Network and Information Infrastructure Availability

Marko Jahnke / Alexander Finkenbrink
Research Institute for Communication,
Information Processing and Ergonomics (FGAN-FKIE)
Neuenahrer Str. 20, D-53343 Wachtberg
Germany

jahnke@fgan.de / finkenbrink@fgan.de

ABSTRACT

The Network and Information Infrastructure (NII) serves as a backbone for the NEC paradigm. All interaction of entities in NEC – technical, policy or procedural – relies on the timely and reliable transport of information using the NII. In the near future, the NII will comprise different types of networks, including dedicated, leased, or even publicly available network segments from NATO and the nations. In these kinds of environments, the degree of infrastructure availability cannot longer be guaranteed with the existing technologies for different reasons. This contribution discusses these reasons, gives examples, and points out technologies and different ways of their application that need to be developed to support the future high availability of NII.

1.0 INTRODUCTION

The availability of a reliable network and information infrastructure (NII) is crucial for almost any functional entity within the NEC environment. Therefore, an appropriate degree of availability of resources is required providing an adaptive, timely and reliable processing/transport service for all information in the NEC environment, including information used for resource management. Resources include hardware (e.g., the end users node, routers, switches, servers, storage, wires, radios, microwaves, crypto devices), software (e.g., communication protocol stacks, messaging services, middleware, inter-process communication, applications, processes), and human resources (e.g., decision makers, field officers, system operators and management).

1.1 Definition

High availability is the (guaranteed) existence of the infrastructure at any time and place it is needed. High availability requires transparent resource management capabilities for providing the required level of service quality even with a degraded infrastructure (e.g., malfunctioning, usage failures, and while under Denial-of-Service/DoS attacks) and potentially in a cost-sensitive manner (e.g., using existing resources efficiently).

1.2 Relevance to Network Enabled Capabilities

The availability of the NEC infrastructure is (one of) the most important information assurance aspects of the NEC environment, because almost any interaction process between NEC entities relies on the availability of the infrastructure and the timeliness of NEC provided services, including:

- information sharing,
- cooperative command and control processes (example: friendly force tracking),
- trust establishment (mutual authentication of users, devices and software components),
- co-operative security services and management, including availability management,
- NII resource management information.

Depending on the importance of the interaction in military missions, an appropriate degree of infrastructure availability needs to be assured. As an example, the network needs to provide alternative resources which deliver the same requested level of transport and information service quality in case of a degraded infrastructure or unforeseeable circumstances. As long as such an assurance can not be given, the proper functioning of the processes on all layers (technical, user, organisations, and nations) can no longer be sustained.

From the operational point of view, most attention is paid to the availability of infrastructures and the integrity of the infrastructure management, whereas the confidentiality and the integrity of the transported data are of a lower priority. This is absolutely plausible, since the application of security services and their basic functions should to be transparent to the user. E.g., complex and inefficient access control mechanisms for users as well as for technical equipment may fulfil higher degrees of security requirements, but have a large negative impact on the total effectiveness of the Command and Control processes.

The aspect of efficiency in terms of investment as well as operational/maintenance costs will gain more importance in the future. Public and leased infrastructure parts of coalition networks need to be taken into account in order to assure end-to-end availability as many missions have economical constraints.

2.0 CHALLENGES

One of the most important challenges is to manage availability for ensuring operational critical availability service levels even if the network or infrastructure services are degraded. Certain signalling and monitoring information must be transported and processed under all circumstances. Also dynamic leaving and joining of entities in Federation of Systems (FoS) with different domains regarding, e.g., classification, ownership, trust etc., raises the degree of heterogeneity and thus it complicates end-to-end availability.

Current technologies for ensuring the availability of the different resources needed for providing a transport, information and management service for a required level of quality include many successful approaches. These include:

- co-operative computer and network defence (CND) and policy-enforcement measures,
- a high-level of redundancy in hardware and software, including fail-over-mechanisms,
- Quality-of-Service dependent applications which gracefully allow for less rich content depending on end-to-end bandwidth availability and minimum required QoS on capacity,
- trusted platforms and tamper protection and resistance.

