BOF4WSS: A Business-Oriented Framework for Enhancing Web Services Security for e-Business

Technical Report CS-RR-441

Jason R.C. Nurse and Jane E. Sinclair
University of Warwick, UK
{jnurse, jane.sinclair}@dcs.warwick.ac.uk

Abstract

When considering Web services' (WS) use for online business-to-business (B2B) collaboration between companies, security is a complicated and very topical issue. This is especially true with regard to reaching a level of security beyond the technological layer, that is supported and trusted by all businesses involved. With appreciation of this fact, our research draws from established development methodologies to develop a new, business-oriented framework (BOF4WSS) to guide e-businesses in defining, and achieving agreed security levels across these collaborating enterprises. The approach envisioned is such that it can be used by businesses—in a joint manner—to manage the comprehensive concern that security in the WS environment has become.

1. Introduction

E-business has become the fastest growing means of conducting business in today's economy. In achieving the online B2B collaboration between e-businesses, the use of services-oriented computing, by way of Web services (WS) technology, is playing an increasingly significant role [19]. The novel benefit is rooted in its ability to allow for seamless integration of business processes across disparate enterprises, due to the use of standardized protocols and open technologies [4]. As WS' use expands however, securing these services becomes of utmost importance.

In an attempt to address new security challenges accompanying WS, standard-setting bodies have proposed numerous pioneering standards. As WS matures, the move from lower level security details such as standards and technologies, to higher level considerations however, is imminent [13]. Security, irrespective of the context, is a multilayered phenomenon encompassing aspects such as practices, processes and methodologies. This factor is especially true with WS which, as authors [9] note, substantially complicates the security environment for e-businesses.

Considering this, and with special appreciation of the inter-organizational security issue now facing businesses interacting using WS, our research focuses on identifying a novel, business-oriented approach to guide companies in achieving agreed security levels. The approach envisioned will be such that it could be used by businesses—in a joint manner—to manage the comprehensive concern that security in the WS environment has become.

The remainder of this paper is structured as follows: Section 2 contains a brief review of the security advancements in WS use for e-business with the aim of identifying outstanding security issues, and therefore paving the way for this research. Next in Section 3, an overview of the proposed business-oriented framework, including its novelty and use, is given. Future work is outlined in Section 4.

2. Web Services Security within e-Business

2.1. State of the Art

Albeit a promising enabling technology for e-business, WS usage comes at the high price of an unstable security foundation. The literature identifies numerous challenges [1, 13], but the most pertinent for our research is the reality that WS adds significant complexity to the e-business security landscape [9], thus making security a much broader and comprehensive concern which cuts across business lines much easier and quicker than before. As such, an inadequate security posture in one company can mean an increased, real-time security risk for its partners—both immediate and extended.

To address the new security challenges mentioned above, consortiums such as OASIS and W3C have developed and ratified numerous pioneering standards (as can be seen in [13]). These standards aim to both solve problems caused by common threats and also to further the WS paradigm by enabling substantially more dynamic security interactions between services. Beyond addressing the perceived inadequacies of the current standards base, researchers are now targeting the more general components of a security solution such as best practices and processes. These actions give life to a prediction made by NIST, which emphasized that as WS technology matured, methodologies and recommended practices for security would become the next step in the goal of developing secure systems [13].

Some of the most pertinent, and noteworthy proposals focusing on these higher layers are: [2], which builds on existing technologies and the theory of Aspect-Oriented Programming, to provide a framework for securing WS compositions (necessary in collaborative e-business) using the WS-Security and WS-Policy standards; [8] aims to provide a methodical development approach for constructing security architectures for WS-based systems; [14] which provides integrated WS design strategies and best practices for end-to-end security; [17] – a method that uses fuzzy logic to measure the risk associated with WS, with full appreciation of the fact that due to WS' volatility, information on threats is usually incomplete or imprecise; and lastly the Event-driven Framework for Service Oriented Computing in [16] – a standard agnostic, multilayered framework that aims to address the problem of defining and enforcing access control rules for securing services use at the level of business processes. In their work, authors particularly focus on dynamic authorization, independent of specific standards [16].

