

Security architectures for mobile networks

Dirk Eschenbrücher, Johan Mellberg, Simo Niklander, Mats Näslund, Patrik Palm and Bengt Sahlin

Security is a growing issue for carriers and operators. In particular, they are concerned about protecting network infrastructure. Ericsson shares these concerns and is putting great emphasis on secure products and security features.

A holistic perspective is needed for planning the security services and functionality to be implemented in nodes, subnetworks, and at the network level. Decisions affecting security services and functionality need to be based on a coherent, well-defined security architecture.

The day is gone when vendors and standards could dictate the environment for deploying the mobile network infrastructure and associated products. Today's solutions and products must be flexible enough for use outside a reference network and resilient and extensible enough for use without external security appliances.

Simple security checkpoints, such as firewalls, no longer suffice. As applications become more complex, general vulnerability to attacks also increases. A defense-in-depth strategy is thus needed, putting security features in each and every node. These features can be complemented with security functionality at site and network levels.

While we acknowledge the importance of physical security, fraud detection, and management, the focus of this article is on logical network security. In addition, although this article primarily deals with GSM and WCDMA, the principles of security architecture presented here apply equally well to other cellular networks, such as CDMA.

The authors describe Ericsson's security architecture for GSM and WCDMA mobile networks. This architecture is based on security principles mandated by standards and experience. Moreover, it is influenced by policies that regulate security, and by vulnerability audits of the mobile infrastructure. The authors also describe security services and functionality, and how low-level mechanisms can be applied to make the mobile network infrastructure more secure. They cite examples from Ericsson's product portfolio, including the security solution designed in the Mobile-PBN reference network.

Goals and strategy

Ericsson understands that to fulfill operator requirements for flexible and secure solutions that involve its products, it must provide technical features that help operators with deterrence, prevention and protection, detection, response, and recovery.

Security should be viewed as a process and not a state (Figure 1). It is about applying fit-to-purpose, cost-effective mechanisms at each point in time throughout the process. A good vendor-operator relationship completes the process with operations feedback from the system, thereby refining and further "hardening" the system. The process must also include operator assistance and service to subscribers—that is, the process must help operators and subscribers to maintain security and safeguard privacy.

Ericsson's approach to security is to build on a strong set of basic security features and inherently secure products that help operators to lower their

- capital expenditures (CAPEX)—that is, fewer dedicated security nodes are needed to protect the network; and
- operating expenses (OPEX)—that is, greater product security reduces the need for administrative actions.

Controlling access is an especially important part of Ericsson's strategy. As security is pushed out to network endpoints, the nodes in access networks will be employed to control access (which includes authentication, authorization and accounting). Notwithstanding, operators must retain the ability to administer security centrally. Ericsson is thus working to give operators better management of nodes in access networks.

Figure 1
The security process.¹



Ericsson is also constantly improving processes surrounding software development to make operating systems and applications more secure. Through careful selection of platforms and software, Ericsson ensures that each product is delivered fit-to-purpose (this is also commonly referred to as *hardening*).

Background

It has been said that there are two main approaches to avoiding exploitable weaknesses in system design:

- one can make the system so complex that it has no obvious weakness; or
- one can make the system so simple that it is obvious it has no weakness.

Ericsson is a strong adherent of the latter approach—simplicity. But where telecommunications network design is concerned it is impossible to entirely circumvent complexity—without complexity, one could not guarantee backward compatibility, multi-access, multi-service, and multiple platform support. Notwithstanding, unless great care is exercised, one ends up with a patchwork of unrelated management and security solutions.

The ideal solution to avoiding complexity-related security flaws is complete system redesign. If researchers and engineers were allowed to start over from scratch, they could create a simple system that operators could use to assess

- the security of each independent component; and
- how each component interacts with other components.

In the real world, however, this is an unrealistic ideal due to requirements put on the upper bound of design, maintenance costs, and practical system usability. Besides, as stated above, security is a process, not a state. Therefore it is impossible to fit every security aspect into the design phase. And let's not forget proper life-cycle management.

Notwithstanding, it is possible to design a secure solution that can be managed at reasonable cost. But doing so successfully requires broad competence—for example, knowledge of the telecommunications business, end-user requirements, and an understanding of the impact of regulatory aspects, as well as technical expertise in operating systems, protocol design, and cryptography. With all this complexity, what operators need are a conceptual model for security in the network and a sound, systematic approach to threat-and-risk analyses.

Security in mobile networks

This article builds on the scenario of a typical third-generation public land mobile network (PLMN) whose services and access roughly correspond to that defined by 3GPP Release 6.

Mobile network evolution and threats

Up to and including second-generation mobile telephony, operators largely based mobile network security on security by obscurity—that is,

- they were secretive about the cryptographic algorithms they used;
- they used proprietary hardware platforms and operating systems;

BOX A, TERMS AND ABBREVIATIONS

2G	Second-generation mobile telephony	IP	Internet protocol
3DES	Triple data encryption standard	IPsec	IP security protocol
3G	Third-generation mobile telephony	ISUP	ISDN user part
3GPP	Third-generation Partnership Project	LAN	Local area network
AES	Advanced encryption standard	MD5	Message digest 5
AKA	Authentication and key agreement	MGW	Media gateway
B3G	Beyond 3G	MPLS	Multiprotocol label switching
BICC	Bearer independent call control	MSC	Mobile switching center
CAPEX	Capital expenditure	O&M	Operation and maintenance
CC	Common criteria	OPEX	Operating expense
CORBA	Common object request broker architecture	OSI	Open Systems Interconnection
CRM	Customer relationship management	PAN	Personal area network
CS	Circuit-switched	PEP	Policy enforcement point
DNS	Domain name server	PIN	Personal information number
DRM	Digital rights management	PLMN	Public land mobile network
ESP	IP encapsulating security payload	RBAC	Role-based access control
FCAPS	Fault, configuration, accounting, performance, and security management	SBT	Secure backbone tunnel
FW	Firewall	SCLI	Secure command line interface
GPRS	General packet radio service	SFTP	Secure file transfer protocol
GRE	Generic routing encapsulation	SHA	Secure hash algorithm
GSM	Global system for mobile communication	SIM	Subscriber identity module
GSN	GPRS support node	SIP	Session initiation protocol
HIDS	Host-based IDS	SNMP	Simple network management protocol
HMAC	Keyed-hashing for message authentication	SSH	Secure shell
HTTP	Hypertext transport protocol	SSL	Secure sockets layer
IDS	Intrusion detection system	TCAP	Transaction capabilities application part
IETF	Internet Engineering Task Force	TLS	Transport layer security
		UMTS	Universal mobile telecommunications standard
		USIM	UMTS SIM
		VLAN	Virtual LAN
		VPN	Virtual private network
		WCDMA	Wideband code-division multiple access
		WLAN	Wireless LAN

- their protocols were practically unknown outside the telecommunications sector; and
- their networks were separate from the public internet.

