Content:

1_ Preface

2_Business

A talk about L-SEC, members and security

Egemin uses Novell’s iChain for secured remote access

Leuven University Hospital (UZ Leuven) protects confidential patient information with VASCO’s Digipass 300

2'_Business Events

It’s up for grabs, so why not take it ... Pondering Digital Rights Management

Business Adoption of Digital Rights Management: controlling the distribution chain of confidential, valuable or sensitive enterprise documents

3_Technology

Increasing virus speed requires effective Patch Management

Privacy and anonymity in electronic services

International certification (EAL 3+) for Banksys’ DEP/PCI host security module

4_Focus On

Worth keeping an eye out for viruses and worms

Enhancing the security of a WLAN

5_Agenda

Upcoming events

Market news
In January 2002, 8 organizations (Banksys, Cryptomathic, Data4S, Hypertrust, Katholieke Universiteit Leuven, Telindus, Ubizen, Utimaco Safeware) have created the Leuven Security Excellence Consortium. L-SEC wants to promote Belgium as an international centre of excellence within the e-security market and to ensure that its members stay at the forefront of innovation by stimulating and supporting knowledge exchange and collaboration.

The achievements of L-SEC in its first 20 months have exceeded expectations: we have organized 6 events and workshops, with a very positive response, a website has been set up, a brochure has been printed, networking activities have started, and IWT-funding has been secured to support our activities in the next 4 years. Moreover, membership has been increased to 28, and a new program for individual membership has been established. In March 2003, Jurgen Truyen has taken on the role as full-time general manager. During his first seven months, Jurgen has played an essential role in stimulating the further growth and development of L-SEC.

You are now reading the next L-SEC initiative: Interface will keep you up to date on developments in L-SEC and in the broader security community. You will find here announcement of events and event reports, a description of business news and business cases, tips and tricks and general security news. We would like to take this opportunity to invite you to submit your inputs for the upcoming issues of Interface. If you have news or information that is of interest to the Interface readers, do not hesitate to send it to info@l-sec.be.

One cannot help but conclude that IT security has gotten worse in the last years. Information technology is spreading further to every aspect of society, and attacks get more and more sophisticated. We have seen more viruses and worms, with a stronger impact and a faster spreading than ever seen before, and the number of break-ins and attacks has certainly not decreased. Copyright violations and intellectual property theft are also a growing problem. All of this seems surprising, as it is clear to experts that at the same time, security technology had improved significantly. One should understand however that securing a complex information infrastructure that was not designed for security in the first place may take a long time. We are now gradually developing and deploying the building blocks: exciting new developments are the initiatives to build more secure systems by including trusted components; examples include the Trusted Computing Group (TCG, formerly TCPA), Microsoft’s NGSCB initiative and the Belgian electronic identity card. An important challenge for our society is to develop technical and legal solutions that offer adequate security without endangering privacy and open markets. Finally the key to improving security lies in understanding that creating security is a process, and secure systems require more than security technical solutions.

I am very pleased to present the next step forward for L-SEC and hope that this will be a useful tool for all information security professionals.

Bart Preneel, Chairman L-SEC
A talk about L-SEC, members and security

For this first issue, "Interface" interviewed representatives of five L-SEC members. Topics for discussion were their L-SEC membership, their view on the current economic situation and finally, the upcoming finance event. A collection of their views...

Among the interviewed are Wim Grobben from Cryptomathic, Ubizen's Carlo Schüpp, and Herman Verrelst from DATA4s, three of L-SEC's founding members. What were their motives in getting L-SEC up and running?

C.S.: In 2001, Ubizen started its first worldwide PR tour. At the time, the Rijndael algorithm, developed by two researchers at the Katholieke Universiteit Leuven, had just become AES, which definitely put Belgium on the map. Being a spin-off of the Katholieke Universiteit Leuven, and realizing just how useful this link with the university could be, we wanted to leverage our heritage. Contacts with professor De Backer and professor Preneel lead to a strong determination to join efforts to promote Belgium as a leading region in the field of e-security. Ubizen really needed that reference framework to support its initiatives on the international markets.

W.G.: To us, the initial aim was networking. From the onset, we were convinced that L-SEC answered real networking needs. It gives us, and others, the opportunity to take part in a variety of activities, to gain brand awareness, not an easy task for a smaller, younger company.

W.G.: And customers... Even though L-SEC might not directly generate sales, it provides opportunities for meeting prospective clients. Just as important is the fact that L-SEC allows us to, in an efficient and economical way, remain informed about evolutions in the sector.

Next to networking, brand promotion appears to be a key factor in L-SEC's offering. To what extent does L-SEC answer this basic need today?

W.G.: So far, we've mainly used L-SEC to raise interest from other players in the business. It's a fact that the L-SEC events are interesting. Presenting our products and discussing technical as well as business aspects with others is of major importance for the development of products, services, and the business as a whole. But it is time now to expand beyond the circle of experts, to also involve for instance the financial institutions whose core business is not security, but who are appreciative of the importance of e-security.

C.S.: International brand awareness is important too. L-SEC is not widely known as yet, but it is clear that it will become renowned in the future.

W.G.: That's right. The brand awareness and credibility offered by L-SEC, you can almost describe it as the L-SEC label, will be a major differentiator.

H.V.: True. For a relatively young company like DATA4s, gaining brand and name awareness is a challenge. When people think of e-security, they often do not go beyond cryptography, or beyond security infrastructure. DATA4s is active on a different level, in particular on the business level: monitoring activity on the network, fraud detection, risk monitoring. L-SEC allows us to communicate this to partners and customers, to make ourselves known.

C.S.: We also wanted to present Ubizen as an attractive employer. L-SEC is a valuable promotional tool when recruiting high flyers, interested in the security business. The same goes for potential partners.

Other panel members are Ineke Rampaert from Microsoft and Bart Deschodt, from Vasco Data Security. Why did they join L-SEC?

I.R.: In January 2001, we launched the Trustworthy Computing Initiative as one of the key factors in the Microsoft strategy, both from a product development and a customer experience point of view. With this initiative, Microsoft opts for a proactive
approach to security, on the corporate as well as on the local level. L-SEC is one of the local initiatives we absolutely want to be involved in.

