Secure Service Centered Networking for Nomadic Usage

Position Paper

Matthias Hollick
GMD - German National Research Center for Information Technology
Integrated Publications and Information Systems Institute (IPSI)
Department Mobile Interactive Media (MOBILE)
Dolivostrasse 15, D-64293 Darmstadt, Germany

matthias.hollick@darmstadt.gmd.de

Abstract Visions and expected predictions of future networking paradigms often include heterogeneous networks build upon an IP-based core. Future services form a key component within these networks and are expected to include support for nomadic and ubiquitous usage. This paper comprises a discussion of nomadic usage scenarios within service centered networks. Thereafter secure service discovery under nomadic conditions is explained by means of a model introduced in this contribution. This model embraces the nature of nomadic computing as *macro-nomadic* vs. *micro-nomadic* depending on the use case. As a conclusion unresolved problems concerning service security within the given boundaries will be presented.

Keywords Service Centered Networking, Security, Nomadic and Ubiquitous Computing

1. INTRODUCTION AND MOTIVATION

During the last decades computer systems and networks have been subject to frequently changing paradigms. In *Beyond Calculation: The Next Fifty Years of Computing* [DeMe1997], Gordon Bell and Jim Gray describe the evolution of computers and networks and estimate future usage. While the current situation is described in terms of "scalable networks and platforms" they envision a future where "all information services are pr ovided with a single, ubiquitous, digital dial tone".

This prediction emphasizes the value of ubiquitous services for upcoming networks. In fact, we assume that ubiquity can be reached by convergence among all networks with heterogeneity of parts of the network as a key factor (for an excellent treatment of the topic of heterogeneity in networks see [Schmitt2000]). Likewise, the paradigm of a unified services

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35413-2_36

R. Steinmetz et al. (eds.), *Communications and Multimedia Security Issues of the New Century*

infrastructure as described in the ICEBERG approach (see [RKJ2000]) stresses the importance of service centered networking.

How does this relate to nomadic computing? Which problems exist in the field of service usage and management and where is security involved? We assume that the near future will include more nomadic and mobile usage towards so called seamless and ubiquitous computing (see [Weiser1991]). Since nomadic computing entails the mobility of users and services it presents the ideal research platform for secure service centered computing on the way to seamless, pervasive and ubiquitous appliances.

In Section 2 we will present a nomadic usage scenario to further elaborate the claim made above. Section 3 will focus on security related issues in the field of service oriented nomadic computing. Section 4 concludes this paper providing a summary and addresses the own research to be carried out.

2. NOMADIC USAGE AND SERVICE CENTERED NETWORKING

As described earlier, nomadic usage covers a wide area of future application scenarios. Today's nomadic work situation can be best explained using an example (Figure 1 depicts a logical view on the involved network facilities):

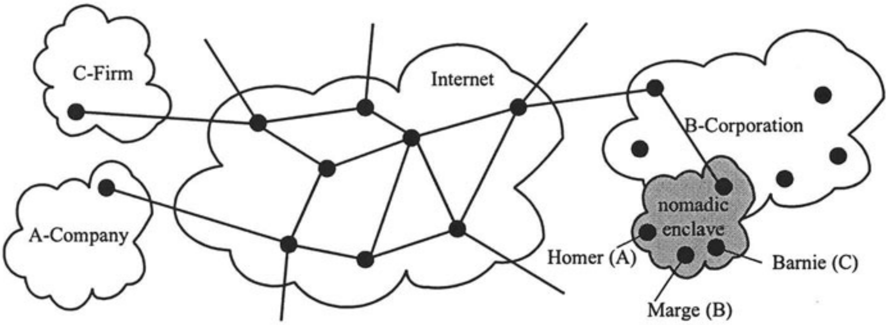

Fig. 1. Logical network topology for nomadic usage

A specialist (Homer) from the A-Company is hired to work in a project at B-Corporation for a limited period. He joins a development team to prototype some complex device. There are different other specialists from *supporting companies collaborating in the ad hoc working group to fulfil the mission. Due to the nature of the project, information has to be kept highly confidential, due to the projects complexity, experts from all over the world have to be consulted to provide parts of the solution.*

Homer needs to access services provided in his home network and in the foreign network. Hereby the nomadic nature requires changing (dynamic) service configurations as easily as possible. Moreover, Homer wants to exchange information with external specialists spread all over the world and not to forget with the other specialists in the project hosted at B-Corporation.

This collaboration involves a lot of support for additional service management. Nowadays, the services involved are far beyond from being easily accessible and manageable, neither in a centralized nor ad hoc based fashion. There are lots of distinct service provisioning protocols: Maybe A-Company uses Microsoft™ Active Directory™, whereas B-Corporation uses an ISO X.500 based address book. On purpose DHCP (Dynamic Host Configuration Protocol) provides for basic network configuration and DNS (Domain Name Service) is in place to allow for all internet based name resolution and provisioning of service information. Perhaps some more exotic proprietary or standardized service discovery protocols are in place: SLP (IETF's Service Location Pr otocol), Salutation™, the JINI™ Lookup Service or Bluetooth™ SDP (Service Discovery Protocol) may provide for service location in different fashion, all of them being widely incompatible.

To simplify the situation, we can break up the nomadic scenario mainly into two different usage styles:

- *Micro-nomadic* usage which includes the communication within the nomadic enclave.
- *Macro-nomadic* usage which includes the communication over wide-area networks.

