TECHNICAL SCIENCES
Abbrev.: Techn. Sc., No 15(1), Y 2012

DELICATED TO THE CRISIS MANAGEMENT SOLUTION COMMUNICATION SECURITY MONITORING AND CONTROL CENTRE

Saioa Ros, Oscar López, Mikel Uriarte

NEXTEL S.A., Zamudio, Spain

K e y w o r d s: Communication Infrastructure, Risk Assessment, Security Mechanisms, Security Model, Awareness, Control.

A b s t r a c t

An emergency situation often occurs as a result of unpredictable events, and as a consequence, existing communications may either get collapsed or congested. The aim of the Communication Security Monitoring and Control Centre (CSMCC) solution proposed in SECRICOM is to provide a suitable security framework that enables the development of security service. These services give response to individuals and institutions operating in heterogeneous communication infrastructures, when responding to major incidents. In the light of this objective, a Security Model has been designed facilitating the measurement of operators' and end customers' confidence in the security of the communication infrastructure, and addressing security challenges in terms of a distributed and heterogeneous solution. The proposed Security Model has been supported by the Security Middleware Service and Framework, which is responsible for measuring, documenting and maintaining the security level of the services provided by the SECRICOM communication system.

ROZWIĄZANIE COMMUNICATION SECURITY MONITORING AND CONTROL CENTRE PRZEZNACZONE DO ZARZĄDZANIA KRYZYSOWEGO

Saioa Ros, Oscar López, Mikel Uriarte

NEXTEL S.A., Zamudio, Spain

S ł o w a k l u c z o w e: infrastruktura komunikacyjna, ocena ryzyka, mechanizmy bezpieczeństwa, model bezpieczeństwa, świadomość sytuacyjna, sterowanie.

A b s t r a k t

Sytuacje kryzysowe występują zazwyczaj w wyniku nieprzewidzianych wydarzeń, co implikuje problemy z niedostępnością lub przeciążeniem systemu łączności. Zadaniem zaproponowanego w ramach projektu SECRICOM rozwiązania Communication Security Monitoring and Control

Centre (CSMCC) jest bezpieczeństwo usług z nim związanych. Usługi te są kierowane do podmiotów obsługujących różnorodne infrastruktury telekomunikacyjne na potrzeby zarządzania kryzysowego. W tym celu opracowano model bezpieczeństwa ułatwiający pomiar bezpieczeństwa infrastruktury komunikacyjnej oraz wspierający rozwiązywanie problemów wynikających z heterogenicznych i rozproszonych rozwiązań. Zaproponowany model jest wspierany przez rozwiązanie Security Middleware Service and Framework, który jest odpowiedzialny za mierzenie, dokumentację oraz utrzymanie poziomu bezpieczeństwa usług oferowanych przez system SECRICOM.

Introduction

The aim of the communication security control centre is the design of a Security Model for the SECRICOM communication infrastructure suitable for secure and interoperable communications under crisis situation. Additionally it has been supported the development of a Security Middleware Services and Framework to measure, document and maintain the security assurance level of services based on telecommunication systems.

On the technical aspect, SECRICOM presents important research challenges for the design of information security management solutions. SECRICOM has provided a heterogeneous communication infrastructure independent from the different civil forces that participate in crisis incidents, and also a boarder cross distributed interoperable solution that allows cooperation among agencies from different countries. The communication infrastructure proposed in the project is able to be dynamically reconfigurable in terms of security settings to address diverse communication-data exchange contexts. Last but not least, SECRICOM solution has provided seamless operation for end-users, so that a user can make use of the communication infrastructure in a transparent manner to the underlying security mechanisms.

From a more pragmatic overview, the challenge of engaging with end-users has been covered, in such a way that meaningful security requirements has been defined for the communication infrastructure. The first responders and commanders are under stress and very busy while trying to handle the situation. It is not likely that they turn to different communication system than the one they are used to from day-to-day operations just because of security issues. The system is prepared to be used in daily and able to handle the emergency situation specifics. The security mechanisms and policies have been built in by default. As a result of this, SECRICOM provides secure communication services for day-to-day operations and on-site-deployable infrastructure for crisis situations in a very efficient manner.

Security Objectives

These challenges are met in the design of a Security Model suitable for secure and interoperable communications under crisis. The scope of the Security Model is based on the structure of security objectives (Information Security) that represent the principles on which an effective security has to be established.

