Defending Academic Networks: The Organizational Implications

Kenji RIKITAKE

Academic Center for Computing and Media Studies (ACCMS),
Kyoto University
rikitake@media.kyoto-u.ac.jp

Abstract

Information networks have become a critical infrastructure for the academic institutions. The security management and incident response of the networks in proper and timely manner is essential to minimize the risk and damage of the organizational assets and reputation. In this paper, the author discuss the general implications of the academic organizational culture on the security management, and the difference of requirements and methodologies for enforcing the security policies and procedures from those of business organizations.

Disclaimer

The views and positions expressed in this article are solely personal opinions and do not in any way reflect the views and positions of the author's employer Kyoto University or any members thereof.

1 Introduction

Security in the academic institutions is as critical and important as in the other organizations or societies. The requirements and methodologies for maintaining the security and enforcing the policies and procedures are largely different from those of the business organizations. For the business corporations, the management has the ultimate decision hierarchical privilege for each and every action happening in the corporation's activities, as in the military organizations. In the academic institutions, the decision making process and culture is not as straightforward and is traditionally based on autonomy and consensus, so different approaches should be taken.

Information networks have become an essential and critical infrastructure for the academic institutions. The mainstream distribution of research journals and reports have already changed to computer media from the traditional papers and books. The students and researchers actively exchange their ideas over the Web and other interactive means such as social networking services (SNSes). They continuously communicate with the laptop computers and mobile devices such as smartphones, both on the wired and wireless network infrastructures, either on and off the campus, thanks to the broad coverage of cell phone networks.

Boundaries of the academic institutions get more and more blurred and vague as more research projects become inter-organizational and interdisciplinary, and so does the usage pattern of computer systems over the networks. No organization will be able to conduct a research activity without allowing access to the external resources. Researchers and students consider network accessibility as critical part of the academic freedom, and take it for granted as a part of public utilities provided by the institution, such as the water and electrical power supplies.

On the other hand, the security precautions each academic institution have to take are getting more complex and diversed, as the users explore new ways of communication over the computer networks. As the age of cloud computing comes, more people have put their pieces of information over the cloud storage and other application services. Rumors and speculations about the students and professors spread very fast over the public SNSes which are *not* under control of the institution they belong to.

Every academic institution has a lot of confidential information as well as the business organizations does, such as the individual evaluation data for the personnel, grade information for the students, and the budget details of each research project and suborganizations. Classified information can leak through multiple paths not only over the campus information networks, but also the cell phone networks and personal memory devices such as USB flash drives and digital cameras. Protecting these data against unauthorized access and unwanted disclosure is critical to retain the business integrity of the academic institutions.

Maintaining the inter-organizational connectivity while keeping the confidential information secure has been one of the most difficult issues on the network management in the academic institutions, as well as maintaining the academic freedom and ethical integrity while minimizing the unresolved technical and legal incidents happening inside. The traditional laissez-faire policy framework towards the activities inside the academic societies no longer works; proper defense against known vulnerabilities, such as spam filtering and monitoring with intrusion detection systems (IDSes), are essential to mitigate the risks of the external and also *internal* threats. The operational considerations of the technical measures, however, are largely different from those of the business computer networks, due to the non-restrictive nature of academic and research activities.

Introduction of emerging technologies are also an important part of the computer network management. For example, Internet Protocol version 6 (IPv6) will soon become a mandatory choice for new large-scale applications which requires peer-to-peer (P2P) connectivities, as one prediction shows that Internet Protocol version 4 (IPv4) address allocation poll will be exhausted by July 21, 2011[*1]. Adding IPv6 support to the existing IPv4 networks will open up new vulnerabilities, and the security management will be a serious issue.

Another important emerging technology is DNSSEC [2], an authentication scheme of the Domain Name System (DNS), which required all DNS zone data to be signed by the administrators of the zone and the parent zone. The zone signing on the `.jp` domains will start from October 2010 [3], and the registration of the DNSSEC-signed `.jp` domains will start from 2011.

In this paper, the author first describes the trend and individual issues of changing security requirements of the university networks upon the working experience at the Kyoto University in Section 2. The author then explains the implications of organizational and cultural factors for facilitating the secure networks at the academic institutions in Section 3. Section 4 summarizes the paper and proposes a future direction for defending academic networks.

2 Changing security requirements and how Kyoto University cope with them

University campus networks were once believed to be a set of self-manageable autonomous networks administered by the laboratory staff controlling the networks. This assumption is no longer valid due to the massive changes of the general security requirements, including:

- increasing complexity of the protocols in the network (IPv4/IPv6), transport (TCP/UDP), and the application (HTTP/DNS) layers;
- vastly increasing number of devices connected to the networks;
- massive number of complexity of vulnerability exposed, which mandates continuously applying patches to the operating systems and application software on the connected devices;
- decreasing number of the skilled staff members who can effectively manage, control, and administer the networks; and
- multiple choices available for the means of connecting to the Internet, not only restricted to the campus networks, but also through the mobile cell phone networks.

