Web Services for rural areas – Security challenges in Development and Use

Elias Pimenidis
School of Computing, Information Technology and Engineering, University of East London, 4-6 University Way, London, E16 2RD, United Kingdom, Tel. +44 208 2237655, e.pimenidis@uel.ac.uk

Christos K. Georgiadis
Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece

Web Services (WS) are the modern response of traders and online service providers to satisfying the increasing needs and demands of the digital communities. WS formation and operation is based on a software system designed to support interoperable machine-to-machine interaction over a network. Security is of paramount importance to WS and the ability to measure and evaluate the level of security available, is key to establishing and continuing to develop the level of trust based on reputation developed by the provider of the WS. The greatest challenge in offering secure WS is to groups of people where the level of expertise of the user is low and the need for transparency of the service provision quite high, such as the case with services offered primarily to people in rural areas. Providers of such services face many challenges in balancing the requirements for performance, interoperability, and security against the cost of implementing secure systems and running profitable operations through low income generating WS. A review of services offered, of the users and the challenges in building online trust amongst providers and users are discussed for the case of rural areas in the United Kingdom.

Key Words— Web Services, WS Security, WS and Rural Areas, WS development challenges

1. INTRODUCTION

WS are the modern response of traders and online service providers to satisfying the increasing needs and demands of the digital communities.

WS formation and operation is based on a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the WS in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with XML serialization in conjunction with other Web-related standards as illustrated in figure 1 below.

From the above it is evident that human interaction is minimal with the components of the service. Thus the whole responsibility of compiling and orchestrating the service lies with a single member of the instantaneous online community that is established temporarily to meet the needs of the public. This is the service orchestrator, i.e. the entity that interacts with the public, responds to their needs and coordinates the formation of the service in completing the transaction with the requester. Once the transaction is complete the instantaneous community which has provided the service is disbanded. The whole concept is based on trust relationships established with the public by the initiating partner and ensuring that it is adhered to by the participating partners. According to Haley et al (2004) a trust relationship is one that involves multiple entities (e.g. people, companies, or software components), while trust is the quantified belief in the competence, honesty and reliability of the trustee by the entity that engages in a trust relationship with them.

Security therefore is of paramount importance to web services and the ability to measure and evaluate the level of security available, is key to establishing and continuing to develop the level of trust based on reputation developed by the provider of the WS.

Figure 1 To be inserted here

This paper looks at the key features of security implementation for WS provision, provides an analysis of various evaluation criteria discussed in the literature and proposes the authors' own approach to evaluating security of WS. The emphasis here is on application areas where the level of expertise of the user is low and the need for transparency of the service provision quite high, such as the case with services offered primarily to people in rural areas.
The first section of the paper addresses WS and their development platforms. The following section looks at WS and security issues, security implementations and some security evaluation criteria. The third section looks at WS across different application domains. Security provisions and security challenges for WS offered to primarily urban populations versus those mostly offered to populations in rural areas are discussed in the last section. A brief look at intermediate results of an ongoing research with some reference to early conclusions is also provided.

2. Web Services – An Overview

WS integrate applications owned by different organizations (even if they are developed in different programming languages and deployed on different platforms) to provide a loosely coupled architecture for building distributed systems with universal interoperability. As a result, WS have been widely adopted in industry as a standard platform-independent middleware technology.
Cooperative services are capable of intelligent interaction and are able to discover and negotiate with each other, mediate on behalf of their users and compose themselves into more complex services. These exact properties of WS are the ones that present most challenges and raise the issue of guaranteeing a given "quality" of services to final users. This concept of quality is expressed in terms of functional and non-functional requirements, such as performance or security and it is these two particular attributes that attract researchers in their quest for means of evaluating WS.
A WS is a software system identified by a URL, whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems. These systems may then interact with the WS in a manner prescribed by its definition, using XML-based messages conveyed by internet protocols. This definition has been published by the world-wide-web consortium W3C, in the WS Architecture document (Booth et al, 2004).
Demand and offers for WS expand on a daily basis. The need for advanced tools to help identify services that match a service customer's functional and non-functional requirements becomes increasingly important.
Similar needs exist on the service requesters' side to describe their requirements in an unambiguous and machine-interpretable way (Bichler and Lin, 2006).
To effectively provide WS of high and competitive standard virtual enterprises need to effectively manage workflow within the confines of their enterprise. This can be achieved by a software running one or more workflow engines, which is able to interpret the process definition, interact with workflow participants (systems managing processes within individual participants) and, where required, invokes the use of IT-tools and applications (Gortmaker et al, 2004).
A further challenge in the provision of WS is that of supporting automated discovery and selection of world-changing services. Service descriptions must be unambiguous about what situations will guarantee successful service uses, and what new situations will result from those uses. This is essential as service

behaviour may vary with time, location, user history, and pre-existing contractual commitments (Martin, 2006).

Service-oriented computing and WS are becoming more popular, enabling organizations to use the Web as a market for selling their own services and consuming existing services from others. Nevertheless, the more services are available, the more difficult it becomes to find the most appropriate service for a specific application (Birukou et al, 2007).

Addressing the problem of WS transaction successfully, requires the establishment of a generic and reusable WS *coordination* architecture. Transactions are capable of managing and coordinating multiple tasks. In addition, to automate complex business processes using WS, future applications must be built based on long-lived loosely coupled asynchronous transactions. This is due to business processes consisting mainly of multiple transactions for routing documents (document-style WS) to the applications and users that implement the business process (Kaye, 2003).

Thus, supporting transactions depends significantly from the approach used to connecting WS together to form meaningful business processes. Initially, terms such as "*WS composition"* and *"WS flow"* were used to describe the composition of the WS in a process flow. More recently the following terms are used (Kaye 2003, Georgiadis and Pimenidis 2006):

- *Orchestration* describes how WS can interact with each other at the message level, including the business logic and execution order of the interactions. These interactions may cross applications or/and organizations and actually formulate a transactional, long-lived multi-step process model. WS *orchestration* describes the way WS coordinate complex multi-party business processes.
- *Choreography* is typically associated with the public message exchanges that occur between multiple WS, rather than a specific business process that is executed by a single party. While for *orchestration*, the process is always controlled from the perspective of one of the business parties, *choreography* is more collaborative in nature: each party involved in the process describes simply the part they play in the interaction.

