

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

When computer systems communicate sensitive information, it is often desirable, if not imperative, that one party know certain properties about the other. This may be as simple as confirming the external party's identity, e.g. by checking a signature against a known public key, as is ubiquitous among internet protocols. Alternatively, one party may demand stronger guarantees before engaging in sensitive communication. For example, it may wish to know that the target system is reasonably secure. The target could respond to such a request with evidence that it is running trusted anti-malware software and routinely scanning for threats. Perhaps this evidence is sufficient in the current context, or perhaps the other party demands deeper evidence, such as a glimpse into a portion of the current kernel memory, as in to detect an evasive rootkit.

All of these activities may be generalized into the broader notion of remote attestation, which is defined as 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 its private keys. If an application on the system is able to distort this sensitive attestation data without detection, then the attestation evidence can no longer be considered trustworthy. Thus, popular general-purpose operating systems such as Windows or Unix derivatives form an insufficient architectural foundation as a result of their loose and dynamic memory semantics.

Ideally, systems in need of rigorous attestation capabilities would be built atop a separation kernel which could statically isolate sensitive attestation data from the rest of the system. Existing systems could be ported to such a kernel, but in practice, doing so would be prohibitively time-consuming. Instead, we offer a generic solution which accommodates a multitude of existing systems by embedding

a general-purpose operating system into a separation kernel, and providing attestation capabilities to both layers. Specifically, we use seL4 as our separation kernel, and a sandboxed Linux virtual machine running under seL4 as our general-purpose operating system. Not only is the seL4 microkernel formally verified with respect to its specification, it has also been proven to enforce memory isolation under proper configuration [1], the defining property of a separation kernel.

Existing Linux systems are effortlessly incorporated into our attestation architecture by dropping them into the Linux virtual machine layer. Also present in the Linux layer is an attestation component which is able to measure the Linux layer, but is unable to observe the outer seL4 layer. The seL4 layer is likewise equipped with an attestation component. However this component can measure not just its own layer, but also the embedded virtual machine. In this schema, the Linux attestation component is responsible for the majority of attestation, while the seL4 component is largely relegated to routine measurements that aim to abate the aforementioned concerns regarding attestation within Linux. Collecting attestation measurements within Linux is more performant and easier to implement than at the seL4 layer, but also less trustworthy as a result of the lack of stringent memory separation. Conversely, measurements made by the seL4 attestation component are highly trusted due to the static memory isolation enforced at this layer. Therefore, measurements made by the Linux layer may be bolstered by coupling them with recent evidence collected by the seL4 layer demonstrating the Linux virtual machine to be free from malicious processes tampering with the attestation process.

Our architecture enhances trust in attestation by continually extending trust at runtime from the seL4 layer to the Linux virtual machine layer. We aim to extend this chain of trust backwards as well, such that trust is not placed in the seL4 layer a priori, rather it is derived from some check during the boot process that the proper image is loaded into memory. Naturally, this chain of trust would extend all the way down to some root of trust, likely a secret hardware-specific private key. Finally, we aim to incorporate key management into the chain of trust process, whereby a layer's private key is only delivered to its attestation component after it has been measured. Ultimately, we hope to have an architecture which both establishes trust in the boot process, but also continues to establish trust through attestation.

ACM Reference Format:

Grant Jurgensen, Michael Neises, and Perry Alexander. 2020. An seL4-based Architecture for Layered Attestation. In *Hot Topics in the Science of Security*

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

HotSoS '20, April 7–8, 2020, Lawrence, KS, USA

© 2020 Copyright held by the owner/author(s).

ACM ISBN 978-1-4503-7561-0/20/04.

<https://doi.org/10.1145/3384217.3386398>

Symposium (HotSoS '20), April 7–8, 2020, Lawrence, KS, USA. ACM, New York, NY, USA, 2 pages. <https://doi.org/10.1145/3384217.3386398>

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>