ISSA The Global Voice of Information Security

The Path to Assured Solutions

By Carlos Trigoso
Carlos.trigoso@pirean.com

An international article brought to you from the UK.

Security architects and practitioners need to develop an integrated data model that will enable end-to-end user management and access auditing. This article proposes a data model and reviews ideas that could constitute the basis for Security Management enhancement and progress.

There is constant progress in the Security Management discipline. Now we see IT Security Management as a continuous process, similar to other business activities.[1]

Security definitions have moved through six stages, passing from the early association to perimeter protection, to security education and risk management, and reaching finally a compliance and auditability focus.

On the negative side, this new vision has obscured the technical level. While we know where to position security in the general picture, it is not so clear what to do in each of the areas included in Security Management.[2]

For example, ITIL Security Management and COBIT, although collating all the aspects and measurements of the security discipline[3, 4], fail in addressing technological choices.[5, 6]

As a result, business leaders are aware of the relevance of a security process, but mid-level management and technical personnel are in the dark about how to connect the abstractions with the tools they have.

Where We Stand Now

Enterprise security is not only about “information security.” The time where information was “discovered” as a business resource is over, and Security Management is not restricted to “confidentiality, integrity and availability” anymore: It is essential to link it to Systems Management disciplines to achieve provisioning, patch management, continuity and storage management.[7]

Thanks to this progress, there is now a strong dependency between Security Management and Business and IT Continuity Management. Security is not anymore a collection of obscure, closed-door technologies, but synonymous with “dependability” and “trustworthiness” of IT services that are now viewed as “utilities.”[8, 9]

I believe that we need to look now at the subprocesses of Security Management in the same way as the ITIL defined Services Support and Delivery. This will help us to bridge the gap between strategy and implementation.

Security Data Types

The essence of Security Management is a data structure. Although simple at the core, its ramifications are not. It is a series of mappings:

▲ Users to user names
▲ Users to passwords
▲ Users to tokens (or certificates)
▲ Users to accounts
▲ Users to groups
▲ Users to roles
▲ Users to services
▲ Users to objects (operating systems and devices)
▲ Users to proxy objects
▲ Users to permissions
▲ Users to events (audit events)

Together, these mappings form a single data type at the core of all security technologies.[10, 11]

A data-centric security approach allows us to see implementation tasks beyond point solutions. It answers to the need of efficiently managing **data** and mappings by crossing technological and platform boundaries.

This is a first insight for the technologist: Security needs user data and mappings integration. Without this, what you have is a collection of trendy but disparate products. These may be more or less effective, but on the whole do not increase trustworthiness and instead multiply risks and uncertainties.

A data-centric approach recognizes the diversity of data mappings within the enterprise, and the need to achieve enterprise-wide user data synchronization.[12]

A Secure System

To continue we need to address a key problem: A completely secure system is one that does not allow the flow of information. Not one that has a well-defined and controlled security policy, but one that does **not** have a security policy as explained in A Theory for Systems Security.[13]

This is so because a security policy can only specify which information exchanges are valid. A security policy (an access matrix for example), does not transform insecurity into security, but only brings the security level to an accepted level.

If the security policy is well defined, then the factor of decrease is a known quantity.

Mapping users and entities in the system sets up its “security policy.” By this mapping, users are able to interact with the assets, and to exchange information.

This is why multiple user repositories are not a problem. The problem is the diversity of mappings between those users and the assets they need to be productive (applications, Web services, e-mail servers, for example). The issue is provisioning those accounts efficiently while complying with the law and company policies.

We need a technical implementation where–despite the variety of tools and targets–we are able to tell when a user is accessing a specific object and for what purpose.

Ideally, we should be in a position where, knowing all access information, we are able to block or disallow invalid changes, and to roll back these changes after a security breach.

Data-driven security architecture enables all of this.

Data-Driven Security and Assurance

How should we address “information assurance”? This includes the analysis of failures and semantics of “trust” and “confidence.”[14] Is the technical specialist able to vouch for the security process in these terms?

