Norbert Pohlmann
Helmut Reimer
Wolfgang Schneider

Securing Electronic Business Processes

Highlights of the Information Security Solutions Europe 2009 Conference

Contents

Standards and technical Solutions 221

Preface

Dear Readers,

ENISA has once again co-organized the ISSE 2009, Information Security Solutions Europe Conference 2009 together with eema, TeleTrusT, the ‘Identity 2009’, and the city of The Hague.

The purpose of the ISSE has been to support the development of a European information security culture throughout the years. This goal is more than ever valid for the future of the Internet, with its ever increasing demand for cross-border framework of trustworthy IT applications for citizens, industry and administration.

The ISSE is designed to inform ICT professionals, key policy makers and industry leaders on the latest developments and trends in technology, as well as best practices. ENISA is highly committed to these targets, as the Agency is pursuing a strategy of mitigating risks through awareness, studies, reports and Position Papers on current NIS matters.

In this quest, we assist and advise the European Commission, Member States, and the business community in the field of Network and Information Security.

The security of communication networks and information systems is of increasing concern, in particular for the economy of Europe. Clearly, cooperation is key to address today’s –and tomorrow’s -complex information security challenges. Only by working more closely together, can we generate new strategies to manage these problems. In bringing together the wealth of industry knowledge, information and research in Europe (as well as worldwide) the ISSE 2009 has been an event that we could not miss.

The success of this event is based on the unique backgrounds of its 400 participants: governments, academia and other key stakeholders. This line up guarantees an impressive blend of ideas from actors in different sectors of society, thus generating new ways of thinking.

The ISSE is a platform for open, vivid policy and technical debates in a non commercial setting. Through new insights and sharing of different perspectives, experiences and solutions on current topics of IT security, the independent and vast nature of the event guarantees highly relevant results. This year, the main focus is cutting edge security and related issues, like Large Scale Public Applications, Security Management & Economics of Security, Cloud Computing and Awareness Raising, selected by worldwide security specialists.

This edition contains a selection of some key topics presented at this year’s conference. As such, this compilation will serve as a valuable point of reference for IT security industry professionals. We hope that you will find it a useful, professional read.

Andrea Pirotti, Executive Director, ENISA

About this Book

The Information Security Solutions Europe Conference (ISSE) was started in 1999 by eema and TeleTrusT with the support of the European Commission and the German Federal Ministry of Technology and Economics. Today the annual conference is a fixed event in every IT security professional's calendar.

The integration of security in IT applications was initially driven only by the actual security issues considered important by experts in the field; currently, however, the economic aspects of the corresponding solutions are the most important factor in deciding their success. ISSE offers a suitable podium for the discussion of the relationship between these considerations and for the presentation of the practical implementation of concepts with their technical, organisational and economic parameters.

From the beginning ISSE has been carefully prepared. The organisers succeeded in giving the conference a profile that combines a scientifically sophisticated and interdisciplinary discussion of IT security solutions while presenting pragmatic approaches for overcoming current IT security problems.

An enduring documentation of the presentations given at the conference which is available to every interested person thus became important. This year sees the publication of the seventh ISSE book – another mark of the event's success – and with about 35 carefully edited papers it bears witness to the quality of the conference.

An international programme committee is responsible for the selection of the conference contributions and the composition of the programme:

- **Jeremy Beale, ENISA**
- **Gunter Bitz, SAP** (Germany)
- **Ronny Bjones, Microsoft** (Belgium)
- **Lucas Cardholm, Ernst&Young** (Sweden)
- **Roger Dean, eema** (United Kingdom)
- **Jan De Clercq, HP** (Belgium)
- **Marijke De Soete, Security4Biz** (Belgium)
- **Jos Dumortier, KU Leuven** (Belgium)
- **Walter Fumy, Bundesdruckerei** (Germany)
- **Robert Garskamp, Everett** (The Netherlands)
- **Riccardo Genghini, S.N.G.** (Italy)
- **John Hermans, KPMG** (The Netherlands)
- **Jeremy Hilton, Cardiff University** (United Kingdom)
- **Willem Jonkers, Philips Research** (The Netherlands)
- **Francisco Jordan, Safelayer** (Spain)

- **Frank Jorissen, McAfee** (Belgium)
- **Jaap Kuipers, DigiNotar** (The Netherlands)
- **Matt Landrock, Cryptomathic** (Denmark)
- **Madeleine McLaggan-van Roon, Dutch Data Protection Authority** (The Netherlands)
- **Norbert Pohlmann (Chairman), University of Applied Sciences Gelsenkirchen** (Germany)
- **Steve Purser, ENISA**
- **Bart Preneel, KU Leuven** (Belgium)
- **Helmut Reimer, TeleTrusT** (Germany)
- **Joachim Rieß, Daimler** (Germany)
- **Wolfgang Schneider, Fraunhofer Institute SIT** (Germany)
- **Jon Shamah, EJ Consultants** (United Kingdom)
- **Robert Temple, BT** (United Kingdom)

The editors have endeavoured to allocate the contributions in these proceedings – which differ from the structure of the conference programme – to topic areas which cover the interests of the readers.

Norbert Pohlmann *Helmut Reimer* *Wolfgang Schneider*

eema (www.eema.org)

For 22 years, eema has been Europe's leading independent, non-profit e-Identity & Security association, working with its European members, governmental bodies, standards organisations and interoperability initiatives throughout Europe to further e-Business and legislation.

eema's remit is to educate and inform over 1,500 Member contacts on the latest developments and technologies, at the same time enabling Members of the association to compare views and ideas. The work produced by the association with its Members (projects, papers, seminars, tutorials and reports etc) is funded by both membership subscriptions and revenue generated through fee-paying events. All of the information generated by eema and its members is available to other members free of charge.

Examples of recent EEMA events include The European e-ID interoperability conference in Brussels (Featuring STORK, PEPPOL & epSOS) and The European e-Identity Management Conference in London (Featuring the 2nd STORK Industry Group Meeting)

EEMA and its members are also involved in many European funded projects including STORK, ICEcom and ETICA

Any organisation involved in e-Identity or Security (usually of a global or European nature) can become a Member of eema, and any employee of that organisation is then able to participate in eema activities. Examples of organisations taking advantage of eema membership are Volvo, Hoffman la Roche, KPMG, Deloitte, ING, Novartis, Metropolitan Police, TOTAL, PGP, McAfee, Adobe, Magyar Telecom Rt, National Communications Authority, Hungary, Microsoft, HP, and the Norwegian Government Administration Services to name but a few.

Visit www.eema.org for more information or contact the association on +44 1386 793028 or at info@eema.org

TeleTrusT Deutschland e.V. (www.teletrust.de)

TeleTrusT Deutschland e.V. was founded in 1989 as a non profit association in Germany promoting the trustworthiness of information and communication technology in open systems environments.

Today, TeleTrusT counts 100 institutional members. Within the last 20 years TeleTrusT evolved to a well known and highly regarded competence network for applied cryptography and biometrics.

In various TeleTrusT working groups ICT-security experts, users and interested parties meet each other in frequent workshops, round-tables and expert talks. The activities focus on reliable and trustworthy solutions complying with international standards, laws and statutory requirements.

TeleTrusT is keen to promote the acceptance of solutions supporting identification, authentification and signature (IAS) schemes in the electronic business and its processes.

TeleTrusT facilitates the information and knowledge exchange between vendors, users and authorities. Subsequently, innovative ICT-security solutions can enter the market more quickly and effectively. TeleTrusT aims on standard compliant solutions in an interoperable scheme.

Keeping in mind the raising importance of the European security market, TeleTrusT seeks the co-operation with European and international organisations and authorities with similar objectives.

Thus, the European Security Conference ISSE is being organized in collaboration with eema, ENISA and the Municipality of The Hague this year.

Contact:
Dr. Holger Mühlbauer
Managing Director of TeleTrusT Deutschland e.V.
holger.muehlbauer@teletrust.de

Welcome

It is an honor for the city of The Hague and me to welcome the conference of ISSE in our International City of Peace and Justice. Tens of thousands of people in The Hague are working together towards making the world a better place. It is a unique concentration of international expertise and knowledge. The Hague is the city of the Peace Palace, the International Court of Justice, Eurojust, the International Criminal Court, the Organisation for the Prohibition of Chemical Weapons, the International Criminal Tribunal for the former Yugoslavia and Europol. And last nut not least we are making the dream of a sustainable city coming true in projects like the Seawater Power Station.

