I/O Vivat

Year of publication 21, vol. 4,
September 2006
ISSN: 1389-0468
Circulation: 2300

I/O Vivat is the periodical magazine of Inter-Actief (the study association of Computer Science, Business Information Technology and Telematics) and ENIAC, the alumni association of Computer Science students from the Univeristy of Twente.

Editorial Staff
Alexander Spannenburg (chairman), Jan-Willem Dijkshoorn, Bram van de Laar, Mark Timmer

Kryptos Committee
Kimberly Lemmens (chairman), Eelco Eerenberg, Ivar Pruijn, Stephan Roolvink, Alexander Spannenburg and Koen Voermans

Guest Writers
Gerrit van der Hoeven, Michel Jansen, Tim van Eijndhoven, Joris Janssen, Jerry den Hartog, Olivier Toelen, Kahuna, Dirkjan Bussink, Geert Vos, D. van 't Oever, J.J. de Wit, ir. Joost van Beek, ir. Martin Krans, Francis Henninger, Deloitte

Printer
Van den Bosch & Fikkert

VAN DEN BOSCH & FIKKERT
DRUKKERS SINDS 1932

Adresses

E-mail: vivat@inter-actief.net
Telephone: 053-4893756
Fax: 053-4894571
Post. add.: Inter-Actief
Postbus 217
7500 AE Enschede
Internet: www.inter-actief.net
Kryptos: www.kryptos.nl

Thanks to all senders of articles. The study association would like to thank all the advertising companies for the good cooperation.

Front page: We would like to thank Bram de Vries for lending his laptop

Kryptos Vivat

This fall thirty students and two professors of the former Computer Science faculty will go on the journey of their lifetime. We will go on an adventure to the United States of America. This adventure is a study tour and we will visit both universities and companies in Boston, New York, Washington D.C. and San Francisco. During this study tour Harvard University, Stanford University and MIT will be attended. Also Philips Medical, Deloitte, The Pentagon, Sun Microsystems, HP and several other companies will be visited. This special edition of the I/O Vivat will be provided to the hosts and speakers on each visit, therefore this special publication, called the Kryptos Vivat, is written in the English language.

The name of this study tour is Kryptos. If you knew that this name is related to the research subject of the study tour, then you immediately could guess that the subject is IT security. Therefore this I/O Vivat is filled with articles in the IT security area.

As a preparation for the study tour to the United States the participants of the study tour went to Getronics PinkRoccade in Apeldoorn for a company visit. As a result of this visit an article about this company visit is published in this Kryptos Vivat.

Some of the participants of the study tour have written a contribution to this issue as a result of a preliminarily course of the study tour. The subjects of these articles are about Security and Instant Messaging, Security and Linux and Risks of DigiD.

Moreover, this edition contains an interview with Ronald Leenes from the Tilburg Institute of Law, Technology and Society. And as every issue of the I/O Vivat there is a "Visiting…" (better known as "Op bezoek bij…"). This time "Visiting… Fox-IT"; this company only accepts special ICT Security projects, so if you are curious what these projects are, you should read this interview.

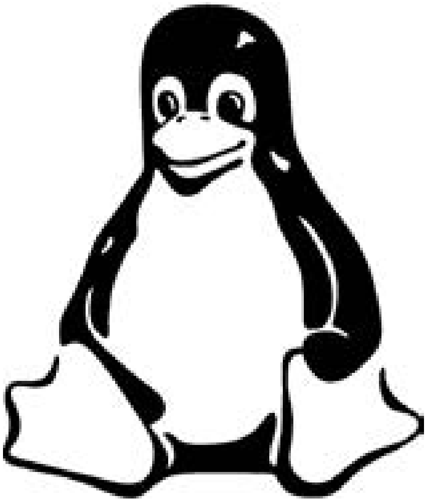
Furthermore the proceedings of the Kryptos Symposium are presented. This symposium about IT Security will take place on September 13th. There will be several lectures and workshops of major businesses and universities. If you are interested in this subject I recommend visiting www.kryptossymposium.nl for more information about it and subscription to this great event.

To conclude this preface I wish you much reading pleasure with this special Kryptos Vivat. ■

Kimberly Lemmens, Chairman Kryptos Study Tour

Contents

Visiting... Fox-IT (page 4)



Security Enhanced Linux (page 32)

"A study tour is nothing like a binge trip. With over twenty companies to visit in three weeks, the study tour is stuffed to the rim."

9

"Some of the topics that will be discussed are digital rights management, cyber crime, security architecture and biometrics."

18

"To cite Cardinal Richelieu: "If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him"."

28

What is Van der Hoeven searching for...

A sense of security?

Some day I was visiting an institution, with some colleagues, that manages and processes large quantities of sensitive information. The demands for reliability and protection (against unauthorized access) there are very high. We got a tour. Evidently many threats were thought of. A considerable bombardment would not worry the company. On the way back we wondered how sadistic and unscrupulous we would have to be to, via a familiar person within the company, one of our alumni for instance, force access and by-pass all protection measures. Much more unscrupulous and sadistic than we would think of ourselves, and without the guarantee of success. But there are more sadistic and unscrupulous people on this world than those that are capable of a bombardment. Why did we hear so much about the protection against bombardments and nothing about the protection against unscrupulousness and sadism? And why did not ask about it?

The intention of this piece is not to warn students about the risk of unscrupulous and sadistic teachers. But the role of man in security and protection interests me. The relation between people and their security exhibits some strange traits. Everybody wants to be protected from evil, this is elementary survival instinct. The sense of security is therefore a highly appreciated feeling. But there is no feeling as misleading as that feeling. And it quite often happens to us that we think we are safe, while the contrary turns out to be true. Do we have a repressing mechanism here? Does everyone who thinks carefully about security and reliability see so many threats they cannot protect themselves against that they die from fear? So we rather not think at about it at all? Hmm. Let me not amateurishly psychologize.

The rule of thumb for good protection is “Keep it simple, and don’t trust secrecy”. The background of this rule of thumb is that simplicity and the public nature helps you in seeing your own stupidity, helps you to project into the cleverness of the attacker, and protects you against your own misplaced carelessness. Hmm. Stupidity, cleverness and carelessness, are those not human traits for gentle nerds? Where is the true human evilness?

I take back what I said earlier about unscrupulous teachers. Should you ever think about security, quickly forget your image of the somewhat dopey teacher who is so boring and professional. He is standing behind you, and he is cruel and depraved. He knows everything about you, and nothing that is dear to you is worth anything to him, your life to the least. Now think calmly about security. I will feel safe at your simple solution.

Gerrit van der Hoeven

Have you always been fascinated by forensic investigations as seen in the television series Crime Scene Investigation, but are you wondering how a background in computer science can be combined with it? We visited a company that links both worlds: Fox-IT. From Pim Fortuyn's computer to state secrets of the national government, for Fox-IT it is all in the game. We spoke with managing director Ronald Prins.

Visiting...

Fox-IT

The company

Generally speaking Fox-IT provides IT Security, but within this area only special projects are handled. Assignments are only accepted if they are special: special for being of high technological level, or special because the customer has very distinct demands. The emphasis at Fox-IT is on 'exciting' projects, amongst others because this keeps the employees well-motivated.

In 1999 Fox-IT was founded by Ronald Prins and Menno van der Marel. Both had worked for the Nederlands Forensisch Instituut (Dutch Forensic Institute). The challenge there, however, was not very great, which during a game of squash made them decide to move on to corporate life. Fox-IT is in a lesser amount involved with work for police and justice department, but mainly with large multinationals and governments.

The company is divided in five Business Units: Forensics & Audits, Crypto, Projects, Managed Security Services en Training.

The Business Unit Forensics & Audits is in fact the basis of the company. Today many networks are still hacked and internal employees lower their efficiency by looking at adult material during working hours. Recently Fox-IT worked on a case in which a managing director of a large multinational had embezzled forty million euros.

To prevent abuse the auditors of Fox-IT work in a pragmatic way by first using a 'cowboy approach' to fiddle with systems, and later on perform structural penetration tests. Eventually an advice is given to achieve better security, which often results in a secondary assignment to implement the recommendations (by the Business Unit Projects).

Should anything have already gone wrong, Fox-IT looks for traces that may have been left on systems, using in-house developed techniques and methods. Employees who – against the company policy – have watched adult material during working hours can for instance be fired with a good reason. The experience that is gained at Forensics directly flows back to Audits, so prevention methods continuously match the attacks that are used.

Prins mentions that in fact there is not a single company that offers the same total package as Fox-IT. Companies like Deloitte and KPMG come close considering audits, and concerning forensics Fox-IT can be placed next to 4iTrust and Hoffmann, although Fox-IT focuses more on technology. In assignments such as checking systems behind the gates of prison cells, Fox-IT is unique, Prins states.

From a commercial point of view seen the market segment that Fox-IT is in might not even be the best choice, but the priority is on exciting and fun projects.

Working at Fox-IT

After having started in 1999 with two men, Fox-IT now already has about

ADVERTENTIE

Fox-IT

65 employees. The background of these people is a multidisciplined one: there are mathematicians, physicists, computer scientists, industrial engineers and even a graduated law student. The focus is on young people, who do not necessarily need to have a lot of working experience. With ten running vacancies at the moment the company is fast-growing.

In an interview procedure the study of the candidate is checked to measure the work and thinking level of a potential employee. Furthermore it is valuable that one for instance has been experimenting behind an Atari as an 8-year old. A tendency for paranoia does not hurt either. For a programming position only the best applicants are employed.

Often graduate students become an employee, but a graduate position does not guarantee a job: out of four graduates usually only one is found fit to stay with the company.

Corporate culture

Cosiness can practically be called a prerequisite to work for Fox-IT. For instance, they will soon be doing Geocaching again: treasure hunting for the advanced, using GPS. Furthermore, the other day they had a barbecue and some time ago they organized a puzzle trip with technical questions. A marketing employee notices that all technical colleagues not only know a lot about their profession, but can also communicate their knowledge enthusiastically which makes these trips fun for everyone.

Another remarkable aspect about the culture is the choice of clothing of employees. Recently a memo was sent from marketing to everyone in the company that bare feet were just a little too informal; this indicates that a suit is definitely not required. For a customer visit people dress a little smarter, but there are no strict requirements here as well. The customer knows that IT-experts are generally not the smartest dressed people. “They will have to accept that”, states Prins.

Hierarchically there are some changes going on. Until recently there was no management layer between the managing director and the employees, but now there is one manager per Business Unit. Still it is not a problem to walk into the office of a director.

> “How profitable a project is doesn’t even have the highest priority.”

All in all Fox-IT seems like an interesting company, with, like the director himself describes, ‘exciting assignments’. The employees see their work as a serious hobby: that can be seen from the fact that they can often be found at work in the evening or even in the weekends. ■

Mark Timmer
samenwerking@inter-actief.net

Being founded in 1887 Getronics PinkRoccade has certainly experienced the information technology stone age and its evolution. However, the title of this article does not refer to Getronics PinkRoccade's almost 120 years of existence, but rather to their view on the IT Security field. This largest IT service provider in The Netherlands has great expertise in directing data streams securely and uninterrupted into the proper lanes, which poses many challenges that have resulted in a well-founded vision on IT security. We went to the Apeldoorn office for a presentation and discussion on the subject. Director of Security Service Haydar Cimen provided us with their view of data and a tour in their secure center.

IT Security Stone Age

History of Getronics PinkRoccade

Getronics PinkRoccade was formed in March 2005 when Getronics, specialized in ICT solutions, merged with PinkRoccade, specialized in printing. Today's Getronics PinkRoccade is part of Getronics N.V. and is active in the Netherlands with approximately 10,000 employees. Worldwide Getronics N.V. has 27,000 employees in thirty countries.

Getronics

The history of Getronics is captivating and rich. In 1887 Groeneveld, Van der Pol & Co's Elektronische Fabriek NV founded a company that installed controls and technical equip-ment for the shipbuilding, utilities and construction industries. From then on the company underwent several transformations and name changes. After the company was reintroduced to the Amsterdam stock exchange in 1983 with the name Geveke Electronics N.V., the company is renamed to Getronics N.V. in 1988. With the adoption of PinkRoccade in 2005, the largest ICT service provider in the Netherlands was established.

PinkRoccade

In 1950 the Rijkscentrale voor Mechanische Administratie (RMA) was founded, which was renamed in 1969 to Rijks Computercentrum (RCC). The RCC acquired the task of 'performing services in the field of the automatic information processing' for departments and (semi-) government agencies. After the company was privatized in 1990 it was merged with Pink Elephant and Bouwfonds Informatica to form PinkRoccade.