Micro-nomadic usage can be described as highly dynamic. The workers taking part in the collaboration may frequently change. They possibly will request and provide new services during the project's lifetime. To further extend this bazaar like micro-nomadicity there may be personal communication among the workers (peer relationships) allowed. Let Homer exchange photos with Marge from B-Corp. but not with Barnie from C-Firm. With decreasing dimension of the network (e.g. in the nomadic enclave) we assume more bazaar-like structures and more direct communication, often based upon trust between individuals.

Macro-nomadic usage in contrast defines the large scale situation. The workers communicate using long term relationships with their home company or associated people. This resembles the situation between trusting parties. They operate there network based on more statically contracts and security-policies. Within the telephone network for example there are contracts between providers to allow for seamless handover and roaming.

To summarize, we expect mainly two usage patterns within nomadic computing environments: The more static macro-nomadic usage and the highly dynamic micro-nomadic usage. There may also be fuzzy transitions between both types.

To allow for nomadic computing to evolve towards future seamless collaboration it is necessary to provide new service paradigms enhancing and combining current approaches. Moreover, future approaches will have to deal with the wide variety of security issues.

3. SECURITY CONSIDERATIONS FOR NOMADIC SERVICE USAGE

In the following we will present means to relate current service security approaches to the already mentioned usage styles. Figure 2 depicts three prototypical use cases: anonymous, pseudonymous and trusted. Each of these (if having distinct security properties) has to be counter measured against security needs to allow for a complete treatment of the topic. For our investigation we will regard the set of *Authenticity, Integrity, Confidentiality, Nonrepudiation, Availability and Privacy* as the security needs.

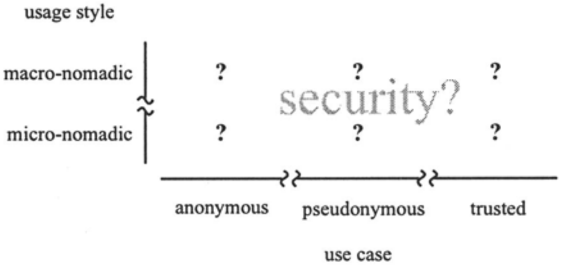

Fig. 2. Usage style of the network vs. use case for nomadic usage

The style of network combined with the intended use case accounts for the possible security mechanisms. For example in a macro-nomadic network the *trusted* usage can be regarded as default. The service provider may want to get paid for the service, if through trusted authentication likely in a postpaid manner, if pseudonymously likely in a prepaid fashion. Anonymous usage doesnt make sense here from the point of view of most service providers, the users on the other hand would like to have this security quality.

In micro-nomadic networks on the other hand, the trust may be more implicit or even impossible, here pseudonymous and anonymous usage will be more common, the ways of establishing trust depend on the situation.

As an example let's assume a trusted communication within an micro-nomadic network. Classical mechanisms (Needham-Schroeder, Otway-Rees, Kerberos) based on symmetric cryptography are likely to fail. There may be no common administrative authority to verify credentials or no ticket granting server available online. Public Key based solutions lack the feature for revocation if no certificate authority is available.

Authentication in ad hoc environments is also tackled with new approaches like the "Resurrecting Duckling" model in [StAn1999] or the general approach for ad hoc authentication in [ZhHa1998].

As a conclusion the above mentioned authentication schemes present parts of a brick towards secure nomadic service management in the area of authentication - in other areas, e.g. privacy, hardly any work has been done yet.

4. CONCLUSION

Bell and Gray state that "Telepresence for work is most likely to be the 'killer" app when we look back in 2047." [DeMe1997]. Even if this prediction will not come true, short term predictions and mid term visions explicitly or implicitly assume networks to evolve towards a more service centered and converging paradigm.

The area of nomadic usage connected with service centered networking is our approach towards seamless, pervasive and ubiquitous computing. Future work will concentrate on tackling problems in the field of service discovery and security to allow for nomadicity and thus including micro- and macro-nomadic usage.

Open research issues to allow for secure service centered networking include the provision of mechanisms to deal with the heterogeneity imposed by the two styles of networks mentioned throughout this contribution. Moreover, service discovery protocols are not restricted to the provision of service information from traditional style services. It has to be investigated whether the provision of information of "security services" reachable in the corresponding ad hoc environment is a feasible aspect for nomadic computing.

ACKNOWLEDGEMENT

This work is funded by the German Research Council (DFG) as part of the program Security in Information and Communication Technologies within the SECCO project.

REFERENCES

[DeMe1997] P.J. Denning, R. M. Metcalf, eds. *Beyond Calculation: The Next Fifty Years of Computing*, Copernicus, NY, 1997, ISBN 0-387-94932-1

[RKJ2000] Bhaskaran Raman, Randy H. Katz, and Anthony D. Joseph, *"Universal Inbox: Providing Extensible Personal Mobility and Service Mobility in an Integrated Communication Network",* Workshop on Mobile Computing Systems and Applications (WMSCA'00), Dec 2000

[Schmitt2000] Jens Schmitt, Heterogeneous Network QoS Systems, PhD-Thesis, Darmstadt University of Technology, Dec 2000

[StAn1999] Stajano, F. & Anderson, R., *The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks*, May 1999

[Weiser1991] Mark Weiser, *The Computer for the Twenty-First Century,* Scientific American, pages 94-100, Sep 1991

[ZhHa1999] L. Zhou and Z. J. Haas, *Securing Ad hoc Networks*, IEEE Network Magazine, vol. 13, no.6, Nov/Dec 1999