Security is a Matter of Trust

interview with Rob J. Nauta

Erik Jan Marinissen

"Computer security is a matter of trust", says Rob Nauta. He knows from experience. As a student Computer Science at EUT, he became involved in the world of hacking, ultimately resulting in a court case. Nowadays, Nauta still follows the developments in the field of computer security, although he himself is not actively involved in hacking.

Introduction

"Safety is what the owner/user of a computer systems wants", explains Nauta. "Safety with respect to his programs and his data. Security is the correct expression for all technical means to obtain safety of programs and data." "Computer security is a matter of trust. Hence, a stand-alone computer, not connected to other computers and used by only one person, who only uses his own floppy disks, has not much of a security risk. However, if a computer has multiple users, the situation is already quite different. One has to distinguish between persons that can be trusted and others who cannot be trusted. Some form of control over who may use the computer is needed. This may be a technical solution which for example requires a user-ID/password combination, but also something simple as the fact that the computer physically resides in a secured office, where only (trusted) colleagues have access to it."

Viruses

A well-known security risk to computers is caused by the data transport via portable media such as floppy disks and CD-Roms. About a decade ago, the newspapers were full with stories of virusses which were transmitted from one infected computer to the other by floppies. To the general public, this has become the most well-known computer security issue. Nowadays, the media attention for floppy-transmitted virusses is almost absent. However, Nauta believes the risk is not. "The most important reason for the reduced media attention is the reduced news value. The problem is known, and every computer does have some 'virus scanner' installed. Just like wars which drag on for years get banned from newspaper front pages, this issue does not have enough novelty any more to write about." "Apart from that, floppies have lost their value as medium for data transport. Their role is reduced to that of medium for personal back-ups. Software is nowadays mostly sold on CD-Roms instead of floppies. And the threshold for making CD-Roms, and hence for putting virusses on them, is higher than it is for floppies, just because of the expensive equipment involved. However, nothing is impossible. There are cases known of newly-bought, shrink-wrapped official software, which upon installation turned out to contain a virus."

A positive side effect of the reduced media attention for floppy-transmitted virusses is the fact that also less virusses are made; for most hackers media attention is the ultimate goal of their activities. Therefore, the focus of many hackers has shifted to networks. Modern data transport and even downloading of software takes place via local and global computer networks. Especially the Internet has invoked a hype in media land, and hence this has become the place to be for any self-respecting hacker.

Rob J. Nauta's Hack Tips Top 5

1 Physical access. No matter how secure your system might be, always be alert for people that can access the machine itself. This involves stealing of the equipment, or, less drastical, rebooting with the opportunity to boot from another disk (or tape, or CD-Rom), through which the hacker can get complete access. This should be secured by passwords etc.

2 The user of 'uuencode' can specify the file name of the uudecoded file. This can be risky if in this file name an entire path is allowed. If for example root can write a file with 'begin 755 /etc/rc2.d/S88suid', then this program will automatically be executed during rebooting. And then the strangest things might happen...

3 You think you know what you are doing, if you issue an 'ls' command. However, if the current directory ('.') forms part of your search path, perhaps a completely different program is executed if you are searching through otherone's directories. This might be even a file which deletes your own directories!

4 Many people look for security holes. Over the years, the standard installation has become pretty secure, because most holes have been discovered and closed. However, the biggest security risks are in the local additions. A small script to start the web server automatically, small program to add new users; they are quickly written, but are they also secure? An error might cause that everybody can enter the system through a wide open door.

5 An ever-remaining risk are the ordinary passwords for users of the system. Before you know it, one of your 1000 users choses an easy password, and you only notices this once your systems floats over with strange files. A real personal identification system, or 'one-time passwords' might make a big difference.

Java interesting news

Nauta calls especially Java applets "interesting news to the computer security world". With a simple mouse click, a World-Wide Web user requests the downloading of (mostly small) programs, and grants the right to immediate execution on his computer *without knowing what the program will do* . It is hard if not impossible to do at-speed incoming inspection of the Java source code for security reasons. Blocking the entrance of all Java code is effective, but also blocks the interesting new functionality which Java unmistakely brings. Nauta: "Sun Microsystems, the makers of Java, have chosen for a compromis between functionality and security. Java applets are not allowed to read and/or write local files, nor can they open network connections. Under the critical eye of the entire world, Sun had no choice then to take the security issue very serious in order to make Java successful. A few bugs have been reported and solved quickly. After Intel's fiasco with the Pentium bug, the entire IT industry is aware of the fact that the best strategy to handle bugs in its products is to be open, admit any real bugs, and try to fix them as quickly as possible."

