



www.cybersecurity-ktn.com

Cyber Security KTN Initial Fact-Finding Document SOA security stakeholder concerns analysis

Dr. Ulrich Lang, Rudolf Schreiner
ObjectSecurity Ltd.
ktn-feedback@objectsecurity.com

Service Oriented Architecture (SOA) as an approach (or buzzword?) promises unprecedented IT flexibility and reuse. However, so far there is a lot of confusion about what SOA actually means in business and technical terms (“Same Old Architecture?”) and what it is good for (“SOA what?” like in “so what?”), what the technical and business show-stoppers are, what the best adoption roadmap is etc.

Unclear security implications are often high on the list of issues raised that slow down SOA rollouts. There are many reasons for the (real and perceived) security and assurance problems of SOA, including immaturity of security standards and technologies, unpredictability and unmanageability etc. Defence faces particular SOA security challenges because traditional assurance accreditation standards (e.g. Common Criteria accreditation of complete systems) cannot easily be used to accredit SOA assurance.

Just like the numerous SOA definitions, there are numerous SOA security concerns that may differ for each stakeholder in the “SOA puzzle”: industry, government, vendors, security experts, consultants, analysts etc. There is also an abundance of literature, most of it biased towards specific aspects, stakeholders, approaches, products etc. Concerns can be about business case, technology, governance, accreditation, deployment, return-on-investment, future-proofing, hype vs. reality etc.

The purpose of this project is to produce a level of common understanding about the main SOA security concerns. The final report will summarise the security concerns of both the end-user side (i.e. organisations that try to use SOA) and the vendor/provider side (i.e. SOA integrators, vendors, universities/educators, consultancies etc.). The final report is intended as a vendor-independent public resource that reflects a broad range of concerns from all involved stakeholders. It is intended to provide a broad understanding about the main SOA security concerns that will help all stakeholders come closer to SOA roll-outs, products and education that include appropriate security.

Please look at the project wiki

www.secure-soa.info

(contributions highly encouraged)

1 SOA

Service Oriented Architecture (SOA) as a buzzword promises unprecedented IT flexibility and reuse. However, so far there is a lot of confusion about what SOA actually means in business and technical terms and what it is good for, what the technical and business show-stoppers are, what the best adoption roadmap is etc. While actual SOA implementations in many organisations today still seem to be early stages, the view is often voiced that “doing nothing” is probably more expensive than “doing something”. While a recent Gartner CIO survey showed “SOA” only as #10 top priority, the same survey showed several potential SOA business benefits higher up on the list. This could potentially be interpreted as “SOA fatigue”.

1.1 SOA definitions

SOA in general means different things to different people. Some vendors market SOA as a mere technology solution based on XML web services based applications (ridiculed as “Same Old Architecture” by others). Others again advocate SOA as an IT architectural style that can range from a simple portal-based web service solution, over loosely coupled interacting web services, to a full-fledged Business Process Model (BPM) driven, orchestrated agile IT environment (with the downside of high complexity). Others again consider SOA mainly a business-led style of “bringing IT back to the business” where the goal is to give the business more control over the IT resources needed to do their business. Other sources (mostly advocacy groups) take a purely business-driven view of IT transformation that is based on business benefits and return-on-investment. Various industry consortia now also provide their definitions and reference models (e.g. the OASIS SOA Reference Model).

Other exemplary definitions found on the internet include¹

- A system for linking resources on demand. In an SOA, resources are made available to other participants in the network as independent services ...
- A SOA defines how two or more entities interact in such a way as to enable one entity to perform a unit of work on behalf of another entity. The unit of work is referred to as a service, and the service interactions are defined using a well-defined description language. ...
- A software design that integrates business functions. Users are able to decide the information which is to be shared between the functions. SOA is therefore more flexible and more loosely coupled than ERP and generally more suitable for service rather than manufacturing companies.
- A paradigm for design, development, deployment and management of a loosely coupled business application infrastructure. ...
- An architecture, the aim of which is to achieve a loose connection between integrated systems. From a common public Danish perspective, the integration of IT systems across public and private organisations is part of the vision of digital administration.
- Essentially a collection of services. These services communicate with one another. The communication can involve either simple data passing or it can involve two or more services coordinating some activity. ...
- An approach to enable better software reuse. Instead of all applications implementing the same business functionality over and over again, for example credit card checks or payments, such functionality is implemented as service and then used by other business processes implementations and services.