Today, however, all this is rapidly changing. Experience has shown that proprietary security solutions eventually “leak” and soon after they break. Cost and interoperability with the public internet are drivers of greater openness. For instance, most of today’s protocols are based on IP, and operators are deploying more and more open platforms (including software). Although a greater degree of openness decreases the risk of unpleasant surprises (unknown vulnerabilities), it also increases the risk that known vulnerabilities can and will be exploited. Openness is thus a two-edged sword. To give the upsides a chance to bear fruit, we must provide cost-effective, fit-to-purpose security measures that guard against the possible downsides. Failure to recognize this fact could be fatal to vendor or operator business, because in essence, it means failure to provide service availability and end-user privacy.

With traditional vertical services, such as circuit-switched voice, end-users need only rely on a single operator who has complete control. But with the rise of multi-access and multi-service networks, end-users must rely on operator, access provider and service provider. This, in turn, affects the security solutions used. End-users, for example, might be asked to authenticate themselves for every access and service they want to use. This is inconvenient at best, and a security nightmare at worst (many end-users tend to use the same user name and password over and over).

At the technical level, some operators of third-generation services want to augment their offering with WLAN hot-spot access. We remind the reader, however, that the WLAN access security architecture was developed using a trust model for corporate access (behind locked doors) and not for public access deployment.

Finally, an extremely important aspect to consider is end-user expectation of security. Most end-users trust operators to handle circuit-switched voice services, but what about new services? What level of security do end-users expect (implicitly or explicitly) when they use chat, gaming, or e-commerce services? Operators who do not understand end-user requirements for security and privacy run the risk of losing subscribers

who feel unsafe or who have unpleasant experiences after having used a service. On the other hand, excessive security might also have a dampening effect due to inconvenience. Indeed, an odd quality of security is that it is most effective when end-users sense neither its absence nor its presence.

Standards

Standardization is needed to ensure interoperability. Open, scrutinized security standards contribute to greater confidence than proprietary solutions. At the same time, there is a need to uphold competitive positions. In this respect, security-related standardization is being driven by the same factors as general-purpose standardization.

Apart from ensuring interoperability, the main goal of standardized security solutions should be to guarantee secure features or services. One must also maintain the high-level view of security services to ensure that security features at different levels and in different systems or services can fit together. This implies a need for coordination between standardization organizations, to ensure that the overall solution provides adequate security, and the components of the solution complement one another.

The most important standardization bodies for mobile network security are 3GPP and IETF. At the application level, standards set in OMA and Liberty Alliance are also very influential.

Structured approach to security

The many facets of security

Given the level of complexity in today’s mobile networks, operators, vendors and manufacturers need some way of modeling them. Likewise, the models they use must allow operators to study security—for example, by allowing them to break the network down into smaller, more manageable components. Likewise, a common language is needed for discussing security.

Identifying needed security services and functions

Security solution development begins with threat-and-risk analysis. Proceeding from a functional description (specification and assumption of logical and physical properties) of the system, one identifies conceivable threats (Figure 2). Next, one estimates the probability of these threats and associated

financial risks. The risks are then grouped into categories such as

- must be minimized or eliminated;
- should be minimized or eliminated; and
- acceptable.

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

Ericsson's reference architecture

In summary, to provide adequate security, one must be able to model the mobile network and analyze threats to assets. Ericsson's three-plane architecture provides a useful and simple way of capturing relevant information (Figure 3).

Security planes

Because there are threats to assets in each of the three architectural planes, security services must be applied in each plane to mitigate them.

Mobile networks should be designed in a way that isolates incidents on any given security plane. This makes it possible to dif-

ferentiate between security concerns and to address each independently. Although the security planes are isolated, they can communicate with one another by means of policy enforcement points (PEP), which deploy access control. If necessary, the security planes can be broken down into sub-planes. Ordinarily, firewalls serve as PEPs for security planes.

The end-user security plane manages subscriber access and use of the service provider's network. It also represents actual end-user data flows.

The signaling-and-control security plane protects activities that enable efficient delivery of information, services and applications across the network.

The O&M security plane protects O&M functions of the network elements, charging functions, transmission facilities, data centers, and back-office systems (operations support systems, business support systems, customer care systems). It also supports fault-, configuration-, accounting-, performance-, and security-management (FCAPS) functions.

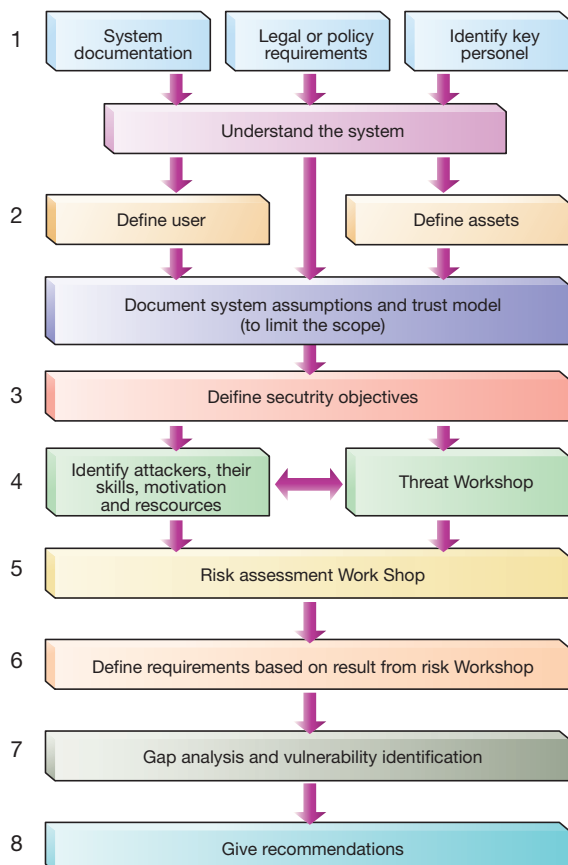


Figure 2
Threat-and-risk analysis.