The answers need a definition general enough to be useful for any business, but also practical enough to describe what needs to be done.

We need to add now the notion of “insecure time.”

“Insecure time” refers to a period where the security policy has failed to stop intrusion or malicious use. A system is secure if its “secure time” is greater than its “insecure time.”[15] Or, more precisely, insecure time is the sum of the time it takes to detect an incident and the time it takes to react to the incident (over all incidents in a given interval).

This gives us powerful guidance: The specific technologies move into the background, and it does not matter how you increase secure time versus insecure time. What matters is that you select suitable tools to achieve good results.

The most sophisticated security product will not be able to reduce the response time (and therefore increase the secure time) if all the security data is not known or is not manageable!

To address the entire lifecycle of the IT system, covering the whole enterprise and its interactions with other organizations and the government, the best solution will be one that encompasses all user mappings mentioned before.

This requires a switch from “feature implementation” to “integration” work, seeing each security project as a data-driven project, as a data integration job.

This removes administrative tasks, enables predictable practices, and focuses on measured competencies and continuously improving results. The Security Process manager will not control a collection of specialists, with differing tools, goals and abilities, but a single integrated team where the common language is Integrated User Data Management.

For some time it has been trendy to speak about the “lifeblood”[16] of the enterprise and to underline how “special” Security Management is.[17]

However, it is not different: Security Management is becoming similar to Systems Management. While the Systems Management database (CMDB) contains configuration item dependency and inclusion mappings, the Security Management Database contains user-to-object mappings. That is the difference.

Information is part of the economic process, and information systems are part of the business infrastructure. Nevertheless, an atmosphere of mystery appears if we do not understand the counterintuitive fact that the most secure system is one that **does not** exchange information with the environment, while a system with a security policy is relatively insecure. This paradox has driven people to try to cancel the “problem” by proposing more and more security technologies that fragment the environment and introduce more sources of risk.

Instead, it is better to accept the insecurity implied in opening a system and move the emphasis of Security Management from policy definition (access matrix and other models) to data-driven security and secure time restoration (“secure” versus “insecure time”).

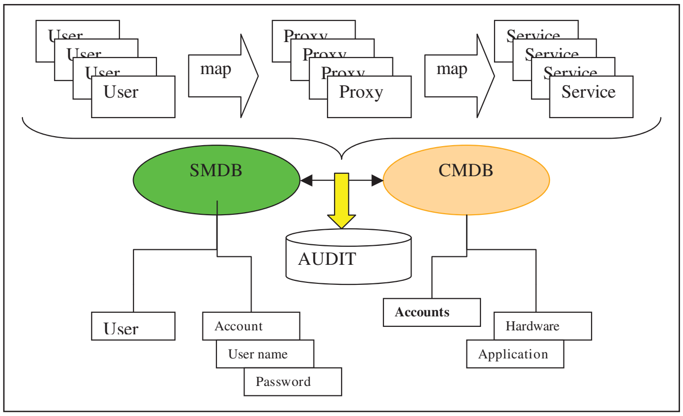

Figure 1: Mapping users and entities in the system

This agrees with the standard good practice that Security Management should aim at supporting the overall business continuity management by ensuring that services recover within agreed business time scales.

Security Management Subprocesses

If we position Security Management at the same level as Services Management, we need to define its subprocesses to have a complete discipline. This will also set the skills profiles and activities of each subarea.

A recently published approach to security process maturity[18] defines five key stages as follows:

1. Protection: Perimeter security, intrusion detection
2. Validation and Provisioning: User to username and password mapping, user to accounts and services mapping
3. Access and Integration: User to groups, roles and objects mapping
4. Compliance: Compliance with the law, individual rights and policies
5. Total Security Confidence: A continuing process of measurement security improvement.

These subprocesses are simultaneously phases in time, layers in the enterprise security, and parts of the total picture. They form an integrated Security Management process.

