ArmoredSoftware: Trust in the Cloud

Perry Alexander, The University of Kansas

October 22, 2014

ArmoredSoftware is a software system designed to provide user-space attestation in a cloud environment. Cloud applications using ArmoredSoftware support run-time software appraisal to assess trustworthiness of running software and the cloud environment. Appraisal results then inform responses to detected run-time hazards ranging from migration to shutdown. ArmoredSoftware is built on open source software—Linux, Xen, and OpenStack—and follows industry trusted computing standards.

The objective of ArmoredSoftware is to provide a *trusted execution infrastructure for cloud-based software systems* based on trusted execution principles developed by the Trusted Computing Group. An ArmoredSoftware component will provide support for trusted computing:

- *Identification*—strongly identifying software components
- *Observation*—gathering evidence of software behavior
- *Appraisal*—assessing and responding to gathered evidence

Using ArmoredSoftware capabilities a cloud computing process can establish trust in its operational environment and other processes operating in the same environment. In turn it can establish its own trustworthiness to other system components. Finally, it can take appropriate action based on results of trustworthiness assessment.

ArmoredSoftware extends open source software to ensure operation in a traditional cloud environment. It currently builds upon Linux, Xen and OpenStack and will be extended to other environments as desired. ArmoredSoftware leverages industry standards to ensure compatibility with traditional trusted computing approaches.

ArmoredSoftware achieves its objective of trusted execution by providing a capsule for executing software components This capsule, referred to as *armor*, provides three major components:

- *Appraiser*—Request and assess measurement information from the operational environment and other armored components.
- *Measurer*—Gather run-time measurement information from its application
- *Attestation Manager*—Assemble and deliver evidence to appraisers in a manner that assures measurement integrity

and is based on concepts from Coker et al. [2011].

Figure 1 depicts interactions among major architectural components of a protected ArmoredSoftware application. The *Application* is the running program to be protected by the infrastructure. It need not be modified or aware of the other armor components unless desired by the user. An *Appraiser* initiates trust assessment by requesting information from the operational environment, other ArmoredSoftware applications and traditional cloud applications to assess the operational environment. The Appraiser specifies what information it needs without specifying how that information should be gathered. The *Attestation Manager* receives a request from an Appraiser and selects an attestation protocol to fulfill the Appraiser's request. It then executes that protocol to gather evidence by invoking measurers along with cryptographic assurance of integrity and confidentiality. It also provides evidence of correct protocol execution and correct Measurer interaction. The *Measurer* performs specific measurement operations on the running application and returns evidence describing application operation. Measurers are specialized for their associated software application and may range from gathering simple values to observing operational state over time. Using evidence gathered by the Measurer and returned by the Attestation Manager, the Appraiser directs response to appraisal. Such responses may include migration, reporting, or shutdown. *Access control* governs access to all critical resources in the protected application to assure secrets are preserved and enforce information flow restrictions.

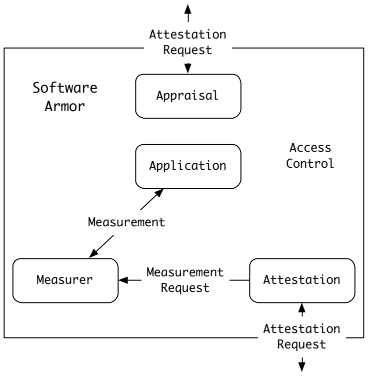

Figure 1: ArmoredSoftware component architecture showing major components of the remote attestation process.

The ArmoredSoftware approach has three significant advantages: (i) flexibility; (ii) simplicity; and (iii) usability. The use of protocols to perform attestation allows operations ranging from simple operational checks to complex interactions among many ArmoredSoftware components. The use of application specific Measurers allows specialization to the component resulting in simpler, more effective evidence gathering. Finally, ArmoredSoftware does not require modification of cloud applications. While users will write applications to take advantage of ArmoredSoftware capabilities, existing applications can be reused without modification.

References

G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen. Principles of remote attestation. *International Journal of Information Security*, 10(2):63–81, June 2011.