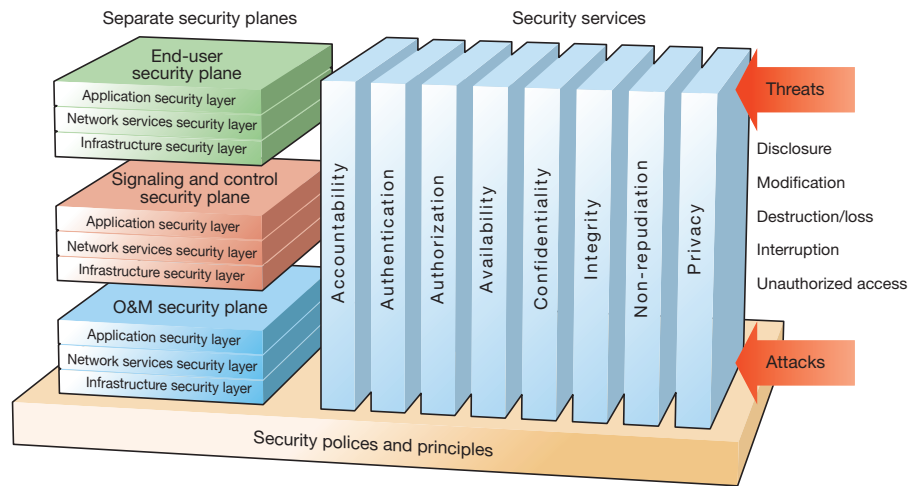


Figure 3 Reference model for security architecture.

Common technologies for separating security planes are physical and logical separation—for instance, firewalls (FW), virtual private networks (VPN), multiprotocol label switching (MPLS), virtual LANs (VLAN) and generic routing encapsulation (GRE).

Security domains

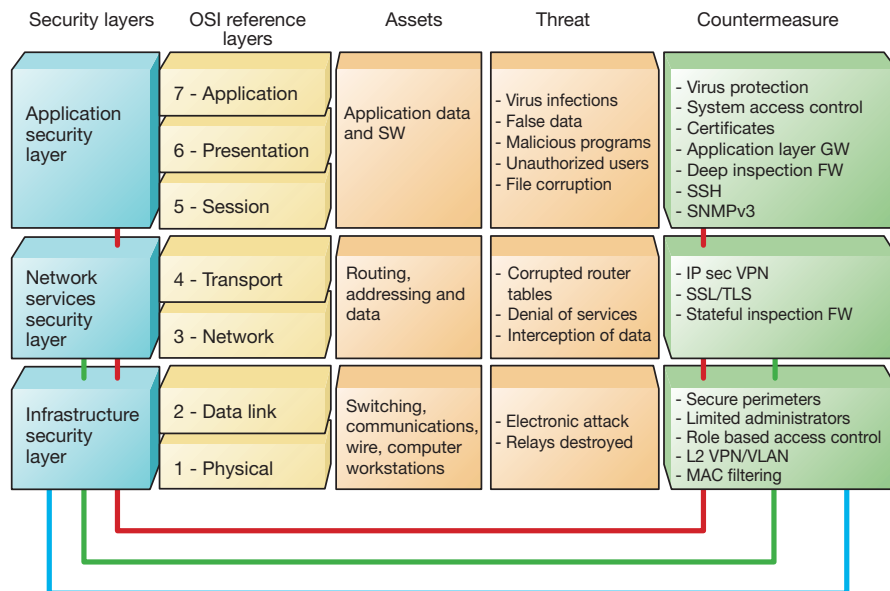
A security domain is a part of a network that shares a security policy issued by a single administrative authority. This is not shown in Figure 3 because the division into domains

is dependent on external requirements derived from the network architecture and business models. Note that a single operator network can be divided into several security domains.

Security layers

Each security plane has been divided into three security layers that identify where security needs to be addressed by providing a sequential perspective of network security. This layered defense strategy acknowledges that each layer has different security threats

Figure 4 Layered defense strategy.



and ensures that solutions can be deployed in each OSI reference layer (Figure 4).

The infrastructure security layer consists of the network transmission facilities and the individual network elements protected by the security services. It represents the fundamental building blocks of networks, their services and applications. Examples of components that belong to the infrastructure security layer are individual routers, switches and servers, and the communication links between them.

The network services security layer addresses network services to end-users. These range from basic transport and connectivity to the service enablers that are necessary for providing network access. The network services security layer protects service providers and their customers—for example, by blocking malicious attempts to keep service providers from offering network services (denial of service) or attempts to disrupt service to individual customers.

The focus of the application security layer is on network-based applications. These applications, which are enabled by network services, include

- traditional voice applications (for example, ISUP and TCAP protocols and application services that use these protocols);
- multimedia applications (for instance, BICC, SIP and H.323 protocols and application services that use these protocols); and
- high-end applications, such as customer relationship management (CRM), electronic and mobile-commerce, network-based training, and video collaboration.

There are four main targets of security attacks in the application security layer: the end-user (or application user), the application provider, the middleware provided by third-party integrators (web-hosting services), and the service provider.

The last column in Figure 4, which shows the relationship between security and OSI layers, lists mitigation mechanisms employed against different threats in the layers. These mechanisms protect stored data and data in transit.

Security service

Security service is a fundamental concept in every security architecture. The service meets the security objectives identified by the threat-and-risk analysis. Security services are implemented by means of *security functions* and *mechanisms*. A confidentiality

protection security service, for example, might be implemented using an IP layer encryption security function. This, in turn, might make use of the AES encryption mechanism. At each intersection point of the security plane or layer, every security service must be evaluated in terms of

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

Authentication is used to confirm the identities of communicating entities (person, device, service or application) and ensures that the entities are not masquerading or attempting unauthorized replay of previous communication.

Authorization protects against unauthorized use of network resources. Access control ensures that solely authorized personnel or devices have access to network elements, stored information, information flows, services and applications. Role-based access control (RBAC) is commonly used to regulate authorization in O&M. Similarly, end-user authorization is used to control accessibility to services.

