JISSec 1(1) 2005

The Information Institute

Journal of Information System Security

www.jissec.org

Editorial

Meeting the Information System Security Challenge

The inaugural issue of the Journal of Information System Security (JISSec) is now with you. The idea for a journal dealing with Information System (IS) Security issues and concerns, covering both theory and practice, was conceived some five years ago. After years of planning and preparation, we are at last able to offer the first issue.

There is no doubt that information is increasingly being recognized as an essential and precious personal and societal asset. Unprecedented technological progress has been made in creating, transmitting, and storing data; however, as we all know, securing the information and its infrastructure remains a challenge. More organizations must address this challenge with new technologies because there is a demand to provide facilities for fast and effective access, secure flow, and control of data. More often than not, what constitutes security evolves alongside what experts regard as threats. Much as with nature, it is the predators that force the prey to change or adapt. Occasionally however, there is wholesale paradigmatic change, such as when the Internet made electronic commerce a reality yet, at the same time, enlarged the reach of predators.

Interpretations of IS Security are needed urgently to address the legal and regulatory requirements for specific types of information: European Union's Information Directives which emphatically affirm EU residents' rights to private data, the U.S. Health Insurance Portability and Accountability Act of 1996 regulations for medical data, or the Digital Millenium Copyright Act constraints on copyrighted material, to say nothing of the Sarbanes-Oxley (often abbreviated as "SoX") Act of 2003 even though the relationship of SoX to information security practices may not be quite as straightforward as at first thought. All of this, in turn, asks questions about the public expectations of privacy and about the appropriate level of awareness. So, it seems we are in the midst of another monumental change today, though of lesser impact compared with the Internet's dramatic fusion of consumers and providers

some years ago. This new departure focuses on information assets, their usage in all forms, and on mobility. Certainly, these elements of change are not new, but the degree to which they have grown in significance is remarkable. The change with the most practical impact is that of the growth of regulation concerning digital assets. Most experts would agree that, in regulating digital assets, the aim echoes the general goals of security technology implementation; namely, authenticity, integrity, confidentiality, and non-repudiation. So, it is no surprise that today regulatory compliance is fast becoming the basis for new investments in information security.

The Computing Research Association's (CRA) Conference "*Grand Research Challenges in Information Security & Assurance*", in November 2003, identified four challenges worthy of sustained commitments in resources and effort:

1. Eliminate epidemic-style attacks (viruses, worms, email spam) within 10 years;
2. Develop tools and principles that allow construction of large-scale systems for important societal applications — such as medical records systems — that are highly trustworthy despite being attractive targets;
3. Develop quantitative information-systems risk management to be at least as good as quantitative financial risk management within the next decade;
4. Give end-users security controls they can understand and privacy they can control for the dynamic, pervasive computing environments of the future.

Certainly, it would be attractive to deal with an Internet that is largely free of viruses, worms and spam. But it's interesting to note that CRA conference attendees agreed that what's needed is a fundamentally new approach to solving the problem, perhaps by moving more of the responsibility to Internet service providers. The second challenge refers to the tools to support large-scale applications, such as voting machines and medical records. What is surprising is that the world has come this far without creating trustworthy tools and widely acceptable standards. People have been trying to tackle the third challenge for some time. Most practitioners would agree that there are many problems with "best practices" in quantifying risk for information management, because these practices simply state that you are as secure as the others following similar practices. Likewise, best practices have no metrics. We just don't yet have good tools or benchmarks to measure the different dimensions of quality of the various security designs or implementations. The last challenge identified is to make security easier to use. Specifically, to give end users control over their own computers, i.e. control in terms of their information system security and privacy. Why not? Aren't they also major stakeholders? If we approach this right, we could fundamentally change the way we think about and work with information systems and pave the way for the future.

Let us take a look at the tactical problems we face today. Since the Internet worm of 1988 and the massive global proliferation of the Internet in the 1990s

and early 2000s, communities worldwide have seen an explosion of security attacks. New types of security-related incidents emerge on a frequent basis and massive effort is required across the globe to mitigate the violations of information security policies and recommended security practices. Most governments and enterprises, locally and nationally, recognize the need to protect their infrastructures, citizens and customers. Since technological, socio-economic and legal challenges cross national boundaries, many observers are aware that it is not enough to address such incidents just at the local level.