SOA seems to have been originally based on the concept of a service in a strict sense. One component provides a service, another component uses this services. This is done as invocations on remote interfaces and implemented, i.e.

¹ http://www.google.com/search?hl=en&rls=com.microsoft:en-US&defl=en&q=define:SOA&sa=X&oi=glossary_definition&ct=title

with Web Services, J2EE or CORBA. Unfortunately, it became very common to call data centric, network centric or message driven systems service oriented as well. The relationship between the terms “service” and “process” is also not well defined. While these unclear terminologies produce a lot of confusion, it turns out that SOA even in the strict sense of synchronous service invocations and the other non-invocation based technologies share the same main security problems, e.g. the necessity to deal with complex, agile and flexible systems. This is caused by the high level of distribution of the systems and complex interactions of components, compared to client/server or 3-tier architectures. The actual communication patterns and technologies play a minor role.

As a first basis for discussion, this document attempts to provisionally structure the different aspects of Service Oriented Architecture (SOA) as follows.

1.2 Business benefits

It is obvious that SOA will only be adopted if it either has clear business benefits. Aspects related to business benefits include:

- **Agility, cost-saving:**
the IT environment can respond quicker and cheaper to organisational changes, for example new markets, services and products.
- **Cost-saving/ROI:**
running legacy IT systems (i.e. investments) can be reused as services and enabled for integrated IT solutions that support the business better
- **“Future-proofness”/ROI:**
business invests in a general architecture that allows future IT to be integrated into the existing fabric without disruptive costs
- **Reusability/ROI:**
The same functionality is implemented once as a service and then reused in other applications.
- **Business-led ownership, aligned business and IT:**
IT architecture is a business concern, rather than a siloed IT department concern. Investments, benefits (and mistakes!) are therefore clearly justifiable to the business. Business Process Management (BPM) driven SOA is an example of a big (maybe too ambitious?) vision of connecting the business and IT in a structured way.

1.3 Technical benefits

It is also possible to justify SOA from technical benefits, e.g. integrators can deploy SOA without the customer’s specific commitment in order to provide the best or most cost-effective solution to the end-customer. Some technology benefits include:

- **Reduced complexity:**
Wrapping all systems into consistent, standardised service² interfaces (e.g. XML) with interface definitions in standardised registries/repositories (e.g. WSDL/UDDI based) and standard protocols potentially helps the IT department to deal with the complexity of today’s ever-growing interconnected IT environments.
- **Easier changes:**
Consistent interfaces and protocols can simplify reconfiguration and adaptation to changing requirements

² Looking at the IT world in terms of services can be seen as a relatively arbitrary design decision which probably comes from previous object/component-oriented middleware approaches. One could also look at the IT world purely data-centric or process-centric.

- Easier reuse and integration of new systems:
Consistent interfaces and protocols can also help with this.
- Consolidated view:
If tied into a business-driven architecture (e.g. BPM SOA), a consolidated architectural view can potentially be achieved, which will support the other benefits.

1.4 Pick & choose?

A SOA definition could “pick & choose” some or all of the following features:

- IT services with standards-based interfaces (potentially XML based)
- standard protocols for communications (potentially XML based)
- standards-based registries/repositories store service information (e.g. location, interface etc.), potentially using UDDI/WSDL XML standards
- Support for flexible on-the-fly service orchestration, e.g. using BPEL
- Support for model-driven specification of information models, service models and business processes, and other functional and non-functional (e.g. security) business and IT environment aspects, e.g. using BPM/BPMN/UML

The KTN and wider community are encouraged to provide further examples of non-security SOA business benefits.

2 SOA security

Unclear security implications are often cited high on the list of issues raised that slow down SOA adoption or limit the benefits of SOA. For example, Aberdeen Group's March 07 benchmark report "Management and Governance: Planning for an Optimized Application Lifecycle" identified the establishment of operational security, governance, and management as the top challenge (44%) in managing an SOA lifecycle. The fact that security issues are different from older IT came second (39%).