By ensuring confidentiality any unauthorized disclosure of communications between two or more parties is prevented. By ensuring integrity data cannot be manipulated during the transmission. Indeed, integrity guarantees that the recipient of some data will realize if any alteration of the originator's message has been done. Additionally, integrity of the data includes the authentication of the user source, which guarantees that network entities are not pretenders. Lastly, by ensuring availability users are always sure that information and resources are available. Though it is not possible to completely avoid Denial-of-Service type of attacks, SECRICOM components such us network monitoring, network control, multiple bearers, policy based routing and dynamic reconfiguration greatly improve the overall service availability and thus provide increased continuity of business processes during disaster relief operations.

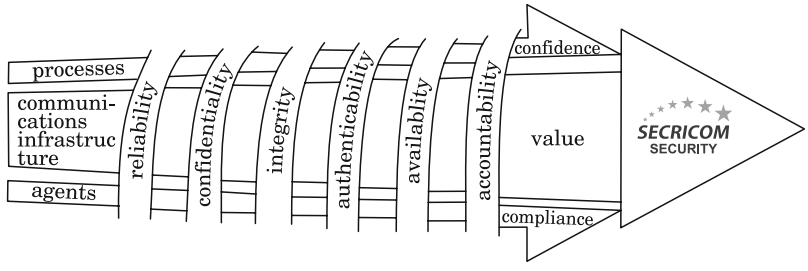

Fig. 1. Security Objectives

Availability of SECRICOM services is guaranteed not only through a balance of risk reduction measures but also through recovery options. The IT Service Continuity Management (IT SCM) plan for SECRICOM ensures that even in case of disaster the system will continue to provide the services. Provision of pre-determined and agreed level of IT services is particularly important for crisis management systems and even in case of interruption it has to support the minimum requirements, by means of the identification of required minimum level of SECRICOM services as well as the development of an IT risk mitigation program.

Responding also to project high level objectives, the design and implementation of assets must be done considering security as an integrated design element in order to ensure the availability, integrity and confidentiality of data and system resources supporting the key security functions.

Secricom Risk Assessment

Taking into account the complexity of the SECRICOM system, a single security technology has not been enough to overcome all the security objectives. The used method has consisted of a set the requirements for the security model that have to address all the security challenges. Thus, firstly a risk assessment (STONEBURNER 2002) and analysis of the heterogeneous communication infrastructure of SECRICOM has been done. The system architecture has been analysed in order to determine the value of assets in terms of impact or criticality for the whole system. SECRICOM infrastructure consists of Secure Agent Infrastructure (SAI), Push-To-Talk Service (PTT), IP Core Network, Legacy network gateways and Communication Monitoring and Control Centre. Furthermore, assets evaluation has been conducted, regarding the offered communication services as well as their relevance for the system.

SECRICOM critical networking, information and operational assets analysis has been helpful to identify the potential weaknesses (Common Weakness...) of the assets. It also permits to estimate the probability of exploiting particular vulnerabilities by a given threat and the potential impact that it may have on the operation of the system. Therefore, it is possible to determine the risk level of each asset. The outcome has been a risk treatment plan and a set of security requirements that need to be fulfilled in order to create an effective security model for a pervasive and trusted communication infrastructure.

In the aim of validating and updating drafted security requirements, a user team workshop was held on 13 April 2011 in London UK, in order to enhance SECRICOM requirements of the security model. The workshop aimed to obtain experience based statements, remarks and suggestions from individuals well versed in crisis management in a structured framework in order to establish the user requirements in terms of the security of the information carried on communications systems used by first responders during crisis management. The impact analysis was set against the background of Civil Protection Agency operational outcomes, such as the importance of having or not having a particular communication asset with reference to saving lives, ability to conduct emergency services, provision of local contingency services, impact on judicial proceedings and impact on foreign relations.

Information Exchange Requirements (IER) analysis results were presented as the starting point for this user team workshop in terms of considering the varying needs for security of communications assets depending on the differing three command levels, that is, strategic, tactical and operational levels. IER describes the process used to enable the Capability/Interoperability shortcomings of current Crisis Management communications systems to be identified. From this study it is possible to conclude that at strategic level, there is an identifiable need for data style communications to assist in decision making and the provision of strategic direction. At the operational level, which is mobile by nature, there is a high level of voice communications. Sitting between the operational and strategic level is the tactical level, which can be fixed and mobile but predominately nomadic (temporarily located at a location for a period of time with a capability to move). This level reflects the need for voice and data capability. What is irrefutable is that all levels have an increasing need for data capability. Thus, in the figure below it is shown that although Voice remains the most significant method of Information Exchange, Messaging (email / text) and other data types, such as web services (understood as services that will be consumed by final users via web interface), file transfer and video, also emerge as prominent, as shown in the figure below.