B.D.: We also experienced the need to deepen local initiatives. While experiencing definite growth on the international markets, Vasco seemed to somehow have lost touch with the Belgian market. The introduction of the digital ID card, for instance, could have been a VASCO story. As it was now, VASCO did not have the time or resources to invest in the required networking within the Belgian market. L-SEC provides us with the right framework to do just that. As it enhances networking and fosters local as well as international initiative, L-SEC is a catalyst for expansion, both here and on the international markets.

I.R.: In addition, the L-Sec-platform is an important communication channel. Microsoft may have been in the line of fire due to recent security attacks, but it is quite important to know that we did provide the required patches way before the vulnerabilities were exploited. That is why our approach to Trustworthy Computing is twofold: we have to focus on security in the product development and release process, but also in clear communication and customer engagement by encouraging customers to keep their IT infrastructure up to date from a security perspective. To us, L-SEC is an excellent communication channel for knowledge sharing and for raising awareness on security.

Many industries today are facing hard times. How do the L-SEC members rate the current economic situation, and which evolutions do they envisage?

C.S.: In 2001, Ubizen decided to opt for Managed Security Services, rather than security applications or devices. We were lucky that way; the road we decided to take appears to be the right one. Our customers, large enterprises, multinationals, are aware that investing in the management of security is at least as important as merely employing security solutions and applications. As far as industries are concerned, we move from the financial institutions to other sectors, like healthcare, life sciences and the pharma industry.

H.V.: We mainly target on Finance and Telecom. Our market is geographically diverse. We work in the Benelux and the UK but also, via partners, in the US. We aren’t among the major players yet and we operate in a niche market. As such, we are less severely impacted by the economic downturn. At the same time, risk management has been identified as a priority, so the future is definitely not grim.

W.G.: We too consider the financial institutions as our major customers. That’s why L-SEC’s upcoming security event is so important to us. Concerning the current situation, … the economy may be picking up, but I don’t think we can really speak of a major improvement just yet. We are convinced though that security remains a growth market.

C.S.: That’s a fact. Managed Security Services are taking off, and security in general continues to gain momentum. Most probably, this has to do with what’s going on in the East, and with the continuous threat of worms.

H.V.: What we do notice though is that customers are more cautious when ordering, that decision processes are prolonged. That’s not necessarily bad though: the economic situation forces us to be more creative, to really tune in to customer requirements.

B.D.: That’s our experience too. As every IT company will agree, orders are no longer placed that swiftly, so we need to take more initiative at our own risk. At the same time, though, we know that the security market expands. Some countries we had not reached so far are interested in our products. Next to geographic expansion, the introduction of the new EMV cards may result in new forms of electronic banking, and changes in current authentication infrastructures. This may lead the way to further innovations in products and services.

I.R.: As far as market evolutions are concerned, we expect flat growth for the coming months. One of our focus areas is on continuously building the Trustworthy Computing Initiative. And we want to achieve this up-front, before products are released. The release cycle of Microsoft Windows Server 2003, for instance, was prolonged because we deliberately allowed for an additional security assessment cycle. It’s worth it, as today, Trustworthy Computing is key to customer engagement and – in the end - to business growth.
Bart Deschodt referred to the introduction of the EMV card as a possible trigger for growth. The electronic ID card may also open up new perspectives. Do the L-SEC members think these innovations will lead to major changes?

B.D.: Not right away. Though we are definitely ahead on standardization in Belgium, I still consider authorization using electronic IDs to be wishful thinking. Many of the parties involved, especially the banking world, are still apprehensive. But millions of EMV credit and debit cards will be distributed in the Belgian market as of 2005, so EMV will definitely change the market.

W.G.: From a business point of view, the electronic ID is a great initiative. Our business contacts in the Netherlands expressed downright envy, as they expect this initiative to trigger a host of new applications. Though the card in itself will not cause major change, it is a step on the way to the next generation of products.

H.V.: The introduction of the digital ID will probably change the face of crime, as well as its geographic distribution. We may soon face an upsurge in white-collar crime, perhaps, or an evolution from consumption fraud towards extensive money laundering. Either way, DATA4s sets out to tackle changing needs.

Cryptomathic, DATA4s, Microsoft, Ubizen and Vasco Data Security are among the presenters during the upcoming L-SEC event, “Security in the financial sector”. What does this event mean to them?

H.V.: We are very happy with the initiative. It’s the ideal forum, with the ideal list of attendants to present our application level strategies for risk and fraud management.

I.R.: It is a great opportunity, indeed. To us, the event is quite important as Microsoft has several customers in the Finance Sector, and we’re delighted to present Microsoft’s PKI strategy.

B.D.: Visibility, that’s what it’s about. We want to show the Belgian and the Dutch markets that we are a reliable supplier, that we know which role we want to play and that we take it seriously. We want to leverage the visibility offered by L-SEC. As Finance is Vasco’s core business, the L-SEC event allows us to expand our credibility and brand identity in the sector we actively target.

W.G.: We too have great expectations. To us, the finance event really illustrates L-SEC’s added value. It allows us to show our products and to discuss evolutions in the market with other major players. We perceive L-SEC as a trigger for growth.

I.R.: I think it’s a bonus that this event does not just revolve around the merits of a few players – security should basically be an industry effort, but allows all participants to gain in-depth and broad understanding of security in the financial industry, of current investments, and of technological evolutions. As it provides an overall view of e-security in this market, this event is a valuable opportunity for both the industry players and for the Finance customers.

An Schollen

For more information about the upcoming Finance event see News & Agenda section
As an L-SEC Member, you will receive:

- Invitation to the L-SEC annual event focusing on new trends, challenges and solutions in e-security
- Invitations to market or solution specific events focusing on e-security developments and evolutions for that specific area
- Invitations for our advanced workshops intended to promote the e-security aspects within a specific domain
- Receive the quarterly newsletter with market and e-security information
- A 50 € rebate for the annual and market specific events (minimum 3 events yearly)
- Discount to attend the workshops
- Discount to attend the education and training program
- Access to presentation section for members only

Who should join us?