A service composition combines services following a certain composition pattern to achieve a business goal, solve a scientific problem, or provide new service functions in general. Service compositions may themselves become services, making composition a recursive operation. (Curbera et al, 2003). Specifications such as the Business Process Execution Language (BPEL) and the WS Choreography Interface (WSCI), focus on tying multiple WS together to create multi-step applications, such as filling a purchase order or resolving an insurance claim. While specifications such as BPEL and WSCI provide the mechanism for extending the WS Description Language (WSDL) layer to identify a series or sequence of execution for multiple WS, the following coordination-oriented specifications define the complementary system layer necessary to ensure that the multiple WS achieve the desired results of the application, and that the cooperation of multiple WS from whatever source (local or remote) produces predictable behavior despite system failure and leaves the system in a known state (Little, 2007).

3. Web Service Security Considerations

The WS model consists of three entities, the service provider, the service registry and the service consumer. The key requirements for any service provider are: Interoperability, Security and Performance. Most researchers focus on a common belief that interoperability of WS must come along with considerable performance penalty (Georgiadis and Pimenidis, 2007). One common finding is that all three could be affected by the automatic choice of partners in forming a WS and that all three could mutually affect each other (Casola et al, 2007).

The most attractive feature of WS is its interoperability in a heterogeneous environment, and exposing existing applications as a WS increases their reach to different client types. Security measures are not something that can be added in a certain system's architecture, without having thought of them and

designed them at the very early stages (Chen et al, 2007). The integration of context into WS composition/transaction ensures that the requirements of and constraints on these WS (either security- or interoperability-oriented) are taken into account. Context may support WS in their decision-making process when it comes to whether accepting or rejecting participation in a transaction (Casola et al, 2007, Georgiadis and Pimenidis, 2007).

Casola et al (2007) argue that although a service provider is able to guarantee a predefined service level and a certain security level the mere nature of service integration and interoperability and the utilisation of state of the art technologies does not allow for automatic measurement of such attributes. The most common approach amongst service providers is the "Service Level Agreement" (SLA). At the state of the art, SLAs are primary related to the quality of service and not to security. To reach the aim of SLA dynamic management to support the interoperability among services, a formalized approach both for defining the different quality factors of a service in a SLA, and for evaluating them automatically is required.

Current WS specification on security, trust and agreements (WS-Security, WS-Trust) promote the adoption of policies as the basis on which to interoperate. Policy languages are now widely available (e.g. WSPolicy, WS-Agreement) but they do not specify how to automatically evaluate and compare the related security and quality provisions (Casola et al, 2007, Chen et al 2006). These are of primary importance in engaging and maintaining the trust of users.

The solutions to the security challenges are still evolving and so pre-standard workarounds to security problems provide a critical aspect of the whole process. A complete security solution should include multiple platforms. The path of a WS request message is followed in the sample configuration of figure 2, to illustrate an indicative way to combine the responsibilities of the various security platforms-solutions (Chen et al, 2006):

- Data of critical importance, with high-level requirements for confidentiality and integrity, must be encrypted using host-based (or application-based) security mechanisms. By performing encryption (at requestor's side) and decryption (at provider's side) as close to the application as possible, data integrity and confidentiality are protected over the greatest percentage of its route. This platform is capable to perform more granular authentication and authorization than is possible in the XML/Application firewall.
- The XML/Application firewall verifies XML syntax and checks documents against business rules. Moreover, it authenticates and verifies the authorizations of entities submitting external requests. Finally, it may encrypt data of less importance. Because it is separate from the WS, the XML firewall is able to provide security for multiple WS applications. By handling all encryption and decryption tasks, it provides a complete set of integrity and confidentiality services covering both component-level issues and end-to-end issues for multi-hop systems. It may perform authentication tasks at multiple levels, including multi-party and bi-directional authentications. Since it may read the content of WS messages, and to authenticate their authors, XML firewall is the ultimate authorization mechanism: it may support loosely coupled authorization models and it may include sophisticated rules-based engines to express complex authorization logic.
- Between **t**he network firewalls of the WS endpoints and the WS network, Virtual Private Networks (VPNs) are implemented which have the primary responsibility for the integrity and confidentiality of data as it passes through the Internet. Network firewalls and their network layer security offer simple and effective transport-layer encryption for either temporary (using Secure Sockets Layer, SSL protocol), or persistent (using VPN mechanisms) point-to-point connections. To establish a VPN, considerable business and technical negotiations between the parties are required. But even then, only a part of the WS security challenges are solved: simple point-to-point links are used only by WS without intermediaries. Thus, network firewalls and VPNs can only play supporting roles for integrity, confidentiality and authentication. They can not provide end-to-end related security attributes in a multi-hop architecture. Moreover, network firewalls are intended to prevent access and to hide

systems, whereas WS require the exposition to the outside world of those very same systems. In WS, as the WS architecture layers indicate, the general goal is to move security out of the lower network and transport layers and into the upper message-oriented layers. This allows security concepts to be implemented independently of any particular network or transport protocol. Network- and transport-independent security is required for any message that will be routed over more than one protocol on the way to its final destination.

Figure 2 To be inserted here

There have been a number of initiatives that incorporate engineering applications to address the security and privacy concerns of WS. Many corporations and standards organizations are currently undertaking this task, having developed specifications and tools to address these concerns, but this effort is largely a work in progress, despite having started since the early days of the current decade. Promising approaches in this context, aim to enhance WS support for security and federation across trust domains. Brokering trust relationships among WS in various domains is essential when developing large, multi-organizational distributed systems. Respecting privacy and maintaining security through trust relationships among entities is essential for this interaction to occur (Van Dyke, 2004).

