

MANAGING NETWORK SECURITY

October 2006

White Paper

Network security needs to be addressed using
a coherent approach.

Contents

1	Executive summary	3
2	What causes problems in telecom networks	4
3	Structured approach to security.....	5
3.1	Identifying needed security services and functions	5
3.2	Network Security Architecture Reference Model	6
4	Managing Security.....	8
4.1	Introduction	8
4.2	Common Principles.....	8
4.3	The Security Wheel	9
4.4	Security – A continuous process	10
4.5	Business Continuity Management.....	11
4.6	Network Security Design	12
4.7	Network Configuration / Integration.....	13
4.8	Network Security Audits	13
4.9	Network Security Implementation.....	13
5	Conclusion	14
6	Acronyms	15
7	References.....	16

1 Executive summary

As new end-user services are introduced in today's converged multi-service networks, telecom network security becomes more of an issue for operators and a demand from public users, enterprises and government agencies. If not given the appropriate attention, the technologies that deliver these services may actually degrade the security of the network over which the service is delivered.

Security breaches, whether they disrupt services or compromise information, cause financial losses. Examples are financial penalties for failing to maintain performance agreements, lost revenue caused by network disruptions, lost consumer loyalty, ill will, lawsuits, and industrial espionage.

Moreover, individual public users, agencies and corporations are demanding highly secure connections to telecom networks; service providers with roaming agreements want secure interfaces with their roaming partners and insurance providers, always conscious of risk, are insisting upon stringent security. Telecom Network Security awareness and acting proactively can, apart from reducing risk, also reduce operational cost.

The operator needs a trustworthy security story if they are to be taken seriously in the marketplace.

The Ericsson approach is to address security at an early stage in a structured manner; from procedural, personnel, physical and technical points of view. In this way a secure, cost effective security solution can be established and maintained to protect sensitive information and network operator business.

2 What causes problems in telecom networks

Traditionally, telecom networks refer to the infrastructure required to establish an end-to-end transfer of analogue or digital information. This comprised the transmission and switching infrastructure. Today, the infrastructure is divided into layers in order to achieve a higher level of service integration. The new infrastructure supports fixed and wireless network services.

Telecom networks distinguish between traffic (e.g., voice, data and multimedia) and control (signaling). A different layer, called connectivity network, is defined for traffic, and another layer, called control layer, is defined for signaling. As more applications and services appeared, another layer was introduced, the service layer. Operations & Maintenance (O&M) networks require high security, and that leads to another sub-layer within the core network.

With all the advantages that we can mention about the integrated layered architecture of telecom networks, we should not overlook the increasing number of security concerns that apply to all types of services and all levels of the telecom network. Access networks are subject to denial-of-service attacks and various unauthorized-access attacks. Fixed networks suffer from clip-on access and associated fraud, as well as violation of privacy. Wireless networks do not require physical access, and are even more exposed. Mobility adds other vulnerabilities and threats, including SIM card cloning, subscription frauds, man-in-the-middle attacks and so on.

Core networks have a multitude of interconnection points, which mean different security requirements and possible exposure to a wide range of threats and vulnerabilities. Attacks on the core would lead to larger impacts on the different services and stakeholders, such as end users, service and application providers, and the operator itself. Stealing passwords and accessing the management ports, attacking the signaling layer, targeting databases of subscribers, HLRs, OSSs, network elements, gateways, and application servers could lead to security violations, fraud and service interruption.

As networks grow and become increasingly complex, the risk of holes in security due to configuration and/or design mistakes increases. As increasingly more business-critical applications rely on the availability of the networks, the exposure to loss is also becoming drastically higher.

Users expect reliability in all transactions, independent of access, and guaranteed connection quality. From a security point of view, the user expects no viruses, no worms, no fraud, nobody listening in, and the ability to know who requests a communication session.

3 Structured approach to security

3.1 Identifying needed security services and functions

Security solution development begins with threat-risk analysis. It is required to identify assets, threats and vulnerabilities, rank the different assets in the order of their importance for the business, and evaluate different alternatives to handle the risk.

The risks are then grouped into categories such as:

- Must be minimized/eliminated
- Should be minimized/eliminated
- Acceptable.