The Hague forms likewise the heart of Dutch democracy. The most striking building on 'Het Binnenhof' is the Knights' Hall, built in the 13th and 14th centuries as the castle for the Earls of Holland. It is the building where the decision was made to build the first modern republic! So history is in the air in this city, but the future also. On the The Hague historical grounds we will discuss modern developments.

And those contemporary developments are – as we all know – severe: the economical crisis grips us all to think about the coming weeks, months and years to develop new strategies. And that is why cities are important. Here the key-issues of the web 2.0 are developed and proven in the practice of all day living activities in the metropolitan areas. That is why in this conference we are discussing issues in a city like The Hague where security plays an important role in everyday life. The Knowledge Society will play a role in the sustainability of the society as a whole. And ICT-security of all the essential economic features is a sine-qua-non for the coming recovery and revival of the Information Society!

ISSE 2009 will in our view serve as the building stone of a scenario to re-establishment of a secure and sustainable society. We hope that the topics discussed during the event will serve as a reference for the work of the organisations involved in this interesting field.

Frits Huffnagel

Vice Mayor for Citymarketing, International Affaires and ICT

Microsoft Sponsoring Contribution

Claims and Identity: On-Premise and Cloud Solutions

Vittorio Bertocci

Microsoft Corp.,
http://blogs.msdn.com/vbertocci.

Abstract

Today's identity-management practices are often a patchwork of partial solutions, which somehow accommodate but never really integrate applications and entities separated by technology and organizational boundaries. The rise of Software as a Service (SaaS) and cloud computing, however, will force organizations to cross such boundaries so often that ad hoc solutions will simply be untenable. A new approach that tears down identity silos and supports a de-perimiterized IT *by design* is in order.This article will walk you through the principles of claims-based identity management, a model which addresses both traditional and cloud scenarios with the same efficacy. We will explore the most common token exchange patterns, highlighting the advantages and opportunities they offer when applied on cloud computing solutions and generic distributed systems.

1 The Sky Is the Limit

When you look at a cloudy sky, your inner child probably sees dragons and castles; don't be surprised if your inner architect, after having read this article, will see dollar signs. Cloud computing promises to bring radical advantages to the way in which we think of IT: Its basic idea is that companies can host assets outside of their own premises, reaping the benefits of those assets without the burden of maintaining the necessary infrastructure. This is somewhat similar to the idea of SaaS, where companies can avoid the burden of maintaining on-premise applications that are not specific to their core business, buying the corresponding functionality as a service. Cloud computing, however, pushes the bar further. Instead of buying complete applications provided by third parties, such as the classic CRM and HR packages, the cloud offers the possibility of *hosting your own resources* in data centers that are exposed to you as a *platform*. You have all the advantages of retaining control of the resource, without the pain of CPU and bandwidth usage, dealing with the hardware, cooling the room; you don't even need to worry about patching your system. If your Web application produces new data every day, using a data store in the cloud saves you from constantly buying hardware for accommodating growth. The best part is that you can expect to be charged an amount proportional to the usage you actually make of the resource, instead of having to invest in hardware and infrastructure beforehand. This “pay-per-use” pattern is one of the reasons for you will often hear the term “utility computing” instead of “cloud computing,” and it is even more evident in CPU-intensive tasks. Imagine if, instead of sizing your data center for handling its maximum forecasted peek and underutilizing it most of the time, you could deploy your most CPU-hungry processes in a data center of monstrous proportions: The CPU utilization could grow as much as requested, and you would pay your cloud provider in proportion. Those are some of the advantages that will light a sparkle in the eyes of your IT managers, but the Cloud holds even more interesting properties for architects. Since the cloud provider hosts resources on a common infrastructure, it is in the position of offering services that can be leveraged by every resource simplifying development and maintenance. Obvious candidates are naming, message dispatching, logging, and access control. Once a resource uses the cloud infrastructure, implementing those functionalities can be factored out from the resource itself.

The diligent architect, at this point, is likely to wonder, “Is my company ready for this?” Not surprisingly, answering this question is a complex task and requires considering many aspects of your architecture and your practices. In extreme simplification: If you run your business according to solid service orientation (SO) principles, you are in the ideal position to take advantage of the new wave. After all, if you respected autonomy, exposed policies, and used standards, who cares where your services run? If you are in that position, you have my congratulations. In my experience, however, nobody ever applies SO principles in excruciating detail. For example, services developed with the same technology offer special features when talking with each other, and there are situations in which it makes perfect sense to take advantage of those.

Identity management and access control are most likely to be affected by this phenomenon. Enterprises typically have their directory software, and they rightfully leverage that for many aspects of the resource access control; sometimes it works so well that developers are not exposed to identity concepts, which is actually a good thing, but that rarely happens. When faced with tasks involving some form of access control management, such as federating with partners outside the directory or using different credential types, you can expect developers to come out with the worst swivel chair integration solutions. If identity brings out the worst from development practices, why do we get away with it? The easy answer is that sometimes we don’t. I am sure you have heard your share of horror stories of access control gone wrong. The subtler answer is that we get away with it because, until we own the majority of the infrastructure, if we exercise iron-fist governance, we can somehow handle it: We may use more resources than needed, we may deal with emergencies more often than needed, but somehow we go on. In fact, “we own the majority of the infrastructure” is a fact that is challenged by growing market pressure. When a lot of your business requires you to continuously connect and onboard new partners, where does your infrastructure end and theirs begin? Cloud computing is going to snowball this: Once the cloud is just another deployment option, crafting custom access code for every resource will simply be not sustainable.

The good news is that there is an architectural approach that can help manage identities and access control for generic distributed systems, and it works for on premise, cloud, and hybrid systems alike. The core idea is modeling almost everything as exchanges of claims, and model transactions in a much more natural fashion.

This article is an introduction to this new approach. Special attention will be given to the aspects that are especially relevant for the cloud, but the vast majority of the concepts and patterns presented can be applied regardless of the nature of the distributed systemWhile the principles laid down here apply to any system, hence also to simple cases, their expressive power is best utilized for scenarios including partnerships, complex access rules, and structured identity information.

2 Claims-Based Solutions

The issue with classic identity-management solutions can be summarized as follows: They presume too much.

The most common assumption is that every entity participating in a transaction is well known by some central, omnipresent authority that can decide who can access what, and it what terms. This is usually true in self-contained systems, such as enterprise networks managed via directories, but fails when business processes begin to require alien participant such as software packages with their own identity stores, partners and customers accessing your extranet, and consultants. Tactical solutions, like using shadow accounts, often have to do with pretending to be able to manage something we don't own; and as such, they are very brittle.

Another common assumption is that every participant in a transaction uses a consistent identity-management technology. Again, this is a fair assumption for self-contained systems (think network software), but it fails as soon as you let aliens in the process. The common practice in accommodating different technologies is treating those cases as exceptions. As a result, the resources themselves end up embedding a lot of identity-management plumbing code, written by developers that usually are all but identity experts. This is every bit as bad as the old taboo for embedding business logic in the presentation layer, perhaps even worse. Handling identity plumbing directly inside the resource not only makes the system brittle and hard to maintain, it also makes the life of system administrators miserable. How can you manage access control at deployment time if the logic is locked inside the resource itself?

The claims-based approach defuses these issues by assigning each task to the entities who are its natural owners, and avoiding introducing artificial dependencies and expectations by respecting the autonomy of all participants – nothing but good old SO architectural principles.

3 Basic Definitions

Here I will present a bestiary of the various concepts and constructs you will encounter while exploring claims-based approaches.

Claims

A claim is a fact about an entity (the "subject"), stated by another entity (the "authority").

A claim can be literally anything that describes one aspect of a subject, be it an actual person or an abstract resource. Classic examples of claims are "Bob is older than 21," "Bob is in the group "remote debuggers" for the domain Contoso.com", and "Bob is a Silver Elite member with one Star Alliance airline." A claim is endorsed by an authority; hence one observer can decide if the fact the claim represents should be considered true according to the authority's trustworthiness.

Trust

An entity A is said to trust an entity B if A *will consider true the claims issued by B*. While very simplistic, this definition serves our purposes here. Trusting what B says about a subject saves A from the hassle of verifying the claim directly. Entity A still needs to make sure that the claim is actually coming from B and not a forgery.