2.2. Outstanding Security Issues

WS security approaches should aim to be thorough in planning, developing and maintaining an adequate solution. Standard security components encompass technologies, but as recent literature [12] in the study of security has emphasized, they also include policies, processes, and best practices. To WS' detriment, this fact does not appear to be unanimously shared as any attention on these other aspects has been drowned out by a proliferation of new technology standards. It may therefore be very tempting to regard such mechanisms as the 'solutions' to the WS security problem. Whilst the works of technologists are valuable to building security and trust however, they cannot form the entire solution. In fact, all these mechanisms address is the technology layer of security, and threats which emanate at that level; thus only providing a stepping-stone in the goal of comprehensive, multilayered security. This perspective is supported by [13] as they identify tasks such as effective risk management, and defence-in-depth through security engineering, as critical to developing robust, secure systems.

A final concern regarding standards is that there are already too many available [7]. Therefore, as opposed to benefiting WS, this plethora of sometimes overlapping standards ultimately confuses developers and acts to complicate secure WS implementation and use. The importance of these factors is magnified when assessing WS use for the already complex field of e-business.

To briefly assess the aforementioned research in [2, 8, 14, 17], these are all seen to successfully complement available technologies, and provide useful security approaches. Their main caveat however is that they consider security predominantly from one company's internal viewpoint i.e. what should a company do internally to secure itself. This highly isolated perspective is inadequate due to the very nature of WS, and the high degrees of interconnection between businesses—spanning exposure of legacy systems to purpose-built Web applications—that WS readily facilitates. In [16], even though this allows for a layered, and more comprehensive model for WS security during business process execution, its predominant focus is towards access control, and particularly for highly dynamic environments. Both these aspects act to make it too specific a framework for our purposes as mentioned in subsequent sections.

Looking beyond these advancements, an intriguing research area which has received little emphasis is at the level of cross-enterprise interaction (i.e. interactions spanning, and including collaborating businesses and their systems). Specifically we refer to providing some comprehensive approach to aid businesses, in collectively handling security as the broad, inter-organizational concern it has become. This approach would not be solely at the technical level but look generally at a number of other fundamental aspects (e.g. security directives, policies, government regulations, best practice security standards, business risk considerations, and negotiations necessary) that businesses should jointly consider when engaging in B2B interactions employing WS. The next section presents current research thinking for this approach.

3. BOF4WSS

3.1. Overview

To address the outstanding security issues mentioned to above, and strengthen available solutions, the Business-Oriented Framework for enhancing Web Services Security for e-business (BOF4WSS) in Figure 1 was conceived. As is illustrated, the framework consists of nine stages which in general, semantically resemble those found in typical systems development methodologies. Again, like some methodologies, bottom-up progression through feedback is allowed, even though the process is suggested to be mainly top-down, and sequential from Stage 1 to Stage 9.

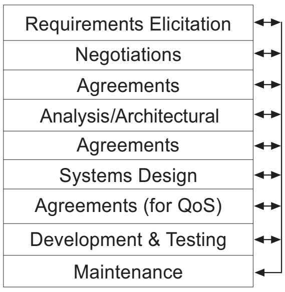


Figure 1. BOF4WSS Overview

The prime novelty in the BOF4WSS is its emphasis on providing an expanded formalization of a development methodology that focuses on security, which can accommodate multiple autonomous businesses working together. Below, we focus on giving a brief, largely textual description of each stage to provide an overview of the process. Within the actual framework however, specific, detailed guidance is given on what should occur and how, and its pertinence in attaining desired levels of holistic security across these collaborating enterprises. This includes defining the expected inputs to stages, along with their required outputs/outcomes, but especially the recommended low-level goals, activities, and steps within those stages that can help achieve the outcomes. Where suitable, this guidance reuses existing methods and practices, thus concentrating on the compilation of these into a coherent, well-defined process instead of reinventing standardized security components. To provide a more practical example of the framework's actual activities, after outlining the first three stages below, we include a diagram illustrating their respective workflows. Our overview also assumes that businesses have previously agreed (through feasibility studies, initial dialogue, and so on) to use WS for a generally defined business scenario.