These mechanisms provide a decent level of availability and service quality for parts of the infrastructure with respect to network overload and malfunctioning, DoS attacks, attacks against service integrity, and hostile jamming, as long as they work in a dedicated or homogeneous environment or in networks with already available interoperability. Since the NEC environment is dynamic and heterogeneous, the

challenge is to extend current technologies mentioned above.

The NEC environment will include many types of different networks and information processing systems, which differ in technical implementations (e.g., physical links), and in terms of ownership (e.g., nations, coalition, commercial, public). Such an environment no longer allows cross-network guarantees for issues like:

- complexity of an end-to-end risk analysis of the dynamically changing infrastructure in terms of, e.g., technology, operational routing, changing nodes, changing private connections, changes in coalition partnership,
- visibility of quality-of-service and capacity management of NII information transport tunnels from within the 'wrapped' information stream,
- increasing exposure to hostile disturbances attempts (more technologies to aim at),
- consistent and synchronised protection against largely scaled and distributed DoS attacks and jammed (wireless/mobile) links,
- possibilities to apply high-assurance hardware and software measures (e.g., for tamper protection and protection against unauthorised traffic on the network), and
- seamless interoperability of devices, services and management,

which are some of the basic requirements for ensuring a guaranteed level of availability and service delivery. Thus, the probability for inconsistencies in the degree of infrastructure availability becomes fairly high. This is due to many reasons, including the following:

- Along the information transport paths, many kinds of interaction between technical components are required to ensure the end-to-end availability, such as protocol signalling and exchange of management information.
- An automated and co-ordinated approach of responding to denial-of-service attacks against the NEC end-to-end infrastructure in a reliable, timely and flexible manner does not yet exist.
- A lack of a holistic view on risk management for highly dynamic NEC environments with a multitude of military and civil partners, and a multitude of chained communication elements.

3.0 RESEARCH

3.1 Summary of current and planned activities

Since the majority of the existing CND and policy management research efforts is spent on national and non-coalition oriented activities, only a limiting set of existing R&D approaches focus on the above requirements, such as Coalition CND [1], [2], [3] and Coalition Policy Enforcement [4].

Some de facto standards for data models and attack information exchange have been proposed [5], [6] and implemented in research prototypes [1], commercial products, as well as open source projects [11], [12].

Within the Trusted Platform Community there are several approaches, implementations, and products for establishing a trusted path from the user to the processor and the memory and thus to processing and storing information [7], [8]. Also an extended trusted path to IPSec [10] has been defined to extend the trusted information path in terms of confidentiality, integrity, and peer authentication. Techniques for protecting technical devices against various forms of tampering (e.g., cash dispensers, crypto communication devices, multi-purpose crypto processors) as well as electro-magnetic emission shielding techniques for physical communication media have been developed for many years and are still evolving

(see [9]). However, no significant efforts for expanding these ideas to a heterogeneous network environment are known.

Risk management [13] deals with the process of assessing risk values and developing strategies to manage risk factors in many application contexts, such as economics, general project planning, critical infrastructures and ICT security. Recent works focus on e.g., taxonomy-based methods for facilitating a systematic and reproducible identification of risk associated with software development projects [14].

In the area of QoS, DiffServ [15] has largely supplanted other mechanisms (such as IntServ) as the primary means of ensuring service in IPv4 based computer networks. Concerning IPv6, QoS is an integrated protocol feature (Traffic Class and Flow Label [16]) that promises a higher degree of end-to-end interoperability. IPv6 QoS is supported by some commercial available network equipment. Although there are approaches for ensuring the interoperability of the different QoS measures [17], passing QoS information across security boundaries, e.g., between the black and red side of crypto equipment and VPN, is still an open issue.