Accountability procedures are used to keep track of who does what and when. Accountability functions track the usage of security services and network resources. Accountability logs facilitate recovery and fault discovery.

Availability means that authorized entities have access to network elements, stored information, information flows, services and applications regardless of incidents that affect the network. Common techniques for ensuring availability are redundancy, perimeter protection and node hardening.

Confidentiality entails protecting data from unauthorized disclosure. Data confidentiality ensures that data content cannot be understood by unauthorized entities. Encryption (for example, 3DES and AES), access control lists, and file permissions are frequently used to protect data confidentiality.

Integrity ensures the correctness or accuracy of data—the data is protected against unauthorized modification, deletion, creation, and replication. Integrity features might also indicate unauthorized activities. Keyed hashes are commonly used to guarantee integrity—for example, HMAC-MD5 and SHA-1.

Non-repudiation guarantees that an entity cannot deny that it has performed an action. Some common techniques for providing non-repudiation are authentication combined with the logging and signing of communication content with private keys.

Privacy entails giving an entity (usually a person who is acting on his or her own behalf) the right to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information on itself with others (anonymity). Privacy is also about protecting information that might otherwise be obtained from observing network activities—for example, the websites a user has visited, a user's geographic location, calling and called telephone numbers, and the IP addresses and DNS names of devices in a service provider network. Likewise, privacy entails the filtering of unwanted or indecent information.

Security principles

Ericsson uses certain specific security principles and best practices as a basis for providing network protection. One important principle, *defense in depth*, calls for the employment of security mechanisms and security layers. If one mechanism or line of defense fails, the remaining mechanisms and lines of defense will provide adequate protection. This principle is frequently used to protect the site perimeter.

One other fundamental principle, *least*

privilege, states that entities should solely be given the privileges they need to perform their tasks. This is especially important where node protection is concerned. The services running on a node need only have the privileges that are necessary for providing the service. Moreover, the node should not run any unnecessary services.

Ericsson strongly believes in employing the *fail-safe* principle in its systems and nodes. In essence, this means that system or node failure must not allow harmful side effects. Consideration for this principle determines which features are implemented and how solutions behave.

Ericsson also recommends the *diversity-of-defense* principle, which is based on using different types of systems to provide specific kinds of protection. If one of the systems is vulnerable, for example, the other systems might be less vulnerable, thereby mitigating the overall impact of vulnerability.

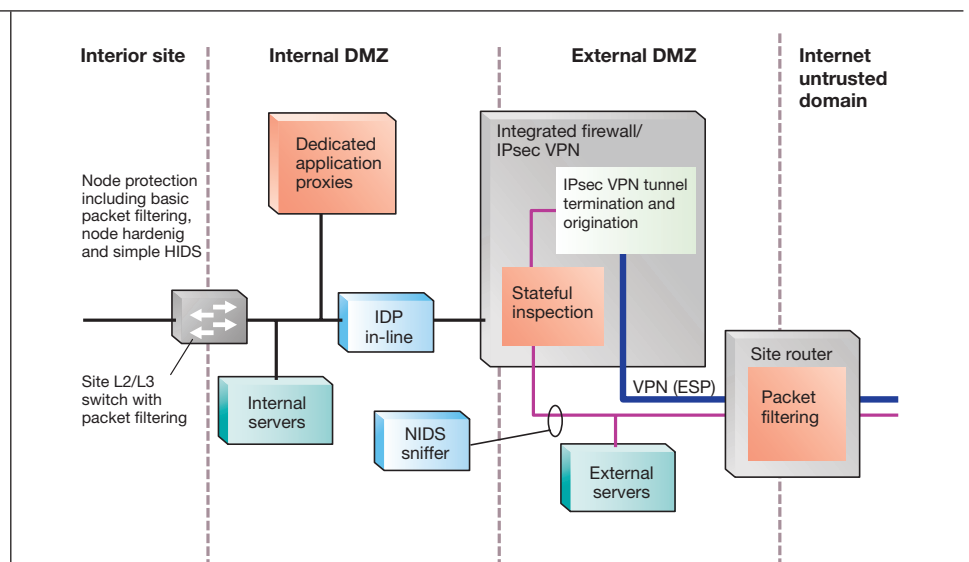
A *choke point* forces attackers to use a narrow channel that can be monitored and controlled. In network security, proper site perimeter protection constitutes a choke point. In other words, any attempt to attack the site from the outside must pass through that channel.

Implementing the security architecture

Strong site protection

Figure 5 shows a high-level view of the relevant components in an advanced security

Figure 5
Example of advanced site
perimeter protection.



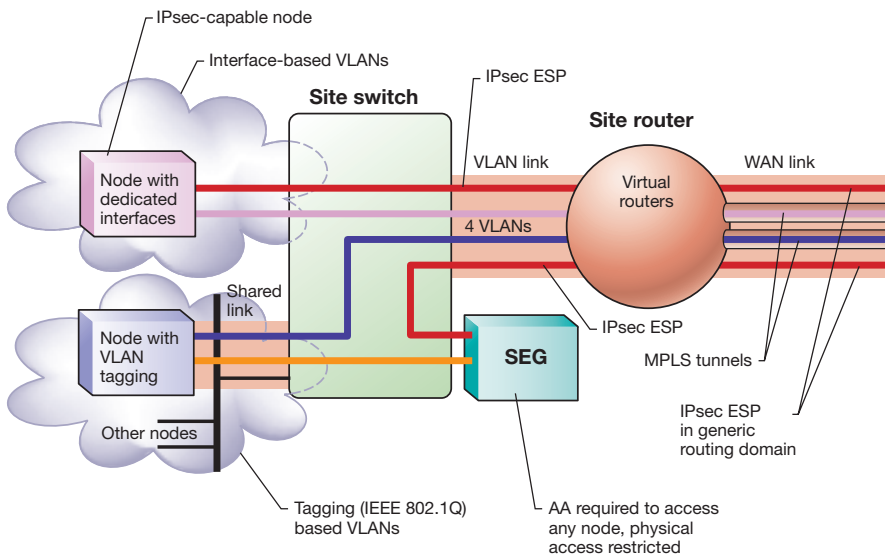


Figure 6
Example of traffic separated into VPNs.
Note: The term *IPsec ESP* denotes a tunnel—either IPsec transport mode or IPsec tunnel mode.

solution (site protection). It also depicts the basic components of node protection, such as packet filtering, node hardening and simple host-based intrusion detection systems (HIDS—file integrity checker, minimum audit logging, security alarm generation, and so forth). The figure does not illustrate fault tolerance or network resilience. In practice, high-availability configurations (duplication of routers, firewalls, security gateways, and switches that employ hot-standby or load-sharing mechanisms) are needed to avoid single points of failure. Several lines of defense from the outer shell to the core of the inner site illustrate the defense-in-depth principle.

