FOI
Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Phone: +46 13 37 80 00
Fax: +46 13 37 81 00

www.foi.se

Problem Statement

LARS WESTERDAHL

FOI-R--2825--SE
ISSN 1650-1942

Userl Report
September 2009

Information Systems

Lars Westerdahl

Problem Statement

Object and Service-Based Security

Titel	Problembeskrivning – Objekt- och tjänstebaserad säkerhet
Title	Problem Statement – Service and Object-based security
Rapportnr/Report no	FOI-R--2825--SE
Rapporttyp Report Type	Användarrapport
Månad/Month	September/September
Utgivningsår/Year	2009
Antal sidor/Pages	25 p
ISSN	ISSN 1650-1942
Kund/Customer	Försvarsmakten
Kompetenskloss	26 IT-säkerhet
Extra kompetenskloss	
Projektnr/Project no	E53055
Godkänd av/Approved by	Pär Carlshamre

FOI, Totalförsvarets Forskningsinstitut	FOI, Swedish Defence Research Agency
Avdelningen för Informationssystem	Information Systems
Box 1165	Box 1165
581 11 Linköping	SE-581 11 Linköping

Sammanfattning

Den här rapporten beskriver problemområdet och de mål som projektet Objekt- och tjänstebaserad säkerhet har.

Försvarsmakten har beslutat att utveckla sina ledningssystem mot en tjänstebaserad IT-arkitektur. Det är ett naturligt beslut då mer och mer av verksamheten går mot fredsbevarande insatser i samarbete med NATO och EU.

Styrkan i en tjänstebaserad arkitektur ligger i dess förmåga att hantera skillnader i varierande antal användare samt att anpassa sig till nya förutsättningar. De säkerhetsmässiga förutsättningarna i en tjänstebaserad miljö är komplexa. En tjänst är en tillämpning av teknik och processer, vilka kan variera med tjänstens nyttjande. Det finns ett behov av en säkerhetslösning vilken bevarar fördelarna med tjänstebaserad arkitektur och samtidigt ger ett tillräckligt IT/IS-säkerhetsskydd..

Det här projektet skall undersöka möjligheterna att transformera delar av befintlig IT/IS-säkerhetsfunktionalitet till IT/IS-säkerhet vilken erbjuds i form av en distribuerad tjänst. I form av en tjänst kan säkerhetslösningen bättre anpassa sig efter användarnas antal samt ge ett mer dynamiskt nät.

Nyckelord: SOA, Säkerhet som en tjänst, IT/IS-säkerhet, Tillit

Summary

This report describes the problem area and the goals of the project Object and Service-Based Security.

The Swedish Armed Forces has decided to move towards a Service Oriented Architecture in the development of new command and control systems. This is the natural direction to follow as peace-keeping missions in coalitions with NATO or EU has become more common.

The strength of Service Oriented Architectures is the ability to scale and adapt to new events and environments. The security environment in service oriented architecture is complex. A service is an application of technology and processes, which varies by the use of the service. There is a need for a security solution which has the benefits of the service oriented architecture.

This project will explore the ability to transform part of the host-based security into a distributed IT/IS-security service. As a service, IT/IS-security would be more scalable and, in future systems, provide a more dynamic network.

Keywords: SOA, Security as a Service, IT/IS-Security, Trust

Index

1 Introduction

1.1 Motivation

The main purpose of this document is to describe the background and motivation for the project *Object- and Service-Based Security*, as well as explore the research questions put forward.

It also identifies those organisations that are primary stakeholders when it comes to determine needs and requirements for security in Command and Control systems.

Initially a short study was performed in order to determine the most suitable manner in which the project can achieve service oriented security. Two major candidates, one derived form Service Oriented Architecture, SOA, and Software as a Service, SaaS, area, and one based on virtual machines, where evaluated. It was decided that virtual machines where of interest, but the SOA and SaaS approach was closer to the project goals. Virtual machines may still however be of interest as a tool for achieving specific functionality.

1.2 Method

The needs presented in this document are derived from both military requirements and vision as well as from the business use of the information technology and systems. The North Atlantic Treaty Organisation, NATO, is the dominating force within the military domain. Thus much consideration is given to the thoughts and ideas that guide the development within NATO. The European Union, EU, is slowly establishing itself but they also follow the NATO guidelines to a large extent.

