Network Security Workshop

In conjunction with SANOG25 – Kandy, Sri Lanka

Hosted by LEARN

Presenters

- Champika Wijayatunga – ICANN
- Fakrul Alam (Pappu) – bdHUB
- Yoshinobu Matsuzaki (Maz) – IIJ
- Sheryl Hermoso (Shane) – APNIC
- Amila Bhagya Perera – TechCERT
- Nalinda Herath – TechCERT

SANOG

Agenda

- Day 1
  - Network Security Fundamentals
  - Asset & Threats Models
  - Security in Layers and Attack Mitigation
  - Threat Pragmatics, Cryptography Basics
  - Cryptography Applications / SSH & Two Factor Authentication [LAB]

Agenda

- Day 2
  - Cryptography Applications / PGP [Lab]
  - Securing NW Infra, Router and switch protection
  - Route Filtering
  - TLS/SSL [Lab]

Agenda

- Day 3
  - Incident Verifications
  - Network Forensics Essentials
  - CSIRT Update

SANOG

Agenda

- Day 4
  - RPKI (including demo)
  - IPSEC
  - DNS Security
  - DNSSEC

SANOG

Agenda

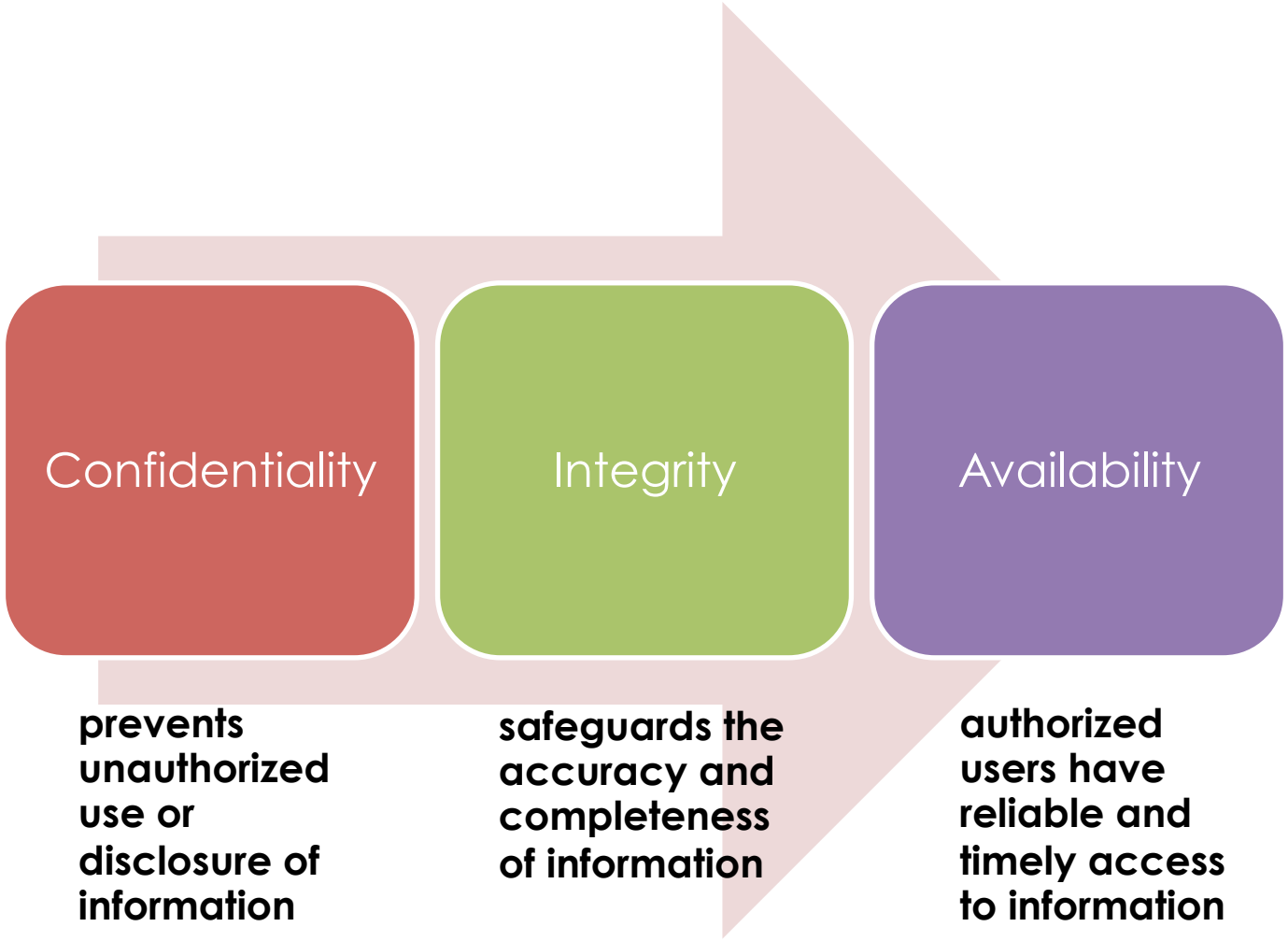
- Day 5
  - DNSSEC (lab)
  - SNORT
  - Wireshark [Lab]

Network Security Fundamentals

Why Security?

