

Analyzing inconsistency in evolving security requirements

Security requirements of computer-based systems describe the constraints on systems functionality to protect assets from harm. As systems evolve due to changes in their requirements and the environment in which they operate, security requirements need to be re-validated, or changed, to ensure an appropriate level of protection of assets. Research problems around these issues are many, from eliciting and analysing security requirements, to analysing the nature and impact of change on the satisfaction of such requirements.

Relevant topics of interest include analysing natural language requirements using NLP techniques, semi-formal reasoning such as structured argumentation to analyse security problems, and automated software engineering techniques for security requirements engineering. The supervisory team has a longstanding interest in inconsistency management, which may provide an additional dimension to the research.

Recently, the creation of several technological advances like the Internet has rightly created issues about privacy protection, as well as the protection of personal information. The use of electronic networks has made the ability to obtain other's personal data a greater threat, and this creates a fear that the easy obtain ability of personal information can mean that it is more likely to be abused in situations like identity theft.

One of the huge creations that is fueling this ever-increasing concern is the use of the Internet. While the Internet has allowed for people around the world to become more interconnected and also allows for a rapid exchange and gathering of information, making it much easier for people separated by distance to communicate, the Internet does not come without its own risks. One of these risks is the fact that personal data can be widely circulated, and therefore more easily abused (Kaeo, 2003).

The Internet is certainly useful for many individuals, but it also contains much about individuals as well. Part of the problem is the fact that many websites require personal information to be entered for things such as orders and accounts. So, most websites are able to get a good deal of information about their customers. Another problem is the fact that many websites use items of data collection that users may not even be aware of—for instance, cookies (Mann, 2002).

A further issue to examine here is the fact that the usage of the Internet is only increasing, not decreasing, so the amount of personal information being gathered and circulated is also increasing. The Internet is becoming more and more important as a tool for commerce. In the United States, for instance, the Department of Commerce recently announced that online sales tripled from approximately \$3 billion in 1997 to approximately \$9 billion in 1998. In addition, Internet commerce has also been growing quite rapidly in a number of other countries. Trends of Internet usage demonstrate that Internet usage is only likely to continue to increase, not decrease, in the coming years. Therefore, it is important to address the issue of personal privacy and the Internet (Kabay, 2002).

In order for a company to develop a security infrastructure, it must be aware of what is protecting against. Below is a list of security problems that computer-based systems will need to consider when attempting to resolve inconsistent security problems:

1. A denial of service (DOS) is one aimed at depriving an organization of a resource it expects to be able to use.
2. *Buffer overflows* are the most common type of DOS attacks. Here, an attacker sends more data than the application's buffer can hold. When the amount of data exceeds the buffer

size, the extra data overflows onto the stack, often causing the application or entire system to crash. In some cases, the data can be carefully crafted to include machine code that will execute when it overflows onto the stack.

3. A *SYN attack*, also known as a *SYN flood*, takes advantage of the TCP implementation. When a connection request is sent to a system, the packet contains a SYN field that represents an initial communication request. The receiving system responds with a SYN/ACK, holding the SYN packet in memory until it receives final confirmation, or ACK (Acknowledgment), from the initiating system. Communication between the two systems can then begin.
4. The *teardrop attack* exploits the IP implementation. When a packet is too large for a router to handle, it is broken into smaller packets called *fragments*. In order for the fragments to be reassembled when they arrive at the packet's destination, the fragment packets contain an offset value to the first packet. An attacker can put a confusing offset value in the second or later fragment packet. This incorrect value causes the receiving system to crash when it tries to reassemble the packet.
5. *Intrusion attacks*, the most common type, allow attackers to gain access to your systems and use resources. Some attackers want to gain access for fun and bragging rights, whereas others want to use systems to launch more attacks against unsuspecting targets.
6. *Information theft attacks* allow an attacker to steal data from a target. These attacks do not always require that the attacker gain access to the target's systems. Most information theft attacks rely on misconfigured systems that give out more information than they should (Fisch, and White, 1999).