Most military organisations have identified a need for using commercial products as much as possible. Thus it is necessary to study how the technology and the use thereof are developing in the business area.

1.3 Report layout

The report is divided into six sections. Section Two is a list of abbreviations used throughout the report. The next section, Section Three, describes the problem area from which the research questions are derived. Section Four presents briefly the main actors within the problem and solution area. In section five the goals of the project are described along with a deeper analysis of the meaning of the research questions. The last section contains references.

2 Abbreviations and definitions

C2	Command and Control (sv. Ledning)
CIS	Communication and Information System
EDA	European Defence Agency
EU	European Union (sv. Europeiska unionen)
IEG	Information Exchange Gateway
IST	Information System Technology
NATO	North Atlantic Treaty Organisation
NBG	Nordic Battle Group
NACOSA	NATO CIS Operating and Support Agency
NC3A	NATO Consultation, Command and Control Agency
NC3TA	NATO Consultation, Command and Control Technical Architecture
NATO RTO	NATO Research and Technology Organisation
OASIS	Organization for the Advancement of Structured Information Standards
SOA	Service Oriented Architecture (sv. Tjänstebaserad arkitektur)
SWECCIS	Swedish Command and Control Information System

3 Problem statement

One of the most important capabilities for the Swedish Armed Forces is to be able to take part in an international coalition of armed forces[1]. This capability means that the Swedish Armed Forces must be able to communicate and share command and control, C2, information with other coalition members.

To a certain extent, this is no different than communicating within the Swedish Armed Forces on a national level. The main difference is, thus far, that most coalitions have been lead by the North Atlantic Treaty Organisation, NATO. NATO itself is not a solid body when it comes to how equipment is procured. Thus there exist standard agreements within NATO of how to communicate and common goals of how, amongst others, future C2 systems are to interact. There are several standard agreements. The common goals of how to interact within and to the outside of NATO networks are described by NATO Consultation, Command and Control Agency, NATO C3A[2], in the architecture NATO C3 Technical Architecture, NATO C3TA.

As a current coalition partner with NATO the Swedish Armed Forces need to adapt to NATO standard agreements. It is also natural that the future Swedish C2 systems align with intentions of what is expressed in the NATO C3TA. This architecture is a living entity which adapts to new requirements and changes in technology. The purpose of the architecture is to ensure controlled communication between NATO networks. How communication and sharing of information is conducted on a national level by a NATO country, or even a non-NATO country, is of no concern as long as proper measures are taken to ensure the assurance necessary for the security level of the network.

The European Union, EU, is also an initiator for a coalition force. Sweden acts on EU mandate in the Nordic Battle Group. Most countries within EU however are also members of NATO. This means that NATO standards and agreements are also important for EU comprised units.

The following subsections will explore the current needs in C2 systems in generic terms.

[1] Regleringsbrev för budgetåret 2009 avseende Försvarsmakten, 2008

[2] NATO Consultation, Command and Control Agency, http://www.nc3a.nato.int/Pages/Home.aspx (2009-09-17)

3.1 Flexibility

Currently, military conflicts are usually handled by coalitions[3]. A single state can rarely handle a conflict on its own and the conflicts fought are over issues that concerns several states. Coalitions are not solid entities however. A few nations initiate the coalition but others may join or leave during the lifetime of the coalition.

The C2 system of the coalition cannot be dependant on a given infrastructure of the coalition members. It has to be able to scale up and down during the operation. Also, the C2 system should not discriminate between users based on a preconception of whom to share information and services with.

3.2 Sharing information

Taking part in a coalition means collaboration. Coalition members should be able to fight side-by-side and use each others resources as needed. This requires sharing of information and services across the local boundaries within the coalition. Taking a high-level perspective on the information sharing problem, it is quite obvious that coalition members need to share resources. As the perspective narrows in on reality it becomes a bit more complicated.

