SECURITY METRICS AND TRUSTED SYSTEMS

Measurements and metrics

- Measure: A pure number
- Metric: A ratio of two or more related measures.
- Measurement is defined as the process of assigning symbols, usually numbers, to represent an attribute of the entity, by rule.
- Metrics are the means of interpretation for the collected data.
- A metric is defined as a standard of measurement using quantitative, statistical or mathematical analysis.

Security metrics

- **Measuring security** is an important discipline in order to understand whether your security posture is improving or degrading and to understand if your security programs are having the desired effect.
- **Infosec metric** is the application of quantitative, statistical or mathematical analysis to measure infosec functional trends and workload.
- Metrics enable continuous improvement.

Security metrics classification

- Security metrics model consists of 3 components:
  - The object being measured
  - The security objectives
  - The method of measurement

Security objectives

- Security objectives are divided into:
  - Security requirements such as specifications, standards and control objectives and common criteria
  - Best practices
  - Security baselines
  - Security management based on experience
  - Maturity models such as SSE-CMM and Infosec assurance capability maturity model (IA-CMM).

Methods of measurement

- Methods of measurement include the following:
  - Direct testing
  - Evaluation
  - Assessment
  - Training/education/level of competence
  - Observation of system performance

Types of security metrics

- Different types of security metrics that organizations can focus on can be:
  - Business impact
    - Business value gained/lost
    - Acceptable loss estimate
  - Program Results
    - Timeliness of security service delivery
    - Operational results
  - Process implementation
    - Level of implementation
    - Implementation totality

Why security metrics are important

- Identifying key risks within the organization
- Targeting remediation/mitigation action
- Measuring internal compliance with organizational policy
- Discovering internal process breakdown
- Taking advantage of security related sunk costs

Security models

- Bell-LaPadula model
  - Confidentiality
- Biba model
  - Integrity
- Clark Wilson model
  - Integrity

Terminology

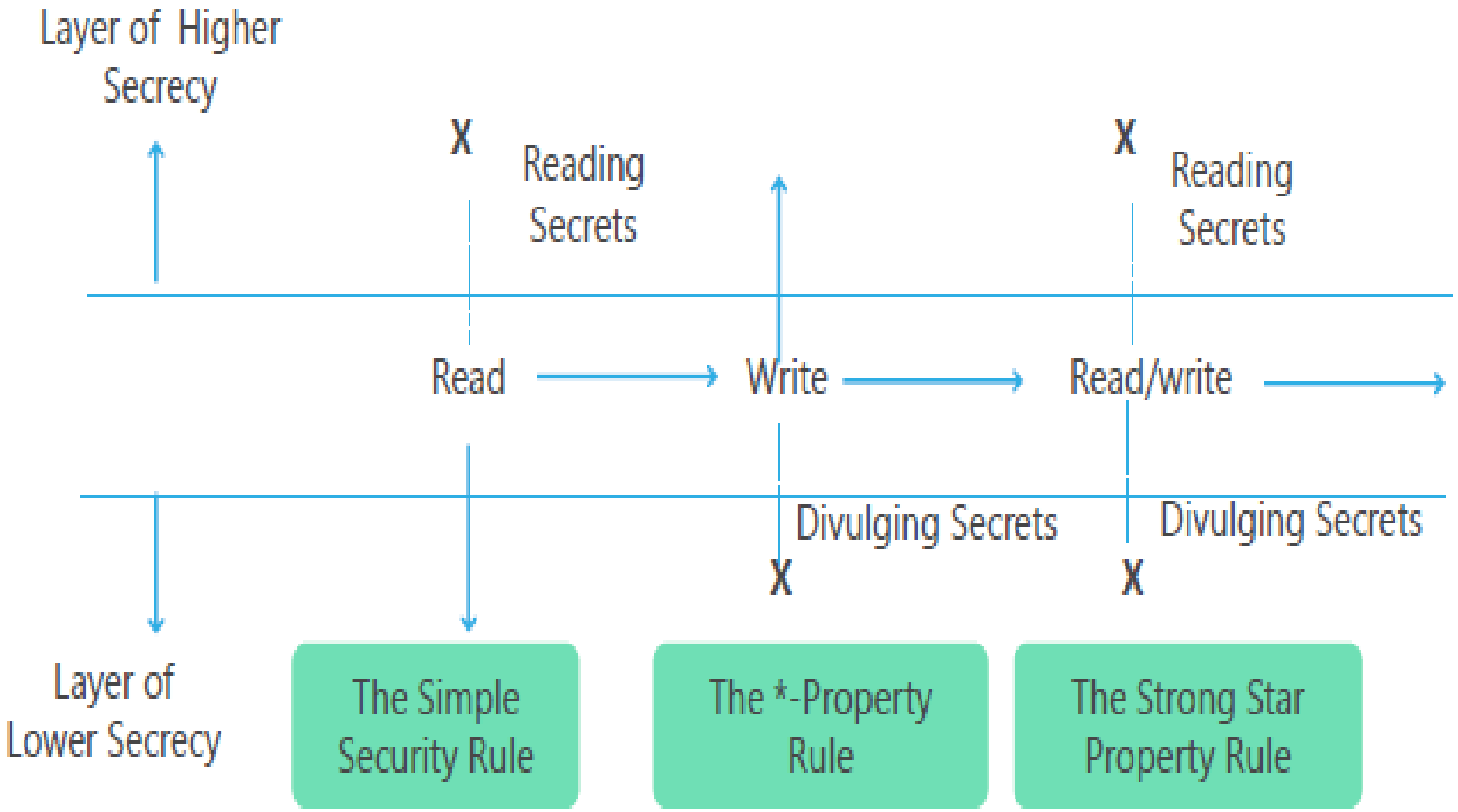
- Subjects
  - Subjects are active
  - Eg: Users/ Programs
- Objects
  - Objects are passive
  - Eg: Files

Bell-LaPadula Model

Bell–LaPadula Confidentiality Model is focused on maintaining the confidentiality of objects.