- IT Security Consultants who guide their clients towards the right level of security
- Security Officers who wants to be kept informed about the latest evolutions and trends in the e-security market
- Hosting companies, B-to-B, B-to-C companies, consultants: who needs to be aware of the fast evolving security solutions required to protect the assets of their clients.
- Security and network administrators and those who are responsible to protect the company’s electronic infrastructure, privacy and information.
- IT Auditors and controllers who help companies verifying the information infrastructure and control mechanism

Register on-line for individual membership www.l-sec.be
Egemin uses Novell’s iChain for secured remote access

As we cover the entire supply chain process, from consultancy and implementation up to and including service, most of our people are constantly in the field”, explains Gert Vanden Bergh, Egemin’s ICT Systems Manager. “However, to do their job properly, they need instant remote access to all the latest data, wherever they are. In the past, they used to call in with a simple modem connection, but the data volume has become too large and the information too sensitive for such a slow and insecure link. What’s more, an ever increasing number of customers has been asking for remote access too in order to facilitate cooperation on their projects. So after long and careful consideration, we decided to go for a solution built around Novell’s iChain, which guaranteed us the necessary security by means of tokens”.

Egemin has been using several Novell products for many years. This time too, they decided that Novell’s iChain was the solution that best suited their needs. The main assets identified were proven quality and ease of implementation. For that implementation, Egemin called on Novell Business Expert Partner 4all NetWorks, a Belgian consultancy with a European customer base. Using Novell Portal Services, they built a portal which allows employees to access all the information they need, securely controlled by iChain and using Citrix for non-Web enabled applications. The same portal also provides room for communities and discussion forums, which is highly appreciated by the customers. Once the system had been implemented, users only had to be informed about the use of the token, as such training efforts were minimal. Users reported to be delighted about the single sign-on feature provided by the token.

With iChain, very strong authentication can be enforced, without making changes to the backend applications. This reduces implementation time as well as costs. Quite unique in the implementation at Egemin was that secure identity management concept was applied to Citrix as well. As a result, users who want to initiate a Citrix session, even directly, have to go through the authentication process on iChain. Implementation just involved tailoring Citrix to suit iChain.

To provide high availability, Egemin uses Novell’s Clustering Services. All of the applications run on central servers at Egemin’s headquarters. These servers which can be accessed 24 by 24 from all over the world. On average, Egemin registers two dozen simultaneous users out of the 250 who have received their tokens so far. The scalability of the solution will facilitate the addition of future features and services, both for employees and customers. Egemin’s employees are very positive about the system, and the executives see the solution as a technological showcase for their company.
Leuven University Hospital (UZ Leuven) protects confidential patient information with VASCO’s Digipass 300

**Introduction**

Leading medical technology, high-quality innovative medicine, care and trust are part of the Leuven University Hospital’s mission. With its 1927 beds and more than 7300 staff members, the UZ Leuven is one of the largest and most renowned healthcare centers in the Benelux.

| Number of beds | 1 927 |
| Number of consultations per year | 546 420 |
| Number of admissions per year | 62 598 |
| Number of day hospital admissions per year | 85 940 |
| Number of staff | 7 390 |

The UZ is also a leader when it comes to ICT. With the patient’s consent, doctors who are not part of the hospital’s permanent staff can consult their patient’s UZ Leuven file through the Internet. Specialist research carried out at the UZ can be interpreted online in a local doctor’s practice and employees can access the UZ network from home. A sufficiently high level of security is crucial in making such applications function properly. In order to guarantee that only authorized users have access to the applications they need, the Leuven University Hospital has decided to use VASCO’s Digipass 300.

**Background**

When in 1999, the hospital decided that all medical files should be made accessible to external third parties through the Internet, the UZ’s ICT managers faced two major issues: how could the Internet, which is an open system, be made secure enough; and how can unauthorized access to the UZ network be prevented? The answer was easy: by combining a secure, encrypted connection with strong authentication. The preferred authentication product was VASCO’s Digipass 300. The UZLeuven started using Digipass 300 at the end of 1999.

**Applications**

VASCO’s Digipass 300 is used for an increasing number of applications.

**LISA (“Leuvense Internet Samenwerking Artsen”, the Internet cooperation agreement of Leuven-based GPs):**
LISA offers GPs, specialists and other medical practitioners the possibility to access patient files available to staff at the hospital. These external practitioners are only given access to the patient’s file if the patient has authorized this by signing an ‘informed consent agreement’. More than 99% of the patients invited also give authorization. The interaction between external healthcare providers and the UZ Leuven is secured with VASCO’s Digipass 300. Currently, some 200 doctors who refer patients to the UZ and use a Digipass participate in the LISA-project. More than 23,000 patient files can be accessed through LISA.

**Vlaams Ziekenhuisnetwerk KULeuven (Flemish Hospital Network KULeuven):**
Various hospitals in the Flemish Hospital Network KULeuven use applications that require increased user authentication. From now on, one single Digipass will be sufficient to allow practitioners to access several applications.
PETNET:
Within the framework of nuclear medicine, very specific and exceptional research is carried out at the UZ Leuven. Digipass 300 delivers strong authentication when specialists based elsewhere request and interpret research results from their own offices via PETNET.

Remote access:
Digipass 300 enables hundreds of UZ employees to securely access the hospital’s network, wherever they are. This enables staff to work on solutions for urgent problems at all times.

The technical aspects
UZ staff or local GPs are not necessarily computer specialists. That is why the UZ’s Information Systems service focused on the user-friendliness of the system. And successfully! The LISA-program was integrated in a browser, which means users do not need to go through the download of cumbersome programs. Determining factors for choosing VASCO’s Digipass were security and the user-friendliness of the software.

