Information & Security: An International Journal

Sadiku, Alam, and Musa, vol.36, 2017 https://doi.org/10.11610/isij.3604

INFORMATION ASSURANCE BENEFITS AND CHALLENGES: AN INTRODUCTION

Matthew N.O. SADIKU, Shumon ALAM, and Sarhan M. MUSA

Abstract: Information assurance (IA) is the practice of protecting and defending information systems by ensuring their availability, confidentiality, integrity, authentication, and nonrepudiation. As a discipline, IA grew from the practice of information security. It plays a crucial role in a networked infrastructure of e-commerce, e-business, and e-Government. For this reason, IA is a serious worldwide concern of organizations, industry, governments, and academia. This paper provides a brief introduction on information assurance, the benefits it brings, and the challenges in the implementation of the concept.

Keywords: Information assurance, information goods, information services, information security, computer security.

Introduction

Due to security concerns, organizations worldwide need to continuously seek safety and protection of information assets such as patient information, key components of the technical information system, and critical personnel. Consumer fraud on the Internet is mounting, resulting in financial losses and distrust in e-commerce websites. Information assurance (IA) has been proposed to counter this trend. It is the process of protecting information from theft, destruction, or manipulation. IA is increasing in importance as threats (e.g., virus, rumor) abound in the highly connected and distributed information sharing environment.

The term "information assurance" was first used by the U.S. government. Information assurance is an interdisciplinary field which requires expertise in computer science, systems engineering, law, risk management, information security, forensic science, and criminology. It plays a crucial role in the information infrastructure that supports commerce, banking, telecommunications, health care, and national security.

Information assurance is more inclusive than information security in that it involves not only protection and detection but includes survivability and dependability of the information system that has been subject to successful attack.

Pillars of Information Assurance

Information assurance includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.

- *Integrity*: This is making sure that no one tampers with an information system. IA maintains integrity by having anti-virus software in place so that data is not tampered with.
- *Availability*: This ensures that information is timely made available to users who are allowed to have reliable access to the information system. This may involve protecting against any threat that could block access to the system.
- *Authentication*: This is ensuring that users are who they say they are. This is done using user names, passwords, biometrics, tokens, etc.
- *Confidentiality*: This ensures that information is kept confidential. For example, confidentiality is important in the military, where only people with clearance can access classified information.
- *Nonrepudiation*: This ensures that the sender of the data is provided with proof of delivery by the recipient so neither can later deny having processed the data.

IA involves all of the people and technologies employed to ensure that the fundamental pillars are satisfied throughout the lifecycle of the information system. These five pillars are not independent. Interactions between them can be problematic. For example, availability introduces conflicts with at least three of the other four pillars – confidentiality, integrity, and authentication.[1]

Benefits and Challenges

AI promises to provide effective and efficient ways to protect information systems. This can be challenging even with the most advanced technology and trained IT professionals. Some of the benefits of effective IA include operational benefits, tactical benefits, strategic benefits, and organizational benefits. These benefits are illustrated in Figure 1.[2]

There is a need to produce more qualified IT professionals in information assurance to meet the workforce shortage. It is urgently imperative that students in computer science, engineering, and business be trained in IA. The long-term goal may be to develop a track in IA at the undergraduate and graduate levels. Such efforts will provide

students with technical concepts as well as hands-on experience in securing the world's information systems.[3] Companies such as Cisco, SANS, and CompTIA provide industry-based certifications on IA. But training students for degrees and certificates in IA is challenging. It is difficult to have a consensus on what to cover and to determine a measure of success. Due to the fact that Information Assurance is a relatively new field of study, it suffers accreditation.[4]

Success of IA policy critically depends upon whether employees comply with it. The propensity for IA compliance may vary from individual to individual depending on attitude and previous experience with technology. An employee who has a positive attitude toward technology will have a stronger intention to comply with IA policy.[5] Another challenge with IA is the pressure on IT professionals to remain current with the ever-changing security technologies.

