



HELSINKI UNIVERSITY OF TECHNOLOGY



The case for automated Vulnerability Management

A Software Business Lab Whitepaper, © 2010

Christian Frühwirth
Software Business Researcher
BIT Research Center, Helsinki University of
Technology, TKK
Espoo, Finland

Ron Perris
Chief Technology Officer
Outpost24 AB
Karlskrona, Sweden
www.outpost24.com

Table of contents

1 Introduction	3
1.1 Outline	3
1.2 What is security and vulnerability management?	3
1.3 What is driving vulnerability management improvement efforts?	4
2 Challenges	5
2.1 Opportunities	6
3 Changing the game of vulnerability management	7
3.1 Change driver: Growing dynamics	8
3.2 Change driver: COTS software	8
3.3 Change driver: Common standards for vulnerabilities	8
3.4 Change driver: Compliance	9
4 Compliance with an automated vulnerability management lifecycle	10
4.1 A modern vulnerability management lifecycle	10
4.2 Limits of automation in vulnerability management	13
5 Conclusion	13
6 References and further reading	16

1 Introduction

This paper aims at industry practitioners and the challenges they face in managing IT security vulnerabilities in their organizations. In the course of this work we will pin down the most important challenges and introduce possible solutions. We outline the benefits and opportunities that come with these solutions, as well as their limitations.

Our goal is to show how vulnerability management can be a valuable organizational tool for companies to:

- 1) Reach continuous compliance with legal regulations,
- 2) become more cost effective in their IT operations and
- 3) build a more robust business environment that allows them to compete with ever more professional attackers.

1.1 Outline

In the remainder of this section, we will introduce the basic concept of vulnerability management and its driving forces.

Section 2 will outline the challenges that vulnerability management faces today, along with the opportunities that arise from addressing them.

Section 3 presents recent developments and new requirements in security management, that changed the way vulnerabilities are managed today.

Section 4 lays out a modern vulnerability management lifecycle, that is built to address the challenges raised in section 2 and accounts for the requirements presented in section 3.

Finally, we conclude in section 5 with a set of recommendations about what to look for in a modern vulnerability management solution.

1.2 What is security and vulnerability management?

Vulnerability management is an integrated part of security management and belongs the domain of risk management.

Vulnerabilities in IT systems and software are caused by various factors, but most commonly faulty system configurations, bad system design or poor quality. In the case of faulty configuration, the cause of the vulnerability and responsibility to fix it lies in the same hands: the user's. In the latter cases however, one might argue that the responsibility to find and fix a vulnerability are on the vendor's side. Unfortunately, there too the user is often required to take matters into their own hands. Clever vendors have realized the business risks that come with software vulnerabilities and consequently try to externalized them: They've created end-user license agreements (EULA) which free the vendors from security vulnerability related liabilities [Anderson01] and place the task of finding and fixing vulnerabilities back in the hands of the user.

Even where vendors discover a vulnerability and try to alert their customers, there are often no means available to assess the individual risk exposure and response for each individual customer setting. Thus, it is up to the individual user again to identify their vulnerability risk and find ways of addressing it. This is what we consider vulnerability management.

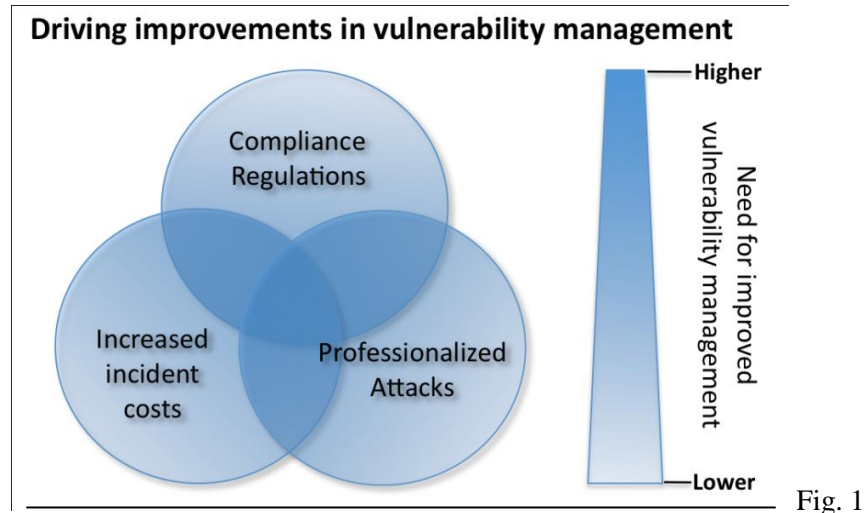
1.3 What is driving vulnerability management improvement efforts?