- The Internet was initially designed for connectivity
  - Trust assumed
  - We do more with the Internet nowadays
  - Security protocols are added on top of the TCP/IP
- Fundamental aspects of information must be protected
  - Confidential data
  - Employee information
  - Business models
  - Protect identity and resources
- We can't keep ourselves isolated from the Internet
  - Most business communications are done online
  - We provide online services
  - We get services from third-party organizations online

Goals of Information Security



Access Control

- The ability to permit or deny the use of an object by a subject.
- It provides 3 essential services:
  - Authentication (who can login)
  - Authorization (what authorized users can do)
  - Accountability (identifies what a user did)

Authentication

- A means to verify or prove a user's identity
- The term "user" may refer to:
  - Person
  - Application or process
  - Machine or device
- Identification comes before authentication
  - Provide username to establish user's identity
- To prove identity, a user must present either of the following:
  - What you know (passwords, passphrase, PIN)
  - What you have (token, smart cards, passcodes, RFID)
  - Who you are (biometrics such as fingerprints and iris scan, signature or voice)

Two-factor Authentication

- Requires a user to provide at least two authentication 'factors' to prove his identity
  - something you know

  Username/userID and password
  - something you have

  Token using a one-time password (OTP)
- The OTP is generated using a small electronic device in physical possession of the user
  - Different OTP generated each time and expires after some time
  - An alternative way is through applications installed on your mobile device
- Multi-factor authentication is also common

Authorization

- Defines the user's rights and permissions on a system
- Typically done after user has been authenticated
- Grants a user access to a particular resource and what actions he is permitted to perform on that resource
- Access criteria based on the level of trust:
  - Roles
  - Groups
  - Location
  - Time
  - Transaction type

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity
  - Senders cannot deny sending information
  - Receivers cannot deny receiving it
  - Users cannot deny performing a certain action
- Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention and after-action recovery and legal action

Source: NIST Risk Management Guide
Technology Systems

Integrity

- Security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity
- Data integrity
  - The property that data has when it has not been altered in an unauthorized manner
- System integrity
  - The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation

Source: NIST Risk Management G
Technology Systems

Threat

- “a motivated, capable adversary”
- Examples:
  - Human Threats
    - Intentional or unintentional
    - Malicious or benign
  - Natural Threats
    - Earthquakes, tornadoes, floods, landslides
  - Environmental Threats
    - Long-term power failure, pollution, liquid leakage

Vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
  - Software bugs
  - Configuration mistakes
  - Network design flaw
  - Lack of encryption
- Where to check for vulnerabilities?
- Exploit
  - Taking advantage of a vulnerability

Risk

- Likelihood that a vulnerability will be exploited
- Some questions:
  - How likely is it to happen?
  - What is the level of risk if we decide to do nothing?
  - Will it result in data loss?
  - What is the impact on the reputation of the company?
- Categories:
  - High, medium or low risk

What are Security practices?

- Controlling Data Access
- Controlling Network Access
- Protecting Information in Transit
- Ensuring Network Availability
- Preventing Intrusions
- Responding To Incidences

Why Worry About Security?

- How much you worry depends on risk assessment analysis
  - Risk analysis: the process of identifying security risks, determining their impact, and identifying areas requiring protection
- Must compare need to protect asset with implementation costs
- Define an effective security policy with incident handling procedures

Characteristics of a Good Policy

- Can it be implemented technically?
- Are you able to implement it organizationally?
- Can you enforce it with security tools and/or sanctions?
- Does it clearly define areas of responsibility for the users, administrators, and management?
- Is it flexible and adaptable to changing environments?

RFC 2916 - http://www.ietf.org/rfc/rfc2196.txt

Attack Sources

- Active vs. passive
  - Active involves writing data to the network. It is common to disguise one's address and conceal the identity of the traffic sender.
  - Passive involves only reading data on the network. Its purpose is breach of confidentiality. This is possible if:
    - Attacker has gained control of a host in the communication path between two victim machines
    - Attacker has compromised the routing infrastructure to arrange the traffic pass through a compromised machine

Active Attacks	Passive Attacks
Denial of Service attacks	Reconnaissance
Spoofing	Eavesdropping
Man in the Middle	Port scanning
ARP poisoning	
Smurf attacks	
Buffer overflow	
SQL Injection	

General Threats

- Masquerade
  - An entity claims to be another entity
- Eavesdropping
  - An entity reads information it is not intended to read
- Authorization violation
  - An entity uses a service or resource it is not intended to use
- Loss or modification of information
  - Data is being altered or destroyed
- Denial of communication acts (repudiation)
  - An entity falsely denies its participation in a communication act
- Forgery of information
  - An entity creates new information in the name of another entity
- Sabotage
  - Any action that aims to reduce the availability and/or correct functioning of services or systems

Mistakes IT People Make

- Connecting systems to the Internet before hardening them.
- Connecting test systems to the Internet with default accounts/passwords
- Failing to update systems when security holes are found
- Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI
- Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated
- Failing to maintain and test backups
- Running unnecessary services : ftpd, telnetd, finger, rpc, mail, rservices
- Implementing firewalls with rules that don't stop malicious or dangerous traffic - incoming and outgoing
- Failing to implement or update virus detection software
- Failing to educate users on what to look for and what to do when they see a potential security problem

Questions?

SANOG