IT Security

Getronics PinkRoccade is an inventive IT service provider that provides optimal availability and security in the areas of architecture, infrastructure and applicative service provisioning. If requested worldwide, 24 hours a day, 7 days a week. This puts heavy constraints on security in all levels of Getronics PinkRoccade's operations. Some of their experiences are described below.

Stone Age

One of the main surprising observations of Getronics PinkRoccade's view on IT security is that the security field is in the Stone Age of its time. The immaturity of the field can for instance be seen from a financial point of view; the costs of IT security are approximately 2.3 times higher than normal IT expenses. This is partly the result of the immense complexity of the area (without considering for example integrity, privacy, and non-repudiation, authentication alone is an issue with a fast array of complicated solutions); however, just as important a factor is the immaturity of solutions nowadays.

Currently many security issues are discussed and tackled on a deeply technical level, which is similar to the status of many technical solutions in their infancy that are now in every day use. For instance, some twenty years ago, setting up a mobile phone project was a painstaking process of discussing every (small) technical detail, whereas today providing a mobile phone is a no-brainer. Mobile phones have become a commodity, which is where Getronics PinkRoccade believes IT security should and will eventually move to. However, currently many solutions are 'backlogged' in this sense and need to crystallize into commodities, so security issues can be handled from a higher level of abstraction than is currently possible. Since a lot of solutions have not yet matured, costs are high, and therefore many companies do not implement required measures, despite the availability of unlimited time or possibilities and the fact that there are many issues to be addressed.

Issues

Vulnerabilities have increased due to the rise in e-business and many new security problems arise that come with the fast pace of acceptance of new technologies used in businesses today. However, the level of awareness of the need for IT security is low and too little knowledge and know-how on the subject is present in most companies. This leads to a discrepancy between the costs of IT security and other IT related expenditures, since much more is spent on IT than on security. Businesses lag behind in new security developments, whereas they should be an integral part of business processes. After all, many issues touch the core business of companies, such as compliancy, espionage, and the impact of incidents on reputations, operations and budget.

Other developments in the field are paradigm shifts. When companies first became connected to the Internet many security solutions were based on a Demilitarized Zone (DMZ) that protected the internal company network from intrusions from the 'big-bad-outside'. The focus has shifted towards internal security and currently to using point-to-point security using tunnels. The future will show more and more integrated solutions.

Legislation and rules on security are both encouraging and obstructing. It provides a high level of standard that must be met. But at the same time it can restrain security measures. An example is that Getronics PinkRoccade, being a Certificate Service Provider, performs signing of unique keys to be used in root certificates and digital signatures, which is incredibly expensive because of legislation that requires disproportional efforts to secure the process. A good balance between legislation and security still needs to be found.

Market drivers

Nowadays the digitalization of businesses is carried through to great lengths; therefore businesses are increasingly concerned with security and the need for security specialists is high. One of the business issues that Getronics PinkRoccade copes with is the seamless integration of security in corporate processes, while solutions need to remain scalable and flexible. Another driver is that organizations are getting more and more complex; therefore managing security within the organizational complexity is extremely challenging.

Another major market driver for consulting security specialists is the lack of access to experienced, qualified and specialized work force. There is a shortage for such personnel and therefore companies need to outsource their security issues, also for cost efficiency reasons, for instance by security service provisioning.

Secure data centre

The data centre of the Apeldoorn office is a perfectly applied example of how security works in the real world. The Getronics PinkRoccade data centre offers storage and data management services to many companies and the government. It is said that of every citizen of The Netherlands some data resides in this data centre. Therefore it is not excessive that several security checks are performed before the secure data centre can be entered, as we have experienced in the flesh. Within the data centre there are several server rooms which are extra secured by biometric security checks.

Besides the security checks the location is also a security measure. The data centre lies at seventy meters above NAP and the centre was build during the Cold War period. Therefore the centre has six meter thick walls and supposedly a plane can crash on it without damaging the data centre inside.

Working at Getronics PinkRoccade

Getronics PinkRoccade invests in their employees and the organization. They believe that people develop themselves continuously. This can mean an increase in responsibilities and complexity of their function. But just as well it can mean a new function or working at another department.

The first years of a young professional at Getronics exists of a training. This training is aimed at gaining valuable certifications, such that new employees can work on clients' projects with increasing complexity. One of the trainings is given in India to acquire thorough knowledge of system development within a month, which would take about a year in the Netherlands. Getronics PinkRoccade has its own e-learning environment and several management development, personality and mentoring programs. Therefore its personnel can always acquire knowledge concerning the newest technologies.

To conclude, our visit to Getronics PinkRoccade has given us a refreshing insight into the security operations of the largest IT service provider in The Netherlands and the current security issues they face. The field of IT security is complex and will remain challenging in the future. Getronics PinkRoccade certainly seems up to the task of bringing IT security to an even higher level. ■

"(...) the security field is in the Stone Age of its time"

Kimberly Lemmens
Ivar Pruijn

References:

www.getronicspinkroccade.nl

Middenwoord (From the chairman)

The importance of a study tour

When I first heard of the concept of a study tour, I had a completely wrong impression of what such a tour is all about. Like so many others, I pictured it as a nice long trip of three weeks to a distant country with a large group of familiar students, paying some visits to interesting companies, experiencing a foreign culture and engaging in relaxing group activities. To make it all a bit more useful you have to follow some courses and a part of the travel costs has to be earned by performing contract reasearch for a company, but apart from that it's "sit back and relax", while the study tour committee puts together one hell of a trip.

Having spent a few months with the committee now, my view on what study tours are and why they are so important has changed radically. A study tour is nothing like a binge trip. With over twenty companies to visit in just three weeks, the tour program is stuffed to the rim. These company visits aren't just meant to be interesting and fun, they are part of the research the group as a whole conducts; serious research, that starts in the Netherlands with a global overview of important factors concerning the chosen theme and country. It's clear a study tour is a lot more than a holiday, but is it useful?

First of all, a study tour provides an invaluable source of experience for students. It offers an opportunity to explore new cultures, visit a foreign country and learn to perform research in a large group to participants. To committee members it offers a way to try their organizational skills on a large and unique project.

Secondly, study tours form a way for the university's teachers to get to meet important people in their field, get to know their students and in general gain some extra practical experience, adding to their personal development and continued education.

Moreover, a study tour is a great way for a university to promote itself internationally. It doesn't happen every day a large group of well-prepared students from one of your faculties gets the chance to make their first impression on a foreign company, university or research institute. On each company visit the participants present a specific part of their research and in the end the entire research is bundled in a report, which is being distributed to all parties involved. To the university this is great publicity.

All in all, it may be clear study tours are of priceless value to all parties involved. Students broaden their view, teachers enlarge their networks and universities get to profile themselves. I didn't even mention the value of the tour research to the visited companies. Study tours are a core activity of Inter-*Actief*, defining our study association. Let's keep it that way. ■

Michel Jansen

This September 13th the Kryptos Symposium on IT Security will take place. Several aspects of IT security are discussed during the presentations and workshops. The location will be University of Twente, the Waaier.

Proceedings Symposium Kryptos

IT Security

The Kryptos Symposium speakers have different perspectives on the subject. Some of the topics that will be discussed are digital rights management, cyber crime, security architecture and biometrics.

Leading speakers in the IT Security field will be talking on the subject, like Frank Kamperman from Philips Research, Hans Appel from Sun Microsystems, Jacques Buith from Deloitte ERS, Peter Went from WCC and Albert Verhulst from NOD32. Furthermore, there will be speakers from Getronics PinkRoccade, CapGemini, Better.be, Fox-IT and Madison Gurkha.

In addition to the presentations there are workshops from Deloitte, Quarantainenet and a workshop hacking. All in all, a full-day program about IT Security.

09:00h	Arrival and coffee		
09:30h	Start by chairman of the day Pieter Hartel		
09:45h	Deloitte ERS Jacques Buith “Global IT Security Survey”		
10:45h	CapGemini	NOD32 Albert Verhulst “Cyber crime”	Better.be Theo Balijon “Security architecture”
11:30h	Break		
12:00h	Philips Research Frank Kamperman “Digital rights management”	TU/e Sjouke Mauw	Madison Gurkha Walter Belgers
12:45h	Getronics PinkRoccade Rob Zouteriks	WCC Peter Went “Search technology in the biometry”	Fox-IT Oscar L. Bal “Forensics and audits”
13:30h	Lunch break		
14:00h	(workshop) Deloitte Wouter van Voorst tot Voorst		
14:30h		(workshop) Quarantainenet Casper Joost Eyckelhof “Honeypots, exploits, quarantainenet”	(workshop) Pine Frank van Vliet “Hacking”
16:00h	Sun Microsystems Hans Appel “Life and work in the new reality”		
17:00h	Forum		
17:30h	Informal drinks		

The concept program

To give you an impression of the speakers, we introduce two of them:

Hans Appel

CTO Sun Microsystems
Presentation: "Life and work in a new reality"

Hans Appel has been working in the computer industry for some 35 years. After his study in electronics, he began building and programming hybrid analog/digital computer systems in the late nineteen-sixties.

"For subscriptions: www.kryptossymposium.nl"

In the early seventies he took up employment with Sperry UNIVAC, a company that was engaged in designing, building, and selling mainframe computer systems. After working in different functional areas in systems programming, he took his first steps in the world of marketing in the late seventies.

With the rise of computerization in the early eighties, Appel went to work at WANG, a company that was, in those days, a leading innovator in the area of computer technology for the office environment. At WANG he held various positions within the company's marketing departments.

In the late eighties he crossed over to Apple Computer, a company that wanted to change the world. A company which also has a very unique vision of computer technology being used by everyone. For many years Apple was a model for continuous and groundbreaking innovation. Here again, marketing was Apple's main credo.

Since 1996 Appel has been working at Sun Microsystems Nederland B.V. Sun is one of the few IT organizations where the design of a product, from silicon to end product, still occurs within the same company. It is a company in which the human-technology interface occupies an important place, right next alongside the marketing of highly professional IT-technology.

Appel always says: "I have two professions: technology and marketing. The combination of the two fields forms a tremendous challenge. Keeping up with these two dynamic areas is an enormous motivator to excel."

Peter Went

CEO WCC
Presentation: "Search technology for biometry"

Peter Went is the Chief Executive Officer of WCC, where his role is to oversee the company's operations in The Netherlands and the United States.

Mr. Went founded WCC in 1996 after a frustrating search for a new house exposed the fact that existing database technologies were ill-equipped for performing certain types of searches. This revelation led him to develop a search tool that worked more like the human mind, and set the foundation for WCC's ELISE fuzzy database technology.

Prior to WCC, Peter Went held a number of leadership positions with different high tech companies. He served as CTO of Quality System Development, which developed and marketed an integrated banking system for European banks. He also was Founder & CEO of UniSoft, where he orchestrated the company's expansion into Prague.

Mr. Went's experience also includes various roles in both software development and business consulting. He has served as lead developer with Shell International, principal consultant at James Martin Associates and principal consultant with Platinum Technology.

An internationally recognized expert in relational database systems, Mr. Went has spoken at a number of conferences including IBM Guide event, Security Symposium, HR-XML. ■

Kimberly Lemmens

For subscription:
www.kryptossymposium.nl

KRYPTOS
Study Tour Inter-*Actief* 2006

With the huge gain in popularity of the Internet, many companies have made the switch to selling and promoting products online. Traditionally commerce on the Internet has the problem of verifying the identity of the customer. Many websites try to solve this identification problem with providing the customer with a username and a password. This often leads to the use of the same username/password combination for different websites and the use of so-called "weak" passwords; passwords which can be easily guessed or found through "brute force" attacks [Eug92].

Recently the Dutch government introduced the DigiD service [Dig06], a central authentication service for government websites. This service provides access to the personal details of the citizen and should therefore be adequately secured.

See the Kryptos website for the full paper.

The key to DigiD

Risk analysis of the authentication used by the Dutch government

RESEARCH QUESTIONS

Since more and more governmental services are offered online, it is essential to have a look at the possible risks. Therefore this research focuses on the security of the DigiD system.

What are the security risks to the DigiD service?

What measures can and have been taken to minimize the risks?

Firstly the system architecture is described. Secondly the possible risks for this system are listed. Thirdly the security measurements are analysed. Based on these findings an overall conclusion is presented for the security of the DigiD system.