Following that approach, it is possible to have a more detailed breakdown, into specific views:

1. Protect: User platform to network mapping
2. Detect: User to protocol and network layer mapping
3. Validate: User to user name and password mapping
4. Provision: User to services and accounts mapping
5. Authorize: User to groups and objects mapping
6. Integrate: User to roles mapping
7. Verify: User to security policies mapping
8. Audit: User to logged event mapping
9. Manage: User identity and access management policies and risk management
10. Improve: User identity and access management continuous improvement

The guiding principle for this subdivision is associating data mappings with each of the subdisciplines. For example, the first process (Protection) maps the client platform, because security practices at that level focus on hardware and infrastructural measures. Further investigation will give an even more detailed picture of the data-driven security approach.

Assurance

In this way, we arrive at an idea of security assurance that is far from hype and trends. This idea of assurance is similar to "old" approaches in the literature.[19, 20]

Following work by Williams, Ferraiolo, and others, I have adopted here the notion that assurance is a measure of confidence in the accuracy of a risk or security measurement and not a measure of the degree of satisfaction.

A measure of satisfaction would depend on a nonexistent measurement of the security needs. How do you measure what you need so you can measure what you do to satisfy it? While there are many ways to express risk quantitatively, there is none to express "security needs." This originates solutions with technologies that are not complete.

Assurance is orthogonal to risk. They are different dimensions and should not be confused. A high assurance rating is not equal to a high security and low risk rating.

In the "secure system" model, there is no information exchange. No information goes in and no information goes out. Is that scenario compatible with a high assurance rating? It is not: If no users have access to the assets, this cannot represent any "security needs."

Compared to this, but equally problematic, if a system has strong access controls but lacks auditing functions, how can we tell when the installed parts are functioning properly? If we confuse assurance with security, the system will appear to be safe, while in fact there is high uncertainty about its state!

Separating assurance and security becomes especially interesting when we consider the needs of the decision maker. After making a risk assessment, she may have a quantitative idea of the risk level, but what if the confidence in the gathered data is low? In that case, she will be not sure whether the risk is acceptable or not.

If confidence in the risk assessment is high, then it makes sense to add new security mechanisms. If the confidence is low, adding a new tool will increase the uncertainty in the system.

The best solution is to increase the assurance level with better information on the severity of the risk, the state of the system and its parts.

As references 19 and 20 show, assurance arguments are a powerful tool to reduce uncertainty in security assessments.

The common response has been to multiply the technologies and services employed to enforce "security," claiming to address uncertain or imagined levels of threat. This explains why most security products and services converge on the protection and detection subdisciplines. By doing this, vendors and consultants are answering to short-term preoccupations of business managers.

It seems easier (and less expensive) to secure one perimeter than to secure a large volume of applications or multiple internal networks.[21]

At the same time, the compliance and audit subprocesses of Security Management were sparsely populated. Just ask your security specialists how they are collecting and aggregating the traces and logs of all their security servers and tools.

These problems have had only a few answers from a handful of visionary but small companies.[22]

The approach in references 19-20 teaches us that in selecting assurance methods, we should measure these against their cost. Assurance can be expensive if extensive testing is necessary. Therefore, it is better to adopt the most generic and stable method or a combination of methods.

Reducing uncertainty in a secured system always requires setting up known channels of information and foolproof methods of data aggregation, including data on the security components themselves.

Data flowing through those channels is meta-data (data about the user mappings). A single meta-data format is possible and necessary, and there are already tools that track security information and increase the assurance levels.[23, 24]

In the audit subprocess, we need to carry out the notion of "negative evidence," which is any event that will increase uncertainty. Intrusions and security incidents are negative evidence. We can return to the definition of insecure time: Negative evidence produces insecure time. Only complete meta-information eliminates negative evidence.

Assured Solutions in Security Management

Starting from these ideas, it is possible to propose Security Management "assured solutions," contrasting with the lack of guarantees usually found in commercial security implementations. The lack of contractual assurance is usual in software offerings, as vendors are "not responsible" for the failures and limits of their products.