There are three major influences that drive improvement efforts in today's vulnerability management:

- 1) Attacks on the IT systems of organizations and individuals are increasingly professionalized.
- 2) The costs from security incidents and their counter measures are rising: In 2007 the CSI Computer Crime and Security Survey found that the average annual costs for reported security breaches in U.S. companies had nearly doubled since 2006 [Richardson07] [Welberg08].
- 3) New corporate governance legislation now mandates adequate security vulnerability management processes in companies and organizations which handle financial records, payment card information or privacy-critical data.

Individually, these factors already drive organizations to invest more in their security efforts, but where two or more of them apply at the same time, the need for improvement becomes even more evident.

Fig.1 depicts the growing importance of improvements in which several vulnerability management several factors overlap.



2 Challenges

Each of the three driving factors of vulnerability management presents a distinct set of challenges that organizations need to address in their improvement efforts.

Driving factor: professionalized attacks

Many practitioners describe IT-security management as a continuous arms race between the organization and its potential adversaries. In this race, it appears far too often as if the potential attackers had all the advantages: While an organization needs to defend itself against every possible form of attack, the attacker may only require a single point of entry to successfully breach security [Welberg08] (e.g. attackers can exploit a vulnerability in the implementation of an email server which is connected to both the internet and the local network to gain access the organization's internal information).

1st challenge: Attacker and defender fight on unequal terms.

Recent developments have elevated that problem: The attacks on organizations and individuals are increasingly professional and profit-driven. In the context of today's Black-Hat¹ community, professionalization means more resources are available to develop highly sophisticated tools, which allow attackers to automatically scan for exploitable security vulnerabilities in potential targets. The application of automation further enables attackers to use economics of scale to their advantage, by conducting parallel vulnerability scans on thousands of targets at the same time instead of just one, with little or no additional risk for the attacker.

Driving factor: Increased costs

While attackers use the economics of scale, the defense side largely relies on the effort of dedicated individuals to identify and patch vulnerabilities in their systems. Servers, infrastructure and software applications are tested for vulnerabilities on an irregular basis and often run vulnerable applications for months without notice.

The reasons are partly economical, since security efforts have to compete for resources with other business areas or are simply prohibitively expensive. Thus, far too many vulnerabilities (even those that would be extremely easy to find) remain open and expose the organization to outside threats.

¹ The 'Black-Hat community' refers to individuals in the area of IT security which tend to use their skills for malicious purposes, as opposed to those who consider themselves members of the 'White-Hat' community which use theirs to raise awareness of security issues and strengthen security in general.

2nd Challenge: Attackers can leverage the economics of scale while defenders often rely on individual efforts, resulting in a long half-life of unpatched vulnerabilities in organizations.

A well known example where unattended vulnerabilities caused significant losses was the outbreak of the “Code Red” and “SQL Slammer” internet worms. SQL Slammer exploited a weakness in Microsoft’s popular SQL server, for which a patch had been available 6 months earlier. Still thousands of systems remained unpatched and vulnerable when the worm hit.

Organizations that fell victim to the attacks often suffered costly interruptions of their business processes due to unscheduled maintenance work or reboots of production systems to clean up after the infection.

A related issue with increased costs is that the perception of their cause can be biased. The public media coverage of security incidents and the associated costs tends to single out high-profile cases such as the mentioned SQL-slammer, while omitting the fact that there are now more than 20 new vulnerabilities published every day [NVD2010].

Driving factor: Compliance regulations

Aside from interrupting business processes, the biggest issue for organizations whose’ security had been compromised is the loss of trust in the integrity of their data. The protection of data integrity however is vital for companies’ efforts to meet compliance regulations created by the PCI (Payment Card Industry’s PCI-DSS), ISO (ISO/IEC 27001) or legislation based on the Sarbanes Oxley Act (SOX), Basel II, etc.

3rd Challenge: Protecting the integrity of systems and data is essential for achieving continuous compliance with regulations like the PCI-DSS, ISO 27001, SOX and others.

2.1 Opportunities

Addressing the challenges of vulnerability management opens up new opportunities for gaining competitive advantages.

1st Challenge: *Attacker and defender fight on unequal terms.*

Organizations can resort to modern software tools and vulnerability discovery techniques that match those used by the attackers.