Regarding the circumstances, Kyoto University has migrated into a mixed policy set of networks, which allows running publicly-accessible servers and protected client and internal servers under a set of private networks.

Kyoto University Integrated Information Network System (KUINS) was first established in 1988 as a campus Local Area Networks (LANs)

[*1] Predicted by Huston [1], as of 0758UTC, August 21, 2010.

and inter-campus link between the University's Yoshida and Uji campuses [4]. Since 2002, KUINS is operated by the Institute for Information Management and Communication (IIMC), as a part of the campus-wide information system. The transition from a set of global-IPv4-only networks to a global-and-private-IPv4 set of networks was done on 2002, when KUINS-III [5, 6] started the production-level operation.

As of August 2010, KUINS has two major sets of networks as follows [7]:

- KUINS-II, a set of global IPv4 address networks which are globally reachable, managed per the assigned IP address number or blocks; and
- KUINS-III, a set of *private* IPv4 address networks which are *not directly* reachable to the global Internet, managed per the assigned Virtual LANs (VLANs) and the internal IPv4 address blocks.

And the network management policies of the two KUINS networks are as follows:

- for each KUINS-II IPv4 address, all Ethernet MAC addresses must be registered and only the registered devices can communicate with the outside;
- for each KUINS-III VLAN, the KUINS operation staff assigns the subnets from the private network address space, and the DHCP and fixed address blocks;
- for all the KUINS LAN information wall outlets, the inter-VLAN connectivities and the identities of connected devices are fully controlled and monitored by the KUINS operation staff; and
- for all the KUINS Point-to-Point Tunneling Protocol (PPTP) and Secure Shell (SSH) forwarding services, including those provided on the campus wireless LAN, the user authentication based on the Integrated Authentication System (IAS) is mandatory.

Figure 1 shows the configuration of KUINS-II and KUINS-III network connectivity and the security subsystems as of August 2010. KUINS-III has its own proxy and network address translation (NAT) servers at KUINS-II for the external access, such as e-mail, DNS, and Web, run by IIMC. IIMC also provides the general-purpose hosting services, including web hosting systems and e-mail forwarding systems.

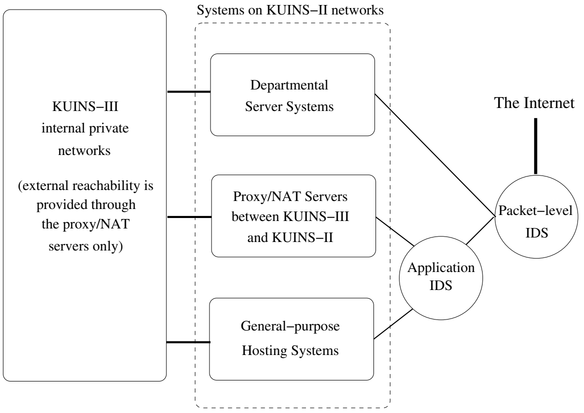
Systems on KUINS−II networks
KUINS−III internal private networks
(external reachability is provided through the proxy/NAT servers only)
Departmental Server Systems
Proxy/NAT Servers between KUINS−III and KUINS−II
General−purpose Hosting Systems
The Internet
Packet−level IDS
Application IDS

Fig. 1 KUINS-II and KUINS-III network connectivity and security subsystems.

On the other hand, many University departments still run their own server systems on KUINS-II, with the different specific requirements for the *educational and research perspectives*, from the systems provided by the IIMC.

From the security management points of view, the role diversity of the server systems on KUINS-II means that imposing the unified access control policies over all the KUINS networks with the strict access control via the firewalls is practically impossible [6, Section 1].

The current security subsystems of KUINS networks include the router filtering, packet-level intrusion detection system (IDS), and the application IDS for specifically monitoring the proxy/NAT servers and the general-purpose hosting systems.

Incidents detected by those IDSes are reviewed and responded by the Information Security Management Office (ISMO) [*2] of IIMC, under the delegation of Kyoto University Information Security Committee and the Rules for Using the Kyoto University Campus-wide Information System [8].

[*2] Disclaimer: the author is the Chairman of ISMO Steering Committee, as of August 2010.

3 Organizational implications for facilitating the secure networks

3.1 Change of the demands to the network administrators

The user's demands to the university information networks, including those of the administrative, technical and educational staff, and the students and visiting researchers, have been rapidly changing, as the society does.

