Secure Sharing of Design Information with Blockchain

Sven Wohlgemuth[1] Yusuke Mishina[2] Katsuyuki Umezawa[3] Kazuo Takaragi[2]

[1]Hitachi Ltd., R&D Group, Yokohama, Japan <sven.wohlgemuth.kd@hitachi.com>
[2]Advanced Industrial Science and Technology (AIST), Information Technology Research Institute (ITRI)
<{yusuke.mishina, kazuo.takaragi}@aist.go.jp>
[3]Shonan Institute of Technology, Department of Information Science <umezawa@info.shonan-it.ac.jp>

1. Introduction

To defend against evolving cyberattacks, defenders alone have limitations to prevent attacks from multiple and powerful attackers. The effect of Artificial Intelligence (AI) has already led to a change in the understanding of security. AI shows its superior capacity in optimization and completeness of problem solving in several domains with derivation of knowledge. Humans are not considered as competitive anymore. So that humans can benefit from AI-supported machines as intelligence amplifier, information needs to be shared acceptably.

The focus of human is transdisciplinary and unique in his or her capabilities, qualifications, and interests due to biometrics, innate talents, cultural origin, and experiences. The focus of AI is on decidable problems and depends on authentic data or at least with a known error rate. This data comprises the initial model with rules for state transitions, criteria for classification, and eventually training data. The inevitable problem for usable secure human-computer interaction (HCI) is security, i.e., safety as a verifiable statement whether a data breach in an information sharing occurs. This vulnerability, in turn, implies cascading unknown misuse of the affected information. At present, secure information sharing is in general a matter of trust and neither of proof nor test on the existence of data breach.

What is required for usable secure HCI in the general transdisciplinary – in other words multilateral – setting of humans as both teacher and student and AI-supported machines as intelligence amplifier are transaction-based agreements on information sharing with personal accountability on security incidents and compliance. In other words, regarding information sharing, you should first decide the rules for an information sharing and then take accountability so that each will keep it. But with whom should you decide the rules and on which premise?

With our work, we show a new way for defenders to collaborate closely and to make the necessary security by design for the transaction phases of an information sharing. The proposal of our scheme is use of cryptographic-based blockchains as an open distributed trust database in addition to vulnerability databases for evaluating authentication of information and reputation of identities. It is not perfect so that all vulnerabilities on data breach can be detected, but compliance with documented contractual information sharing is verifiable. For reducing vulnerabilities of data breach in the information phase of a transaction, our scheme allows a secure search on security design information.

2. Secure Search for Threat Analysis

A sharing of security design information is a transaction between at least two and at present in general between three parties. Cryptographic scheme of digital signature should achieve accountability in distinguishing between defenders and man-in-the-middle attacker or compromised identities. If two defenders cannot establish an authentic channel for the necessary key exchange to prevent a man-in-the-middle attack, a third party acts as an intermediary and so as central point of control. Whereas the limitation of the security model of access control are well known, technological development in cryptoanalysis and scalable computing resources turn mathematical hard problems as foundation of cryptography into solvable ones. This leads to a universal break of the underlying cryptographic key management and, in turn, on verifiable personal accountability [3].

The current approach on improving security design documents vulnerabilities as Open Data except for Zero-Day exploits and incidents. Fail-stop digital signature schemes allow to detect a compromise of the cryptographic signature key pair. This information is on events but not on the necessary data provenance of security design information as Ground Truth to judge on accountability on multilateral security, i.e., privacy of an information sharing.

Our way uses blockchain as a distributed ledger for long-term preservation of Open Data and its reliable broadcast among registered identities, i.e., anonymized audit trail on use of registered digital signature keys, authorizations, and granted access decisions. The mode of operation for reporting on AAA for accountability is described in [4].

2.1 Phase 1: Check on Compliance

Instead of immediately sharing security design information with inevitably vulnerable identities, our way is to anonymously first search for the required information and then to establish a transaction-specific contract to define the rules for this given information sharing. In the first phase, to confirm whether a defender can trust the other party anonymously, the requesting defender asks for a proof of the desired properties of the requested design information. Like allowing proof of membership for a property set, our

way allows proof on inequality, e.g., as given by anonymous credential system [1]. The replying identity provides this proof zero-knowledge so that both his or her identity and concrete details on the security design information remain protected. Whether this certified security design information is indeed authentic is the result of an audit of the certification's data provenance including check on compliance of the accountable certifying identity, i.e., audit on false positive of a data breach and balancing the related known vulnerabilities with proven compliance. This realizes a secure – in other words privacy-preserving – search. It requires Ground Truth on data access, compliance to the related rules, and on cryptographic signature key pairs. Figure 1 illustrates the cryptographic protocol flow between two machines O_H and O_P on getting access to security design information of human O_S and his or her data controller O_C. The auditor O_A has solved the next block.