Separation between functions and traffic types (planes/domains)

Sensitive traffic needs further protection (encryption). SCL and SFTP of the SSH protocol suite are used to protect O&M access and traffic. If SNMP and CORBA are used, then IPsec or TLS/SSL should also be used. For the best possible protection, operators might also physically separate O&M traffic from other traffic.

Traffic in the user plane should be separated from other traffic in the network. To further protect user traffic, Ericsson advises operators to employ end-to-end security mechanisms per application.

Internal architecture in nodes (layers)

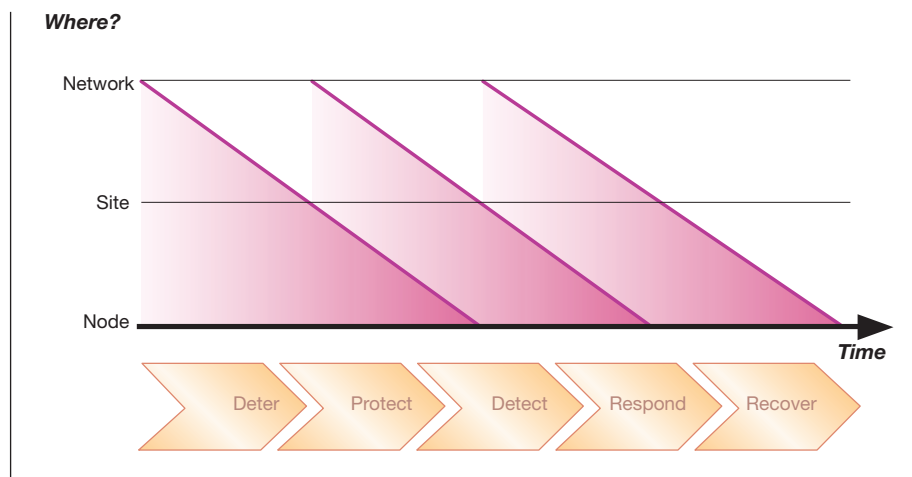
At the node level, Ericsson's system architecture is mainly reflected by separation into security planes. Within a security plane, security functions, such as per-node packet filtering, help enforce layering. This design may be repeated in the system's sub-units. The fundamental concept dictates that every available security service must be deployed to the extent required by threat or risk at every connection point where security planes and security layers communicate. Defined security policies must be enforced at these connection points (PEP).

End-user plane

Needless to say, because subscribers are the ultimate asset, operators must take adequate measures to protect them. Today, every mobile phone call is encrypted (over the air interface), but only a small percentage of e-mail messages sent over the internet are protected. Why is this? In a word, convenience. Once a subscriber has entered his personal identification number (PIN) the mobile network (via SIM/USIM) transparently handles all key management. By contrast, the average PC user is intimidated by the idea of having to install security software and certificates.

Finally, user privacy (which is already

Figure 7
Investing in security.



being driven by regulatory requirements) is becoming increasingly important and will affect the entire network. The time will soon come for true end-to-end protection of user traffic, because increasing network heterogeneity will make it impossible to trust every hop in a path. This does not in any way diminish the role of the operator or SIM card, because very convenient network-assisted key management solutions can be used in end-to-end scenarios, even when one of the end-users is a subscriber and the other is an arbitrary internet user.

Striking the right balance

The bottom line is that if the mobile network is not secure and cannot be trusted, then nobody will use it and operators will not receive any revenue. On the other hand, excessive security measures can easily have the same effect due to greater inconvenience. Moreover, the cost of developing and running a super-secure system could easily eat up all revenue. As we have argued above, security is a process. In the long run, operating expenses (network management, training of staff, and so on) will, in all likelihood, be more critical than capital expenditures.

How, then, should one invest in security? Figure 7 roughly outlines the prioritized steps of the security process. The initial priority is at the functional level—that is, protection mechanisms are given greater priority than detection mechanisms. Sim-

ply put, it makes little sense to spend huge sums of money on detection mechanisms without first adding some means of protection. Otherwise, the detection system will be overloaded. However, this does not mean that one can forget about response until detection has been added. A sprinkler system, for example, is very useful when used in combination with a smoke detector. But even without the smoke detector it can play a significant role.

Ericsson recommends that operators implement security in a layered manner, by considering network, site, and node levels. Each level requires a baseline of inherent security, but protection can also often be added outside-in, by

- strengthening defense around the network perimeter;
- adding a second line of defense at site level; and
- strengthening node and platform security.

Although OPEX is generally more an issue than CAPEX, one should not downplay the role of the supplier. Operators can obtain networking (security) products from any number of sources, but it pays to choose a supplier who understands mobile telecommunications and who can provide support for the entire lifetime of the system. Operators should also think end-to-end when addressing security, because no chain is stronger than its weakest link. Here again, there are obvious advantages to choosing a

supplier who understands and can deliver complete end-to-end solutions.

It might also pay to view investments in security as something more than a “life-vest”. Greater security can mean greater value, which in turn, often results in greater income. A sufficiently secure digital rights management (DRM) solution, for example, might spell the difference between having small or having ample amounts of content flowing in the network. Mobile phones (with SIM cards) are positioned to become a universal security and payment token.

Examples: security solution, analyses

Ericsson has developed a verified reference network design that optimally integrates its GSM and WCDMA technology with site and backbone IP infrastructure. The Mobile Packet Backbone Network (Mobile-PBN), now in its third release, integrates Ericsson’s core network products (for example, GSN, MSC, MGW) and includes optimized designs for many other integrated solution modules, such as the service network, network management center, network synchronization, and so on. Mobile-PBN, which is offered as part of Ericsson’s network design services, incorporates the security principles and services described in this article into a highly complex WCDMA/GSM network (including the service network and IPMM/EIT).

Network security design development process

From the outset, Ericsson has interwoven security into the Mobile-PBN network design development process. First, it assessed risks using a rough design template. All assets were then accounted for, and finally, related threats and the probability of related attacks were considered.

