Identification, Authentication, and Authorization

Cristina Laing

Cybersecurity Principles

CYSE 600

August 6, 2021

Dr. George Mikulski

Old Dominion University

Author Note

This is my own work and has been done solely by me. This paper has been written for the Old Dominion University's CYSE-600 Cybersecurity Principles class and not used for any other purposes.

Cristina Laing

Abstract

This essay looks at two published papers that explore access control concepts such as authorization, identification, and authentication in two different settings. This paper will focus on the issues access control (i.e., authorization, identification, and authentication) will resolve and what complications each setting present. This paper will compare the methods and conclusions each paper comes to, as well as any gaps or limitations in each field.

Interchangeable? Identification, Authentication, and Authorization

Security in the cyber world is vast and complex. One major security topic is access control. Access control is encountered by all of us daily, and its continuously going through modifications to keep up with both standards in the security sector and criminal sector. Though access control is used by everyone every day, the key building blocks that makeup access control: identification, authentication, and authorization, are not fully understood by users and are spoken about interchangeably. Before moving on with this paper, let us discuss these terms

- Identification is the act of showing a person or thing's identity. In other words, knowing who somebody is
- Authentication is the act of proving the identity of the person or thing
- Authorization is the task of specifying access rights/privileges to resources, such as persons and things

The internet has changed the world, top to bottom, from the individual level up. Most of the population owns smartphones devices, and in addition, organizations, businesses, and governments are migrating many of their services online. As a result, we are constantly identifying, authenticating, and authorizing without realizing it. The amount of data and the type of data that is interchanged daily is a concern, though when it comes to new tech trends (i.e., IoT or Internet of Things), convenience trumps security. Nevertheless, in specific sectors establishing robust and reliable access controls is vital, such as infrastructure, healthcare, and voting.

In the paper, *Block Enable Online-Voting System*, the authors Shah, Sodhia, Saha, Banerjee, and Chavan propose a blockchain-enabled online-voting system that will allow a secure voting method in the near future. In a second paper, *Identity Identification and Management on the Internet of Things*, authors Houhamdi and Athamena argue that user

identification, authentication, and authorization are required to keep confidential and private data flowing from machine-to-machine (M2M) in an IoT environment; the authors propose a Device Recognition Algorithm.

Similarities can be observed between the two papers:

- Both papers propose a multilayer method of stacking identification, authentication, and authorization.
- Both papers focus on the user to initiate identification, authentication, and authorization. Though IoT is mainly autonomous, the authors of Identity Identification and Management on the Internet of Things identify the user as a central component of the IoT.
- Both papers suggest that their access control methods are extensible, dependable, scalable, and flexible.

In *Block Enable Online-Voting System*, the device recognition algorithm incorporates various login methods, serving different devices and different situations for a single user (i.e., username, password, or key) therefore allowing for flexibility and extendibility. Differences are also evident between the two papers. First are the different methods used to establish control access effectively. For example, in *Block Enable Online-Voting System*, authors suggest using a combination of Blockchain, hashing, voter registration, and voter login. In contrast, the authors of *Identity Identification and Management on the Internet of Things* suggest using a two-list system. One list is assigned to a user listing all devices belonging to that user. While the second list, previously compiled, is used to compare the number of devices. Second, though both papers are on the topic of access control, *Block Enable Online-Voting System* is more concerned with the integrity of all data, and *Identity Identification and Management on the Internet of Things* is

concerned with authentication in a homogenous environment. Third and final, it is essential to point out that protecting the data of individuals using IoT is important; however, devising an electronic voting system for any country with a thriving democracy brings a different level of responsibility.

Challenges encountered with establishing access controls in the IoT environment, Houhamdi and Athamena discovered, that the number of devices one individual managed and the multiple identities one individual possessed made it difficult for identity management systems to work efficiently. Due to identity management systems only successfully working when all identities and devices are established at inception. Shah et al. ran into the challenge of the size of the operation. In Shah et al., paper on e-voting, the author explains that the proposed system has only been used for small businesses. In addition, the proposed system does away with hardware such as Electronic Voting Machines that have been approved and used by many governments. Governments will push back on a system that is built on user devices with no oversight.

In conclusion, both papers present good algorithms and systems to establish strong access controls: identification, authentication, and authorization. The research in the paper approaches the issue of privacy and integrity from different perspectives. Nevertheless, both encounter scaling challenges due to the number of homogenous devices, size of the population, and multiple identities per user. For example, in *Block Enable Online-Voting System*, a significant gap is that the Blockchain process for electronic voting has only been applied on a small scale. Thus, there is no assurance that the proposed system will work on a larger scale. In comparison, *Identity Identification and Management on the Internet of Things* designates significant responsibility to the user as the operator of the IoT ecosystem, which does not account for leads the degrees of technological knowledge between users. Nevertheless, these two papers are a

fruitful start to the topic of access controls. Perhaps in the future, a well-secure IoT ecosystem will complement a secure e-voting system.

References

Houhamdi, Zina, & Athamena, Belkacem. (2020). Identity Identification and Management in the Internet of Things. International Arab Journal of Information Technology, 17(4A), 645-654.

Shah, Akhil, Sodhia, Nishita, Saha, Shruti, Banerjee, Soumi, & Chavan, Madhuri. (2020). Blockchain Enabled Online-Voting System. ITM Web of Conferences, 32, 3018.