Abstract

The Wireless Sensor Networks (WSNs) have applications typically in ubiquitous and pervasive environments that make ensuring the security therein critical. Despite deployment with utmost stringent security measures, the intrusions and the adversarial attacks like node compromise and node tampering cannot be prevented. Hence, there is a need for devising an intrusion detection and prevention system that can withstand the resource constraints and work feasibly within the same. One such intrusion detection technique is code attestation which is useful for verifying the program integrity of nodes in such networks. Our focus here is on software based remote code attestation. The static code attestation techniques published in the literature only check the integrity of the static code embedded within sensor nodes whereas the dynamic data attestation techniques check the structural integrity of dynamically created data. We believe that an integrated approach that uses both the static and dynamic code attestation techniques can leverage the effectiveness of an intrusion detection system. In this paper, we propose our integrated approach for countering attacks based on code attestation. As we demonstrate using our experimental simulation studies, with the marginal increase in memory and computational overhead, our approach ensures improved overall security. To the best of our knowledge ours is the first attempt in following such an approach.
References

A Static Code and Dynamic Data Attestation based Intrusion Detection System for Wireless Sensor Networks

- TinyOS tutorial, http://www.tinyos.net/tinyos-1.x/doc/tutorial
- H. Shacham,&quot; The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86)&quot;, In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS), 2007
- A. One, "Smashing the stack for fun and profit", Phrack, 7(49), Nov. 1996.
- Ferguson, C., Gu, Q., and Shi, H., "Self-healing control flow protection in sensor applications", In WiSec (2009), ACM.

Index Terms

Computer Science

Networks

Keywords