DIGID

The government is merging its Internet activities by providing one system for authenticating citizens: DigiD.

Every citizen of the Netherlands can request an account at the DigiD website [Dig06]. This requires a valid social security number and address information. Subsequently the citizen has to choose a unique username and enter a password. The first step is completed.

The information is checked and the citizen will receive a letter by postal mail. This letter contains an activation code. The code has to be entered on a website to activate the account. After this step is completed, the DigiD account can be used.

A-SELECT AUTHENTICATION SYSTEM

The DigiD infrastructure is based on the A-Select authentication system. This software is developed by Alfa & Ariss for SURFnet [Ase06].

The goal of this software is to create "a centralized, web-based user authentication service for web applications. It allows users to gain access to A-Select enabled web applications in a uniform way by using A-Select to establish their identity and pass it on to the application" [Ase06].

The system is based on Authentication Service Providers (AuthSP's). These services are capable of identifying users. Examples of AuthSP's are internet banks, RADIUS servers and DigiD.

General authentication procedure

A general authentication procedure will consist of the following steps: Users connect to the webserver of the service they would like to use. This webserver redirects the user to the webserver of the AuthSP. In this web environment the user enters its credentials. Once the credentials are verified, a reply is sent to the initial service for which the procedure was started. This service can not see the credentials of the user, but only receives the username information and the certainty about its appropriate use.

Security levels

The A-Select system defines different levels of security. If a user would like to access a resource with a lower level of security, this access is granted immediately. In Table 1 the security levels of A-Select are defined.

Level	AuthSP Functionality	DigiD
10	IP based authentication	
20	RADIUS password authentication	
30	LDAP back-end password authentication	Basic
40	Mobile phone (SMS) authentication	Medium
50	PKI certificate authentication	High
60	Online banking authentication	Medium

Table 1: Security levels of A-Select with analogue DigiD labels [Ase06]

DigiD security levels

The Dutch government distinguishes three levels of security for protecting electronic government communication; the applied level of security depends on the information exchanged.

* **Basic**: username and password authentication.
* **Medium**: basic level extended with mobile phone authentication.
* **High**: authentication is provided by using an electronic national identification card (eNIK) used for asymmetric cryptography with the government.

"Key to this is the lack of understanding on the use of the credentials"

Currently the eNIK card is not available for Dutch citizens. The highest level of security is therefore not available at the moment.

POSSIBLE ATTACK VECTORS

The potential vectors of attack mentioned contain the most commonly used attack vectors on the types of systems like the DigiD system. In order to create an overview of the security risks involved, they will be categorized according to the TCP/IP (the internet protocol) four-layer system as used by De Vivo et al. in Figure 1 [VVI98].

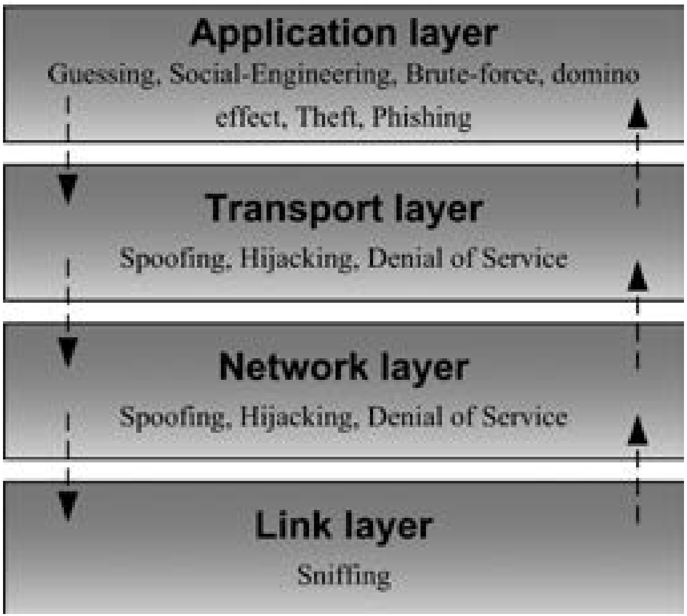

Application layer
Guessing, Social-Engineering, Brute-force, domino effect, Theft, Phishing
Transport layer
Spoofing, Hijacking, Denial of Service
Network layer
Spoofing, Hijacking, Denial of Service
Link layer
Sniffing

Figure 1: Possible attacks on different levels of communication

Application layer

The possible attacks on the application layer all focus on obtaining the authentication token of the user. This can be done on the "something you have"-partly by *theft*, but is mostly done on the "something you know"-part of authentication. User accounts are often being hacked by *guessing* or *brute-forcing* (trying every combination) passwords; these techniques were already known in 1979 [MT79].

Another method often used is *social engineering* where hackers obtain passwords by gaining the trust of the victim an abusing it. Key to this is the lack of understanding on the use of the credentials [WS02]. Closely related to social-engineering is the digital form of it called *phishing*, in which a user is tricked into filling out his credentials into a fraudulent website [DTH06].

When these are combined with the *domino effect* of using the same credentials in various places it enables a hacker to target the "weakest" system and use the credentials found there on the "stronger" systems [IWS04].

Transport and Network layer

Well known techniques on the network layer are tricking the system or a network to trust a malicious system, called *spoofing*, and bringing down a service with a *denial of service* attack. Another possible attack is *hijacking* an authenticated session from a client [VVI98].

Link layer

On the link layer there is the possibility to eavesdrop the Ethernet packets that are sent over the network, called sniffing [VVI98].

SECURITY ALTERNATIVES

There are a couple of techniques known to enforce the use of "stronger" passwords. For example using a *password generator* instead of allowing the user to pick one [BCR97]. Another option is using pictorial passwords instead of textual ones. This should lead to stronger passwords since *pictorial passwords* are easier to remember [WWB05; TT05].

Authentication can also be implemented by "physical" authentication tokens such as *key authentication* for signing and encrypting messages [VVI98] or the related *certificate authentication* which is based on a trusted party supplying a certificate to someone to use it for proving its identity. Another option is using *physical passwords generators*. These devices generate one-time codes [Eov06].

Eavesdropping on the network can be prevented by *segmentation of the network* or *encrypting* the messages over a connection [VVI98].

The use of *local trusted resources* provides a solution to the spoofing problem by using these resources to cross-check the connection [VVI98].

In order to protect the user against social-engineering and phishing attacks the *user should be educated* on how to pick passwords, how to handle them and their importance [BCR97]. For more physical measures against phishing, Dhajima and Tygar provide a technique of using *graphical codes* [DT05; DTH06].

If it all goes wrong anyway, the system should be *closely monitored* all the time to enable quick reaction to problems with system services and resource utilization [MR04].

DIGID PROTECTIVE MEASURES

SSL Connections All of the connections used in the DigiD system are secured by the use of Secure Socket Layers. This ensures that the communication channel is encrypted.

PKIoverheid is a Dutch network of trust in which only certain suppliers are trusted by the government (root certificate) to hand out certificates to other parties.

SMS Authentication requires the user to be able to receive an SMS message sent to the number associated with the user.

User Education is provided on the DigiD website. It contains information on how the service works, which security measures have been taken and how to check the legitimacy of the server.

Network segmentation is provided by the Internet topology, which is comprised of switched networks.

These measures are cross-checked against the preventive measures mentioned earlier, see Table 2. This table provides an insight on the preventive techniques already used in the DigiD system. It does however not mean that all of these measures are taken for every step in the system.

SUGGESTIONS FOR IMPROVEMENT

A username password combination for authentication is sufficient for most unimportant web services. However communication with the government requires a higher level of authentication. One should consider upgrading from the basic level to at least the medium level.

In the high level authentication, a lot of strong constructions are possible. One requires an electronic identification card (eNIK). This card can contain several PKI features to ensure safe communication. The government can support the research currently done, in order to improve the DigiD system.

CONCLUSION

Based on the information available a theoretical analysis is done on the DigiD authentication system. It is essential for the Dutch government to protect its expanding web services against abuse.

> “A username-password combination is sufficient for most unimportant web services”

	Threats										DigiD measures				
	Guessing	Social-Engineering	Brute-Force	Domino Effect	Theft	Phishing	Spoofing	Hijacking	Denial of Service	Sniffing	SSL Connections	PKIoverheid	SMS Authentication	User education	NetworkSegmentation
Password generator	■			■											
Pictorial passwords	■			■											
Key authentication	■		■									■			
Certificate Authentication	■		■			■	■				■	■			
Network Segmentation										■					■
Encryption								■		■	■				
Local trusted sources							■								
Graphical codes						■									
User Education	■	■		■	■	■								■	
Detailed Monitoring									■						
Physical password gen.	■		■										■		

Table 2: Protective measures to defense to threats and the DigiD measures implemented

The DigiD service provides one authentication system for all (Dutch) government web services. It uses sufficient encryption for sending privacy sensitive information between the client and server systems. Overall, its security level is sufficient for the current state of technology.

The basic authentication system is weak. The idea of using a username and password only has many disadvantages. The government should further stimulate research on enhanced authentication systems as public key infrastructure (electronic identification card: eNIK) . ■

Tim van Eijndhoven
Joris Janssen

REFERENCES

[Ase06] A-Select project documents including “Operational Concept and System Description” and “Configuration Instructions for A-Select Server 1.3” retrieved May 8th 2006 from http://www.a-select.org/doc/select1.4.1.ocd.html

[BCR97] F. Bergadano, B. Crispo, G. Ruffo, Proactive password checking with decision trees, Proceedings of the 4th ACM conference on Computer and communications security, Zurich, Switzerland, 67-77, 1997

[Dig06] DigiD project website retrieved May 8th, 2006 from http://www.digid.nl

[DT05] Rachna Dhajima, J.D. Tygar, The battle against phishing: Dynamic security skins, Proceedings of the 2005 symposium on Usable privacy and security, Pittsburgh, Pennsylvania, 77-88, 2005

[DTH06] Rachna Dhamija, J.D.Tygar, Marti Hearst, Why phishing works, CHI 2006 proceedings, Montreal, Quebec, Canada, 2006

[Eov06] E-Overheid (E-Government). Website of the Interior and Kingdom Relations (BZK) retrieved May 8th from http://matrix.e-overheid.nl/ row.aspx?matrixid=eloprojecten&rowid=5&view=Architectuur

[Eug92] Eugene H. Spafford. Opus: Preventing weak password choices. Computers & Security, 11(3):273–278, 1992.

[IWS04] Blake Ives, Kenneth R. Walsh, Helmut Schneider, The domino effect of password reuse, Communications of the ACM, Volume 47, Number 4, April, 75-78, 2004

[MR04] Jelena Mirkovic, Peter Reiher, A taxonomy of DDoS attack and DDoS defense mechanisms, ACM SIGCOMM Computer Communication Review, Volume 34 , Issue 2, April, 39-53, 2004

[MT79] Robert Morris, Ken Thompson, Password security: a case history, Communications of the ACM, Volume 22, Number 11, September, 594-597, 1979

[TT05] Thomas S. Tullis, Donna P. Tedesco, Using personal photos as pictorial passwords, CHI ‘05 extended abstracts on Human factors in computing systems, Portland, Oregon, USA, 1841-1844, 2005

[VVI98] Marco de Vivo, Gabriela O. de Vivo, Germinal Isern, Internet security attacks at the basic levels, ACM SIGOPS Operating Systems Review, Volume 32, Issue 2, 4-15, 1998

[WS02] Dirk Weirich, Martina A. Sasse, Pretty good persuation: a first step towards effective password security in the real world, Proceedings of the 2001 workshop on New security paradigms, Cloudcroft, New Mexico, USA, 137-143, 2002

[WWB05] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, Nasir Memon, Authentication using graphical passwords: effects of tolerance and image choice, Proceedings of the 2005 symposium on Usable privacy and security, Pittsburgh, PA, USA, 1-12, 2005

> “Overall, its security level is sufficient for the current state of technology”

Our society increasingly depends on ICT for day-to-day activities, both at work and in our private lives. As a consequence, our society has become ever more vulnerable to failure and abuse of this digital infrastructure. This explains the growing interest in and importance of computer security. Indeed, there is a growing demand for trained computer security experts in industry, applied research and academia.

Computer Security

a new master

Starting September 2006 a 2-year computer security masters programme is offered by the Kerckhoffs Institute for Computer Security, a collaboration between the computer science departments of the University of Twente, the Eindhoven University of Technology and the Radboud University Nijmegen. This article describes this masters programme.

