Information Security Best Practice Dissemination: The ISA-EUNET Approach*

Diomidis Spinellis and Dimitris Gritzalis
Department of Information & Communication Systems
University of the Aegean
dspin@aegean.gr

Department of Informatics
Athens University of Economics & Business
dgrit@aueb.gr

Key words: Information Systems Security; SME dissemination activities; World Wide Web.

Abstract: The rising deployment of mission-critical systems over public data networks is prompting enterprises of all types and sizes to re-examine their approach towards the security of their information technology systems. We present ISA-EUNET, an integrated approach comprising security technology awareness, support, education, training, and dissemination aiming towards the diffusion of security and safety know-how to SMEs. The main technological drivers behind the SMEs' need for education are information system risk analysis, development of secure software systems, and provision and utilisation of Trusted Third Party services. The provided education and training is based on a phased approach, a set the security project selection

* In Simone Fisher-Hübner and Louise Yngström, editors, *WISE 1: First World Conference on Information Security Education*, pages 111-136, Kista, Sweden, June 1999. IFIP TC11 WG 11.8.

criteria, and an innovative decentralised, yet identity-preserving, structure. An important part of the ISA-EUNET approach is security information dissemination throught a Web-based Technological Knowledge Office database.

1. INTRODUCTION

The rapidly increasing adoption of Internet-based solutions for disseminating corporate information, conducting electronic commerce, teleworking, implementing virtual private networks, and setting up extranets is prompting enterprises of all types and sizes to re-examine their approach towards the security of their information technology (IT) systems. Through the adoption of multimedia email, Java and Javascript Web applets, and Internet-connected corporate networks modern IT systems are becoming vulnerable to a wide variety of threats affecting the availability, integrity, and confidentiality of the information they handle.

In front of these changes, the European SMEs face a big challenge and, at the same time, demonstrate specific points of cultural weaknesses. The majority of the European SMEs do not have a clear operational and cultural approach to the problems generated by “security hidden requests”, legal constraints, new regulations and directives; moreover they have limited time to study and test the new methods, ongoing research, and tools necessary to give a correct answer to the deployment of secure software systems. On the other hand, SMEs must remain competitive if they want to survive in the new world-wide scenario. which will become larger and larger (from the business point of view) in consideration of the new opportunities generated by the new expanding area of Internet-based electronic commerce applications. All European SMEs developing or depending on secure IT systems have in common the need for personalised and direct support in order to solve concretely and successfully the practical problems they face in their day-by-day operations. This includes education and hands-on direct training on consolidated European Best Practices and local support and tutoring on a wider set of subjects related to the solution of their practical problems on security issues.

This paper presents an integrated approach comprising security technology awareness, support, education, training, and dissemination aiming towards the diffusion of security and safety know-how to SMEs. The remainder of this paper is structured as follows: Section 2 introduces the ISA-EUNET approach and its objectives, its context within EU-funded research activities, the project's goals, and its strategy; Section 3 details the main technological drivers behind the SMEs' need for education, namely

information system risk analysis, development of secure software systems, and provision and utilisation of Trusted Third Party services; Section 4 describes a phased approach for providing security-related consulting services to SMEs, the security project selection criteria, and the key elements of the ISA-EUNET structure; Section 5 describes the schema, design, and implementation of the project's Technological Knowledge Office database, while Section 6 concludes the paper with a summary of the project's main achievements.

2. THE ISA-EUNET APPROACH

ISA-EUNET aims towards the establishment of a high-technology software European lean network of experts in security and safety applications to directly support SMEs at a regional level. The specific objectives of our approach are: to raise awareness of SMEs on the different aspects of software intensive systems for security and safety applications, to support the same SMEs with proper training on European software best practices, methods and tools, to provide on-site tutoring, to promote the circulation of “validated” information in the specific technological areas, to improve the effectiveness of European SMEs business operation and, finally, to create a new market niche for the security and safety technology operators.

ISA-EUNET is part of the ESSI-2 Software Best Practice initiative within the framework of the specific research and technological development programme in the field of Information Technologies. The aims of ESSI are to promote best practice and thereby improve the software development process in industry, through the take-up of well founded and established but insufficiently deployed technological support, so as to achieve greater efficiency, higher quality, and greater economy. This is to be accomplished by applying state-of-the-art software engineering techniques in a wide range of industries, taking into account moving targets and changing cultures in this rapidly evolving area. The full impact for Europe is to be achieved through a multiplier effect, with the dissemination of results across national borders and across industrial sectors. And guiding aspect for ISA-EUNET and at the same time an important part for ESSI are the Pro-Active Software Best Practice Networks (ESBNETs). These aim towards the establishment of European networks of organisations managing locally a set of closely related software best practice activities including hands-on activities — like the performance of small scale PIEs, assessments, improvement plans, etc. — information brokerage, experience exchange networks, demonstration sites, executive industrial visits or other schemes particularly tailored to meet the needs of the SMEs. The ISA-EUNET approach evolved as a result of ISA-EUNET: an

ESPRIT ESSI-funded project. The composition of the ISA-EUNET consortium is outlined in Appendix A.

