Distributed IoT Attestation via Blockchain

Ira Ray Jenkins, Sean W. Smith
Dartmouth College
Hanover, New Hampshire, USA
{jenkins, sws}@cs.dartmouth.edu

***Abstract*—We propose a novel attestation architecture for the Internet of Things (IoT). Our distributed attestation network (DAN) utilizes blockchain technology to store and share device information. We present the design of this new attestation architecture as well as a prototype system chosen to emulate an IoT deployment with a network of Raspberry Pi, Infineon TPMs, and a Hyperledger Fabric blockchain.**

***Index Terms*—IoT, Remote Attestation, Blockchain, Security, Distributed Systems**

I. Introduction

IoT devices manifest many of the same resource constraints as prior generations of disconnected embedded systems, such as low power consumption, limited hardware support, and prolonged life cycles. Unfortunately, the IoT has also inherited security vulnerabilities from prior hardware, firmware, and software, as well as those generally associated with networked devices. The always-on, inconspicuous, and noninteractive nature of the IoT, combined with security failings, has meant that IoT-targeted attacks are now a legitimate concern.

Attestation is the process by which verifiable evidence about a system's state or properties is shared between devices. The trustworthiness of this evidence is based upon a *root of trust*, often a hardware device like a *trusted platform module (TPM)*. Traditionally attestation has been *static*, with a focus on measured binaries and disk images. More recent work has focused on *dynamic* attestation which seeks to verify runtime integrity.

Many attestation schemes require a priori knowledge of "good" properties. This data is often stored within a database. Arguably, a data storage solution for a heterogeneous, multi-organization IoT attestation network ought to be distributed and decentralized. *Blockchain* provides just such a cryptographically secure, decentralized *distributed ledger*.

In this paper, we propose our *Distributed Attestation Network (DAN)*: a novel architecture for distributed attestation within the IoT. DAN relies on blockchain technologies to store and distribute device information, but also to facilitate attestation through the use of smart contracts. We present a prototype system of IoT-analogues using a network of Raspberry Pi, Infineon TPMs, and a Hyperledger Fabric blockchain.

This material is based upon work supported by the U.S. Department of Energy under Award Number DE-OE0000780. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of United States Government or any agency thereof.

The remainder of this paper is organized as follows: Section II introduces our distributed attestation network. Section III discusses our implementation. Section IV presents some analysis. Section V discusses general network feasibility. Section VI considers works related. We present our concluding thoughts in Section VII.

II. Distributed Attestation via Blockchain

We consider a heterogenous network of IoT-like devices that may be resource-constrained. We assume a dense network such that each network node has multiple immediate neighbors, and all nodes are free to logically communicate. We allow that nodes within this network may be under the authority of diverse, cooperative, but mutually competitive organizations. Finally, we assume that the devices on the network that will participate in attestation must have some root of trust.

The adversary or attacker may be passive or active. We consider primarily an adversary that may introduce malware into a (small) fraction of devices over a given time period. Additionally, the adversary may introduce new devices into the network environment, and supply malicious inputs to public interfaces. As is standard in single-prover attestation schemes, we ignore both denial of service (DoS) and physical attacks in this work.

DAN is the first attestation architecture to utilize blockchain as more than simple distributed storage, but as a prime actor in an attestation protocol. Our distributed attestation network is a generic and flexible attestation architecture. DAN does not specify the attestation protocols, or define the data and properties of interest, or limit the actors and relationships involved. For more details, we refer the reader to the extended version of this paper [11].

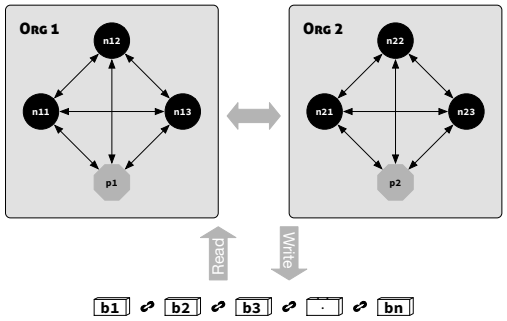

Fig. 1. DAN organizational chart featuring two organizations, each with multiple networked nodes, and a shared blockchain.