The UZ Leuven’s Information Systems service built its own security infrastructure and acquired the Digipass 300 and Digipass Libraries from VASCO in order to guarantee verification. The system also uses a Java Applet implemented SecureShell solution.

www.vasco.com

Professor Dr. Bart Van den Bosch of the UZ: “With VASCO we have been able to make the Internet a secured channel.”
a few hours ago, L-Sec’s DRM event closed with a heated panel discussion. I decide to complement impressions left by the event with some field research. The field, this time, is the pub, natural habitat of the largest part of the public held responsible for the abuse of digital data. I want to confront them with some of the views adamantly defended by the ardent specialists who spoke this afternoon. One of them, Marcel Heymans of IFPI (organization representing the international recording industry) explained that the industry suffers most from people in the <25 age group. These days, older age groups, like the >45 group, are buying more CDs than they ever used to. The in-betweens represent the status quo. That means I can rest assured, safely lingering in the group that seems to have been found “not guilty”. But as far as guilt is concerned, identifying the real culprit in these matters is an impossible mission, as every party involved accuses another. Customers point an accusing finger to the industry, while the industry blames the customers, but also the politicians. The politicians, in their turn, blame no one, and do nothing. Better safe than sorry, they may think. Result: against the backdrop of the digital age, initiatives that foster actual protection of copyrighted material progress at a snail’s pace.

So what’s at stake here? Digital Right Management involves managing digital content in such a way that the rights of authors and publishers are safeguarded without impacting ease of use. We’re talking about preventing illegal downloads, infringement of user rights or privacy rights, unauthorized distribution of digital content. Content can be a variety of sorts: data used within enterprises, exchanged between companies or between companies and users. All this information should be managed in such a way that everyone gets his fair share. The author or musician wants to be paid for his work, the publisher for the use of his distribution channels. And what the user wants is a fair price for the product of his choice.

But what does this mean, a fair price, for, let’s say, a music CD?

When drafting the seminar program, it became clear that the DRM topic can be divided up in three domains: business aspects, the legal framework and technology. KUL professor Bart Preneel provided the introductory presentation. The problem of protecting intellectual rights is definitely not new. In the seventeenth and eighteenth century, people also tried to protect their intellectual property, logarithm tables for instance. The introduction of easy-to-use recording devices, audio cassettes, floppy disks, writable CDs, transportable gigabit hard drives has set a totally new scene though. But compared with former technological innovations, the Internet changed that scene dramatically, allowing unimpeded exchange of business information, confidential data, publications, software, audio and video files. The Internet works wonders for millions of people, allowing them to carry out enormous amounts of work with a minimal amount of computer knowledge. At the same time, though, it also allows the biggest dimwit to ravage cyberspace. Hacking tools are easy to download and open up sources villains could only dream of in the past. Evolution taking its toll? DRM is a delicate matter, that’s for sure. Academics, for instance, are held personally responsible for reporting security breaches in techniques to protect copyrighted material. Punishment for the bell ringer, it’s the world upside down, to stick with seventeenth, eighteenth century imagery.
Let's get back to business, more particularly to the poor soul representing the music industry, continuously hassled by the press, blackened by incorrect or biased information, attacked by users and what's more, put on the spot during DRM seminars, forcing one into defensive mode. What's at the root of the music industry's problem? Let's say current CD prices come about through contractual arrangements with artists, combined with marketing costs and distribution costs. How would this change if the music industry were to go online? The contracts would stay, marketing costs would remain important, distribution would be facilitated. But would this bring about major discounts? And if users are not willing to pay their 15 euro for a CD in the shop, why would they suddenly change their mind if a downloaded version would cost them, let's say, 12 euro?

Add 3 euro for the CD burning and the difference in price is gone. Assumptions of course. . .

Let's look at it from a different angle, a cultural one. Music, books and video, it's all part of our culture. Are consumers unwilling to pay for culture? Or does this only go for certain parts of culture? Gigs, for instance, attract increasing numbers of people. Yet at the same time, the audience won't buy CDs. They just copy them from friends or relatives. Maybe this is where the government should come in: sponsoring culture, supporting artists and ensuring that there is a sufficient, subsidized artists base. But is this the government's responsibility? Ensuring an extended and supported legal framework which leaves no opportunity for free interpretation is definitely one of the governments' tasks. And because we live in Europe, why not go for European legislation? Different laws in the member countries result in a variety of viewpoints and practices. In the UK, you cannot copy a purchased CD for your own private use, while in Belgium, this is explicitly allowed. So what should we think of CDs that simply cannot be recorded on the medium the user prefers? And can CDs be released in the UK, then imported into Belgium? And what about the copyright contribution I pay for my brand new car audio installation? I can't even play some of my CDs on it, as they have been protected against unauthorized copying. Unsettling questions for Christophe De Preter, in charge of the legal aspects at the L-Sec event.

And can't technology fit the bill? According to Ivan Lepla, who presented technological aspects at the event, technology can't solve the issue, at least not on its own. If we cannot even count on technology these days, where will this all end? But disconcerting as it may sound, it is true that bits will be bits and guaranteed security is, as always, impossible. Some good news though! We are on the right track. Various security technologies, some more efficient in the fight against unauthorized use than others, are being piloted and used today. One big question remains: Will we accept technology imposed by multinationals to impact our privacy, or will open source that can be adjusted by anyone with a feel for software be the way to go?

Meanwhile, striking views are revealed in the pub... Do students copy or download music? Baffled faces; of course they do! When asked why, a straightforward answer: 'simply because it is within reach, it's up for grabs'. My amazement puzzles them. 'What's so strange?', they ask, 'music is available everywhere on the internet. You have free access to all genres, bands, in all shades of quality'. When asked if they do the same in a music shop when the shop owner can't see, the answer is quite revealing. 'Of course we don't, that would be theft!' So one central issue is the interpretation of theft. In the virtual world, taking without paying is not classified as theft, in a real shop it is. Is that due to the lack of physical experiences on the net? Virtual reality, virtual ethics? Maybe. But do these youngsters know and care about the repercussions for the artists? They do think it impacts artists, but, according to them, it's the industry's responsibility to do something about it. Fair enough, but how about the impact on privacy? Is it acceptable to be monitored all the time? "Absolutely not, no big brother mentality!", a clear cut answer. So that's where it leaves me, trying to put together the pieces, assembling an objective picture of the issue, not knowing who to back now: the industry, wanting to protect its assets, which may imply limitation of online privacy, customers saying the industry should resolve issues without diminishing privacy.

"Up for grabs", they say, "so better enjoy it" .... Why didn't I just enjoy my pint and talk about the weather?

Jurgen Truyen, L-SEC
After the first introduction session about all aspects of Digital Rights Management, L-SEC and MediaNet Vlaanderen organizes three more in-depth workshops. This first workshop focuses on the business aspects of DRM. The presentations will handle the impact of DRM in daily business operations. Separated over the different kind of organizations involved such as authors, distributors and business associations, speakers will highlight the most important concerns and working solutions.