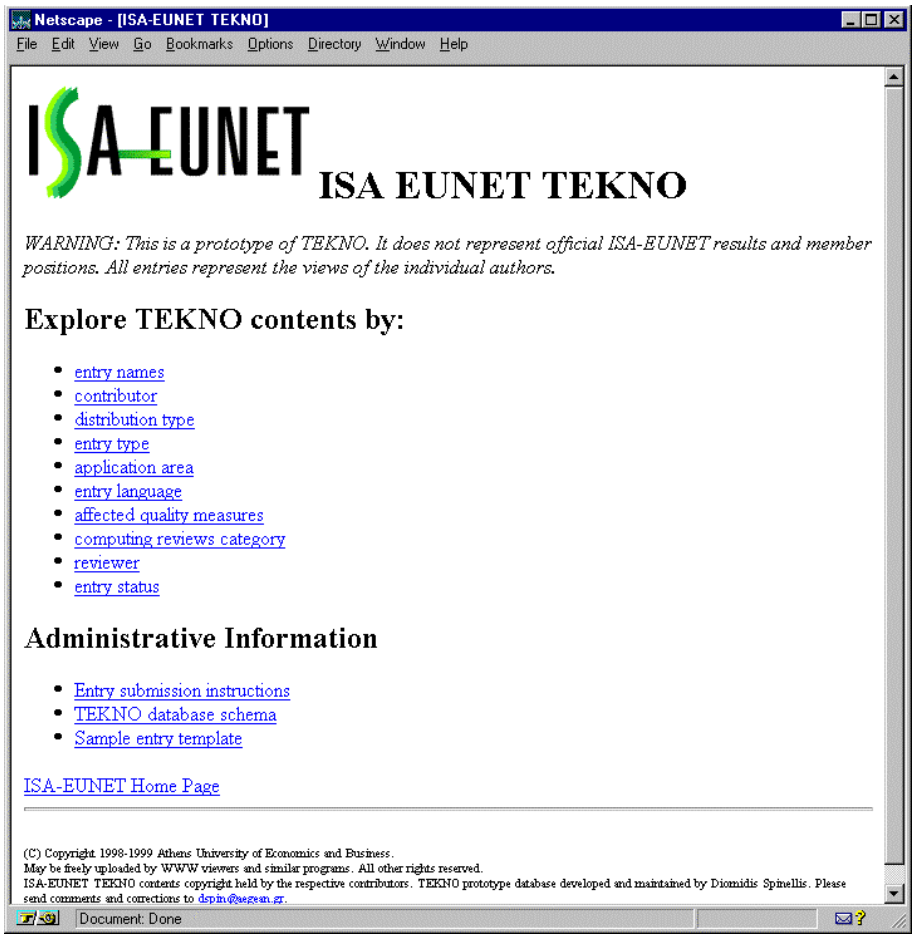

Figure 1. The TEKNO main page

The ISA-EUNET Consortium uses its scientific, technical and market competencies at different levels to reach the goals described. All partners (including the co-ordinator) implement specific direct actions towards SMEs at the regional level according to the ISA-EUNET Work Plan, take part in the central supporting activity of the TEchnical KNowledge Office ("TEKNO" — illustrated in Figure 1 and described in Section 5), and activate links with national ESPINODES. The ISA-EUNET co-ordinator performs the linking activity, (links with ESBNETS, international Partners, other Academic Institutions and Research Centres) focusing and monitoring the overall efforts

of Partners, maintaining the identity and the consistency of the Consortium, while stimulating actions to promote business results in the medium term time-frame. Finally, subcontractors are used only marginally and only to cover either new specific high-technology issues (with niche activities to be done by SMEs) or to support the telematic applications on the World Wide Web.

The strategy of the ISA-EUNET approach is based on three main elements: TEKNO, the regional nets of direct links between the Partners and the local SMEs, and the strong proactive co-ordination.

- TEKNO is a central cultural kernel of scientific and technical competencies of the partners which puts together the best of European experiences and research in software intensive systems for security and safety applications technological areas and Software Best Practices, including Quality and Software Development Process Management. This kernel is the heart and the brain of the Consortium and guarantees for all the practical actions of the project stakeholders:
  - the respect of a scientific approach and the validation of the information which circulates inside the informatic nets and the person-to-person nets of ISA-EUNET,
  - the correctness of the technical solutions and methods proposed to SMEs,
  - the uniformity of the training (methodology and contents) proposed to the target SMEs, and
  - the consistency of the internal evaluation criteria for the specific (short and medium term) initiatives of partners.

- At the regional level the single Partners have the responsibility of dealing with their target SMEs giving them the necessary direct support, training, and tutoring. Seminars, conferences, visits and workshops are organised at regional level. Each partner has the possibility of choosing one or two Target Enterprises with which he will test the more crucial aspects of methodologies and implement the first SBP applications.
- Finally, the co-ordinator organises the global European events with the support of partners, plans the meetings of TEKNO delegates, maintains the consistency of the Consortium and forces the respect of the contractual conditions. The co-ordinator also develops the long term plans for the activities of partners after the completion of the project.

3. TECHNOLOGICAL DRIVERS

An important part of the ISA-EUNET approach concerns the characterisation and analysis of the emerging business context formed by the deployment of large integrated digital infrastructures and embedded software systems, and the technological, legal, societal, and cultural drivers behind the SMEs needs.

A study performed in the Greek IT market through interviews with selected target SMEs aimed towards identifying SME security-related needs. We expect similar trends to be prevalent throughout Europe. The Greek IT industry [Vei98] is undergoing a very promising transition. A number of players in the channel have advantageously positioned themselves to make the most of joining the EMU with software development being quite mature. There are exports in the Balkans area. Most software development companies are focused on the SME market providing packaged products and custom-developed solutions. There are around 200 mature software development companies.

An important market characteristic is the large participation of the public sector creating around 30% of the demand. Software is also needed by the private industry, especially shipping, banking (which is currently in a consolidation and restructuring phase), and financial institutions. As manufacturing is decreasing a lot of demand is coming from the service sectors. A problem, identified by the study, that influences ISA-EUNET directions is the perceived shortage of skilled staff.

Software products are currently undergoing a transition moving from stand-alone platforms to networked client-server architectures. With the rapidly improving Greek Wide Area Network (WAN) infrastructure, the opening of the telecom market for data, and the emergence of a number of reliable Internet Service Providers, large companies, the government, but also SMEs are increasingly networking geographically dispersed offices and using software over public networks. The increasing use of the Internet and the World Wide Web in particular, have also contributed to this trend. Activities related to electronic commerce and EDI are on the ascend fuelled by European Union funded R&TD projects.