Goals & Points of Departure

The Kerckhoffs computer security master's programme prepares its students to occupy leading positions in the computer security arena, as scientists, researchers, consultants or developers, both in industry as well as academia. The graduates will know the state-of-the-art in computer security. They will be able to analyze complex security situations and to reduce them to solvable problems, taking the societal context into account.

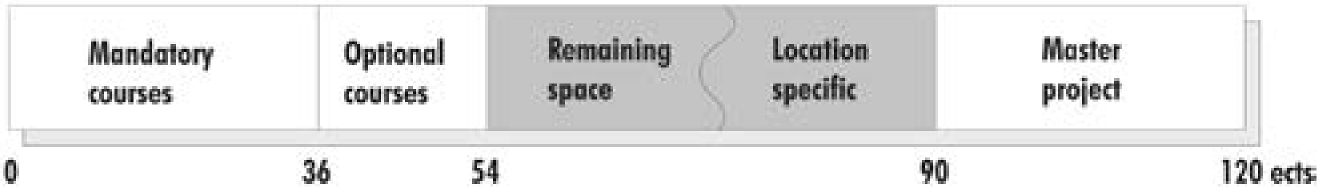


Figure 1: Mandatory, optional, project and remaining space

The contribution of the three universities to the Kerchoffs masters provides a uniquely large pool of expertise on the diverse area of computer security from which the students can benefit. Students can follow courses at each of the three universities. The need for student travel among sites to attend courses is minimized by a properly designed schedule. (See also Figure 2.)

The programme consists of six mandatory courses, providing a solid basis for the security engineer in training and is supplemented with optional security related courses which can be selected from the courses offered by any of the universities, allowing the student to select their own focus. Also each university provides a unique profile, expressed in its location specific courses. The programme is completed with a master's project in which students perform independent research and write a master's thesis.

The two year master's programme is open to all computer science bachelor students (or bachelors from a different but related discipline like electrical engineering or mathematics), provided their curriculum sufficiently covers the prerequisites of the master's programme.

Course descriptions

The mandatory and optional courses offered are shown in the curriculum schedule in figure 2.

Each site offers two mandatory courses and three optional courses. The mandatory courses are scheduled together with optional courses given at the same site on the same day to minimize student travel, on Mondays and Fridays to minimize inconvenience. Students of any site are required to travel one day a week on average.

> "Students of any site are required to travel on average 1 day a week"

The mandatory courses in the programme provide the fundamental knowledge and ability essential for any security engineer. First a general overview is provided into computer security and cryptography, then the toolbox needed by any security system is treated. Protocols can be hard to get right. The Protocol Verification course shows methods to detect subtle errors in the protocol design that may compromise the security. Common vulnerabilities encountered in software, such as the infamous buffer overflow, along with methods to prevent these are treated in the course Software Security. Security evaluation, risk assessment and risk management, all needed to make solid business decisions in matters of IT Security, is treated in the course Security in Organizations. As practically all computers systems are currently part of a networked system, the Network Security course describes the threats and protection methods part of the networked world.

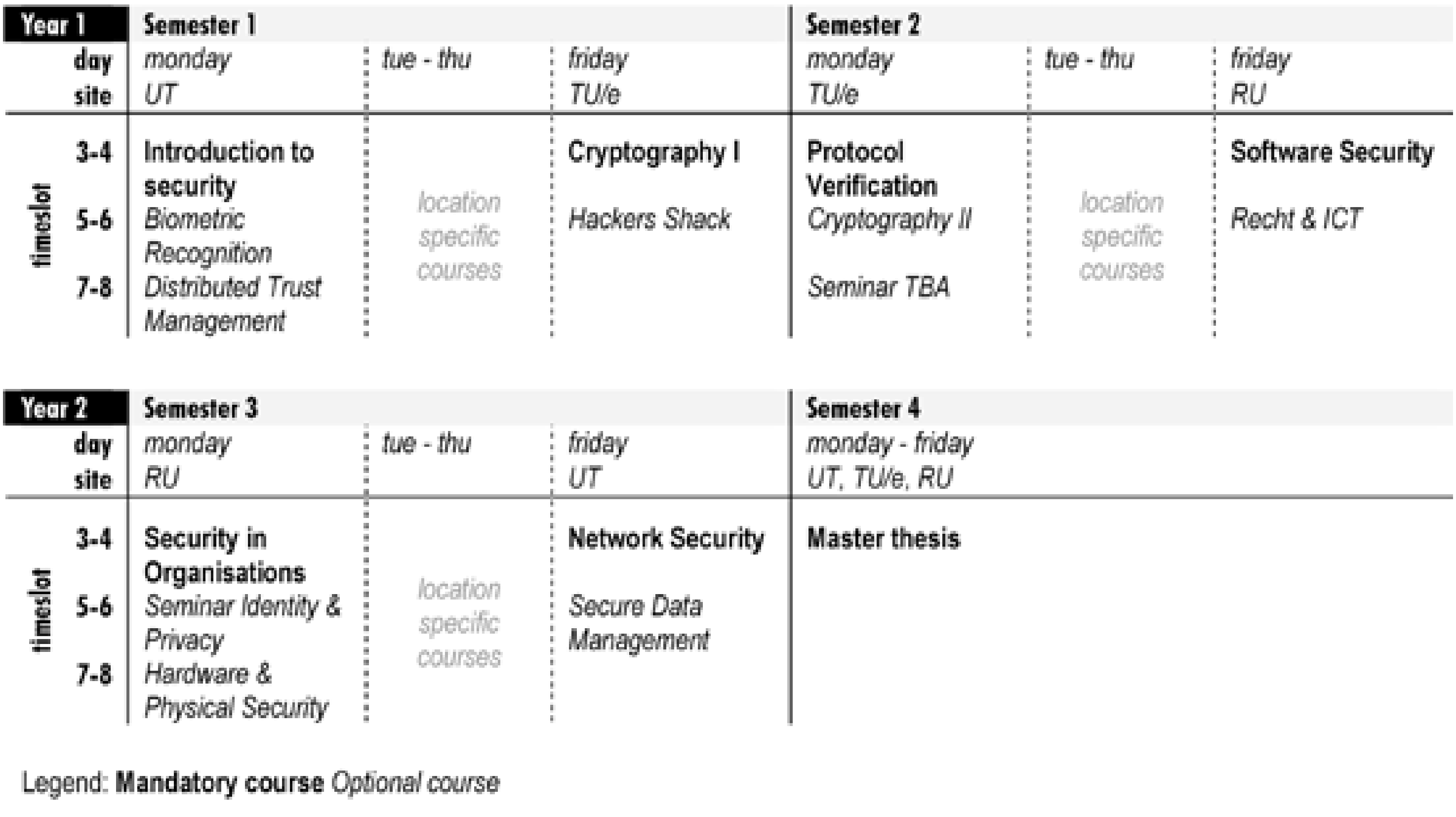
ICT Security education in the Netherlands

The Kerckhoff Computers Security master complements the security related educational programmes in the Netherlands by offering a programme of a technical nature to full-time computer science students. Other security related education programmes in the Netherlands are:

- TIAS Master of Security in Information Technology, headed by prof. H van Tilborg (TU/e). This is a post doctoral programme, with a broader, more business school oriented curriculum. The intended audience consists of people currently working in ICT and EDP auditing, running for several years now.
- TIAS Master of Information Security Management, headed by mr. P. van Dijken. Similar to the other TIAS master's course, except the curriculum covers the non-technical aspects of information security. Opens September 2006.
- The Hogeschool Arnhem Nijmegen (HAN) will offer a master of Risk and Security Management starting September 2006.

Finally, more information can be found on the website www.kerckhoffs-institute.org ■

Jerry den Hartog



Year 1		Semester 1			Semester 2		
	day	*monday*	*tue - thu*	*friday*	*monday*	*tue - thu*	*friday*
	site	*UT*		*TU/e*	*TU/e*		*RU*
timeslot	3-4	**Introduction to security**	location specific courses	**Cryptography I**	**Protocol Verification**	location specific courses	**Software Security**
	5-6	*Biometric Recognition*		*Hackers Shack*	*Cryptography II*		*Recht & ICT*
	7-8	*Distributed Trust Management*			*Seminar TBA*		

Year 2		Semester 3			Semester 4
	day	*monday*	*tue - thu*	*friday*	*monday - friday*
	site	*RU*		*UT*	*UT, TU/e, RU*
timeslot	3-4	**Security in Organisations**	location specific courses	**Network Security**	**Master thesis**
	5-6	*Seminar Identity & Privacy*		*Secure Data Management*	
	7-8	*Hardware & Physical Security*			

Legend: **Mandatory course** *Optional course*

Figure 2: Curriculum schedule

Although rootkits have been given a lot of media attention lately, a thorough explanation of what this term actually entails is rarely seen. As a result, many misconceptions about them seem to be floating around.

Rootkits Unveiled

Take the notorious Sony Rootkit as an example. While this topic has been covered extensively in all kinds of media outlets, misunderstandings about it are wide-spread. Most people seem to think that it is a real rootkit, while its name is actually nothing more than an ironic reference to the fact it simply uses techniques that are commonly used by rootkits. The main aim of this article is therefore to try and improve the general understanding of the nature of rootkits. To do this, one of the more successful rootkits, *adore-ng*, will be briefly examined as a case study.

While the term itself is too young to appear in any dictionary, rootkits are commonly defined as a tool (or a set of tools), used after successfully breaking into a computer system, which purpose is to give crackers an automated, and hence lightning fast, means to hide their presence on compromised systems. Usually rootkits hide logins, processes and logs, as well as sometimes even sniff terminals, connections and possibly even the keyboard. Not only will a rootkit generally try to hide any evidence that a breach of a system has occurred, it will also try to continuously hide the presence of the cracker after the actual break-in itself.

Originally (i.e. at the end of the 80's), the term rootkit was used to refer to a set of standard UNIX binaries like *ps*, *netstat* and *password*, which were slightly modified and recompiled. The idea was to use them to replace those standard programs on cracked systems. These new binaries would then carefully hide any trace of the cracker that would normally be shown by their original versions. While probably still effective on many systems, nowadays it is easy to protect oneself against these "application level" rootkits by using file integrity systems, like the popular multiplatform tool Samhain.

As a counteraction, in the mid 90's, a new type of rootkit emerged, the so-called kernel level rootkits. While the previously mentioned rootkits were restricted to user space, these new types resided in kernel space. Theoretically, this would give the rootkit complete control over the system and hence, all detection tools run from within user space could potentially be deceived by the rootkit. Luckily, in practice this is something impossible to achieve, yet we see that detection methods are always one step behind on the latest rootkit techniques. The two key elements for protecting oneself against this threat are therefore prevention and preparation. It should be prevented that a system can easily be infected by a rootkit and the necessary information should be extracted from a clean system before putting it in a hostile environment. To effectively implement a strategy based on this it is first necessary to known the enemy. Let us therefore take a look at a real kernel level rootkit, adore-ng, and see how this knowledge helps us in defending against it.

There are two ways adore-ng can take over a system, both relying on Linux Loadable Kernel Modules (LKMs). These LKMs are small object files that can be dynamically loaded and unloaded from the Linux kernel. The original method employed by adore-ng was to load an LKM containing adore-ng, followed by loading a special cleaner LKM which completely hides the LKM which was loaded last (which should be adore-ng).

As soon as tools started to show up that could detect these hidden LKMs, a new method was added to adore-ng though. This method consists of infecting other LKMs already residing on the system, which is done by adding adore-ng's own initialization and exit procedures to the infected LKM, which both contain references to the original init, respectively exit procedures. As a result, the LKM will still behave exactly like before, except that it now also secretly inserts adore-ng in the kernel as soon as it is loaded. A good way to prepare a system against these attacks is again by using file integrity checks, this time on the LKMs. In addition one should keep track that no rogue modules are loaded. An alternative strategy would be to disable LKM support in the Linux kernel after booting. Finally, some programs, like the already mentioned Samhain, offer ways to verify the integrity of a running kernel.

While effective strategies to rapidly discover adore-ng infections or to avoid them altogether hence exist, they rely on the fact that the system has been secured while it was still clean. However, detecting adore-ng on a system which has not been prepared in advance can be a difficult task. One reason for this is the complete absence of adore-ng in user space. While adore-ng can be used to hide files and processes on a system and to execute programs as root from within user space, this functionality is only available when a shell authenticates first using a secret key. If no knowledge of this key is available, adore-ng will stay completely hidden.