A nation may join a coalition for several reasons. They may even have some intentions which are not necessarily contradicting to the coalition mission, but which may result in information which they do not want to share. A nation may share intelligence, but do not necessarily want to reveal or release control of the source. Some nations have a tradition of working together and sharing information. As mentions earlier, NATO is a common leader of coalitions. That does not necessary mean that all coalition members being part of NATO. Sweden for one is not. Thus there may be information and services open to NATO-members, but not those outside the alliance.

There is an understanding that information and services need to be shared albeit not all and not at any time. To a certain extent, information sharing is controlled by network the information resides on. Sharing information between coalition countries, as described above, is not the only issue however. Within one nation's C2 system there are usually networks with different security levels. Information often needs to be shared between these networks as well.

[3] NATO Network Feasibility Study, NC3A, 2005

3.3 The value of information

An information system's primary task is to provide information. If the system cannot provide information to a user when asked, provided of course that the user is entitled to the information, the system is not of much use. The value of a piece of information is not constant. If the information system presents old or outdated information, then the search function or the indexing system is not functioning properly. But information can also have different value to different users. Old information may not be valuable for some but valuable for others. The granularity of the information may also be a divider of value. For instance, the existence of a special weapon system within a given area may be useful enough at one level whereas, on a lower level, the exact position of these weapons is what matters. Different value is not only described as age or freshness, it can also be a question of geography. Some information may be necessary to be available to users in a given area, say on a mission. The same information has no practical value for users elsewhere and thus should not be allowed access from outside the mission.

3.4 Information-centric systems

There are several reasons why it can be difficult to obtain the information or services a user may need. Thus far nation boundaries and secrecy has been mentioned. Information is, in one way or another, labelled at time of creation. Marking data such as origin and time does not change over time and is thus uncontroversial. Other markings such as security level are a valuation of the data at the time of creation. By marking a piece of information with a valuation, this information will be locked for the foreseeable future regardless of need or other circumstances. It is common practice to separate networks by their security level. Thus any information created on a network with a security level SECRET will receive a SECRET tag. However, not all information residing on a SECRET network is necessarily secret.

Other difficulties to obtain information or services come from legacy. The armed forces are comprised of different branches such as the air force, army, and navy. These branches have their own C2 systems. Collaboration between these branches is more common on a joint level and through liaison officers, whereas direct communication on unit level is more difficult. The difficulties are partly technical and partly structural with different traditions and standards. The non-technical issues are outside the scope of this project. The technical issues however create "stove pipe systems" that limits information dissemination almost as well as physical separation. The result of this is that it may be more important which system, or which equipment, a user has access to than what information the user needs. Although some of these "stove pipe systems" has disappeared with the use of contemporary technology such as Service Oriented Architecture, SOA, they still exist and affect the usability of C2 systems.

For an information system to be effective the availability of information should be the central issue - not where the information resides.

3.5 Security issues

IT/IS-security can somewhat bantering be described as the opposite of what is asked for above. Most often IT/IS-security has been about defining a boundary and then focusing on keeping the outside on the outside and the inside on the inside.

Providing security is about providing control. The more structure a system has and the more segregated the use of system resources are the easier it becomes to provide security. This may, however, result in security for the sake of security. The strictest security policy, which implies that information must not fall into unauthorised hands, will most likely lead to a behaviour where the authorisation system rather would hinder access to a valid user than risking allowing access to an unauthorised user.

Security is often described by the properties confidentiality, integrity and availability. Often the properties are prioritised in the above order, which makes information sharing difficult. From a sharing point of view the priority should be the opposite. The need for security is not derived from technology, or at least it should not be, rather it is a need from a management perspective. Thus, providing a good security solution is more than keeping a secret. Integrity, the amount of trust that can be put in that the information is correct, and availability, the likeliness that a user can find and access the information needed, are just as important as confidentiality. Sometimes even more.

In an information-centric system the security solution should maintain availability of information and services to authorised coalition members at any time. The solution also needs to be flexible in the sense that it needs to be possible to handle coming and going coalition members. The Data Strategy of the NATO C3 TA[4] suggests a net-centric paradigm of “post before processing”. It means that information should be made available as quickly as possible but the processing of the information, such as setting access rights, is made the through the current policy. Such a system requires functionality that the can interpret and validate a policy against the content of the information.