The Greek government is also creating demand through the KLISTHENES project aiming in the further utilisation of IT in the public sector. Important parts of the project currently under-way include the integrated system for tax revenue management (TAXIS project, one of the biggest projects in Europe, with a 500 million ECU's budget) and the introduction of IT in the public health-insurance, pension, and health-care systems.

The recent establishment of an independent authority (National Data Protection Board) to enforce the Greek Law 2472/97 for the protection of individuals from the processing of personal data is expected to severely influence the security requirements of those projects.

All these market trends are fuelling demand for secure information systems. Such systems have to be reliable and secure following a rigorous risk analysis. For many activities occurring over public data networks trusted third party (TTP) services providing public-key certificates will be required. These identified specific needs are expanded in the following sections. In summary, the three main security-related technological drivers that emerged during the analysis phase, are:

– information system risk analysis,
– development of secure software systems, and
– provision and utilisation of Trusted Third Party services.

3.1 Information System Risk Analysis

An enterprise cannot reasonably develop efficient security policies and procedures without clearly understanding the systems that must be protected, as well as how valuable they are to the enterprise. In addition, one must determine the probability that the assets will be threatened. Therefore, the objective of a risk analysis review is to identify and assess the risks to which the IS and its assets are exposed in order to select appropriate and justified security safeguards [Com93].

The analysis of risks is performed in four stages [ELB93,WK96]:

1. asset identification and valuation,
2. threat identification and assessment,
3. vulnerability assessment, and
4. risk assessment.

Assets are the elements of an IS that possess a value. A security incident that will affect an asset will also have an impact on the owner of the asset (i.e. the organisation, the enterprise or the individual). Assets are valuated according to the impact of a probable asset impairment. Threats need to exploit a certain vulnerability in order to cause a security incident. Therefore, threats, vulnerabilities, and impacts should be combined together to provide a measure of the risk an IS is exposed to.

3.2 Development of Secure Software Systems

A result of an initial study on security-related SME software development was that SME software development organisations were mainly developing

client-server systems [Sin92,DCS98] with Web-based systems an emerging new activity. SMEs need to be educated on the aspects of Secure Software System Development outlined in the following paragraphs [FNS91]. As client-server information flows through a corporate or public network environment, in any instant, it can be in one of the below states [Pfl96]:

Storage: data that is in either in volatile memory or in permanent storage, on either the client an intermediate proxy, or the server computer system.

Processing: operations performed on data by the client or the server computer system.

Transmission: the process of conveying data through a certain medium, part of a LAN or a WAN.

In each of these certain states, the potential threat agents may be [MSB95]:

Malicious authorised users: users who are definitely authorised to access some information may do an illicit action, behaving as an intruder, in order to access or to modify information in an unauthorised manner.

Negligent authorised users: users who are definitely authorised to access some information may accidentally do something resulting in the modification of that information or disclosing it to another user who is not unauthorised.

Outsiders: users who are not authorised to access or modify some information, acting as intruders, may attempt to achieve that specific goal.

An important part of creating a secure and safe environment for a program to run is facing the potential threats inherent in distributed client-server and Web technology [GS97] which may be exploited by any of the threat agents mentioned above.

The main threats can be classified with respect to the potential result as [MSB95]:

- **disclosure**: loss of confidentiality and privacy,
- **modification**: loss of integrity,
- **fabrication**: loss of authenticity, and
- **repudiation**: loss of attribution.

Accordingly, the way these specific threats can apply to data on clients, in transit, and on servers are presented.

3.2.1 Disclosure: loss of confidentiality and privacy

For data on servers a threat agent may exploit inadequate access control, programming errors, or use impersonation. Legitimate users may disclose data to third parties who have not this right. This threat applies particularly to private corporate data distributed on an Intranet. Data in transit can be observed via wiretapping, misrouting, or accessing server and proxy logs and

cache structures. Unprotected networks and applications are vulnerable to all threat agents, but protected ones are only exposed to vulnerabilities by authorised agents. Data on clients is vulnerable to disclosure when residing on an insecure operating system, or when executing Web-obtained software. Client masquerading may also be used to cause disclosure.

3.2.2 Modification: loss of integrity

Weaknesses on servers or the operating system they reside on can (and have been) exploited to cause server data modification. Wiretapping may also be used to modify or destroy data packets in transit. In addition, data on clients is vulnerable to modification when executing Web-obtained software.

3.2.3 Fabrication: loss of authenticity

Threat agents may create masquerade servers or documents on a server. For data in transit a threat agent may falsify the source of information (server or individual). A threat agent may also falsify the user or host identity presented to the server.

3.2.4 Repudiation: loss of attribution

Users sending information to a server may repudiate their actions and document authors may falsely claim not to be the document's true author. The first threat is particularly relevant to Web-based transactions used e.g. for on-line shopping, while the second one applies to the distribution of illegitimate content.

The ISA-EUNET approach is using the outlined threat model as a basis for characterising SME needs, and documenting the information disseminated to them.

3.3 Provision and Utilisation of Trusted Third Party Services

A new emerging business environment is expected, especially with Electronic Commerce poised for rapid growth, a vast number of potential opportunities are unfolding. It is estimated that there were 75 million Internet users at the end of 1998. Internet shopping is becoming a reality with sizeable initial projects backed by major national and international corporations (e.g. Visa and MasterCard). The largest Internet retailer, *amazon.com* now has over one million customers. It follows that Internet security is becoming increasingly important [Bhi96]. Banking has been made available to the

general public with the advent of the worlds first “Internet only” bank Security First Network Bank. All banks are now looking at how they can utilise the Internet to offer a new delivery channel to their customers and many have started pilot projects.

Up to now the view of security was relatively confined but a new definition is emerging. This is centred around the use of Public and Private keys to allow authentication and digital signing. In most countries around the world projects have started to offer certification (which is a means of publishing a person's public key for authentication use in e-commerce).