During the process, Ericsson could see that a layered approach to security would be needed to complete the task. The security of the physical layer has a direct impact on security measures at higher layers. For instance, an insecure backbone is at greater risk of attack, which puts data running over the backbone at risk.

Forming security domains

One other high-level aspect to consider when designing a secure network is parti-

tioning—that is, of dividing the network into security domains. Each domain may thus represent a part of the network with dedicated security requirements. In terms of organization, partitioning gives various user groups access to specific parts of the network. This results in a network that is split into multiple security domains.

Although security domains are kept strictly separate there is often a need to exchange data between them. In such cases, a security gateway—usually an advanced firewall product—serves as a policy enforcement point, inspecting all traffic between domains. Figure 8 depicts a network seen purely in terms of security domains.

What constitutes a security domain? The layered approach once again provides us with the answer: in the physical layer, a domain is defined by a set of physical interfaces and their interconnections—that is, physical separation is necessary to separate domains at this level. In practice, domains extending to higher layers often share the physical layer and must therefore be separated logically.

The most critical entity is the node. In reality, few nodes belong to a single security domain. Each network node or server generally has several interfaces. Some interfaces might be reserved for a single security domain (such as O&M); others might be shared using virtual interfaces. Therefore, the application level inside the node must provide the security level needed to separate security domains.

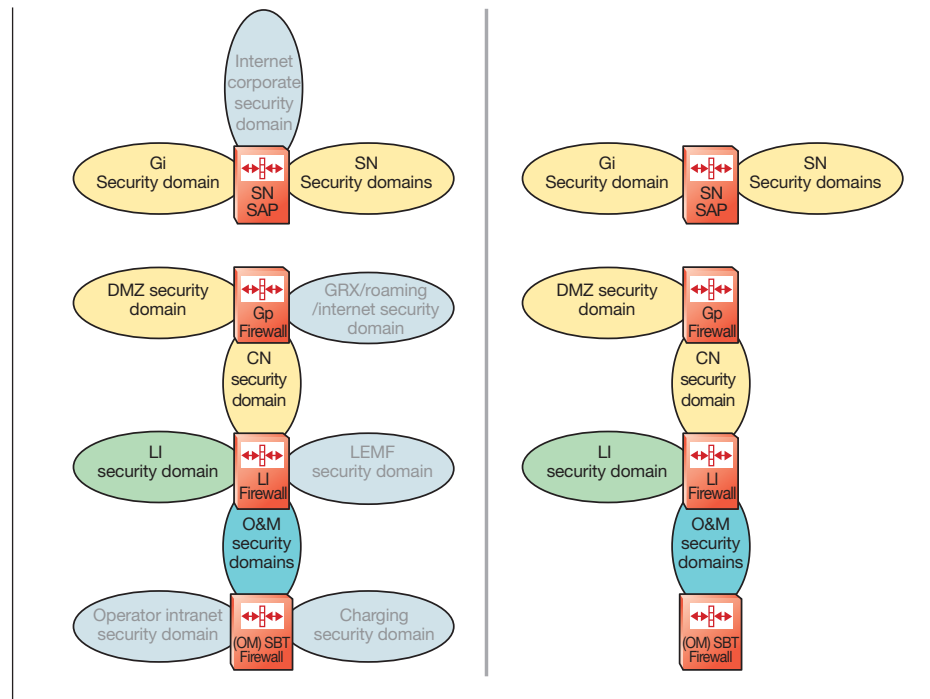
Ericsson’s Mobile-PBN solution makes extensive use of logical separation. On-site logical separation is realized using VLANs and IPsec.

Site perimeter protection

As indicated in Figure 8, a network may contain internal and external security domains. Seen in terms of the physical layer, the internal domains are domains that reside within a physically protected area that can only be accessed by authorized O&M personnel. An external security domain might reside in publicly accessible areas or protected areas to which the owner of the network does not control access. In Mobile-PBN terminology a protected area with its internal security domain is called a site. Likewise, the desirable access-control mechanism constitutes a foundation on which higher security layers can be built or added.

Physical access is based on regional char-

Figure 8
Mobile-PBN R3 security domains with and without adjacent external zones.



acteristics, such as buildings, rooms, doors, and corresponding mechanisms, such as gatekeepers or electronic devices. In Figure 9, physical site protection is depicted by a double ring around the Mobile-PBN site.

A Mobile-PBN site connected to external security domains must be protected against potential attacks from these domains. In the network layer, firewalls provide this protection.

Some external networks, such as a roaming partner, might require access to network elements within the site, whereas other networks will only use the Mobile-PBN as a transport network to other external security domains (for instance, user traffic that is being tunneled between mobile users via the Mobile-PBN network). A “demilitarized zone” is created for networks that must have access to internal network elements. The optimum solution for external security domains is to be tunneled through the Mobile-PBN is to configure the packet filter in the site router to solely allow traffic to and from the tunnel.

Secure site connection

As opposed to simple corporate networks, WCDMA and GSM networks are not restricted to a single site. Instead, they are

composed of multiple sites with various different functions. One must thus also consider another layer of security to guarantee secure transport of strictly separated data through a potentially insecure backbone.

The assignment of appropriate security services to protect data passing through the backbone is based on type or class of data. The Mobile-PBN security policy classifies information in accordance with the security reference model (Figure 3). Ericsson has based Mobile-PBN on an MPLS-enabled backbone to provide traffic separation and other non-security-related benefits. To protect sensitive data, Mobile-PBN employs confidentiality, integrity, and authentication security services over IPsec tunnels between site firewalls. In Ericsson Mobile-PBN terminology these are called secure backbone tunnel (SBT) firewalls.

Bringing it all together

As we have seen, Ericsson has given proper consideration to the physical layer, inside as well as outside sites. Mobile-PBN derives its physical access areas (site, backbone, and external) from this layer. Security domains have then been defined in the network and at higher layers. These can extend across ac-

cess areas, which is to say the classified data of a related security domain may cross the physical access layer via a network layer. Moreover, security domains may traverse multiple access areas, and a given access area may contain multiple security domains.

In summary, the security of the physical layer has direct impact on all higher layers. Let us assume for example, that a man in the middle has a physical connection to network equipment that transports sensitive data. If he possesses the “right” know-how and tools, and appropriate security service have not been applied, then he can easily tap the wire and capture data. Even worse, a malicious person in this position could replay, insert, and modify data or even bring down the entire network.

