2 Research and Development of Traceable Network

KADOBAYASHI Youki

In today's Internet, necessary actions for root-cause analysis and recurrence prevention are ignored in most cases, resulting in the overall inefficiency of security countermeasures. In this paper, we argue that three mechanisms are necessary to address this problem. We then discuss the necessity of research efforts in the intersecting areas of networking technology and security technology. Our traceable network research group tackles these challenges by combining research disciplines of architecture, algorithm, system and networking research. This paper gives overview of our research efforts, along with connection to subsequent papers in this special issue.

Keywords
Traceable network, Network security, Accountability

1 Introduction

The usage of the Internet today is not limited to simple messaging tool or information exchange; its use encompasses across variety of purposes, such as electronic commerce and digital entertainment. While electronic commerce necessitates confidentiality and integrity, anonyms and pseudonyms are commonly used for entertainment purposes.

The Internet, being a flat network, has incurred unintended interactions among communications with different security requirements. In other words, information systems with higher security levels — those with authentic user information — coexist with information systems that only offer lower security levels through pseudonym or anonym. These systems with varying security levels interact with each other, when program bugs are triggered or when users make mistakes during operation, resulting in unwanted end result.

In today's Internet, sender's responsibility is avoided, and accountability for the end result of abuse and negligence remains unanswered, due to the mixed problems of user's lack of adequate knowledge, operational mistakes, communications in pseudonym or anonym, and everlasting program bugs[1]-[3]. As a result, the root cause of unwanted result remains to be addressed, which in turn leads to recurrence of the same problem. This recurrence is one of the factors that have made security countermeasures inefficient.

Three mechanisms are considered to be missing, in order to make the Internet more secure. First, a mechanism for soliciting responsibility is missing: in today's Internet, it is difficult to trace the origin of problematic communication. As a result, we cannot ask the originator his/her responsibility by associating a specific communication with its originator.

Second, a mechanism for identifying root cause is missing: in the past, it was difficult to comprehend what happened and where. It is essential to be accountable for "why, how the incident happened" in addition to "what" and

"where" in order to prevent further incidents of similar kind. Enormous amount of time has been required to identify root cause, however.

Third, an incentive mechanism[4] for proliferating security countermeasures is missing. Although many effective security countermeasures have been developed and packaged as products, their installation, from the viewpoint of whole Internet, is quite limited. Since many of these devices work alone, they do not interoperate with each other to achieve network effect. Although some of these devices are capable to interoperate among several devices, their interoperability is usually limited to product lines from the same manufacturer; we cannot expect interoperability among multiple vendors. Consequently, there is a lack of incentives to adopt security countermeasures.

2 Traceable network

We argue that the problems described in the previous section arise from mutual interactions of network technology characteristics and security technology characteristics. We must tackle the problems in different ways, if many of today's problems are occurring in the intersecting areas of network technology and security technology. The approach should be different from traditional one, where networking requirements are defined from network technology perspective, and security requirements are defined from security technology perspective.

In the traceable network research group, we recognize the importance of filling the gap between network technology and security technology. We have outlined security requirements from network technology perspective, and networking requirements from security technology perspective, as described in the following paragraphs.

First, we discuss security requirements. Traditionally, common security requirements were confidentiality, integrity and availability as defined in OECD guideline[5], and authenticity, accountability and reliability as defined in ISO/IEC TR 13335[6]. From network technology perspective, we believe that three new characteristics are required in addition:

(1) Interoperability: Most of existing systems and algorithms assume interactions with operators but nothing else. In order to improve efficiency of security countermeasures and reduce the burden of operators, these systems or algorithms should interwork with each other.
(2) Domain decomposition: Since the Internet comprises of multiple organizations (domains), demarcation of the problem into affected domains, and establishing contacts among them, is essential. In addition, it is especially important to preserve privacy if operators must deal with the problem across multiple organizations.
(3) Scalability: Since bandwidth of the Internet is doubling every year[7], designed systems or algorithms must possess adequate scalability that can follow the fast pace of bandwidth growth.

Next, we discuss networking requirements. From security technology perspective, we believe that the following two new characteristics are required:

(1) Accountability: it is essential to maintain accountability for both root cause and development process of problems observed in the network.
(2) Availability: higher availability is required especially in the application layer, such that single point of failure can be eliminated, flash crowd can be mitigated, and large-scale failure can be avoided.

In our research group, we are engaged in research and development activities that bring these characteristics to networking and security technology. Furthermore, we outlined the following engineering goals:

1. Expedite root-cause analysis process: we are trying to expedite the root-cause analysis process, which traditionally required few days, down to few hours or half an hour.
2. Coverage of the problem domain: we are trying to develop methods and systems for securing accountability and

availability in various networked applications.

3 Toward the deployment of traceable network

In order to materialize traceable network, narrow effort within single theory or single system is far from sufficient. Our research group has been conducting variety of research efforts that encompasses architecture, algorithm, system, and networking research. We believe that combining deliverables from these four areas can only satisfy the requirements that we outlined in the previous section.

The most important element for materializing traceable network is its architecture. Traceable network architecture comprises of various elements, such as the monitoring and abstraction of both computers and networks through variety of algorithms, parallel inference engine with input from monitoring components, evidence seizure and analysis systems that acts upon inference results. We are currently engaged in the materialization of message bus that interconnects these elements to form a working system. We are expecting the first system-level test within this fiscal year, for the validation of our proposed architecture.

Interconnection of systems, while feasible within single organization through the use of both header and payload, becomes a fundamental challenge when the interconnection encompasses across multiple organizations; involved parties must tackle the identical set of data without disclosing header or payload. We have been working on pragmatic use of the privacy-preserving cryptographic protocols: more specifically, design of high-performance privacy-preserving cryptographic protocols, its security validation, and high-performance implementation using multi-core processors. Paper **3-1** in this special issue elaborates more theoretical details.