> “a solution to a problem rarely comes as a single tool”

When there is the suspicion that a system has been compromised by a rootkit, the first thing that comes in mind is probably to run a rootkit scanner. This could however cause a feeling of false security. During recent tests, it was discovered that when adore-ng was busy hiding files and processes, the scanners indeed detected the rootkit. However, when adore-ng was not doing this, its presence went completely undetected!

New proof-of-concept tools have recently emerged that could scan kernel memory looking for signatures of adore-ng. Yet, these are still not very practical and very prone to generating false positives. Recently, in the paper “Searching for the Adore rootkit : ng” a new technique has been discovered that could detect adore-ng and even recover its secret key. While proof-of-concept code was added to the paper, currently no tools exist that implement this method.

Even in this brief case study, we see a concept that seems to return in all aspects of computer security: a solution to a problem rarely comes as a single tool. Only through knowledge, prevention and preparation systems can truly be secured from rootkits. ■

Olivier Toelen

Links :
http://stealth.openwall.net/rootkits/
http://www.la-samhna.de/samhain/
http://www.irc2.com/adore-ng-detection.pdf

Belastingdienst FC

Internet wordt vuiler en vuiler, de virussen slimmer en agressiever.

Het moment is nabij dat u de narigheid niet meer buiten de deur kunt houden. Althans, als u blijft vasthouden aan het 'kasteel-concept' van beveiliging. Wat houdt dat in?

kahuna

Maak een hotel van uw kasteel

'inchecken'

Virtuele kasteelheren zien hun organisatie als een losstaand bouwsel dat ze afdoende denken te beschermen met een enkele firewall en antivirussoftware tussen internet en het eigen netwerk – de dikke muren, de slotgracht en de ophaalbrug van vroeger. De traditionele kastelen hebben echter geen verweer tegen alles wat uit de lucht of uit de grond komt. Elke innovatie in de oorlogsvoering, zoals de uitvinding van het buskruit en de ontwikkeling van het vliegtuig, verzwakte het kasteelconcept. In onze tijd is het nagenoeg onbruikbaar geworden. Ook in informatiebeveiliging tekent zich een wapenwedloop af. Het traditionele beveiligingsconcept – het 'kasteel' – is niet opgewassen tegen de aanvallen van vandaag en morgen. Die aanvallen zullen alleen maar agressiever en vernuftiger zijn.

Er valt niet aan te ontkomen: uw eigen netwerk raakt straks net zo vervuild als het publieke internet. Wat te doen? Het 'hotel-beveiligingsconcept' biedt soelaas. In een echt hotel zijn er heel wat ruimtes algemeen toegankelijk: de receptie, de lobby, het restaurant. De bezoekers worden ongemerkt in de gaten gehouden door de portier en de andere hotelmedewerkers. De beveiligingsdienst houdt met camera's en detectiesystemen een oogje in het zeil. De hotelkamers en de 'werkruimtes' – de keukens, de voorraadkamers en de kantoren – zijn veel strenger beveiligd: daar kom je alleen in als je bevoegd bent. Het hotel vertoont een prettige en werkbare combinatie: semi-open als het kan, gesloten als het moet. Die kant gaat het op met informatiebeveiliging.

In het hotel-concept fungeert elke pc en elke server als 'hotelkamer'. Een personal firewall, een certificaat en encryptie zorgen ervoor dat onbevoegden niet bij de pc naar binnen kunnen. Ook de servers worden uitgerust met certificaten, host firewalls en specifieke applicaties voor authenticatie en tweedelijnsbeveiliging. Tussen de cliënten en de applicaties komen firewalls met tal van DMZ's (demilitarized zones) voor de neutralisering van het dataverkeer. VLAN's en systemen voor bandbreedtecontrole bewaken de bandbreedte en segmenteren het netwerk om een uitbraak te beteugelen. Systemen voor intrusion detection en prevention weren ongewenste aanvallers en sluiten netwerknodes af bij verdacht verkeer. Volledig geautomatiseerd op basis van artificiële intelligentie

Rhett Oudkerk Pool, CEO and founder Kahuna group en vooraf gedefinieerde rules. Alles wordt dubbel uitgevoerd: valt de ene verdedigingslinie uit, dan schuift de andere er voor in de plaats.

Toekomstmuziek? Bepaald niet. Kahuna brengt dit beveiligingsconcept dagelijks in de praktijk. Toonaangevende opdrachtgevers zoals Nederlandse Spoorwegen en Wehkamp zijn beveiligd volgens het hotel-concept. Een open omgeving zoals de NS kan zelfs niet zonder de hotel-aanpak. Stationsgebouwen zijn bij uitstek open, publieke gebouwen. De kans dat iemand binnenkomt en ergens op het netwerk inprikt is niet denkbeeldig. Dan biedt een traditionele firewall maar beperkte bescherming. Daarom beveiligt NS ook het interne verkeer tussen mensen en bedrijfssystemen. De NS heeft een centrale omgeving gecreëerd waar de bedrijfskritische systemen staan opgesteld en waar al het interne en externe verkeer langskomt. Die omgeving is totaal gecontroleerd. Het is onze stellige verwachting dat elke organisatie van een zekere omvang het hotel-concept zal omarmen.

Hoe dan ook: U bent beter af in een hotelkamer dan in een tochtig kasteel! Tijd om in te checken! ■

Over Kahuna:

Kahuna Groep

Kahuna helpt organisaties op elk moment, op elke plaats veilig en efficiënt informatie uit te wisselen. Vandaar het credo: control the flow.

Kahuna Network Solutions biedt in de vorm van Managed Security snelle, veilige en altijd beschikbare technologie, specifiek gericht op informatiebeveiliging en thuis/telewerken. Kahuna Network Solutions adviseert ook over security beleid.

Kahuna Business Solutions levert innovatieve toepassingen op het gebied van eCRM en Business Intelligence&Monitoring waarmee organisaties grote aantallen klantcontacten effectiever en efficiënter kunnen afhandelen en managen.

Kahuna is een Nederlands bedrijf, opgericht in 1997 en gevestigd in Amersfoort. Kahuna heeft ongeveer 70 medewerkers in dienst. Kijk voor meer informatie op www.kahuna.nl.

Het blad Banking & Finance heeft de digitale kluis-technologie van Kahuna genomineerd voor de Innovation Award 2005. Het Weekblad Intermediair heeft Kahuna in 2004 opgenomen in de top-20 van innovatieve ICT bedrijven. Kahuna is voor het vierde opeenvolgende jaar te vinden in de Deloitte Fast50 (Nederland) en Fast500 (EMEA) van snelgroeiende hightech-bedrijven. Kahuna is winnaar van de ComputerPartner Award 2003 voor de meest innovatieve reseller en van de ICT Company Award 2002.

In the nineties, the concept of Instant Messaging was introduced and became very popular. Today, IM is not only used by end users, but also companies use it for their internal communication. What kind of security risk is there for those users and companies? How easy is it to intercept messages sent across IM networks? And, how sure can you be about the identity on the other side of the line?

See the Kryptos website for the full paper.

IM Network Security

How safe is your chat?

Protocols

The biggest IM networks currently are MSN, AOL/AIM and Yahoo [1]. Due to their size there is a lot of documentation available and there are also alternative implementations for the protocols they use in other clients. The fourth protocol we investigated is the Jabber protocol. This is a fully open specification, contrary to the other three protocols. The new chat client by Google, Google Talk, also uses Jabber as its protocol.

Oscar (AOL / ICQ)

The Open System for Communication in Realtime (OSCAR) protocol [2] is the official AIM protocol created by AOL. This protocol is also used by the ICQ chat client. When AOL bought Mirabilis (the creator of ICQ), the ICQ protocol developed towards OSCAR until the moment where it is compatible with OSCAR. Nowadays, OSCAR is the recommended way of connecting to the ICQ network [3]. Contrary to its name, the protocol is not open and all the knowledge outside AOL comes from reverse engineering the protocol.

OSCAR uses a mechanism where a separate authentication server is accessed and a session cookie is retrieved. This session cookie is used in further communication with the different OSCAR services. This session cookie could be intercepted and this would allow the attacker to impersonate the legitimate user. This is not trivial, as it would require that the valid user does not try to re-authenticate. This is necessary because OSCAR does not allow for a user to be logged in multiple times [6, 11].

OSCAR does not send its messages encrypted over the network by default. This means that eaves-dropping is very easy if one can access a machine that is in the path of the messages. In a student dorm which uses for example a NAT router, the student who administers this system could easily eaves-drop on his roommates without them knowing.

In AIM version 5.2, AOL introduced a feature that gives users the ability to communicate securely using a PKI encryption system. The certificates can be used to send encrypted and signed messages. Encrypted chatting requires that both users have a public/private key. The encryption system can also be used for file transfers and in chat rooms with multiple users [7].

The default OSCAR client, namely AIM, stores a digest of the password on the system of a user. This digest could be obtained by an attacker so they can login as the attacked user.

This is extremely hard to prevent, because the official client has to be able to sign in, so a malicious application can also do it the same way the official client does it. The only way to prevent this is using advanced access control systems that can operate on an application level and to only allow access to specific information for a certain application.

MSN

MSN is the Microsoft solution for Instant Messaging. It uses the proprietary MSN Messenger protocol for communication between client and server. Currently the protocol is fairly known to the community due to an IETF internet draft describing an early version of the messenger protocol[5]. The protocols did change a lot since then, but an active community of engineers tracks those changes constantly.

In this section we will focus on MSNP9, which is an older, but well documented version of the MSN protocol. MSNP9 uses three different servers. When a user first connects to the network, he is connecting with a Dispatch Server. This server will negotiate with the client about the protocol version to use and then refers the user to a particular Notification Server (NS). This NS is the main server component of the MSN network. It authenticates the user, synchronizes its properties and handles all asynchronous events. The connection with the NS is a persistent connection that will remain during the complete session [8, 9].

The largest vulnerability of the MSN protocol lies in the fact that MSN handles are also used for many web applications served by Microsoft, such as Hotmail. If an attacker could obtain the session cookie he could hijack the session and login to change the password of the account.

Currently all versions of the MSN protocol use plain text messages to communicate with the MSN servers. As a result of this everybody in the route of the message can read the conversation with an Ethernet sniffer.

Denial of Service attacks (DoS) on MSN accounts are easy to perform. A protection mechanism of the service can be abused to shutdown an account for 24 hours. The attacker fires many logins with the wrong password and the MSN service will disable the account.

"Many tools exist to "recover" a lost password from a local machine"

All versions of MSN Messenger provide the user with options to store their password. Due to the weak encryption that MSN clients use to store the password, decrypting these saved password is just a matter of milliseconds. Many tools exist to "recover" a lost password from a local machine.

Yahoo!

Yahoo! Messenger uses the proprietary Yahoo! Messenger protocol. This protocol is not documented anywhere and the information that is available is reverse engineered and not always accurate. Though the protocol is poorly documented, there are some key issues that can be identified [10].

As with many other IM protocols, Yahoo! Messenger does not provide encryption. Any person with access to an intermediate router is able to sniff packets containing Yahoo! Messenger conversations.

Older versions of Yahoo! Messenger were vulnerable for Denial of Service attacks. These versions crashed when a TCP connection was made on port 5010 and some random bytes were send. This problem is currently fixed.

The Yahoo! Messenger client also provides a save password function like all the other clients. At the time of this writing, the client is at version 7.5 and most password recovery is not yet supported, but older versions are vulnerable.

Jabber (XMPP)

The XMPP protocol developed by the Jabber foundation is a completely open protocol that has been approved by the IETF as RFCs 3920 and 3921 [4]. The protocol is XML based and its architecture greatly resembles email. User accounts are in the form of user@domain.com and each domain provides its own Jabber server, creating a large distributed network. Jabber is also the protocol used by Google Talk.

Besides encrypting the connections using TLS/SSL, it is also possible to sign and encrypt the messages that are sent individually. This can be done using GnuPG in almost the same way as with email. This prevents the Jabber servers from reading the messages and gives the receiving party the opportunity to verify who sent it.

Because of the decentralized architecture of the Jabber network, it is very hard to attack with a denial of service, simply because there is no single point of failure. The different server implementations can also contain rate limiting in order to prevent mass messaging or an unlimited amount of connections. This is for example available in the open source Jabberd2 implementation [5]. These limitations make a denial of service attack extra hard.