Before the computer networks became popular, university computing systems were centralized (e.g., time-sharing services by a centralized single computer). The systems then changed to the cluster of autonomous servers and clients in the laboratories. The cloud computing trend has come and the consolidation of the physical or virtual servers into a computing cluster gains more popularity to minimize the budget expense while allowing the extensibility. The cost of managing individual server hardware is rapidly rising, and the lab staff consider the cost a huge overhead which hampers their primary research activities, as the budget for each department is tightly controlled.

As more and more services are emerging *outside* the campus networks, the campus computing facilities will not be able to cover all the emerging new services. Outsourcing computing facilities, both internally and externally with a service provider, should be seriously considered for the sustainable services.

As Internet access gets popular among the university members, they are familiar with the popular Web services such as Google Apps and SNSes, and consequently they demand the same accessibility from inside the network. This trend requests the campus network administrators to completely change the security system assumptions; perimeter-based network defense policies will become less effective.

The network operators have to think about the answer to this question: *how academic institutions should handle the complex and increasing demands from the network users?* The author thinks the traditional network security industry and communities do *not* provide the definitive answer and solutions for this question, for the following reasons:

- the network security industry does not put the operational ease and operator's convenience on the top priority, and they rather want to *sell their products* than the services;
- security-related expertise and case studies are still not actively and openly discussed among the network security operators;
- the network security operators do not necessarily fit well into the current network routing and connectivity operator's communities due to the confidential and sensitive natures of the security technologies; and
- network security routine operation itself gives very little chances to learn new things for the staff.

To meet the demands from the users, academic institutions should assign more dedicated research staff for the operation for the following reasons:

- traditional part-time assignment of the administration role to the teaching/educational staff is no longer sufficient to respond to the security incidents;
- research staff with the educational skills can give the opportunities for the technical/administrative staff to learn emerging technologies to develop the fundamental skills; and
- surveying the emerging vulnerabilities and new solutions are critical to prevent the security risks, and only those who have flexible ways of thinking can cope with and solve the unforeseen problems such as exploitation against unknown vulnerabilities.

3.2 Security policies and the freedom of education and research

Academic institutions are a part of the greater society, and must abide the information security rules and laws. Distributing the malwares and the denial-of-service (DoS) attacks are now considered criminal activities rather than benign experiments. On the other hand, universities should harvest the innovation and protect the freedom of education and research; simply saying a no-no to the unexpected and unauthorized usage without sufficient explanations based on the written rules is almost always the worst way to solve the security problems.

Academic institutions nowadays face the following three major security risks:

- damaging organizational reputation, primarily by not persecuting the illegal or unethical activities, such as copyright infringement or public defamation;
- becoming a security threat against other organizations, primarily by willingly or even accidentally distributing malwares, unsolicited messages, and harmful pieces of information which may render other network systems unusable; and
- violating the acceptable use policies of academic resources, such as abusive spending of the research budgets.

Kyoto University handles those risks by defining the rules for the following issues:

- responsible use of the information assets, including the resolution procedure of disputes by the possible unethical behaviors [9];
- protection of the campus-wide information system from the malwares [10], including the reporting procedures of network security incidents [8]; and
- campus-wide and departmental security management structure, and the education and training requirements to all the members of the University [11].

The author should note that those policies and procedures are *not* enforcing the deny-first-and-allow policies, and that they are rather for resolving the issues to maximize the allowance for the freedom of education and research, while preventing taking the unnecessary risks.

And there is a fundamental question: *does monitoring the organizational traffic constitutes a censorship case?* The author thinks it does not, since the monitoring is inevitable for a faster response to the possible security incidents. Tracking down the root cause of a security incident is a mandatory procedure to respond to complaints from outside the organization.

For example, PubMed [*3], a popular biomedical literature database, rejected access from Kyoto University for four days from May 29, 2010 [12]. The author thinks this case would have not been resolved in such a short term if the root cause were not immediately tracked down.

3.3 Is global endpoint reachability a part of the academic freedom?

For many years, university networks were considered the most transparent ones to the global Internet, and the author finds still many researchers consider the privilege is taken for granted. This is no longer the case anymore, as the global IPv4 address space will be exhausted in a few years. Global endpoint reachability is something should be paid for; in another words, freedom has its own cost.

For example, American Registry for Internet Numbers (ARIN) proclaims that IPv4 address spaces are no longer free even for those who are under coverage of the Legacy Registry Service Agreement before ARIN's inception on December 1997 [13, 14]. Japan Network Information Center (JPNIC) plans for a similar fee schedule from 2011 [15].