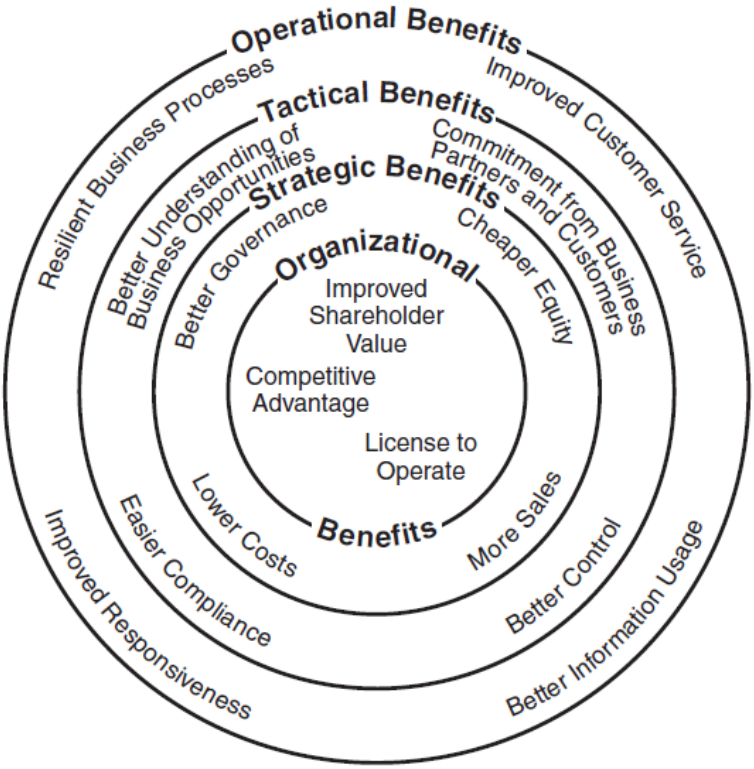

Figure 1: Benefits of Effective Information Assurance.

The commonly assumed attributes of sensor nodes, such as low energy, low computational power, unattended operation, and wireless connectivity have posed as challenges in implementing IA in sensor networks.[6]

Conclusions

Effective information assurance is crucial to reliable management decision-making, lasting customer trust, and good governance in all industry and government. An effective approach to IA requires an on-going assessment of evolving cyber threats. IA is of both national and international concern because of the increased reliance of governmental, military, and financial institutions on networked infrastructure. There are standards on information assurance issued by several national and international bodies.

References

1. Kelce S. Wilson, "Conflicts among the Pillars of Information Assurance," *IT Professional* 15, no. 4 (2013): 44-49, https://doi.org/10.1109/MITP.2012.24.
2. Jean-Noël Ezingeard, Elspeth McFadzean, and David Birchall, "A Model of Information Assurance Benefits," Information Systems Management 22, no. 2 (2005): 22-29, https://doi.org/10.1201/1079/45159.32.11.20050501/87704.1.
3. Cynthia Y. Lester, Hira Narang, and Chung-Han Chen, "Infusing Information Assurance into an Undergraduate CS Curriculum," *Proceedings of the Second International Conference on Emerging Security Information, Systems and Technologies SECURWARE'08* (Cap Esterel, France, 25-31 August 2008), 300-304, https://doi.org/10.1109/SECURWARE.2008.63.
4. Stephen Cooper, Christine Nickell, Victor Piotrowski, Brenda Oldfield, Bill Caelli, Lance Hoffman, et al., "An Exploration of the Current State of Information Assurance Education," *ACM SIGCSE Bulletin* 41, no. 4 (2009): 109-125, https://doi.org/10.1145/1709424.1709457.
5. Sherrie Drye Cannoy and A.F. Salam, "A Framework for Health Care Information Assurance Policy and Compliance," *Communications of the ACM* 53, no. 3 (2010): 126-131, https://doi.org/10.1145/1666420.1666453.
6. Budhaditya Deb, Sudeept Bhatnagar, and Badri Nath, "Information Assurance in Sensor Networks," Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications WSNA'03 (San Diego, CA, 19 September 2003): 160-168, https://doi.org/10.1145/941350.941373.

About the Authors

Matthew N. O. SADIKU is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE. His major research interests are in computational electromagnetics and computer networks.
E-mail: sadiku@ieee.org.

Shumon ALAM is the director and researcher at Center of Excellence of Communication Systems Technology Research (CECSTR) and SECURE Center of Excellence respectively at Prairie View A&M University. His research interests are in the areas of control, communication systems, networking, cybersecurity, and signal processing.
E-mail: shalam@pvamu.edu.

Sarhan M. MUSA is a professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow. E-mail: smmusa@pvamu.edu.