Many of the different security measures mentioned in the previous criteria, depend on whether it is supported by the client. Almost all clients support TLS and/or SSL for encrypting the connection, but only few offer signing and encrypting individual messages. Because of the open nature of Jabber, new features are developed continuously. This makes it very hard for clients to support all these features. The diversity of clients makes it also less interesting for hackers to create for example a worm if a vulnerability is found in a certain client. The user base they can affect is relatively small compared to for example the user base of the standard AIM client.

Conclusion

It is strange to see that the most popular networks, Oscar, MSN and Yahoo!, do not use any form of encryption. All three protocols send the messages as plain text over the Internet. It is also very clear that the Jabber community developed a potentially much stronger and safer IM protocol that is, with TLS/SSL and GnuPG installed, hardly beatable for attackers.

An other conclusion we can make is that all security measures stop at the computer where the client software is installed. If a password is saved on the local machine it can be exposed. In order to prevent this, far more sophisticated access control systems are necessary that operate at application level. These techniques are still in development and not part of the everyday computer system.

Recommendations

We think that most IM networks would benefit from the use of encryption. Everybody with access to for instance the router in a student dorm can create logs of all conversations made. Encryption like Jabber provides, does not only prevent eaves-dropping, but also prevents man-in-the-middle attacks.

Also, the signing option offered by Jabber should be considered by other IM vendors. Signing makes impersonating virtually impossible. AOL already has implemented this in AIM and we think that is a good thing. ■

Dirkjan Bussink
Geert Vos

References

[1] Andrew Lipsman -comScore Networks. Europe surpasses north america in instant messenger users, comscore study reveals. http://www.comscore.com/press/release.asp?press=800, 2006.

[2] AOL. OSCAR: Open System for Communication in Realtime. , 2005.

[3] Gaim. Gaim protocols. http://gaim.sourceforge.net/protocol.php, 2006.

[4] Jabber Software Foundation. Extensible Messaging and Presence Protocol (XMPP). http://www.xmpp.org/, 1999.

[5] W. Kamishlian and R. Norris. Jabberd 2 Installation and Administration Guide. http://jabberd.jabberstudio.org/2/docs/jabberd_guide.html, 2003.

[6] K. Leam, D. Walluck, T. Hoover, and R. Tenney. The OSCAR protocol documentation project. http://joust.kano.net/wiki/oscar/moin.cgi/, 2005.

[7] J. Lin. AIM Encryption Certificates. http://www.ocf.berkeley.edu/~jjlin/aim-certs. html, 2006.

[8] M. Mintz and A. Sayers. unofficial guide to the MSN Messenger protocol. http://www. hypothetic.org/docs/msn/, 2006.

[9] R. Movva and W. Lai. MSN Messenger Service 1.0 Protocol. http://www.hypothetic.org/ docs/msn/ietf_draft.txt, 1999.

[10] L. Project. Yahoo Messenger Protocol v 9. http://libyahoo2.sourceforge.net/ymsg-9. txt, 2004.

[11] A. Shutko. OSCAR (ICQ v7/v8/v9) protocol documentation. http://iserverd.khstu.ru/ oscar/, 2005.

ADVERTENTIE

Quinity SK

Dr. Ronald Leenes is associate professor at the Tilburg Institute of Law, Technology, and Society, where he is responsible for monitoring new technologies and their legal implications. His current research interest is identity fraud and identity management and he is currently involved in the PRIME (PRivacy and Identity Management Europe) project, which aims to provide an architecture for privacy enhanced identity management in Europe.

We asked him some questions about future developments in IT-security technologies and their influence on our privacy.

IT Security and Privacy

interviewing Ronald Leenes

According to dr. Leenes, one of the most important technological developments in the near future on the subject of privacy and security will be RFID (Radio Frequency IDentification). From august 2006, RFID chips will be incorporated into our passports, initially containing a facial scan and eighteen months later also fingerprints. Because RFID tags are readable from a distance, this might seriously impact our privacy. The information on our new passports is secured by a key generated from two lines at the bottom of the passport called the “machine readable zone”, but anyone with physical access to the passport can generate this key and thus read the embedded information. Dr. Leenes is afraid that access to this information will not be limited to the public sector for which it was meant, but that it will also be available to hotels, travel agencies and other parties of whoms intentions one can only guess. While the information itself isn’t even that special, the digital form it has makes it possible to do more with it than with the conventional paper kind. Imagine, for example, using the facial scans to detect a person in a crowd by means of cameras. Once your data gets “out there”, you lose all control over it.

As technologies like RFID become more and more established, the amount of data that can be gathered about a person increases rapidly. Not only physical objects, but also people are likely to have themselves tagged. At the Baya Beach Club, you can already receive a sub dermal RFID chip for easy entry and payment, but these chips are plain RFID tags, which are readable by anyone who wants to. This makes it easy to link who you are to where you’ve been, without you knowing about it. There is already a lot of data being accumulated. Dr. Leenes explains it is hard to get a grip on what data controllers, the people that collect personal data, want to use this data for, but apparently they seem to have a general idea that something useful can be done with it. Decisions are already taken based on this data, influencing our freedom of choice. Based on profile data that exists beforehand, companies like travel agencies decide whether you are a desired customer and if not, offer you absurd prices or refuse to serve you at all. This kind of profile data is gathered for example by major advert suppliers who aggregate information about visitors of the many websites showing their adverts.

Although we already have some legislation in the Netherlands that limits what companies can do with our personal data in the form of ‘the law on the protection of personal data’,

which balances on two basic ideas: first of all it is important that information can be exchanged freely. It is of economic interest that (personal) data is exchangeable under certain circumstances. Secondly, this personal data is closely related to one’s privacy, so the law also attempts to protect individual’s privacy by limiting what one can do with personal data and under what conditions. In short, the purpose for which the data is being collected must be clear to the person it concerns. This so called data subject in many cases has to give his permission if the data is to be used, and then it may still only be used for (with some exceptions) the primary purpose as explained to the subject. It may certainly not be sold to someone else.

Our legislation on this subject is not too bad, according to Ronald Leenes, but the law on the protection of personal data is based strongly on the idea that there is a single data controller involved who collects personal data about a data subject, like in the classic directory of addresses. With the development of technologies like ambient intelligence, we are moving to a scenario where it is unclear who the data controller is. To recognize and anticipate one's personal preferences to, for example, adjust the temperature and light to one's liking, a system needs personal data about a living person. Under these circumstances many data can be regarded as personal, certainly IP-addresses but maybe even sets of preferences relating to temperature, humidity, luminance etc. If you have an intelligent home, who then is the data controller? Is it you? What if your refrigerator contacts the supermarket to tell them you're out of milk? That would make the supermarket the data controller. The concept of a data controller will become more diffuse and at the same time, the definition of what is considered personal data becomes more vague. The profile data mentioned earlier is like a cloud of clicking behaviour, search keywords and more, which doesn't fall under the current definition of personal data.

> "Once your data gets "out there", you lose all control over it"

However, this might change in the future. When companies use profile data to take decisions about you, we might want to consider this data "personal", because it touches our autonomy to make our own choices. Dr. Leenes expects the law is reaching some limits, so we have to rethink what we are trying to accomplish. Basically we want a decent treatment of individuals which must be reflected in the regulations. In time, we might conclude that the current legislation doesn't accomplish this, but rather the subset that deals with classic databases. The law on the protection of personal data is currently being evaluated, so it is quite possible there will be some changes to the legislation in the future.

Of course, the law on the protection of personal data is like any law. There are plenty of people driving too fast on our highways, even though there are laws that forbid this. Some of them may have missed a sign and may not be aware of the speed limit in effect, but others make an assessment of the risks and stakes, because speeding will gain them more than a possible fine will cost. This is also the case for the law on the protection of personal data and we should ask ourselves if this kind of behaviour is intended and desirable. In general, we can say the instrument isn't working perfectly, because the Data Protection Authorities are not very active and do not have proper resources and powers.

A solution to ensure compliance to the law at hand is to be found in technology. This is not something new. We've been using speed bumps to make speeding impossible for years, so we can make it physically impossible to do certain operations on data as well. This can be compared to digital rights management systems for music. Most of these systems work by encrypting the data such that a key is required to play the music and this key in turn is linked to a valid purchase of the music. The same can be done to personal data: encrypt it with a key, which is only available to people who are eligible to use the data. By using this kind of Privacy Enhancing Technologies we can enforce what can or cannot be done with the data. In a way, our government has made an attempt to do this with the new passports, but it is doubtful whether this protection is adequate in this case.

Another party that is interested in our online and offline whereabouts is our government itself. The adoption of a directive on data retention by the European Council cleared the path for member states to oblige public communications providers to collect and keep data for the purpose of the investigation of serious crime. Dr. Leenes states we're bound to get in trouble, because it is unclear what exactly "serious crime" is. Obviously simple theft doesn't justify the police snooping into your personal data, but what does? When it comes to dealing with this kind of power, people always start off with the best intentions, but it always slowly turns into a situation where everyone is convinced that everything is functioning as it's supposed to, while in reality things are happening that are obviously unacceptable.

According to Dr. Leenes, it's all about balance of powers. Power corrupts. If you put a single party in charge, there is bound to be trouble, so we need to build in checks and balances. Therefore, if society wants to go down the path of data retention, we should at least try to prevent the abuse of data by storing it where it is generated, and have the justice department query this data in cases where this is justified after having obtained proper warrants. Even though it might seem tempting to have the justice department bear the costs for something they wanted in the first place, but such a centralized storage of data with the same department that intends to use it is deadly. It will be impossible to know if the data is abused, let alone control it. Furthermore, such a single point of failure poses a serious security risk. In any way, there have to be checks and balances when it comes to deciding when to use the data. There should be at least an independent party involved when such a decision is made, for instance a judge, since judges look after interests other than the apprehension of criminals.

Having a centralized database of personal traffic and communications data introduces another possibility: preventive detention. Because there is so much information available, it is tempting to execute regular “fishing expeditions” on this data to determine beforehand which persons poses a risk and detain them. Dr. Leenes thinks this is an utmost dangerous development. To cite Cardinal Richelieu: “If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him.” How long do I have to be watched to get the equivalent of six lines? By allowing preventive detention, we move the burden of proof from the accuser to the accused. Currently, in order to prosecute a suspect, the public prosecutor has to clearly state the crimes the suspect is accused of and has to prove that the conditions of the respective legal provisions are indeed met. When you can get accused on grounds of a supposedly suspicious pattern found in a database, it becomes very hard to prove that the conclusions taken were wrong, that the data was interpreted incorrectly and means something else. Furthermore, most data, like e-mail messages and IP-addresses, can easily be manipulated, which makes it most questionable data. In general, this means that real criminals and terrorists can easily withdraw themselves from so called ‘fishing expeditions’ by simply not using cell phones, e-mail and so on, while normal people become suspects of things they never did, with evidence that is very hard to disprove.

In general, there seems to be an overly optimistic view on what kind of relevant conclusions can be drawn on the basis of traffic data, but if we are so eager to decide that we want to collect and keep this kind of data, it is better to do it in a well-considered way than to just start recording and see what can be done with the resulting data. We should not rush into this kind of measures because of terrorist attacks where these measures would not even have been the least effective.

A more important effect of data retention is that once people know they are being observed, they tend to adjust their behavior. If you put speed cameras alongside the road, they don’t have to be loaded with film in order to make people slow down and obey the speed limits. If you know your boss watches your web browsing history, you won’t visit adult sites. Observation makes the observed behave in the way he thinks is considered socially desirable by the observators. In the case of data retention, who will be the observator? We might trust our current government and our current employer, but who is to say what they will be like in five to ten years? Obviously we have to think about the consequences before we allow all kinds of things to be done with collected data.

When it comes to our privacy, how it will all turn out in the future is hard to say. On one hand, the signals are positive. The European Commission is working on the so-called 7th framework, of which privacy protection is an important aspect. On the other hand, the same European Commission approved the data retention directive that seriously influences that privacy aspect. At least it is promising to see that even large parties like Microsoft are currently seeking to increase privacy, after the failure of their attempt to provide a federated identity management service. In the adoption of more privacy friendly technologies, market forces might turn out to be very important. Customers need to learn to speak up more when they feel their privacy is being undermined. Only then will businesses realize there is a market for privacy friendly services and adopt them. In the end, privacy friendly services are just as bound to Metcalfe’s law as the fax machine: if two people have one, it’s a worthless device, but if everyone has one, it has become an incredibly useful communications device. ■

Michel Jansen
Stephan Roolvink

ADVERTENTIE

Philips SK

More and more critical services depend on computer networks and these networks are increasingly vulnerable for cyber-terrorism and attacks due to their connection to the Internet. To provide sufficient protection against these threads a secure operating system is mandatory. NSA's Security-Enhanced Linux (SELinux) is such an operating system. This summary of the original paper will describe the theoretical principles upon which SELinux is build. Then it explains how these principles are used to protect your system. Finally the paper lists a couple of alternatives to SELinux.