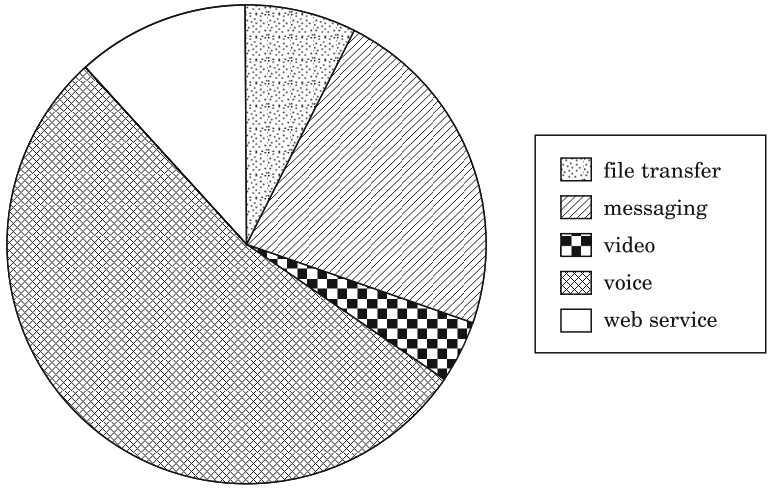

Fig. 2. IER distribution grouped by Communication Service

Back to the user workshop, these services have been the communication assets that have been analyzed and weighted in terms of impact against the operational outcomes described before and in terms as well of continuity and service operation for the typical information security components of Confiden-

tiality, Integrity and Availability. A standard risk assessment process was adapted to assist the users in prioritising different security requirements for the communication assets. Subsequent analysis and evaluation of the workshop findings concluded in the following table that illustrates the impact perspective of all the three command levels for each communications asset for the core security requirements of Confidentiality, Integrity and Availability.

Table 1

Communication Asset value

Assets	Strategic			Tactical			Operational		
	confidentiality	integrity	availability	confidentiality	integrity	availability	confidentiality	integrity	availability
Voice	5	5	5	6	5	5	6	6	6
Messaging (e-mail, data/text)	4	2	2	3	4	4	3	3	3
File Xfer (dokument)	4	2	2	3	4	4	3	3	3
Video	2	2	2	2	2	2	2	2	2
Web	0	2	2	3	1	1	3	1	1

Where “6” represents a “High” risk impact level and “0” represents “None”.

The key security requirements findings that emerged from the workshop were as follows:

– Voice communications at all three levels of command and between agencies, is seen as critical and therefore would require the highest level of security in terms confidentiality, integrity and availability.

– Messages and file transfer are seen as the next important communication assets in terms of security requirements.

– Web services are the least valued communication assets at all levels of command with video considered the next least valued communications asset.

– In comparison to Integrity and Availability, Confidentiality is considered a lesser requirement; probably reflecting the desire for as flexible communications as possible when life is at risk.

– Integrity, across all three command levels, is seen a key requirement (voice in particular) for all communications assets. I.e. a message sent in any medium during a crisis has to be received in a format that the receiver understands the message so that the requested action, decision etc is carried out.

– Availability of all communication assets, apart from voice which is viewed as essential, is seen as moderately important across all three levels of command with messaging and file transfer being viewed more important than video and web.

Hence, security objectives concentrate the security requirements that have to be covered by a set of appropriate countermeasures and security mechanisms (Implementing Network...) identified through the risk management process. These mechanisms support the three integral concepts of a holistic security program: detection, reaction and protection. Detection monitors for potential breakdowns in protective mechanisms that could result in security breaches. Reaction responds to detect breaches to thwart attacks before damage can be done. Protection provides countermeasures such as security policies, procedures, and technical controls to defend against attacks on the assets being protected. A security policy is a set of rules that dictate how sensitive data has to be managed, protected, and distributed. It provides the security goals that the system must accomplish. The level of security that a system provides depends upon how well it enforces the security policy, and a security model is a statement that outlines the requirements necessary to properly support and implement a certain security policy.