Opportunity: This enables organizations to prepare and evaluate their security measures from an attacker’s point of view, giving them a new vantage point on their security operations. Improved

oversight, combined with an organization's unique knowledge of their system's internal architecture opens the possibility to stay one step ahead of external adversaries.

2nd Challenge: *Attackers can leverage the economics of scale while defenders rely on individual efforts, resulting in a long half-life of unpatched vulnerabilities in organizations.*

The second challenge can be tackled by bringing the economics of scale back on the side of the organization and the people that work to defend its systems.

Opportunity: Security managers can establish processes and employ tools that are automated and re-usable across different platforms and systems within the organization. This relieves security staff from performing repetitive tasks like vulnerability discovery or reporting for each system individually, and the freed resources allow security managers to become pro-active again in previously neglected activities like patching or system documentation.

3rd Challenge: *Protecting the integrity of systems and data is essential for achieving continuous compliance with regulations like the PCI DSS, ISO/IEC 27001, SOX, Basel II, PCI and others.*

Maintaining well-documented systems is a key success factor for regulatory compliance. In most cases regulations are not a one-time task, but mandate a continuous and repeated efforts.

Thus, to achieve continuous regulatory compliance requires the capability to efficiently re-run security management processes on a regular basis. Automation can be used in this context to facilitate repeating tasks, such as monthly threat assessments, vulnerability discovery scans, or patch roll-outs.

Opportunity: Performing such tasks repeatedly comes with increasing learning effects (e.g. the efforts needed for compliance are reduced over time) and this opens the opportunity to discover trends that would have otherwise gone unnoticed (e.g. the monthly threat assessments may show an increased number of vulnerabilities since the switch to a new IT service provider).

3 Changing the game of vulnerability management

How did organizations engage in security vulnerability management before and what changed their way of thinking?

When the vulnerability management issue first appeared in organizations, their security staff often created individual solutions, that could be executed manually and were tailor-fit to the organization's particular environment.

The manual approach was well suited for highly customized and fairly static systems, but it brought along a series of problems, that did not surface until organizations started to grow and their IT systems began to change. In the context of vulnerability management, four particular issues stand out as 'game-changers': 1.) growing dynamics, 2.) commercial off-the-shelf software, 3.) industry standards, and 4.) compliance regulations.

3.1 Change driver: Growing dynamics

Organizational growth, faster technology cycles, and growing business dynamics create a series of problems for manual vulnerability management:

- As a company introduces new systems more often, it needs to conduct vulnerability assessments in shorter intervals [Wales03].
- Changes in IT systems require customized vulnerability solutions to be adapted or replaced.
- Frequent changes in vulnerability management tools and processes make it hard to compare results across platforms or over time. Time comparison is valuable to identify trends and evaluate the success of management decisions (e.g. “have our recent IT investments made us more secure, compared to last year?”).
- Timely patching of vulnerabilities becomes increasingly important: The time period between the public announcement of vulnerabilities and the availability of first exploits has been shrinking, thus leaving organizations with less time to find and react to threats.

“Organizations that frequently introduce new systems and software should conduct a vulnerability assessment more often.” [Wales03]

3.2 Change driver: COTS software

Many custom applications required unique vulnerability management solutions, which effectively prevented organizations from establishing economics of scale in their security efforts. The advent of commercial off-the-shelf software (COTS) products greatly improved this situation by standardizing interoperability between software systems and vulnerability management solutions.

3.3 Change driver: Common standards for vulnerabilities

In an effort to further advance interoperability, industry organizations introduced a set of vulnerability standards.

Two of the most influential ones are the CVE and CVSS: The Common Vulnerability Enumerator “CVE” established a dictionary of publicly known security vulnerabilities and enables different security solutions to share a common language when referring to particular vulnerabilities.

The Common Vulnerability Scoring System “CVSS”, was introduced to enable comparison and prioritizations of vulnerabilities based on their severity. CVSS uses a scores between 0 to 10, where 10 indicates the most critical vulnerabilities.

3.4 Change driver: Compliance

Legislators and industry organizations worldwide established corporate governance regulations in an attempt to improve the transparency and accountability of corporate governance processes. A central goal of these efforts was to establish common standards for risk management across organizations that include the management of information security and vulnerabilities.