This is hardly sustainable in a mature IT services market. To assure a solution in an uncertain environment, with increasing security threats and continuous technological change, you need to start by understanding that information security is a business issue, and not a technological matter. The levels of "insecurity" in a system depend directly on the "security policies" that you apply, and a Security Management process boils down to user management.

Against the present predominance of point solutions and technological silos, you need to see security management as a cyclical change process, continuously meeting the demands of the enterprise. It must enable and improve all other business processes, and at the same time be cost-effective to fulfill, run and control.

To progress we need to speed up division of labor within Security Management, to allow for more precise and measurable, traceable subtasks and subprocesses. If there is no progress, we will continue having more complex but partial solutions and low assurance ratings.

Carlos Trigoso has worked more than 20 years in the IT industry in South America, Europe and the Far East. He presently works for Pirean Ltd as the Security Management Principal and also as a consultant for IBM on Identity Management project support in Europe. Carlos is a member of the ISSA UK Chapter.

[1] Information Security as a Business Process, Paul Evans, Solbrekk Field Service Director, Volume 2, Number 7 October 2004, IT Network Solutions

[2] ISD Conference '04: Security from the inside out, By Bill Brenner, 07 Oct 2004, SearchSecurity.com

[3] ITIL Security Management, Cazemier & Overbeek, Office of Government Commerce, United Kingdom, 20th April 1999

[4] Quality Model Mania, Gary H. Anthes, ComputerWorld Development Topics, March 2004

[5] Combine CobiT and ITIL for Powerful IT Governance, Simon Mingay, Steve Bittinger, Gartner Report, 1st June 2002

[6] Best practices in support of IT Governance and Regulatory Compliance, Erik Guldentops, Advisor to the Board, The IT Governance Institute, 18 November 2004

[7] Central control: Let's get it all together, Chris Pick, November 1st 2003, SC Magazine

[8] Applying the Dependability Paradigm to Computer Security , Catherine Meadows, Center for High Assurance Computer Systems, Washington DC, 1995

[9] An Introduction to Utility IT, Pirean Ltd., 2005

[10] MSDN, Authorization Data types. Security Descriptor Control, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secauthz/security/security_information.asp

[11] RFC 1509 - Generic Security Service API : C-bindings, J. Wray, Digital Equipment Corporation, September 1993

[12] Directories, Meta-Directories and Virtual Directories, OctetString, Inc., 2002

[13] A theory for Systems Security, Kan Zhang, Cambridge University, Computer Laboratory.

[14] A Framework for Reasoning about Assurance, Jeffrey Williams, Arca Systems Inc., November 30, 1995

[15] A taste of computer security, Amit Singh, 2004 http://ils.unc.edu/~brunkb/inls187/papers/A_Taste_of_Computer_Security.pdf#search='secure%20time%20insecure%20time'

[16] An example is here: http://www.netpulse-nms.com/includes/pages/library/brochures/eNMSbrochure.pdf#search='lifeblood%20of%20the%20enterprise'

[17] The high cost of not finding information, IDC white papers, Susan Feldman, Chris Sherman, July 2001

[18] Modern business challenges – Compliance and Total Security Confidence, Stuart Wilson and Chris Ayres, Pirean Ltd. 2005. And: ITIL Security Management, Carlos Trigoso, Pirean Ltd. 2005

[19] Distinguishing Security Engineering Process Areas by Maturity Levels, Karen Ferraiolo, Joel Sachs, Arca Corporation, 1996

[20] An Enterprise Assurance Framework, Douglas J. Landoll , Jeffrey R. Williams 1996

[21] Perimeter Defense Model for Security, Adam Lipson, EVP Client Services, Product Development, Vigilinx

[22] The log management industry, SANS analyst program, Stephen Northcutt, Jerry Shenk, April 2004

[23] RFC 3881 Internet RFC/STD/FYI/BCP Archives, Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications, G. Marshall, Siemens, September 2004

[24] Ensuring Security and Compliance through Enterprise Log Data Management, SenSage Corp, 2004