**EVENT PROGRAM**

13u30 – Registration

14u00 – Ted Shapiro,
Vice President & General Counsel -
Europe Motion Picture Association

14u30 – Louis Vuchelen,
Coordinator Multimedialoket - SABAM

15u00 – Peter De Smedt,
IDTV Product Design Engineer - Telenet

15u30 – Coffee Break

16u00 – Hans Maertens,
Algemeen Directeur – Uitgeversbedrijf TIJD NV

16u30 – Discussion panel

---

Date: Thursday October 23, 2003
Free entry. Registration before October 21, 2003

Location: ESAT, K.U.Leuven room 00.62,
Kasteelpark Arenberg 10, 3001 Leuven (Belgium).

For more information and registration visit
www.l-sec.be/communication_events_agenda.asp
Business Adoption of Digital Rights Management: controlling the distribution chain of confidential, valuable or sensitive enterprise documents

What is Digital Rights management?
Digital Rights Management (DRM) technologies enable the defining and enforcing of policies on digital information. Examples of these policies include prevention of printing, prevention of unauthorized forwarding or enforcing time-limited access. Digital Rights management adds a final and crucial value to current IT systems like access control lists or transport technologies based on digital certificates. These systems guarantee authorized access and encrypted transport but fail to control what is happening with the information once it is handed over to the final recipient. Digital Rights Management technologies were first applied to prevent piracy, when new business models such as pay per view or digital lending were introduced for the distribution of electronic media content, like music or video. Gradually, DRM principles have been integrated in business applications to help safeguard sensitive information, no matter where it goes.

How does it work?
Digital Rights Management architectures rely on 3 components:
- **A policy editor**: this is usually a component at the content distributor side allowing definition of permissions (redistribution, printing, expiration dates...).
- **A licensing authority**: a central server encrypting the content and generating a license containing the decryption key and business rules (defined by the policy editor) to activate the key (e.g. activate during 3 weeks, resulting in a digital lending model, with virtual shredding of the digital content after expiration of the license)
- **A DRM client**: a piece of software required to interpret the license and to unlock the content in accordance with business rules.

One example is the commercial director who needs to distribute a proposal containing business intelligence to prospects. The director does not want the targeted prospect to forward the proposal to a competitor. He also wants the proposal to be made inaccessible after its binding validation date. SecureAttachment, an Enterprise DRM architecture provided by Info2clear and Adobe, has an Outlook Plug-In as Policy Editor, allowing definition of the permissions regarding documents enclosed in a regular email message. The email attachments will pass the licensing server (based on Adobe DRM), which will convert the content in Acrobat PDF files, encrypt the attachments and issue a license for the prospects. The prospect accesses the encrypted Adobe Acrobat file and requests the permission from the license authority server in order to unlock the content. Once a valid license has been delivered, the content can be opened in Acrobat Reader.

A critical parameter defining the business application of DRM is the spread of the DRM client. Many popular content access tools such as Adobe Acrobat or Windows Media Player do have DRM capabilities. This means that protected content can be distributed to consumers without them having to install additional software to unlock the content. Due to the mass distribution, the level of protection is lower and the rules are more rigid compared to DRM architectures which require dedicated client installations. They do, however, add an additional barrier from a financial or user experience point of view.
Two fundamental business application domains can be distinguished, based on the DRM client penetration: Business Applications for widespread DRM clients and Business Applications for dedicated DRM clients.

**Business Applications for widespread DRM clients:**
Substitution of Paper fulfillment into electronic courier express shipping

Business documents often need to be distributed outside the enterprise boundaries. Often, these distribution processes are still paper-based. DRM protected email attachments allow enterprises to substitute paper fulfillment by a more cost-effective, faster and much more secure and manageable distribution process.

Examples include broadcasters of confidential or discrete documents such as payroll services agencies, brokers, pension’s funds, couponing, ticketing, publishers of industry reports, as well as companies that need to exchange confidential or valuable information, like company advisors, HR organizations, and law firms. DRM suppliers include Adobe Content Server and SecureAttachment (based upon Adobe Content Server).

**Business Applications for dedicated DRM clients:**
Information sharing within the organization

Information theft within companies is a problem on the rise. Companies require disclosing of sales forecasts, financial forecast, R&D information on corporate intranet portals. The access is often protected by means of passwords, certificates or tokens, but once access has been provided unauthorized redistribution may occur. Gartner reported that “corporations do lose intellectual property through employees. Whether intentionally or inadvertently, electronic files containing corporate intellectual property can eventually show up on an outsider’s web site or, worse, in competitors’ hands”. The site [http://www.internalmemos.com/memos/](http://www.internalmemos.com/memos/) is listing various confidential internal memos of thousands of large corporations, adding reality to the Information Security Breachers Survey 2002, which stated that “32% of the worst security incidents were caused by insiders”. Within one single enterprise or business unit, a clear ICT policy can be enforced, as the system administrators can manage the pre-installation of dedicated DRM clients for unlocking protected confidential information published as web-, email or office documents. DRM suppliers include Windows Rights Management Services, SecureAttachment (based upon Windows Rights Management), Sealed Media, and Trusted Edge.

**Increasing virus speed requires effective Patch Management**

Viruses like CodeRed and the SQL Slammer worm acted on vulnerabilities that were more than half a year old. The latest generation of virus builders, however, are acting much quicker.

The Blaster worm was wreaking havoc only four weeks after Microsoft announced the vulnerability. Software manufacturers, in their turn, are responding increasingly fast too: Microsoft, for instance, releases patches within days after the discovery of a vulnerability. "The number of software vulnerabilities has doubled every year since 1999," says Casey Dunlevy, manager of the CERT Analysis Center at Carnegie-Mellon University, which tracks this data as part of its ongoing effort in issuing the closely watched CERT security alerts. "Last year there were 4,200 different vulnerabilities in software products, the year before there were 2,100," Dunlevy says. "And it looks like figures will double again this year."