A WS indicates its requirements and other security related information in its policy document together with the privileges to be granted for the entities satisfying these requirements. If an access request arrives without having the required proof of claims, the service provider ignores or rejects the request. These claims are contained in security tokens. A security token is a representation of security-related information conveyed within the format of a SOAP message. If an issuer cryptographically endorses a security token, the token is called a signed security token. A security token service (STS) is a WS that issues security tokens, i.e. making assertions based on evidence that it trusts to whoever trusts it. To communicate trust, a security token service requires proof, such as a security token or a set of security tokens, and issues a new security token with its own trust statement. Another important related service is the attribute service. This is a WS that maintains attribute information about entities within a security domain (Wu and Weaver, 2006a).

With these services one entity can rely upon a second entity to execute a set of actions or to make a set of assertions about a set of subjects or scopes, called trust establishment. Trust relationships can be established by exchanging private attributes or bridging existing trust relationships. These techniques focus on owner control and utilizing extant trust relationships respectively.

To support the establishment of trust relationships, Wu and Weaver (2006b) proposed an indirect trust establishment mechanism to incorporate owner control into the process of bridging extant trust relationships.

The proposed indirect trust establishment mechanism uses a common third party as the anchor to bridge two extant trust relationships. An extant trust relationship is represented as a trust group element which includes a trust relationship name, a list of participants involved in this relationship, and a list of privileges granted for that relationship. This trust relationship can be established via an on-line trust negotiation or a written contract. In the bridging protocol, the common third party needs to discover any difference in privileges granted to the two participants in order to provide the two participants equal standing and the opportunity to make their own subjective decisions for the new trust relationship.

Interesting research proposals claim for the integration of trust negotiation techniques with Semantic Web technologies, such as semantic annotations and rule-oriented access control policies (Gavriloaie et al, 2004). In this approach, the resource under the control of the access control policy is an item on the

Semantic Web, with its salient properties represented as RDF properties. RDF metadata, managed as facts in logic programming, are associated with a resource and are used to determine which policies are applicable to the resource. In a service-oriented environment, the semantic layer ensures that data embedded within messages are interpreted by providers and consumers as representing the same concepts, relations, or entities in a suitable abstraction of the real world. Semantic Web concepts are about how participants can interpret descriptions and data items in the system with respect to some ontology of the business domain and how this interpretation can be shared and made transparent throughout the infrastructure. In fact, the semantic layer covers objects, events, states, and anything else that can be conceived, expressed, and exchanged over a communication network (Vetere and Lenzerini, 2005).

The characteristics of the open Web environment, where interacting subjects are mostly unknown to each other, has led undoubtedly to the development of the trust negotiation approach as a suitable access control model for this environment (Yu et al, 2003). Trust negotiation itself has been extended with adaptive access control, in order to adapt the system to dynamically changing security conditions (Ryutov et al, 2005). When extending a WS with negotiation capabilities, the invocation of a WS has to be managed as the last step of a conversation between the client and the WS itself. The rules for such a conversation are defined by the negotiation protocol. Several models already proposed for peer-to-peer negotiations assume that both parties are equipped with the same negotiation engine that implements the mutually understood negotiation protocol. This assumption, however, might not be realistic and may prevent the wide adoption of negotiation-enhanced access control models and mechanisms. To fill this gap, research efforts (such as the proposed model Ws-AC1 by Bertino et al (2006)), focus on proposing a WS access control model and an associated negotiation protocol based on a declarative and highly expressive access control policy language. Such a language allows one to specify authorizations containing conditions and constraints not only against the WS parameters but also against the identity attributes of the party requesting the service.

4. Web Services in the rural areas - Applications and Security

The authors' previous work on WS comprises efforts at proposing and validating a WS evaluation framework (Georgiadis and Pimenidis, 2006, 2007). The main focus of that framework has been on two categories of criteria those of technical and those of user-oriented as summarized below:

Technical Criteria:

- Interoperability
- Quality
- Security

User-Oriented Criteria:

- User Trust
- User Loyalty (Georgiadis and Pimenidis, 2008)

It is the authors' view that this set of criteria can be applied across a wide range of WS with equal success rates, irrespective of the application or the intended audience. In their efforts to assess the suitability of the above criteria the authors reviewed a variety of WS and were particularly intrigued by the WS that are available to people in the rural areas.

In considering rural areas, a number of problems exist related to economic, ecological, and social aspects with effects to rural development and environmental conservation. The disparity of services and fragmentation of information often causes major obstacles in completing transactions and business deals effectively.

The forest industry for example faces a number of malfunctions and marketing problems mostly because of the lack of quality, lack of speed in public service provision, and service provision in terms of the needs of the residents of rural areas at a low cost rate. Furthermore service requesters in rural areas face various difficulties in searching for market participants. Other sources of difficulty are due to the insufficient

transfer of information concerning new markets, market requirements, and demand and movement within local and export markets; the lack of specialized, certified and quality education material such as production methods, new business practices; and certainly to the remoteness and isolation of forested areas (Costopoulou and Tambouris, 2004).

Forest-related information is scattered across numerous databases, Web sites and portals at different locations and systems. Finding relevant and accurate information is often time-consuming and requires access to multiple systems. As a consequence, forest stakeholders lose a lot of productive time. In order to handle these limitations, the innovative WS-based technologies can be used. Using the open standards of WS makes the development of composite services possible - either via service orchestration, or via service choreography. These value-added services may actually integrate a number of services that can be dynamically changed, in order to correspond to complex situations or business scenarios. Such cases could be those that involve companies and self-employed individuals in rural areas and call upon public services and / or initiate interactions with public authorities.