978-1-7281-6095-5/20/$31.00 ©2020 IEEE
DOI 10.1109/CCGrid49817.2020.000-7

An example organization chart is shown in Figure 1. Each organization maintains a number of nodes. Additionally, each organization maintains a set of peers—here, $\{p_1\}$ and $\{p_2\}$.

Peer nodes here represent those nodes with access to the blockchain ledger. A network may have one or many peers with which a single node can communicate. In the case of traditional computers, every node in a network might be a peer; however, given the resource constraints of individual IoT devices, it may be necessary to offload the blockchain management to an intermediate and more powerful node.

A goal of a DAN is for the individual nodes within the network to be attested. *Producer* nodes submit attestations into the blockchain. This may be the result of a challenge-response protocol. Alternatively, attestations may simply be submitted on a periodic and autonomous schedule.

Once attestations are present within the blockchain, *validator* nodes are able to evaluate the attested information. The results of such validation are then included in the blockchain, linking a producer and validator with a timestamped and immutable record of attestation. The final nodes within a DAN are the *consumers*. Consumers want to interact with producer nodes; however, there may be distrust in this transaction. Consumers rely on the validated attestations within the blockchain to formulate trust decisions about producers. Thus decoupling the trust relationship between producer and consumer. Figure 2 depicts this scenario.

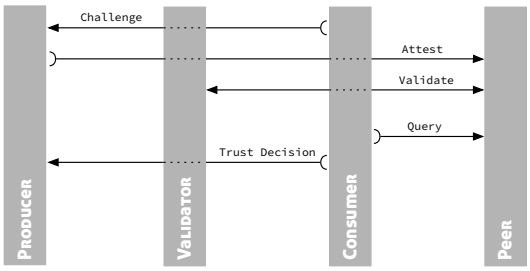

Fig. 2. Example challenge-response protocol within a DAN. The consumer initiates attestation. The producer submits attested information to the blockchain. A validator submits validation to the blockchain. The consumer awaits validation, and finally makes a trust decision.

This sort of network aligns nicely with the envisioned IoT, where devices may perform multiple tasks which in turn depend upon the services of other network devices. Consider, for example, an energy delivery system (EDS) comprising grid operators, consumers, and federal regulators. Grid operators may manage a variety of sensors, controls, and smart meters within their network. An individual consumer may have a variety of "smart" things attached to the network, such as meters, backup generators, and alternative energy production mechanisms. Regulatory officials, while not operating network nodes themselves, have direct interests in validating and monitoring compliance of such critical infrastructure. With a DAN, the devices within the network can be attested in a semi-public, or access-controlled, fashion. Grid operators may be context-dependent producers, consumers, and validators. Service consumers may act as both producers and consumers. Instead of relying on grid operators to self-report, regulators can now query the devices themselves. In this case, regulators may act as validators, having direct knowledge of the hardware, firmware, or software deployed. Some consumers may derive trust from such government oversight; however, building a more diverse trust portfolio for this example might involve the inclusion of original equipment manufacturers (OEMs), distributors, or contractors. In this way, trust relationships can be chosen and distributed, with ground truth device-dependent and decentralized.

III. Implementation

The goal of our implementation was to prove feasibility and provide a testbed for further experimentation. We used Hyperledger's Fabric [3], version 1.4, to provide our blockchain infrastructure. Fabric allows flexible, plug-and-play services for blockchain functionality, such as membership, cryptography, and consensus.

First we simulated a DAN using Docker containers. We utilized one node for each producer, consumer, and validator. Additionally, we relied on a single peer node for blockchain interactions. In our initial implementation, we followed the example challenge-response protocol shown in Figure 2. Attestation and validation were triggered manually. In this case, we did not rely on a trusted computing base (TCB), but assumed the attestations reported were valid. For attestation data, we simulated TPM quotes by generating random measurement lists, and calculating hashes for "known good" states. For these trials, we ignored PKI and signatures on the attested data.

