Trust areas: a security paradigm for the Future Internet

Carsten Rudolph

Fraunhofer Institute for Secure Information Technology – SIT
Rheinstrasse 75, Darmstadt, Germany
Carsten.Rudolph@sit.fraunhofer.de

Abstract. Security in information and communication technology currently relies on a collection of mostly un-related and un-coordinated security mechanisms. All in all, the end-user has no chance to get a good perception of the security properties satisfied for actions she is executing in the Internet. Classical approaches (e.g. perimeter security) do not work in open and heterogeneous communication environments. Federation of single security mechanisms only works for particular applications and for a small subset of security properties. Thus, new views on trust and security are required for the Future Internet. This vision paper proposes the concept of *Trust Areas* as one candidate for a security paradigm for the Future Internet and identifies some open research challenges.

1 Introduction

Security in IT systems relies on the existence of trust relations. Bi-lateral trust relations are often sufficient for secure applications. However, already in communication networks existing today such bi-lateral trust relations are not efficient and in a large scale impossible to be managed. Thus, hierarchical or federated security infrastructures have been established. Such security infrastructures are then used to define more or less static relations for VPNs, client-server applications, or network access control. So far, this approach provides a reasonable basis for the development of secure systems [1]. Nevertheless, converging networks on all layers from hardware (one device with all types of communication interfaces) to the applications (software as a service, cloud computing) creates a new networking landscape.

Current IT Infrastructures (the Internet in a wide sense) consist of various protocols, different underlying technologies to connect devices, transmit data, and different layers of distributed applications. Some of these technologies and protocols are transparent from a user's point of view. This trend towards transparent use of heterogeneous technology will continue towards seamless applications. In the long run, it will evolve to a converged infrastructure, the *Future Internet*. Thus, in the Future Internet we expect that in many cases users and also applications are indeed unaware of the underlying technology used. Therefore, the Future Internet will in fact consist of physical communication channels under the control of various network operators and a variety of overlay networks

such as low-level peer-to-peer infrastructures, industrial control networks, virtual private networks, service infrastructures, cloud computing infrastructures, logical backbones, or special purpose networks (e.g. for online gaming). In this Future Internet security infrastructures need to be open, flexible, cross-domain and ubiquitous. Further, user and device shall be clearly distinguished and users must have the possibility to be in full control of their data and to decide which other users or devices will get hold of this data.

Boundaries will disappear on physical and technical communication layers but also on the logical level of applications and services. Current security solutions are similar to building gated communities in the real world. Federation means that identification for one gated community is accepted by others and, in the best case, there are secure ways to get from one community to the other. However, in the Internet it is not possible to draw clear boundaries and to always make users aware of these boundaries. Similar to the physical world, security cannot be guaranteed.The approach of virtual gates and walls currently works more or less for enterprise networks, although even those are divided into distinguished network zones.The situation is even more complex in the more open Internet. Security issues go way beyond federating authentication and encrypting communication channels. Some of the relevant keywords include privacy, data collection and aggregation, user profiling, use of processing and storage power of clouds to build huge data-bases, confidentiality of personal data, accounting, money, economical processes. Many other topics could be mentioned. Additionally, the attack landscape is also changing towards more targeted attacks and advanced persistent threats that can be in place unnoticed for a long time before they become evident. Such attacks can be the vehicle of organized crime to cause high financial damage.

This position paper introduces the vision of a security paradigm for the Future Internet, the so-called multi-domain *trust areas*. These trust areas formulate the goal of suitable security infrastructures for the Future Internet. Multi-domain trust areas shall not replace existing security infrastructures, but shall complement and be combined with identity management, PKIs, security information and event management and other existing technologies. However,trust areas provide a new view on scope of trust relations and the required (and possible) flexibility of security mechanisms and also of the necessary awareness and security perceptions on the side of the end-user. The notion of trust areas can provide guidance for future research on trust and security in the Future Internet.

