Trust as a challenge in distributed information systems – a contribution to the RTO Technical Report on NEC Security Research Strategy

Tor Gjertsen

Forsvarets forskningsinstitutt/Norwegian Defence Research Establishment (FFI)

09.11.2007

FFI-rapport 2007/02450

1086

ISBN 978-82-464-1266-5

Keywords

Nettverksbasert forsvar

Tillit

Sikkerhet

Informasjonssikkerhet

Approved by

Anders Eggen	Project Manager
Vidar S. Andersen	Director

Sammendrag

Fremtidige militære operasjoner vil kreve høy grad av dynamikk, og utstrakt og tidsriktig informasjonsflyt mellom samarbeidende parter i en koalisjon. Etablering av tillit på et tilstrekkelig tillitsnivå i taktiske omgivelser vil være en forutsetning for et nettverksbasert forsvar, NEC (Network Enabled Capability). Dette er en problemstilling som ennå ikke er løst. En tillitsmodell som gir skalerbare og fleksible løsninger må finnes, så vel som en politisk og policymessig plattform for å kunne stole på en samarbeidspartner, og være villig til å dele informasjon i en netverksbasert operasjonsmåte.

English summary

Future military operations require high dynamics and extensive and timely information flow between cooperating parties in a coalition. The establishing of a level of trust in such an environment is a prerequisite for NEC, which is not yet solved. Scalable and flexible trust models and solutions for trust management must be found, as well as the political and policy foundation for trusting cooperating parties and the willingness to share information in a network enabled capability.

Contents

1 Introduction

The NATO Network Enabled Capability (NNEC) vision is designed to increase the effectiveness of military operations and provide strong networks, communications, systems, and information infrastructure capabilities perspective grounded in the concepts of information sharing, trust, policy, shared awareness, interoperability, flexibility and dynamics.

The Information Systems and Technology (IST) Panel's Task Group on Network Enabled Capability Security (TG NECSec, RTG-017/IST-045) has studied the information assurance and information security implications of NII and NEC. The NECSec group hosted a Spesialist's Meeting, "Research Strategy for Information Security i Network Enabled Capabilities" (IST-073/ RSM 003), see annex 1. The NECSec results will be publishet in an RTO Tecnical Report on NEC Security Research Strategy". The objective of that report is to highlight critical topics, information assurance (IA) and security challenges areas for the evolution to a fully functional NEC and the analytical framework in which continual analysis ought to be conducted.

Annex 2 is a reprint of FFI's contribution to one of the topics in the RTO-report; **Trust**, and a presentation on this topic was also given at the RTO Specialist's Meeting in Brussels 16-17 April 2007.

Appendix A RTO Specialist's Meeting, IST-073/RSM-003

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

SPECIALISTS' MEETING

Research Strategy for Information Security in Network Enabled Capabilities

IST-073 / RSM-003

organised by the

Information Systems and Technology Panel

to be held at the

BELGIAN DEFENCE STAFF

Brussels, Belgium

Monday 16 April 2007 -Tuesday 17 April 2007

This Specialists' Meeting is open to citizens from NATO nations only

Latest Enrolment Date:

Monday, 9 April 2007

Enroll Online at:

http://www.rta.nato.int

Please enroll for this Specialists' Meeting via internet at http://www.rta.nato.int

Once your enrollment is validated, you will receive a General Information Package (GIP) giving you further necessary details about the meeting.

If you are unable to enroll via the internet, please contact the IST Panel Assistant at: apaydina@rta.nato.int

GENERAL DETAILS

The Network Enabled Capabilities (NEC) operational concept faces security threats – some new, some more intense - which need to be addressed in order to diminish the operational risk, guarantee availability, and ensure operational integrity. Current security policies, architectures, services and mechanisms will be insufficient to provide the right protection of information assets within the dynamic and complex multi-national NEC environment. For that reason, the NATO RTO/IST Task Group on NEC Security (~ NECSec/RTG) has spent the past three years analysing the security implications of the future NEC environment and has aimed to develop an evolutionary research strategy for NEC Security for NATO, NATO member nations, and coalitions. As a result of this analysis, NECSec/RTG is conducting a NATO RTO/IST Specialist Meeting (RSM) to disseminate the results and discuss the findings, and establish a roadmap for research and development of NEC Security.