The main target groups of certification and digital signature services could be the following:

– Individuals who need to exchange in a secure way email and documents over Internet.
– Retailers who need to set-up a commercial Web storefront that could be certified digitally by a trusted organisation in the Greek environment. This certification will enhance their credibility on selling products or services over the Web especially to customers located in the Greek region.
– Wholesalers who need to support or carry out on-line orders in a secure way over electronic networks.
– Companies with branches distributed across a territory wishing to exchange sensitive data (e.g. financial documents, marketing data) over open networks.
– Service providers who need to offer their customers the ability to pay electronically their bills check statements indicating service usage etc.
– Banks that wish to offer to their customers (individuals or businesses) secure banking services via Internet.
– Medical institutions and members of the medical profession who want to securely store and exchange patient information [KSIB98].

Software development SMEs have to cater to the needs of all the categories listed above. They therefore need expert guidance for providing and deploying the necessary products and services.

4. TECHNIQUES AND TOOLS

An important part of the ISA-EUNET strategy is the establishment of a common initial approach to target SMEs. At the local level the Target Enterprises need direct and personalised support to be motivated to fill the cultural gap which may generate weakness in a global competitive scenario. The objective of ISA-EUNET was to prepare plans of actions for Partners in order to give timely and effective support to the target SMEs. We therefore

decided to define and standardise some common protocols which should permit us to have a common approach to SMEs needs, independently of the national diversities. In order to establish this protocol it was important to take into account the information dissemination strategies that can be applied across all SMEs. We therefore proposed a staged approach towards the target SMEs together with detailed project evaluation criteria for selecting viable SMEs and projects. As the ISA-EUNET project is financed by the European Commission some of the practical support and tutoring/mentoring provided to the SMEs are to be performed without charging the full cost to the respective SME.

4.1 Security Consulting SME Approach Strategies

We proposed a staged approach towards each individual SME. For each stage, we describe the respective actions from an ISA-EUNET member and the target SME.

Table 1. SME Contact Approach

Stage	Activity	Objective
1	Distribution of general ISA-EUNET information to existing contacts (via phone calls, post, email)	Create awareness, get companies/customers interested
2	Direct contact with selected companies (based on reactions in telephone conversations, reactions to email, etc.)	Introduce SIS SA services and strive at getting company visits accepted
3	Company visits (discussing problems/needs of companies, presentations on SIS SA services)	Define a mini/micro-PIE
4	Carry out mini/micro-PIE (6-8 days, intensive collaboration and discussions with target enterprise)	Get results from the mini/micro PIE
5	Organise plenary/public meetings to present results (towards other existing contacts)	Attract companies/customers and set up new experiments (and subsequently continue with Stage 2)

4.1.1 Stage 1: Initial Contact

At the initial stage the target SME may be unaware of any specific security education needs. The initial approach to target SMEs has to be specified formally so that it can be applied by each partner in the same structured and uniform way. The initial approach described here is based on experiences in the first four months of the ISA-EUNET project (July to October 1998). The experiences are derived from company visits, telephone

communication, and presentations at public seminars. The explicit philosophy behind the initial approach, that is described below, is that step by step confidence has to be gained from SMEs, which are preferably existing contacts. In the first step a restricted amount of existing contacts are used to create initial awareness and interest, subsequently a selected set of companies will be contacted directly to make appointments for carrying out experiments. As such a kind of centre-out approach is followed: first getting (at least) one company interested to do a micro-PIE, subsequently using the experiences to do public presentations to convince other companies and to carry out new experiments. The initial approach consists of the five phases outlined in Table 1.

4.1.2 Stage 2: Requirement Analysis

The target SME will try to shift the partner's work towards solving its specific problems (e.g. a specific intrusion threat or a runaway project). The goal of the ISA-EUNET partner will be to shift the — possibly vague — target SME requirements towards the partner's specific capability (e.g. consulting on TTP implementation).

4.1.3 Stage 3: Proposal Drafting

A target SME will typical respond to a successful requirement analysis with questions directed towards establishing the feasibility of a specific product. The SME's managers will prepare a cost-benefit analysis and an internal proposal to obtain the budget needed. The ISA-EUNET partner will provide the target SME with background information (e.g. cost estimates, case studies, technical articles) to help its staff draft the internal proposal. This stage presents a perfect opportunity for establishing a close and friendly working relationship based on mutual trust between the employees of the SME and the ISA-EUNET partner. This relationship will be an important asset during the following stages.

4.1.4 Stage 4: Project Finalisation

At this stage the target SME, having secured the internal approval for budget, will try to identify possible bidders and write a request for proposal. In order to win this proposal the ISA-EUNET partner will have to discuss as early as possible the related terms and conditions and discover the basis on which the bids will be judged, as well as the available budget. The contacts established at the previous stages will prove valuable at this point.

4.1.5 Stage 5: Request for Quotation

The target SME will publish a formal request for quotation which has to be studied by the ISA-EUNET partner in order to prepare a proposal and a quotation. At this stage the ISA-EUNET partner will have to determine whether the target SME is a suitable customer candidate. Following a positive decision, the ISA-EUNET partner should stress its specific strengths, track record, emphasise the access to the common pool of ISA-EUNET knowledge and the TEKNO database, and provide a quotation consistent with the SME's available budget and the prevailing market condition. For security reasons the proposals would be submitted close to the tender closing time.

4.1.6 Stage 6: Fine Tuning

A successful proposal will result in the ISA-EUNET partner being selected for a short-list of prospective suppliers. The SME will ask for the best and final offers from the favoured suppliers. The ISA-EUNET partner must, at this stage, fine tune the bid and adjust the price (upwards or downwards) depending on its knowledge of other contenders. It is important to keep in mind that ISA-EUNET offers an exclusive pool of specialised knowledge which should not be downmarketed.

4.1.7 Stage 7: Contract Negotiation

At this stage the ISA-EUNET partner and the SME will negotiate the final contract. The negotiation includes the detailed schedule of the consulting provided, the price, access to the SME material, rights to use and publish results, and other terms and conditions. The goal at this stage is to close the deal.