In Kyoto University, KUINS has two different fee schedules by the global reachability [16]:

- for KUINS-II, JPY1500/month for each global IPv4 address; and
- for KUINS-III, JPY300/month for each information wall outlet.

The author thinks these schedules effectively reflects the cost of the global IPv4 addresses.

4 Conclusions

In this paper, the author discussed the issues of enforcing the security on the academic networks and the organizational implications, with the work experience of Kyoto University. The major issues were: 1) assignment of the dedicated research staff, 2) operation under explicit and flexible policies and procedures, and 3) proper internal cost transfer for the security enforcement activities.

The network security operation itself, however, does not have any academic value if no research effort is made to maximize the efficiency for handling massive amount of the security events and the related data. The author expects the emerging concurrent and parallel programming technologies will be a viable future direction to go.

[*3] http://www.ncbi.nlm.nih.gov/pubmed

Acknowledgments

The author would like to thank Prof. Yasuo Okabe and Prof. Tetsutaro Uehara of ACCMS, Kyoto University, and Prof. Hiroki Takakura of Information Technology Center, Nagoya Univesity, for their insights and helpful discussions. The author thanks Prof. Takashi Matsuyama, Chief of IIMC, Kyoto University, for his leadership and support of the security management activities. The author would also like to acknowledge that the stable operation of KUINS is made possible by the KUINS operation team and the ISMO members.

Notes on References

In the References section, the article titles and author names originally written in Japanese without the official English translations are translated into English by the author.

References

[1] G. Huston, "IPv4 Address Report." http://www.potaroo.net/tools/ipv4/.

[2] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," March 2005. RFC4033.

[3] Japan Registry Services (JPRS), "DNSSEC Introduction Schedule to the JP domains." http://jprs.jp/info/notice/20090709-dnssec.html, last updated July 21, 2010 (in Japanese).

[4] Institute of Information Management and Communication (IIMC), Kyoto University, "Organizational History of IIMC (1960-2005)." http://www.iimc.kyoto-u.ac.jp/ja/organization/pdf/iimc_history.pdf (in Japanese).

[5] KUINS Organization, Kyoto University, "Summary of KUINS-III Project: A Safe Gigabit Network," KUINS News, no.34, pp.427–429, March 2001. http://www.kuins.kyoto-u.ac.jp/news/34/kuins3.html (in Japanese).

[6] H. Takakura, Y. Ebara, S. Miyazaki, A. Sawada, M. Nakamura, and Y. Okabe, "Structure and Security Strategy of a Secure Gigabit Network system, KUINS-III," IEICE Trans. Commun. (Japanese Edition), vol.J86-B, no.8, pp.1494–1501, Aug. 2003.

[7] KUINS Operation Committee, Kyoto University, "KUINS Operation Committee Information Web Site." http://www.kuins.kyoto-u.ac.jp/ja/index.php (in Japanese).

[8] Kyoto University, "Rules for Using the Kyoto University Campus-wide Information System." Effective January 12, 2010, http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/documents/pdf_p/rules-for-using-the-kyoto-university-campus-wide-information-system.pdf (English version).

[9] Kyoto University, "Kyoto University Rules For Information Asset Use." Effective October 1, 2007, http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/documents/pdf_p/rules-for-infomation-asset-use.pdf (English version).

[10] Kyoto University, "Kyoto University Guideline for Measures against Invasion by Malicious Programs to Campus-wide Information System." Effective January 12, 2010, http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/documents/pdf_p/Guideline-for-Measures-against-Invasion-by-Malicious-Programs.pdf (English version).

[11] Kyoto University, "Kyoto University Information Security Program Standards." Effective April 1, 2009, http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/documents/pdf_p/information-security-program-standards.pdf (English version).

[12] Information Security Management Office (ISMO), Kyoto University, "On Proper Use of Electronic Journals and The Public Contents." June 4, 2010, http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/whatsnew/news/detail/03798.html (in Japanese).

[13] American Registry for Internet Numbers (ARIN), "Fee Schedule." https://www.arin.net/fees/fee_schedule.html.

[14] American Registry for Internet Numbers (ARIN), "Legacy Registration Service Agreement." https://www.arin.net/resources/legacy/index.html.

[15] Japan Network Information Center (JPNIC), "On Revising The Fee Schedule for IP Addresses and AS Numbers ." June 2, 2010, http://www.nic.ad.jp/ja/materials/ip/20100602/fee-pi-as.pdf.

[16] Kyoto University, "The Usage Fee Schedule for The Connectivity of KUINS-II and KUINS-III." http://www.iimc.kyoto-u.ac.jp/ja/organization/pdf/KUINS_service_riyoufutankin.pdf (in Japanese).