The Application of Blockchain in Advancing Information Security

Dr. Yuanxiang John Li
School of Management
Harbin Institute of Technology
Harbin, China
yxli@iastate.edu

Dr. James Davis
College of Business
Iowa State University
Ames, Iowa
davis@iastate.edu

Extended Abstract:

In the era of big data and analytics, information assets are one of the most valuable intangible productive capital for a company to compete with its rivals. From lead generation and conversion to customer care to analysis of performance, the integrity and confidentiality of information assets is of utmost importance to the viability and competitiveness of the business. In recent years, information systems and services have become interdependent and complex, making the task of protecting such sensitive information extremely challenging. As we are reminded on an almost daily basis with accounts in the news of data breaches that cause considerable damage to corporate and individual victims, information assets are continuously under attack from external actors as well as current employees ("insiders"). While their methods may vary, their goals are similar.

Classic approaches to securing information center on building defenses to handle the most aggressive attack by encapsulating information within layers of diverse protection mechanisms. Contemporary security architectures support extensive monitoring and recovery methods to detect and contain an attack before the end goal is achieved. In contrast, we will explore here the notion of improving information security through an approach that undermines the motivation of an actor to the point where carrying out an attack becomes fruitless. Specifically, we rely on the Theory of Bounded Rationality to show how the application of Blockchain technology can reduce the motivation for would-be intruders where the goal is financial gain, thereby potentially reducing the occurrence of information breaches in the cases considered.

Rationality is widely used as the core assumption for studying individual behaviors in microeconomic models. It assumes that one shall always behave selfishly. Accordingly, the rational agent is assumed to consider all available information and potential costs as well as benefits in determining preferences, and to act consistently in choosing the self-determined best choice of action. Rational choice theory also assumes that an individual has a well-organized and stable system of preferences, and is capable of finding the highest attainable point on a preference scale among all alternative choices. Herbert A. Simon (1955) instead argues that humans are limited for the tractability of the decision problem, the cognitive limitations of his minds, and the time available for him to make the most optimal decision. When an individual uses heuristics to make decisions rather than a strict rigid rule of optimization due to his inability to process so many complex alternatives, this is Bounded Rationality. This Theory of Bounded Rationality has been widely used in economics, political science and related disciplines for its

practical view of human rational decision making (Gigerenzer and Selten 2002). However, for protecting information assets and preventing data breaches from a managerial perspective, bounded rationality is underexplored.

Essentially, stolen information can be sold or traded because it has value. Value and profitability is contextual. For example, stolen email accounts and passwords are abundantly available and therefore are of limited value generally; conversely, stolen medical records can be leveraged for a higher profit and are therefore more valuable. Likewise, corporate intellectual property may be of great value to competing organizations. We note that data protected by strong encryption has little value to an attacker if it cannot be decrypted.

There are three generally recognized goals that motivate an actor to carry out a cyber-attack: monetary gain; nation sate or political purposes; and personal emotional self-actuation (e.g., revenge or curiosity). We focus on those intrusion activities based on monetary gain although the other two motivations for intrusions are also important. We believe cutting off intruders' avenue to "cash out" stolen data should be a key security strategy. We claim that emerging Blockchain applications, specifically cryptocurrencies, may have the basic properties needed to thwart external and internal attacks by eliminating the ability of the attacker to create personal financial gain.

There are several key properties of the Blockchain ecosystem (Murck 2017) that make it interesting to consider in the context of improving information security. Processing occurs through coordinated distributed agents working on replicated and consistent copies of a transaction ledger, thereby alleviating the need for a central trusted organization. The distributed nature of the ledger effectively makes the ledger immutable to attackers. Communication is robust, occurring in a peer-to-peer fashion without trusted intermediate nodes. The content of transactions and the identity of participants is masked through the use of public key cryptography. Finally, the transactions themselves are able to execute code when processed, which can be used to implement, for example, policy directives.

These basic properties of Blockchain applications make it difficult to steal objects of value and transfer ownership to the attacker. Transferring ownership would require circumventing layers of encryption as well as updating at least half of the distributed ledgers that track transaction for a particular Blockchain application. The inability to transfer ownership renders a cryptocurrency token useless (or a general object invalid) to an attacker because it cannot be used in subsequent transactions. In the end, the motivation of an attacker to steal protected objects for personal financial gain is significantly reduced.

References:

Gigerenzer, G., and Selten, R. 2002. Bounded Rationality: The Adaptive Toolbox. MIT press.

Murck, P. 2017. "Who Controls the Blockchain?", from https://hbr.org/2017/04/who-controls-the-blockchain

Simon, H. A. 1955. "A Behavioral Model of Rational Choice," The quarterly journal of economics (69:1), pp. 99-118.