Security plan

The operation of many companies nowadays depends on computers. Hence, it is important for companies to set up a computer security plan. Nauta: "In such a plan should be defined who has access to what and how to protect hardware and software from unauthorized access. For example, a security plan could state that it is not allowed for employees to bring floppies from outside the office, or take company floppies home. How to enforce this, is another question, but the security plan provides a company rule to fall back on in case of problems." "Another item in a security plan is the connection of the internal company network to the outside world. In the old-fashioned way, all internal computers were externally accessible. Nowadays, it is generally recognized that it is better to have one entry point to the external world. This makes it a lot easier to create a 'firewall' to protect the company's network."

Hacking

Rob Nauta became involved in hacking during his time as student Computing Sciene at EUT. "The

university was also very thrifty with computer accounts, CPU time, and access to the Internet." A group students united under the name 'Timewasters' used the university computers for exactly that: spending many hours in playing games and hacking. Nauta: "My personal motivation was to get access to Unix machines and Internet. Nowadays, with Linux for PCs and an Internet provider in every town, that is easy. But in those years, only available to large companies and institutions." One thing led to another, and soon Nauta had the doubtful honor to be one of the first in The Netherlands to be legally accused of breaking into otherone's computer. The police confiscated his PC and other computer equipment for some time. Later, during the actual court case, the judge dismissed the charges because of improper proceedings by the prosecution.

From experience, I know that many people are trying to break the smartcard's security sustem.

Nauta says he is not involved in hacking activities anymore. However, he still follows the developments in the area of computer security. The Internet is of course an important means to exchange information on computer security, between system managers and hackers alike. Nauta: "At the end of the 1980s there was Zardoz, a closed mailing list on computer security. Access was only allowed to the 'root' of large institutions. The secrecy of that mailing list naturally provoked hacker's interest, and through some break-ins, the hackers community was soon able to read the mailinglist as well. And apart from that, hackers created their own mailing lists, which often contained interesting security news before the Zardoz list did. Current security mailing lists are open to system managers and hackers alike." Apart from the mailing lists, there are also newsgroups, such as `alt.security`, `comp.security.unix`, etc. However, over time these newsgroups have become polluted, and their technical level has decreased. Nauta: "It takes a lot of time to work yourself to all the junk in these newsgroups and the yield is low."

Smart cards

What is a hacker? Nauta: "A hacker is somebody who does smart things on a computer. This might be breaking the security firewall of a company or institution, but can also be in the area of programming. The vast majority of the hackers community has no evil in mind. The small group that does are called 'crackers', criminal hackers. However, this does not mean that not also the non-evil-minded hackers might cause damage when breaking in into a computer system, e.g., in the form of CPU and network costs."

"Hackers are interested in three things:

1 *Money.* In this respect, hackers are not different from other people. Here lies the origin of hacking in the 1960s; trying to manipulate telephone switches in order to make free telephone calls.

2 *Publicity.* For many hackers it is a sport to get into a secured computer system. Recognition of their achievement is obtained through publicity. Break-ins into the Dutch Viditel system and the computers of the Dutch PTT are well-known examples. The Dutch hacker's association HackTic often collaborated actively with journalists.

3 *Challenging technology.* It is a fascinating experience to understand a complex high-tech system into such depth, that you are able to do what others cannot."

The chip- or smartcard is an object which has all three properties that might attract hackers. And indeed, it has caught the warm interest of the hacking community. Nauta expects the smartcards to be a field in which we can expect a major hacking breakthrough on the short term. "From experience, I know that many people are trying to break the smartcard's security system. In the hackers club 'Het Klaphek', about 50% of the 30 members are in one way or the other busy with smartcards." Our readers who use smartcards, and that will probably soon be everybody, are warned! □