We then built a practical testbed, implementing a DAN using eight Raspberry Pi, models 2B and 3B+, as our IoT nodes. The Pi has become synonymous with IoT research and development. They are low-cost, credit-card sized, relatively powerful, and highly expandable. Each producing Pi used an Infineon Optiga SLB 9670 TPM2.0 iridium board. These boards communicate over SPI using Infineon's Embedded Linux TPM Toolbox 2 (ELTT2).

We setup two "organizations" each with 3 compute nodes and a single *gateway* node. Each organization was assigned a blockchain peer that ran inside a Docker container on a consumer desktop. The same protocol transactions were tested for consistency. Our simulated attestations were produced from random measurement lists that were hashed into the TPM PCRs and read out again. This implementation allows us to further explore a variety of applications.

Producer nodes were scripted to "ping" consumers at regular intervals. Attestations of the producer nodes were submitted to the blockchain on a periodic basis. Additionally, random groups of validators were chosen to verify attestations. We tested several scenarios in which consumers required single and multiple validators to sign off on attestation. Trust decisions by consumers were made on varying aggregate validations, e.g., certain consumers only trust specific validators, require multiple validations, or require more *fresh* validation. On a failed validation, consumers would instantiate

an iptables firewall rule to DROP traffic from the abusing producer. Manual triggers were used to introduce potential errors such as to delay attestations from a producer, force invalid attestations into the blockchain, or interrupt validators from reading attestations or writing their results.

IV. Evaluation

Primary concerns for IoT attestation are the cryptographic and blockchain operations on resource-constrained devices. In our example DAN, the TPM must generate hashes over static measurement lists. To isolate this computation, we performed a comparison between SHA1 and SHA256 hashing on randomized payloads ranging from 1 to 100 bytes. The Infineon TPM requires less CPU time, and is roughly twice as slow as the Raspberry Pi on any payload size. These results were expected given the TPM's 43Mhz transfer rate on the SPI interface, and the relative power of the Raspberry Pi.

Communication within the DAN is ad hoc. A proving device need only attest periodically or when requested. Validators and consumers primarily communicate with blockchain peers. In our conception, these peers are somewhat more robust than the IoT devices on the edge of the network. Thus, communication is thus limited by the throughput of the blockchain peers, as well as the bandwidth and latency of the network.

Each entity within the network needs only the credentials to interact with the blockchain peers. More advanced attestation schemes may require more storage; however, proving devices need only enough storage to generate attestation since all the protocol data elements are stored within the blockchain on peer nodes. Additionally, it is worth mentioning that by adding a physical TPM, a device gains access to some additional non-volatile RAM (NVRAM) (in the case of our Infineon TPM, 6962 bytes).

During the hashing experiments, we monitored the power usage with the combination of a consumer-grade wall-outlet electricity usage monitor and multimeter. While these measurements may lack resolution, their relative comparison is instructive. On average, the Raspberry Pi requires 10% more power than the TPM during hashing. Additionally, at peak load, the Pi draws 5% more power based on watt calculation. These results suggest that, even though the TPM is powered by the Pi, when performing these cryptographic operations the TPM is more efficient.

V. Discussion

A major IoT constraint is often power, with many devices relying on batteries. In the future, we'd like to compare the power draw during common attestation and cryptographic operations between our hardware TPMs and SGX or TrustZone. However, any attestation represents additional overhead. For some applications, runtime attestation may be unnecessary. Attestation may only be needed occasionally, with long (e.g., days) periods between successive attempts. Hardware roots of trust will only become more efficient and smaller. Alternatively, some applications may only need the security guarantees of a software-based attestation method.

In the proof of concept that we built, blockchain operations are performed by peer nodes within docker containers on consumer desktops. In a real-world deployment, these may remain containerized within the cloud. Alternatively, there are current efforts to build so-called "light clients" that may allow resource-constrained IoT devices to interact individually with the blockchain. However, storage will remain a problem. It may be feasible to move blockchain storage to an intermediate device like a gateway or base station, further into a data center, or even the cloud.