Noting the above issues the authors researched the status of WS targeting exclusively or primarily individuals and businesses in rural areas. The aim of this work is to identify the level of security provision, while maintaining simplicity of access and developing trust. A further objective is to assess the suitability of the indirect trust establishment mechanism proposed by Wu and Weaver (2006b) and how this could influence the author's work on the WS evaluation framework. This particular phase of the research involved WS available in the United Kingdom and comprised the thorough examination and review of more than one hundred WS available to residents of rural areas primarily. Most of the WS offered were targeting individuals; while there have been a small number that were related to local business needs.

In categorizing these WS one can classify them as:

- Transactional WS – involving commercial or other forms of transactions where exchanges of goods or information take place through the WS.
- Social Interaction
- Information Provision

The above categorization is not a standardized one, but one that closely reflects the different grouping of services encountered. WS are commonly classified as REST, RPC and Hybrid based on the underlying technology utilized, e.g. HTTP, SOAP or XML and a combination. The classification adopted here though aims to identify the use of these services as under the continuously evolving semantic web architecture emphasis will be given on the descriptions of the services as these will provide a means of semantic analyzing them and consequently lead to different formats of classifications based on Heuristics (Corella et al, 2006).

The challenges to the coordinators of all these WS are essentially those reflected by the user-oriented criteria as reflected in the authors' previous work (Motahari-Nezhad et al, 2006, Tang et al 2006, Georgiadis and Pimenidis, 2008): User Trust and User Loyalty. To meet those criteria, providers have to ensure that they offer users maximum security through their transactions, while at the same time ensuring that the process is not compromised by complexity of the application. This is essential in the rural areas in particular where there is a higher impact of the Digital Divide across the society compared to urban populations (Bolissian et al, 2006).

The research shows that most WS providers opted for an one-stop registration / sign-in security feature, even in cases where the user was receiving simple information such as the weather report for farmers or flood warning information (a common phenomenon in rural England). The one stop sign-in process maintains the complexity of access to a minimum while it maintains the sense of trust and inclusiveness, elements which are essential in small societies. It also provides a security and trust mechanism across the WS which is transparent to the WS user who might be a casual and hence untrained ICT user.

More than 90% of providers aimed at such a security feature, although the WS composition hardly involved

more than three services providers in most cases as seen from the diagrams in figure 3 below. For the purposes of the authors' research these findings are encouraging as they are compatible with the proposed framework and appear to support their view for its wide applicability. Furthermore the examples studied mostly involved in the WS provision either local services / business or large mainly public / state controlled organizations. In both cases trust can be either easily cultivated and /or verified, or is inherent due to the status of the organization involved.

Figure 3 To be inserted here

Figure 4 To be inserted here

In the case of local provision the indirect trust provision mechanism proposed by Wu and Weaver (2006b) appears excessive and redundant. This proposes the use of WS enhancements that provide additional functionalities for security, privacy and many other purposes. WS enhancements are a series of specifications describing security, privacy and other contexts applied to WS by several industrial practitioners. The above authors describe an indirect trust establishment mechanism using WS enhancements for bridging extant trust relationships to produce a new one. This is based on the exchange of privileges obtained from a common third party (who has established trust relationships with both participants) and thus avoids disclosure of any private attributes. Meanwhile this mechanism still allows free negotiation and trust agreement selection between the involved participants when subjective judgments have to be made. Such an approach could be considered extremely useful though for the purposes of involving large organizations at national level that would need the above provision to interact with and support WS at local level as these would be in a multitude, largely unknown and often exhibiting infrequent interaction patterns. Thus the above mechanism could be considered as an element in the authors' work on a WS evaluation framework.

Further data relating the provision of WS in the rural areas surveyed has revealed the reasons / concerns of WS providers with respect to investing in sophisticated security systems to safeguard their WS provision and to gain the trust of their clients. Figure 5 provides a graphical representation of the above data showing the three main reasons that WS providers are cautious if not reluctant to provide advanced security features with their WS provision. Although performance appears to be a key concern, cost of development and operation (third party services) appear to be the more decisive factors.

Figure 5 To be inserted here

This focus on costs can be primarily attributed to the fact that most of these services are offered on a local basis servicing the needs of relatively small local communities. The potential source of income is further limited by the reluctance of such communities to pay for such services or even the expectation that such services should be offered for free. Thus provides of WS often rely on income from advertising which given the size of the target groups is rather low. Such approach by the public is not unexpected as it is a key characteristic of a society that is rich and overloaded in information, hence the perceived value of information is rather low (Bolissian et al, 2006). On the contrary in more information deprived societies where the digital divide's impact has a heavy bearing, people are more willing and able to pay for them to offset the much higher costs of poor transportation, unfair pricing, and corruption (Pentland et al, 2004, Parikh, 2005).

A final graph showing the demographics of usage of the WS discussed here is presented in figure 6 below. The graph shows percentage of users per age groups of the different types of services offered. It is clear that the more "vulnerable" groups of users (13-24 and more than 55 years old) have considerably less use of transactional WS. This is usually attributed to users in those groups being less prone to perform transactions due to limited funds (younger group) or being more cautious in their approach towards online transactions due to lack of trust (55+ group). In contrast to this the younger generations of users appear to make extensive use of social WS (80% of users 13-24 year olds) and it is these services that are more critical to privacy and trust as they are the ones to which personal details are exposed. Combined with the results of figure 4, it appears that market reasons are possibly forcing WS providers to undercut investment on security systems in services that are primarily targeting vulnerable sectors of the society.

Figure 6 To be inserted here

As the issue of trust evolves as a major challenge in personal as well national security, it is reasonable to suggest that for the case of WS the type of service offered would be a critical factor in assessing and evaluating the various provisions. Thus the authors' previous work on evaluating WS could be expanded to consider the type of service in special cases where offerings to rural communities are assessed.