2 The vision of multi-domain Trust Areas

A fully secure Internet will remain an illusion (similar to overall security in human societies). However, in the "physical" world people have a perception of the risks they are exposed to. In a town, one can know which areas are safe and secure and which areas shall be avoided. Moreover, in physical social networks trust relations are established (often depending on behaviour, look, and "gut feeling") and identification is achieved by various non-technical means. All

these naturally human techniques cannot be easily transferred to the Internet. Nevertheless, for the Future Internet people will also build some kind of trust and security perception related to their actions in the Internet. Security and trust mechanisms need to support the establishment of such a perception in a way that it enables users to know what the risks are. Consequently, in contrast to existing information and communication technology (ICT) infrastructures, the Future Internet shall provide inherent support for trust and security in terms of so-called multi-domain *trust areas*. The next paragraphs provide a first definition of this term and the related concepts.

Trust Historically, various different notions of trust can be found, each addressing particular aspects of ICT systems, e.g. trust in electronic commerce systems based on reputation and recommendation, or trust in public key infrastructures. While these notions support the understanding of trust establishment and degrees of trustworthiness in their respective application domains, they are insufficient for the more general notion of trust.For the notion of trust areas the term *trust* expresses the view of a particular entity or agent of the system on particular (security) properties of a system [4].

Area For many applications, it is not necessary that trust relations are established with a huge number of entities. Trust is relevant for a particular set of entities that is actually involved in a process. In many scenarios, such a subset can be open and dynamic. The appropriate term for such an open set is the term *area*. For motivation of this choice compare with the entry in Merriam Webster:[1]

> **Entry Word**: area. **Function**: noun. **Meaning**: 1. a part or portion having no fixed boundaries 2. a region of activity, knowledge, or influence.

In the context of the Future Internet, the *area* denotes an open set of physical and logical entities, such as network components, services, but also identities or actions executed within a particular process.

Multi-domain In current ICT networks and even more in future ones security cannot easily be build on central trusted authorities. In contrast, only subsets of network components, applications or other entities can be under a common control with respect to those properties that someone might want to trust. A set of network components and applications under a common control is now denoted with the term *Domain*. It should be noted that with respect to different properties to be trusted a single entity can belong to different domains at the same time. Processes will be *multi-domain*, i.e. they will cross different domains. Domains can intersect and that a multi-domain area not necessarily completely includes all domains it touches.

[1] http://www.merriam-webster.com/thesaurus/area

Multi-domain trust area

> A *trust area* is defined as an open cross-layer section of a heterogeneous ICT network (i.e. the Future Internet) with the following properties:
> - Users can be aware of the actions and processes they can do without leaving the trust area.
> - Security mechanisms exist that enable users to make a well-founded decision on which security properties can be trusted with respect to the actions and processes executed within the trust area.

It should be noted that trust areas are not "Secure Areas". Users need to be able to achieve a good perception of the security properties satisfied for particular actions and also of the risks involved. Also, view on security properties within the trust area can be very different for different users depending on their view and knowledge.

A trust area should cross many layers and exist orthogonal to different overlay networks. Within a trust area, users should be able to establish trust relations and users can know and can be made aware of what they can securely do and what the risks are. The concept of trust areas can be compared to a social community (or a town) where citizens know whom to trust and in which areas they can securely and safely live, shop, dine out, and in which area they should be more careful. The Future Internet shall support a trust infrastructure with inherent support for trust areas as well as trusted means to provide situational security awareness for the users.

3 Research tasks and challenges

Trust areas require new combinations of existing security mechanisms and possibly the development of totally new approaches in particular for supporting the users' perception of security.Clearly, a trust area will not be something monolithic. Some of the open issues to be approached are given in the following paragraphs.

Identification and expression of typical actions and processes with their trust and security needs A careful study of cross-domain activities in the Internet with an identification of the trust and security needs of different stakeholders should give a first idea of the scope for trust areas. In addition to the obvious security properties of confidentiality, authentication, integrity and non-repudiation, some of the interesting issues to look for are accounting (e.g. world-wide cross-domain roaming services) and responsibilities (e.g. who is responsible for financial losses, breaches of national and international laws).

