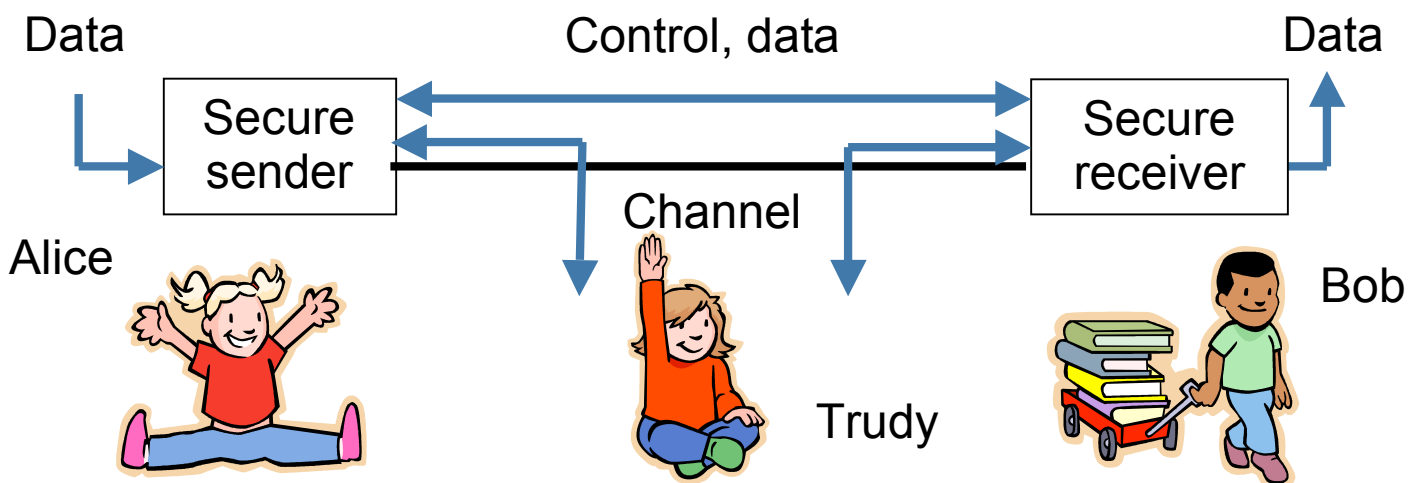


Lecture Notes

IT Security in Networks



Julia Stoll

Spring 2007

IT Security in Networks

Julia Stoll, Spring 2007

Brief Course Description

In the course *IT-security*, we focus on the *practical needs* in small, middle-sized and partly large *companies*, where an IT-security manager is responsible to establish a *safe and secure IT-system* based on intranet technologies, Internet and Web technologies, and WLAN-technologies. Note that the focus is on distributed working environments. IT-security therefore is *not only a technological problem*. We must focus on planning and managing using the IT-security typical *plan-protect-respond cycle (PPR-cycle)* as well.

We start with the determination of fields and problems in IT-security in a distributed environment. We distinguish between *safety, security, protection and privacy* as terms to characterize the common problems in intranet and the Internet. Additionally, we give a brief introduction to questions of legislation and regulations in the European Union. *Safety* is of an IT-system is implemented by its functionality of subsystems (and/or components) to its specification. *Security* is the inherent property of the considered systems to guarantee that system states are only reached as specified. *Protection* is the property of the considered system to guarantee that nobody is allowed unauthorized access to system resources, including data. (Right of) *Privacy* is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations. Obviously, privacy is not a technical task, but it has surely to be taken into account, if we discuss personal communications all over the world established network infrastructures.

After an introduction to the main terms and open questions of IT-Security by *analyzing typical attacks (viruses, worms and Trojan horses) over the WWW*, we consider system architectures to obtain a secure and safe communication process across different networks. Therefore we study networks architectures and network protocols, like TCP/IP standards versus ISO/OSI reference model. The main task is on layer cooperation. This requires that we review IP, TCP, UDP and ICMP from an IT-Security viewpoint. Why they are unsafe and insecure? Why can protection not be guaranteed? What does it mean for privacy? The question, what can we do to obtain safe communication structures, leads us to the next main topic: HW-infrastructure to obtain secure networks.

As a consequence it is our focus on *firewalls and host security*. The stepwise process to become a secure IT-system infrastructure is called hardening. What can we do to harden our systems? We consider firewall hardware and software. We study firewall techniques, like static package filtering, state-full firewalls, NAT and application firewalls to understand firewall architectures in relation to our IT-system architectures. Host security is based on the considerations of host installation and patching, turning of unnecessary services, managing users, groups and permissions. Beside advance server hardening techniques we consider hardening of clients.

A safe network is not necessarily secure; the reader might check the terms above. To obtain *data security* we talk about encryption for confidentiality. Confidentiality is supported by symmetric key encryption as well as public key encryption. We discuss both models and processes of these encryption methods. They are different! Observe that property of authentication is also guaranteed by encryption methods, but the underlying process requires other algorithms again. We discuss digital signatures. After the introduction of cryptographic

systems we study the software tools and their functionality to implement data security. This means we consider SSL/TLS, PPP, PPTP, and L2TP, IPSec and Kerberos.

In the final part we review our knowledge, which we will get so far by the study of incident and disaster response, including IDSs. We review and develop *guidelines* to obtain a safe and secure IT-system located in networks, including policies, risk analysis and control principles for IT-security.

Content of the Fontys booklet

These materials consist of a set of slides presented in the lectures. The lecture notes are divided into five parts:

1. An introduction to explain why IT-security is a hot topic,
2. Definition of basic terms, the analysis of typical IT-security problems and its consequences,
3. Networks and firewall technologies,
4. A brief introduction to data security, and finally
5. IT-security guidelines.

Some references

- [1] Federal Office for Information Security (BSI): <http://www.bsi.de/english/gshb/guidelines/> (BSI's IT-Grundschutz Manual, 2004)
- [2] C. Eckert: IT-Sicherheit. Konzepte-Verfahren-Protokolle. Oldenbourg Verlag. München, Wien. Oct. 2004.
- [3] U. Moser: Sicherheit in applizierten Rechnern (SIAR). Lecture Notes, FH Konstanz 2003.
- [4] R.R. Panko: Coporate Computer and Network Security. Pearson Education Prentice Hall, Australia, Dec. 2004.
- [5] M. Penttonen: Data Security. Lecture Notes, Dept. of Computer Science, University of Kuopio. <http://www.cs.uku.fi/~penttone/secu2003> , 2003.
- [6] M.-T. Tinnfeld: Einführung in das Datenschutzrecht. Oldenbourg Verlag München, Wien 2004 (4.Aufl.)