4.1.8 Stage 8: Contract Execution

After the contract starts, the ISA-EUNET partner must inform the target SME of the progress using suitable reports as well as any unavoidable changes in the established plan. The ISA-EUNET partner should also monitor the SME's use of the provided services and provide assistance so that results will match the initial expectations. Contract extensions and further work will be provided to the ISA-EUNET partner only if the target SME sees concrete value being delivered during the contract execution.

4.1.9 Stage 9: Further Work

Inevitably, once an initial working relationship has been established, the ISA-EUNET partner should start discussing the SME's future security-related requirements and develop the required capability — possibly in co-ordination with other ISA-EUNET members — to meet those future needs.

4.2 Security Consulting Project Selection Criteria

As discussed in the previous section, when a request for quotation is received from the SME the ISA-EUNET partner will have to decide whether the nature of the work fits with its capabilities, short and long term strategic goals, work schedule, staff levels, and work load. The following criteria should be used when selecting projects:

- How closely are the SME's security needs aligned with the ISA-EUNET member's business strategy?
- How closely are the SME's needs aligned with the strengths of the ISA-EUNET Consortium?
- How serious is the SME for improving its processes using outside help?
- What are the security-related technical risks, and their cost and legal implications?
- What are the commercial risks? Is the target SME financially secure?
- What is the value of the potential contract?
- What is the value of follow-on opportunities? IS the SME deploying or merely using Information System Security infrastructure?
- What is the ISA-EUNET partner's probability of winning?
- How profitable is the deal likely to be? How can the cash flow be funded?
- What is the cost to prepare the bid? How will the bid preparation affect existing work?
- How can other ISA-EUNET partners help and take part in the bid?
- What effect would winning a contract with the specific SME have on the ISA-EUNET member's other work?

ISA-EUNET Consortium uses the best of its scientific, technical and market competencies at different levels to reach the final goals of the project. All partners (including co-ordinator) do implement specific direct actions towards SMEs at regional level according to the Work Plan, and take part in the activities of the TEKNO structure. The co-ordinator performs the linking activity, stimulating, focusing and monitoring the overall efforts of the partners, maintaining the identity and the consistency of the Consortium. The subcontractors are used only to cover either new specific high-tech issues, or to work on specific tasks for Web implementations.

Three key elements are used by the Consortium for performing the proposed set of operations and activities:

1. the technical knowledge office structure,
2. the established net of relationships (deriving from the previous EU initiatives), and
3. the strong proactive co-ordination of Partners' actions.

4.3 Technical Knowledge Office

In this age of information overload, finding the right information can be a challenge for SMEs, and trusting it often requires a leap of faith because we cannot be sure where it came from or which is its practical value. To help operators of ISA-EUNET to share information and SMEs to use it without fear, we have realised a TEchnical KNowledge Office (TEKNO) which is a lean, flexible, virtual structure designed to disseminate information of the ISA-EUNET internal network. TEKNO searches, generates, links, organises, updates and presents information that ISA-EUNET Partners use most often about methodologies, research, and tools applicable to software intensive systems for security and safety applications. The team working on this TEKNO task is a virtual team built with the contribution of key people working part-time in the different European regions of ISA-EUNET, and linked person to person via the Internet plus some group meetings (usually via teleconferences, Internet chat, etc. and sometimes with real physical meetings of the interested people in occasions of seminars and other main events with SMEs). In addition to this validation activity, the TEKNO proposes and develops medium term strategic plans for driving correctly and consistently the overall actions of the Consortium with the important by-product of promoting possible self-sustained activities (that is a set of activities acceptable and paid for by SMEs) towards the regional SMEs in the future, after the completion of the ISA-EUNET project.

4.4 The Regional Network

At a regional level the ISA-EUNET partners can work with SMEs using a large set of technical, training and business relationships which were set up in the last years in connection with direct deals and some EU funded actions (which include DG III ESPRIT “SCOPE”, DG II ESSI “ESSI-SCOPE” and “ENCRESS”, etc.). Starting from these initial informal relationships between partners and with local SMEs, an unstructured network was generated. During 1996-97 there was a first effort, at regional level only, to give to the now available network a partial formal structure. The network nowadays exists and it is deployed in all the countries covered by ISA-EUNET (and in

many others including France, Norway and Portugal) and consists of several regional nodes each with a number of operational links with local SMEs and institutions (15 to 35); this network is used, with some low cost but very important telematic and procedural improvements, as a key tool for achieving ISA-EUNET goals.

4.5 Strong Central Proactive Co-ordination of the Consortium

The third element of the of the Consortium's strategy is an innovative approach to the co-ordination of partners which opens an new dimension of economical relevance for the future of the Consortium. Proactive co-ordination means the promotion of the partners' level of freedom and, at the same time, the protection of Consortium identity. The two concepts are not in contrast and their implementation has been properly balanced by the co-ordinator partners appointing as Director of ISA-EUNET an executive manager with international experience in large EU funded and industrial multinational projects, for achieving the Consortium goals.

Due to the pace of security-related technological advances, partners are absolutely free to take any decision under their responsibility (with reference to their contractual and budget commitments); to implement this concept the first task of the Director is to increase the level of freedom for the specific partner promoting new local initiatives and mainly removing the “not-yet-known” barriers in the area of security-related software. The speed of circulation of ideas and applicative information available in the internal network is the mechanism which is used to permit the growth of innovative ideas and solutions for SMEs, in the action of partners. The speed of circulation of information is of vital importance and the co-ordinator also takes care of implementing low cost telematic links permitting the achievement of this goal, which break the limits of regional industrial culture producing benefits both for Partners and for SMEs.