The core objective of the RSM is to outline a research strategy for NECSec, give all the participants a common understanding of the NEC Security issues, and to follow up on the security issues outlined in the NNEC feasibility study. In addition, there will be a discussion on how collaborative research and development can be carried out to obtain the goal of a secure NEC environment.

This Specialist Meeting will combine keynote and invited speakers, NECSec/RTG presentations and panel/group discussions on the topics mentioned below in order to facilitate exchange of ideas and networking between participants. Participants will gain an understanding of the issues confronting real time information sharing in a fully federated cooperative trust environment. This should enable the participants to coordinate and prioritise the funding of R&D for NEC security.

BACKGROUND AND JUSTIFICATION (Relevance to NATO):

A Network Enabled Capability is seen as the future concept for military operations. However, the requirements on the Network Information Infrastructure set forth by this concept are large. Security is currently lagging in solutions to achieve a good capability, and research should be intensified. The RTO task group on NEC Security has been investigating the topic, as have several nations. Combining efforts and working together is important in order to reach the proper level of secure interaction that is required of NEC military operations.

OBJECTIVE(S):

The objective of the specialist meeting is to achieve a common understanding of the security topics that need to be researched, the effort that is required, and the relevance of timely availability of the security technology in the NEC perspective. This objective will be achieved through tutorial sessions held by experts with previous experience from related activities, including dissemination of the results achieved by NECSec/RTG, as well as discussion sessions with national research coordinator and military operational personnel.

TOPICS TO BE COVERED:

A number of topics that are considered to be important areas of research in order to achieve NEC will be addressed. The topics are a follow up on the security issues of the NNEC feasibility study, i.e. for security policy and architecture, transport, information and management domain.

In particular, the RSM will address the following topics:

- Federation of Systems
- Policy of Sharing
- Policy Based Access Control
- Trust
- Security Assurance
- Dynamic Risk Management
- Security Architecture
- Security Lifecycle Management
- Flexibility and Scalability
- NII Availability
- Coordination of research

Program Committee Co-Chairmen:

Mr Dennis McCALLAM, Northrop Grumman Information Technology, USA
E-mail: dennis.mccallam@ngc.com

Dr Michel LEONARD, NATO/NURC, ITA
E-mail: leonard@nurc.nato.int

Members

The Program Committee is the Members of the IST-045 / RTG-017 Task Group on NEC Security (~ NECSec/RTG).

RTA Panel Office - Point of Contact

Lt.Col. Patrick PRODHOME
IST Panel Executive
RTA Paris
Tel: +33 (0)1 55 61 22 80
Fax: +33 (0)1 55 61 96 07
Email: prodhomep@rta.nato.int

Mrs Ayşegül APAYDIN
IST Panel Assistant
RTA Paris
Tel: +33 (0)1 55 61 22 82
Fax: +33 (0)1 55 61 96 26
Email: apaydina@rta.nato.int

IST-073 Specialists Meeting on "Research Strategy for Information Security in NEC"

Programme

Monday 16 April 2007

08:15		Registration
09:00		Opening Ceremony
		Introduction by Prof. Jürgen GROSCHE, IST Panel Chairman, DEU
		Introduction by Maj. Erik van de SCHOOR, Local Host, BEL
		Introduction by Mr Dennis McCALLAM, Specialists' Meeting Co-Chairman, USA
09:30		KEYNOTE SPEECH: "Challenges and Security Concerns in a Federated Environment" by Lt.Gen. Ulrich H.M. WOLF, Director, NATO CIS Services Agency
10:15		BREAK

