# On the Future of Security in Future Internet

Peter Schoo
Fraunhofer Institute for Secure Information Technology SIT,
Network Security and Early Warning Systems
Parkring 4, 85748 Garching near Munich, Germany
Email: peter.schoo@sit.fraunhofer.de

One of the recognised deficiencies of the Internet is that security was not considered in the Internet design early on to the extend it is required today.

> *Although military security was considered when the Internet architecture was designed, the modern security issues are much broader, encompassing commercial requirements as well. Furthermore, experience has shown that it is difficult to add security to a protocol suite unless it is built into the architecture from the beginning.* (RFC 1287)

Both the experiences made with the Internet as recognized by the IETF community, and the infrastructure dependencies that were created in our societies using the Internet, indicate strongly that this should change in the future: the design of Future Internet has to consider security as one of its chief ingredient. This has been recognized since the early discussion of the Internet renovation [1], [2] and is continuously repeated. In fact, any discussion about Future Internet without also discussing security will not be sufficient.

## I. Future Internet

An encouraging research environment can be enjoyed since a while now, in which a variety of new approaches were researched and contributions have been made. Some of them build on the existing Internet and its deployed technologies. These consider migration from Internet as of today towards future improvements. Others follow the Clean Slate approach, i.e. redesigning the Internet from ground. All these approaches are understood to progress towards the Future Internet. However, these approaches need also to explain about their contributions regarding improved security, at least to the level existing in todays Internet.

## II. Design principles

For designing and building Future Internet there are some design principles to, in the widest sense, improve the protection and availability of such systems. Derived from the shortcomings of the Internet as we see it today, such principles address overall goals:

- Reliable authentication and authorisation,
- communication integrity, or even confidentality,
- misuse prevention, and
- ensuring availability.

Building on these overall goals, design principles will be presented at the workshop that can be grouped into general, architectural, protocol and operational security design principles.

These principles can not be applied straight forward, as their application needs consideration of and rationalization within the technology of the specific Future Internet approach they are applied to. They depend on the actual technology as well as non technical influences as e.g. legal liability for held communications.

## III. Instruments

It can be observed that individual proposals for Future Internet sometimes encompass some consideration of some security aspects. While such considerations are already advantageous they are in most cases not sufficient, since a holistic view on the security aspects and an approach based on some qualified methodology are missing, which enable and assist to derive comprehensive solutions. Well suited and proven instruments that help achieving comprehensive security engineering are:

- cryptography as the major security tool,
- mechanisms protecting data in communication,
- software and hardware security, and
- (organisational) processes maintaining the level of protection.

Moreover, building on standard security solutions actually reduces R&D risks and costs, and experiences helps to apply these instruments effectively and efficiently.

## IV. Caveat and Summery

In this workshop contribution, wanted security properties and design goals are suggested addressing industrial applicability of the results of current research on Future Internet. The major instruments to implement such goals complete the discussion. Though finding suitable security solution is not an easy task, early consideration how to design and integrate protections is clearly indicated as we see demands on Internet today. Retrofitting security has shown to lead to suboptimal results only.

## References

[1] D. Clark, K. Sollins, J. Wroclawski, D. Katabi, J. Kulik, X. Yang, R. Braden, T. Faber, A. Falk, V. Pingali, M. Handley, and N. Chiappa, "New arch: Future generation internet architecture," Defense Advanced Research Projects Agency (DoD), Information Technology Office (ITO), Tech. Rep., 2003.

[2] D. Clark, L. Chapin, V. Cerf, R. Braden, and R. Hobby, "Towards the future internet architecture," Internet Engineering Task Force, RFC 1287, Dec. 1991. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1287.txt