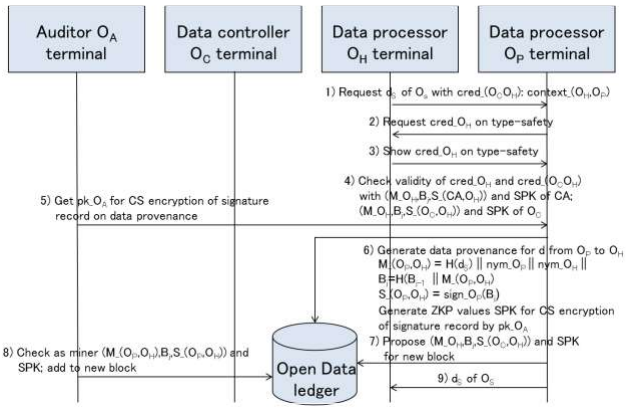

Fig. 1 Check on compliance

2.2 Phase 2: Document Contract on Usage

After a search has been completed successfully in finding the desired information, the requesting and providing identities agree in the second phase on the rules, i.e., contract for this information sharing, and generate the related Ground Truth on authorization. Informatics provides with delegation of rights a cryptographic-based formalization of rules into smart contracts. Accountability on their compliance requires reliable broadcast and long-time storage of these authorizations together with audit log of access decisions of the acting identities. This is personal information. Enhanced with zero-knowledge proof and hysteresis digital signatures our scheme allows a privacy-preserving generation of Ground Truth on accountability. By documenting smart contracts and access decisions, the premise for a proof on accountability on privacy is given. Figure 2 illustrates the cryptographic protocol run.

Our way of using cryptographic-based blockchains as an open distributed vulnerability and trust database has another effect: It realizes a verifiable reference monitor as the trusted computing base (TCB) for information sharing without single-point of failure and with economic compensation for accountability and incentive for auditing on compliance [3]. Sharing information is in economics a trade of property rights on shared goods. With our scheme for secure delegation of rights, we introduce the kernel for a secure open marketplace on trading rights on use of security design information including secondary use. Our scheme, in turn, introduces price discrimination for a trade of rights in addition to the current practice of anonymization as with k-anonymity or differential privacy.

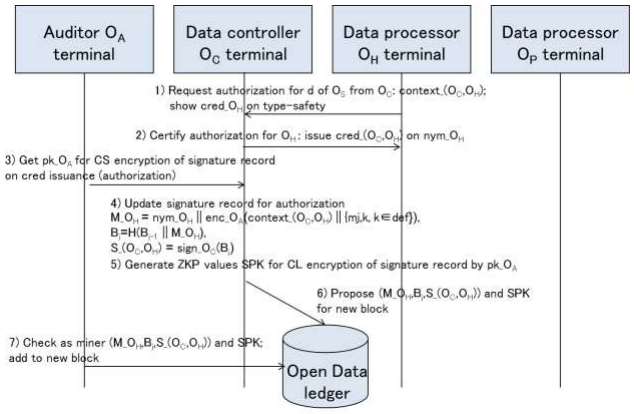

Fig. 2 Document contract on using

3. Call for Participation

We call for contributions in usable secure HCI for defenders with AI as intelligence amplifier by scientific exchange, R&D activities, risk scenarios, and technology transfer for best practices, e.g., ISO-IEC 27035 [2], to name a few options. Bootstrapping of our scheme should be based on registered identities in a privacy-preserving identity management system. The ultimate expected effect is a sustainable knowledge society by "Unity in Diversity".

Acknowledgments

This work was supported by Council for Science, Technology and Innovation (CTSI), Cross-ministerial Strategic Innovation Promotion Program (SIP), "Cyber Security for Critical Infrastructure" (funding agency: NEDO).

4. References

[1] IBM Research Zurich Security Team, Specification of the identity mixer cryptographic library, version 2.3.40, Technical Report, IBM Research, Zurich, 2013.

[2] ISO/IEC JTC 1/SC 27/WG 4, Information Security – Security Techniques – Part 3: Guidelines for incident response operations, Working Draft, June 2018.

[3] Takaragi, K., Wohlgemuth, S., "Current Situation and Issues of Cryptography and Quantum Computer," Practice, policy and law of blockchain, Edited by Takashi Kubota, Chuokeizai-sha Inc, pp. 131–153, 2018.

[4] Wohlgemuth, S., Takaragi, K., Privacy-enhancing Trust Infrastructure for Process Mining, IEICE Transactions of Fundamentals of Electronics, Communications and Computer Sciences Special Section on Cryptography and Information Security Vol. E101-A, No.1, IEICE, pp. 149-156, January 2018.