There are many reasons for the (real and perceived) security and assurance problems of SOA, including immaturity of security standards and technologies, unpredictability and unmanageability, hard to carry out traditional assurance accreditation (e.g. Common Criteria) etc.

2.1 SOA security concepts

Just like the numerous SOA definitions, there are numerous SOA security concerns that may differ for each stakeholder in the "SOA puzzle": industry, government, vendors, security experts, consultants, analysts etc. There is also an abundance of literature, most of it biased towards specific aspects, stakeholders, approaches, products etc. Concerns can be about business case, technology, governance, accreditation, deployment, return-on-investment, future-proofing, hype vs. reality etc.

From an abstract perspective, the basic SOA security requirements do not seem to differ much from those of other IT environments:

- Confidentiality, integrity:
Information usage, storage, and transmission, as well as access to IT resources, may need to be governed
- Availability:
Availability of the IT resources to the business may be desirable or necessary
- Accountability:
Usage of resources and information may need to be governed e.g. to demonstrate regulatory compliance
- Manageability:
IT security should be manageable without undue complexity/cost, which can be hard in large, unstructured, heterogeneous IT environments

2.2 SOA security complexities

However, SOA may introduce (or make evident) a number of additional complexities related to security, including:

- Heterogeneity:
Security in large IT environments may mean that many different security technologies have to be deployed to meet specific requirements. These security technologies also might have to protect different middleware platforms.
- Multi layer protection:
The assets have to be protected as various layers and at different places. For example, to enforce the confidentiality of data it might be necessary to use file access control, encryption of backup files, database access control, middleware layer access control, transport layer encryption and IP filtering.
- Agile security:
Security is harder in agile/changing IT environments such as agile SOA. Mechanisms and policies need to be constantly kept coherent with the actual high level security policies, and operational and functional requirements. This makes a protection and also accreditation of complete applications a great challenge, because there are no static systems anymore.

- **Opened-up information sources:**
In SOA, many previously siloed (and thus easier-to-secure) information resources are typically made available on the network as service to enable SOA integration, instead of monolithic applications; this move has obvious significant security implications because a much better, more fine-grained level of security may be required and the protection cannot be implemented in the application itself anymore.
- **High complexity of interactions:**
Single business process are not implemented as monolithic applications anymore, but as complex interactions of many services. This greatly increases the complexity of protection and the related security policies. A single action of a user now results in sequences of service interactions, which all have to be protected based on fine grained security policies and context information. Human administrators are normally not able to define security policies with sufficient correctness and assurance.
- **Manageability:**
Security policies typically get large, complex, unwieldy, and frequently changing. SOA security needs to have good security policy management support designed in from the beginning to ensure cost-effectiveness and trustworthiness into the security. This includes unified and automatic policy updates to keep to enforce a consistent security policy and a central notification of relevant events.
- **Security architecture:**
In more “evolved” versions of SOA, the security architecture needs to be aligned with business security requirements (e.g. business processes) to make sure all stakeholders are “on the same page” with respect to their security requirements.
- **Technology driven security:**
Today, security is looked at from a technology driven perspective, in terms of firewall and cryptography. It is necessary to “bring security to the business level”, to think in terms of services, resources and high level security intent.
- **Who is responsible for security?**
In most enterprises, the responsibility for security is scattered to different departments, e.g. the networking department runs firewalls and VPNs, the application developers implement application level security and so on.
- **Security standards and technologies are in a flux:**
A particular complexity of SOA security is that “vendors and committees have thrown a bewildering plethora of immature or incompatible security specs and solutions at us”³. There are numerous SOA/XML related consortia that all standardise overlapping specifications. There is little overarching architecture and/or harmonisation. This results in significant SOA security roll-out complexity.
- **Insufficient security infrastructures:**
In the past, organisations made considerable investments into security infrastructures like identity management. These infrastructures might not meet the requirements of SOA anymore.
- **Regulatory requirements:**
Business applications have to meet specific regulatory requirements. In monolithic applications, the security requirements derived from these regulatory requirements were hard coded. This is not possible anymore.
- **Separation of concerns:**
In monolithic systems, the enforcement of complex security policies was mostly hard coded. In SOA based systems, it is not possible to hard code security enforcement anymore, since this would be an obstacle to service reuse. Now a separation of concerns is required, the service implements pure business functionality, and complex security policies now have to be enforced in a different way. Using standard security systems like identity management, this might be difficult to impossible.

