Journal of
Electrical & Electronic Systems

Hu, J Electr Electron Syst 2013, 2:2
DOI: 10.4172/2332-0796.1000111

Review Article Open Access

Challenges in Building a Trustworthy Network

Yen-Hung Hu*

Department of Computer Science, Hampton University, Hampton, Virginia 23668, USA

Abstract

An open challenge in trustworthy computing is the development of a trustworthy network since network plays an essential role of current computing infrastructure (e.g., grid computing, cloud computing, etc.). In order to have a trustworthy network, security, privacy, and reliability must be protected on every major network component. For instance, if there is no trusted mechanism to enforce security protection of every data transaction on major network components, a network cannot be relied on performing trustworthy computing. It has been observed that trustworthy network cannot be practically achieved if there is no trusted integration of major network components. In this paper, we discuss the challenges in building a trustworthy network and develop a trustworthy network model that is both scalable and interoperable with existing and future network architectures.

Keywords: Trustworthy computing; Trustworthy network

Introduction

It seems there was no proper definition of trustworthy until Mundie et al. [1] in 2002 raised the key questions of considering trust from the user's point of view and brought this concept to public attention. In November 2003, Computing Research Association (CRA) sponsored its second "Grand Research Challenges in Computer Science and Engineering" conference to define technical and social challenges in trustworthy computing [2]. In March 2005, Microsoft revealed its approach of improving software trustworthiness [3] by depending on the Trustworthy Computing Security Development Lifecycle (SDL) to enhance software to withstand malicious attacks. One month later, the National Science Foundation (NSF) established the Cyber-security center TRUST led by University of California at Berkeley, to investigate key issues of computer trustworthiness [4]. The NSF continues to support trustworthy computing research and education programs throughout various resources and initiates.

Several researchers have studied the implementation of trustworthy systems [5-13]. However, we have observed that trustworthiness could not be achieved if there is no trusted integration of major network components. For instance, without trusted data, a system can't be trusted to perform trustworthy computing.

The remainder of this paper is organized as follows: Section 2 discusses the challenges in building a trustworthy network. Section 3 introduces a novel trustworthy network model. Section 4 describes X-axis: countermeasures in the trustworthy model. Section 5 describes Y-axis: trustworthy characteristics in the trustworthy model. Section 6 describes Z-axis: network components in the trustworthy model. Section 7 concludes this paper and points out future work.

Challenges in Building a Trustworthy Network

There is no mature implementation of building a trustworthy network although the concept has been discussed more than ten years. We have observed that trustworthiness could not be achieved if there is no proper integration of major network components. Several examples are listed as follows.

- Difficulty in verifying network components: The biggest challenge of the implementation is in verifying network components to ensure they are capable of protecting security, privacy, and reliability. Since hardware and software are manufactured by various vendors across different countries, quality control relating to security, privacy, and reliability is very difficult to achieve. Vulnerabilities could exist in some of them and trigger threats.
- Difficulty in administrating network components: In case management relating to security, privacy, and reliability of network components is guaranteed, vulnerabilities of the network could be eliminated and trustworthiness of the network would be achieved. However, since network components usually cross several different domains and are managed by various administrations, the operation to ensure the protection of network security, privacy, and reliability is very complicated and difficult to achieve.
- Difficulty in protecting data crossing over different network components: Although every network component could implement its own mechanisms to protect network privacy, security, and availability, there are some potential threats could exist in the gap between two components. For instance, the gap between hardware and software. Halderman et al. [14] demonstrated a technology to bypass all disk encryption methods.

To conquer challenges and make it possible to build a trustworthy network, there are some regulations and policies must be implemented. This is not easy when various network domains and components are involved. However, just like the ISO 9001, it would be doable while demands increase.

Trustworthy Network Model

In this paper, we depict a novel trustworthy network model. Our approach is based on an observation that trustworthiness cannot be accomplished by technology or any countermeasure solely. It requires teamwork and needs to integrate every countermeasure together.