Tokens

A security token is an XML construct signed by an authority, containing claims and (possibly) credentials information.

Security tokens are artifacts, XML fragments described in (see Resources: WS-Security), which can fulfill two distinct functions:

- they provide a means to propagate claims
- they can support cryptographic operations and/or have a part in credentials authentication

Thanks to the properties of asymmetric cryptography, the fact that a token is signed makes it easy to verify the source of the claims it contains.

Tokens can also contain cryptographic material, such as keys and references to keys, which can be referenced in encryption and signatures in SOAP messages; those operations can be used as part of credentials verification processes. In this context, we consider a "credential" any material that can be used as part of some mechanism for verifying that the caller is a returning user: Passwords and certificates are good examples (for more details, see Resources: Vittorio Bertocci's blog, The Tao of Authentication).

Tokens can be "projections" of specific authentication technologies, such as X509 certificates, or they can be issued (SAML, a popular token format you may have heard mentioned in the context of Web services security, is one example of an issued token). The system is future-proof: As new technologies emerge, suitable token "projections" can be documented in profile specifications.

Security Token Services (STS)

A Security Token Service is a Web service that issues security tokens as described by WS-Trust (see Resources: WS-Trust).

An STS (see Figure 1) can process requests for security token (RST) messages and issue tokens via requests for security token responses (RSTR). Processing the RST usually entails authenticating the caller and issuing a token that contains claims describing the caller itself. In some cases, the STS will issue claims that are the result of transformations of claims it received in the RST. (For more details, see Resources: Vittorio Bertocci's blog, R-STS.)

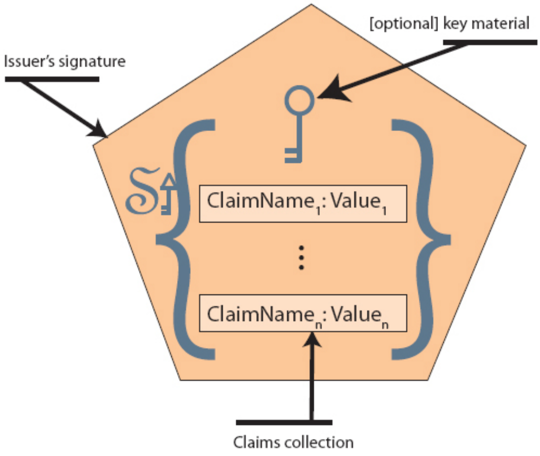

Fig. 1: Anatomy of a security token

Economics of Security and Identity Management

Measuring Information Security: Guidelines to Build Metrics

Eberhard von Faber

T-Systems
Eberhard.Faber@t-systems.com

Brandenburg University of Applied Science
Eberhard.vonFaber@fh-brandenburg.de

Abstract

Measuring information security is a genuine interest of security managers. With metrics they can develop their security organization's visibility and standing within the enterprise or public authority as a whole. Organizations using information technology need to use security metrics. Despite the clear demands and advantages, security metrics are often poorly developed or ineffective parameters are collected and analysed. This paper describes best practices for the development of security metrics. First attention is drawn to motivation showing both requirements and benefits. The main body of this paper lists things which need to be observed (characteristic of metrics), things which can be measured (how measurements can be conducted) and steps for the development and implementation of metrics (procedures and planning). Analysis and communication is also key when using security metrics. Examples are also given in order to develop a better understanding. The author wants to resume, continue and develop the discussion about a topic which is or increasingly will be a critical factor of success for any security managers in larger organizations.

1 Intention and Scope

Enterprises need to determine the current status or quality of information security and the maturity of their security processes and practices. There are several reasons for that. (i) In order to be able to improve something in a targeted way, one first needs to be able to measure it. In this context, the measurement basically provides the information being required for any action. In the first place, problem areas can be identified and found. Then the measurement shows if the right actions are taken and if they are effective or not. (ii) Enterprises need to justify costs and any allocation of resources for information security. Here the measurement means comparison on a relative level. Information is given about the effectiveness of current information security efforts. (iii) Enterprises need to benchmark in order to find out if the effort or expenditure is appropriate. This allows enterprises to control and adapt overall costs for information security. The measurement need to use an absolute level since it provides information about the efficiency. In summary, enterprises need to know if they do the right things, in the right way with the right intensity.

A metric is a means to measure against a predefined target. As a result the enterprise or authority can determine the status of information security, check the effectivity of actions, and control the costs allocated to information security. The metric must define the method and procedure of the measurements but also the target level. (iv) Enterprises need to take decisions on a sound, negotiable basis. A metric is the basis for taking such decisions, more precisely business decisions. This means that the target

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2009), 17-26

should be defined such that the impact on the enterprises' business or the authorities' mission is being determined. This is important and not self-evident. Security actions are designed and selected with the intention of a concrete effect. This assumption needs to be proven using metrics as an objective testing method. Simultaneously, a metric relates effects to causes. It removes uncertainty as well as chance and helps organizations to create, track and increase accountability. (v) Finally, measuring information security can be an efficient way or contribution towards demonstrating compliance with laws as well as external and internal regulations. Also the maturity [ISO21827] can be determined as an overall measure of information security practices.

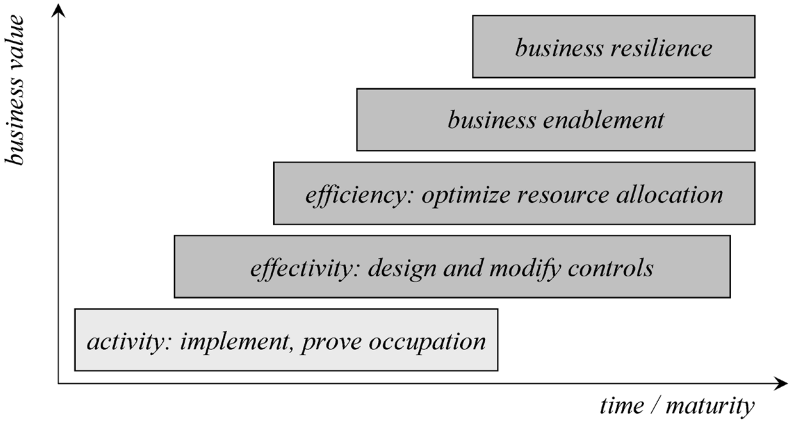
business value
business resilience
business enablement
efficiency: optimize resource allocation
effectivity: design and modify controls
activity: implement, prove occupation
time / maturity

Fig. 1: Motivation for security metrics: evolvement of business value (schematic)

Each of the above objectives or targets contributes to the organization's success in a specific way as visualized in Fig. 1. The measurement also develops from tactical to being strategic as program maturity evolves. Note, however, that measuring security does not affect information security, it helps to understand and interpret reality and thereby to affect information security deliberately.

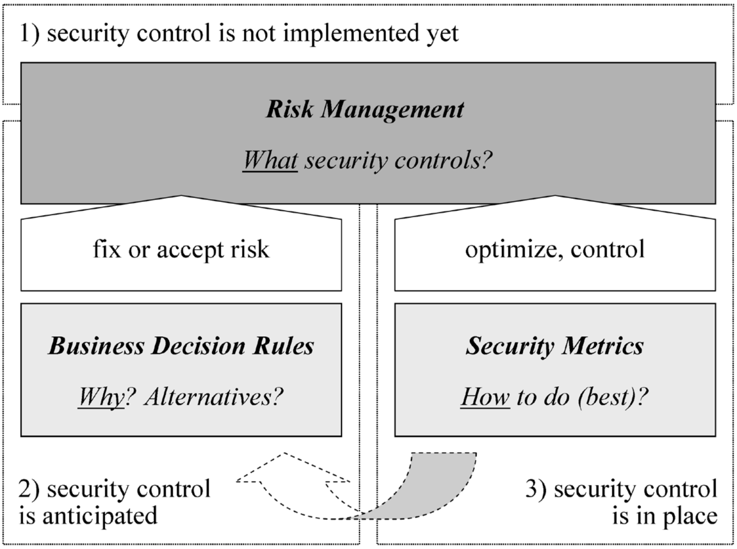

Fig. 2: The Risk Management Process and relation of business and metrics

Risk Management is vital for any organization. Though this process means rating and judgment, security metrics will not replace risk management as claimed in [Jaqu07]. *Security Metrics* as understood here are a mean supporting Risk Management (refer to Fig. 2). Metrics are (mostly) used when security controls are already implemented. Risk Management is the total process of identifying, assessing, and eliminating or controlling uncertain events that may affect valuated assets. The iteration starts (1) when some security control is not yet implemented and includes (2) planning and (3) control. Critical decisions are to be taken by the business unit not by IT or security people. This area with the underlying *Business Decision Rules* also supports Risk Management and is not superseded by metrics.