See the Kryptos website for the full paper.

Toward a Safer System With Security Enhanced Linux

Introduction

The number of computers connected through networks has grown rapidly over the last decades and more and more critical services totally rely on these computer networks. The networks are often connected to the Internet making their hosts vulnerable for cyber-terrorism, espionage, viruses, worms and malicious hackers. The operating system is an important link in end-to-end security, it is responsible for protecting application-space against hostile attacks. A flaw in this protection will result in system-wide vulnerabilities.

The U.S. Department of Defense's National Security Agency recognized the importance of a secure operating system and came up with a solution called Security-Enhanced Linux or SELinux for short. SELinux was introduced in the open source community in December 2000.

The following sections will describe SELinux in more detail. Section 2 will elaborate on some of its key features. Then sections 3 shows how you can protect your operating system with SELinux. Section 4 describes possible alternatives to SELinux and section 5 will conclude the paper.

SELinux

SELinux is a flexible implementation of a mandatory access control architecture called Flask that can be built into the Linux kernel. It is based on the principle of 'least privilege' and protects the system from malicious or flawed applications. Key features of SELinux are mandatory access control (MAC), role-based access control (RBAC) and type enforcement (TE). These features as well as the Flask architecture will be discussed in the following subsections.

Mandatory Access Control

SELinux is based on MAC, a secure type of access control. In a MAC architecture access decisions are based on labels that can contain a variety of security relevant information instead of only the user identity as with discretionary access control (DAC), which is used in most operating systems. SELinux has three security context attributes: an identity, a role, and a type.

A MAC policy is defined by a security policy administrator and consists of a set of functions that take security attributes of subjects and objects as input and output whether access is granted or not.

SELinux supports two complementary approaches to configure the system, type enforcement and role-based access control.

Type Enforcement

Type enforcement is used to describe fine grained access controls. Each object in the system is assigned a type and each subject has an associated domain. In the policy configuration is specified which domains are allowed to access which type. Also the interactions among domains that are allowed are specified. Users are then authorized to access a specific set of domains.

SELinux differs slightly from the traditional TE model as described above, since it makes no distinction between domains and types. Domains are simply types assigned to processes. Another difference is the way user privileges are assigned. Instead of authorizing users to access domains users are assigned to roles. RBAC is then used to assign privileges to the different roles.

“The main memory has always been subject to many attacks”

Role Based Access Control

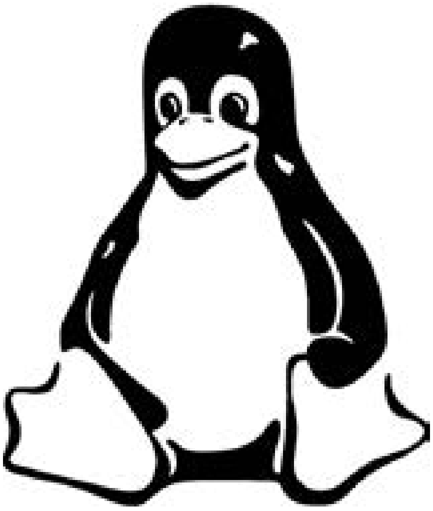
The RBAC configuration file defines an extensible set of roles that can be assigned to users. Which roles a user can adopt and the domains that can be accessed by these roles are specified by the security policy. It is also possible to specify a dominance hierarchy in which one user can dominate the privileges of other users.

Flux Advanced Security Kernel

As mentioned earlier SELinux is an implementation of the Flux Advanced Security Kernel (Flask) architecture. One of the characteristics of Flask is that it separates the security policy logic from the mechanism that enforces the policy. A security server holds the security policy logic and provides interfaces for obtaining security policy decisions while object manager components are responsible for enforcing the security policy. An object manager communicates with the security server to perform permission checks and update permissions. This communication goes through the Access Vector Cache (AVC). This component caches access decisions to speed the process up.

Protecting your OS with SE-Linux

As stated in the introduction, a lot of harm can be caused to computer systems and there is a great demand for more secure operating systems.



But what exactly should be protected? Are the SELinux components MAC, TE and RBAC sufficient to protect systems against the attacks mentioned?

Vulnerabilities

Let’s have a look at the typical weak spots in a system. There are three main categories that need protection: the main memory, the file system and the network.

The main memory has always been subject to many attacks, such as buffer overflows, heap overflows and all kinds of variants resulting in the possibility of executing malicious code or by changing the control flow of a program.

The file system usually contains data and programs that should not be accessible by all users. Exploits in the file system often attempt to gain access to these data or programs.

Well known network exploits are Denial of Service (DoS) attacks, eavesdropping, backdoors and Man in the Middle attacks. Luckily only the applications that are accessible trough the network need protection, but the attacker can be anywhere, and with so many users on the Internet there will be users that have bad intentions.

Solutions

SELinux policies can enforce restrictions on every file but also on processes and sockets. However, SELinux can not protect against buffer overflow exploits or code injection.

The power of SELinux lies in restricting and minimizing the damage that is often the result of the exploits: gaining illegal access or corrupting a system. Buffer overflows are often used to acquire root access. Suppose an attacker exploits and overflows a buffer of a program that runs with super user rights. With a good policy, the damage will be much less than without such a policy, because every program in each domain is set up with limited capabilities.

Alternatives

Besides SELinux there are many other attempts at creating a more secure operating system. This section will give a very short overview of the other available operating systems that have their main focus at security.

Adamantix

Adamantix started in an attempt to provide better security in a way that it is: ‘Light, comfortable, low-maintenance and affordable’ This distribution was formerly known as Trusted Debian. Key features are: Rule Set Based Access Control (RBSAC), Buffer overflow protection using

PaX and ProPolice, Easy security policies and fast and efficient tools.

Next Generation Secure Computing Base

Next Generation Secure Computing Base (NGSCB) is a vision of Microsoft to create new security technologies for the Windows platform. It was announced years ago, at that time it was called Palladium. This architecture requires special hardware support to perform its task. The project has not yet found its way into an operating system yet. However there is a small piece, BitLocker, that will be included in Microsoft Vista that can provide secure startup.

OpenBSD

OpenBSD is a fork of NetBSD and has a very strong focus on security and code correctness. It differs from the SELinux vision that states that there will always be bugs, so the best way to minimize the damage is by controlling the consequences. Whereas OpenBSD heavily tries to prevent and remove all bugs from the source code. OpenBSD includes a wide range of security features from cryptographic and randomization features to code audits and tools like ProPolice and W^X.

TrustedBSD

TrustedBSD is a fork of FreeBSD and has begun as an implementation of Common Criteria, an international standard on computer security (ISO/IEC 15408). Key features are: MAC, Access Control Lists (ACL), TE and an implementation of the FLASK architecture.

Trusted Solaris

Trusted Solaris is based on the Solaris UNIX platform by Sun Microsystems. It is mostly used by governmental organizations and intelligence agencies. Parts of Trusted Solaris are detailed task auditing, pluggable authentication, MAC, RBAC and the operating system is Common Criteria certified.

Conclusion

A secure operating system is the missing link in end-to-end security. SELinux has enhanced security mechanisms that are based on techniques such as mandatory access control, type enforcement and role-based access control. These techniques are also the pillars under most alternatives to SELinux and can be used to restrict user's privileges according to the principle of least privilege. This way applications get only access to objects they need and malicious applications are prevented from damaging anything outside their domain. Thus adding SELinux to your operating system can tremendously improve its security. ■

D. van 't Oever and J.J. de Wit
Faculty of EEMCS
University of Twente
P.O. Box 217, 7500 AE Enschede,
The Netherlands
{d.vantoever, j.j.dewit}@student.utwente.nl

This headline will make you, student, shiver. Imagine that TOST would allow any visitor (e.g. potential employer) to view all of your study results and effort. That would feel uncomfortable. Not only to you, but also to Application Service Providers – the parties that host ASP-applications. No ASP can afford these things to happen, so they take the best measures to prevent unallowed access to your data. Organisations spend a lot of money on security. However, security of (shared) web applications differs from 'ordinary' security. Not everyone acts sufficiently on that – as we can conclude from the occasional appearance of privacy-revealed-stories in the news.

Web application reveals students' personal data

Security of ASP-based web applications: what's up?

Web applications compared to 'traditional' applications

Before we will focus on security of web applications, we will start with a brief introduction on ASP-based web applications: what are they, and how do they differ from traditional applications?

The main difference with ASP is that you do not buy an application. Instead you subscribe to a service – an application service. Imagine you have some valuable goods you want to keep in a safe place. You could buy a strongbox, install it in your home and put your stuff in. Instead, you could go to a bank, rent a safe deposit, and you're doing the ASP-style. In the latter case you don't have to bother how to secure it, nor about maintenance. On the other hand, you put your eggs in someone else's basket, hoping that it is the expert he surely claims to be: he assures he won't break them and will prevent his other customers from doing the same. (And, he will prevent you from breaking someone else's eggs in the same basket).

Now, onto security. What are the differences between web applications and other applications, concerning security? The last decades we gained a lot of experience in securing applications. Why isn't that applicable to current web applications? Before we dive into that question, it is good to realise that a user runs through three steps while logging onto a secured application.

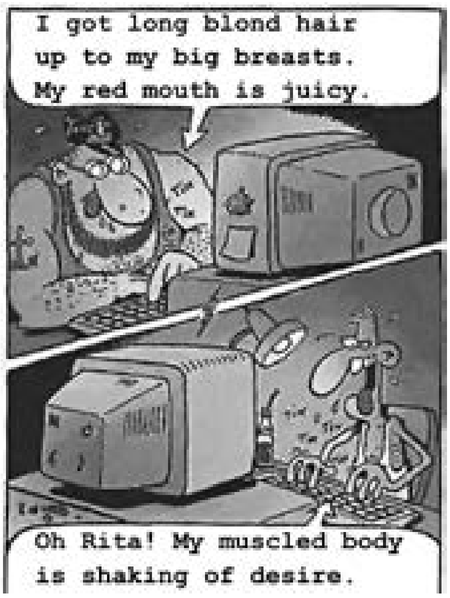
1. identification: who claims the user that he is?
2. authentication: is the user really the one he claims to be?
3. authorisation: being who he claims to be, what permissions does the user have?

Besides secured applications, these steps also apply to other circumstances in daily life, for instance to an airport. Before you depart, you have to check in (identification) and show your ticket and passport (authentication). Then, you are allowed to have a seat in the plane's passengers room, but you are not allowed to enter its cockpit (authorisation).

These three steps assist us in explaining the differences between securing web applications and securing traditional software.

Identification: who's there?

Several ASP providers provide their applications through the Internet. This highly increases the number of potential abusers compared to applications provided through a secured intranet. On the Internet, the natural barrier of a company's physical front door is absent. Anyone could "walk into your office" and try starting to identify himself as you.


I got long blond hair up to my big breasts. My red mouth is juicy.
Oh Rita! My muscled body is shaking of desire.

Thus, web applications need stronger protection on identification – a digital equivalent of a company's front door, like VPN connections. Other possibilities include putting stronger demands on usernames and passwords (requiring minimal lengths, obligatory use of special characters and unspecific error messages in case of wrong username / password. (Not: "password is wrong", but: "wrong username or password").

Authentication: do you pretend to be someone else?

Usually, identification is paired to authentication. Whereas the same characteristics count, ASP applications need extra security measures as well for authentication, compared to traditional applications. This can include smartcards, PKI (server-to-server certificates) and IP whitelisting. For highest level security (obliged when dealing with level3-personal data, like medical files) even a formal security policy is obliged by law – applying not only to the application and its data, but also to the physical security of the building and the people that operate and maintain the application and the data.

Authorisation: building Chinese walls?

Lots of ASP applications are used by several organisations (e.g. mortgage brokers using the same mortgage proposal application), where traditional applications are not. As a consequence, authorisation is needed both to protect the application from the outside world and to shield the customers' domains from each other (sometimes called "Chinese walls"). To continue the airport example, clients are only allowed to enter the plane's passenger's room, but some clients are allowed to enter the business class while others are not. The mortgage broker is only allowed to work with his own customers and products and not with his competitor's.