General security countermeasures are antivirus software and perimeter security solutions, like Firewalls and Intrusion Detection Systems. Though these countermeasures reduce the symptoms, vulnerabilities can only be kept to a minimum by effective patch management.

Patching must be part of the general security policy, with outlines timing as well as the decision process underlying patch installation. Installing patches is a risk management exercise. It involves decisions on how long installation of patches can be postponed. It also requires taking into account business aspects when creating the policy, and maybe even in the operational decision process. On the operational side, one person in the company, most probably the security manager, has to have the end responsibility for the patch management process. The patching process has to be automated, as manual installation of patches is expensive and error-prone. Rather than to opt for a manual, reactive approach, the preferred solution is a pro-active automatic patch management tool that can distribute patches in a controlled manner. This patch management tool should be complemented by a scanning tool to check patch tool effectiveness and policy compliance.

Patching processes conflict with the general Change Management policy of not changing server and desktop configurations without extensive testing. Usually, server and desktop installations are controlled by using standardized setups. In addition, they are released in a controlled way. This allows IT departments to provide configurations that guarantee continuity and to control the environment.

Software quality assurance does not always include the scan for vulnerabilities, so software is often released with security-related bugs, so called vulnerabilities. These vulnerabilities are exploited by malicious programs such as viruses and worms. The impact on business can be enormous: loss of productivity through loss of data, loss of network connectivity, loss of business and, finally, loss of manpower on fixing the issues.
Vulnerabilities and the viruses and worms exploiting them are threatening the continuity in such a way that immediate intervention is necessary once a new vulnerability is discovered. This changes the normal change management process dramatically. Where the testing of new Desktop and Server environments based on new operating system releases or service packs could easily take weeks or months, the patches now have to be tested within days or even less.

An overview of possible patch management solutions:

Do it yourself.
Keep track of server and desktop versions and latest patches in a database. This might be perceived as less expensive than buying patch management software, but it might involve extra efforts in terms of maintaining own applications or monitoring for security alerts.

Implement a system management solution.
Use a system management package that includes a patch-update component. This ensures patches are an integral part of the overall computer inventory and configuration process. It can, however, be more expensive than just buying a patch management point product. Also, unless the package includes specific security alerts, you may need additional features.

Employ a specific tool.
Use a stand-alone patch management tool. This might be less expensive than a systems management package, but it requires close evaluation, as products differ widely in the applications and operating systems they support. Also important is the difference between so-called agent-less or agent-based software. Products are changing rapidly in terms of the degrees of automation of the patch process.

Examples of System management solutions are Microsoft SMS, ConfigureSoft, Ecora, IBM Tivoli and LANDesk Software. Examples of commercial patch management software are BigFix, PatchLink, St. Bernard Software and Shavlik Technologies.
People tend to perceive that they are "anonymous" while developing these electronic activities. However, tracking Internet users is much easier than tracking people in the real world. Let us have a look at the following example. While surfing the Internet, it is common to get banners together with the web pages. Companies such as DoubleClick manage many of these banners, inserting them in a wide range of websites. In order to customize the service, DoubleClick stores cookies in the users' computers. These cookies have a unique identifier, so the company can build a very detailed profile of the user without the user even knowing it. All this information is stored in databases and the user has no control on how long it is kept and what DoubleClick does with it.

Anonymity techniques do not focus on protecting the confidentiality of the information transmitted, but on the traffic data. This data is not as innocent as it may seem, and as users become aware of the threats to privacy resulting of the public availability of traffic data, they also become interested in the tools they can use to be anonymous. In order to clarify the difference between content and traffic data, we could think of the phone system. Would you like the list of numbers you call from your telephone to be made publicly available? Probably not, even if the content of the conversations remains confidential. Without taking special measures to protect your privacy, virtually anyone willing to listen to your communications can find out what you are doing in the Internet.

Other systems, such as anonymous electronic payments, have been thoroughly studied, but are not being deployed yet, probably because banks prefer to keep control on what their clients do with their money. In any case, as people become aware of the value of protecting their privacy, the demand of privacy-friendly systems is expected to increase.

Claudia Diaz, SCD/COSIC K.U.Leuven

In the past few years, many theoretical and practical systems for protecting privacy through anonymity have been designed.

Some of the systems you may use allow you to send anonymous email, surf anonymously the web, or vote electronically without revealing (not even to the voting authority) whom you voted for.
International certification (EAL 3+) for Banksys’ DEP/PCI host security module

Banksys recently obtained the Common Criteria certification for its DEP/PCI host security module. The certification was granted by the German BSI authority (Bundesamt für Sicherheit in der Informationstechnik).

The DEP/PCI module, a graphic accelerator card, is one of Banksys’ Data Encryption Peripherals (DEP), supporting secure generation, storage and use of cryptographic keys. It comes as a single PCI board that can be installed in any server or PC running on Windows NT or Linux. The DEP/PCI card is designed with a tamper-proof and tamper responsive module that physically protects all cryptographic processing. All plain text keys are protected inside the tamper resistant module, which can only be accessed through trusted user and command authentication. Any drilling, electrical probing or chemical attack will instantly trigger an alarm system while all key information stored on the board is erased. As such, the card can be used to ensure the security of critical network applications, including PKI components, payment systems, e-commerce, m-commerce, e-banking, key management applications, and payTV access control.

The DEP/PCI card is the first host security module to achieve Common Criteria EAL 3+ certification. The Common Criteria, described in ISO 15048, are an internationally recognized set of requirements that relate to the security properties of IT products. They allow organizations to demonstrate conformance of their product to its so-called Security Target, a document detailing the product specifications and the security requirements it meets. Certification of the DEP/PCI card involved independent evaluation by TNO/ITSEF BV, an ISO 17025-accredited IT Security Evaluation Facility, which tested every confidentiality and integrity feature of the module at every stage, from design and production through delivery and operation. The module achieved Evaluation Assurance Level 3+ (EAL3+).

Common Criteria certification is a valuable asset for promoting any security product. For Banksys, this certification is an important achievement, as it reflects the company’s dedication to high-level security, and ensures worldwide recognition and proven trustworthiness of the DEP/PCI card. The DEP/PCI host security module’s Security Target is publicly available via the BSI website.

www.banksys.com
On November 27, 2003, L-SEC, the Leuven based e-Security cluster, organizes “Security in the financial sector” Trends, Visions and Challenges. This event will present the latest security solutions and business cases for the financial market.