This information enables decision-makers to capture requirements and to specify the implementation of security services and functions.

3.1.1 Security Policy

A security policy should be a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives. The policy performs several functions that help ensure the effectiveness of whatever security strategy the organization pursues. Specifically, it:

- Defines information security and its overall objectives and scope.
- Defines acceptable security practices; a framework for setting control objectives and controls, including the structure of risk assessment and risk management.
- Establishes roles and responsibilities; a definition of general and specific responsibilities for information-security management, including reporting information-security incidents.
- Briefly explains the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:
 - Compliance with legislative, regulatory, and contractual requirements
 - Security education, training, and awareness requirements
 - Business continuity management.

The security policy framework should be the “hub” around which all security-related services and functions evolve.

3.2 Network Security Architecture Reference Model

To provide adequate security, it is important to be able to model the mobile network and analyze the threats to assets. The following three-plane architecture (based on the international standard X.805) provides a useful and simple way of capturing relevant information. This model consists of four architectural components: separate security planes, security layers, security services, and security policies & principles.

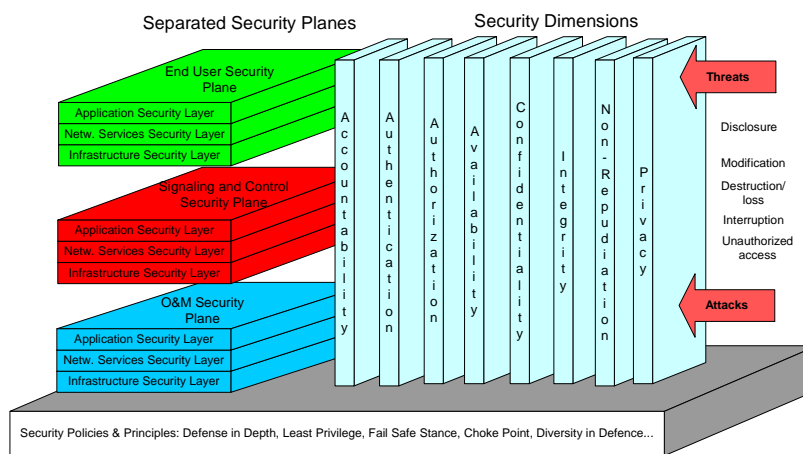


Figure 1. Network Security Architecture Model

3.2.1 Security Planes

Networks should be designed in such a way that events on one security plane are kept totally isolated from the other security planes. The concept of security planes provides the ability to differentiate and address security concerns independently.

The End-User Security Plane addresses security of access and use of the service-provider's network by customers. This plane also represents actual end-user data flows. *The Signaling and Control Security Plane* covers protection of the activities that enable the efficient delivery of information, services and applications across the network. *The O&M Security Plane* covers the protection of operation and maintenance functions.

3.2.2 Security Dimensions

The security dimensions are system aspects which run through all security solutions. However, security solutions and mechanisms are used for implementing the security dimensions. All security dimensions should be evaluated in each security plane/layer intersection point. The most common ones are:

- authentication
- authorization
- accountability
- availability
- confidentiality
- integrity
- non-repudiation and privacy

3.2.3 Security policies & principles

To enhance protection of the network, specific security principles and best practices are commonly used. Probably the most important one is the defense-in-depth principle: employ several security mechanisms and security layers to provide protection. If one of the mechanisms or layers fails, the other mechanisms and layers are still in place to provide sufficient protection. This principle is commonly used to protect the perimeter of a site, as depicted earlier in Figure 1.

The least privilege is another fundamental security principle. It means that an entity should only have the privileges it needs to perform its tasks. This is of utmost importance when considering node protection. The services running on a node should have only the privileges they need to provide the service and the node should not be running any unnecessary services.

Systems and nodes should also implement the fail-safe principle. This means that when the system or node fails, it should fail without harmful side effects.

Sometimes, the diversity-of-defense principle might also be useful. This principle is based on using different types of systems to provide a certain kind of protection. If one of the systems contains vulnerability, the other systems might not have that vulnerability and the impact of the vulnerability is thus mitigated.