Session Day 1:

Chair - Dennis McCALLAM, USA

10:45	1	Overview of NATO Networked Enabled Capability by Geir HALLINGSTAD, NATO C3 Agency, NLD
11:30	2	Introduction to the NEC Security Research Strategy by James SIDORAN, AFRL, USA
12:00		LUNCH
13:30	3	Federation of Systems by Mert UNERİ, TUBITAK-UEKAE, TUR
13:50	4	Policy of Sharing by Eric LUIIJF, TNO Defence,Security and Safety, NLD
14:10	5	Policy Based Access Control by Daniel CHARLEBOIS, DRDC, CAN
14:30		BREAK
15:00	6	Dynamic Risk Management by James OBAL, NATO ACT
15:20	7	Trust by Tor GJERTSEN, FFI, NOR
15:40	8	Security Assurance by Geir HALLINGSTAD, NATO C3 Agency
16:00		PANEL DISCUSSION Moderator: Michel LEONARD, NATO URC
16:40		Wrap Up of Day 1 by Michel LEONARD, NATO URC
17:15		RECEPTION HOSTED BY THE BELGIAN DEFENCE AGENCY Transport from hotel for spouses/companions

Tuesday 17 April 2007

Session Day 2:

Chair - Michel LEONARD, BEL

09:00		Introduction to Day 2 by Michel LEONARD, Specialists' Meeting Co-Chairman, NATO URC
09:15		KEYNOTE SPEECH: "Availability Challenges and Security Concerns in a Network Enabled Capabilities Environment" by Brig. Nick POPE, Chief CJ6 ISAF IX, GBR
10:00	9	Security Architecture by John MELROSE, DSTL, GBR
10:20		BREAK
10:50	10	Security Lifecycle Management by Michel LEONARD, NATO URC
11:10	11	Flexibility and Scalability by Bartosz JASIUL, MCI, POL
11:30	12	NII Availability by Marko JAHNKE, FGAN, DEU
11:50		LUNCH
13:10	13	Coordinating National Research by James OBAL, NATO ACT
13:30	14	NEC Security Challenges by Alfred MOELLER, DALO, DNK
13:50		INVITED PRESENTATION: "International Research Collaboration on Cooperative Security Issues" by Michael CORCORAN, Research and Development Coordinator, National Infrastructure Security Coordination Centre, GBR
14:30		BREAK
15:00		PANEL DISCUSSION Moderator: Dennis McCALLAM, Northrop Grumman, USA
15:45		Wrap Up and Way Ahead by Dennis McCALLAM, Northrop Grumman, USA
15:55		CLOSING CEREMONY

Appendix B The FFI contribution to the topic ”Trust”

Trust

Tor Gjertsen
Norwegian Defence Research Establishment (FFI)
P.O. Box 25, 2027 Kjeller
Norway

Tor.Gjertsen@ffi.no

ABSTRACT

Future military operations require high dynamics and extensive and timely information flow between cooperating parties in a coalition. The establishing of a level of trust in such an environment is a prerequisite for NEC, which is not yet solved. Scaleable and flexible trust models and solutions for trust management must be found, as well as the political and policy foundation for trusting cooperating parties and the willingness to share information in a network enabled capability.

1.0 INTRODUCTION

The decision to trust someone or something is more a policy decision than based on objective evidence, since it can not be measured accurately. Trust relates to the interaction between two parties over time, and is often based on intuition and the expectation that the other party behaves according to certain rules or agreements. Traditionally, such interaction was carried out face to face and a lot of different observations impacted the trust decision. Now interactions are also carried out by electronic devices, information systems and often via communication networks, but the importance of and need for trust still exists. In addition to trusting the other party, we have to trust the technical solutions and the implementation of systems in use. Trust is a critical consideration for security.

1.1 Definition

There are numerous definitions of trust since the term is used in many different areas like psychology, sociology, and in information science and technology. However, there is no widely accepted definition of trust. Listed below are some examples.