³ <http://blogs.zdnet.com/service-oriented/?p=925>

- Cross domain issues:
SOA applications can span multiple organisations which normally do not fully trust each other. Also, organisations will provide services for other organisations, like in the grid vision. This leads to many additional regulatory and security issues.
- Availability of human resources:
Is sufficiently skilled personnel available? This is esp. doubtful because in the past not even much more simple systems were sufficiently protected.
- How is SOA security related to overall enterprise security?
Does SOA security require specific security architectures and systems? Or can SOA security be well embedded into overall enterprise wide security. For example, is a single security architecture able to support SOA and also data driven, message driven and event driven architectures as well?
- Integration with Intrusion Detection Systems (IDS):
With the introduction of SOA, the traffic both on internal networks and gateways to the outside world is becoming much more complex. This greatly complicates the use of network based Intrusion Detection Systems, because it is now much harder to separate suspicious from legitimate traffic.

2.3 What are really the main SOA security concerns?

This question forms the central part of the discussion (workshops, document feedback, wiki etc.). One main purpose of this project is to ensure that the wider community has more of an understanding of the real SOA security concerns. The KTN and wider community are highly encouraged to provide further examples of SOA security aspects.

Concerns that need to be answered include:

- It is clear that SOA security is a relevant problem – but are we asking the right questions?
- Is SOA security really perceived as a show-stopper?
- Why is SOA security difficult or perceived as difficult?
- What approaches and solutions are out there?
- Who is to be responsible for security of SOA applications?
- Does SOA security require specific training and education?
- Where is SOA security today? Does it meet end-user requirements?
- Where will SOA security be in 1, 2, 5, 10 years? Will SOA still be around? Will it deliver?
- Does SOA security fit into the future trends and developments in security? Can it be reused for data centric or message oriented systems as well, or does it require specific security architectures?
- Where are the standards going? Will they consolidate, or will there be a “next best thing” instead?
- How can we document, demonstrate, or even prove that the SOA is secure, especially if it is rapidly changing (e.g. Common Criteria)?
- How can SOA security be governed well (within an overall SOA governance approach)

The SOA security concerns identified in this initial document will be used as a basis for an ongoing online survey located at www.secure-soa.info. The findings from the survey will be used as input for the final document.

3 Document and project overview

3.1 Planned project purpose

The purpose of this project is to produce a level of common understanding about the main SOA security concerns in different domains, e.g. business, defence or critical infrastructure. The final report will summarise the security concerns of both the end-user side (i.e. organisations that try to use SOA) and the vendor/provider side (i.e. SOA integrators, vendors, universities/educators, consultancies etc.). The final report is intended as a vendor-independent public resource that reflects a broad range of concerns from all involved stakeholders. It is intended to provide a broad understanding about the main SOA security concerns that will help all stakeholders come closer to SOA roll-outs, products and education that include appropriate security.

The aim is to include as many relevant concerns as possible using a process that is as open and inclusive as possible. To achieve this, the project purpose is also open to discussion (within the project scope) by the KTN.

3.2 Planned project approach

This project is run as open as possible. The KTN circulates an initial fact-finding document, then run several consultation workshops with end-users, suppliers (products, solutions, services, training/education), and analysts to collect their views on SOA security concerns. The KTN set up an informational website and a blog/wiki etc. area where we will facilitate additional dialogue between interested parties. The KTN will also connect with various suitable SOA industry consortia to solicit input. In addition, the KTN will set up an on-going online survey (located at www.secure-soa.info) to assess how UK stakeholders see SOA security and SOA in general. The findings from the survey will be used as input for the final document.

The purpose is twofold: firstly to get as broad as possible input to ensure the deliverable accurately captures real problems and solutions from all angles (business, vendors, science, market etc.); secondly, to facilitate the creation of a SOA security community across the UK and across all stakeholders involved.

3.3 Fact-finding document purpose

The purpose of this document is to “set the scene” for the discussion within the KTN, the wider community and the workshops. The document offers a first range of definitions of SOA, and a first number of SOA security concerns. This document is circulated to the community for feedback and input. This will allow all stakeholders to provide their views.

