



Wireless World Research Forum (WWRF)

A Security and Trust Framework for a Wireless World: A Cross Issue Approach

Stewart Kowalski¹, Nick Edwards²

¹ Ericsson, Sweden
stewart.kowalski@ericsson.com

² BT, UK
nick.edwards@bt.com

Abstract—The vision of the Wireless World Initiative (WWI) is that in the future, advanced communications systems will enable easy access to information and services anywhere and at any time. These systems offer new applications, exploit both new and existing radio interfaces, and operate in a dynamic and reconfigurable way. Users will be interacting with other entities dynamically, so the potential risks may be significant. As these technologies develop, a fundamental aspect to consider from the beginning therefore is security and trust. This paper outlines the framework for security and trust that is being developed by the Ambient Network Work Package 7 Cross Issue team within the scope of WWI.

Index Terms—Requirements capturing, Security Frameworks, Trust Modeling.

INTRODUCTION

IN this paper we outline the framework for security and trust that is being developed by the Ambient Network Work Package 7 Cross Issue team within the scope of the Wireless World Initiative (WWI). The WWI consists of four EU 6th Framework integrated projects:

- Ambient Networks – creating the network solutions for mobile and wireless systems beyond 3G. It will enable scalable and affordable wireless networking while providing rich and easy to use communication services for all.
- WINNER (Wireless World Initiative New Radio) – developing a new radio interface with significantly improved capabilities in terms of performance, efficiency, coverage and flexibility.
- E²R (End-to-End Reconfigurability) – developing reconfigurable devices which offer an expanded set of choices to users including aspects such as management and control, download support, regulatory framework and business models.

- MobiLife – taking a user-centred approach to develop and deploy new applications and services with a focus on personalisation, privacy and trust, context-awareness and semantic interoperability.

The framework is being used as means to handle security and trust requirements between the different integrated projects and to describe, build and predict the security properties of future wireless communication systems.

The paper is divided into three major sections. In the first section we outline the basic conceptual building blocks of the security framework. We discuss how the high level security objectives of availability, integrity, confidentiality, accountability, privacy and assurance are related to the abstract security functions, which are deter, protect, detect/monitor, respond and recover. We give an example of how this “security matrix” is currently being used to compare and analyze both high level of low level security requirements between the different integrated projects.

Section two begins with a discussion of definitions and foundations of trust in the current literature. A number of aspects of trust such as its relationship to security, risk, identity, privacy and authorization, as well as the modeling and brokering of trust are reviewed. At the end of this section an approach for modeling trust within the WWI is proposed.

We conclude the paper with some reflection on current trends in systems security and how the proposed security and trust framework can continue to be adapted to deal with these new trends.

The Security Matrix

Capturing and coordinating security and trust requirements for future communication



Wireless World Research Forum (WWRF)

systems is a non-trivial task that faces a number of well known so-called “wicked problems” [1] that have been dealt with for a number of years with a number of notable failures and relatively few successes. The reasons for the large number of failures vary from general problems of systems requirement capturing to specific problems of security requirement capturing.

In order to deal with both these classical requirement capturing problems, the Ambient Networks Work Package 7 Cross Issue team is developing a matrix to capture and coordinate requirements between the integrated projects

At present the matrix is constructed using six high level security objectives as rows and six abstract security functions as columns.

Security Objectives

Objectives numbers 1-5 are adapted from *Underlying Technical Models for Information Technology Security* [2]. These cover a particular, well-proven tradition developing from the US Department of Defense Trusted Computer System Evaluation Criteria [3] with its focus on accountability, assurance and security policy (principally concerning access control and non-disclosure) through to the standardization of the Common Criteria [4] by ISO. Objective number 6 is included to cover a broad concern about the control of and responsibility for private information – data-traffic and location, principally.