Multilevel precedence and pre-emption (MLPP, [18]) was developed for military communications, which is a priority scheme for assigning one of several precedence levels to specific calls or messages so that the system handles them in a predetermined order and time frame. MLPP encourages gaining controlled access to network resources in which calls and messages can be pre-empted only by higher priority calls and messages.

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

Obviously, many parts of the overall challenge are addressed by today's and near-future research efforts. However, they focus on network-wide highly available infrastructure components. From a holistic point of view, many approaches are not yet expanded to NEC specific application contexts. In other cases, the "glue" for filling the gaps between current solutions and the wider multi-organisational responsibilities and risk management is missing. Examples include the following:

- Although coalition-wide aspects of CND have been examined and several prototypical solutions have been presented, the support for automated and real-time capable reactions against largely scaled as well as synchronised digital threats (worms, botnets) is limited. This is not only a technical issue, but also a problem of existing co-operation policies in terms of CND.
- Since, e.g., trusted platform products are currently primarily focussed on personal or end-user systems, these technologies are not yet available for protecting network equipment. The situation is the same for tamper-proof devices which are mainly applied to financial equipment (e.g., Cash Dispensers). Although the basic technologies seem to be transferable, approved devices are either not yet available, or mutually accepted standards do not exist.
- Proper end-to-end Quality-of-Service signalling is not yet feasible for heterogeneous environments where different technical, administrative and security boundaries are crossed. Also the potential problem of adversary traffic flow analysis that can be performed on QoS information is not solved yet.
- Risk assessment and prioritisation render a complex task, especially if many types of different networks include different concepts, technical implementations, and legacy systems. Thus, the underlying model for mapping existing systems and networks reaches a huge level of complexity that cannot be handled efficiently.

These challenges might be induced by the fact that a multi-national NEC environment has not been identified as a commercial market potential. But as soon as experiments and prototypical solutions proof the basic feasibility of the NEC-adapted technologies, this situation may change significantly.

3.3 How can research address the challenge?

For achieving the above goals and filling the gaps between existing products, prototypes and approaches, developing solutions for the following aspects may help:

- coalition-wide co-operative automated and timely attack response mechanisms for heterogeneous network environments,
- high-assurance technologies and standards for protecting network equipment and communication media in order to provide a guaranteed level of transport and information service quality,
- applications that allow graceful quality-of-service being aware of current end-to-end QoS and bandwidth limitations,
- technologies for detecting and avoiding unauthorised traffic on the network that may have an positive impact on the transport and information service quality,
- interoperable cross-domain interaction interfaces for the above resources (hardware, software, management), including open standards,
- highly efficient and flexible (e.g. fully distributed) access control mechanisms for allowing access to authorised users even under degraded infrastructure,
- dynamic risk management end-to-end across multiple organisations in the NEC environment, i.a.w. how to use services without degrading or even jamming the total NEC network behaviour,
- technologies for out-of-band QoS signalling across black-red divides.

However, infrastructure availability alone does not increase the capability of the NEC operations, because an appropriate degree of availability of resources only provides an adaptive, fast and reliable transport and information service for both content and management information.

A supporting measure for respecting the heterogeneity, larger scalability, and dynamically changing topologies of future NEC environments might be the establishment of ongoing cooperative or distributed but synchronised experimental activities. The setups for these experiments should:

- be heterogeneous in technical implementations,
- comprise of different administrative and security domains,
- be oversized,
- be (partially) irrationally connected.

The experimental setups should contain components that are

- improvised (contain temporal solutions and fixes),
- malfunctioning,
- misconfigured,
- useless, or even
- misused, attacked or jammed.

Dealing with these kinds of setups may help to observe effects and to point out problems that would not arise when concepts and systems are designed and planned properly. The results of these experimental activities should be reviewed before new concept developments are launched. This might provide a systematic way to derive ‘lessons learned’ for new developments so that the according requirements can

be integrated in an early stage.

