The Basics

The research-group "Institut für Telematik" of the department for computer-science at the University of Trier is a research and development-center formally administered by the Fraunhofer Society and was established on January 1, 1998 and has since then evolved into an ever-growing competence center that develops solutions for problems in the interfaces between telecommunications and information technology. Around 30 scientific staff members from various countries who are experts in different areas of science are currently with the institute.

The scope of the working group "Institut für Telematik" covers a wide spectrum: From application-oriented information technology and telecommunications research to the development of customized solutions and pilot systems for commerce, industry, medicine and administration. It is also focusing on new media training and continued education, which is offered to cooperation partners as well as employees of companies domiciled in the region and in other areas.

Project Partners

High tech businesses, as well as large and even small and medium sized companies support the institute as project partners. The partner firms implement the institute's scientific findings in practical applications. The focus of the work is on the development and utilization of new information and communications media for technical, medical and social applications.

Areas of Competency

The current research and development projects aim at the practical implementation of the latest scientific findings in the areas of electronic publishing, Internet/Intranet, tele-medicine, secure data transfer, system development and analysis. The Institut für Telematik focuses primarily on the following technological applications:

- Editor systems: Web-based information and knowledge management
- Navigation systems: Processing of information, data interfaces, EAI, data warehouse
- Database management: Innovative middleware on open standard basis, e.g., Smart Data Server (SDS)
- Open network security: Architecture, policies
- Network security: Firewalls, Lock-Keeper, Tiger Teams, CERT
- Content security: Public-Key-Infrastructures, digital signatures
- Mobile technologies and applications: Ubiquitous Computing, Mobile Security, ad hoc-Networks, Smart Cards
- Tele-medicine: Patient CD, DICOM-image management and compression,
- Consulting: Studies, evaluations, audits

Patent Protection has already been awarded to the institute for two of its solutions: <Lock-Keeper> – a security <sluice> between Internet and Intranet, that protects users more effectively against online attacks than firewalls – and <Dicomzip> an image compression process that reduces the transmission times of medical images from several hours to just a few seconds.

Universität-Trier

Institut für Telematik

Hightech-Forschung rund ums Internet

IT Security Analysis

FG Institut für Telematik
Bahnhofstr. 30-32
54292 Trier, Germany
Telephone: +49 (0) 651 - 97551 - 0
Telefax: +49 (0) 651 - 97551 - 12
E-Mail: info@telematik-institut.de
Internet: www.telematik-institut.de

Head of working group:
Univ.-Prof. Dr. sc. nat. Christoph Meinel

IT Security Risks

The number of uncovered vulnerabilities of IT systems is growing constantly. In the following, a few selected problem areas are described that we check during the analysis of your IT infrastructure.

Attacks Against Web Servers

In recent years, the formerly simple web servers have become comprehensive application servers that perform a broad range of tasks. Due to their significance for the presentation of companies in the Internet and the large number of known security holes, web servers are preferred targets of hackers. Thus, missing patches as well as faulty configurations can endanger their secure operation. Typical problems of web servers are:

- The readability of web server directories and files, for example, administration directories, script directories, and password files
- The ability to take control over a system by exploiting buffer overflows in server components
- The readability of source code of Active Server Pages by which hard-coded passwords might be given away

Furthermore, many CGI (Common Gateway Interface) scripts that are executed on the server side and which are partially installed in conjunction with a web server have proven to be problematic:

- Leakage of user information by cross site scripting attacks
- Execution of arbitrary commands on the server
- Access to the file system of the web server

Denial-of-Service Attacks

Denial-of-Service attacks aim at disabling single services or complete systems and networks. Hackers execute DoS attacks both on the TCP/IP level and by malformed requests to applications. While the number of successful DoS attacks on the network level decreases due to improved implementations by the operating system vendors, many modern applications and products are susceptible to DoS attacks.

Cracking of Passwords

Guessing passwords is still the simplest and most efficient method to compromise a computer system. In particular, if employees use terms from their closer environment (such as the name of their girl-friend or project) or, for convenience, choose passwords that only consist of a few letters and involve no special characters, their passwords can be cracked very easily.

Security scanners are able to detect too simple or too short passwords by two different strategies:

- Dictionary attacks by which a set of predefined terms and their combinations are tested
- Brute force attacks by which all possible combinations of letters, digits, and special characters are tried out successively

Many manufacturers ship their systems with preconfigured standard accounts and passwords for administration. If these passwords are not changed later, hackers have an easy play.

Backdoors

A backdoor is a program that a hacker installs on the victim computer after a successful attack. The backdoor allows him to get unhindered access to the system at any time, even if the original security hole has been fixed in the meantime.

Sometimes, backdoors are used for distributed denial of service attacks, where the victim computer itself is abused as an attacker. Among the most popular and most dangerous backdoors are *BackOrifice*, *CodeRed*, and *SubSeven*. Security scanners allow to check whether a system has been infected by a backdoor. In addition, they look for regular application software that allows remote access and thus can be used as a backdoor in case of erroneous configuration.

Superfluous and Outdated Services

Very often, computer systems provide services which functionalities are not needed in general or which are only installed for compatibility with older machines. Even if no vulnerabilities are known yet for these services, it is strongly recommended to deactivate them precautionary. Services that fall into the category of redundant or outdated services are, e.g., *chargen* and *daytime* but also the more popular *rlogin* und *telnet*.

Attacks Against Firewalls

Peculiar security requirements must go for firewalls. If a firewall is compromised or behaves erroneously, the most important protection shield of the corporate network drops out. In particular, there is a risk that the more complex application gateways do not filter critical data correctly. Two methods to by-pass the rules of a firewall are:

- Access to a mail server that is located behind a firewall by special SMTP commands
- Access to *telnet* or other interactive services by http requests with certain port parameters