1. Availability (of systems and data for intended use only)

Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users. This objective protects against:

- Intentional or accidental attempts to either:
 - perform unauthorized deletion of data or
 - otherwise cause a denial of service or data.
- Attempts to use system or data for unauthorized purposes

2. Integrity (of system and data)

Integrity has two facets:

- Data integrity (the property that data has not been altered in an unauthorized manner while in storage, during

processing, or while in transit) or

- System integrity (the quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation).

3. Confidentiality (of data and system information)

Confidentiality is the requirement that private or confidential information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.

4. Accountability

Accountability is the requirement that actions of an entity may be traced uniquely to that entity. This encompasses non-repudiation, and is related to authentication and access control.

5. Assurance (that the other objectives have been adequately met)

Assurance is the basis for confidence that the security measures, both technical and operational, work as intended to protect the system and the information it processes. Assurance is essential; without it the other objectives are not met.

6. Privacy

Privacy is the requirement of an entity to determine the degree with which it interacts with its environment, including willingness to share information about itself with others.¹

Continuum of Security Function

Security objectives can be achieved and maintained to a given degree of predictability against threat agents and processes by apply a number of different abstract security functions. In the cross issue team we are proposing a complete chain or continuum of security functions that begins with deterrence and ends with recovery.

1. Deter

Deterrence can be achieved using a number of different means depending on who or what the threat agents are. A

¹ There is still some discussion with the WWI cross issue groups as to the definition of privacy, and the definition here is given as a working example.



Wireless World Research Forum (WWRF)

simple banner warning on a WebPages can be used for some attackers while for advanced attackers, long encryption keys can be used to deter exhaustive key searches.

2. Protect/control

The two basic means to protect a system are either to allow or deny access to individuals or processes as they attempt to enter or use a system.

3. Detect/Monitor

Once the protection functions are covered, the next abstract security function is to detect individuals or process who have violated the protection or to monitor those individuals or process which have been granted access to the system and have the possibility to violate security procedures.

4. Respond

Once detection of a security event has occurred there must be functions in the systems to respond to such the event in an appropriate and timely manner.

5. Recover

If none of the security functions above have succeeded in stopping the threat agent or process there should be function in place to recover from a security violation.

Capture and Co-ordinate

The integrated projects that make up the WWI are currently in different stages of the security requirements capturing process. The Ambient Networks project has documented approximately 200 security requirements [5] while the Mobilife project has just started to formulate use case scenarios. The WINNER project has produced a draft report [6] with a

number of tables of security requirements. Table I is an extract from one of these tables.

The E²R project has produced documents containing over 30 security requirements from the three different perspectives: E²R systems perspective, Equipment Management Perspective and Network Support for Reconfiguration [7].

Below are three different examples of requirements taken from the three projects:

WINNER

- R3.1 Authorisation of valid subscribers
E²R Authentication of the User (4.1-1)
- In the case of reconfigurable equipment upgrade, the user/subscriber shall be authenticated.

AN Security R174

- Users should be able to use different types of authentication on different types of device e.g. biometrics with Ambient Network devices. Identity related equipment may need to be separable from communications equipment.

Table II is an example of how the security matrix is being used to map and label the different security requirements of the different project integrated project within the WWI.

As the integrated projects develop and the non-related security requirements become better and better understood, security requirements can be collected and sorted into the matrix.

Trust Modeling Definition, Foundations and

TABLE I
WINNER SECURITY REQUIREMENTS

| Require-ment | Asset | Threat | Requirement | Comment |
|--------------|--|--|------------------------------------|--|
| R3.1 | Access by mobile terminal to radio access network | Unauthorized access by mobile terminal | Authorization of valid subscribers | |
| R3.2 | Access by mobile terminal 1 to another mobile terminal 2 | Unauthorized access by mobile terminal 1 | Authorization of valid 'guests' | Peer-to-peer/Ad hoc networking, gaming, access to printers etc |

TABLE II
WORKING SECURITY MATRIX

| | Deter | Protect | Detect | Respond | Recover |
|----------------|-------|--|--------|---------|---------|
| Availability | | | | | |
| Integrity | | | | | |
| Confidentially | | | | | |
| Accountability | | Winner R3.1, R3.2 E2R 4.1-1 AN 174 | | | |
| Assurance | | | | | |
| Privacy | | | | | |