Trust: Strong belief, in the goodness, strength, reliability of something or somebody, responsibility. (The Oxford English Dictionary).

Trust: the assured reliance on the character, ability, strength, or truth of someone or something. (Webster Dictionary).

Trustworthy and trust: An entity is *trustworthy* if there is sufficient credible evidence leading one to believe that the system will meet a set of given requirements. *Trust* is a measure of trustworthiness, relying on the evidence provided.[1].

For NEC all these definitions are relevant, the first two on the organisational and personal level, the last taken from computer science, on the system/technical level.

The terms ***trust*** and ***assurance*** are often used interchangeably, but in practice, especially from a systems perspective, these topics are quite different. Trust is a subjective measure that is based on some sort of evidence or beliefs on how the other entity will behave. Security assurance (or assurance) is an objective measurement of how well a device/product does what it is supposed to do supported by evidence resulting from the application of assurance techniques. The security assurance of a particular product can be measured by methodologies such as Common Criteria and associated product evaluation standards and ultimately assigned an evaluated assurance level value. This value can subsequently be used as a reference measurement to establish a level of trust in that the product will behave as designed. It should be noted that having the evaluated assurance level value to the product in itself is not sufficient to attain the required trust. Other factors such as the scope of the evaluation process used to obtain the value and the credibility of the evaluation source and similar factors also contribute to the trust factor.

1.2 Relevance to Network Enabled Capabilities

The establishing of trust between cooperating parties is a prerequisite for NEC. This applies to all levels: the political, organisational, personal, information exchange, procedural and technical levels. A level of trust must be in place for the parties to be willing to co-operate in common operations and to exchange sensitive information in a timely manner. The willingness to share and accept information depends heavily on mutual trust between the information provider and the recipient.

To illustrate the significance of trust, shopping via the Internet can be used as an example. Some sort of trust has to be established between the parties. The buyer has to believe that the selected item will be delivered to the agreed price before he/she is willing to initiate the payment. The trust can not be measured exactly, and may be based on rumours, recommendations, and third party fair trade labels. Less trust means higher risk for a transaction. However, if the value of the item is low, the buyer may accept the associated risk. For NEC it may be a requirement for quantifying the trust and the acceptable risk, as input to the process of deciding on the security requirements.

2.0 CHALLENGE

To realise NEC, trust has to be established at the political, organisational, personal, information exchange, procedural, and technical levels before NATO Nations, coalition partners, and other organisations are willing to share classified and even unclassified information. Current security policies in the nations or organisations when it comes to classified material, typically default to distrust each other. The security and information exchange policies must be opened to allow the interconnection of systems and the sharing of information between nations, organisations, and other parties. This still requires the premises of maintaining the security principles and concepts such as clearance, authorisation, and need to know.

Security goes hand in hand with trust, and trust is necessary to achieve security. Confidentiality, integrity, authentication, non-repudiation, and availability are central elements of security. The implementation thereof involves cryptographic methods which again rely on trusted security keys. How to trust the keys and their handling? You have to trust the organisation that issues the keys, and you have to trust the delivery process of the keys.

In a NEC environment, the introduction of a Public Key Infrastructure (PKI) seems feasible. For military systems current policy is that the PKI system shall have a hierarchical trust model with only one common root Certificate Authority (CA). A **trust model** describes how the PKI enables

trust between the users of the PKI services. In this hierarchical model, trust links are enabled between different sub CAs based on their trust in the root CA. Interoperability between different PKI domains must be supported, and various methods of cross-certification or bridging will be required. Today's policy is that this shall be handled at the root CA. However, such as a heavy reliance on a single trust point may be inconsistent with operational NEC requirements.