The **Requirements Elicitation phase** is the first stage and within it each company works largely by itself, analyzing internal business objectives, constraints, security polices, relevant laws and regulations and so on, to determine their high-level requirements for the expected WS business scenario. To aid in this process, the phase utilizes the methods proposed by [6], which focus on the definition and analysis of business process models to elicit requirements. This approach is preferred due to its innate emphasis on business processes—i.e. the culmination of service interactions.

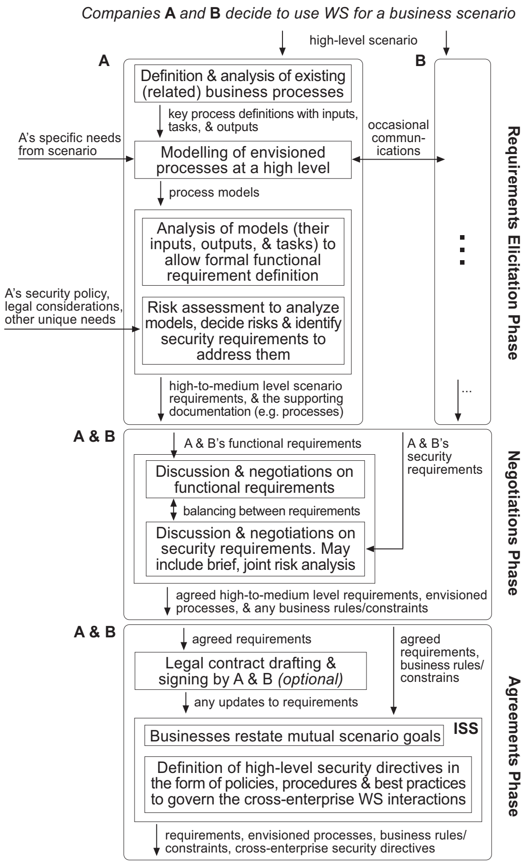
In brief, this approach consists of gathering relevant knowledge about the process domain and what influences it; analysis and modelling of current processes to enable for a full appreciation of key process flows, inputs and outputs; modelling of new processes; and finally requirements determination through analysis of the new processes. In addition to the security requirements identified in that approach, a scenario risk assessment is strongly suggested to provide more detailed security information. This enables identification of risks and their priority levels (i.e. severity and impact if they materialize), and the resulting security requirements that should be factored in during these WS communications.

In the **Negotiations phase** next, companies meet, bringing together their requirements for discussion. The purpose is to chart an agreed path forward especially with regards to the varying expectations each company has towards security. This phase facilitates this aim by accepting that each business constitutes a different security domain (and is likely to have different desires and obligations), and therefore explicitly stresses the need to negotiate on security requirements. This is rather than adopting one company's needs, or assuming integration of desires at this level will be seamless. Work in [15] clearly highlights that in forming these extended networks or partnerships of companies, this integration task is formidable. Regardless however, this is a necessary, and pivotal precursor to engaging in interactions.