Modeling of Trust

A definition of trust [8] appropriate for the WWI is “the firm belief in the competence of an entity to act dependably, securely and reliably within a specified context”. In this definition, it is significant that trust relates to a “specified context”, as two parties may trust each other in one respect but not another. Trust implies a level of uncertainty and judgment (as indicated by the word “belief” in the above definition), which may depend on many factors, e.g. a party’s willingness to take risks, the cost of establishing an agreement, etc. Wilhelm *et al.* [9] define four foundations of trust within a communications context:

- Blind trust (depending on personal judgment or instinct)
- Trust based on a good reputation (e.g. a well known brand, or recommendations)
- Trust based on control and punishment (linked to contractual agreements)
- Trust based on policy enforcement

An additional foundation for trust within the WWI context is:

- Trust that a device or process will behave in a particular way based on its design.

When we discuss the concept of a trust model, it may have two different meanings:

1. A trust computation model, which is used by each single entity to manage the trusts that are relevant to itself, such as a probability and rule based model (a quantitative view)
2. A global view of trust relations between each pair of entities. This should be studied in the high-level design of a system (a qualitative view)

Both views are potentially important for the WWI. High level assumptions, for example, that an end user trusts his home network operator to provide a given service and to bill correctly for it may be fundamental. On the other hand, the ability for organizations base business decisions on real time assessments on trust is also important.

The WWI vision brings many new challenges:

- A very large number of network and service providers who cannot have bilateral service agreements (this means that one or more brokers will be required)

- A large number of parties may be involved in the delivery of a service to an end user (leading to complex dependencies). For example, a user may choose to purchase a service rather than network connectivity.
- The networks, applications and communications will be very dynamic. Entities will form new relationships rapidly with automatically negotiated agreements. Furthermore, even when an agreement is established, the trust relationship may change over time.

A new approach to trust modeling is therefore needed.

Transitivity and Brokering of Trust

If A trusts B and B trusts C, then does A trust C? This aspect of trust, transitivity, holds in some circumstances. Transitivity of trust is required within the WWI architecture when trust is brokered by a third party. This is of particular value where a large number of entities are involved because the number of relationships rises as the square of the number of entities, but with the addition of a single trust broker is linear, as shown in Fig. 1.

In practice it is likely that at least two trust brokers will be involved in establishing a relationship, because each entity will wish to

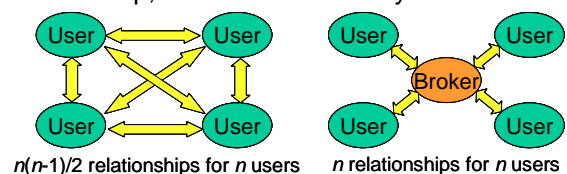


Fig. 1. Use of brokering to reduce number of bilateral trust relationships

choose its own trust broker. In addition to simplifying the process of establishing a relationship, a trust broker could also act as a guarantor (following models in the financial industry where trust is also linked to guarantees). An example of this might be that if a user establishes connectivity via a trust broker, the broker pre-pays the network provider and the user post-pays the trust broker.

Trust, Privacy and Identity

Trust is often linked to identity, and so will be underpinned by the identity framework used within the WWI. This may include



Wireless World Research Forum (WWRF)

hierarchical structures (e.g. X.509 [10]) or peer-to-peer approaches (e.g. PGP [11]). The use of cryptographically Generated Addresses is an approach for strengthening the identity role of network addresses. An IPv6 address can be cryptographically generated by computing a hash from a public key and other parameters. Only an entity that possesses the corresponding private key could have generated the address. Protection works without a certification authority or other security infrastructure [12].