The designers of the Mobile-PBN have given due consideration to the direct relationship between physical and network security. This is expressed via a security matrix (Figure 10).

Traditionally, there have been two competing principles of security design: network-centric security design and site-centric security design. Although the focus of network-centric security design is on protecting networks it often overlooks physical impact. By contrast, the focus of site-centric security design is on protecting the site perimeter—the assumption being that everything inside the domain can be trusted. Obviously, this assumption does not work for complex GSM and WCDMA networks. Mobile-PBN brings it all together, by incorporating network- and site-centric security principles (Figure 11).

As stated above, Mobile-PBN incorpo-

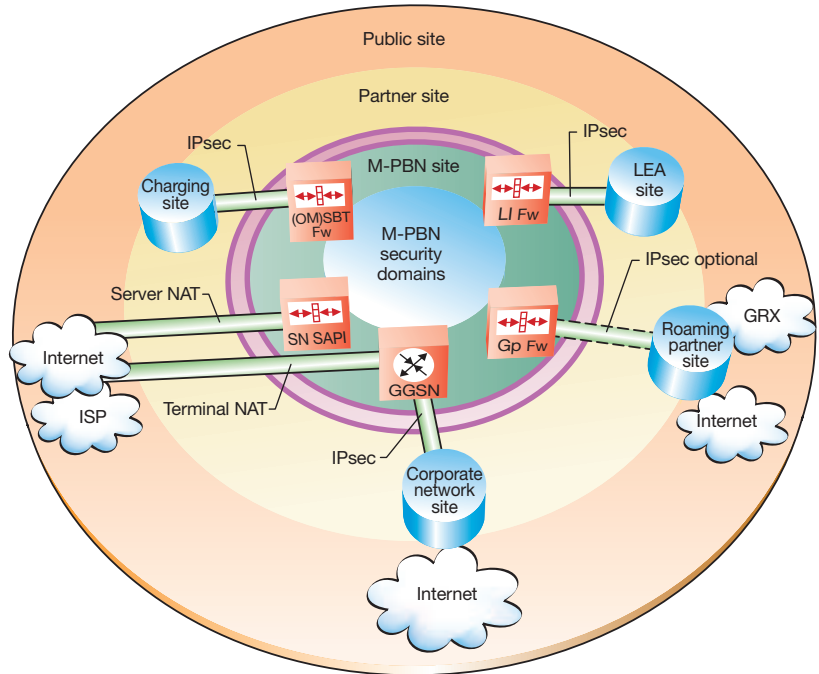


Figure 9
Mobile-PBN perimeter site protection.

rates an advanced security concept for mobile networks, based on a comprehensive security policy. This policy is realized with a consistent security solution enforced by best-of-breed security products. The Mobile-PBN security concept fits well into Ericsson’s overall security architecture and is greatly appreciated by internal and external customers alike.

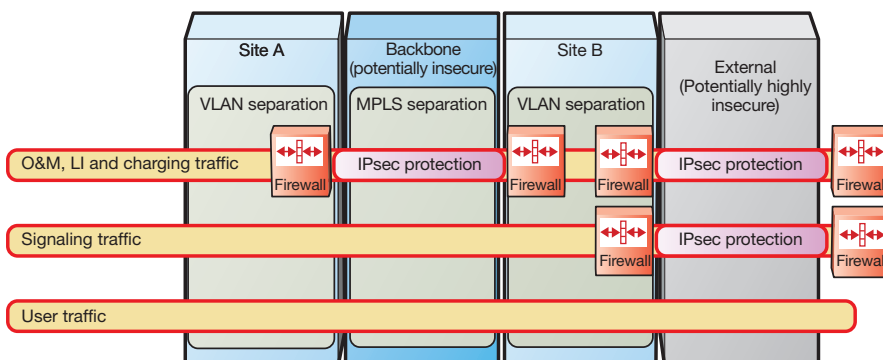


Figure 10
Mobile-PBN R3 security matrix.

Ericsson as a partner in security

Ericsson has extensive experience of fixed and mobile telecommunications and has been a major driver of standardization for third-generation mobile networks. In particular, Ericsson has gone to great lengths to drive security-related standardization in 3GPP, IETF, and other standards bodies. Ericsson also complies with and monitors regulatory bodies to guarantee that the functionality of its products supports regulations concerning end-user privacy.

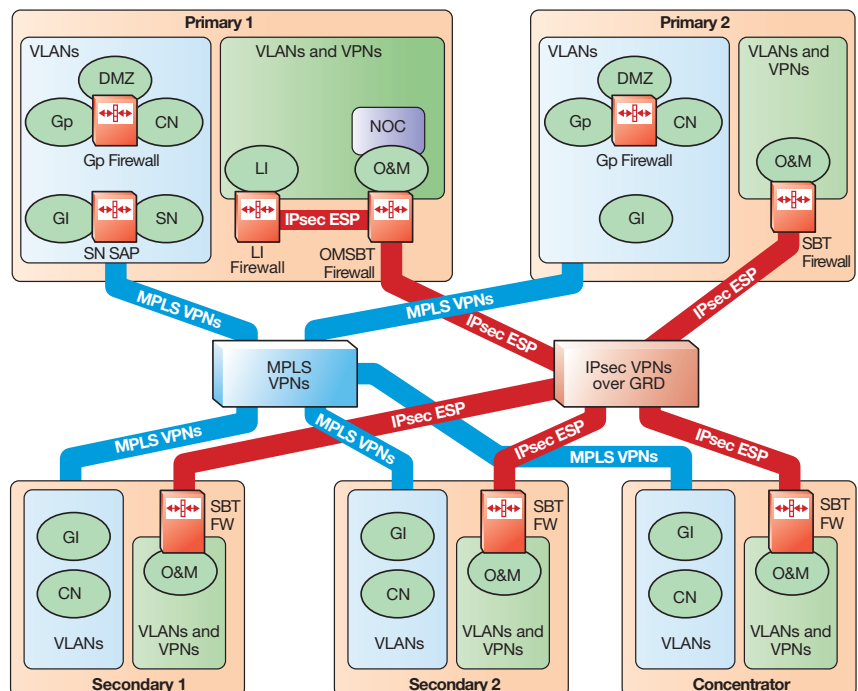
Ericsson's implementation of security in its product offerings begins with basic inherent security in nodes. Its design and implementation are based on best-practices concerning virtually every detail including choice of pseudo-random number generators and choice of locks on cabinet doors. When applicable, Ericsson partners with leading suppliers of security technologies, such as firewalls and intrusion-detection systems, to give its customers technology that has been adapted to the special needs of

mobile networks. Ericsson is committed to provide efficient customer support as needed via software updates, security patches, and so on. Ericsson has coordinated its product portfolio to provide a uniform, easy-to-manage and cost-effective security architecture that yields carrier-grade security. To ensure that the right security solutions are developed for post-3G mobile networks, Ericsson is also actively participating in, and is the driving force behind, a number of research projects in the Fifth and Sixth Framework Programs of the European Union.