Several of these standards, like the PCI-DSS², ISO/IEC 27001³, Sarbanes Oxley Act (SOX section 404)⁴, GLBA⁵ or Basel II are particularly relevant for security management issues, and have changed the way vulnerabilities need to be managed [Blount06]. In order to achieve continuous compliance, companies need to fulfill new requirements that strain the possibilities of traditional, manual vulnerability management processes.

Even though the compliance requirements differ between the individual standards, we can identify a set of common requirements in the security and vulnerability management context⁶:

- Req.1 - Proactive Vulnerability Analysis: An organization needs to actively search for potential points of weakness in their systems.
- Req.2 - A consistent auditing model across all platforms: All platforms (e.g. operating systems, application servers, etc.) need to be subject to the same security baseline and auditing.
- Req.3 - Documented processes: The security management activities are to follow a consistent and formalized process.
- Req.4 - Advanced reporting capabilities: Reports should be generated in human-readable ways, where the understanding of complex issues can be facilitated through meaningful forms of representation (e.g. graphical).
- Req.5 - Report customization: Reports should be tailored to the individual business context to improve applicability and reduce overhead.
- Req.6 - Flexible Alerting and notification services: Discovered security issues should be brought to the attention of the responsible roles within the organization in a timely manner.

² PCI DSS - Payment Card Industry Data Security Standard

³ ISO/IEC 27001:2005 - Information technology, Security techniques, Information security management systems and Requirements

⁴ Sarbanes Oxley Act -Corporate and auditing accountability and responsibility act.

⁵ GLBA - Gramm–Leach–Bliley Act requires financial institutions to develop a information security plan to protect clients' personal information.

⁶ Based on a combination of [Welberg08] and [Blount06]

4 Compliance with an automated vulnerability management lifecycle

The previous sections identified the major challenges, change drivers and a set of compliance requirements in vulnerability management. In this section, we will present a vulnerability management lifecycle, which is designed from the ground up to address these compliance requirements and support the use of advanced automation tools.

Based on the requirements raised in sections 2 and 3 we will lay out the activities of the vulnerability management lifecycle and give examples of how these activities can benefit from automation in Table 1. Finally we will compare the automated activities with the requirements R1-R6 (see 3.3) in Table 2 to determine whether all of them can be met by the presented approach.

4.1 A modern vulnerability management lifecycle

The iterative process of such as lifecycle follows three main phases:



Fig. 2

- Phase 1 - Identify the threat exposure: Which systems are vulnerable and are those vulnerabilities exposed to potential attackers?
- Phase 2 - Quantify the risk: How severe is the vulnerability compared to others, and how dangerous is it in the organization's particular business context?
- Phase 3 - Manage countermeasures: Identify and apply available countermeasures to resolve the vulnerability.

Each phase in the vulnerability management lifecycle consists of a number of individual process activities. The following Table 1 lists examples of these activities for each of the three lifecycle phases (P1-P3) and exemplifies how automation can be integrated in them.

Table 1:

A list of activities in the vulnerability management lifecycle and examples of how automation can be integrated in their execution.

Example activities and automation potential in the vulnerability management lifecycle			
Phase 1 Identify Threat Exposure	Phase 2 Quantify Risk	Phase3 Manage counter measures	Documentation (continuous)
<p>Example activity (Act.): List all applications with external exposure (e.g. that are listening on open ports on a web server).</p> <p>Example automation potential (A): A1 Use automatic, non-intrusive, scans to discover open ports. Conduct “fingerprinting” analysis to identify the applications that are listening on these ports.</p> <p>Act.: Acquire a list of known vulnerabilities for the identified applications.</p> <p>A2: <i>Integrate standardized, public vulnerability databases, like the National Vulnerability Database (NVD) or OSVDB in the vulnerability management tool.</i></p> <p>Act.: Test the identified applications for known vulnerabilities where possible.</p> <p>A3: <i>Use automated in-depth vulnerability scans or probing to complement non-intrusive scans..</i></p>	<p>Act.: Cross-check the list of relevant vulnerability list with the application list and identify matches.</p> <p>A4: <i>Automatically compare latest common vulnerability enumeration” (CVE) information with the scan results from A1 and A2.</i></p> <p>Act.: Quantify the relative severity of identified vulnerabilities, based on the possibility of their exploitation, the business impact of a successful an exploit, etc.</p> <p>A5: <i>Automatically calculate severity scores using NVD information gathered in A2 and the Common Vulnerability Scoring System (CVSS)</i></p> <p>Act.: Prioritize the vulnerabilities based on their severity on the particular business.</p> <p>A6: <i>Extend the basic CVSS scores with business context information according to the CVSS “Environmental metrics” specification.</i></p>	<p>Act.: Identify remedy or solution for the identified vulnerabilities.</p> <p>A7: <i>Search for solutions by using CVE information identified in A4.</i></p> <p>Act.: Upgrade application versions, apply patches or develop workarounds.</p> <p>A8: <i>Workflow support in a multiuser environment.</i></p> <p>Act.: Re-evaluate the vulnerability situation after the latest patches were applied.</p> <p>A9: <i>Automatically re-run the vulnerability scanning processes of A1-A6 after vulnerabilities were mitigated. Evaluate the results against the previous baseline.</i></p>	<p>Act.: Document the start, progress and results of a process.</p> <p>A10: <i>Use automatic reporting in each step of a vulnerability management processes.</i></p> <p>Act.: Summarize and report the results of a process in a meaningful and human-readable form of representation.</p> <p>A11: <i>Use a set of different predefined report templates to generate summaries at the required level of granularity.</i></p> <p>Act.: Compare the reports over a period of time. Identify indications of improvements or potential weakening of security baseline.</p> <p>A12: <i>Automatically compare vulnerability scan results and reports from A1-A6 to calculate deltas and identify trends.</i></p>