The global threats of the near future are not simply from hackers but also could come from international terrorists and other organized criminals. Coordinated attacks exploiting high speed networks are likely to target critical infrastructures, the foundations of today's developed societies. For the years to come, if we are to address Internet security and privacy attacks, increasingly efficient cooperation and communication between incident response teams will have to remain a high priority for worldwide organizations such as United Nations who promote cooperation among nations. FIRST is currently carrying some of that responsibility, yet communications and standards need further progress. Another example is eEurope 2005 effort. IT Security is one of its six policy priorities. Supporting eEurope 2005 security policies, the European Network and Information Security Agency (ENISA) was set up to enhance the capability of the EU community, the Member States and consequently businesses, to prevent, address and respond to computer security problems. It will be interesting to see how ENISA will work with FIRST and CERTs across the world.

What about the cutting-edge devices and appliances that are emerging on a massive scale? For instance, in the not-too-distant future, distributed intelligent, wearable devices containing advanced sensing and communication capabilities hold out the promise of many societal benefits. Nonetheless, they will give rise to opportunities for miscreants to reenter, "camp out" or inject malware in ways previously unimaginable. Their ubiquity, mobility and capability to diffuse information pose new challenges in the areas of security, privacy and ethics. In addition, there are legal and economic considerations that must be addressed, as exemplified by the potential tradeoffs between security system design and the personal expectations of privacy. That is why many experts believe security should be designed and evaluated in the upcoming information systems from the economic standpoint just as quality and reliability are.

Many countries have outlined several practical challenges to their national security. These have broad applicability. More research effort should be diverted to impact directly these challenges. The incorporation of broader aspects of policy, law, and social impact early into the design of systems will make the effort worth the investment. As in the case of the U.S. Department of Homeland Security, high level information systems security efforts are under way in several countries such as Germany, Israel and India to develop a strategic framework for the design, implementation, and deployment of

science and technology systems. Some of the initial focus security applications include the development of advanced detection systems, authentication of objects and people, sensing of objects and vehicles crossing the borders by air, land, and water; and surveillance using video cameras networked with complementary sensors.

Generally, public health and well-being is one of the most important areas of focus for government agencies and other organizations delivering public services, where security plays a huge role. Emergency preparedness and response is a critical aspect of security. Worldwide, we need innovative regional emergency response partnerships to facilitate speedier incident storage, analysis, management and response.

In conclusion, defining and analyzing the challenges in information security seems a useful exercise for anybody interested in improving security. But the real value of this work must be seen in providing direction that others can discuss, learn from, and perhaps follow. It's easy to get bogged down in the minutiae of security, with all its virus fighting tools, complex encryption algorithms, public-key infrastructures, disk sanitization and other nuts-and-bolts issues. However, in the final analysis, we need to work strategically, innovatively and cooperatively if we are to confront the increasing number of challenges posed for information systems security today.

Nature and Scope

Given this background, it is important to consider how the issues and challenges related to IS security will define the nature and scope of JISSec. Clearly IS Security is a broad and an eclectic subject area. Irrational adherence to particular viewpoints and beliefs is perhaps going to do more harm than good to the subject area. Indeed a focus on the tools and techniques without understanding the methodological issues is detrimental, likewise a lack of appreciation of ontological and epistemological questions.

Our mission, enabled by JISSec, is to establish a broad appreciation for IS security concerns. A narrow focus on good security policies, superior perimeter defenses, or on implementing excellent encryption will fall short of ensuring security. While it is impossible to have complete security, it is indeed possible to strive for adequate security that goes beyond narrow concerns and incorporates a well thought out protection agenda. We hope that subsequent volumes and issues will regale us excellent discussions on a wide range of technical, formal and behavioral controls that might be established within and beyond organizations and on the policy issues that surround them.

Generating a discussion on what IS security is and how it can be established in organizations is not a trivial task. While there is limited agreement on definitions for IS security, there is a prevailing consensus, both in academia and practice about the seriousness of the challenges we are facing. Overcoming such challenges and developing understanding of the emergent views of IS security crystallizes what we as editors are striving for.