The **Agreements phase** builds on the concluded negotiations and initially advocates a legal contract to cement the understanding of the requirements between companies thus far. This legal document is followed by the Interaction Security Strategy (ISS) which, as opposed to the contract, is a less rigid management structure that defines high-level, cross-enterprise security directives to guide the interactions. This strategy stresses the consideration of legal and regulatory requirements (e.g. data protection/privacy), and also the incorporation of best practice security standards (e.g. ISO-27001/27002) by companies when approaching inter-organizational security. Examples of what the ISS would purport include the specification of best practices each company should abide by internally, definition of scenario incident response activities, and also the creation of a cross-enterprise team to handle security matters, and update the ISS and other security measures as appropriate. Another key goal of this strategy is to foster trust amongst business partners through predictability and transparency in security approaches, by outlining a structure that all businesses agreed to adopt and follow. With the preceding three stages outlined, we now show a more detailed example of the activities that take place in Figure 2.

From the workflow model in Figure 2, one can see how companies move from the initial decision to use WS, to begin creating a solution architecture which emphasizes high levels of security. Most of the aspects depicted in the diagram have been discussed previously therefore will not be reviewed again. The two key parts that should be noted however are (i) the practicality of the activities—the framework is in essence a set of tasks guiding companies to view WS security for e-business more holistically; and (ii) the flows of information within, and across these collaborating parties as they work to put the requisite security in place.

Having presented these three stages and their interfaces



Companies A and B decide to use WS for a business scenario
high-level scenario
A
B
Definition & analysis of existing (related) business processes
key process definitions with inputs, tasks, & outputs
A's specific needs from scenario
occasional commun-ications
Modelling of envisioned processes at a high level
process models
Analysis of models (their inputs, outputs, & tasks) to allow formal functional requirement definition
A's security policy, legal considerations, other unique needs
Risk assessment to analyze models, decide risks & identify security requirements to address them
high-to-medium level scenario requirements, & the supporting documentation (e.g. processes)
...
Requirements Elicitation Phase
A & B
A & B's functional requirements
A & B's security requirements
Discussion & negotiations on functional requirements
balancing between requirements
Discussion & negotiations on security requirements. May include brief, joint risk analysis
agreed high-to-medium level requirements, envisioned processes, & any business rules/constraints
Negotiations Phase
A & B
agreed requirements
agreed requirements, business rules/ constrains
Legal contract drafting & signing by A & B (optional)
any updates to requirements
ISS
Businesses restate mutual scenario goals
Definition of high-level security directives in the form of policies, procedures & best practices to govern the cross-enterprise WS interactions
requirements, envisioned processes, business rules/ constraints, cross-enterprise security directives
Agreements Phase

Figure 2. Stages 1-3 in more detail

in more detail, we resume our overview of the framework with the **Analysis/Architectural phase**. This phase's purpose to enable companies to take the agreed requirements and jointly define conceptual business process models for the foreseen interactions. With this in place, the directives (policies, best practices, and so on) from the ISS can then be applied to secure the models. This two stage method to securing business processes is adopted from research done in [11], which focused on decomposing processes into flows with inputs and outputs, then applying derived security objectives to secure process components. For our framework therefore, this stage's expected output is a blueprint for the high-to-medium level process flow, and also the respective security architecture. Following the formal process definition, the framework suggests the use of another **Agreements phase**, this time in the form of a more thorough legal contract reflecting detailed expectations of the parties. Contracts are used primarily as a safety net, and leave the role of governing day-to-day interactions to the ISS.

The **Design phase** next is analogous to a company's internal systems design process (for e.g. see [14]) and therefore helps businesses define a logical, low-level systems view of exactly how the conceptual model from the Architectural phase will be achieved. Specific objectives constituting this aim are: the identification of relevant WS standards; a trade-off analysis of their use; and the actual application of standards where appropriate (e.g. WS Choreography Description Language (WS-CDL) to specify top-level process models). Agreement is paramount noting the often confusing standards sets now available. Beyond standards agreement, harmonizing data and process semantics is also an issue worthy of consideration when discussing inter-company interactions as stressed in [10]. A semantics framework and shared vocabularies are therefore to be specified in this stage. With these aspects and the stage complete, a specification document is produced that is appropriate for systems and software developers to implement.

