James Birdsong
Professor Newman
Information Security
8 February 2016

Project Proposal: Schematic Protection MAC

Project: Schematic Protection Model Access Control Mechanism Implementation

The Linux landscape currently include a number of access control mechanisms implementing Mandatory Access Control, Discretionary Access Control, and a selection of other access control models. However, between Linux distributions and to other platforms including Mac OS X and Windows, there does not exist a single, easy to use, secure information security mechanism for controlling the distribution and access to information and privileges. In light of recent insider threats such as leaks of pre-release movies and government secrets or external threats such as hackers and malware, a single unified information security system represents a useful tool in the fight to contain and manage threats to an organization's critical information infrastructure.

In this project, I seek to implement a daemon and a portable client library implementing a variant of the Schematic Protection Model. The daemon will be called the "protection controller" and serves as the reference authority for the client library component. The client library will communicate with the controller for privileged authentication, policy enumeration, and subject-object creation and manipulation. The security data and metadata will be backed by a fast in-process SQLite3 database. The daemon acts as the secure gatekeeper and enforces the policies defined in the schematic protection model.

Goals:

1. Implement a working SPM mechanism and associated tools
2. Gain experience writing Python programs and interfacing with C++ modules
3. Implement fast and reasonably secure authentication protocol

Deliverables:

1. Specification of authentication and communication protocol
2. SQL database schema implementing SPM and supporting authentication
3. Implementation of SPM protection controller daemon
4. Client library interface to securely access the remote daemon

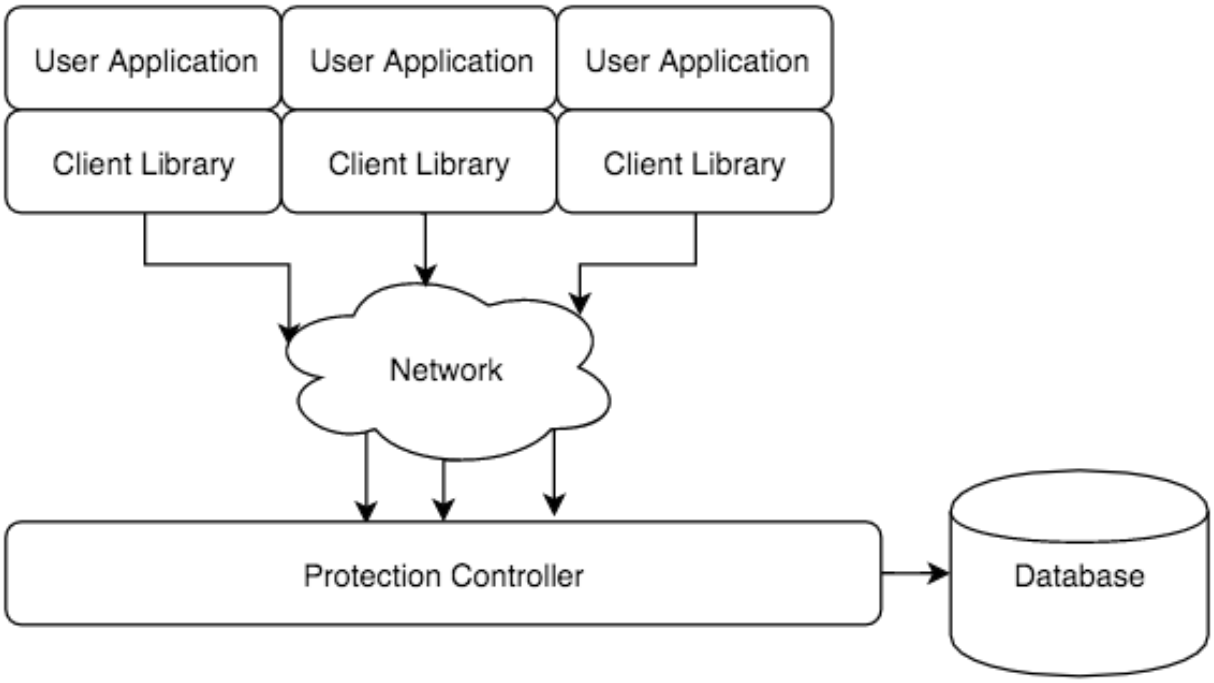
Estimated Timeline:

1. Protocol specification and database schemas (1 week)
2. Protection controller (4 weeks)
3. Client library (2 weeks)
4. Software testing and debugging (1 week)

Resources Found:

1. http://www.sis.pitt.edu/jjoshi/IS2935/p404-sandhu.pdf
   Schematic Protection Model details
2. https://www.python.org/doc/
   Python documentation and references
3. http://www.netzmafia.de/skripten/unix/linux-daemon-howto.html
   Ideal daemon behavior and interaction with the Linux system
4. http://www.cix.co.uk/~klockstone/xtea.pdf
   Encryption algorithm to be used as the stream cipher in the protocol
5. https://www.ietf.org/rfc/rfc2898.txt
   Key stretching and derivation function

Project Diagram:



Only the Protection Controller and Database are trusted. It is assumed that clients may not collude outside the protection controller. Connections will be encrypted and authenticated using XTEA, SHA1, and shared-secret protocol.