There are concerns about scaling given the long running estimation of IoT devices, and the desire to maintain a complete lifecycle history. One potential mitigation for these concerns is checkpointing [10]. Additionally, at least in the case of the current generation of IoT devices, firmware and software updates are few and far-between. When considering dynamic attestation, there are efforts to increase efficiency by only considering security critical sections of code. All of these factors may help to reduce the overhead of blockchain storage and computation.

DAN is the first distributed attestation architecture that utilizes blockchain as a principal component to facilitate remote attestation. It provides flexibility in establishing a given attestation protocol. It mirrors the envisioned topology of IoT systems. And it naturally satisfies the five constraints of an attestation system provided by Coker et al. [6].

DAN facilitates the measurement of diverse aspects. DAN is not limited to a particular attestation method. Both static, load-time measurements and dynamic runtime measurements may be recorded within the blockchain. DAN supports separate domains for measurement. In the prototype we built, we rely on hardware TPMs to facilitate our root of trust. As discussed earlier, hardware mechanisms for trust are evolving to satisfy the constraints of the IoT. Trust anchors are transparent to DAN implementations. Similarly, DAN's trust base is self-protecting. The trusted base for an individual device's attestation may vary depending on services being attested, or the requirements of the validator that is used.The principles of DAN naturally allow multiple verifiers or validators of attestation. In fact, it is easily conceivable that different attestations may be verified by multiple different validators. This creates the opportunity for trust decisions based on a more comprehensive assessment of a target device. Finally, the blockchain can naturally realize an attestation manager by providing a distributed ledger containing all of the measurement and attestation tools currently supported by various devices. The DAN, as we have implemented it with Hyperledger Fabric, can also enable the constrained disclosure requirements by utilizing customized membership services and standard PKI.

VI. Related Work

Yang, Wang, Zhu, and Cao [14] propose two distributed software-based algorithms for detecting compromised nodes within unattended sensor networks. Chen and Wang [5] consider homogeneous wireless sensor networks, and show optimal metrics for how often to attest and how many neighbors to

require. CIoTA [9] is a framework for anomaly detection that relies on blockchain. An anomaly detection model is attested to the blockchain, and used to iteratively build a combined, dynamic model that is distributed to each device. DAN is more general, allowing more applications than just compromise or anomaly detection. Part of this is due to DAN's integration of smart contracts into the attestation scheme over simple storage.

SEDA [4] and SANA [1] provide collective attestation techniques for swarms. WISE [2] is a flexible swarm attestation scheme that allows subsets of devices to be attested based on the history or characteristics of each device. RADIS [7] is a protocol for distributed service attestation. The authors rightly consider the cascading effect of compromised dependent services and describe a method of attestation in which attesting service 1 on device 2, may require attesting service 2 on device 3. These network topologies often require every node within a network to participate in attestation, and limits each node to communications with direct neighbors. Additionally, the end-result of these swarm techniques is that each device within the network is attested. These assumptions reduce the inefficiencies of multiple single-prover attestations; however, it does require all nodes to participate. DAN is more flexible than prior attestation methods. A DAN can efficiently enable both single- and multi-prover attestation schemes in which one or many devices are attested.

Tan et al. [13] consider a multi-tier attestation protocol that relies on more powerful devices with hardware TPMs, and more anemic devices utilizing software roots of trust. Fremantle et al. [8] proposed the use of blockchain for IoT devices with a reliance on intermediate, more powerful devices, termed *pythia*. Liang et al. [12] use SGX-based remote attestation and Hyperledger to build a secure membership services platform. The current implementation of DAN relies on a hardware root of trust; however, software-based attestations are equally supported. DAN facilitates all communication via the blockchain with requests for attestation, subsequent results, and validation all published and distributed. This allows multiple and varied attestation schemes, and a variety of attesting relationships across multiple organizations.