[4] NATO C3 Technical Architecture Vol 2 Architectural Descriptions and Models, 2005

Viewing security from an infrastructural point of view, where the most important issue is the ability to store and transport information from point A to B, then the available security solutions are fairly solid and will most often provide sufficient security. Taking a “business-perspective”, where the use of information and services are the focal point, the security issues become more difficult. Now it is not just a question of being on the inside or outside, but also when and where services are needed and in which capacity they are asked for. The use of the technology today is not just about getting information from one source to another. Current information technologies gather information and services from different sources through the use of, for instance, Web Services and Web 2.0. This result in different IT/IS-security needs. IT/IS-security has not, unfortunately, evolved in the same pace as the usage of information technology[5].

Exchanging information between nations in military coalitions, and thus between different security domains, is in NATO’s Technical Architecture regulated by the use of an Information Exchange Gateway, IEG. The purpose of the IEG is to guard against unintended information leakage between networks. It has been noticed that, however, that sharing information and services over the IEG is difficult due to IEG constraints[6]. Similar problems have also been noticed in the research community[7].

[5] Peterson, G., 2009

[6] Dialogue with NATO RTO IST-ET-057, 2009

[7] Menzel, M. et al., 2007

4 Actors and contributors

In this section a short introduction is given of the main actors and contributors that identify the needs and requirements of command and control systems.

4.1 International actors and contributors

Coalitions are formed by a number of nations. The main actor in most coalitions in resent years is NATO. EU is an upcoming actor with a military connection to Sweden through the battle group concept. These are the main actors when it comes to defining the needs and requirements for communication, interoperability and information exchange in command and control systems.

4.1.1 North Atlantic Treaty Organisation, NATO

NATO is a large organisation made up by 28 countries. Being such a large organisation of different countries, interoperability issues and information security issues are familiar questions within the organisation. These issues, however, are tackled from different perspective from different parts of the organisation.

NATO Consultation, Command & Control Board. The NATO Consultation, Command & Control Board, NC3B, supervises eight subcommittees and oversees two agencies; the NATO Consultation, Command & Control Agency, NC3A, and NATO CIS Operating and Support Agency, NACOSA.

The subcommittees are focused on different aspects of information system, security, and radio frequencies. The work done in the committees of Information Systems and Information Security Systems are of primary concern to the project.

The NC3A is primarily concerned with identifying long-term capabilities requirements for the architectural framework and to implement changes. One of the most guiding documents for C2 systems development that have been produced by NC3A is the NATO Network Enabled Capability Feasibility Study[8]. This study suggests a Service Oriented approach for realising a Network Enabled Defence.

NATO Research and Technology Organisation. The Research and Technology Organisation within NATO, NATO RTO, provide a wide range of research for defence science and technology. The focus areas are divided into six technical panels where, from the Object- and Service-Based Security project's

[8] NATO Network Enabled Capability Feasibility Study, 2005

point of view, the Information System Technology Panel, IST, is the most interesting. IST supports several projects. From some of these projects publications are openly available, whereas from others access to publications is members or partners only.

4.1.2 European Union / European Defence Agency

The European Defence Agency, EDA, is an agency within the European Union, EU. EDA's main purpose is "to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future"[9]. Even if the EU and EDA have a long-term vision[10] of their own, they do follow the development and guidelines of NATO. This is quite natural as most of the EU members also are members of NATO. This means that the EU also strives for a service oriented approach to command and control systems.

EDA has made a similar work as the NATO Network Enabled Capability Feasibility Study, which has resulted in a Strategic Framework of how to develop European expeditionary capabilities[11].

4.2 National actors and contributors

The Swedish Armed Forces has decided[12] to use a service oriented approach to new C2 systems. The guiding framework is the OASIS Reference Model for Service Oriented Architecture[13].

The Swedish Armed Forces and the Swedish Defence Materiel Administration have studied service oriented architecture through the work on the future command and control system.

The work performed by the technology part of the Network Based Defence development, LedsystT, Swedish Command and control information system, SWECCIS, and the Swedish Armed Forces Concept and Development initiative, FM KE, all serve as great input and reference to this project.