At this point, the low-level processes and services are defined, thus the following phase concentrates on **Agreements** necessary at the quality-of-service (QoS) level. The purpose is to specify the mutual understanding of the priorities, responsibilities, and guarantees expected by each business for the actual Web services. QoS elements decided include service availability needs (e.g. uptime of 99.98%), performance requirements (e.g. average response time of 30 milliseconds) and so on. Apart from natural language statements which form what is commonly known as a Service-Level Agreement, specification is done using relevant policy and service agreements standards such as WS-Policy.

The penultimate stage is the **Development & Testing phase**. Due to its focus on internal company systems, it is largely carried out by companies individually. Occasional joint interactions are however appreciated for testing, and system verification (to established requirements). The input to this stage is the agreed systems design specifications (natural language and standards-based) and the service-level agreements. These are used by the individual companies to steer their internal systems implementation.

To aid in this internal process, the framework builds on current research and suggests the use of guidelines from more detailed and tested approaches such as [8, 10]. In the former work the aim is on the development process for secure WS, whereas the latter article presents a lifecycle methodology that focuses on critical aspects such as application integration, migration from old to new Web services-based processes, and the 'best-fit' ways of implementation which appreciate company constraints, risks, costs and returns on investment. A key benefit to using these approaches is that information gathered and produced earlier in the framework can be reused to quickly complete their initial stages. Such information includes functional, security and QoS requirements, risk assessment data, and business process models. The last step in this phase is to verify that developed systems have achieved the requisite amounts of application-level security. To aid in this, an evaluation is advocated through the use of penetration testing and WS-specific approaches such as those presented in [18].

Having developed this comprehensive, multilayered security solution, its upkeep becomes the next crucial undertaking. The BOF4WSS addresses this and other typical monitoring and preservation tasks in the **Maintenance phase**. Specifically, this stage will involve functional system enhancements, but additionally will stress the continued updating and enforcement of security measures, both in developed systems and the ISS. The cross-enterprise team mentioned in the first agreements stage is integral in this process. They are entrusted with the responsibility of monitoring the internal and external environments, and considering new threats, laws, and business requirements, and how these will be included in solution updates.

As can be seen from the preceding paragraphs, the framework provides a detailed guidance model for inter-organizational cooperation. Beyond this, the next aim in our research (discussed in Section 4) is to drill down into the framework's specifics and provide a practical implementation base. This includes investigation into how stages of the architecture can be expanded, when or where can existing mechanisms be used, and lastly in the provision of suitable infrastructure and tool support to aid in framework use.

Reflecting on our approach in its entirety, specially with regard to its use by companies, it is obvious that this is not a process to be taken flippantly. In the design of this framework, not only were security practices within WS and business processes in general assessed, but also literature on joint business ventures such as the extended enterprise (e.g. [5]), and how security—beyond the technical layer—is reached, and maintained across enterprises there. With these factors in mind, the framework is thus aimed particularly towards businesses that emphasize trust and medium-to-high levels of security, and expect long-term interactions as opposed to the short-term, highly dynamic, e-marketplace-type interactions also possible with WS. To utilize this approach, companies will have to be prepared to work together and devote resources—financial and nonfinancial (e.g. time, skills, experience)—to this venture. Many changes in how the businesses worked before WS adoption will be necessary. However as stated in [3] concerning WS in general, "the potential benefits — both financial and strategic — to adopting Web services are sufficiently large to justify such [business] changes." The same fact is true when focusing on security specifically.

Another crucial factor supporting the highly involved approach to security central to the BOF4WSS, is the emerging legislative requirement-base. These regulations (partially shown in [14]) demand that companies now look both internal and external (i.e. business relationships) in their considerations of security. In [9], authors commenting on the new security responsibilities in WS, state that "risks must be assessed and managed across a collection of organizations, which is a new and very challenging security responsibility". They also make the point that to ensure collective WS offerings between businesses are secure, elements such as strategies and structured approaches to security must be used [9]. All these requirements fuel the need for a security approach such as the BOF4WSS. The following section continues the framework presentation by discussing how it enhances security in a WS-enabled e-business scenario.

