TinyWIDS

A misuse-based Intrusion Detection System for IEEE 802.15.4 Wireless Sensor Networks

Center of Excellence DEWS
University of L'Aquila, Italy

What is WIDS/TinyWIDS? – WSN Intrusion Detection System (WIDS) [1][2] is an Intrusion Detection System designed to be deployed on the resource-constrained IEEE 802.15.4 WSN. WIDS exploits the *Weak Process Models* (WPM) to track and estimate the current state of WSN nodes. When a dangerous state is detected, WIDS can send notifications and/or perform user-defined reactions. *TinyWIDS* is the implementation of WIDS on the *TinyOS* framework. It is designed to run on all major WSN node architectures (e.g., *telosb, MicaZ, IRIS*).

Architecture – TinyWIDS allows developers to define a set of *metrics* of interest (e.g., # of incoming messages per time unit, # of CCA and/or CRC failures etc.) and a set of *Observables* (i.e., an event which is detected by the IDS). Observables are spawn when one or more metrics have values beyond the *threshold function* defined in the Observable itself. At regular intervales, TinyWIDS looks for new Observables and, if any is present, tries to estimate the state of the WSN node by updating the WPM of every *Attack (Attack Models)*. When one or more Attack models are in a *dangerous state, TinyWIDS* sends a notification to the higher level logic which can implement a proper reaction depending on the detected attacks. *Metrics, Observables* and *Attacks* can be easilly added to TinyWIDS to enhance its capabilities and detection rate.

Threat Modelling – Every Attack Model is a WPM and it is described by means of a graph representation. The graph contains a set of states, which can be *normal states* or *high/low danger* states. When one of the latter coincides with the estimated state, the attack is *detected.* Additional features (e.g. *Threat score, Aging etc.*) are present to limit wrong detections. Developers can easily create new models using a JSON-based description.

Why TinyWIDS? – TinyWIDS is designed to be as flexible as possible with a very small resource footprint (tens of kilobytes). Attack models can be described easilly and can be made as general as possible to detect also new (unknown) types of attack.

Current status – TinyWIDS is currently under development to fully implement WIDS. Some basic and advanced attacks are under modeling and will be included in the release. During DATE19 University Booth, TinyWIDS is deployed on a WSN composed of 2 IRIS nodes. A third node (*attacker node*) will be programmed to perform some basic attacks (e.g., jamming/replay attack) to show TinyWIDS in action.

Contacts: Walter Tiberti (walter.tiberti@graduate.univaq.it), Luigi Pomante (luigi.pomante@univaq.it)

References

[1] S. Marchesani, L. Pomante, M. Pugliese, F. Santucci. "WINSOME: A Middleware Platform for the Provision of Secure Monitoring Services over Wireless Sensor Networks". 9th International Wireless Communications & Mobile Computing Conference (IWCMC 2013), Cagliari, Luglio 2013.

[2] L. Bozzi, L. Di Giuseppe, L. Pomante, M. Pugliese, M. Santic, F. Santucci, W. Tiberti. TinyWIDS: a WPM-based Intrusion Detection System for TinyOS2.x/802.15.4 Wireless Sensor Networks. Fifth Workshop on Cryptography and Security in Computing Systems (CS2 2018).

This work has been partially supported by the ECSEL RIA 2015 SAFECOP project.