An seL4-based Architecture for Layered Attestation

Grant Jurgensen
Michael Neises
Perry Alexander
gajurgensen@ku.edu
m811n155@ku.edu
palexand@ku.edu
ITTC - The University of Kansas
Lawrence, Kansas, USA

ABSTRACT

Remote attestation refers to the process in which a computer system constructs evidence reflecting its state and/or identity, with the purpose of convincing an external system of its trustworthiness. For systems which communicate sensitive information, remote attestation is an essential tool for identifying malicious or compromised actors. However, attestation evidence can only be considered as trustworthy as the architecture it was collected on. Trusted attestation demands strong memory separation properties to guarantee the integrity of its measurements and the confidentiality of it private keys. In this sense, popular general-purpose operating systems such as Windows or Unix derivatives form an insufficient basis, as a result of their loose and dynamic memory semantics.

In contrast, the formally verified seL4 microkernel is proven to enforce memory isolation under proper configuration [1], making it a natural foundation to our attestation architecture. Ideally, existing systems in need of rigorous attestation capabilities would be ported to such an environment. In practice, however, it is unrealistic to suggest all such systems be ported. Instead, we offer a generic solution utilizing a Linux virtual machine running in seL4, which allows us to effortlessly lift legacy systems into our architecture. In this layered attestation paradigm, the sandboxed systems can be measured from the outside with the aforementioned benefits of guaranteed memory separation, or the inner layer may more conveniently perform measurements on itself. Finally, we attempt to compose a chain of trust in the boot process originating from a root hardware key, thereby establishing the system's architectural integrity.

ACM Reference Format:
Grant Jurgensen, Michael Neises, and Perry Alexander. 2020. An seL4-based Architecture for Layered Attestation. In *No Book.* ACM, New York, NY, USA, 1 page. https://doi.org/0000

REFERENCES

[1] Toby Murray, Daniel Matichuk, Matthew Brassil, Peter Gammie, Timothy Bourke, Sean Seefried, Corey Lewis, Xin Gao, and Gerwin Klein. 2013. seL4: From General Purpose to a Proof of Information Flow Enforcement. *34th IEEE Symposium on Security and Privacy* (May 2013), 415–429. https://doi.org/10.1109/SP.2013.35

Attestation Architecture, 20 January, 2020, Lawrence, KS

ACM ISBN 0000…$0.00
https://doi.org/0000