VII. Conclusions

In this paper, we introduced DAN: a distributed attestation network that utilizes blockchain technologies to decentralize, and distribute attestation. DAN is the first attestation architecture in which blockchain integrates directly with the attestation protocol. DAN allows a variety of complex relationships to exist between producers, consumers, and validators. Additionally, DAN is flexible enough to support a multitude of validators using different attestation mechanisms at the same time. By relying on the blockchain, new and interesting applications are possible, for example device lifecycle histories and forensic audits. In the future, we plan to extend current state of the art attestation protocols into DAN, and continue to use our testbed for quantitative evaluation and feasibility testing, such as comparing the power efficiency between hardware and software roots of trust. The security of DAN is currently based upon the assumption of guarantees provided by the underlying hardware, protocols, and cryptographic infrastructure of the blockchain. A more formal model of these primitives and interactions is needed to prove the security and scalability of IoT attestation.

References

[1] M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A. Sadeghi, and M. Schunter, "SANA: Secure and scalable aggregate network attestation," in *Proceedings of the 23rd ACM Conference on Computer and Communications Security (CCS '16)*. Vienna, Austria: ACM, October 24–28 2016, pp. 731–742.

[2] M. Ammar, M. Washha, and B. Crispo, "WISE: Lightweight intelligent swarm attestation scheme for IoT (the verifier's perspective)," in *Proceedings of the 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '18)*. Limassol, Cyprus: IEEE, October 15-17, 2018, pp. 1–8.

[3] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the 13th EuroSys Conference (EuroSys '18)*. Porto, Portugal: ACM, April 23-26, 2018, pp. 1–15.

[4] N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, and C. Wachsmann, "SEDA: Scalable embedded device attestation," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*. Denver, CO, USA: ACM, October 12–16 2015, pp. 964–975.

[5] I. Chen and Y. Wang, "Reliability analysis of wireless sensor networks with distributed code attestation," *IEEE Communications Letters*, vol. 16, no. 10, October 2012.

[6] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen, "Principles of remote attestation," *International Journal of Information Security*, vol. 10, no. 2, pp. 63–81, June 2011.

[7] M. Conti, E. Dushku, and L. V. Mancini, "RADIS: Remote attestation of distributed IoT services," in *Proceedings of the Sixth International Conference on Software Defined Systems (SDS '19)*. Rome, Italy: IEEE, June 10-13, 2019, pp. 25–32.

[8] P. Fremantle, B. Aziz, and T. Kirkham, "Enhancing IoT security and privacy with distributed ledgers - a position paper," in *Proceedings of the Second International Conference on Internet of Things, Big Data and Security (IoTBDS '17)*. Porto, Portugal: SciTePress, April 24-26, 2017, pp. 334–349.

[9] T. Golomb, Y. Mirsky, and Y. Elovici, "CIoTA: Collaborative IoT anomaly detection via blockchain," in *Proceedings of the First Workshop on Decentralized IoT Security and Standards (DISS '18)*. San Diego, CA, USA: Internet Society, February 18 2018.

[10] G. D. Hunt and L. Koved, "Checkpoints for permissionless blockchains," United State Patent 10 523 421, December 31, 2019.

[11] I. R. Jenkins and S. W. Smith, "Distributed IoT attestation via blockchain (extended version)," Dartmouth College, Computer Science, Hanover, NH, Tech. Rep. TR2020-877, February 2020. [Online]. Available: https://www.cs.dartmouth.edu/~trdata/reports/abstracts/TR2020-877

[12] X. Liang, S. Shetty, D. Tosh, P. Foytik, and L. Zhang, "Towards a trusted and privacy preserving membership service in distributed ledger using intel software guard extensions," in *Proceedings of the 19th International Conference on Information and Communications Security (ICICS '17)*, Beijing, China, December 6-8, 2017, pp. 304–310.

[13] H. Tan, G. Tsudik, and S. Jha, "MTRA: Multiple-tier remote attestation in IoT networks," in *Proceedings of the 5th Annual IEEE Conference on Communications and Network Security (CNS '17)*. Las Vegas, NV, USA: IEEE, October 9-11, 2017, pp. 1–9.

[14] Y. Yang, X. Wang, S. Zhu, and G. Cao, "Distributed software-based attestation for node compromise detection in sensor networks," in *Proceedings of the 26th IEEE International Symposium on Reliable Distributed Systems (SRDS '07)*. Beijing, China: IEEE, October 10-12, 2007, pp. 219–230.