Security topics beyond 3G—identity and trust management

A sound approach to security architecture must consider changes in society, technology, network architecture, and the emerging business and role models of various players. It is thus interesting to contemplate what mobile networks might look like in, say, ten years.

Figure 11
Mobile-PBN R3 approach to security design:
distributed security domains.



One thing we can expect to see more of is specialization, as players tend to optimize their business in a narrower niche. New participants, such as providers of content, identity, trust, and payment, will be increasingly interested in mobile clients. This, in turn, will affect basic trust models. Other trends, seen in terms of technology, are new (high-speed) access, and personal area networks. Social aspects might also play a role. User communities, for instance, might want to create private overlay networks. In summary, we might very well have a scenario such as that depicted in Figure 12.

What role does the operator have in this model and what are the needs for security? Services that guarantee end-user privacy, security and trust, coupled with convenience. Greater fragmentation implies that users will find security and convenience in having a trust-anchor that manages ID, authentication, secure payments, and so on. Operators can also provide end-users with greater territorial privacy, by filtering out spam and unwanted content.

We cannot stress the convenience aspect enough. Thanks to SIM cards, end-users with a mobile subscription need not configure security. Compare this to the challenge most end-users face when trying to make e-mail secure on a PC. This is why the majority of e-mail traffic is completely unprotected. Where security and private services are concerned, the full potential of SIM cards and mobile terminals is far from exhausted. In principle, network-assisted, end-to-end protection can also be based on SIM cards. Indeed, this might become a requirement in the near future, given the heterogeneity of "beyond 3G" (B3G) networks and the impact they have on trust models.

From the network point of view, greater focus must be put on security domains. There is a need for strong policy enforcement at domain edges and intrinsic infrastructure security at site, node and platform levels.

Conclusion

Regardless of how complex mobile networks become, the issue of security should always be approached and managed in a structured and uniform way. Otherwise, gaping holes are left in a patchwork of non-interoperable solutions that are difficult as well as expensive to operate.

Likewise, investments in security should follow a balanced, well-thought-out plan. In

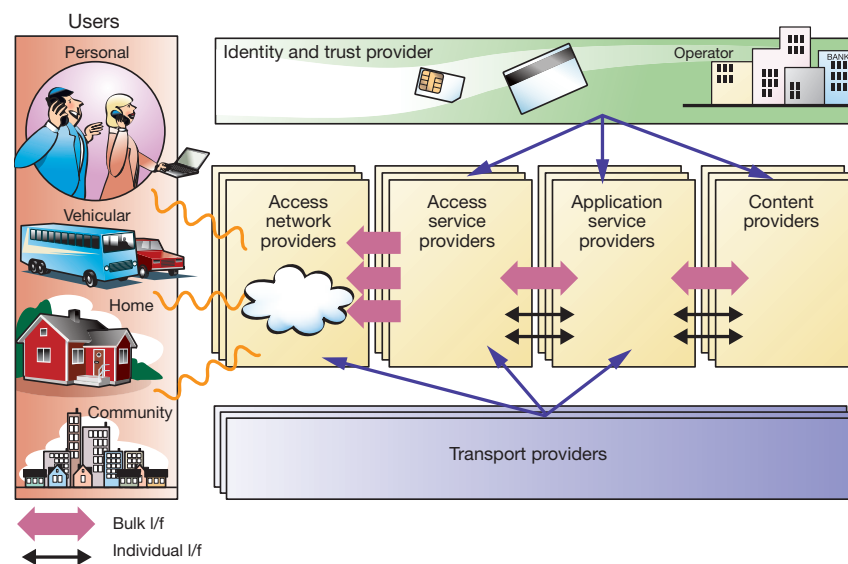


Figure 12
Future mobile network scenario.

this context, choice of supplier is very important, because only a total system supplier can truly understand the telecommunications business and offer life-cycle support for uniform, easy-to-manage, end-to-end solutions with the right balance between cost and security.

Ericsson is a firm believer in resolving security issues through standardization, not just to guarantee homogeneity, but also to ensure that emerging security standards give proper consideration for the mobile and wireless aspects of data- and telecommunications.

REFERENCES

- 1 Stewart Kowalski, Mariné Boden, Value Based Risk Analysis: The Key to Successful Commercial Security Target for the Telecom Industry, 2nd Annual International Common Criteria CC Conference Ottawa 2002, <http://www.icc-conference.com>
- 2 Ahonen et al: Taking Security Beyond 3G, Contribution to the 7th WWRF Meeting, Eindhoven, The Netherlands, December 3-4, 2002.
- 3 September 11, 2001: Infrastructure Impacts, Implications, and Recommendations; Yankee Group Special Report; September 19, 2001.
- 4 EU Council Resolution on Network and Information Security 2002/C 43/02.
- 5 EU directive 2002/58/EC.
- 6 The Three Phases of Security: Product, Pervasive, and Persistence; Yankee Group; June 17, 2003.
- 7 To serve and protect: Operator strategies for selling security; Strategy Analytics Industry Report; July 2001.
- 8 Wireless spam could cost operators USD 2 billion per annum; Strategy Analytics Insight; August 22, 2002.
- 9 Sue Uglow, Structuring for survival: Strategies for telecoms players, Ovum Report, April 2002
- 10 US (Ca) Database Security Breach Notification Act, of July 1, 2003.
- 11 Ambient Networks, <http://www.ambient-networks.org/>
- 12 ITU-T recommendation X.805, Security architecture for systems providing end-to-end communications