2 Required Characteristics

In order to deliver the above benefits, the metrics should have minimum characteristics (confer also [Wheat08]): (i) *consistent, reproducible,* as well as *reliable* since quantitative indicators are used, (ii) *relevant* because being correlated to security actions, (iii) *useful* or informative and functional, (iv) *high-piled* or sectional and at distinct level, and (v) *manageable* with low overhead and costs and *understandable*. These characteristics are discussed now.

The metric must first use quantitative (or at least quantifiable) indicators which can be obtained objectively and reproducibly. The latter characteristics mean that the result is independent from whom performed the measurement and that it can be repeatedly be obtained. The repeatability or reproducibility is important since one need to make comparisons of earlier and later values and to find trends. As a matter of course, the metric must provide consistent results (otherwise it is not reproducible). Note that this first requirement is often the reason for security managers to flinch from measuring security. But information security is not a feeling or notion. If risks are real, countermeasures must also be substantial which one should be able to demonstrate in some way.

Secondly, the rating produced by the metrics must allow to be attributed to a specific action or a group of actions for information security. Without such causality between measured data and information security action, the organization can not benefit from the metric because nothing can be learned. On the other hand this means that changing the action will effect the measurement. As a result, one can make improvements through controlling actions. Measuring parameters which are beyond the organization's control may provide quite interesting background information, mostly however the effort spent is for the birds.

This leads thirdly to the requirement that the metrics must provide enough information to enable the security managers to add or modify actions in a systematic manner. When designing a security metric it must at least be considered that the measured data can and will vary over time. But more over, the metric should be such that it provides benefit for the organization as described in Chapter 1. Specifically, the measurement should directly be aligned with the organizations' mission. Without a clear definition of the target the measurement will fail to accomplish anything real.

In practice, this requires a hierarchy. There are security measures on different levels. On each level transparency and the ability to control is required. Simultaneously, an aggregated rating with respect to security is required directly related to the organizations' mission.

Factor number five which should be considered when designing security metrics is rather pragmatic. The measurement should be manageable in every-day life. It should produce low overhead and costs. In addition, the results shall easily be communicated and clearly understandable – eventually, after some aggregation, also for the management board.

3 How to measure

Before any measurement is planned or done, there are some crucial questions which should be addressed. The starting point is to ask for the reason and the goal to be achieved. What is the purpose of the measurement? What shall be the benefit? Then it is important to know how the measurement will be used. Who will use it and how? What kind of result is expected and how should it look like? After having answers to such questions one can develop a suitable metric.

3.1 Approaching quantities

Fig. 3 provides further guidance. First one has to determine the *Purpose* (or goal) of the measurement. The figure shows three subjects (security controls, related processes and achievement of goals) and the five parameters from Fig. 1. So, one can aim to measure the effectivity of a security control for example. Second one needs an *Observable* (as the real-life source of information). Third a *Method* must be selected. One can count things, determine the coverage or density, meter length or durations, quantify frequencies or rates, determine a magnitude or degree, and find out costs or any effort. Fourth, one should consider the role of the information and decide if it directly evaluates towards the purpose (direct indicator), if more contextual information is being provided, or nothing of both. This is discussed in more detail in Chapter 3.2 below. Fifth, in most cases several measurements have to be *aggregated* and also be *interpreted* to obtain functional information.

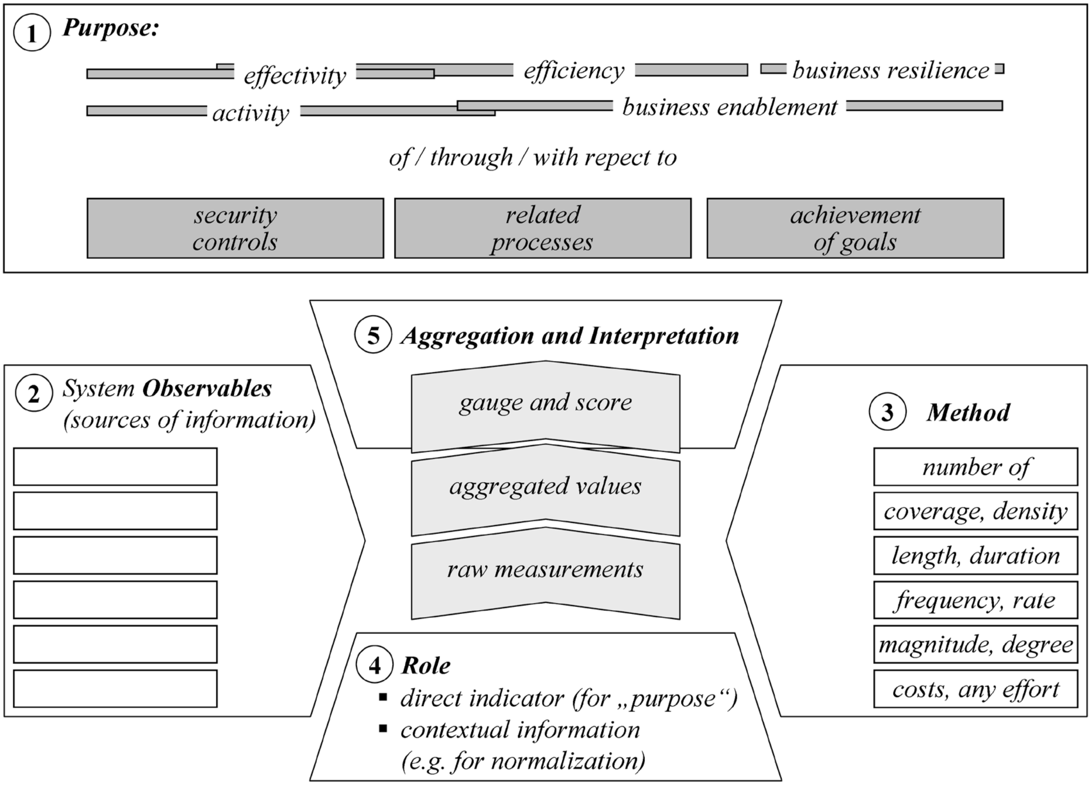

Fig. 3: Components and relations for the design of metrics (schematic)

Security Services and Large Scale Public Applications

User and Access Management in Belgian e-Government

Jos Dumortier · Frank Robben

Interdisciplinary Centre for Law and ICT (ICRI), K.U.Leuven
Sint-Michielsstraat 6, B 3443
BE – 3000 LEUVEN
jos.dumortier@law.kuleuven.be
frank.robben@ksz.fgov.be

Abstract

Efficient e-government is not possible without integrated information management. From a privacy protection perspective systems integration has to be preferred over data integration. A well-accepted model for the organisation of user and access management in this perspective is a federation based on circles of trust. The following pages describe how this model is implemented in Belgium, using five building blocks: unique identification numbers, the electronic identity card, validated authentic sources, service integrators and sector committees for data protection. Using these building blocks user and access management is organised following a generic policy decision model. The objective is to illustrate that integrated e-government is not necessarily incompatible with optimal protection of privacy.

1 E-Government Requires Integration

Information management in the context of e-government has to ensure that the government can provide effective services to citizens, companies and other organisations. This is not possible without far-reaching integration. Citizens and companies assume that the government as a whole will only request the necessary information once and, after checking for accuracy, will then reuse the information whenever it needs to do so. With this in mind, agreements must be reached between government echelons and agencies. Which agencies gather which information, check it for accuracy, store it and make it available for other echelons and agencies?

Everyone expects services from the government aligned to specific situations and also offered as far as possible in personalised form.[1] The alignment of services to specific situations can be achieved by offering services from the perspective of the user. Citizens and companies no longer have to find their own way through the labyrinth of government institutions and competences, but receive integrated services relating to events taking place throughout their lives: birth, work, housing, illness, retirement, death, starting a business, etc. However, this presupposes that these services are offered across all government echelons, government agencies and private bodies.