The reason for this approach is because one problem related to SOA security is that there are many different aspects, views, and opinions, which results in quite a bit of confusion in the end-user community. Because of the underlying lack of consensus of what SOA means, the fact-finding document will also collect different views about SOA definitions. This is an important part because some SOA security concerns will obviously depend on the particular chosen definition of SOA.

The collected input will form the basis for further scoping/de-scoping and the approach.

3.4 Project scope

As mentioned above, there is a lot of confusion about what SOA actually means in business and technical terms (“Same Old Architecture”?) and what it is good for (“SOA what?” like in “so what?”), what the technical and business show-stoppers are, what the best adoption roadmap is etc.

This initial document does not restrict the definition of the term SOA or the list of security concerns. Depending on the feedback from the community, the final report will be either broad (if many different views are presented) or deep (if there is a topical convergence).

3.5 Outputs – for the KTN, UK PLC, government, and academia

The deliverable will be a publicly report about SOA security concerns (depending on update, also a community website that will be handed over to the KTN, and hopefully also an interactive UK stakeholder SOA security community.

The document will help end-users identify what is important from a security perspective when rolling out SOA. Vendors and universities will benefit from an improved understanding of the real business concerns of SOA security, so they can better align their products and research with end-user requirements.

3.6 Approach – Workshops, surveys

This project will be run as open as possible. We will run several consultation workshops with end-users, suppliers (products, solutions, services, training/education), and analysts to collect their views on SOA security concerns. We will also set up an on-going online survey to assess how UK stakeholders see SOA security and SOA in general. We will set up an informational website and a blog/wiki etc. area where we will facilitate additional dialogue between interested parties. We will also connect with various suitable SOA industry consortia to solicit input.

The purpose is twofold: firstly we want to get as broad as possible input to ensure the deliverable accurately captures real problems and solutions from all angles (business, vendors, science, market etc.); secondly, we want to facilitate the creation of a SOA security community across the UK and across all stakeholders involved.

3.7 Project timetable

The project will be based around the following key dates:

- 31 June
Circulate short introductory paper with provisional definitions, goals, issues, solutions, market maturity and direction assessment etc. to the KTN and the wider community to invite feedback
- 20 August – 15 September
1-day SOA “consumers” workshop: End-user SOA security workshop – discuss end-user concerns (without vendor focus) with government (civilian/defence), industry, and analysts/experts
- 20 August – 15 September
1-day SOA “suppliers” workshop: SOA security vendor workshop – discuss solutions and concerns (product focussed, training focussed), e.g. problems to get SOA adopted; suppliers incl. analysts/experts/universities etc.
- 01 October
Circulate draft deliverable of the final report that takes all input into account, circulate to KTN for feedback
- 14 November
Finalised report handed over to KTN
- 04 December
Findings presented at KTN Christmas event in Bletchley Park

The project wiki, webpage, and mailing list will be available throughout the project.

3.8 ObjectSecurity’s role

Although ObjectSecurity’s offerings include SOA security, ObjectSecurity’s staff will act as an independent facilitator because the benefits of the project can be expected to be maximised if the final report fairly reflects the inputs of the entire community. Particular vendor/supplier/educator products and services will only be mentioned if necessary for the discussion, or e.g. if a general SOA security product/services catalogue is deemed appropriate by the community.

This initial fact-finding document reflects ObjectSecurity’s assessment of the subject area. It is produced to “set the scene” and to foster further discussion to reflect the wider community’s views in the final report. ObjectSecurity’s

team is qualified for this project because it is currently involved as the security consultant (and potential vendor) in a number of SOA projects, and has therefore first-hand experience in the issues and concerns that need to be addressed. ObjectSecurity:

- has real-world market experience in SOA security procurement (from a vendor & consultant perspective)
- has internationally acclaimed scientific and technical competence in the area of SOA security, middleware
- has several thousand related business connections to end-users (government and commercial) and vendors
- has a useful track record in a number of SOA projects both as a consultant and vendor
- has significant experience in running SOA security workshops similar to the ones proposed for this project
- has some in-house assurance accreditation knowhow (e.g. understanding of Common Criteria)
- has significant experience in the development of SOA security related documents that cover both business/technical breadth and technical depth