* RemovedHostedProgram(childSubprin auth.SubPrin) error: kill hosted program.
* TaoHostName() auth.Prin: Get the Tao principal name assigned to this hosted Tao host. (Unix pathname with hashes, right? --- )for a hosted program under the linux tao, the TaoHostName might be something like tpm([...]).PCRs(...))

A hosted system represented by a tao, tao, obtains the pointer to its host interface by calling tao.Parent().

The network interface for the Tao channel:

* func DialWithKeys(network, addr string, guard tao.Guard, v \*tao.Verifier, keys \*tao.Keys) (net.Conn, error)
* func Listen(network, laddr string, config \*tls.Config, g tao.Guard, v \*tao.Verifier, del \*tao.Attestation) (net.Listener, error)

**The API -- C++**

**Installing Cloudproxy**

As quick as possible

**Skeleton application example**

Three application elements:

1. Simple Client
2. Simple Server
3. Simple Security Domain Signing Service

The Simple Server makes up a secret and stores it. The Simple Client uses a Tao channel to contact the Simple Server to learn the secret and store it securely. We don’t implement rollback protection or distributed key management for intermediate secrets just to keep the example as simple as possible. We give sample code in Go and C++ for the Simple Client and Simple Server. The sample application also uses a Simple Security Domain Signing Service which checks the measurements in the Attestations for the Simple Client and Simple Server and, if the measurements are correct, it signs the Program Certificate. We did not provide sample code for this since the Simple Security Domain Signing Service is, well, simple and need not run on Cloudproxy (although there are good reasons for doing so --- see the key management scenarios below for some reasons). The Fileproxy application (in ~/cloudproxy/go/apps/fileproxy) implements a more complicated service and includes a skeleton rollback server and signing server.

***Simple Client in Go***

***Simple Server in Go***

***Simple Client in C++***

***Simple Server in C++***

**Upgrade and key management scenarios**

Since sealed material is only provided to a Hosted System with exactly the same code identity that sealed the material while running on the exact same Host System, while isolated by that Host System. You may be worried about lost data or limitations that affect key management, software upgrade or distribution on other Host Systems. In fact, it is rather easy to accommodate all these circumstances, and many others, efficiently, securely and in most cases automatically using Cloudproxy although the Cloudproxy applications must make provisions for this during development.

Below are sever example key management techniques that can be used when a Cloudproxy application is upgraded, a new Cloudproxy application (in the same security domain) is launched, or as applications migrate to other Host Systems. All these mechanisms preserve the confidentiality and integrity of all Cloudproxy applications and data used and produced in the security domain or particular host hardware.

There is a discussion of many of the mechanisms as they might affect client software used across different security domains by users with no control over the application code while supporting consumer transparency (the most challenging case) in [4]. Here we restrict ourselves to cooperating server applications.

1. Vanilla cloud key mgmt
2. Prod-id equivalent management
3. Auto upgrade using authority
4. Auto upgrade
5. Certificate based key transfer to new version
6. Shared keys without central authority

**References**

**[1] Manferdelli, Roeder, Schneider, The CloudProxy Tao for Trusted Computing,** <http://www.eecs.berkeley.edu/Pubs/TechRpts/2013/EECS-2013-135.pdf>.

**[2] CloudProxy Source code,** [http:/](http://www.eecs.berkeley.edu/Pubs/TechRpts/2013/EECS-2013-135.pdf)/github.com/jlmucb/cloudproxy.

**[3] TCG, TPM specs,** <http://www.trustedcomputinggroup.org/resources/tpm_library_specification>

[4] **Beekman, Manferdelli, Wagner,** AsiaCCS, 2016.

The Guard interface:

* Subprincipal() auth.SubPrin: returns a unique subprincipal for this policy.
* Save(key \*Signer) error: writes all persistent policy data to disk, signed by key
* Authorize(name auth.Prin, op string, args []string) error
* Retract(name auth.Prin, op string, args []string) error
* IsAuthorized(name auth.Prin, op string, args []string) bool
* AddRule(rule string) error
* RetractRule(rule string) error
* Clear() error: removes all rules.
* Query(query string) (bool, error)
* RuleCount() int
* GetRule(i int) string.
* String() string: returns a string suitable for showing auth info.