***Corresponding author:** Yen-Hung Hu, Department of Computer Science, Hampton University, Hampton, Virginia 23668, USA, E-mail: yenhung.hu@hamptonu.edu

Received July 20, 2013; **Accepted** September 10, 2013; **Published** September 12, 2013

Citation: Hu YH (2013) Challenges in Building a Trustworthy Network. J Electr Electron Syst 2: 111. doi:10.4172/2332-0796.1000111

Copyright: © 2013 Hu YH. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

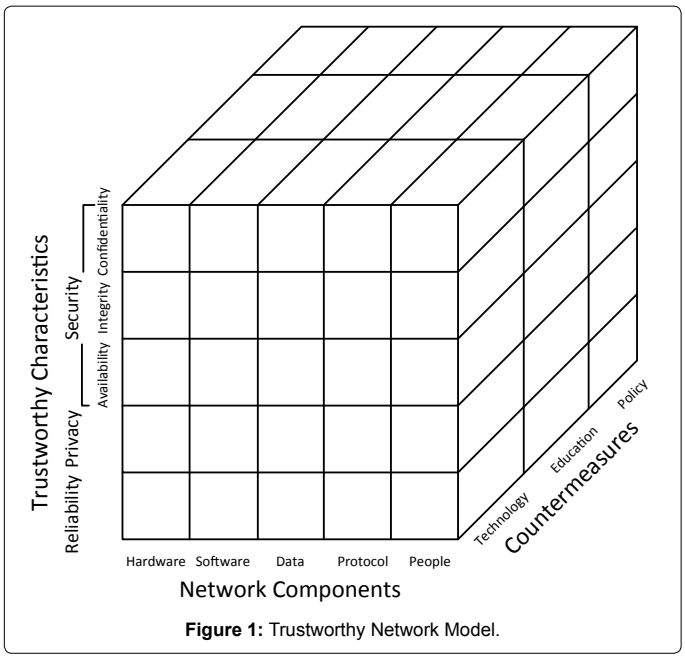

Figure 1: Trustworthy Network Model.

Meanwhile, every network component needs to be considered as a whole.

The trustworthy network model used to enhance the implementation of a trustworthy network is shown as the Figure 1. We integrate countermeasures, trustworthy characteristics, and major network components into this model.

This 3D model includes three axes and 75 cells (i.e., 5 x 3 x 5).

- X-axis: This axis introduces five major network components ($\{x_1, x_2, x_3, x_4, x_5\}$): hardware, software, data, protocol, and people.
- Y-axis: This axis covers three countermeasures ($\{y_1, y_2, y_3\}$): technology, education, and policy.
- Z-axis: This axis represents three trustworthy characteristics ($\{z_1, z_2, z_3\}$): security, privacy, and reliability. After thoroughly examining the security characteristic, we update this axis to five trustworthy characteristics ($\{z_1, z_2, z_3, z_4, z_5\}$) since security could be achieved by enforcing confidentiality, integrity, and availability.

To interpret this model, let's consider the instance: John is an IT staff in the ABC Company and responsible for developing a reliable framework in the company's trustworthy network project. What kind of education background does he need to accomplish this task?

To answer this question, let's check with the trustworthy network model. Since John is IT staff, his education background needs to cover all five network components: $\{x_1, x_2, x_3, x_4, x_5\}$, one countermeasure: $\{y_2\}$, and one trustworthy characteristic: $\{z_1\}$, it will need five cells (i.e., $\{x_1, y_2, z_1\}$ $\{x_2, y_2, z_1\}$ $\{x_3, y_2, z_1\}$ $\{x_4, y_2, z_1\}$ $\{x_5, y_2, z_1\}$) to achieve his goal. Briefly, John needs to possess sufficient knowledge to enforce reliability in hardware, software, data, protocol, and people involving in the project. Therefore, to accomplish this trustworthy network project, the ABC Company needs to address all 75 cells.

X-Axis: Countermeasures

To build a trustworthy network, the protection of security, privacy, and reliability of major network components must be ensured. Many solutions have been proposed to improve the protection [5-13]. In general, they can be categorized into three types: technology, policy, and education.

- Technology: Technical solutions, no matter hardware or software, relating to the protection of network security, privacy, and reliability are included in this category. For instances: hardware and software access control, intrusion detection, firewall, cryptosystem and tools, redundant systems.
- Policy: Policies are regulations and rules in the workplace relating to the protection of network security, privacy, and reliability. Policies binding to the expectations of employees perform as organization laws. These expectations including acceptable and unacceptable behaviors must be described in detail and distributed to all individuals who are agreed to comply with them. Once policies relating to the protection of network security, privacy, and reliability are issued. Administration in the organization must enforce them without doubt.
- Education: Education includes formal and informal training programs relating to the protection of network security, privacy, and reliability. Employees involving in network security, privacy, and reliability operations must possess certain degrees and certificates addressed in the employment policy.