To verify this further work on WS in rural areas in other countries such as Greece and Australia is under way. Analysis of the participating service providers and the different groups of people that access and use the WS regularly is required. Comparison between different societies, different markets and different target audiences (urban versus rural areas) could further shed more light into the potential of expansion and further refinement of the authors' previous work. Furthermore the study of societies and services offered to them in rural areas of poor and developing countries could allow for further refinement of the results. These combined with the issues of the potential of the semantic web could help establish new standards of requirements on WS as the trade off between security, interoperability and performance will no longer be an issue, but the requirements for trust and security would remain unaltered.

5. Conclusions

WS are the modern means of conducting business and providing services online. Their instantaneous nature of formation is the driving feature of success but at the same time the one introducing most challenges to developers and providers alike. User participation is closely related to user trust and loyalty. Providing a security driven WS is a key feature in attaining trust and maintaining loyalty. Different

approaches in cultivating trust are being proposed. At the same time security mechanisms aim at minimizing the burden on performance and usability. The challenge remains in improving the WS provision without compromising security. This is particularly important in rural areas where the effort to simplify access to the WS could lead to compromises in security; a feud that affects even areas and groups where the communities are considered 'technologically savvy'. The research discussed in this paper shows that in rural areas of the United Kingdom, usage of Web Services is widely spread across different age groups, with informational web services dominating the preferences and social web services mostly attracting the attention of younger generations. A further finding of this work suggests that despite the need for enhanced security features, many providers of web services targeting populations in rural areas find difficulty in continuously keeping up with improvements in security features of their services. This is largely attributed to concerns about escalating costs, while there is also skepticism as to the effects that more complex security features might have on the performance of the services. This research is ongoing and aims at establishing a framework for evaluating WS irrespective of application domain or target audience. The particular challenges in providing financially viable WS to rural communities depend on the level of security achieved, without that burdening the providers, or being a deterrent to the casual user. The level of security supported by the WS provider would be the main feature in evaluating WS in a fully semantic web.

6. References

Bertino, E., Squicciarini A.C., Martino L., Paci F. 2006. An Adaptive Access Control Model for Web Services. International Journal of Web Services Research, Volume 3, Issue 3, 27-60.

Bichler, M., Lin, K-J. 2006. Service-Oriented Computing. IEEE Computer, Vol. 39, issue 3, 99-101.

Birukou A., Blanzieri E., D'Andrea V., Giorgini P., Kokash N., 2007. Improving Web Service Discovery with Usage Data. IEEE Software, Vol. 24, issue 6, 47-54.

Bolissian J., Pimendis E., liadis L., Andreopoulou Z. 2006. E-Readiness or Digital Exclusion – Evaluating a Country's Status. In: Proceedings of the 2nd E-Democracy National Conference with International Participation, Athens Bar Association and the Scientific Council for the Information Society, Athens, Greece, pp. 87-96.

Booth, D., Haas, H., McCabe, F., Newcomer, E., Champion, M., Ferris, C., Orchard, D. 2004. Web Services Architecture, W3C Working Group Note 11, February, W3C Technical Reports and Publications, http://www.w3.org/TR/ws-arch/.

Casola V., Fasolino A. R., Mazzocca N., P. Tramontana P. 2007. A policy-based evaluation framework for Quality and Security in Service Oriented Architectures. In: Proceedings of the IEEE International Conference on Web Services ICWS 2007, Salt Lake City, Utah, USA, pp. 1181-1190.

Chen S., Yan B., Zic J., Liu R., Ng A. 2006. Evaluation and Modeling of Web Services Performance. In: Proceedings of the IEEE International Conference on Web Services ICWS 2006, Chicago, Illinois, USA, pp. 437-444.

Chen S., Zic J., Tang K., Levy D. 2007. Performance Evaluation and Modeling of Web Services Security. In: Proceedings of the IEEE International Conference on Web Services ICWS 2007, Salt Lake City, Utah, USA, pp. 431-438.

Corella M.A., Castells P. 2006. A Heuristic Approach to Semantic Web Services Classification. In: Knowledge-Based Intelligent Information and Engineering Systems, Proceedings of the10th International Conference, KES 2006, Bournemouth, UK, Proceedings, Part III, Lecture Notes in Computer Science, Vol. 4253/2006, pp. 598-605.

Costopoulou C.I., Tambouris E. 2004. One-stop eServices for the forest sector. Information Services & Use 24, 135–145.

Curbera, F., Khalaf, R., Mukhi, N., Tai, S, Weerawarana, S. 2003. The Next Step in Web Services. Communications of the ACM, Vol. 46, No. 10, 29–34.

Gavriloaie, R., Nejdl, W., Olmedilla, D., Seamons, K.E., Winslett, M. 2004. No registration needed: How to use declarative policies and negotiation to access sensitive resources on the Semantic Web. In: Proceedings of the 1st European Semantic Web Symposium, Heraklion, Greece, 342-356.

Georgiadis C.K., Pimenidis E. 2006. Web Services Enabling Virtual Enterprise Transactions. In: Proceedings of the IADIS International Conference on E-Commerce, Barcelona, Spain. pp. 297-302.

Georgiadis C.K., Pimenidis E. 2007. Proposing an Evaluation Framework for B2B Web Services-based Transactions. In: Proceedings of the E-Activity and Leading Technologies conference, IASK, Porto, Portugal, pp. 164-171.

Georgiadis C.K., Pimenidis E. 2008. Service-enabled Business Processes: Constructing Enterprise Applications – An Evaluation Framework. In: Sobh T. (Ed) Advances and Innovations in Systems, Computing Sciences and Software Engineering, Springer, pp. 125-130.

Gortmaker, J., Janssen, M., Wagenaar, R.W., 2004. The Advantages of Web Service Orchestration in Perspective. In: Proceedings of the ICEC'04, Sixth International Conference on Electronic Commerce, ACM, pp. 506-515.

Haley C.B., Laney R.C., Moffett J.D., Nuseibeh B. 2004. The Effect of Trust Assumptions on the Elaboration of Security Requirements. In: Proceedings of the 12th IEEE International Requirements Engineering Conference (RE'04), Kyoto, Japan, pp. 102-111.