3.2. Application Scenario

Background: Companies A and B are two e-businesses previously unknown to each other that are entering into an agreement to use WS to support their joint B2B interactions. Thus far, they have started initial discussions on processes and functional service requirements. At the point of examining the security of processes and services, the businesses quickly call upon their technical personnel, and prime topics of interest include decisions on standards to be used, and what levels of security are desired and accepted. Assuming all goes well, and agreed-on standards are implemented, both companies feel that a good level of security is in place to protect their joint WS offerings.

Problem: Overall, Company A deems security as a higher priority than it is regarded by Company B. As a result, in A's decision to engage in WS, they conducted a number of risk assessments, analyzed numerous factors that may affect services and external partners, and then put the necessary policies, practices, and mechanisms in place to treat them. Company B however, did not conduct these internal assessments, and therefore have not noticed vulnerabilities in their web site that can be used to hijack their services. Assuming the case where B's services are hijacked, A is directly threatened as an attacker can send inaccurate messages, SQL injection attacks, oversized XML payloads and so on to A, under the disguise of B. Furthermore, if A's message checking policies towards known parties is less stringent, A may not check for, or detect these attacks, thus resulting in a security breach in their systems.

Problem statement: Predominant focus on technical WS solutions (e.g. standards) leads to false sense of security.

Framework's contribution: The joint process advocated by the framework emphasizes comprehensive security, and thus considers factors beyond technical implementations. For this scenario, the first two stages are especially relevant. The Requirements Elicitation stage for example, advocates risk assessments amongst other things to determine each business's security requirements for the scenario. The Negotiations stage that follows, brings companies together to deliberate on these requirements, and to decide an agreed path forward regarding service, and general communications security. The first point of note is that in accordance with the framework, B would be expected conduct a detailed risk assessment for the expected interactions, then to bring deduced requirements into Stage 2 for discussion.

At the Negotiations stage, each party would have the opportunity to assess the other's requirements, inquire about other security measures if necessary, and finally put forward their requirements for the scenario. During this assessment therefore A is likely to recognize areas not analyzed by B and follow these up, or if crucial, request the need for a security audit of B before proceeding. It is accepted that charting a way forward will not be an easy task, as synchronizing best practices and negotiating desires are formidable tasks. However, both of these are important steps to achieving a comprehensive, cross-enterprise security solution agreed, supported, and trusted by participating companies.

4. Conclusions and Future Work

In this paper, we introduced the BOF4WSS—a comprehensive, grounded framework geared at enhancing the currently available approaches to WS security within e-business. We argued that because of the nature of WS, the security of collaborating e-businesses was now a much broader, more critical, and more real-time issue than ever before. This is due to immediate threats to a company, but also threats that easily propagate from poorly secured business partners. The novelty of our approach is that it considers the full nature of WS, and its security implications (technical and otherwise); recognizes and targets the 'live' inter-organizational security issue now faced by interacting e-businesses; and finally, promotes the use of a joint approach where businesses work closely together and follow a well-defined process, to achieve enhanced levels of security and trust across partners. Our approach therefore aims to be a facilitator of, instead of a panacea to WS security.

Regarding future work, the first area of interest is the provision of systems support for the framework itself. As can be seen, BOF4WSS is a complex and extensive process. To aid in its use therefore, we intend to further examine each stage and the interface between stages, and provide support wherever applicable. One potential area already identified (through an initial exploratory investigation), concerns the outputs from one stage and their immediate usefulness as inputs to subsequent stages. Particularly of interest is traversing between individually and jointly completed phases e.g. the Requirements Elicitation to Negotiations phase respectively, where there might be vastly different ways, or formats in which requirements are produced by companies. Possible directions under research are providing systems support based on open technologies, WS-based and otherwise, to streamline this stage transition.