Although it is common to exclude users from certain parts, authorisation can also be used the other way around: to explicitly grant access to each other's data. An example of this is a medical administration system, which general practitioners use to keep track of their patients. In a shared environment, where doctors can stand in for each other, it is very useful they also can share their files in a controlled way. In fact, this is a benefit of an ASP application: it is shared. Without ASP, general practitioners would not be able to view each others' files (thus not knowing the exact state of the visiting patients) nor could they update them.

Until now, we have been focussing on differences between web applications and others, concerning security. We will finish this article with some general remarks (not to say: common misunderstandings) on securing applications – both ASP and other.

No worse security than virtual security

At any cost, prevent virtual security. Virtual security is the comfortable feeling that your stuff (building, application, anything) is perfectly secured, when in fact it is not. For example, imagine an application that is protected by the best and most outstanding security methods. So good and outstanding, it scares away the users. Instead of using that perfectly secured application, they create their own system – often involving Word, Excel and lots of paper, insecurely stored on local computers, desks or open cabinets. You thought your application was secure? It is, but nobody uses it. Virtual security.

> "You thought your application was secure? It is, but nobody uses it. Virtual security"

The disadvantages seem evident: not only is the data insecure, you also lose control on your process management, thus on your management information, your power of action and even your competitive advantage. Nothing is as insecure as that.

Security is an organisational responsibility

Besides all technical and system oriented security measures, another very important one exists: the procedural security, usually supported by technical measures like logging and tracing.

Procedural security defines what is allowed and prohibited. Compare this to traffic rules: we are to stop at red traffic lights and to obey speed limits. No technical measurements (apart from trucks equipped with speed limiting devices) are used to force us to obey these rules (and even the speed limiting is adjusted above the speed limit). Traffic cameras act as a tracing mechanism for people disobeying the rules, and penalties (varying from fines to losing your driver's licence) are the consequences of disobeying the rules.

The same goes for applications: instead of creating a very complicated technical solution that allows users to view their own files and, in specific circumstances, specific files of specific co-workers, why not create a procedure describing which files you are allowed to use on what terms. Logfile analysis shows users who disobeyed the rules, and 'career restricting penalties' prevent them and others from disobeying these rules again. This is far more effective and much easier to maintain.

Conclusion

To prevent the title of this article coming true, web-based ASP applications need to be secured tightly. However, the very nature of ASP applications (web based; large scale application distribution; lots of potential users and abusers; more often the recording of either organisation critical or privacy related data, et cetera) results in several very specific security issues. These come on top of the already not to be underestimated security issues of "traditional" applications, making security of ASP applications a complex matter and an art in itself. ■

Ir. Joost van Beek, Ir. Martin Krans – Topicus B.V. – www.topicus.nl

ENIAC-activiteiten

27 augustus 2006 - Beach-Volleybal

Het traditionale strandevenement van ENIAC. Gezellig met je mede-alumni volleyballen en tegelijkertijd bruin worden (voor diegene die dat nog niet zijn). Trommel je jaargenoten op en maak op een sportieve manier duidelijk dat jouw jaar het sportiefst is. Uiteraard kan er ook voor, tijdens, of na het beachvolleyballen gezwommen worden, om bijvoorbeeld overtollig zand af te spoelen of ter verkoeling. Daarnaast kan er dan nog even genoten worden van het eind van de vakantie, een barbecue en bijkletsen met andere alumni.

Het programma ziet er als volgt uit:

- 13:30 Verzamelen & team-indeling
- 14:00 Start Toernooi
- 18:00 Borrel & Prijsuitreiking
- 19:00 BBQ

De exacte locatie wordt nog bepaald en zal later op de website worden gepubliceerd.

10 september 2006 - Zeilen Loosdrechtse plassen

Van naast het water naar op het water, en wel op de Loosdrechtse plassen. Jammer genoeg zijn er nog niet heel veel details bekend. Het programma ziet er globaal als volgt uit:

- Verzamelen
- Vrij zeilen
- Finish bij de vertrekhaven
- Borrel
- Presentatie
- Borrel en diner

22 septeber 2006 - Borrel Op Location Philips Research

De klassieke borrel op location en dit keer bij Philips Research. Momenteel is alleen de algemene opbouw van het programma bekend, alsmede de begin- en eindtijd:

Start programma: 11:00h

- Algemene presentatie Philips Research
- Aantal inhoudelijke presentaties
- Diverse demonstraties op een aantal werkplekken.

Afsluiting: 16:30h

18 november 2006 - UT Alumnidag

De algemene alumnidag in samenwerking met alle alumniverenigingen van de UT ter ere van het 45-jarig bestaan van de UT. Op de start van deze dag organiseert ENIAC een klein symposium in het teken van 'Gaming'. Ongeveer halverwege de dag wordt er overgegaan op het algemene deel programma van de UT. Deze wordt afgesloten met een concert van Ilse de Lange.

- Verzorgd door ENIAC
  - o 10.00 - 10.30 Ontvangst
  - o 10.30 - 12.00 Programma deel 1
  - o 12.00 - 13.00 Lunch
  - o 13.00 - 15.30 Programma deel 2
- Verzorgd door de UT (centraal programma)
  - o 15.30 - 16.00 Centrale ontvangst met koffie in het Sportcentrum
  - o 16.00 - 16.15 Opening en welkom door het College van Bestuur
  - o 16.15 - 17.15 Cursus Humor (cabaret)
  - o 17.30 - 18.30 Borrel in de Faculty Club
  - o 18.30 - 20.30 Diner in de Faculty Club
  - o 20.30 - 00.00 Optredens van Ilse de Lange e.a. in het Sportcentrum

Voor bovenstaande activiteiten kun je je inschrijven via de ENIAC website www.eniac.utwente.nl/activiteiten of door een e-mailtje sturen naar aanmelding@eniac.utwente.nl. ■

Namens het bestuur,

Francis Henninger
Activiteitencommissaris 2006
Alumnivereniging ENIAC

Deloitte.

TMT Security Survey

Protecting the digital assets

Digital information and digital technology have become the lifeblood of the technology, media and telecommunications (TMT) industry. This fundamental shift is creating tremendous opportunities and, for savvy companies, considerable value. But the move to digital also presents significant new challenges and risks, including security threats such as computer viruses and intellectual property theft that can disrupt or even disable a business.

In the aftermath of the dot-com bubble, TMT companies have generally had their hands full dealing with major challenges such as uncertain economic conditions, rapid technology advances and digital convergence – and, as a result, may have overlooked security. But many are now realizing that security is simply an integral part of conducting their business and thus too important to ignore.

Against this backdrop, the Deloitte Touche Tohmatsu (DTT) TMT Industry Group, made up of DTT member firms' TMT practices, conducted an in-depth survey of security practices at TMT organizations around the world, primarily through face-to-face interviews with senior security executives.

The survey of 150 TMT organizations shows that although TMT businesses are making significant strides to improve their security, they still have much to do. The report examines the industry's security issues in greater detail, and provides a number of specific insights to help companies protect their information and digital services.

Security long neglected in the TMT industry

Security has long been neglected in the TMT industry and the problem continues today – despite the TMT industry's growing reliance on digital information and technology. This inadequate response has left many

TMT companies critically vulnerable to attacks.

Over half of the TMT companies surveyed suffered a security breach in the preceding twelve months. Some companies surveyed reported breaches causing millions of dollars' worth of damage. And both the frequency and sophistication of the attacks are growing. Yet many companies continue to underestimate the need for security.

Common shortcomings include:

"More than half of the companies (...) said their systems were breached over the last 12 months"

- Inadequate resources and funding
- Ineffective actions that do not address the latest threats
- Lack of awareness and management support
- Insufficient attention to internal risks
- Failure to plan for serious attacks and business disruption.

Part of the challenge is that many companies do not appreciate the full magnitude of the problem. Although companies that have been the victim of security breaches are able to appreciate the direct impact and financial losses that ensue, they often overlook indirect and intangible factors such as brand damage, customer dissatisfaction, market erosion and lost productivity.

The survey suggests that companies that have developed strategies, policies and procedures are much less likely to experience security breaches or financial losses. Yet most TMT companies surveyed are not investing enough time, money and resources to protect themselves adequately. In fact, many TMT executives surveyed believe their companies are "falling behind" – or at best "catching up."

Carefully structured and managed security may not be a substantial source of sustainable competitive advantage, but it is certainly a critical part of any mature and well managed business in the 21st Century. Customers instill a great deal of trust in contemporary TMT companies, and may increasingly migrate towards those which are able to demonstrate a comprehensive and credible approach to securing all of their digital assets, processes and transactions.

TMT companies' digital information and technology vulnerable

Information security is commonly considered to revolve around three fundamental principles: confidentiality, integrity and availability. In most businesses, that translates into protecting the company from unauthorized access to property and information, preventing fraud and embezzlement and avoiding business interruption. But in the TMT industry, security also relates to the protection of digital media, content, intellectual property and services.

Security incidents are in the news every day, and the overall risks are growing. TMT companies are particularly vulnerable because their businesses increasingly revolve around digital information and technology. For example:

- Technology companies are increasingly using offshore resources to accelerate product development cycles. While this approach saves time, it may increase vulnerability to intellectual property theft.

- Media companies are increasingly creating their content in all-digital form, and distributing it online. While this has created a market for digital music downloads that is already worth in excess of $1 billion, it has also created multiple opportunities for theft, data corruption and large-scale piracy.

- Telecommunications companies are increasing the launching of Voice-over-Internet Protocol (VoIP)-based services, which exposes phones to the risk of viruses.

The list of external threats includes everything from viruses, spyware, worms and trojans to denial of service attacks, wireless network breaches and social engineering (that is, tricking people into divulging confidential information in order to impersonate them). And while TMT companies are gradually expanding their focus on security to combat these threats, DTT's 2006 TMT Security Survey indicates that hackers appear to be consistently a step or two ahead.

More than half of the companies surveyed said their systems were breached over the last 12 months. Even worse, both the magnitude and complexity of the attacks are increasing. Roughly a third of the breaches reportedly resulted in a significant financial loss of up to several million dollars. And that is even without considering the indirect and intangible losses – such as damage to the company's reputation and brand, system down time and lost revenue – which can add up quickly. Even by conservative estimates, the indirect cost in terms of lost revenue alone can easily exceed $12,000 per employee, for each virus-infected PC.

TMT companies face a bewildering and growing list of digital threats, which derive both from the digitization of their own commercial operations to the increasing number and diversity of malicious and criminal digital activities.

DTT's 2006 TMT Security Survey looked at what TMT companies around the world are doing to secure their businesses and protect them from attack. Most of the data was gathered through structured, face-to-face discussions with security executives and security management of TMT clients of DTT member firms around the world. In total, TMT companies from more than 30 countries participated.

The survey identified the types of security threats that are of the greatest concern to TMT companies and the level of resources being used to address them. It also examined which technologies are being implemented to improve security and the value TMT companies are deriving from their security investments.

Conclusion: security is an increasingly critical problem

Companies in the technology, media and telecommunications industry have tended to treat security as a relatively minor issue. This is in part because of the rapid pace of change in the TMT industry. The digital age has come upon us in under two decades, and few corners of the industry remain unaffected. As a result, security – as it pertains to digital assets, processes and transactions – is a relatively new phenomenon. But the time has come for the TMT industry to recognize that substantial action is necessary.

The volume, sophistication and potential damage of security attacks continue to grow. More than half of the companies in DTT's 2006 TMT Security Survey had their systems breached in the last 12 months – and roughly a third of those breaches resulted in significant financial losses of up to several million dollars. Factor in the indirect and intangible losses, and the impact is even higher.

What can TMT companies do to address this increasingly critical problem?

- Establish formal security strategies, policies and procedures. Stay abreast of the latest challenges and threats.
- Improve security awareness and training at all levels of the organization – starting at the top.
- Focus more resources on internal security threats.
- Allocate sufficient budget and resources to get ahead of security threats. Playing catch-up is not good enough.
- Develop and maintain a formal contingency plan for business continuity.

Although different TMT sectors face their own unique challenges, one thing they have in common is increasing vulnerability to attack. Security is no longer a minor operating detail, or a problem best left to the IT department. Today, security is a fundamental business requirement – and a strategic imperative.

If you would like to receive a copy of the full report "Protecting the digital assets; The 2006 Technology, Media & Telecommunications Security Survey", please contact Jacques Buith at jbuith@deloitte.nl or Hans Bootsma at hbootsma@deloitte.nl .

> "security is an increasingly critical problem"