An alternative solution is the meshed PKI model, where all the entities in the network can be a trust point which can issue certificates to each others. The trust is bi-directional and forms a network of trust. In this scheme it is easier to incorporate new users, but it has a lot of implications and makes the certification path more complex. The "web of trust" is one example of this scheme which is best known for its use in the email security system PGP (Pretty Good Privacy). The web of trust is now used in a number of other applications and is established as a method for doing non-centralised PKI in the civil community.

The NATO NEC vision is to connect users and service providers to the protected network via NEC security devices as part of a very flexible cross domain information network strategy. Users and resources can dynamically enter and leave the network without any preplanning of the movements. The security devices will contain all kinds of security functionality like encryption, authentication, etc. They provide security services to the end systems in a way that makes security transparent for the users. Such units will play a critical role in a dynamic NNEC, and it will be a big challenge to find a suitable trust model for the operation of the security devices.

At the technical level, the proper secure implementation of the NEC security devices and the corresponding security functions of the end systems is critical in order to establish trust in the NEC information infrastructure. The assurance level of an implementation can be used to aid in the establishment of a trust level. Higher levels of assurance could equate to higher the level of trust. However, trust must be established at the organisational level as well. Finding methods to establish such coherent and harmonised levels of trust between coalition partners and their infrastructure is a challenge.

In a dynamic environment the risk may change quickly. A system in operation has to be monitored and risk management has to be performed on a timely basis in order to maintain a sufficient level of trust for the system. If the risk gets to high, the system can no longer be trusted without sufficient additional countermeasures.

3.0 RESEARCH

3.1 Summary of current and planned activities

The International Telecommunication Union (ITU) works on trust in the commercial electronic environment. Also, the G8 sponsored World Summit on the Information Society's (WSIS) "Declaration of Principles" states that strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among Information and Communications Technology (ICT) users.

TERENA has developed a relative simple scheme called Trusted Introducer (TI) for the CERT community. The base concept may be an input to look for directions to address the identified challenges.

In the academic community work has been going on for years in the area of trust for, which also may be of relevance to NEC. In [3], the relationship between trust and security are elaborated, as well as alternative trust models and what level of trust can be expected in different scenarios.

3.2 How do the current activities fail to address the problem?

Existing solutions aim at controlling the establishment of connections and the information flows between protected areas, and to some extent to pass information between different domains in a controlled way governed by the security policy. This will not work in a highly dynamic cross domain environment.

The NEC vision is to accept all connections, and to control the information flow end-to-end via access control mechanisms regardless of the domains. Access to information is based on the content given by the signed label, and the role and privileges of the requesting user. This strategy is assumed to be an enabler for a far more flexible information flow.

3.3 How can research address the challenge?

A trust model that fits the dynamics of the NEC environment has to be developed. The security infrastructure of a nation must be able to function autonomously, but it shall also function in a coalition. Methods for establishing trust between coalition partners have to be found. Interoperability must be established in a timely manner when new partners enter the infrastructure. The solutions for this must scale well. Alternative methods and strategies for cross-certification or bridging need to be examined to find proper solutions. Research will be necessary in the areas of trust models and trust management to bring the technology to a maturity level that meets NEC functional needs and security requirements.

4.0 CONCLUSION AND RECOMMENDATIONS

The establishment of trust between the parties in a coalition is a prerequisite for any joint operation. Mutual trust must exist at all levels of the participating organisations, to their administrative procedures and to the systems in operation.

Work has to be done to understand the process of building trust, and to develop agreed methods for establishing and maintaining trust in a dynamic, multinational NEC environment. Also the policy work for NEC has to address this to open for mutual acceptance of trust in a coalition.

5.0 REFERENCES

[1] Matt Bishop, “Computer Security: Art and Science”, Addison-Wesley Professional, ISBN 0201440997, 2003.

[2] H. Li and M. Singhal, “Trust management in Distributed Systems”, IEEE Computer Society, February 2007.

[3] Pradip Lamsal, “Understanding Trust and Security”, Department of Computer Science University of Helsinki, Finland, October 2001.