4.0 CONCLUSION AND RECOMMENDATIONS

A highly available NII is a key requirement for establishing NEC in NATO, member nations and missions. In order to provide efficient, secure and robust end-to-end transport services, future heterogeneous and large-scaled networks need better protection against service degradations due to malfunctioning, misconfiguration, abuse and attacks.

Our first recommendation is to revise existing research efforts. In many cases, existing and emerging technologies for ensuring end-to-end QoS, for obtaining a higher degree of infrastructure robustness, and for assessing, avoiding, detecting, and mitigating attacks against the infrastructure only need to be transferred and expanded to take into account the heterogeneity, the dynamically changing topology and the large scalability of future network infrastructures.

Our second recommendation is to engage more cooperative or distributed but synchronised experimental activities prior to developing concepts and implementations of security solutions, maybe as an ongoing campaign. These activities need to consider large-scale setups with differences in technical implementations and different administrative and security domains. It makes sense to make these setups larger than a rational concept would allow. Also the way of connecting parts of the setups should sometimes not follow rational guidelines. The setup should also contain ‘odd’ components, which may be improvised, malfunctioning, useless, misconfigured, or even misused, attacked or jammed.

5.0 REFERENCES

[1] RTO/IST Exploratory Team on Coalition Information Assurance Common Operational Picture (CIACOP).

[2] RTO/IST Exploratory Team on Incident Reaction (proposed activity).

[3] M. Jahnke, J. Tölle, S. Henkel und M. Bussmann. Components for Cooperative Intrusion Detection in Dynamic Coalition Environments. In: Proceedings of the RTO/IST Symposium on Adaptive Defence in Unclassified Networks, Toulouse, France, April 2004.

[4] G. Martínez Pérez, A. Gómez Skarmeta, S. Zeber, J. Spagnolo, and T. Symchych. Dynamic Policy-Based Network Management for a Secure Coalition Environment. IEEE Communications Magazine, Novembre 2006.

[5] H. Debar, D. Curry, B. Feinstein. Intrusion Detection Message Exchange Format - Data Model and Extensible Markup Language (XML) Document Type Definition. IETF RFC 4765 http://www.rfc-editor.org/rfc/rfc4765.txt.

[6] B. Feinstein, G. Matthews, J. White. The Intrusion Detection Exchange Protocol. IETF RFC 4767 http://www.rfc-editor.org/rfc/rfc4767.txt.

[7] Trusted Computing Group homepage. Online available at http://www.trustedcomputinggroup.org.

[8] Open Trusted Computing Consortium homepage. Online available at http://www.opentc.net.

[9] R. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. John Wiley and Sons, Inc. January 22, 2001. Available online at

http://www.cl.cam.ac.uk/~rja14/book.html

[10] S. Kent. R. Atkinson. Security Architecture for the Internet Protocol (RFC 2401). Online available at http://www.ietf.org/rfc/rfc2401.txt, 1998.

[11] Snort IDMEF - An IDMEF XML plugin for Snort. Online available at http://http://sourceforge.net/projects/snort-idmef

[12] Prelude IDS - The Hybrid IDS Framework. Online available at http://www.prelude-ids.org

[13] M. Van Horenbeeck, Annotated Risk Management Bibliography. Online available at http://www.daemon.be/maarten/riskannbib.html

[14] CMU Risk Management. Online available at http://www.sei.cmu.edu/publications/documents/05.reports/05tn036.html.

[15] K. Nichols, S. Blake, F. Baker, and D. Black. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers (RFC 2472). Online available at http://tools.ietf.org/html/rfc2474.

[16] S. Deering, R. Hinden Internet Protocol, Version 6 (IPv6) Specification (RFC 2460). Online available at http://tools.ietf.org/html/rfc2460.

[17] Cisco Systems, Inc. DiffServ - The Scalable End-to-End QoS Model, White Paper. Online available at http://www.cisco.com/en/US/pro ucts/ps6610/products_white_paper09186a00800a3e2f.shtml]

[18] Federal Standard 1037C: Glossary of Telecommunications Terms.