Secricom Security Model

The output of the risk analysis and the identification of the security mechanisms solutions that will provide the required security services is the set of security requirements presented in Table 2.

All these requirements are aggregated in the specification of a suitable security model. The SECRICOM Security Model proposes the application of these security principles to define the guidelines and rules for achieving a secure infrastructure. The security model does not define how to build or implement a secure infrastructure, but instead defines the properties, capabilities, processes and controls that a secure infrastructure contains to protect against a range of threats.

The SECRICOM Security Model defines two fundamental security objectives that are total visibility and complete control. Total visibility consists of identifying and classifying users, traffic, applications, protocols and usage behaviour; monitoring and recording activity and patterns; collecting and correlating data from multiple sources to identify trends and system-wide events; detecting and identifying anomalous traffic and threats. Complete control consists of hardening IT infrastructure, including individual devices and increasing network resilience; limiting access and usage per user, protocol,

Table 2

Security Requirements

Security Architectural Principle	Description
Defence-in-Depth	Never assume that a single control can provide sufficient risk mitigation for specific threat. Deploy multiple layers of controls to prevent, identify, and delay attacks in order to contain and minimize damage while an organization responds.
Service Availability and Resiliency	Ensure service availability through device hardening and by strengthening the resiliency of the network to adjust to and recover from abnormal circumstances.
Segregation and Modularity	Infrastructure is organized in functional blocks with distinct roles facilitating management, deployment, and securing of the devices and business assets within each block.
Regulatory Compliance and Industry Standards	Follow industry standards and best practices to facilitate the achievement of regulatory compliance.
Operational Efficiency	Simple and efficient configuration, deployment, and management of the infrastructure, throughout it entire life cycle, increase control and visibility allowing for faster auditing, troubleshooting, problem isolation, and incident response.
Confidentiality, Integrity and Availability	Security controls work to provide acceptable levels of confidentiality, integrity and availability of data.
Auditable and Measurable Controls	Security controls must be auditable and measurable to be effective.
System-wide Collaboration and Correlation	Infrastructure security is not a set of independent point solutions. Effective security requires sharing, analysis, and correlation of information from all system-wide sources.

service and application; isolating users, services and applications; protecting against known threats and exploits; dynamically reacting to anomalous events. The success of a security architecture and infrastructure implementation ultimately depends on the degree to which they enhance visibility and control. Without visibility there is no control and without control there is no security.

Secricom Security Model middleware

As a result of the performed analysis, the need of a SECRICOM Security Model software approach has been identified, which conducts, aggregates and integrates the necessary security protocols and mechanisms. This approach consists of an intelligent security framework and middleware service for adaptive information security management. It is represented by the Communication Security Monitoring and Control Centre (CSMCC). The CSMCC surveys if network infrastructures are resilient to both well-known and new forms of

attack, implementing a cyclic assessment approach by means of network enumeration, network scanning and security assessment for dynamically plugged assets. CSMCC covers an increased scope for asset protection, including information protection mechanisms, access control and usage policies, scalable architecture, auditing tools and security assurance monitoring. It also manages improved detection processes and network forensic solutions in terms of new traffic patterns and enhanced event correlation mechanisms. Not only awareness and detection capabilities, but CSMCC has also enhanced reaction capabilities for hostile environments, such as traffic blocking, alternative routing solutions and isolation mechanisms. CSMCC includes fast recovery plans for crisis critical communications as well, to provide quick and efficient recovery mechanisms (CA eTrust...).

In order to be able to cover in an efficient manner the wide and heterogeneous communication infrastructure of SECRICOM, CSMCC follows a distributed architecture composed by a centralized server, which manages all the security information, and distributed sensors and agents, which are responsible for security information gathering.

Figure 3 describes the distributed architecture for security management, which enables to deploy the different components for monitoring and control, where some valuable enhancements with regards to legacy systems have been done.

– Agent level: Adaptive agents that fetch the state and the behaviour of the components of the SECRICOM multibearer and interoperable communication solution specifically deployed for this context.

– Sensor level: Adaptation and normalization of data specifically for each type of event generated by the agents.

– Correlation level: Intensive stress tests have provided a balanced performance between sensibility and time reaction, reducing the false positives events.