Once the detailed framework is complete, our next goal will be its application to a case scenario to critically evaluate its suitability and strength. Noting the framework's complexity, key areas for immediate evaluation will be the practical, system supported stages such as those targeted above. The evaluation process in its entirety however is pivotal, as it enables for the assessment of how well the framework's aims of enhancing security and trust across businesses have been achieved, but also to facilitate any needed refinement.

Acknowledgement

The authors would like to thank Darren Mundy for his insightful feedback and comments on this work.

References

[1] R. J. Boncella. Web services and web services security. *Communications of the Association for Information Systems*, 14(18):344–363, 2004.

[2] A. Charfi and M. Mezini. Using aspects for security engineering of web service compositions. In *IEEE International Conference on Web Services*, pages 59–66, Orlando, 2005.

[3] S. Chatterjee and J. Webber. *Developing Enterprise Web Services: An Architect's Guide*. Prentice Hall PTR, Upper Saddle River, NJ, 2004.

[4] M. Chen. An analysis of the driving forces for web services adoption. *Information Systems and e-Business Management*, 3(3):265–279, 2005.

[5] E. W. Davis and R. E. Spekman. *The Extended Enterprise: Gaining Competitive Advantage through Collaborative Supply Chains*. FT Prentice Hall, Upper Saddle River, NJ, 2004.

[6] O. Demirörs, Ç. Gencel, and A. Tarhan. Utilizing business process models for requirements elicitation. In *29th Conference on EUROMICRO*, pages 409–412. IEEE, 2003.

[7] S. Fischer and C. Werner. Towards service-oriented architectures. In R. Studer, S. Grimm, and A. Abecker, editors, *Semantic Web Services: Concepts, Technologies, and Applications*, pages 15–24. Springer-Verlag, Berlin, 2007.

[8] C. Gutiérrez, E. Fernández-Medina, and M. Piattini. PWSSec: Process for web services security. In *IEEE International Conference on Web Services*, pages 213–222, Chicago, IL, September 2006.

[9] B. Hartman, D. J. Flinn, K. Beznosov, and S. Kawamoto. *Mastering Web Services Security*. Wiley, Indianapolis, 2003.

[10] M. P. Papazoglou. *Web Services: Principles and Technology*. Prentice Hall, Harlow, Essex, 2007.

[11] S. Röhrig and K. Knorr. Security analysis of electronic business processes. *Electronic Commerce Research*, 4(1-2):59–81, 2004.

[12] B. Schneier. *Secrets and lies: digital security in a networked world*. Wiley, Indianapolis, 2004.

[13] A. Singhal, T. Winograd, and K. Scarfone. Guide to secure web services (NIST SP 800-95). Technical report, National Institute of Standards and Technology (NIST), 2007.

[14] C. Steel, R. Nagappan, and R. Lai. *Core Security Patterns: Best Practices and Strategies for J2EE^{TM}, Web Services, and Identity Management*. Prentice Hall PTR, 2005.

[15] J. S. Tiller. *The Ethical Hack: A Framework for Business Value Penetration Testing*. Auerbach Publications, Boca Raton, FL, 2005.

[16] W.-J. van den Heuvel, K. Leune, and M. P. Papazoglou. EFSOC: A layered framework for developing secure interactions between web-services. *Distributed Parallel Databases*, 18(2):115–145, 2005.

[17] P. Wang, K.-M. Chao, C.-C. Lo, C.-L. Huang, and M. Younas. A fuzzy outranking approach in risk analysis of web service security. *Cluster Computing*, 10(1):47–55, 2007.

[18] W. D. Yu, D. Aravind, and P. Supthaweesuk. Software vulnerability analysis for web services software systems. In *IEEE Symposium on Computers and Communications*, pages 740–748. IEEE, 2006.

[19] J. Zhang. Trustworthy web services: Actions for now. *IT Professional*, 7(1):32–36, 2005.