Y-Axis: Trustworthy characteristics

The main objective of building a trustworthy network is to ensure there is a network that is trusted to perform data acquisitions and transactions. This trust involving technology, policy, and education must be enforced to protect network security, privacy, and reliability.

- Security: The assessment of a security implementation is in the measurement of the degree of protecting information confidentiality, integrity, and availability. Metrics of assessing system components exhibiting properties intrinsically or extrinsically that matter security has been widely discussed [1,3,15-18]. Cryptography has served as the major security countermeasure to protect confidentiality, integrity, and availability of data along with those components which touch such data. Two approaches have articulated and promoted the original security metrics to more comprehensive level by adding more security countermeasures and characteristics: McCumber Cube [15,19] and Maconachy, et al. Information Assurance Model [16].
    - The McCumber Cube is a three-dimension cube having three axes: (X-axis) Information States including storage, processing, and transmission; (Y-axis) Information Characteristics including confidentiality, integrity, and availability; and (Z-axis) Security Countermeasures including policy, education, and technology. It can be depicted as a 3 x 3 x 3 cube with 27 cells.
    - The Maconachy, et al. Information Assurance Model adds two more security characteristics (i.e., authentication and non-repudiation) into Y-axis of the McCumber Cube and updates its Y-axis title from Information Characteristics to Security Services. The Maconachy, et al. Information Assurance Model includes 45 cells (i.e., 3 x 5 x 3) and can facilitate more security services than the McCumber Cube.
- Privacy: You shall gain control over your own information.

Others involving in using your information shall adhere to fair information principles [1,17]. For instance, after receiving a treatment from your dentist, anyone working in the dentist office can not disclose your information to others who are not involved in this treatment without your permission. To protect privacy, enforcement of policy and education will be much more efficient than that of technology. Currently there is no clear framework that is able to enforce this requirement and conduct proper assessment without disrupting mutual trust between services provides and receivers. Several U.S. laws [19] have been issued to deal with this matter.

- The Federal Privacy Act of 1974 regulates government agencies to hold information of individuals and businesses accountably if such information is released without permission.
- The Electronic Communications Privacy Act of 1986 regulates the interception of wire, electronic, and oral communications.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulates the collection, storage, and transmission of sensitive personal health care information.
- The Financial Service Modernization Act of Gramm-Leach-Bliley Act of 1999 regulates the usage of personal information facilitated by banks, insurance, and securities firms.

- Reliability: In brief, reliability means availability and correctness. Systems for providing services must be always available and correct and commit to fulfill every request from the legitimate users. This topic brings many challenges beyond current security deployments even when the most promising cryptographic system and security model are implemented. Therefore, an approach that considers redesigning the strategy of installing and deploying system components to accommodate all service interruptions no matter if they are known or unknown has to be accepted in any cost. For instance, electric power backup and redundant system, network backup and redundant system, computation backup and redundant system, storage backup and redundant system, software backup and redundant system. Another concern is correctness. It is very difficult to define correctness in the network system. However, if data integrity and secure operation are enforced, correctness would be accomplished.

Z-axis: Network components

To be a trustworthy network, major components in this network must be able to protect security, privacy, and reliability of data that are storing, transmitting, and processing in the network. These major components include hardware, software, data, protocol, and people.

- Hardware: Hardware is the physical technology that stores, processes, and transmits data; executes software; interacts with applications and operating systems; and compromises with protocols. Physical access control with appropriate policies and tools could protect hardware asset. Well certified hardware with redundant systems could protect hardware reliability. Unfortunately, there are still some issues related to data residing in the hardware could not be solved easily. For instance, a hacker could break in hardware though software vulnerability even through the physical security is well enforced.
- Software: The software component of the network includes operating systems, applications and utilities. Since state of software changes from time to time, it is perhaps the most difficult network component to be secured [19]. Vulnerabilities such as bugs, backdoors, etc. are in the software since the nature of software project management: short development cycle with limit time, budget, and manpower. These vulnerabilities could be mitigated by adopting secure coding mechanisms and using formal expressions to verify codes and functions in the software development phase. Unfortunately, software security is all too often implemented as an afterthought rather than developed as an integral component from the beginning [19]. A rapid and real time approach for fixing software vulnerabilities is emerging and should be enforced as well. Reliability is another issue that affects software trustworthiness. Software may crash and leads to service disruption since its vulnerabilities or hardware resource errors.
- Data: the data component of the network indicates any form of information appearing in the network. Since it is the most valuable asset in the network, data processed, stored, and transmitted though the network must be protected. Data is virtually untouchable and can't be useful without interactions with other network components. Therefore, the protection of data security, privacy, and reliability has to consider the entire network as a whole.
- Protocol: Protocol indicates criteria and mechanisms used in the network communication. There are hundreds of network protocols issued. Some embed with security functions (e.g., HTTPS, SSH, etc.) and are highly adopted. Some have vulnerabilities and (e.g., FTP, TELNET, etc.) will cause security breaches. Proper choice of protocols will significantly strengthen network security. Since most network communications are not carried out in the same network domain, protocol selection and verification may not be done efficiently. In fact, hackers may take advantages of those insecure protocols to gain administration privileges of the victims.
- People: We may often overlook this topic. People have always been a threat to the network security [19]. Unless policy, education, and technology are properly employed to prevent people from accidentally and intentionally damaging the network system, they will remain the weakest link. We have seen several instances of how a disloyal employee could lead to huge destructions of employer's network systems. Administrative policies in job description, interview process, background check, employment contract, new hire orientation, on-the-job security training, performance evaluation, and job termination should be reviewed and updated carefully to prevent potential threats.