[9] http://www.eda.europa.eu/genericitem.aspx?area=Background&id=122 (2009-08-28)

[10] http://www.eda.europa.eu/genericitem.aspx?id=146 (2009-09-17)

[11] European Defence Agency's Strategic Framework, EDA, 2009

[12] SwAF CIO Decision Direction (Inriktning FM anpassning mot OASIS SOA RM version 1.0), Försvarsmakten CIO, 2008

[13] OASIS Reference Model for Service Oriented Architecture 1.0, OASIS, 2006

5 Project scope

Naturally, all security issues cannot be solved at the same time. There is a long-term research vision that spans past this project and specific goals that are sought within the projects' lifetime.

5.1 Research vision

The long term research challenge is to make information objects independent of its security classification. That is, an information object should not be classified with a valuation that will follow it throughout the lifetime of the information object. The information should rather be subjected to a current security policy that will determine the current classification level and the current need for protective measures. With these prerequisites, information can be given different importance, as far as security and access is concerned, during the lifetime and location of the information and its publication.

5.2 Project goals

It is the goal of this project to show that some security functionality can be transformed into services. There are several reasons for exploring the possibility for service oriented security:

1. The main purpose is that a system based on services is more flexible than a system with only locally implemented functionality. A flexible system can more easily adapt to new mission prerequisites and surroundings.
2. The flexibility also implies a more dynamic security structure where the security configuration can be adapted to the current needs, and where the changes can be configured to only apply to a given portion of the network.
3. Extracting security functionality from applications and hardware simplifies maintenance and replacement of products.

It is also a hypothesis that separation of security functionality from applications and hardware is a step towards a generic object security solution.

5.3 Research questions

Moving towards an architecture, where information is self contained entities and where usage of these entities is controlled by services requires a different security setup than what is in use today. This project carries three main questions which will guide the research forward.

- Which security functionality can be transformed into a service?
- Which security functionality must be executed locally?
- How do we set the security level to match current needs and the ability to adapt to new needs as the situation changes?

These questions can be pursued from different angles. A descriptive exploration follows below. The project also has the task of following the development of object based security.

5.3.1 Which security functionalities can be transformed into services?

Transforming a network into a service oriented network means transforming the way the network is used for supporting the mission. To make the security solution follow the transformation a revised view of how security is implemented is necessary.

To date, most security functionality is embedded in or around the application where the information is stored or at some node within a network where specific functionality is needed. Just as business services are repeatable business task separated from the initiating applications, security services will be repeatable security tasks which can be called upon by other services and applications. With a service oriented security the security functionality, to a certain extent, would be distributed and provided by the network.

A key question here is of course which functionality that can be transformed into services. Some security functionality easily lends itself to this line of thinking in the current security paradigm. Key distribution and certificate distribution and validation are already working in this manner. Another function that should be, more or less, easily transformed is a Policy Decision Points.

Two needs that will follow the search for transformation of security are flexibility and user friendliness. A security architecture must support the current mission of an enterprise. The security architecture must on the other hand be flexible enough to function even if the mission changes or at least the parameters within the mission changes. The technology and equipment used in one mission is, more or less, the same as what will be used in the next mission. Missions are often carried out by a coalition, which means that coalition partners may come and go during the mission. It is therefore necessary to have an open architecture so that coalition partners can design their national command and control system accordingly.

Some practical and successful results in separating security functionality from applications have been achieved during Coalitions Warrior Interoperability Demonstration[14].

5.3.2 Which security functionalities must be executed locally?

Even if a service oriented paradigm is what is sought after in this project there is a need for some locally hosted functionality. This implies to ask the direct opposite question as compared to the last section; which functionality cannot be transformed into a service?

Host security will be as necessary in the future as it is now for stored information and host integrity. Information and applications enters a network from different access points. It is unlikely that all input into the network can be efficiently controlled with the use of services. Some security functionality should be local to maintain efficiency. From a military perspective it may also be necessary with local, “always present” functionality in case of a needed service is out of reach.

Another aspect of services is the possible ability to provide secure platforms. A security application needs a secure environment, a trusted computer base, to ensure correct behaviour. The interesting question here from a service perspective is not what needs to be hosted locally, but rather if a secure environment can be presented in an uncontrolled environment. Can a trusted computing base be distributed? And what assurance does it carry? With the long term goal set for object-based security architecture the need for controlling the host is eminent. Being able to provide a secure platform anywhere would be of great value.