A choke point forces attackers to use a narrow channel, which can be monitored and controlled. In network security the proper perimeter protection for the site is such a choke point; anyone attacking the site from the outside will have to go through that channel, which should be defended against such attacks.

4 Managing Security

4.1 Introduction

To be able to make sound security judgments, both the particular business context and the networking environment must be fully understood. To support the whole telecom system life cycle, from end-to-end, the following operations have to be undertaken:

- Business Continuity Management
- Network Security Design
- Network Configuration / Integration
- Network Security Audits
- Network Security Implementation
- Fraud Management.

4.2 Common Principles

The security operations address:

- Risk Management: all network operation implies a certain risk that must be accepted, avoided, reduced or transferred.
- Business Continuity: the operator's critical processes and information should be protected from disclosure and/or disruption.
- Lowering operator costs: well thought-out security solutions provide a payback in terms of reduced operating costs, reduced risk of fraud, a reduced risk of critical security-related network outages and potentially less churn.

The following chapter describes how the different sub-operations complement each other and fit into the "Security Wheel" concept, forming continuous security management.

4.3 The Security Wheel

This industry-standard model has been chosen to illustrate where security management fits in, and how all security activities in a network must evolve around the security policy; see figure in chapter 4.4.

The concept sees network security as a continuing process built around a corporate security policy. This process is divided into the stages:

- Implement network security
- Monitor network and respond to incidents
- Test the security of the network
- Improve network security.

Implement network security – Security devices such as perimeter nodes, VPN devices, firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and authentication devices are planned, configured and integrated. The purpose is to prevent activities that the policy has defined as threats.

Monitor/Respond – The implemented security policy is validated using intrusion detection, as well as log and other auditing techniques, to watch for violations.

Test – The effectiveness of the policy should be evaluated at regular intervals through security audits, vulnerability scanning and/or penetration tests.

Manage/Improve – Information gathered from previous steps is analyzed and used together with developments in the security market to improve the policy, moving around the circle to the first step again.

4.4 Security – A continuous process

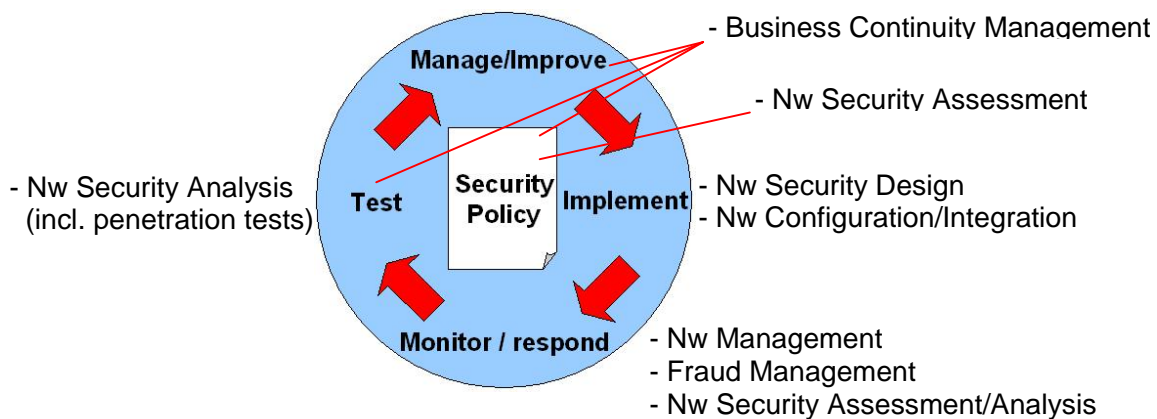


Figure 2. The Security Wheel model

Security Policy – Is, together with the Risk Analysis, the most fundamental part of any company's security/business continuity process. These can be checked and/or developed as a part of either the security assessment service or the business continuity service. Business Continuity also includes such aspects as, for example, crisis management, disaster recovery, and organization resiliency.

Risk Analysis and Readiness planning is of utmost importance in guaranteeing the safe launch of a new service.

Implement Network Security – Network Security Design ensures that security is implemented according to best telecom practices, and the level planned for in the security policy. Also, configuration and integration must be performed in the most secure manner possible, and according to plans.