Conclusions

In this paper, we discuss the challenges in building a trustworthy network and depict a novel trustworthy network model that is both scalable and interoperable with existing and future network architectures. We introduce countermeasures, trustworthy characteristics, and major network components into the trustworthy network model and describe their functions as well. In the future, assessment of every cell in the trustworthy network model will be conducted and analyzed.

References

1. Mundie C, Vries Pd, Haynes P, Corwine M (2002) Trustworthy computing. Microsoft White Paper.
2. Computing Research Association (2003) Four Grand Challenges in TRUSTWORTHY COMPUTING. Second in a Series of Conferences on Grand Research Challenges in Computer Science and Engineering.
3. Lipner S, Howard M (2005) The trustworthy computing security development lifecycle. Microsoft Corporation.
4. TRUST (2006) 2005-2006 Annual Report.
5. Irvine CE, Levitt K (2007) Trusted hardware: can it be trustworthy. Proceedings of the 44th annual Design Automation Conference (DAC '07).
6. Eisenbarth T, Guneysu T, Parr C, Sadeghi A, Schellekens D, et al. (2007) Reconfigurable trusted computing in hardware. Proceedings of the 2007 ACM workshop on Scalable Trusted Computing (STC' 07).
7. Shieh A, Williams D, Sirer EG, Schneider FB (2005) Nexus: a new system for trustworthy computing. Proceedings of the twentieth ACM symposium on Operating Systems Principles (SOSP '05).
8. Platte J, Naroska E (2005) A combined hardware and software architecture for secure computing. Proceedings of the 2nd conference on Computing Frontiers (CF '05).
9. Garfinkel T, Pfaff B, Chow J, Rosenblum M, Boneh D (2003) Terra: a virtual machine-based platform for trusted computing. Proceedings of the nineteenth ACM symposium on Operating systems principles (SOSP '03).
10. Aaraj N, Raghunathan A, Jha NK (2008) Analysis and design of a hardware/software trusted platform module for embedded systems. Transactions on Embedded Computing Systems (TECS).
11. Reid JF, Caelli WJ (2005) DRM, trusted computing and operating system architecture. Proceedings of the 2005 Australasian workshop on Grid computing and e-research 44: 127-136.
12. Heiser G, Elphinstone K, Kuz I, Klein G, Petters S (2007) Towards trustworthy computing systems: taking microkernels to the next level. SIGOPS Operating Systems Review 41: 3-11.
13. Morris FL (1973) Advice on structuring compilers and proving them correct. Proceedings of the 1st annual ACM SIGACT-SIGPLAN symposium on Principles of programming languages.
14. Halderman JA, Schoen SD, Heninger N, Clarkson W, Paul W, et al. (2008) Lest we remember: cold boot attacks on encryption keys. Proceedings of 17th USENIX Security Symposium.
15. McCumber J (1991) Information systems security: a comprehensive model. Proceedings of 14th National Computer Security Conference.
16. Maconachy WV, Corey CD, Ragsdale D, Welch D (2001) A model for information assurance: an integrated approach. Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.
17. Fair Information Practice Principles, Federal Trade Commission.
18. Jansen W (2009) Directions in security metrics research. NISTIR 7564.
19. Whitman ME, Mattord HJ (2009) Principles of information security. (3rd edn.). Thomson Course Technology.