The goal for this project is to identify which functionality needs to be run in a controlled environment and to explore the possibility of distribute a trusted platform.

[14] Secure Service Oriented Architectures (SOA) Supporting NEC, NATO RTO TR-IST-061

5.3.3 How do we set the security level to match current needs and the ability to adapt to new needs as the situation changes?

What constitutes good security may vary from time to time. What is regarded as good security at one time may be a hinder at another time. The reasons that set the security level at one time are not necessarily the same at another time, even if the information is the same.

In NATO N3TA it is suggested that information should be tagged with metadata describing the content of the information rather than a label with an evaluation of the information. A security labels, such as RESTRICTED, is an evaluation of the content that will follow the information object. But it is also an assumption about future users, where they might be and what they might need. The circumstances resulting in a security label at creation time can change drastically through the lifetime of the information. Thus it would be of great value if the security evaluation could be carried out at the time when the information is requested. With an accurate description the content of what the information, the result would in a more flexible way adjust security decisions and needs. A policy could then dictate how classes of information should be managed and such a policy could both be global (network wide) or local (a subset of the network).

Ideally, a proper labelling and a good policy could be a step towards handling several security classes in one network.

5.3.4 The prognosis of object based security

The project has been given the task to follow the development of object based security. As the reader has noticed the research goal is to obtain object based security, although it is not feasible to believe that it can be done within this projects lifetime.

Object based security is a security model where, ideally, the confidentiality (if necessary) and integrity of information object is carried within the information itself. With a self-contained security model the actual location, and thus the need to protect that location, will decrease. This will in turn promote availability.

Although some software manufactures claim to have object-based security solutions, there has not yet been a generic solution. The solutions presented by manufactures so far are bound to that manufactures product line.

A generic solution, at least with a high assurance level, is unlikely in the near future. The project shall follow how the area is developed and evaluate the availability of such technology in the future.

5.4 Demarcations

Initially, the goal is to provide security services within one domain or type of network. If an acceptable interdomain solution is achieved within given time, a global solution will be sought.

5.5 Benefit of research

The purpose of having secure information systems is to be able to use the systems even when they are attacked and to maintain trust in the systems over time.

Security is all about control. Thus far control has been established by local functionality, a solutions which is not necessarily bad but more difficult to change. The main benefit with a service based security solution is flexibility. This flexibility will become useful when new or unplanned situations occur.

6 References

European Defence Agency's Strategic Framework, *EDA*, 2009, http://www.eda.europa.eu/WebUtils/downloadfile.aspx?fileid=651 (2009-09-17)

Inriktning FM anpassning mot OASIS SOA RM version 1.0, *Försvarsmakten CIO*, 2008

Menzel, M. et al., "SOA Security - Secure Cross-Organizational Service Composition". In *Proceedings of Stuttgarter Softwaretechnik Forum (SSF)*, Stuttgart, Germany, November 2007

NATO C3 Technical Architecture vol.2 Architectural Descriptions and Models, Ver.7, *NC3A*, December 2005

NATO Network Enabled Capability Feasibility Study Volume 1: NATO Network-Centric Operational Needs and Implications for the Development of Net-Centric Solutions, version 2.0, *NC3A*, October 2005

OASIS Reference Model for Service Oriented Architecture 1.0, *OASIS*, 2006, http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf (2009-09-17)

Peterson, G., "Service-Oriented Security Indications for Use", *IEEE Security & Privacy*, March/April 2009

Regleringsbrev för budgetåret 2009 avseende Försvarsmakten, *Försvarsdepartementet*, 2008-12-18 http://www.mil.se/upload/dokumentfiler/regleringsbrev/Regleringsbrev%20FM%202009.pdf (2009-09-17)

Secure Service Oriented Architectures (SOA) supporting NEC, NATO RTO Technical Report TR-IST-061, 2009 http://www.rta.nato.int/Pubs/RDP.asp?RDP=RTO-TR-IST-061 (2009-09-17)