The second aspect of the proactive action of the Director consists in the day-by-day monitoring action necessary to maintain the identity of ISA-EUNET Consortium (focused on the key common issues of its mission) and in a scout activity addressed to identify among partners and SMEs, any new opportunity of synergism from different academic areas and IT and non IT industrial sectors (energy and process industries, medical equipment, robotics, avionics, aerospace, telecom. etc.) to thus promote cross-fertilisation actions with direct benefits to innovative local SMEs.

As the implementation of these two concepts is adequately balanced there is a good chance that the ISA-EUNET Consortium will be successful because

it is now possible to take advantage from the experience of partners already used to work in large teams with severe and ambitious objectives. In a time frame of three to five years, the success of the proposed project will give origin to other security-related high-technology business operations for SMEs (home safety applications, mass market and extensively deployed products embedding security-related IT, etc.). For these enterprises the presence of a strong technical-managerial co-ordination body maintains in their future common operations the initial benefits of ESBNET.

5. THE SECURITY TECHNICAL KNOWLEDGE OFFICE

As outlined in the previous section a key element of ISA-EUNET is the Technical Knowledge Office which is used to co-ordinate the dissemination of security-related information to SMEs. The TEKNO database is based on a relational structure and is used to organise and categorise entries making them thus accessible to other members of ISA-EUNET and target SMEs. The structure is based on a set of orthogonal TEKNO entry dimensions which are common across all entries. As entries are added to the TEKNO database the structure will ultimately evolve towards the final database schema.

Every TEKNO entry is described using the following index categories:

Entry name The entry name is a descriptive name uniquely identifying the entry.

Contributor The contributor index entry identifies the contributing organisation.

Distribution type The distribution type determines the entry's allowed distribution. It can be one of:

Public: available to all.

User group: available to members of the ISA-EUNET user group.

ISA-EUNET: available only to members of the ISA-EUNET Consortium.

Entry status The entry status identifies the entry's maturity. It can be one of:

- draft,
- under review, and
- ISA-Eunet approved.

Entry type The entry type can be one of:

Technical article giving an overview of a certain topic (e.g. Information System Risk Analysis, Software use in nuclear industry).

Standards and legislation summaries of relevant standards and European directives (e.g. IEC 61508, EN 50126, the EC Machinery Directive).

Case study description of real cases

Methodology description of methodologies which are useful when developing security and safety-related systems (e.g. fault tree analysis, risk analysis, how to perform a software inspection, configuration control).

Tool used to apply a given methodology e.g. CRAMM [CRA96].

Trainig course and seminar invitations to ISA-EUNET events and proceedings from those events (e.g. an invitation to a technical seminar in Munich, copies of PowerPoint slides used at awareness seminars in Sweden).

Administrative information related to the operation and administration of TEKNO and ISA-EUNET.

Application area The application area where the specific entry can be applied. If the entry is application-area-neutral the characterisation "*all*" is specified. Examples:

– Digital large-scale infrastructures
  a) Telecommunications
  b) Financial
  c) Public administration
  d) Health care

– Embedded systems
  a) Automotive
  b) Avionics
  c) Railway
  d) Traffic management
  e) Process control
  f) Medical devices
  g) Nuclear power
  h) Smartcards
  i) Consumer electronics

Entry language The ISO-639 [ISO88] language code and common name for the entry's language.

Affected quality measures The application quality measures affected by the entry, following the CMU SEI STR Technology Descriptions taxonomies

[Car98]. Figure 2 illustrates the taxonomies' root, while Figure 3 the security-related trustworthiness taxonomy.

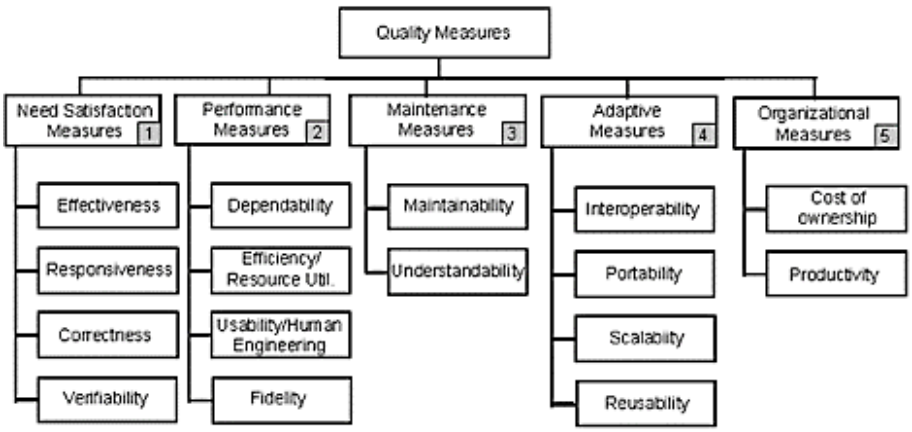

Figure 2. The root of the CMU-SEI Software Technology Review technology description taxonomy [Car98]

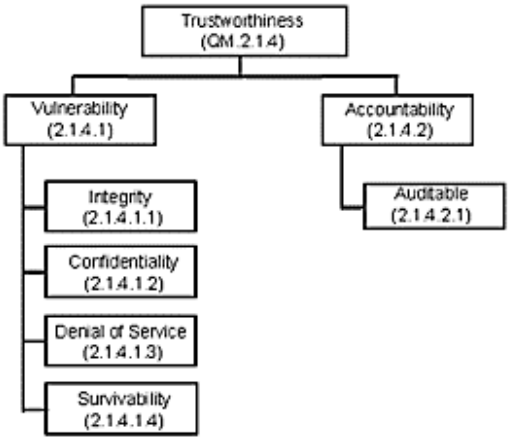

Figure 3. The CMU-SEI Software Technology Review trustworthiness taxonomy [Car98]

Computing reviews category The classification of the area following the ACM Computing Classification System [Ass98].

Other relevant TEKNO items This entry contains list of other relevant TEKNO items with links to their respective entries.

Entry link The entry link is a hypertext URL [BLMM94] link to the entry material.