Despite the fact that the financial sector is leading when it comes to security, the number of breaches still increases. More than ever security is a continuous changing process stimulated by a higher demand to protect assets. These demands are generated by internal controls and audits and more often from external parties such as governmental regulations, privacy control organizations and customers. The technology evolution brings the customer closer to the company, increases the level of interaction through web and online processes, but also brings the potential fraudster and hackers closer to the network and assets. Dramatic steps are taken to improve compliance and security controls and to mitigate the overall risk.

This event will presents methods and solutions to keep ahead on the mounting number of threads and changing governmental regulations. Reaching highest level of security not only involves technology but also controls the usage of technology against regulations and customer demands. The presentations will provide an overview of legal and regulations aspects combined with standards, business demands and technology.

Presentations are grouped in four themes. In "Card & Mobile Technology in Financial Retail institutions", the focus is on smart-card technology and related standards in financial environments. "Security concepts and evolutions" covers regulations and methodologies as well as their link with business operations. "Security and Risk Technology" presents the latest evolutions on security technology and operational risk management. "Security Business Cases" offers a real-life view of security implementations.

For more information about this event or to register on-line visit
www.l-sec.be
Viruses and worms are pieces of code that execute unexpected and even unauthorized functions. They generally do this by exploiting some hole in the system, which can range from an error or oversight in the setup and configuration, or inadequate user and password administration, to a bug in the system software or in one or another application installed on the system.

In addition to executing functions with unwanted side effects, worms and viruses also replicate themselves. And this is what makes them different from adware, spam and irritating pop-up windows in the browser. It’s also what differentiates viruses from worms. A virus is a piece of code that needs some media to attach itself to, such as a floppy in the early days, an e-mail in the networked era and downloaded files in the Internet age. The speed with which a virus propagates and, meanwhile, multiplies itself depends on the medium: spreading a virus with a floppy is a much slower process than spreading a virus via e-mail using spamming techniques.

Yet viruses remain slow compared to worms. Just like real-life viruses are parasites in need of a host, a computer virus needs a medium. And just like a real-life worm functions on its own, the original worms, created in the seventies, were pieces of code working their way through a network of servers, looking for spare capacity to carry out complex scientific experiments and back-ups. Although today’s worms have a malicious nature, they also spread without needing to attach themselves to a medium. As such, they proliferate far more quickly than any virus ever could.

Recent worms like Blaster and Nachi are no longer entering a corporate’s IT infrastructure through major entry points and are not replicated and propagated by major servers. Instead, they penetrate and propagate using desktops. Desktops are traditionally more vulnerable, since their system management is uncertain and their use may go beyond corporate applications.

The result is that, whereas LoveLetter infected several machines in a few hours, the Slammer worm infected an enormous number of machines in just a few minutes on the 25th of January. The Blaster worm even spread many times as fast. Slammer and Blaster brought whole areas and ISPs on their knees and some companies were unable to conduct business for several hours, some even for days.

Is there reason to panic? Traditional virus scanners are no longer effective. They need a signature in order to detect a virus or worm. Anti-virus vendors generally need a couple of days before they release a signature for a new worm. By then, these worms may already have infected an entire infrastructure. This situation calls for a new type of network monitoring, yet using traditional techniques: closely watching the activity on your firewalls and your hosts. Thousands of similar requests on a specific port for example, while normally you’d only expect to register a few request per minute, may be the sign of an infection. Detecting traffic anomalies may not prevent infections. It does provide you with vital information that may help you to quarantine a worm, this way preventing the infection from spreading.

Carlo Schüpp, Ubizen

Worth keeping an eye out for viruses and worms
Enhancing the security of a WLAN

Wireless Local Access Networks (WLANs) are becoming increasingly popular, both for home users and in business environments. At present, new standards for WLAN security are taking shape, but until they’re widely deployed in new products, and until older products get patched, users should, at least, use the existing security mechanisms to enhance the security of their WLAN.

Though the following security mechanisms have proven useless for thwarting a determined and skilled attacker, they will keep most script kiddies away:

Enable MAC filtering
By using this option, you only allow specific systems with certain MAC addresses to access your WLAN. The MAC address is the unique address of the Network Interface Card. Most of the new NICs allow this address to be set to any value. So far for uniqueness...

Enable WEP
WEP is the protocol used in WLANs to ensure protection against eavesdroppers. It is remarkable how many WLANs are set up with WEP disabled, either because it is the default option or because of its difficult key management - the key is set manually every time and on each device. A WEP-protected WLAN is a much more daunting target for script kiddies, as a huge number of packets (in the order of millions) need to be captured before the WEP key can be broken.

Disable SSID broadcast
The SSID is the ID of the wireless network. By default, this ID is broadcast at regular intervals by the Access Point, advertising the existence of the WLAN. By disabling SSID broadcast, the nodes in the WLAN will need to know the ID of the network in order to connect - but hey, they also have to know the shared WEP key, so no added configuration hassle here. However, since the ID is no longer broadcast, an attacker will have a harder time to detect the network. It’s true, it won’t be that hard anyway, because the SSID is sent in unencrypted form in the traffic on the WLAN. In the absence of traffic, though, there’s no indication of the existence of the network.

Remember,
Until the new security mechanisms are deployed, treat any traffic on the WLAN as insecure and employ higher-level security mechanisms to deal with its insecurity (ssh, ssl, imaps etc.).