There is often a trade-off between privacy and trust because an assessment of trustworthiness is often based on an entity's previous behavior. However, a user's privacy may be compromised if current activity can be linked to previous activity. The trust model developed for the WWI must therefore take account of privacy requirements e.g. use of pseudonyms or multiple identifiers associated with a single user. The use of a trusted third-party or reputation manager can help to avoid some privacy problems, as the third party can vouch for a user without requiring that their identity be revealed to a service provider. Specifications from organizations such as the Liberty Alliance [13] may be very valuable in providing mechanisms for management of personal information which respect an individual's privacy rights.

Bootstrapping

Information from which to base decisions about trust will often require the channels of communication which are at that point not negotiated or established. For example, how can a user check the reputation of an access network provider without connectivity e.g. to a reputation server, certificate repository, etc? Security must be carefully considered here, e.g. a possible denial of service attack exists where a client repeatedly asks for trust credentials.

A Proposed Approach to Trust Modeling in the WWI

It is important that the WWI leverages the wealth of literature in many fields of trust modeling. Aspects of trust have been studied extensively with respect to mobile ad-hoc networks (MANETs) [14]. In particular, reputation systems which enable experiences of users to be shared with others have been analyzed. MANETs are a challenging

environment for such systems because they are dynamic and have no fixed infrastructure or widely trusted entities. Trust management systems such as Keynote [15], which allow an entity to check whether a particular action conforms to a security policy, will also be important for the WWI.

Selezynov *et al.* have developed an agent-based middleware architecture for distributed access control [16], specifically designed for use in an ambient computing environment. Here, negotiations occur between mobile user agents, that protect user interests, and authorization agents, which protect network resources. The system allows automation of trust establishment and maintenance of trust in a dynamic environment, and supports user privacy through the use of pseudonyms.

A combination of peer-to-peer information and centralized systems is likely to be the key to trust in the WWI.

It is assumed that for any pair of actors, the level of trust with respect to a particular context will vary according to actors, context and time. As with security a "trust chain" can be considered for any relationship where different aspects of trust are relevant:

- **Design**
Design choices can affect levels of trust required e.g. minimize trust needed through flexible charging, optimize efficiency by allowing high level of trust
- **Base**
Obtain and calculate information on which trust decision can be based (either raw information or calculated trust scores)
- **Present**
Communicate trust related information from one entity to another (including presentation of information to an end-user)
- **Establish**
Establish a trust relationship e.g. defining context and entities
- **Maintain**
Maintain and monitor a trust relationship
- **Recover**
Repair a broken trust relationship

A matrix can thus be formed where elements of the value chain are considered against different foundations of trust. The advantage of this approach is that it can highlight areas where further consideration is



Wireless World Research Forum (WWRF)

required concerning trust, or areas where trust has not been approached consistently. There are many elements that will be necessary to support trust in the WWI, e.g.:

- An identity framework for identification of entities
- Trusted third parties for maintenance of user privacy
- Trust brokers will be needed for facilitation of relationships formation between entities
- Reputation systems for acquisition of trust information and calculation of trust scores
- Common standards for communication of trust information to end-users

One benefit of having a flexible infrastructure where many parties are involved is that it means that the detailed implementation of some aspects of trust establishment may be leveraged from other work. For example, the WWI does not necessarily need its own reputation system: provided that the WWI infrastructure allows a reputation system to gather the necessary information with high integrity on which to base its calculations, and a mechanism to deliver this information as required. The advantage of this approach is that it allows the best-of-breed solutions to be adopted.

Conclusion

Internet security has been steadily developing over the last 20 years. Originally the Internet was a research network, so most threat agents were deterred by group pressure within the research community. As the group grew larger, protection and detection developed into product areas such as firewalls and intrusion detection systems (IDS). Today there is great deal of industrial effort in the Internet industry to develop products which can respond to attacks and provide automatic recovery, as well as efforts to strengthen accountability mechanisms.