Reviewer The reviewer entry contains — where applicable — the name of the entry's reviewer(s).

Currently a prototype of TEKNO has been implemented in order to verify the viability of the database schema, the user interface, and the population dynamics. It is based on a set of dynamically constructed Web pages based on specific templates the entry descriptions. All entries of TEKNO are described using a simple text format like the one presented in Table 2.

Table 2. Sample TEKNO database entry

Entry name: Intrusion Detection
Contributor: Athens University of Economics and Business
Distribution type: ISA-EUNET
Entry status: Under review
Entry type: Training material
Application area: Digital large-scale infrastructures
Entry language: EN - English
Affected quality measures: QM.2.1.4 - Trustworthiness
Computing reviews category: D.4.6 - Security and Protection
Other relevant TEKNO items: None
Entry link: http://www.math.aegean.gr/info-sec/projects/deliverables/isa/intr_det/index.htm
Reviewer: Sokratis Katsikas

A program written in Perl [WS90] goes through all entry descriptions and creates HTML [BLC95] pages presenting a rich cross-indexed structure based on all entry characterisation dimensions. A set of cross-linked associative arrays is used to maintain and expose the free and evolving relational schema of the database without restricting the entry authors to use a fixed set of entry characterisations. The main page of this structure is illustrated in Figure 1.

A separate page is generated for each TEKNO entry, with links to other relevant entries, the descriptions of the database schema, and the main link to the material of the entry. For ISA-EUNET-restricted material a simple password scheme is used to hinder access to unauthorised entities. A sample TEKNO Web entry is illustrated in Figure 4.

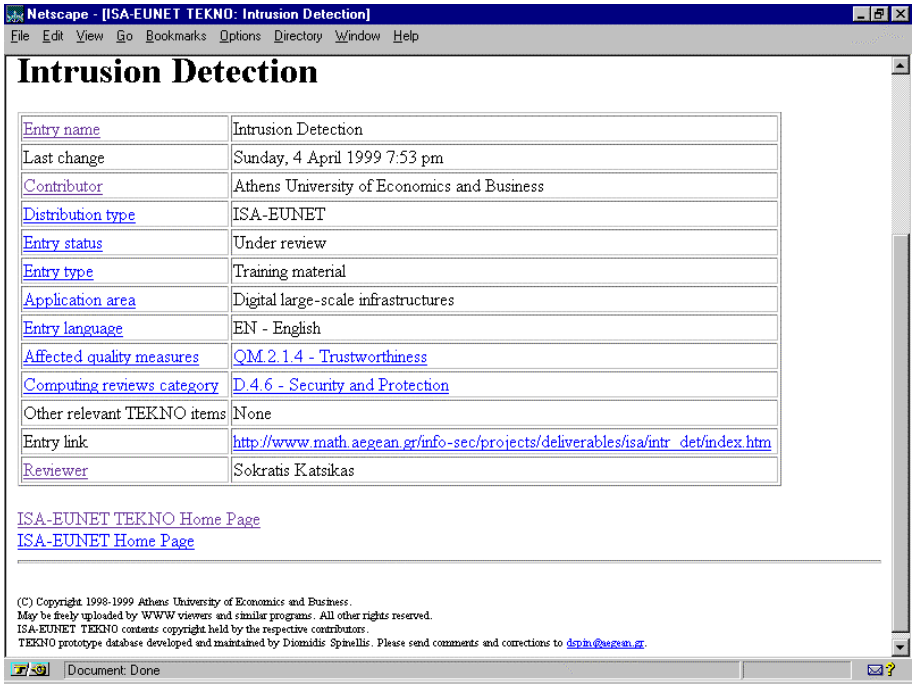

Figure 4. Sample TEKNO entry on the Web

6. CONCLUSIONS

In the previous sections we introduced the ISA-EUNET approach and its objectives, its context within EU-funded research activities, the approach's goals, and its strategy; detailed the main technological drivers behind the SMEs' need for education, namely information system risk analysis, development of secure software systems, and provision and utilisation of Trusted Third Party services; described a phased approach for providing security-related consulting services to SMEs, the security project selection criteria, and the key elements of the ISA-EUNET structure; and outlined the schema, design, and implementation of the project's Technological Knowledge Office database. Our experience so far has been more than positive. The emergence of the Internet has created a new impetus for security technology awareness, support, training, and dissemination activities; ISA-EUNET is currently “riding the wave” of corporate security education a fact which is evident from the attendance of seminars, courses, and other relevant activities. In the following months the completion and deployment of the operational TEKNO will result in additional exposure and, we hope, in subsequent multiplier effects on the visibility of the ISA-EUNET goals and activities.

ACKNOWLEDGEMENTS

The work reported herein was carried out within the context of ISA-EUNET, an ESPRIT (ESSI-ESBNET, project number 27450) R&D project funded by the Directorate General III of the European Commission.

REFERENCES

[Ass98] Association for Computing Machinery. The ACM computing classification system (1998). Online. http://www.acm.org/class/1998/ccs98.html, January 1999, 1998.

[Bhi96] Anish Bhinami. Securing the commercial internet. *Communications of the ACM*, 39(6):29–35, June 1996.

[BLC95] T. Berners-Lee and D. Connolly. RFC 1866: Hypertext Markup Language — 2.0, November 1995.

[BLMM94] T. Berners-Lee, L. Masinter, and M. McCahill. RFC 1738: Uniform Resource Locators (URL), December 1994.

[Car98] Carnegie Mellon University, Software Engineering Institute. Software technology review. quality measures taxonomy. Online. http://www.sei.cmu.edu/str/taxonomies/view-qm.html, December 1998, 1998.

[Com93] Commission of the European Communities. Risk analysis methods database. DGXIII, INFOSEC Programme/S2014, 1993.

[CRA96] United Kingdom Central Computer and Telecommunication Agency, United Kingdom. *CCTA Risk Analysis and Management Method: User Manual.*, version 3.0 edition, 1996. HMSO.