Some of the issues that perhaps need to be addressed are:

Paradigmatic grounding. Over the past decade the discipline of IS has witnessed many challenges related to paradigmatic grounding. Declaring upfront the philosophical orientation has been welcomed by editors and reviewers. This has led to different methodological 'camps' and unseemly in-fighting over philosophical and methodological orientations. Such developments are counterproductive in furthering knowledge. At JISSec we aspire to build an environment of mutual respect and appreciation for divergent philosophical viewpoints.

Theory. Theory plays an important role in research. Not only it allows researchers to understand better the phenomenon, it also facilitates generalization. In the field of IS Security, it is particularly important to engage in theoretically well-grounded research. As Editors of JISSec, we shall encourage publication of research that is indeed theoretically well grounded.

Empirical evidence. Empirical evidence is important if propositions are to be tested or arguments conducted. JISSec welcomes empirical papers. Both quantitative and qualitative papers are welcome, since both inform theory and practice. From time to time, JISSec will also publish case studies which illustrate particular security scenarios. Such case studies form an excellent basis for contextualizing and grounding theoretical arguments.

The First Issue

The first issue of JISSec has an interesting mix of papers. The first paper, "Systemic Risk redefining Digital Security" is an opinion piece by Ian Angell of London School of Economics and Political Science. Angell claims that to succeed, a company must be built around effective digital security – albeit a redefined form of 'security' that depends on 'thinking managers' who are finely tuned to the systemic nature of Information and Communication Technology. The paper argues that digital security is not just about computer crime and the like – it is a consideration of anything digital that compromises the integrity and well-being of the company.

The second paper, "Information Warfare: A Comparative Framework for Business Information Security" is authored by Richard Baskerville of Georgia State University. Baskerville argues that there are fundamental assumptions and premises that distinguish prevalent thinking in business information systems security and information warfare. Thus, an analysis of these two paradigms may lead to improved management of information security activities. In a final synthesis, he suggests that an increasing belief that the essential causal structure of security is based on process will lead to a greater perception that security events are more important than static threats. Furthermore and security failures are a consequence of failure in the processes, rather than breakdown of security safeguards. This shift may lead to increasing use of possibility theory, agility strategies, and exploitative learning strategies.

The third paper, "The Ephemerizer: Making Data Disappear" is a contribution from Radia Perlman of Sun Microsystems. The paper presents a means to keep data for a finite time, making it unrecoverable after that. The paper presents a design that ensures that even if a client's machine gets compromised, and everything in stable storage (including long term user keys) is stolen, any data that has expired before the compromise remains unrecoverable. The paper starts with a description of an existing commercial scheme, and presents improvements to that scheme to eliminate the necessity for per-message state.

Acknowledgements

We would like to acknowledge the support rendered by our respective institutions in making time, space and resources available for establishing JISSec. Virginia Commonwealth University (USA), London School of Economics and Political Science (UK) and Sun Microsystems (USA) all had a part to play. Support from many colleagues from around the world is also warmly acknowledged. In August 2004, for instance, the security specialist group (SIGSEC) of the Association of Information Systems gave its 'blessings' to JISSec and agreed to adopt JISSec as their official journal. Many thanks to SIGSEC Chairs Professors Al Bento (University of Baltimore, USA) and Mark Weiser (Oklahoma State University, USA) for their support.

A journal is as good as the Associate Editors (AEs) and the reviewers. The quality of JISSec editorial team is first rate. Our acknowledgements are due to all the AEs and reviewers who have worked so diligently in writing comprehensive reports and providing useful comments to the authors. We are optimistic that the editorial team will continue with the good work and will help to establish JISSec as the high-quality, preferred outlet for IS Security research.

Much of the mundane task of interacting with the AEs and the authors was undertaken by Ms Sumana Sharma, a doctoral student at Virginia Commonwealth Univeristy. She has done a remarkable job as the JISSec Editorial Assistant. We appreciate her involvement and duly thank her for providing administrative support.

Editors
Gurpreet Dhillon
Virginia Commonwealth University (USA)
James Backhouse
London School of Economics and Political Science (UK)

Industry Editor
Vijay Masurkar
Sun Microsystems (USA)