Citizens, companies and their service providers must be able to find all the relevant information and services using one electronic access portal of their choice. This electronic access portal must not be

[1] The Belgian OECD report on e-Government (2008) reads (p. 19): “Belgian citizens are more interested in accessing relevant, personalised services online, rather than learning the complexities of Belgian governments’ competences”. The full study is available from http://www.fedict.belgium.be/nl/downloads/.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2009), 97-107

unique in the sense that there can only be one, but users must be able to find everything they want regarding a given event on the electronic access portal of their choice. This requires that electronic services from different government echelons and agencies can easily be integrated into electronic access portals by all those who develop them.

Automation today is generally being developed by governments according to a Service Oriented Architecture (SOA). SOA is essentially an architecture for distributed development, management and use of ICT components, which call upon each other as services. It allows all those involved in electronic government service delivery to work together but still to maintain their individual autonomy and specific working methods. Local administrations and associations, health insurance funds, trade unions, banks, accountants, employment agencies, etc., can integrate the electronic services provided by the government – whether or not supplemented by their own services – and then offer them in a manner that is ideally suited to their target group. Companies or other end users can also have their internal company applications interact directly with electronic government services.

Where possible, users want services to be provided automatically. The government can, for example, relieve them of the burden of applying for tax deductions or exemptions, reduced rates for utility services, free public transport or other benefits that are allocated to them based on a social situation previously known to the government. At the same time, however, active contribution and a high level of self-service and self-steering are also appreciated. Services have to be offered in an efficient and user-friendly way, through various channels depending on the user's choice, as well as being reliably, securely and permanently available.

Government policy is expected to be based on objective and updated data. Citizens rightly demand that the government takes a proactive stance and that policy anticipates new trends. Everyone also wants the government to combat all forms of fraud in an efficient manner and to apply the most modern data mining techniques to do so.

All these requirements have to be reconciled with maximum protection of privacy. Of course, that does not happen automatically. In the quest for efficiency, it is easy to fall into the trap of a higher level of data concentration and centralised processing.

The Belgian approach demonstrates how the latter can be avoided, in particular by implementing a federated user and access management. Below we broadly describe how this approach has been conceived in Belgium.

2 Definitions

User and access management consists, as the term itself indicates, of two parts: user management and access management. User management itself covers five aspects: 1) identity registration, 2) user identification, 3) identity authentication, 4) registration of attributes and mandates and 5) verification of attributes and mandates. Access management covers the registration of authorisations and the verification of authorisations.

Within the context of this paper, the following definitions of the above terms are used:[2]

- The *identity* of the user is a unique number or a series of attributes of a user (natural person, company, branch of a company, etc.) enabling the user to be unequivocally identified. This im-

[2] These definitions are also used by the Belgian Privacy Commission in a Recommendation regarding access and user management in the public sector (SE/2008/028) of 24 September 2008 (www.privacycommission.be)

plies that a user has one and only one identity. The fact that a pseudonym can be used in certain situations does not alter this fact.

- An *attribute* is any user characteristic, other than the attributes that determine the identity of the user, such as a specific quality, a position in a certain organisation, a professional qualification, etc. A user can have several attributes.
- A *mandate* is a right granted by an identified user to another identified user to perform a number of well-defined (legal) transactions in his name and on his behalf. A user can grant one or more mandates to one or more users.
- *Registration* is the process used to establish the identity of a user, a user attribute or a mandate with sufficient certainty before resources are made available and that is used to authenticate or verify an identity, an attribute or a mandate.
- *Authentication* of identity is the process of checking that the identity a user claims to hold does indeed belong to him. This can be carried out by checking: a) knowledge (e.g. a password), b) possession (e.g. a certificate on an electronically readable card), c) (a) biometric trait(s), or d) a combination of two or more of these means.
- *Verification of* an attribute or a mandate is the process of checking whether an attribute or a mandate that a user claims to have in order to be able to use an electronic service is actually a characteristic or mandate of this particular user. This can be carried out: a) based on the same type of means as those used for identity authentication, or b) after authentication of a user's identity, by consulting a database (authentic source) in which characteristics or mandates regarding an identified user are stored.
- *Authorisation* is the permission for a user to perform a certain transaction or to use a certain service.

3 Federated user and access management

Theoretically, it would be possible to achieve the objectives of e-government information management outlined in the introduction by centralising all the data concerning natural persons, legal persons and other entities as much as possible. Some years ago, there was a discussion in the Netherlands about a proposal to create a "digital vault" for every citizen. This would be controlled by the data subject and would combine all the data about this data subject that need to be available for use by the government. Ultimately, this idea was abandoned because of privacy and security concerns.

For this reason data protection supervisory authorities are often of the opinion that e-government data exchange should be organised as far as possible based on a distributed and decentralised storage of personal data.[3] A model that is frequently used for this purpose by the private sector is the model of a federation based on circles of trust.[4] Such a model implies that clear agreements are reached among the bodies involved in the electronic service delivery in order to organise user and access management together. Among other things, these agreements establish who performs which authentication, verification and checks, using which means, and who is responsible and liable for them. Agreements are also needed to determine how the results of the authentications, verifications and checks performed can be

[3] In its Working Document on Online Authentication Systems, adopted on 29/01/2003 (WP 68) the Article 29 Working Party writes (p.15): „The adoption of software architecture that minimises the centralisation of personal data of the Internet users would be appreciated and encouraged as a means of increasing the fault-tolerance properties of the authentication system, and of avoiding the creation of high added-value databases owned and managed by a single company or by a small set of companies and organisations."

[4] The model is based on the results of the "Liberty Alliance" project: http://www.projectliberty.org/.

electronically exchanged in a secure way between the relevant bodies. Who maintains which log files and how is it possible to ensure that an investigation – on the initiative of an inspection body or following a complaint – can perfectly reconstruct who has used which service for which transaction involving which citizen or company, when, via which channel and for what purposes?

Data protection supervisory authorities have emphasised that a federated system avoids unnecessary centralisation and the associated threats to privacy. For example, no copies of the validated authentic sources will be circulated. Moreover, multiple identical checks and the redundant storage of log data are avoided. Furthermore, this model also guarantees that every administration is working with the most up-to-date information. For example, if a user loses a characteristic, this will be dealt with in an appropriate way by the system at the time of registration. Finally, the system will liberate users from repeatedly having to provide proof of the same attributes or mandates.

A federated approach however assumes that everyone is singing from the same hymn sheet, so that all the components fit perfectly together. This is important, because administrative processes take place through various government echelons, institutions and agencies. For this reason, the same building blocks must be used everywhere.

4 Main Building Blocks

The most important building blocks used in Belgium in user and access management for e-government are the unique identification numbers, the electronic identity card, validated authentic sources, service integrators and sector committees for data protection. Each of these five building blocks will be briefly discussed below.

4.1 Unique Identifiers

In Belgium, unique identification numbers are used for natural persons and other entities (companies, associations, etc.) throughout the entire e-government data flow, at all levels and by all government institutions and agencies. Belgian citizens and foreigners living in Belgium are identified by their National Number. For other persons, not living in Belgium but who have contact with the Belgian authorities, the Social Security Identification Number (SSIN) is used. Legal persons and other entities are identified by the company number under which the entity is registered with the Enterprise Register (the so-called “Crossroads Bank for Enterprises”).

Sector-specific identification numbers – sometimes presented as more privacy-friendly – are not used in Belgium. There has been some hesitation about using sector-specific identification numbers in the health sector and in field of e-justice, but this idea has finally been abandoned. The Belgian Privacy Commission has explicitly expressed its support to the decision to make use of the National Number (or the SSIN) instead of using a specific patient number in the health sector.

Many applications exceed the boundaries of one particular public sector domain. Working with sector-specific identification numbers can therefore lead to considerable complexity. Experiences in Austria, where sector numbers are used, demonstrate that in practice organisations tend to avoid separate identification numbers in order to work more rapidly and more securely.

The protection of privacy when using unique identification numbers can be guaranteed in various other ways. Use of the number can be restricted or recourse can be sought to strict control on the exchange of personal data that are linked to the unique number.[5] Belgium has opted for a combination of both of these methods.

