Restricted Authentication and Encryption for Cyber-physical Systems

Michael Kirkpatrick
Department of Computer Science
Purdue University
mkirkpat@cs.purdue.edu

Elisa Bertino
CERIAS
Purdue University
bertino@cerias.purdue.edu

Frederick T. Sheldon
Cyberspace Sciences & Information Intelligence Research
Oak Ridge national Laboratory
sheldonft@ornl.gov

Abstract

Cyber-physical systems (CPS) are characterized by the close linkage of computational resources and physical devices. These systems can be deployed in a number of critical infrastructure settings. As a result, the security requirements of CPS are different than traditional computing architectures. For example, critical functions must be identified and isolated from interference by other functions. Similarly, lightweight schemes may be required, as CPS can include devices with limited computing power.

One approach that offers promise for CPS security is the use of lightweight, hardware-based authentication. Specifically, we consider the use of Physically Unclonable Functions (PUFs) to bind an access request to specific hardware with device-specific keys. PUFs are implemented in hardware, such as SRAM, and can be used to uniquely identify the device. This technology could be used in CPS to ensure location-based access control and encryption, both of which would be desirable for CPS implementations.

The submitted manuscript has been authored by a contractor of the U.S. Government under contract DE-AC05-00OR22725. Accordingly, the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

1 Introduction

Cyber-physical systems (CPS) [15, 10], which consist of the integration of networked sensors, computational resources and physical devices, pose a number of security challenges that differ from traditional computing architectures [11, 2]. CPS includes critical infrastructure, for example Supervisory Control and Data Acquisition (SCADA) and Digital Control Systems (DCS). Given the vital nature of these systems, it is crucial that CPS provide a greater level of data integrity than traditional distributed systems.

The first challenge for data integrity in CPS is that of provenance, which refers to the origin of the data. As CPS can be one aspect of a complex system, adequate protections must be in place to ensure the claimed source of the data is accurate and tamper-proof. Additionally, the data may be aggregated with other data, yet the origin must be kept intact. The next challenge is to ensure proper access control for the system. The security mechanisms must ensure that only authorized actors insert data into the supply chain, and the integrity of the received data must be guaranteed. In short, CPS requires that the origin of data be secure and traceable, and that the data is delivered without unauthorized modification. To address these issues, we look to advanced techniques in authentication and encryption.

Traditional approaches to authentication and access control are identity-based. In a typical scenario, a user (or a machine with authority delegated by the user) at-

tempting to make an access request presents a set of credentials that make a claim about the user's identity along with a proof that the claim is correct. The proof may take the form of a password or a digital certificate that includes the user's public encryption key. This form of authentication may be of insufficient strength for critical systems, as users have been shown to have poor security practices, such as revealing passwords in exchange for chocolate [1].

Instead of relying solely on identity-based authentication, CPS systems need stronger forms of assurance, including forms of multifactor authentication. Specifically, we are interested in techniques of binding an access request to specific hardware. Attestation techniques have been proposed [12, 13] that partially accomplish this goal. In these schemes, before a server grants access to certain data or services, the server performs a series of tests on the requesting machine. These tests can report on properties of the remote system configuration. The server can then take this information into consideration with regard to the request.

We see three drawbacks to these approaches in the context of CPS. First, these schemes generally assume the presence of a Trusted Platform Module (TPM) [16] that is capable of a number of operations, including various forms of cryptography. This assumption may be too strong for certain forms of CPS. Second, attestation schemes focus on ensuring the machine is configured in an acceptable manner, rather than identifying the hardware itself. As such, attestation cannot necessarily distinguish two machines that are configured in the same manner. Third, someone with physical access to the machine could disable or reset the TPM, thus denying the requisite assurances.

In this paper, we propose the exploration of other hardware-based techniques for CPS, specifically focusing on Physically Unclonable Functions (PUFs). The inherent physical limitations of manufacturing devices introduce minor differences between multiple copies of the same hardware design. PUFs quantify these variations to produce a value that is guaranteed to be unique for each hardware instance. However, PUFs are deterministic, as repeating the PUF evaluation on the same hardware device will always produce the same value. Thus, PUFs can be used to confirm the unique identity of a hardware device.

Once the hardware instance has been identified, CPS can then enforce a number of additional access constraints. For instance, if the location of the hardware is known, spatial constraints can be applied [4]. Other work has focused on the use of contextual factors [9] for pervasive devices. The hardware identity could be considered as one of these factors.

2 Physically Unclonable Function (PUF)

A Physically Unclonable Function (PUF) [3, 6] (also called a Physical Random Function) is a function that creates a unique value dependent on the physical structure of the hardware itself. Approaches to implementing PUFs include utilizing variations in timing measurements in logic gates or building the PUF directly in SRAM, among others. The key property is that executing the PUF on different physical instances of the same hardware is guaranteed to produce a distinct values. However, repeatedly executing the PUF on a single piece of hardware will always produce the same result.

A common use of PUFs is for the secure storage of cryptographic keys [14, 8, 7]. For example, consider the storage of a private key k. When the key is created or installed into PUF-enabled hardware, the PUF is evaluated to produce a machine-specific value m. This value is then combined with the key via XOR to create a value $x = k \oplus m$. The value x then gets stored locally. At run-time, the private key is reconstructed by combining the stored value with the machine-specific value, i.e., $k = x \oplus m$.