Kaye, D., 2003. Loosely Coupled: The Missing Pieces of Web Services. RDS Press, Marin County, California, USA.

Little, M., 2007. WS-CAF: Contexts, Coordination and Transactions for Web Services. In: R. Meersman and Z. Tari et al. (Eds.): OTM 2007, Part I, LNCS 4803, pp. 439–453.

Martin D., 2006. Putting Web Services in Context, Electronic Notes in Theoretical Computer Science 146 (2006), 3–16.

Motahari-Nezhad H.R., Benatallah B., Casati F., Toumani F. 2006. Web Services Interoperability Specifications, IEEE Computer, Vol. 39, No. 5, 24-32.

Parikh T.S., 2005. Using Mobile Phones for Secure, Distributed Document Processing in the Developing World. IEEE Pervasive Computing, Vol. 4, No. 2, 74-81.

Pentland A, Fletcher R, Hasson A. 2004. DakNet: Rethinking Connectivity in Developing Nations, IEEE Computer, Vol. 37, No 1, 78-83.

Ryutov, T., Zhou, L., Neuman, C., Leithead, T., Seamons, K.E. 2005. Adaptive trust negotiation and access control. In: Proceedings of the ACM Symposium on Access Control Models and Technologies (SACMAT 2005), Stockholm, Sweden, pp.139-146.

Tang K., Chen S., Levy D., Zic J., Yan B. 2006. A Performance Evaluation of Web Services Security. In: Proceedings of the 10th IEEE International Enterprise Distributed Object Computing Conference EDOC'06, Honk Kong, China, pp. 67-74.

Van Dyke, J.W., 2004. Establishing Federated Trust Networks among Web Services. B.Sc. Thesis, University of Virginia, USA.

Vetere, L., Lenzerini, M. 2005. Models for semantic interoperability in service-oriented architectures. IBM Systems Journal, Vol. 44, No 4, 887-903.
Weerawarana, S., Curbera, F., Leymann, F., Storey, T., Ferguson, D. 2006. Web Services Platform Architecture. Prentice Hall, Upper Saddle River, New Jersey, USA.

Wu, Z., Weaver, A.C. 2006a. Using Web Service Enhancements to Bridge Business Trust Relationships. In: Proceedings of the Fourth International Conference on Privacy, Security, and Trust: Bridge the Gap Between PST Technologies and Business Services (PST'06), University of Toronto, Institute of Technology, Markham, Ontario, Canada.

Wu, Z., Weaver, A. C. 2006b. Bridging Trust Relationships with Web Service Enhancements. In: Proceedings of the 2006 IEEE International Conference on Web Services ICWS 2006, Chicago, Illinois, USA, pp. 163-169.

Yu, T., Winslett, M., Seamons, K. 2003. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation. ACM Transactions on Information and System Security, 6(1), 1-42.

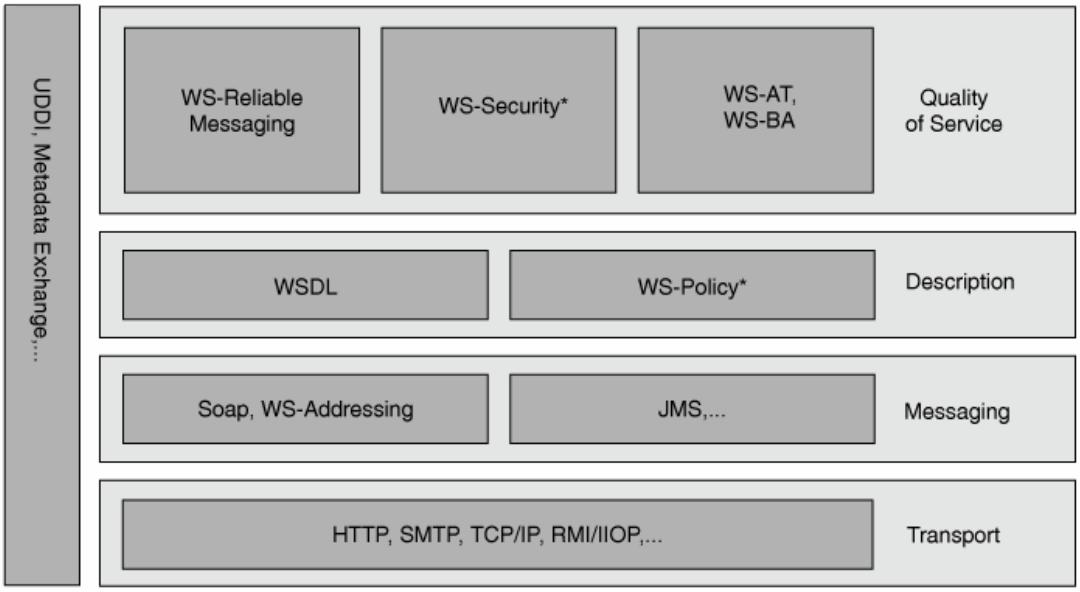

Figure 1 Web Service Architecture (Weerawarana et al 2006)