– Presentation level: Enhanced final user experience for modelling, configuration and reporting, dealing with alarm behaviour and treatment.

Indeed, it should be highlighted that one of the main strengths and unique features of the CSMCC platform in SECRICOM is the set of custom agents that have been deployed along the communication infrastructure in order to adapt to the security requirements that such a scenario as major crisis communication management needs. These enhanced agents provide new detection and action capabilities, such as adaptive routing features in case of network failure or congestion and VoIP traffic monitoring. Furthermore, in order to process the security events detected by this set of agents, the CSMCC platform has defined a set of patterns and policies adapted to the prioritization and correlation of these events, providing them of a meaningful context.

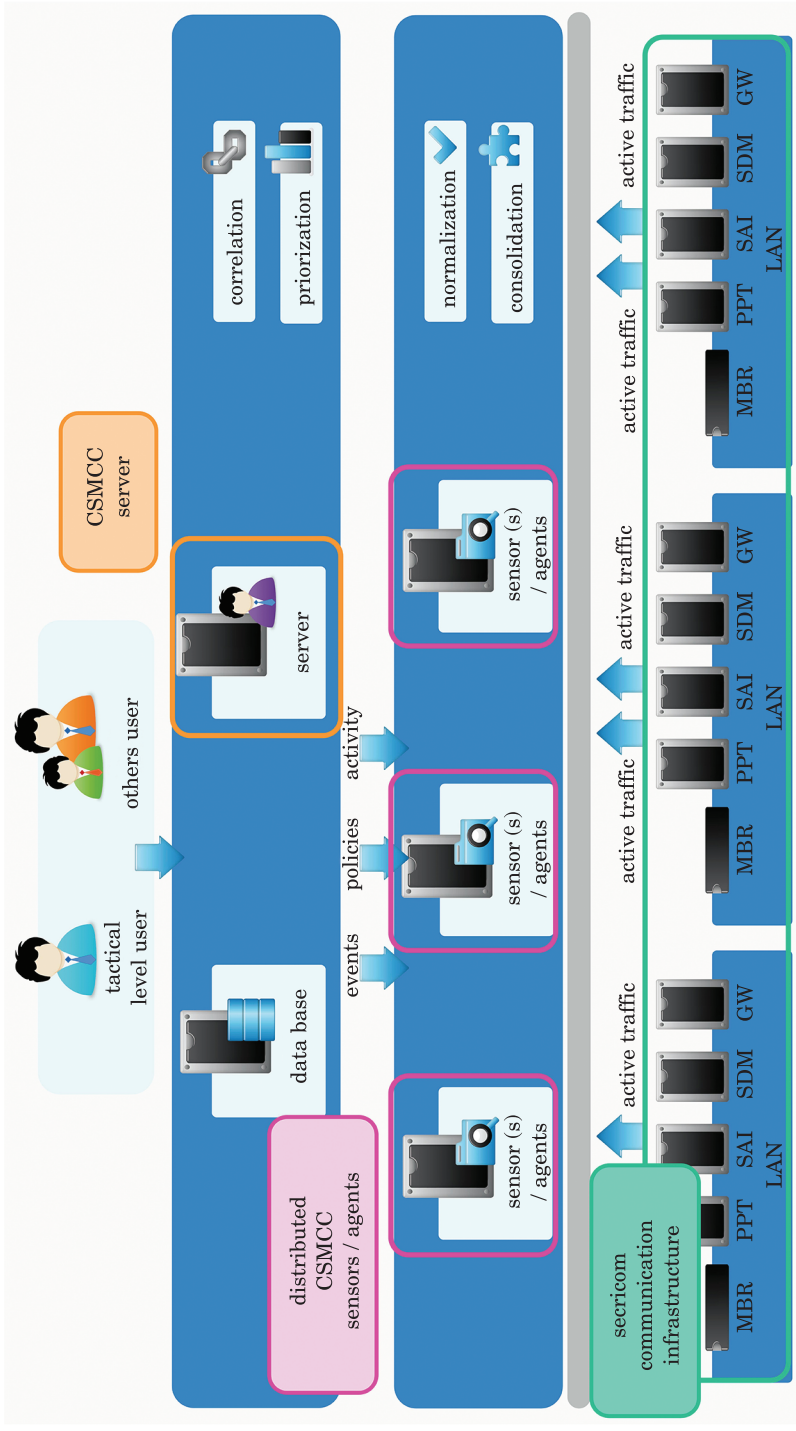

Fig. 3. Security Management Architecture

Finally, in order to cover the security objectives of total visibility and complete control of the security model, CSMCC capabilities are described below and they are split mainly in two categories, those related to security status monitoring and those capabilities related to reaction, that is, awareness and control capabilities.