Having identified examples of automated activities in the vulnerability management lifecycle in Table 1, we can now match them with the common compliance requirements R1-R6 that were stated earlier (see 3.3). Our goal is to have every requirement addressed by at least one automated activity.

Table 2 lists the activities in the columns and compliance requirements in the rows. The resulting matrix indicates which automated activities can be used to fulfill, or facilitate meeting a particular requirement.

Table 2:

Connecting the automated activities of the vulnerability management lifecycle with business compliance requirements: Which automated activity can be used to fulfill or facilitate meeting the compliance requirement.

Business compliance requirements ↓	→ Automated activities			
	A 1,2,4 Automated vulnerability scans incorporating CVE, CVSS industry standards	A9 Regularly scheduled re-runs of automated vulnerability scans	A11 Flexible, customized report generation	A5, A6 Context aware vulnerability prioritization
R1 - Proactive Vulnerability Analysis	✓ fulfills	✓		✓ facilitates
R2 - A consistent auditing model across all platforms	✓	✓		
R3 - Documented processes		✓	✓	
R4 - Meaningful and human-readable reports and forms of representation			✓	
R5 - Reports tailored to the individual business context			✓	
R6 - Flexible Alerting and notification services				✓

Table 2 shows that every compliance requirement that was raised in section 3.3 is fulfilled by at least one of the automated activities in the vulnerability management lifecycle. The literature [Brenner06] suggest that complex, but well structured requirements like analysis and documentation in vulnerability management would particularly benefit from the use of automation and tools. Table 2 confirms this notion as the requirements R1 to R3 are all being addressed by more than one activity.

4.2 Limits of automation in vulnerability management

The automation of vulnerability management activities can bring significant cost savings, but also has its natural limits. Automated scans for vulnerabilities are only one part of a bigger security management puzzle. Human expertise is still needed to identify, for example, architectural flaws or physical weaknesses in a IT system.

Whether conducted by people or tools, all security management activities are also biased to a certain degree when they are conducted internally. Independent, unbiased security assessments by 3rd parties should thus be considered as additions to internal security efforts. Even the most thorough vulnerability management however, can only reduce the cumulative risk for an organization but is not able to ultimately prove that a system is 100 percent secure.

5 Conclusion

What should organizations look for when choosing a vulnerability management solution?

We propose a practical checklist, based on today’s vulnerability management challenges (see section 2), the common compliance requirements (see section 3), and the presented automated activities in the vulnerability management lifecycle (see section 4).

What to look for in a security vulnerability management solution:	
Decision criteria	What to expect
✓ Can identify the threat exposure of vulnerable IT systems.	Vulnerability scans with application fingerprint analysis and automated cross checks with vulnerability databases (e.g. NVD, OSVD, etc.)
✓ Can quantify the risk and prioritize vulnerabilities accordingly.	Calculation of severity based vulnerability scores, like CVSS.
✓ Can manage countermeasures.	Automatic suggestions for known vulnerability resolutions, bug-fixes or patches.
✓ Can perform proactive vulnerability analysis automatically.	Regular automatic vulnerability scans for individual or groups of systems at scheduled times.
✓ Uses a consistent auditing model across systems and platforms.	A unified and comparable vulnerability scan and prioritization model for all systems.
✓ Documents the start, end and progress of activities automatically.	Automated logging capabilities that ensure transparency, integrity and traceability of conducted vulnerability management activities.
✓ Can create meaningful and human-readable reports and trend analysis.	Several different forms of representation for reports, based to the intended audience. Automatic trend analysis and calculation of deltas across reports over time.