Identification of available security and trust mechanisms *and their evolution* A second parallel step needs to create a map of available security and trust mechanisms. As a trust area is not a new mechanism itself it needs to rely on a proper use of existing mechanisms and might also motivate research on totally

new mechanisms. Examples of mechanisms trust areas can rely on include basically all existing and efficiently deployed security mechanisms, such as TLS/SSL for web interfaces, S/Mime for e-mail, web-service security, ticket-based authentication, token-based authentication, electronic ID cards, closed sub-networks, cryptographic protocols for WLAN, VPNs, actively monitored and controlled services, or hardware-based security. In addition to these technical solutions, trust areas can also be influenced by other non-technical things, e.g. contracts and service-level agreements or legal regulations and their enforcement. The Future Internet will continuously evolve and new attack vectors will appear along with new business models. In parallel, one can also expect new security mechanisms to be developed. Thus it will be necessary to establish advanced types of distributed security management for trust areas, including means for an adaptive evolving configuration of security measures according to the evolution of the infrastructure and overlay networks and the situational knowledge about current threats and malicious activities.

Combinations of security mechanisms / trust area security processes Trust areas need to cross different domains and also different physical and/or overlay networks. Thus, it will be necessary to combine different security mechanisms in order to achieve assurance for particular actions or a process within the trust area. These combinations itself, but also the visualisation towards the user and the usability of the combined solutions represent one of the more difficult challenges for the realization of trust areas. Some approaches exist on the level of security patterns and also for automated reasoning on security properties and logical security building blocks. However, in general the combination and integration of security mechanisms needs more fundamental work.

Integration into Future Internet applications and platforms Once the vision of trust areas is developed into a more concrete set of mechanisms, one next step is the integration into applications in order to make users aware of trust relations and enable the users to make well-informed decisions on their actions in the Future Internet with respect to security properties. Network components or network parts might need to provide security information for trust areas (the reliable, secure Internet backbone). Second, network components (routers, switches, but also servers) can have their own more technical view of trust areas and policies can influence the behaviour of these components relative to the current parameters of the trust areas they are in.

Usability and awareness: expressing trust and security / visualisation In the physical world, trust is often a result of relatively clear parameters combined with a "gut feeling". This human perception needs to be replaced with some user interaction with clear semantics. The trust status with regard to a user's current actions needs to be visualised in an intuitive but not over-simplified way. The "SSL lock" in the browser window is not sufficient. One should expect users to be able to cope with visualisations as complex as international traffic signs.

Further, a proper classification and description of security properties with clear semantics is necessary. Such a classification could be based on existing frameworks for security modelling [2, 3, 5, 6]. However, the property description needs to express all relevant parameters (e.g. the local view of the user, underlying security assumptions and underlying trust assumptions).s.

4 Conclusions

This vision paper introduces the notion of trust areas as a proposal for a new vision of security and trust in the Future Internet. This notion can be a vehicle for a more targeted discussion on trust and security issues and can also guide future research in this area. One essential component of trust Areas is the information of the user about the security properties related to the actions she wants to execute in the Internet. Obviously, this information can be quite complex. Therefore, one main task in addition to the technical realisation of security mechanisms is the visualisation of security properties shown in the context of processes and actions executed in the past or to be executed in the future.

References

1. R. J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, 2008.
2. R. Focardi and R. Gorrieri. *Classification of Security Properties (Part I: Information Flow)*, volume 2171. Springer, lncs edition, 2001.
3. R. Focardi, R. Gorrieri, and F. Martinelli. *Classification of Security Properties (Part II: Network Security)*, volume 2946. Springer, lncs edition, 2004.
4. A. Fuchs, S. Gürgens, and C. Rudolph. A Formal Notion of Trust – Enabling Reasoning about Security Properties. In *Trust Management IV: 4th IFIP WG 11.11 International Conference, IFIPTM 2010*. Springer-Verlag, 2010.
5. S. Gürgens, P. Ochsenschläger, and C. Rudolph. On a formal framework for security properties. *International Computer Standards & Interface Journal (CSI), Special issue on formal methods, techniques and tools for secure and reliable applications*, 27(5):457–466, June 2005.
6. H. Mantel. Possibilistic definitions of security – an assembly kit. In *Proceedings of the IEEE Computer Security Foundations Workshop*, pages 185–199, 2000.