- Security awareness:
  - Inventory and auto-discovery of network assets
  - Repository of hosts
  - Policy management to modify the importance of detected events
  - Sensibility policies and correlation management
  - Anomalous traffic detection
  - Intrusion detection
  - Event management
  - Alarm generation
  - Vulnerability discovery that allows a soon awareness of potential weaknesses
  - Network monitoring in terms of network usage and network latency
  - Host and service detail monitoring in terms of availability status
- Control services:
  - Traffic blocking
  - Traffic isolation
  - Alternative routing
  - Agent trust renewal
  - Configuration management

Results and Achievements

The main results achieved during the SECRICOM project in terms of communication security management can be summarized as follows:

– Identification of the security requirements to be covered by the SECRICOM Security Model.

– Delivery of the SERCICOM Security Model that defines security specifications and framework for a trusted communication infrastructure.

– Definition of the software prototype that allows the evaluation of the SECRICOM Security Model: Communication Security Monitoring Communication Centre (CSMCC) Platform.

– Deployment of enhanced and custom agents, responsible for collecting the state of the SECRICOM components.

– Development of a set of functioning patterns and policies adapted to the SECRICOM context.

Conclusions

The followed roadmap to design the communication infrastructure security monitoring and control centre starts with a risk assessment of the SECRICOM system. It consists on a deep analysis of the operation of the system, in order to define the key assets, identify their security vulnerabilities and evaluate the impact in terms of risk. The outcome of the risk assessment is a set of security requirements that the SECRICOM security model fulfils to provide an effective security management. This has been backed by a user team workshop that updated and validated these security requirements. The analysis of the security requirements results in a bunch of countermeasures and security mechanisms to mitigate the risk level obtained and protect the SECRICOM systems against the exposure to security threats. Finally, all these security principles and guidelines are aggregated into the SECRICOM security model, in order to achieve a secure communication infrastructure in a continuous way, ready for the dynamicity of the communications.

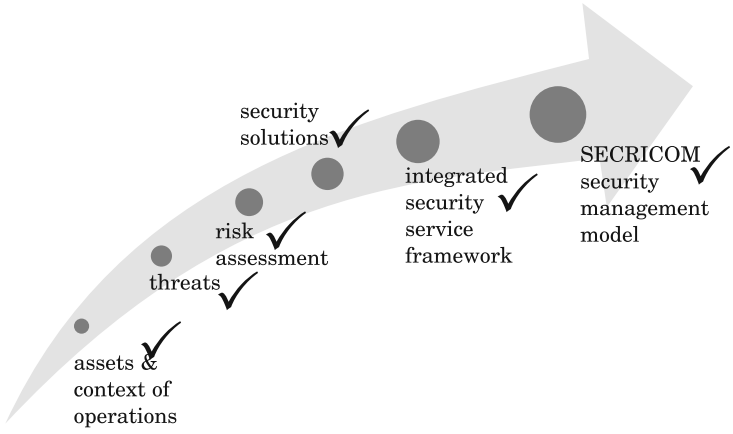

Fig. 4. Security roadmap

The security model is supported by a security middleware named Communication Security Monitoring and Control Centre (CSMCC) that provides not only security information collection and security status monitoring capabilities, but also active control mechanisms, providing enhanced protection, improved detection, faster reaction and stronger risk mitigation, more effective incident's impact mitigation and quicker restoration.

Translated by AUTHORS

Accepted for print 30.06.2012

References

Information Security. http://usdatasecurity.ch/itsecurity

STONEBURNER G., GOGUEN A., FERINGA A. 2002. *Risk Management Guide for Information Technology Systems.* Recommendations of the National Institute of Standards and Technology (NIST).

Common Weakness Enumeration, a Community-Developed Dictionary of Software Weakness Types; http://cwe.mitre.org/index.html

Implementing Network Security Mechanisms; CISCO; http://www.cisco.com/en/US/docs/ios_xr_w/iosxr_r3.3/security/design/guide/sg33impl.html

CA eTrust Security Information Management; "Imposing order on security information overload".