Monitor/Respond – Network Management personnel monitor logs, while Intrusion Detection System real-time alarms detect any signs of attempted policy violations. Fraud-management processes and solutions instantly detect malicious end-user behavior. The network security organization must be continuously updated with the latest methodology to perform IDS/IPS tuning, log analysis and computer forensics.

Test – Detailed system configuration analysis and tests, including penetration tests and vulnerability scanning must be performed on a regular basis. This also includes exercises around selected scenarios in, for example, a company’s disaster recovery plan.

Manage/Improve – A list of suggested security improvements always form part of the output of a security Assessment, Analysis, Fraud or Business Continuity activity. They can be categorized as procedural, physical, technical or relate to the personnel.

4.5 Business Continuity Management

Business Continuity Management (BCM) incorporates not only business continuity planning and disaster recovery, but also the disciplines of crisis management, risk management, facilities management, health and safety, security, quality management and supply chain management. It can be seen as a super set of security management processes.

The BCM process is divided into six stages shown in Figure 3 and explained below.

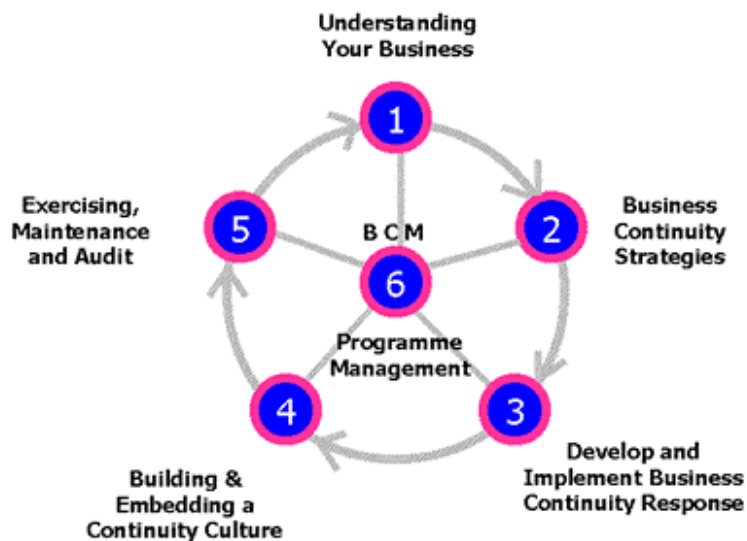


Figure 3: The six stages of Business Continuity Management

Understanding your business: this phase focuses on identifying the Mission-Critical Activities (MCAs) of the business; the underlying technology, internal and external dependencies that support these MCAs; and any existing single points of failure. An example is the impact of a loss of a switch site, HLR, MSC or billing system.

Business Continuity Strategies: the focus of this stage concentrates on the identification and selection of alternative recovery solutions, so that the impact of a loss or disruption of an MCA is minimized and, as far as possible, transparent to the end user. The choice of recovery solution represents a trade-off between investment cost and effectiveness.

Develop and Implement BCM Plans: this phase is concerned with structuring and documenting the Business Continuity Plan (BCP).

Building and embedding a continuity culture: BCM must form an integral part of the organization's day-to-day business environment, so awareness of business continuity must be created and maintained.

Exercise, Maintenance and Audit: exercises provide the opportunity to fine-tune plans, so the BCP and BCM strategies are effective during a crisis.

Program Management: the roles, responsibilities, accountabilities, assurance and authority for BCM need to be clearly defined so there is continued coordination and governance of all BCM-associated activities throughout the organization.

4.6 Network Security Design

Because security has to be an integral part of the system from the start, and cannot be "bolted on" afterwards, it is crucial to get the security design right from the very beginning.

The security policy states the rules, responsibilities and procedures to follow to protect the network and its carried information.

The network design should also apply best common practice for telecom network security. Two main inputs in the designing of network security are a threat/risk assessment and the development of a security policy. The main inputs to a threat/risk assessment are the overall security goals and security budget to ensure the planned level of security is reached.

The network is divided into zones with clearly defined traffic flows. Encryption/VPN technologies are applied where necessary.