Robert Maier, SCD/COSIC K.U.Leuven
Upcoming events

L-SEC Digital Rights Management, Business Workshop
Date: 23 October, 2003
Place: K.U.Leuven, Kasteelpark Arenberg 10, 3001, Leuven · Belgium
Info: www.l-sec.be

Telindus Symposium
Date: 30 October, 2003
Place: Brussels Expo, Brussels · Belgium
Info: www.telindussymposium.com/general/home.htm

Leuven.Inc Protect Your Knowhow
Date: 20 November, 2003
Place: Innovatie- en Incubatiecentrum, Kapeldreef 60, 3001 Leuven · Belgium
Info: www.leuveninc.com

L-SEC Security in Financial Sector, Trends, Visions and Challenges
Date: 27 November, 2003
Place: Kinepolis Brussels, Eeuwfeestlaan 20, 1020 Brussels · Belgium
Info: www.l-sec.be

L-SEC Digital Rights Management, Legal Workshop
Date: 13 November, 2003
Place: K.U.Leuven, Kasteelpark Arenberg 10, 3001 Leuven · Belgium
Info: www.l-sec.be

L-SEC Digital Rights Management, Technology Workshop
Date: 4 December, 2003
Place: K.U.Leuven, Kasteelpark Arenberg 10, 3001 Leuven · Belgium
Info: www.l-sec.be

Leuven.Inc Visionair Seminar: The future of Europe/Flanders?
Date: 4 December, 2003
Place: Auditorium IMEC, Kapeldreef 75, 2003 Leuven · Belgium
Info: www.leuvenInc.com
Technology Nexus AB announces a global partnership with SWIFT

Technology Nexus AB recently announced a global partnership with SWIFT, the financial industry-owned cooperative providing secure and reliable messaging services. This partnership ensures interoperability between Technology Nexus’s desktop security PKI client Personal and SWIFT’s TrustAct Internet-based messaging service.

SWIFT’s TrustAct service allows financial institutions to provide their customers with trusted messaging over the Internet. TrustAct supports online identity validation of businesses in B2B exchanges and adds non-repudiation by timestamping and safestoring all messages exchanged between trading parties. By using TrustAct, financial institutions can deliver online trust and payment services to their corporate customers. Technology Nexus’s PKI solutions add to this the very latest in leading edge smart card technology.

Gustaf Malmros, Head of Secured Business Solutions at Technology Nexus explained:

“Our pioneering work and reputation in highly secured solutions for the online B2B market can really bring added value towards SWIFT’s offerings. We have already sold more than 1.5 million PKI desktop security client licenses, which has given us a strong market presence within Europe.”
Banksys, Interpay and SSB form SiNSYS

SiNSYS, the first pan-European initiative in international card processing, is a joint venture between Banksys (Belgium), Interpay (the Netherlands) and SSB (Società per i Servizi Bancari; Italy). The purpose of SiNSYS is to offer secure, high-quality performance acquiring and issuing processing services at highly competitive prices. The joint venture - represents an important consolidation in the European Electronic Fund Transfer market. This initiative will result in significantly faster product innovation and enhanced service flexibility.

The introduction of the euro has facilitated the development of a European market for payment processing. Many national and international processors are now looking beyond their borders for greater cost-efficiencies. The previously local payment systems are converging in their search for (international) IT standardization, economies of scale and stronger commercial relationships with clients. This suits the needs and demands of banks, who require cross-border solutions to realize their pan-European ambitions. All these clearly defined market dynamics have led to the creation of SiNSYS.

SiNSYS will build on economies of scale combining its founders’ volumes, experience and know-how to provide flexible and competitive services for the processing of international debit and credit card transactions. The joint venture is headquartered in Brussels. Banksys and Interpay each hold a 24.5% interest, SSB holds 51%. The three shareholders - themselves owned by banks - will be its first customers. Growth will be realized through new customers. SiNSYS will be opened to other interbank organizations at a later stage. Current annual volumes amount to 800 million transactions for 18 million cards and 500,000 merchants. These figures are expected to rise to approximately 1.5 billion transactions for 30 million cards and 800,000 merchants by 2007.

A key initial target of SiNSYS is to create synergy between the three partners involved. Processing of international debit and credit transactions of SiNSYS will be subcontracted to the SSB data center in Milan. Software development teams from each of the shareholders will be integrated and placed into three competence centers in Brussels, Milan, and Utrecht. This combination of expertise will greatly reduce the time-to-market of new applications and likewise increase product functions and flexibility into one state-of-the-art platform that will enable SiNSYS to develop new processing services and tailor-made solutions for existing and future clients. The acquiring and issuing processing of transactions will be streamlined, resulting in lower prices for each of these operations. This common platform is ready for any future developments in Internet and international mobile payments, as well as any new standards in the processing industry.

VASCO Launches Digipass GO3


Digipass GO3 is a lightweight, low-cost, strong user authentication token, especially designed for the large volume retail banking market. GO3, which is extremely easy to use, is VASCO’s answer to banks that want to give their retail customers a simple though secure means to use Internet banking applications. GO3 is the secure, cost effective and user-friendly alternative for systems such as TAN-lists (printed lists of transaction numbers).
SecureAttachment integrates Windows Rights Management Services

SecureAttachment, a service for secure e-mail distribution of valuable and confidential documents, will integrate Microsoft Windows Rights Management Services into its enterprise line-of-business systems.

SecureAttachment solutions facilitate the integration of sensitive information protection in corporate messaging, ERP, publishing, and ticketing/couponing systems. SecureAttachment’s clients span various verticals: publishing, finance and capital markets, company advisors and consultancy firms, as well as research and development intensive industries. The integration of Windows Rights Management enriches SecureAttachment’s offering towards HRM organizations, group insurance companies and pension funds, enabling them to fuel sensitive information directly to the employee’s desktop, whether the format is HTML, a Microsoft Office file, or a PDF. Publishers of high-value business information can protect their web content or e-mail attachments with very flexible policies, resulting for example in prevention of unauthorized forwarding or in an imposed expiration date on a published file.

New edition of "Subsidiewijzer voor Ondernemingen"

The Euro Info Centre of the Ministry of the Flemish Community has recently published a new edition of the Subsidiewegwijzer voor Ondernemingen. This guide contains information on the variety of subsidies granted by the Flemish, the Federal and the European government. It offers an overview of the most important support measures that companies, small and medium size enterprises in particular, can benefit from. The Subsidiewegwijzer can be downloaded from www.vlaanderen.be/subsidiewegwijzer. It is also available in print, free of charge, from the Euro Info Centre of the Ministry of the Flemish Community.

For more information, contact the Euro Info Centre,
Ministry of the Flemish Community,
Markiesstraat 1, 1000 Brussel,
phone: 02-553 37 33,
fax: 02-502 47 02,
or e-mail: euro.infocentrum@ewbl.vlaanderen.be.