Thus, when responding to the threat of inconsistency in evolving security requirements, one can see that several threats are in existence (and the number of threats continues to grow on an almost daily basis as new viruses are introduced). Therefore, businesses must stay ahead of the game as far as the issue of threats is concerned. One option businesses can consider policies is to follow the internationally recognized International Standards Organization (ISO) 17799, a set of recommendations organized into ten major sections covering all facets of information systems policies and procedures. Many organizations and consulting firms use ISO 17799 as the baseline for policy best practices. As defined at <http://www.securiryauditor.net>, the ten domains of ISO 17799 and what they help with are:

“1. Business continuity planning

- Counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters

2. System access control

- Control access to information
- Prevent unauthorized access to information systems
- Ensure the protection of networked services
- Prevent unauthorized computer access
- Detect unauthorized activities
- Ensure information security when traveling and telecommuting

3. System development and maintenance

- Ensure security is built into operational systems
- Prevent loss, modification, or misuse of user data in application systems
- Protect the confidentiality, authenticity, and integrity of information
- Ensure that information technology (IT) projects and support activities are conducted in a secure manner
- Maintain the security of application system software and data

4. Physical and environmental security

- Prevent unauthorized access and damage to and interference with business premises and information
- Prevent loss or compromise of assets and interruption to business activities
- Prevent compromise or theft of information and information-processing facilities

5. Compliance

- Avoid breaches of any criminal or civil law; any statutory, regulatory, or contractual obligations; and any security requirements
- Ensure compliance of systems with organizational security policies and standards
- Maximize the effectiveness of-and minimize interference to and from-the system-audit process

6. Personnel security

- Reduce risks of human error, theft, fraud, or misuse of facilities
- Ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work
- Minimize the damage from security incidents and malfunctions and learn from such incidents

7. Security organization

- Manage information security within the organization

Maintain the security of organizational information-processing facilities and information

- Maintain the security of information when the responsibility for information processing has been outsourced to another organization

8. Computer and network management

- Ensure the correct and secure operation of information-processing facilities
- Minimize the risk of systems failures
- Protect the integrity of software and information
- Maintain the integrity and availability of information processing and communication
- Ensure the safeguarding of information in networks and the protection of the supporting infrastructure
- Prevent damage to assets and interruptions to business activities
- Prevent loss, modification, or misuse of information exchanged between organizations

9. Asset classification and control

- Maintain appropriate protection of corporate assets and ensure that information assets receive an appropriate level of protection

10. Security policy

- Provide management direction and support for information security.” (qtd in Feghhi, and Williams, 1998, p. 71)

The aim of this research, therefore, is to demonstrate how companies can use the ever-evolving need of security requirements to protect their information from being made too public.

Inconsistencies in the various forms of security approaches will be analyzed in order to demonstrate which approaches are currently the best to use in the ever-changing world of Internet commerce. Topics to be discussed, most of them briefly mentioned above, will include: automated software engineering techniques, security into software design and implementation, threat models to highlight the need for security requirements, System Development Life Cycles, Software Assurance Maturity Models, the necessity to achieve Regulatory Compliance, and Industry regulations and standards. By taking this into perspective, the researcher hopes to demonstrate what the best strategy is for those businesses currently pursuing e-commerce in the modern world.

References

Feghhi, J. and Williams, P. (1998), Digital Certificates: Applied Internet Security, Addison-Wesley.

Fisch, E. and White, G. (1999) Secure Computers and Networks: Analysis, Design, and Implementation, CRC Press.

Kabay, M., (2002), Computer Security Handbook. John Wiley & Sons

Kaeo, M. (2003), Designing Network Security, Cisco Press

Mann, S. et al. (2002), Linux System Security: The Administrator's Guide to Open Source Security Tools, Prentice Hall.

<http://www.softwaremag.com/L.cfm?doc=1067-7/2007>