It is crucial to develop a Network Plan for Security, comprising a report describing the procedures used, threats mitigated and scalability/functionality paths to follow in future phases of the development of the network. Also shown in the Network Plan are the locations of perimeter protection nodes, placement of IDS/IPS sensors, firewalls, and encryption nodes. Guideline scripts for filtering/security configuration are also produced, along with inputs to the node-hardening process. As with all security configurations, the three aspects of functionality ease of use, and security level must be carefully balanced in the design.

4.7 Network Configuration / Integration

When an end-to-end security architecture network configuration is carefully planned, integration of a new network or an upgrade/enhancement of an existing network can be performed in the best way, helping to guarantee that the planned security levels will be implemented in a structured way.

4.8 Network Security Audits

Network Security audits can be performed on two levels:

- Network Security Assessment
- Network Security Analysis

Security Assessment – Network-common items such as Security Policies and Security Design, or functionality areas such as GPRS, O&M, and billing, are audited on a higher level. Documentation and plans should be studied and compared with industry practice so that, together with interviews with key personnel, recommendations can be produced.

Security Analysis – Functionality areas or specific nodes are examined in a detailed way. Node configuration scripts are checked. Log analysis, vulnerability scanning and non-destructive penetration can also be performed.

4.9 Network Security Implementation

The suggested security improvements from any previous security-related service must be carefully analyzed in order to choose which ones to implement. Suggestions can be procedural, physical, technical or relate to the personnel.

5 Conclusion

Security, in the context of telecom networks, concerns all parties involved: the end user, the service provider, the content provider, the applications provider, and the operator. The concerns can be expressed in terms of loss of service, loss of revenue and image, loss of confidentiality, mistrust, churn, and possible legal actions.

Security controls and safeguards must be implemented to reduce such risks. This should take place in all levels of the network and all stages of network development. The network should be designed with security in mind and be easy to manage. The network should be safeguarded against current vulnerabilities and regularly tested for new vulnerabilities and threats. Risks should be mitigated and attacks logged so as to provide forensic evidence.

Security is not a static procedure that can be applied once and for all. It is a living process that grows with the network, users, applications, technology and offenders. Security should be addressed with technical, administrative, procedural and technical countermeasures.

The primary components of a successful security strategy are:

- Policy: define security objectives, principles and compliance.
- Auditing: thoroughly verify if policies are enforced effectively.
- Detection: watch for violations and fraud on a regular basis.
- Protection: implement safeguards to minimize risks to critical assets.
- Testing: to ensure proactive security measures remain effective.

Only when a structured approach including these components are strictly followed, a sufficient security level can be achieved and maintained.

6 Acronyms

BC	Business Continuity
BCP	Business Continuity Plan
BCM	Business Continuity Management
CDR	Charging Data Record
GDR	Global Data Record
GPRS	General Packet Radio Services
HLR	Home Location Registry
IDS	Intrusion Detection System
IP	Internet Protocol
IPDR	IP Data Record
IPS	Intrusion Prevention System
MCA	Mission Critical Activity
MMS	Multimedia Messaging Services
MSC	Mobile Switching Centre
NW	Network
O&M	Operation & Maintenance
OSI	Open System Interconnect
RDBMS	Relational Database Management System
VPN	Virtual Private Network

7 References

Ericsson Review article, Issue 02/2004:
“Security Architectures for mobile networks”
http://www.ericsson.com/about/publications/review/2004_02/files/2004125.pdf

Ericsson Review article, Issue 02/2006:
“Mobile Platform Security”
http://www.ericsson.com/ericsson/corpinfo/publications/review/2006_02/files/mobile_platform_security.pdf

Ericsson White Paper, 284 23-3064 Rev A:
C4ISR for Network-Oriented Defense
http://www.ericsson.com/technology/whitepapers/3064_C4ISR_A.pdf

Draft ITU-T Recommendation X.805 (Formerly X.css):
“Security architecture for systems providing end-to-end communications”
<https://www.ietf.org/IESG/LIAISON/itut-sg17-ls-x805-end2end-communications.pdf#search=%22%22X.805%22%22>