[DCS98] Peter Duchessi and InduShobha Chengalur-Smith. Client/server benefits, problems, best practices. *Communications of the ACM*, 41(5):87–94, May 1998.

[ELB93] J. H. P. Eloff, L. Labuschagne, and K. P. Badenhorst. A comparative framework for risk analysis methods. *Computers and Security*, 12(6):597–603, 1993.

[FNS91] Claus Fritzner, Leif Nilsen, and Asmund Skomedal. Protecting security information in distributed systems. In *1991 IEEE Symposium on Security and Privacy*, pages 245–254. IEEE Computer Society Press, 1991.

[GS97] Simson Garfinkel and Gene Spafford. *Web Security and Commerce*. O'Reilly and Associates, Sebastopol, CA, USA, 1997.

[ISO88] International Organization for Standardization, Geneva, Switzerland. *Code for the Representation of Names of Languages*, 1988. First edition, 1988-04-01. Reference number: ISO 639:1988 (E/F).

[KSIB98] Sokratis Katsikas, Diomidis Spinellis, John Iliadis, and Bernd Blobel. Using trusted third parties for secure telemedical applications over the WWW: The EUROMED-ETS approach. *International Journal of Medical Informatics*, 49(1):59–68, March 1998.

[MSB95] Kraig Meyer, Stuart Schaeffer, and Dixie Baker. Addressing threats in World Wide Web technology. In *11th Annual Computer Security Applications Conference*, pages 123–132. IEEE Computer Society Press, 1995.

[Pfl96] Charles Pfleeger. *Security in Computing*. Prentice-Hall, 1996.

[Sin92] Alok Sinha. Client-server computing. *Communications of the ACM*, 35(7):77–98, July 1992.

[Vei98] Fiona Veira. Analysis: Greece. *PC Europa*, 8(9):13–17, May 1998.

[WK96] Richard G. Wilsher and Helmut Kurth. Security assurance in information systems. In Sokratis K. Katsikas and Dimitris Gritzalis, editors, *Information Systems Security: Facing the information society of the 21st century*, pages 74–87. Chapman Hall, 1996.

[WS90] Larry Wall and Randal L. Schwartz. *Programming Perl*. O'Reilly and Associates, Sebastopol, CA, USA, 1990.

APPENDIX A: COMPOSITION OF THE ISA-EUNET CONSORTIUM

The ISA-EUNET project is managed by QualityLab (QLAB), a Consortium founded in 1994 and formed by four small already operating enterprises (ARTIS, MAPLE, MetriQs, Performance Research) and one medium company (SIA: Societá Italiana Avionica) in Turin, Ivrea and Milano with headquarters in Turin. The main objective of QLAB is to provide solutions, in support of the whole Software Life Cycle (from Software System Requirements Analysis to the final Software System Testing and Maintenance) and to sell consultancy services and tools both to SMEs and to large multinational European enterprises. Partners in the ISA-EUNET Consortium are:

ENEA the Italian National Agency for New Technology, Energy and the Environment; a scientific research and technology development organisation with vast, internationally recognised experience in conducting advanced research programmes and technology transfer.

ARCS the Austrian Research Centre Seibersdorf. Seibersdorf is the largest independent research organisation in Austria. It is a company with limited liability under Austrian law; approximately 50% are held by the Republic and 50% by private industry. Founded in 1956, ARCS has been engaged in project-oriented contract research and development. The experience in many years of co-operation with industry, governmental organisations and academia has made Seibersdorf a versatile partner for tackling intricate problems encountered by different branches of industry, for technology transfer and training.

DELTA Software Engineering the division within DELTA, an independent centre for advanced software technology, affiliated to the Danish Academy of Technical Sciences (ATV). DELTA has a long standing commitment to software engineering in general and specifically in the area of software best practice. DELTAs main business, as an ATV institute, is to transform knowledge and experiences from both industry and universities into products and services that can be provided to industry (e.g. as consultancy support or specialised training).

GRS the Gesellschaft für Anlagen- und Reaktorsicherheit GmbH is Germany's scientific-technical expert organisation for all issues related to nuclear safety and some sectors within non-nuclear technologies. Its task is to provide scientific results and methods and develop them further for the purpose of protecting man and environment from technical hazards and risks. The work of GRS is based in all sectors on the international state of the art. GRS holds additionally the subsidiary ISTec (Institut für Sicherheitstechnik) whose prime objective is the application of the GRS experience and competence to a wider industrial context by offering services in the field of safety applications and information technology and software development.

AUEB the Athens University of Economics and Business Department of Informatics provides instruction in Computer Science and Information Systems, while placing particular emphasis on business applications of computing. One of the prime objectives of the Department is the application of the experience gained by its staff to a wider industrial context by offering services in fields such as safety and security applications in information technology. In particular, the Department carries out application-oriented research as well as consulting on methods, tools and techniques for safety and information security in information technology. Since 1994, the department runs a two-year postgraduate programme on Information Systems, with a particular emphasis on Information Systems Security.

KEMA an international knowledge-intensive organisation, active in the fields of electric energy systems, environmental technology and management, sustainable energy and information technology. KEMA's competency extends to areas of quality control in relation to product and system certification.

SP the Swedish National Testing and Research Institute a national institute for technical evaluation, testing, metrology, research and development. SP is an EC notified body and accredited test laboratory. Assignments to industry are a major activity. This involves both testing, certification and research work. SP also provides expert advisory service to government, government authorities, and to national and international standardisation activities.

CSR the Centre for Software Reliability is a research centre within the Department of Computing Science at the University of Newcastle upon Tyne; it conducts research on how to achieve improved levels of dependability from computing systems. Current primary areas of research include software and system requirements (their representation, evolution and analysis), formal specification, dependable architectures, and socio-technical engineering issues encompassing cost and dependability trade-offs. CSR has a range of projects funded by industry, the UK government and the EU, with an annual budget of approximately 1 MECU.