Security in Unpredictably Resource Constrained Embedded Environments

Aniket Kate Mike Atallah
Purdue University

I. Background and Motivation

Ever-increasing Security Threats in the Embedded Environment: Security for embedded systems is becoming a greater concern as manufacturers increase connectivity of these traditionally isolated networks to the outside world. For example, the increasing computerization of hitherto purely mechanical elements in vehicular networks, such as connections to the brakes, throttle, and steering wheel, has led to a life-threatening increase of exploitation power. In the event that an attacker gains access to an embedded control network, the attacker can manipulate potentially safety-critical message traffic to induce catastrophic system failures. In recent years, several attacks[1,2] have impressively demonstrated that the software running on embedded controllers can be successfully exploited, often even remotely.

With the rise of the Internet of things (IoT), more non-traditional embedded devices have started to get integrated into personal and commercial computing infrastructures. As a result, security will soon become a paramount issue for the new-age embedded systems.

Inapplicability of Existing Cryptographic Mechanisms: Well-established cryptographic mechanisms (e.g., digital signatures, or MACs) that provide manipulation prevention and authentication can effectively solve most of the embedded system security issues. However, the industry hesitates to adopt those as most embedded devices pose severe resource constraints on the security architecture in terms of memory, computational capacity, energy and time. Given the real-time deadlines, the embedded devices might not be able successfully complete verifications by the deadline rendering all verification efforts useless.

Consider digital signatures that are widely used for data integrity and source authentication. A signature scheme allows a *signer S* who has created pair of private and public keys to *sign* messages so that the signatures can later be *verified* by any *Verifier V* with *S*'s public key. However, RSA and (EC)DSA signatures used in practice today have one severe restriction: their *verification* algorithm can only return a binary answer for the validity of the signature (i.e 0 or 1). Therefore, they may not be useful for a *Verifier* who has limited and predictable computing power or time to completely perform the verification: partial/incomplete verification provide *no* integrity or authentication guarantee whatsoever.

II. Our Vision

Our long-term vision is to solve this appalling problem with employing current cryptographic mechanisms in unpredictably resource constrained environments. In particular, we would like to define cryptographic protocols that can provide some partial/fractional security guarantees if the time and resource constrained protocol participants can only perform some partial computation.

We find that none of existing cryptographic schemes provides such a trade-off between time and security.

[1] Comprehensive Experimental Analyses of Automotive Attack Surfaces: `http://www.autosec.org/pubs/cars-usenixsec2011.pdf`

[2] A Survey of Security Threats and Protection Mechanisms in Embedded Automotive Networks: `https://hal.archives-ouvertes.fr/hal-00852244/file/Studniaetal.pdf`

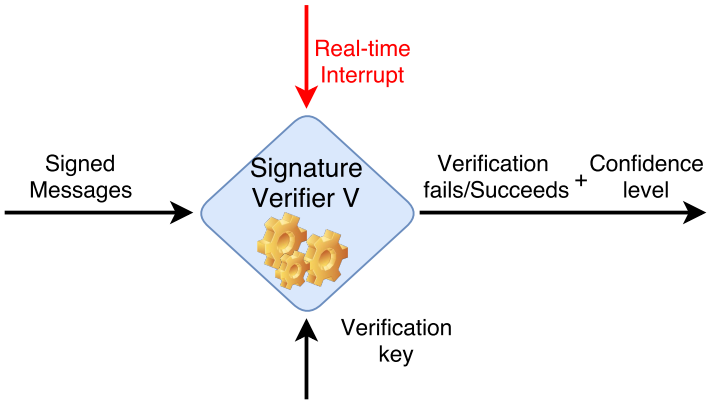

Figure 1: A digital signature (verification) scheme with variable confidence level in $[0, 1]$ decided by the system interrupt

III. Approach and Research Plan

As the first step in this high-risk project, we will consider digital signatures. As shown in Figure 1, our aim is to create a signature scheme in which the verification algorithm allows us to quantify the validity of the signature: more computation the *Verifier V* performs more certain he/she becomes about authentication and integrity. During our initial analysis, we find the hash-based digital signature schemes to be appropriate to the proposed domain. During the current academic year, we plan to develop fully-fledged signature schemes that provides partial verification guarantees, and compare different proposal to each others in terms of industrial applicability. We will then like to communicate with the department's industry partners as we find our signature scheme to be highly useful to their embedded real-time systems.

On the longer run, there is significant research that need to be performed in this challenging area of resource- and time-constrained security. We plan to explore the similar ideas for confidentiality in encryptions, integrity with MACs, and possibly beyond. We believe our revolutionary cryptographic protocols will make the security mechanisms more prevalent in the emerging embedded systems and IoT in general.

IV. Impact

We are observing a growing trend of malicious attacks on vehicular systems. It is inevitable that the next generation vehicular networks will have to employ cryptographic authentication and confidentiality mechanism to mitigate those life-threatening attacks. However, the embedded systems developers will be concerned about computation overhead introduced by those cryptographic mechanisms. The protocols developed in this project can significantly assist the embedded systems developers to allowing them to introduce adjustable security measures fully compatible their critical real-time requirements.

Keywords: Embedded systems; Flexible Security; Resource constraints; Time constraints; Partial Verification.