Note that x has no value in and of itself. If an attacker were to gain access to the storage on the machine, transferring x to another device would not leak information about the key k. That is, evaluating the PUF on a different device would produce $m' \neq m$. As a result, the reconstructed key $k' = x \oplus m'$ would not be the same as k. Thus, PUF offers a unique ability to bind a cryptographic key to the physical hardware of the machine.

3 Restricted Authentication and Encryption

Given a value that is guaranteed to be unique for each instance of a hardware device, CPS can provide advanced forms of authentication and encryption. First, the PUF output could be used as a unique identi-

fier to restrict access control to certain devices. One method for accomplishing this would be to use the PUF output in a zero-knowledge proof of identity, such as proposed by Feige, Fiat and Shamir [5].

Once the proof of the machine's identity has been verified, the server can make an access control decision based on prior knowledge of the machine. For instance, if the machine's trustworthiness has been previously evaluated, the server could grant full or partial access accordingly. Additionally, if there is a strong linkage between hardware devices and users, binding authentication to physical hardware in this manner could be used to detect and track a malicious insider.

Another way to use the PUF-based hardware identifier would be to create cryptographic keys that are unique to each device. These keys can address the problem of data provenance by signing all data generated from that piece of hardware. Even if the data is aggregated at a later point, the provenance can be preserved through the use of aggregated signature techniques. Also, if the location of the requesting device is known, the PUF approach could enforce a type of location-sensitive encryption.

4 Challenges and Open Problems

One problem with the approach of using PUFs for CPS is the current limited availability of the technology. As described previously, PUFs have been implemented in some types of hardware, such as SRAM. However, many hardware devices are based on technology for which no PUF implementation exists. Creating new types of PUFs for other technologies would greatly expand the opportunities for advanced authentication techniques.

Next, protecting the machine-specific value m at run-time presents a significant challenge. Although all computations involving m or the corresponding secret key k occur on the processor itself, the values must be protected from attacks based on information flows or covert channels. If m can be leaked in any way, a malicious party could then forge the authentication required by emulating the device.

Finally, the use of the secret value m needs to be carefully considered. The value could be used as a secret value for a zero-knowledge proof of identity or as a private key for performing cryptographic signatures. However, the device capabilities may be insufficient for protocols that involve complex operations, such as modular exponentiation or elliptic curve calculations. Thus, finding an appropriate protocol to leverage the machine-specific value appropriately may be challenging.

5 Conclusion

Physically Unclonable Functions (PUFs) offer the ability to evaluate a function, the output of which is unique for each hardware instance. The advantage of this result is that hardware can be uniquely identified to offer strong security guarantees for CPS. Given the strong binding of the value to the given hardware, PUFs offer the ability to provide accurate and tamper-proof data in complex systems, ensuring the integrity and authenticity of received messages. Furthermore, the provenance of the data can be kept intact, even after aggregation. As such, PUFs offer many features that would be desirable for CPS implementations, especially in critical infrastructure.

References

[1] Passwords revealed by sweet deal. http://news.bbc.co.uk/2/hi/technology/ 3639679.stm, April 2004.

[2] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee. Security challenges in next generation cyber physical systems. In *Beyond SCADA: Networked Embedded Control for Cyber Physical Systems*, November 2006.

[3] M. J. Atallah, E. D. Bryant, J. T. Korb, and J. R. Rice. Binding software to specific native hardware in a vm environment: The puf challenge and opportunity. In *VMSEC '08*. ACM, 2008.

[4] M. L. Damiani, E. Bertino, B. Catania, and P. Perlasca. Geo-rbac: A spatially aware rbac. In *ACM Transactions on Information Systems and Security*, 2006.

[5] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing (STOC)*, pages 210–217, 1987.

[6] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas. Controlled physical random functions. In *Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC)*, 2002.

[7] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls. Fpga intrinsic pufs and their use for ip protection. In *Proceedings of the 9th Cryptographic Hardware and Embedded Systems Workshop (CHES)*, pages 63–80, 2007.

[8] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls. Physical unclonable functions and public-key crypto for fpga ip protection. In *International Conference on Field Programmable Logic and Applications*, pages 189–195, 2007.

[9] D. Kulkarni and A. Tripathi. Context-aware role-based access control in pervasive computing systems. In *Proceedings of the 14th Symposium on Access Control Models and Technologies (SACMAT)*, 2008.

[10] E. A. Lee. Cyber physical systems: Design challenges. Technical Report UCB/EECS-2008-8, EECS Department, University of California, Berkeley, January 2008.

[11] C. Neuman. Understanding trust and security in scada systems. In *Beyond SCADA: Networked Embedded Control for Cyber Physical Systems*, November 2006.

[12] R. Sailer, T. Jaeger, X. Zhang, and L. van Doorn. Attestation-based policy enforcement for remote access. In *In Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04)*, pages 308–317. ACM Press, 2004.

[13] D. Schellekens, B. Wyseur, and B. Preneel. Remote attestation on legacy operating systems with trusted platform modules. In *Science of Computer Programming*, pages 13–22, 2008.

[14] G. E. Suh and S. Devadas. Physcal unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th IEEE Design Automation Conference (DAC)*, pages 9–14. IEEE Press, 2007.

[15] P. Tabuada. Cyber-physical systems: Position paper. In *NSF Workshop on Cyber-Physical Systems*, 2006.

[16] Trusted Computing Group. Trusted Platform Module Main Specification. http://www.trustedcomputinggroup.org/, October 2003.