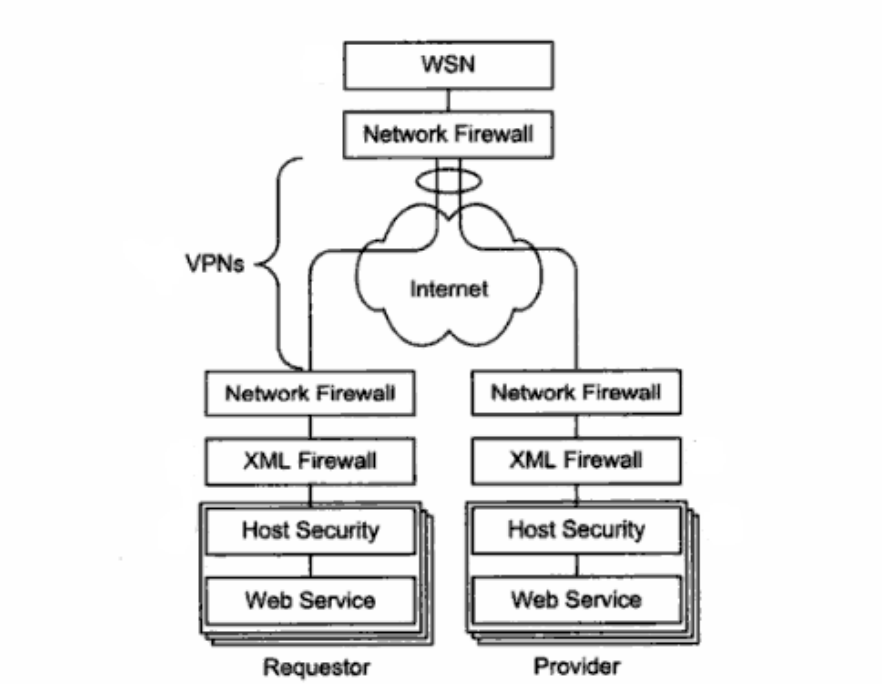

Figure 2 Distributing the Responsibilities of Security Platforms (Kaye, 2003)