4.2 Electronic Identity Card

The preferred method of electronic identity authentication in Belgium is the use of an electronic identity card (EID). However, depending on the required security level, use is also made of either a combination of user name, password and citizen token[6], or a combination of user name and password alone. The EID does, however, offer a range of advantages. It combines possession of a specific document with the availability of particular knowledge (PIN code). In addition, a number of factual and legal factors limit the risk of abuse in the event of possible loss or theft of the card.[7]

Verification of the attributes and/or mandates is not performed using the EID. In addition to a device for creating a qualified electronic signature, the EID is exclusively an instrument for identification and authentication. The information on the card therefore remains confined to the data that are necessary to identify the holder, the certificate that allows the holder to authenticate himself and the certificate that enables the holder to place a secure electronic signature. Data that have nothing to do with the identification or authentication of a physical person or the electronic signature, such as characteristics and/or mandates, do not belong on the EID.[8]

4.3 Validated Authentic Sources

The fact that the identity of a user has been authenticated is not always enough to grant the person concerned automatic access to an electronic service. A user's access rights to an electronic service (authorisation) can be linked to his attributes and/or mandates. Integrated user and access management therefore requires that unambiguous checks can be performed on the relevant attributes of a person or the existence of a mandate given by a legal person or a natural person to which an electronic service relates and the person who is using this service.

The verification of attributes and/or mandates (for example, is the user a qualified physician? Is the user a lawful representative of the legal person?) takes place via channels other than the EID. In this context it is not recommendable to rely on non-validated information that is simply provided by the user himself. These elements have to be checked against a source that offers the required guarantees in terms of accuracy and up datedness of the information it contains. In Belgium such sources are called "validated authentic sources". The government agency in charge of a validated authentic source is responsible for the availability and quality of the information it contains and made available for other agencies and echelons. The State Health Insurance Fund, for example, will be in charge of a validated authentic source of qualified physicians, the Royal Federation of Notaries will keep the validated authentic source of notaries, etc.

[5] The Hungarian Constitutional Court (http://www.ceecprivacy.org/htm/91-15.htm) aptly formulated this alternative as follows: "(...) the use of PINs (Personal Identification Numbers) shall be restricted by security regulations. This can be done in two ways: either the use of the PINs is to be restricted to precisely defined data-processing operations or strict conditions or controlling measures are to be imposed on the availability of information connected to PINs and on the link-up of record-keeping systems using PINs".

[6] A citizen token is a card (with the same dimensions as a credit card) that contains 24 numbered personal codes and that is sent to the person in question by post following verification of certain credentials (National Registration Number, SIS (social insurance number) card number and identity card number). When access to an application is requested (e.g. Tax-on-Web), the user is asked for one of the codes at random.

[7] Danny De Cock, Christopher Wolf and Bart Preneel, The Belgian Electronic Identity Card (Overview), http://www.cosic.esat.kuleuven.be/publications/article-769.pdf

[8] The Belgian Privacy Commission issued an opinion (no. 1/2005 of 7 September 2005) arguing against the inclusion of aspects such as blood group or the consent for organ donation on the electronic identity card.

Privacy,
Data Protection
and Awareness

Simple & Secure: Attitude and behaviour towards security and usability in internet products and services at home

Reinder Wolthuis[1] · Gerben Broenink[1] · Frank Fransen[1]
Sven Schultz[2] · Arnout de Vries[2]

[1]Security
[2]Innovation and User Experience Management
TNO Information and Communication Technology
Groningen, The Netherlands

{Reinder.Wolthuis | Gerben.Broenink | Frank.Fransen | Sven.Schultz | Arnout.deVries}@tno.nl

Abstract

This paper is the result of research on the security perception of users in ICT services and equipment. We analyze the rationale of users to have an interest in security and to decide to change security parameters of equipment and services. We focus on the home environment, where more and more devices are (inter)connected to form a complex end-to-end chain in using online services. In our research, we constructed a model to determine the delta between the perceived overall security and the real security in home networks. To achieve an understanding of perception and how to identify the delta between perceived and real security, our work forms the basis for examining how perception relates to behaviour. Since humans are referred to as the weakest link in security, there are also differences in behaviour and desired behaviour from a security perspective.

1 Introduction

More and more equipment enters the home environment that interacts with each other and is connected to the Internet. Examples that are already common are set-top boxes, PC's, game consoles and smart phones. New networked devices are emerging, such as the heating system, home surveillance systems, smart energy meters and many will follow. With the introduction of these (inter)connected devices all kinds of new services are enabled.

The main reason that these kind of devices emerge is ease of use and efficiency. But with increasingly connected equipment and services, the technical complexity in these chains of hardware and software increases.

When technology gets more complex, security also gets more complex. Often too complex for the average user to comprehend, let alone configure the security functions correctly. Of course we do not want others to have access to our home surveillance system or to our home banking account details, but the average user is not able to configure the technology in a secure way [BrMS08].

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2009), 157-168

The complexity of the security configuration is shown when we take a look at the security warnings and notifications. One we are all familiar with is: “This certificate is not valid. Do you want to continue?”. This is too difficult to interpret and therefore unfit to make a reasoned decision on what to do. The perception of security and trustworthiness by the user often doesn’t match reality as they will under- or over estimate the risks and they may even lose faith in technology in some areas. This is caused by incorrect assumptions, bad security and trustworthiness decisions. Because of these issues, the user is commonly referred to as the weakest link in the security of a system. In order to create easy to use and efficient security solutions we need to know how users experience current solutions, what their perception of security in home networks is and how this perception is formed.

We will state the problem that we tackle in this paper in section 2. In section 3, we will describe the methodology that we used. In section 4 we present a model on attitude and perception and section 5 will expand on some theory on user experience and behaviour. In section 6 we describe a few commonly used security techniques and their user acceptance. Section 7 summarizes the key findings and conclusions and section 8 contains our plans for future research.

1.1 Trends

User education
Current solutions (used by e.g. banks) tend to educate the user how they should behave and how they should react on certain events. Examples in the Netherlands are:

• www.digibewust.nl	(make people conscious of threats)
• www.waarschuwingsdienst.nl	(warning service for security threats)
• www.surfwijzer.nl	(hints to safely surf the net)
• www.driekeerkloppen.nl	(only do online banking after three checks)

Although security awareness should always be part of the solution, this paper states that the burden should not be put one-sidedly on the user alone.

Fading network boundaries
Just like in the corporate world, the boundaries of the home network tend to fade. Wireless LAN networks are sometimes open to users outside the home environment, and some applications enable remote access to content stored in the home network.

Interconnection
More and more equipment and services are interconnected and connected to the internet. In this way, a chain of devices is created, each running their own software or service. On installation usually a default security configuration is used to make things easier for the end-user. This is not always a good thing to do (e.g. default passwords are easy to guess). Because there are many services and equipment that behave like this, the user looses track of the actual security situation in the home environment.

1.2 Scope

The focus of this paper lies on user perception and human-machine interaction with respect to security. Although Privacy and Trust aspect are important factors in security user experience, this will be out of scope for this paper.

Standards and Technical Solutions

KryptoNAS: Open source based NAS encryption

Martin Oczko

Utimaco Safeware AG, Aachen
Martin.Oczko@utimaco.de

Abstract

Even though more and more software based solutions exist that protect data of notebooks and workstations, NAS systems with integrated encryption mechanisms are very rare available on the market. At the same time it is possible to realize a cost optimized secure NAS device with good performance using freely available hardware and open source software. This article describes the research results of the KryptoNAS project which goal was to develop a NAS device with transparent Hard disk encryption based on open source software and standard hardware. The outcome of the project is a pre-product secure NAS device which meets the requirements of SOHO and SME users.

1 Introduction

Although primary Network Attached Storage was designed for the usage in datacenters and as storage for mainframe systems there appear more and more NAS devices on the market which are intended for the usage in SOHO and SME Networks. NAS devices become popular because of easy configuration and administration in contrast to the common server systems. These are indeed more flexible and can provide a bigger range of functions but the ease of use of NAS systems which offer specialized functionality convinced the users. In particular users of small offices and small enterprises without a dedicated IT department or IT administrator appreciate the simplicity of NAS devices. There are a couple of NAS devices available which aim on user groups like surgeries, law and tax consultant offices or home users. These users often have to satisfy security requirements and have to assure that their data is stored securely. Unfortunately, NAS devices which provide disk encryption functionality are very rare and unproportional expensive. This fact and the lack of adequate devices with the required functionality available on the market were the motivation for the KryptoNAS project. The idea behind the KryptoNAS project was to investigate the question whether it is possible to develop a secure and cost optimized high performance NAS device which is completely based on open source software and on minimalistic hardware. The goal was to develop a rudimental prototype of a NAS device which meets the defined requirements with the main focus on security and the performance and which acts as proof of concept for the idea of an open source based NAS device running on minimalistic hardware.