✓	Reports can be tailored to the required level of granularity and individual business context.	Sets of report templates for various levels of detail (e.g. Full technical reports, management summaries and alert digests.)
✓	Provides flexible alerting and notification services.	Timely communication of relevant information about newly identified threats via the best suitable communication channels (e.g. Email, SMS, RSS, etc.)
✓	Incorporating industry standards.	Native adoption of standards like CVE, CE or CVSS
✓	Built-in compliance with relevant regulations	Predefined or built-in checks for compliance regulations like PCI-DSS.
✓	Scalability with a predictable cost structure	Ability of the solution to efficiently grow with the organization at foreseeable costs.
✓	Accuracy and quality of vulnerability coverage	Frequent updates of vulnerability database and live integration of public vulnerability information (NVD, OSVDB or others)
✓	Ease of use	All of the above are accessible to the user in a way that is meaningful, efficient and easy to learn.
✓	False-positive handling	Ability to identify and learn from false-positives.

Conclusion

In writing this paper, we set out to show how organizations can use IT security vulnerability management as a tool to 1.) reach continuous compliance, 2.) become more cost effective in their IT operations and 3.) build a more robust business environment that allows them to compete with professional attackers.

For the first goal, we proposed a vulnerability management lifecycle that is structured, easy to document, and benefits from the use of automated activities.

Automation in the discovery, prioritization, and reporting of vulnerabilities help companies to realize economics of scale and become more cost-effective in their security operations. Effective security reduces the risk to suffer a security breach and helps lowering calculatory costs from the average annual loss expectancy (AALE).

While cost-effectiveness was the primary concern of the second goal, the use of automated and consistent auditing models also improves cost-predictability, by combining a defined process with the known execution costs of software tools.

The vulnerability management activities that were presented in section 4 further strengthen the robustness of systems from both, the compliance as well as the information security perspective.

The inherent documentation of all automated activities facilitates meeting compliance regulations even as they change over time and the ability to re-run automated vulnerability scans on a regular basis, help security managers leap ahead of potential adversaries. This combination of robust security and regulatory compliance creates advantages for organizations, as it allows them to venture in business areas that would be considered too risky by their competitors.

6 References and further reading

- [1] Anderson, R., “Why information security is hard - an economic perspective”. 17th Annual Computer Security Applications Conference. ACSAC. Proceedings (2001)
- [2] Blount, Summer. “The role of security management in achieving continuous compliance”, Whitepaper: Compliance, CA Security Management, October 2006
- [3] Brenner, M. Classifying ITIL Processes; A Taxonomy under Tool Support Aspects. Business-Driven IT Management, 2006. BDIM '06. The First IEEE/IFIP International Workshop on, (2006), 19-28.
- [4] Chen, Y. Stakeholder Value Driven Threat Modeling for Off The Shelf Based Systems. International Conference on Software Engineering, IEEE Computer Society Washington, DC, USA (2007), 91-92.
- [5] Frei, S., May, M., Fiedler, U., and Plattner, B. Large-scale vulnerability analysis. Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense, ACM (2006), 131-138.
- [6] Frühwirth Christian. “On Business-Driven IT Security Management and Mismatches between Security Requirements in Firms, Industry Standards and Research Work”. PROFES 2009: pp. 375-385 (2009)
- [7] NVD, National Vulnerability Database. Available online at <http://nvd.nist.gov> (visited Feb. 1st 2010)
- [8] Wales, Elspeth “Vulnerability Assessment Tools” Network security. Available online at http://www.compseconline.com/hottopics/hottopic_Nov03/Assessment_tools.pdf (2003)
- [9] Welberg, S.M. “Vulnerability management tools for COTS software - A comparison.” Technical Report TR-CTIT-08-15, Centre for Telematics and Information Technology, University of Twente, Enschede. ISSN 1381-3625 (2008)
- [10] Richardson, R., “CSI Computer Crime and Security Survey. 2007”, CSI. Available online at <http://www.gocsi.com>