Algorithm research: we are working on machine-learning algorithm that detects anomalies in the network or in the computer systems with higher precision and performance. In order to adopt machine learning for these purposes, we are working on surrounding issues along with algorithm itself: enrichment of datasets, and benchmarking environment for algorithms.

The parallel inference engine drives individual component based on the result of algorithmic analysis. We are working on a concurrent programming language, based on the intuition that concurrent programming language can be used to build parallel inference engine. Paper **6-1** in this special issue addresses this topic in more detail.

Systems research: we are engaged in research and development from two aspects: targeting new applications, and exploiting new system software technologies. On the application side, we have tackled the problem of securing accountability in peer-to-peer file sharing networks. Peer-to-peer file sharing networks have been used as a medium of information leakage; there is an immediate need to develop countermeasures. Paper **5-1** in this special issue describes one of such development efforts.

Work is under way to exploit new system software technologies such as virtual machine and distributed storage. Our research group modified virtual-machine monitor so that accountability can be secured by storing snapshots of problematic memory segments[8]. Distributed storage technology must possess enough scalability that can deliver required I/O performance for evidence seizure from the network. Our plan is to explore the scalability of various distributed storage technologies from grid computing, cluster file system, and overlay network[9]. Paper **6-2** in this special issue covers various distributed storage technologies.

Networking research: we are engaged in research and development of isolated emulation network for behaviour analysis of malicious program (malware), upon which cause-result database can be derived. Paper **4-1** describes malware analysis in the isolated emulation network.

4 Discussion: can we embrace safer Internet?

In the previous sections, we have described the overview of our research activities on traceable network, which is an attempt to contribute to safer Internet. We do not believe, however, that the safer and monolithic Internet is possible. As we discussed earlier, the Internet today multiplexes electronic commerce and digital entertainment into single infrastructure, and these two major applications have contradictory security requirements; we argue that this internal inconsistency is the root cause of problems.

Unless both program bugs and operational mistakes are entirely eliminated[10], we believe that there is an inevitable need to separate "trusted Internet" from "free Internet". In the trusted Internet, all users and computers are authenticated, and all applications incorporate security countermeasures. Such trusted Internet would be used as a business platform for electronic commerce and electronic government that requires confidentiality, integrity and accountability. On the other hand, the free Internet will be used as an innovation platform for researchers and developers, as applications can use arbitrary protocols and users can be identified in arbitrary way. Under the two-tiered structure of the Internet, security technology will be developed for the trusted Internet, and innovative applications will be developed under the free Internet.

While this seems to be a bold assumption, it must be noted that the Internet in reality has once witnessed the two-tiered structure: more specifically, networks inside firewalls such as enterprise networks, and the rest of the Internet. Since we did not have societal consensus toward the creation of two-tiered structure, we continued to embrace flat communication in e-mail, resulting in the collapse of partition through virus propagation via e-mail. Today, continued attempts are made to construct two-tiered Internet in many ways: extranet, and user federation of specific anti-spam technology are those examples.

5 Conclusion

In this paper, we described three mechanisms for building safer Internet, and then pointed out that crosscutting requirements definition is required to address the problems that are occurring in the intersecting areas of networking technology and security technology. In our traceable network research, five requirements are defined, e.g., interoperability in security technology, and accountability in networking technology; we have been tackling these challenges by combining variety of research disciplines. This paper outlined overview of our research efforts, along with connection to subsequent papers in this special issue. It should be noted that traceable network alone cannot deliver safer Internet; we hope that this special issue enables us to share problem diagnosis and research strategy, leading to more effective research activities in broader community.

References

1 Ross Anderson, "Why Cryptosystems Fail", in Proceedings of the1st ACM Conference on Computer and Communications, pp.215-227, Nov. 1993.

2 Justin E. Forrester and Barton P. Miller, "An Empirical Study of the Robustness of Windows NT Applications Using Random Testing", in Proceedings of the 4th USENIX Windows System Symposium, Aug. 2000.

3 Andy Chou, Junfeng Yang, Benjamin Chelf, Seth Hallem, and Dawson Engler, “An Empirical Study of Operating Systems Errors”, ACM SIGOPS Operating Systems Review, Vol.35, No.5, pp.73-88, Dec. 2001.
4 Ross Anderson, “Why Information Security is Hard-An Economic Perspective”, in Proceedings of 17th Annual Computer Security Applications Conference, pp.358-365 , Dec. 2001.
5 Organization for Economic Cooperation and Development, “OECD Guidelines for the Security of Information Systems”, 1992.
6 International Organization for Standardization, “Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management”, ISO/IEC 13335-1, 2004.
7 Kerry G. Coffman and Andrew M. Odlyzko, “Growth of the Internet”, in Optical Fiber Telecommunications Journal, Vol.ⅣB, pp.17-56, Jul. 2002.
8 Ruo Ando, Youki Kadobayashi, and Youichi Shinoda, “Incident-Driven Memory Snapshot for Full-Virtualized OS Using Interruptive Debugging Techniques”, in Proceedings of the 2nd International Conference on Information Security and Assurance, Apr. 2008.
9 Youki Kadobayashi, “Overlay Network”, Computer Software, JSSST, Vol.23, No.1, pp.15-23, Jan.2006.
10 Ka-Ping Yee, “User Interaction Design for Secure Systems”, in Proceedings of the 4th International Conference on Information and Communication Security, pp.278-290, Dec. 2002.

***KADOBAYASHI Youki**, Ph.D.*
Guest Expert Researcher, Traceable Secure Network Group, Information Security Research Center
Network Security