In the following this document defines different classes of NAS devices and describes the requirements for the NAS device which has to be designed. After this the paper describes the security concept of the NAS device and presents results of some performance measurements and finally ends with a conclusion.

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2009), 223-229

2 NAS Categories

By analyzing the NAS market itself, in principle the available NAS devices can be divided in the three following categories:

SOHO Class: Cheap and low-performance devices without RAID functionality. The data transfer performance of these devices ranges between 3-8 Mb/sec.

SME Class: These devices usually come with RAID functionality and provide the option for several hard disk drives. The data transfer rate ranges between 8-20 Mb/sec assuming a Gigabit Ethernet interface.

Enterprise Class: These devices are designed for the usage in data centers. Devices in this class provide several TBytes of storage space with access over high performance fibre-channel interfaces. The data transfer rate often lies above 100Mb/sec.

Due to the fact that the demands on the devices in the enterprise class are completely different than the demands on devices of the SOHO and SME classes, the enterprise class devices are not considered in the following. Looking at SOHO or SME class NAS devices, there are only a few devices available with integrated encryption functionality. In addition some of the available devices with encryption functionality provide only weak encryption mechanisms and only one-factor authentication. Furthermore these devices come with very low performance (in some cases under 4Mb/sec) if the encryption function is activated.

3 Requirements

Based on this market research a concept for a secure and cost optimized NAS device with a performance according the needs of SOHO and SME users was being composed. The first step was to define the requirements for the new device. These requirements can be divided in general requirements and hardware requirements which are defined as follows.

3.1 General Requirements

- Transparent encryption on device level
- Performance on 100MBit Level (at least 8 Mb/sec)
- Two-factor authentication (token + password)
- Strong encryption (AES-256)
- Open Source software components

3.2 Hardware Requirements

- Minimalistic hardware (low energy consumption, passive cooling)
- Standard components
- Minimal costs

3.3 Hardware Platform

The fist step in this project was the selection of the hardware-platform, on which the KryptoNAS device should be operating on. A market research shows, that only two promising hardware platforms are available today which support the specified requirements for the KryptoNAS. One Platform is the AMD Geode [AMDGeode] processor family, which is used e.g. in Thin Clients and other low-performance systems. These processors offer an integrated crypto engine which accelerates cryptographic operations like symmetric encryption. The other potential Hardware Platform is the Eden processors family, offered by VIA [VIAEden], which also comes with an integrated crypto engine. Compared to the Geode processors, Eden processors support the AES encryption up 256 key length (whereas Geode only supports key lengths up to 128 bit). To meet the requirement for "strong encryption" the VIA Eden processors were chosen as the hardware platform for the project. Enclosed the datasheet for the KryptoNAS main board and a photo from the used hardware:

- 1 GHz VIA V4 Eden CPU with PadLock Security Engine
- Energy consumption : 9W
- Passive cooling
- Hardware acceleration for AES-128/256 and SHA-1
- 1 GB RAM
- 2 x SATA
- 2 GB Compact Flash Card boot device
- 2 x 100MBit LAN
- 4 x USB

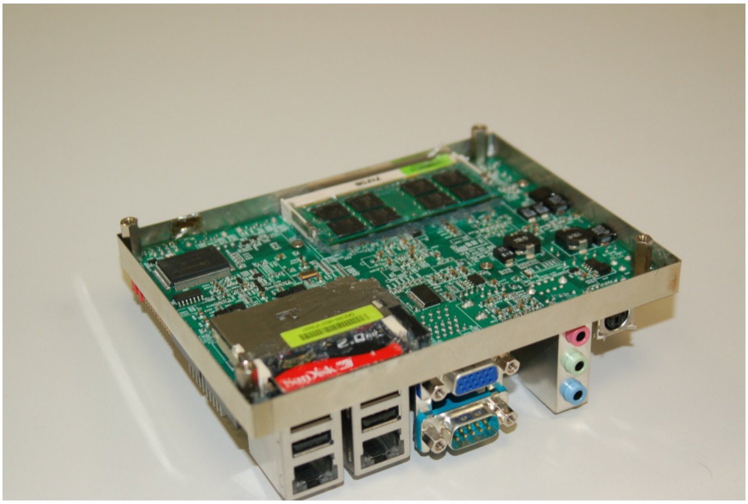

Fig. 1: KryptoNAS mainboard ADE-2100

3.4 Software Architecture

The architecture of the KryptoNAS itself looks similar to usual NAS systems. Based on its own operating system, the KryptoNAS comes with a web based administration console and a fileserver interface.

Secure Software, Trust and Assurance

A Structured Approach to Software Security

Ton van Opstal

Ericssonstraat 2, Rijen, The Netherlands, Ericsson Telecommunicatie BV
Research & Development
ton.van.opstal@ericsson.com

Abstract

Security is an important aspect of software that needs to be considered during the entire System Development Life Cycle (SDLC). A structured and practical approach to handle Software Security is proposed by defining the concept of Security Architecture and by using this Security Architecture as key concept to relate all security activities that need to be performed as defined by the SDLC. The Security Architecture itself is described using a structured definition format, called the Extensible Security Architecture Description Format (XSADF). XSADF can be used as input format for tools that can assess the security aspects of a system under development.

To support the work on a Security Architecture, a Security Architecture Framework is proposed. Software Architects can use this framework as a template to define the Security Architecture for the system they are developing.

The structured approach using XSADF, with a central place for Security Architecture, is a step to achieve „security by design".

1 Introduction

It is now widely accepted and advocated that security should be considered throughout the entire software development life cycle ([HoLi06], [McGr06], [KSS+08]). Considering security during development should lead to a more pro-active "security by design" approach, rather than the current practice of "security by patching".

As part of a "security by design" approach, we should also ensure that the software being developed complies with applicable standards, guidelines, best practices and laws. Software security shall be measurable, to make the result of the effort on software security visible.

However, striving for "security by design" is easier said than done. The current practice in industry typically involves a lot of paperwork. For starters, there is a lot of documentation in the form of standards, guidelines and best practices that serves as input to the development process. On top of this customers provide additional documents with more specific security requirements. In most cases the origin and rationale for these security requirements is not clear. Next to that, development processes require security activities to be performed and security documentation to be produced as a result of these activities. Examples of such activities are: Architectural Risk Assessment, security requirements definition/selection, hardening, and vulnerability analysis.

It is not clear if all the documentation that is produced is actually used in later stages. Doing a security review in the end, e.g. to check compliance to standards, is a tedious task, as it means reading through

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Vieweg (2009), 281-290

piles of documentation filled with details and hidden cross references. Tracking security issues described in all these documents is hard.

We propose a more structured way to realize the "security by design" idea in practice ([Opst08]). Firstly, we introduce the concept of Security Architecture that can be used as the key concept to relate all security activities that need to be performed as part of the development life cycle and as the basis to organise all the associated documentation. Secondly, we propose an XML format for this, so that tool support can be used to find or select relevant information.

Together, this provides a way to get a grip on all existing documentation related to the security, taking the architecture as a base.

2 Software Security Approach

Our proposed approach is a natural extension of the practice at the National Institute of Standards and Technology (NIST) to describe security checklists in a standard format. For our purpose we considered the Extensible Configuration Checklist Description Format (XCCDF), described in [ZiQu08]. A small extension of this format allows us to use this format not just for security checklists, but to describe the whole Security Architecture. We call this the Extensible Security Architecture Description Format (XSADF).

2.1 Security Architecture

The definition of *Security Architecture* that we propose to use is as follows:

> *"The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its security design and evolution. The Security Architecture comprises Security Requirements, Security Controls, Business and Security Architecture Assets (including associated threats, vulnerabilities, and risks), security documentation, and security definitions and abbreviations. It contains those aspects of Software Architecture that are needed to assess the security of a system."*

This definition is in line with the more general definition of Software Architecture and defines what comprises a Security Architecture. A Software Architect is typically the responsible person for assessing the security of a system.

