Bell Labs Network Security Framework

A methodology for assessing, planning, managing and maintaining secure computer and telecommunications networks

In today's IP-based communications world, the challenge of building, operating and maintaining safe, reliable communications networks is more critical – and more complex – than ever before.

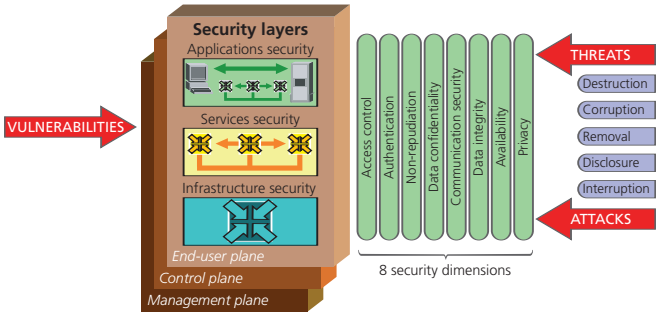
Lucent Technologies
Bell Labs Innovations

The IP architecture of next-generation communications is inherently less secure and reliable than a closed-circuit switched telephony network, but the services that IP networks carry are every bit as mission-critical to today's businesses and users.

According to the U.S. Federal Bureau of Investigation (FBI), the global cost of cyber attacks was $400 billion in 2005. And security threats continue to rise globally – up 22 percent in 2005.

The risk of unsecured networks is significant, not just to devices such as computers and mobile phones, but also to the critical infrastructure of nations around the world. An attack or natural disaster that takes down a network infrastructure can not only cripple businesses and economies, but also put people's lives at risk.

The **Bell Labs Network Security Framework**, now the basis for both the International Telecommunications Union (ITU) X.805 standard and an ISO (International Organization for Standardization) 18028-2 standard, is an end-to-end methodology for assessing, planning, managing and maintaining secure computer and telecommunications networks. This model is a holistic approach that provides vendor- and technology-agnostic guidelines for wireless, optical and wireline voice, data and converged networks.



This figure depicts the concept of protecting a network by security dimensions at each security plane of each security layer in order to provide a comprehensive security solution. It should be noted that, depending on a given network's security requirements, it might not be necessary to have all architectural elements implemented or to have a complete set of the security dimensions, security layers and security planes.

Holistic Security Architecture

Bell Labs' security framework provides a systematic, comprehensive, multi-layered, end-to-end model that addresses the critical challenges for ensuring network security. It fills a void in existing security standards by providing a holistic network security architecture that is applicable to end users, as well as the management and control/signaling infrastructures, services and applications.

The framework comprises a total of 72 security perspectives – three layers used across three planes through eight dimensions. The three key security components of the framework are:

- The **security dimensions** are a set of security measures designed to address a particular aspect of the network security. The Bell Labs model encompasses eight dimensions that protect against all major security threats. These dimensions are not limited to the network, but extend to applications and end user information as well. In addition, the security dimensions apply to service providers or enterprises offering security services to their customers.
- The **security layers** are a series of enablers for secure network solutions; the infrastructure layer enables the services layer, which then enables the applications layer. The Bell Labs Network Security Framework addresses the fact that each layer has different security vulnerabilities and has the flexibility to counter potential threats in a way best suited for each security layer.
- The **security planes** cover a certain type of network activity protected by security dimensions. The security planes addressed in the Bell Labs model are the management plane, the control plane and the end-user plane. These security planes cover network management activities such as network control or signaling activities and end-user activities.

The framework can be applied in its entirety or on an as-needed basis to any or all aspects and phases of a successful security program, including:

- **Definition and Planning:** define comprehensive security policies, incident response and recovery plans, technology architectures and technical requirements;
- **Implementation:** assess how security policies and procedures are rolled out and technology is deployed;
- **Maintenance and Health Check:** manage and assess routine changes in architecture, network equipment, security policies and procedures, incident response and recovery plans.

Multiple Dimensions

The ITU-T X.800 series of recommendations identified five major threats to telecommunications networks, including:

- Destruction of information and/or resources;
- Corruption or modification of information;
- Removal, theft or loss of information and/or resources;
- Disclosure of information; and
- Interruption of services.

The Bell Labs Network Security Framework methodically addresses all of these threats by defining eight basic dimensions, extending beyond the network to include applications and end users, which must be protected.

- **Access management** or **access control** protects against unauthorized use of network resources;
- **Authentication** confirms the identities of each entity using the network;
- **Non-repudiation** proves the origin of the data or identifies the cause of an event or action;
- **Data confidentiality** or **data security** ensures that data is not disclosed to unauthorized users;
- **Communication security** allows information to flow only between authorized endpoints;
- **Data integrity** ensures the accuracy of data so it cannot be modified, deleted, created or replicated without authorization, and also provides an indication of unauthorized attempts to change data;
- **Availability** ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to network-impacting events;
- **Privacy** provides for the protection of information that could be derived from the observation of network activities.

Planes and Layers

To obtain a full picture of the network, the Bell Labs Network Security Framework looks at the types of activities that take place in a network and categorizes them in one of three planes:

- The **management plane** facilitates the operations, administration, maintenance and provisioning (OAM&P) of network elements, transmission facilities, back-office systems such as operations support, business support and customer care, and data centers.
- The **control plane** enables efficient delivery of information, services and applications across the network.
- The **end user plane** allows customers to access and use a service provider's network. This plane also represents actual end-user data flows.

The framework also defines three discrete network layers:

- The **infrastructure layer** includes network transmission facilities as well as individual network elements and hardware platforms, which include hardware and software for each network element and platform.
- The **services layer** comprises all of the services users receive from their service providers.
- The **applications layer** includes network-based applications accessed by service provider customers as well as end-user applications that require network services.

By applying all eight dimensions across the three planes and through each of the three layers, the model can provide a comprehensive, top-down, end-to-end perspective on network security. It also can be applied widely to network elements, services and applications which is critically important in preventing, detecting and responding to threats and vulnerabilities.

Continuous Process

Bell Labs is using this framework to help businesses, government agencies and service providers evaluate the safety of their networks and build plans to protect themselves against attacks and disasters. It can be used over the entire lifetime of a network security program, assisting in the development of policies and requirements as well as forming the basis for periodic assessments.

In addition, the framework can help combat network security threats and potentially save millions of dollars in security vulnerabilities by identifying the security investments that can drive more efficiency into the supply chain and thereby lower costs and raise productivity.

Maintaining a secure network is a continuous process. A well defined security architecture such as the Bell Labs Network Security Framework is an essential tool for providing an orderly, systematic methodology and set of guidelines for network managers faced with managing the day-to-day requirements that protect users, information and the network itself.

To learn more about our comprehensive portfolio, please contact your Lucent Technologies Sales Representative or visit our web site at http://www.lucent.com.

SecurityFramework v1.0806

Lucent Technologies
Bell Labs Innovations