Security for the wireless world has also been moving back and forth along the security continuum of deterrence to recovery. Encryption is now widely used to protect data as it is transmitted over the air, and is now being introduced into the core network and used by applications for end-to-end confidentiality. Personal firewalls are being

introduced to mobile phones [17] and it is only a matter of time before personal IDS are also included into phones. What we see by these trends is that security and trust in communication systems is a never ending story that is constantly changing to deal with similar (but not necessarily new) types of threats and threat agents. By providing a storyboard or framework with fixed objectives and high level abstract security function we believe that we can capture, coordinate and model security and trust requirements within the WWI in a systematic way.

ACKNOWLEDGMENT

The authors thank members of the Ambient Networks Security Work package team and the WWI Security Cross Issue Team for the valuable discussions which have contributed significantly to this work.

This document has been produced in the context of the Ambient Networks Project. The Ambient Networks Project is part of the European Community's Sixth Framework Program for research and is as such funded by the European Commission. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Ambient Networks Project or the European Commission.

REFERENCES

- [1] H. Rittel, M. Webber, "Dilemmas in a general theory of theory of planning", *Policy Sciences*, 4, 1973, pp. 155-169.
- [2] *Underlying Technical Models for Information Technology Security*, NIST Special Publication 800-33, 2001. Available: <http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf>
- [3] *Department of Defense Trusted Computer System Evaluation Criteria – 'the Orange Book'*, 5200.28-STD, 1985.
- [4] *ISO 15408, Common Criteria for IT Security Evaluation*, 1999. Available: <http://csrc.nist.gov/cc>
- [5] G. Kleinhuis *et al.*, "Security Concepts, Requirements, and Architectural Principles", Internal Ambient Networks Report R-7-1, 2004.
- [6] J. Nyström, "Winner Requirements for Security and Trust", WINNER Internal Report, 2004.
- [7] R. Falk *et al.*, *E²R security Requirements*, WWI Internal Report, 2004.



Wireless World Research Forum (WWRF)

- [8] T. Grandison and M. Sloman, "A Survey of Trust in Internet Applications", IEEE Communications Surveys and Tutorials, 2000. Available: <http://www.comsoc.org/livepubs/surveys/public/2000/dec/grandison.html>
- [9] U. G. Wilhelm, L. Buttyán and S. Staamann, "On the Problem of Trust in Mobile Agent Systems", Internet Society's Symposium on Network and Distributed System Security, 1998. Available: <http://www.isoc.org/isoc/conferences/ndss/98/wilhelmsl.pdf>
- [10] "Information Technology — Open Systems Interconnection — The Directory: Authentication Framework", ITU-T Recommendation X.509 version 3 (1997), ISO/IEC 9594-8, 1998.
- [11] PGPi Project "How PGP Works". Available : <http://www.pgpi.org/doc/pgpintro/>
- [12] T. Aura, "Cryptographically Generated Addresses (CGA)", work in progress, IETF, 2004. Available: <http://www.ietf.org/internet-drafts/draft-ietf-send-cga-06.txt>
- [13] T. Watson, "Liberty OD-FF Architecture Overview", 2004. Available: <http://www.projectliberty.org/specs/liberty-idff-arch-overview-v1.2.pdf>
- [14] J. Liu, V. Issarny. "Enhanced Reputation Mechanism for Mobile Ad Hoc Networks" Proceedings of the Second International Conference on Trust Management (iTrust'2004), 2004. Available: <http://springerlink.metapress.com/openurl.asp?genre=article&issn=0302-9743&volume=2995&spage=48>
- [15] M. Blaze, J. Feigenbaum, J. Ioannidis, A. Keromytis, "The KeyNote Trust-Management System Version 2", ETF RFC 2704, 1999. Available : <http://www.ietf.org/rfc/rfc2704.txt>
- [16] A Seleznyov, M. O. Ahmed, S. Hailes, "ADAM: An agent-based middleware architecture for distributed access control", 22nd International Multi-Conference on Applied Informatics. Available: <http://www.cs.ucl.ac.uk/research/mars/papers/adam.pdf>
- [17] *Wireless Developer Network*, "F-Secure Provides Nokia Phone Users With Mobile Antivirus Solution", 2004. Available: <http://www.wirelessdevnet.com/news/2004/sep/27/news4.html>