The Security Architecture comprises security requirements, Security Controls, assets (including associated threats, vulnerabilities, and risks). It effectively documents all the steps in the development life cycle, from security Architectural Risk Assessment to choosing and implementing Security Controls, in the same XML format.

A Security Architecture Framework is proposed that can be used as a template for the definition of a Security Architecture. This framework is defined in our proposed XML format as well. Software Architects define the Security Architecture of the system they are working on using the Security Architecture Framework as a base. This framework is more than a template, since it is constant being updated with new requirements, controls, threats, assets, etc.. It can be expected that a Security Architecture Framework is developed, or further improved, for specific areas or technologies.

The Security Architecture Framework proposed consists of:

- Security Requirements
- Security Controls
- Business Assets (including known Threats and Vulnerabilities per asset).
- Security Architecture Assets (including known Threats and Vulnerabilities per asset)
- Threats and Vulnerabilities
- Definitions and abbreviations: consistent use of this terminology within the Security Architecture Framework is considered important.
- Mapping between Security Controls and Security Requirements
- Mapping between Business Assets and Security Controls
- Mapping between Security Architecture Assets and Security Controls

The base for the Security Controls part of the Security Architecture Framework is taken from NIST Special Publication 800-53 ([RKJ+07]). The reason is to achieve alignment between Information Security and Software Security. NIST Special Publication 800-53 is targeted at Information Security. The mappings are needed to create compliance statements.

2.2 Extensible Security Architecture Description Format

We introduce an XML-based format, called XSADF. This format is based on XCCDF, as stated before. In the table below, we describe the usage of the XSADF XML elements and make a comparison to the XCCDF original intent of these elements.

Table 1: XCCDF and XSADF

XCCDF Element	XCCDF original intent	XCCDF used for Security Architecture (XSADF)
Benchmark	A Benchmark holds descriptive text, and acts as a container for the other elements. An XCCDF document holds exactly one Benchmark object.	Used as in XCCDF.
Profile	A Profile is a collection of attributed references to Rule, Group, and Value objects. A Profile is used to define a baseline of Security Controls; more than one Profile can be defined in an XCCDF document.	A Profile holds (1) baseline of Security Requirements, (2) Security Architecture Assets, (3) definitions and abbreviations and (4) security activities of a SDLC.
Group	A Group can hold other elements and can be selected.	Used as in XCCDF.
TestResult	A TestResult holds the results of performing a compliance test against a single target device or system.	A TestResult holds (5) statement of compliance against a baseline of Security Requirements, (6) statement of compliance against a baseline of Security Controls.
Value	A Value holds a named data value that can be substituted into another XCCDF element's properties.	Used as in XCCDF. In addition a Value holds definitions and abbreviations.
Rule	A Rule holds check references, a scoring weight, and may also hold remediation information.	A Rule holds Security Controls and Security Requirements.
Asset (new)	-	Asset is introduced to hold Business Assets and Security Architecture Assets. Assets marked abstract are part of the Security Architecture Framework, and contain references to applicable Security Controls, Threats and Vulnerabilities.
Risk (new)	-	Risk is introduced to hold business and Security Architecture risks.

CWE™ (http://cwe.mitre.org/) is used in our Security Architecture to refer to software weaknesses (which are the source of vulnerabilities) in an Architectural Risk Assessment. CAPEC™ (http://capec.mitre.org/) is used in our Security Architecture to refer to threats in an Architectural Risk Assessment. Threats are described in CAPEC™ using attack patterns; these attack patterns can be used during Vulnerability Analysis to verify whether the implemented Security Controls are effective to mitigate or reduce the observed risks. CPE™ (http://cpe.mitre.org/) is used in our Security Architecture to refer to hardware.

MITRE (http://www.mitre.org/) mentions Asset Management, but does not have concrete examples on how to do this. Our approach is to extend XCCDF with the necessary elements Asset and Risk. Furthermore some changes are proposed to the existing definitions. These changes are backwards compatible with the original XCCDF specification.

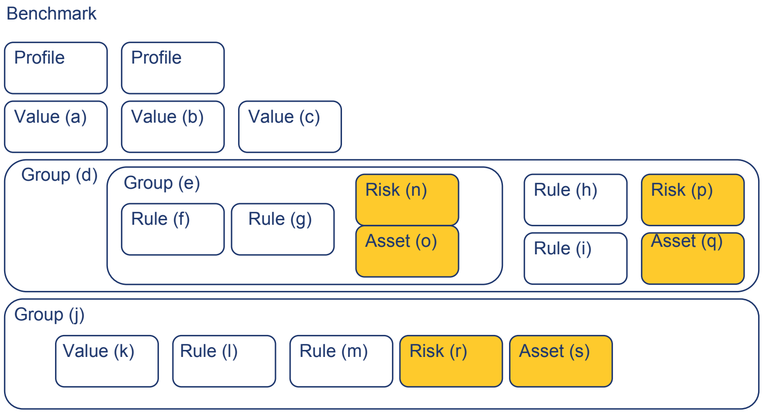

Fig. 1: From XCCDF to XSADF

In the following paragraph the most relevant XSADF elements are discussed in more detail.

Group

Groups are used to create structure in the Security Architecture Framework. During the work of defining a Security Architecture, groups that are not applicable are deselected. By default a group is selected.

Rule

Rules are used to define Security Controls and Security Requirements.

Begin (example: rule)

```
<cdf:Rule id="AU-8-Rule">
   <cdf:title>Time Stamps</cdf:title>
   <cdf:description>The information system provides time stamps for use in audit
                    record generation.</cdf:description>
   <cdf:rationale>Supplemental Guidance: Time stamps (including date and time) of
                  audit records are generated using internal system clocks.
                  </cdf:rationale>
</cdf:Rule>
```

End (example)

During the work of defining a Security Architecture, rules that are not applicable are deselected. By default a rule is selected.

Asset

Assets can be divided as follows:

- Business Assets: these assets have to be protected by the systems that provide them. An example of a business level asset is “a customer database holding details of mobile phone subscriptions”. These assets are considered as part of the focus on Information Security by enterprises, but need already to be considered during an Architectural Risk Assessment performed for a development project (Software Security). When performing such an assessment, the risks related to these assets need to be considered from the viewpoint of the enterprise.
- Security Architecture Assets: these assets form the Security Architecture for a system and need to be considered during an Architectural Risk Assessment performed for a development project (Software Security).

During the work of defining a Security Architecture the assets defined in the framework that are not applicable are deselected. By default an asset is selected.

In the Security Architecture Framework it must be possible to represent a class of assets. This is achieved by using the notion of an abstract asset, which is indicated by assigning the value “true” to attribute abstract (abstract=”true”). An example of an abstract asset can be ‘Password’, while a concrete instance (like ‘root password’) represents an occurrence of that asset in the system under consideration. Abstract assets can be used to include applicable Threats, Vulnerabilities and Security Controls.

Assets are defined in the following way. This example contains one abstract asset and one concrete asset.

Begin (example: Access Control Groups asset)

```
<cdf:Group id=”AccessControlGroups”>
   <cdf:title>Access Control Groups</cdf:title>
   <cdf:description>Overview of all Access Control Groups. Depending on the
                    operating system, each access group has different
                    attributes. Attribute names are between =…=</cdf:description>
   <cdf:Asset id=”access_control_group_abstract” level=”data”
              category=”information” abstract=”true”>
      <cdf:title>Access Control Group</cdf:title>
      <cdf:description>A Group is a list of principals (Security Engineering, Ross
                       Anderson).</cdf:description>
   </cdf:Asset>

<!—Concrete Assets -->
   <cdf:Asset id=”acg-root” level=”data” category=”information”
              extends=”access_control_group_abstract”>
      <cdf:title>root</cdf:title>
      <cdf:description>=Name=’root’</cdf:description>
      <cdf:description>=Members=’root’</cdf:description>
      <cdf:description>=Description=’Standard Linux group’</cdf:description>
      <cdf:platform idref=”SLES 10 Service Pack 2” />
      <cdf:component>Operating System</cdf:component>
      <cdf:deployment>’/cluster/etc/groups’</cdf:deployment>
  </cdf:Asset>
</cdf:Group>
```

End (example)