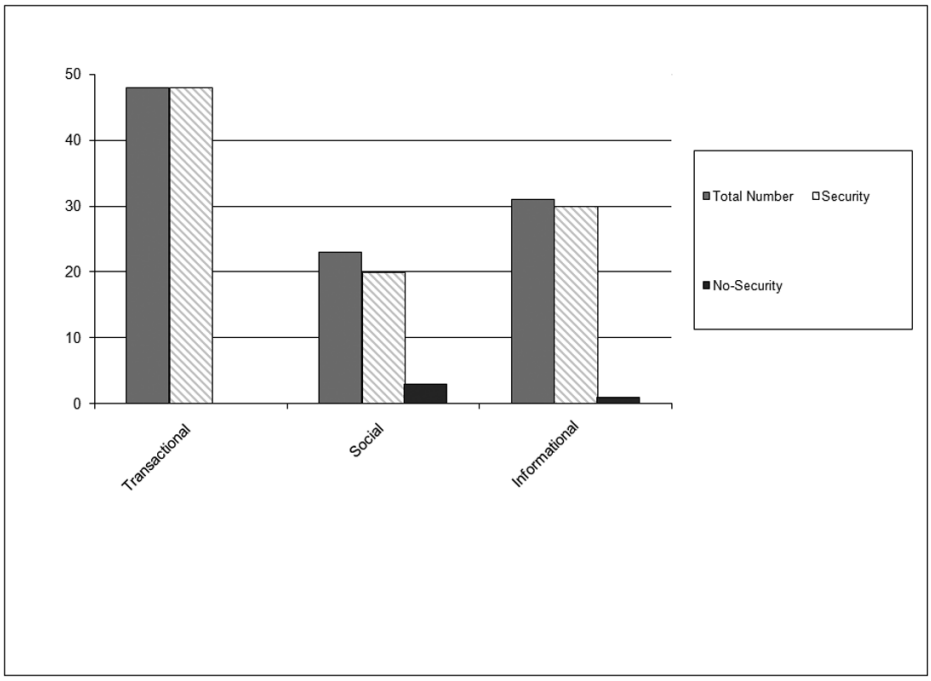

Figure 3 Types of Web Services and Security Provision

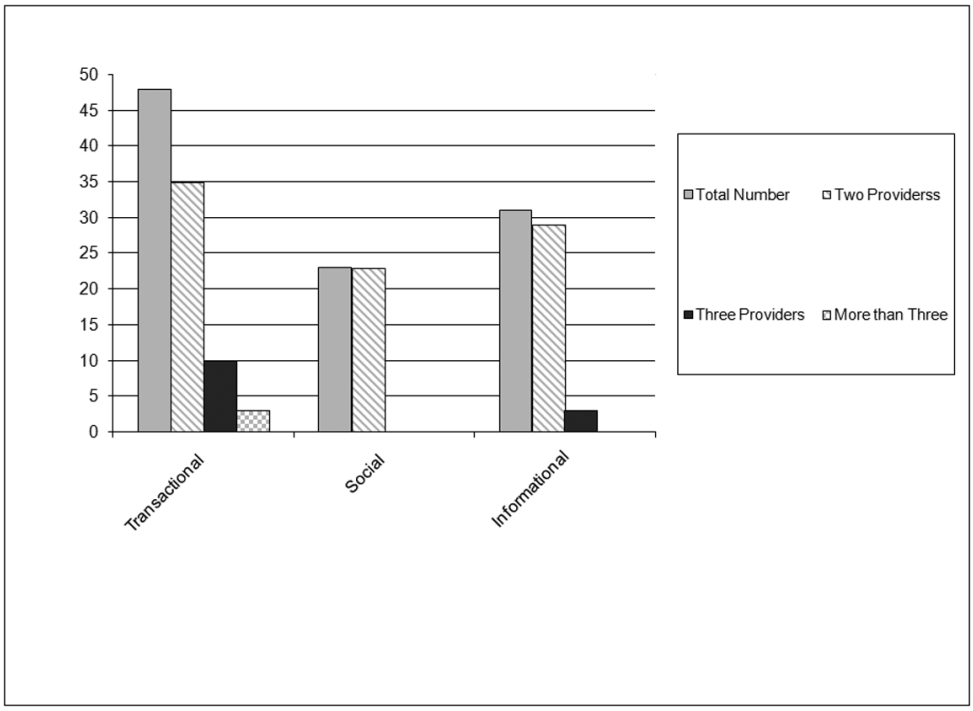

Figure 4 Numbers of Participants in WS Provision

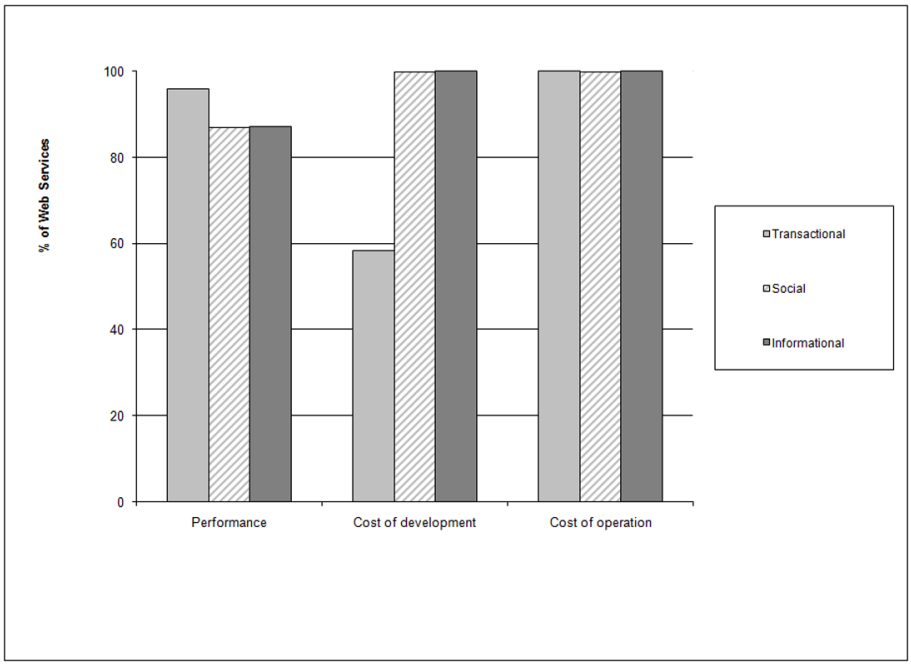

Figure 5 Reasons for lack of continuous of investment in Security systems

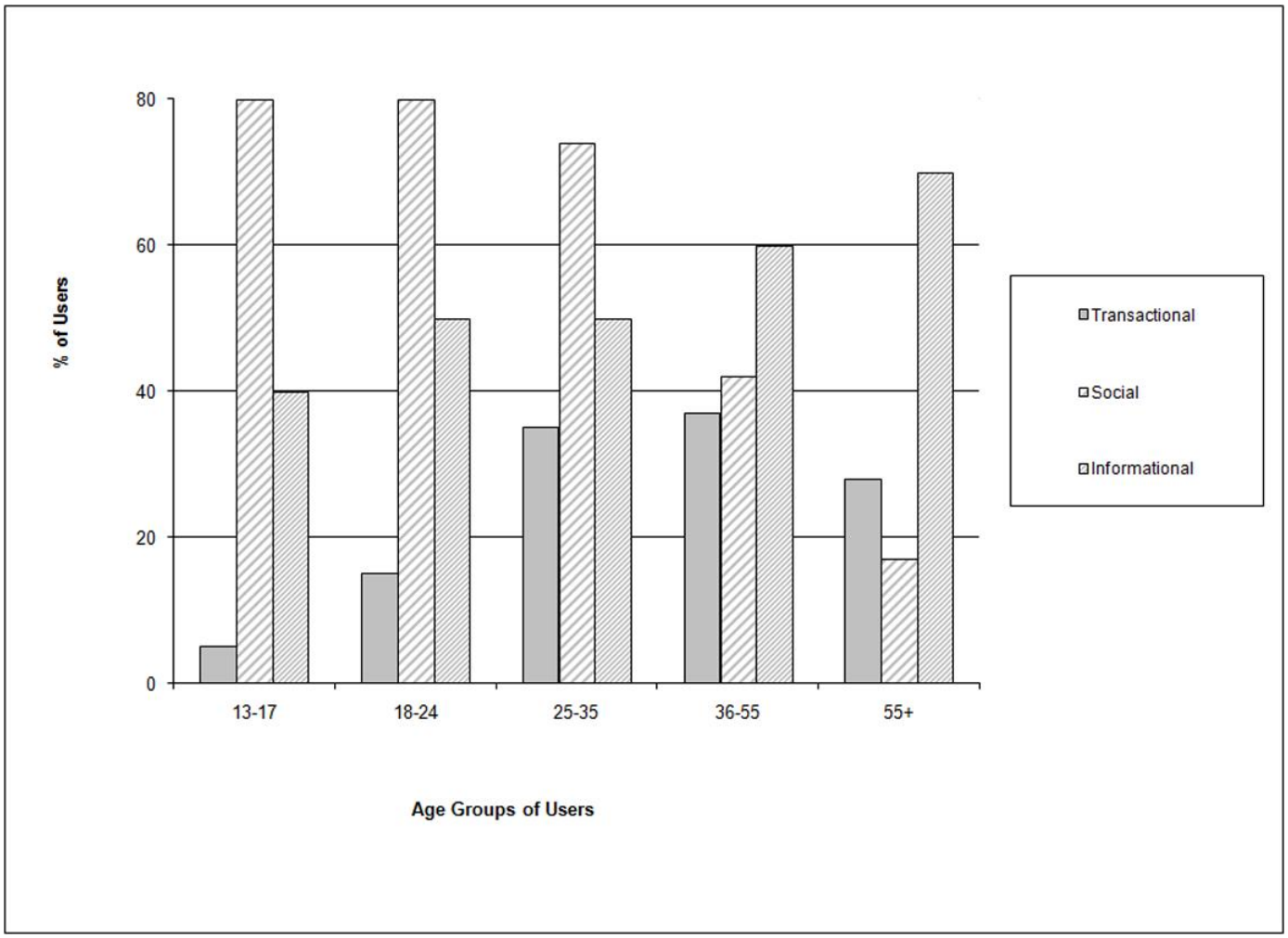

Figure 6 Demographics of use of Web Services in Rural Areas