Role of Policy in Securing the National Infrastructure

P K Singh DDG (SA) DoT

What is a Security Policy ?

- Standard Based Definitions
- A security policy is a written document in an organization outlining how to protect the organization from threats, including computer security threats, and how to handle situations when they do occur. A security policy must identify all of a company's assets as well as all the potential threats to those assets. Company employees need to be kept updated on the company's security policies. The policies themselves should be updated regularly as well
- The policy contains the Security requirements which are both generic and context-specific. In addition, some requirements are well established while others continue to evolve with new applications and the evolving threat environment
- It makes use of tools, personnel, security concepts, security safeguards, guidelines, risk identification & management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, the organization and the user's assets”
- The security policy translates the security goals into organizational processes, high-level and detailed technical security requirements. The technical security policy drives the security life-cycle and the implementation of security across the system/solution life-cycle
- It also takes into account the Government’s requirement into considerations

What is meant by Secure ?

- The Recommendation ITU-T X.805 architecture is defined in terms of three major concepts, security layers, planes, and dimensions, for an end-to-end network. A hierarchical approach is taken in dividing the security requirements across the layers and planes so that the end-to-end security is achieved by designing security measures in each of the dimensions to address the specific threats

- In order to provide an end-to-end security solution, the security dimensions must be applied to a hierarchy of network equipment and facility groupings, which are referred to as *security layers* namely *Infrastructure* layer, *Services* layer and *Applications* layer

- A *security plane* represents a certain type of network activity protected by security dimensions namely Management Plane, Control Plane and User

- A Security Dimension is a set of security measures designed to address a particular aspect of Network Security. Basic security services (authentication, access control, data confidentiality, data integrity , non-repudiation, Communication Security, Availability and Privacy) along with more general (pervasive) services such as trusted functionality, event detection, security audit, and security recovery.

- The dimensions offer additional network protection and protect against all major security threats. These dimensions are not limited to the network, but also extend to applications, processes, information including end-user information.

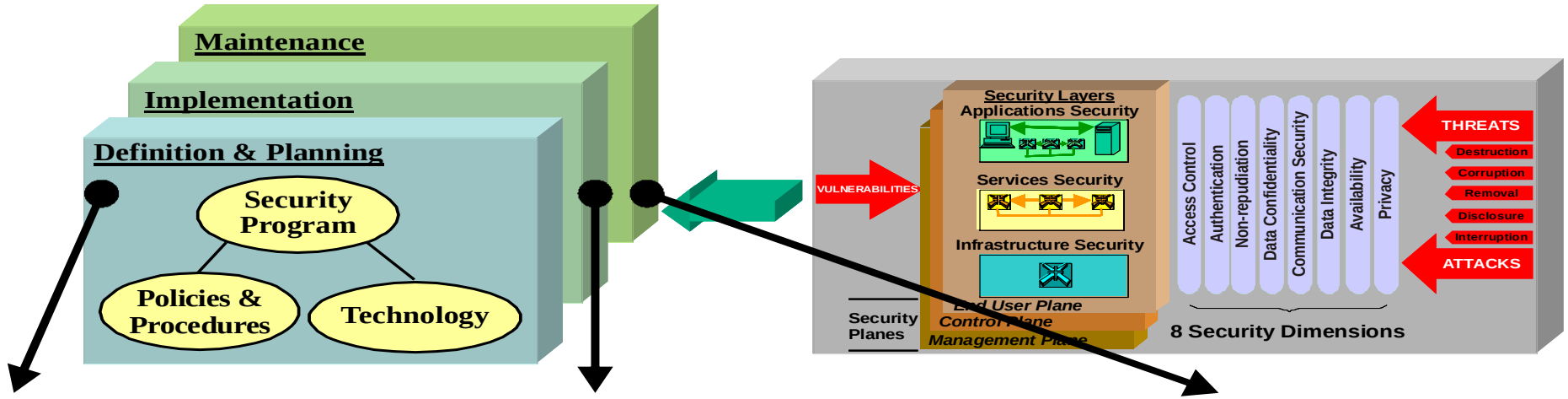
Objectives of Security Policy

- Access to, and use of networks and services should be restricted to authorized users;
- Authorized users should be able to access and operate on assets they are authorized to access;
- Networks should support confidentiality to the level prescribed in the network security policies;
- All network entities should be held accountable for their own, but only their own, actions;
- Networks should be protected against unsolicited access and unauthorized operations;
- Security-related information should be available via the network, but only to authorized users;
- Plans should be in place to address how security incidents are to be handled;
- Procedures should be in place to restore normal operation following detection of a security breach; and
- The network architecture should be able to support different security policies and security mechanisms of different strengths.

Objectives of Security Policy Contd..

- protect assets for:
  - customers/subscribers who need confidence in the network and the services offered, including availability of services (especially emergency services);
  - public community/authorities who demand security by directives and/or legislation, in order to ensure availability of services, privacy protection, and fair competition;
  - network operators and service providers who need security to safeguard their operation and business interests and to meet their obligations to customers, their business partners and the public.
- The assets to be protected include:
  - communication and computing services;
  - information and data, including software and data relating to security services;
  - personnel; and
  - equipment and facilities.

Network Security Life Cycle



Definition & planning

Inputs: Business & security objectives, Regulatory & policy specifications, Architecture, Threats

Gap analysis: Compare security objectives, and threats to planned features.

Results: Recommendations to fix gaps, policy compliance

Design & Implementation

Inputs: Product security requirements, technology security practices, design specifications, Threat analysis, Security assets

Gap analysis: Compare results from phase 1, Implemented security features, threat analysis and testing

Results: Security asset identification, vulnerability management, security design compliance and verification, feedback to development process

Deployment & Maintenance

Inputs: Threat & vulnerability management results & updates, Technology and operational security practices, regulatory guidelines

Gap analysis: Compare inputs with product security & operations requirements.

Results: Updated security base line, Feedback to development process

Importance of Security Policy

- A common approach leads to shared understanding and interoperability in multi-supplier networks
- An identification of hierarchical assets and what is needed to protect them
- A consistent way to look at threats, vulnerabilities for products, regardless of technology
- A systematic analysis assures efficient coverage of network security
- A requirement of Network Forensic after breach/incident detection
- Network and restoration & Resilience in case of a disruption
- Ensure the deployment of Secure product after ensuring the supply chain security and testing and certification
- Preventing Remote Access to critical network elements at the same time ensuring the access for proper operations

Thank you