It includes the following rules and properties:

- The simple security rule—A subject cannot read data at a higher security level (no read up)
- The *-property rule—A subject cannot write data to an object at a lower security level (no write down)
- The strong star property rule—A subject can perform read and write functions only to the objects at its same security level


Layer of Higher Secrecy
X
Reading Secrets
X
Reading Secrets
Read
Write
Read/write
Divulging Secrets
Divulging Secrets
X
X
Layer of Lower Secrecy
The Simple Security Rule
The *-Property Rule
The Strong Star Property Rule

Biba model

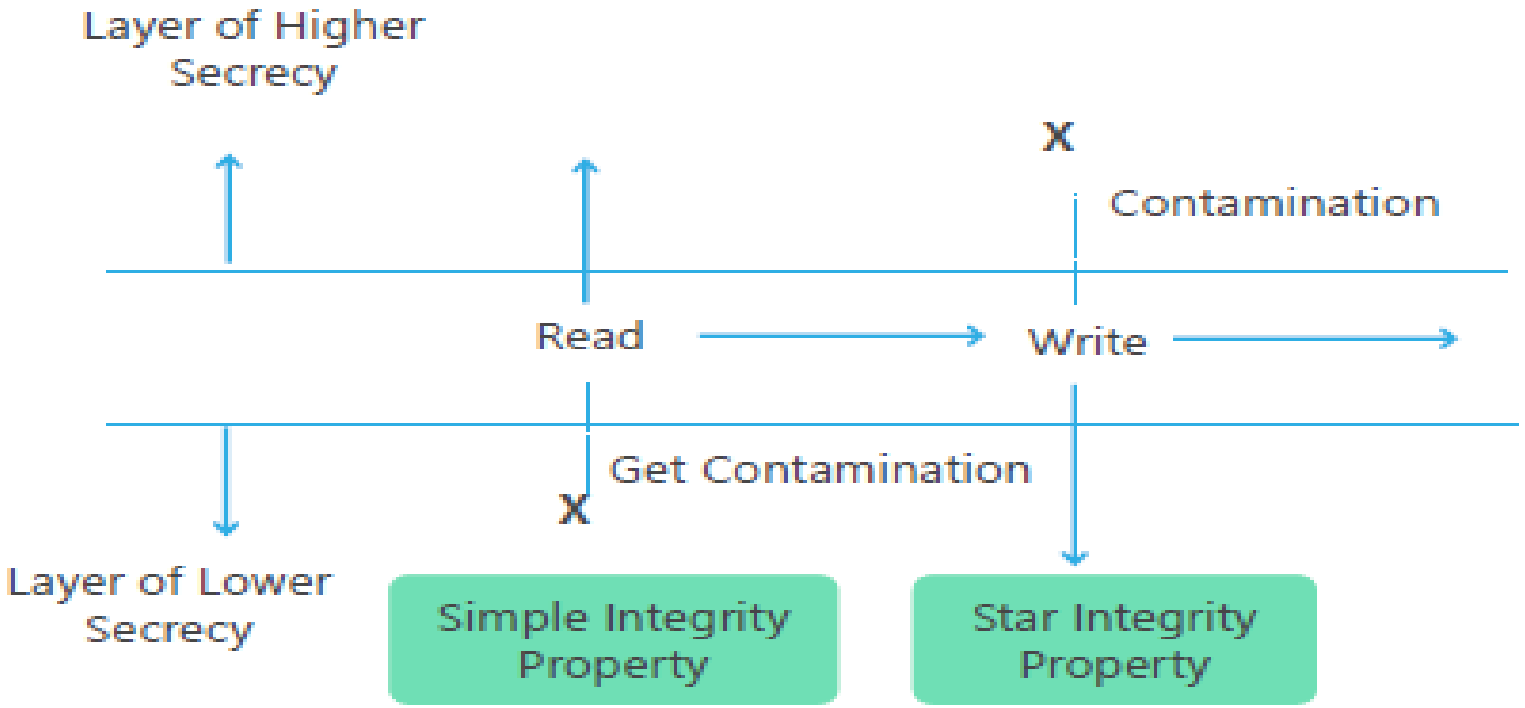
The Biba Integrity Model protects the integrity of the information and the activities that take place within a system. The following are the axioms of Biba integrity model:

The Simple Integrity Axiom

- It states that a subject cannot read data at a lower integrity level or in no read down.
- It means that a subject cannot read documents below its level. This is called no read down, or NRD (read as N-R-D).

The Star Integrity Axiom

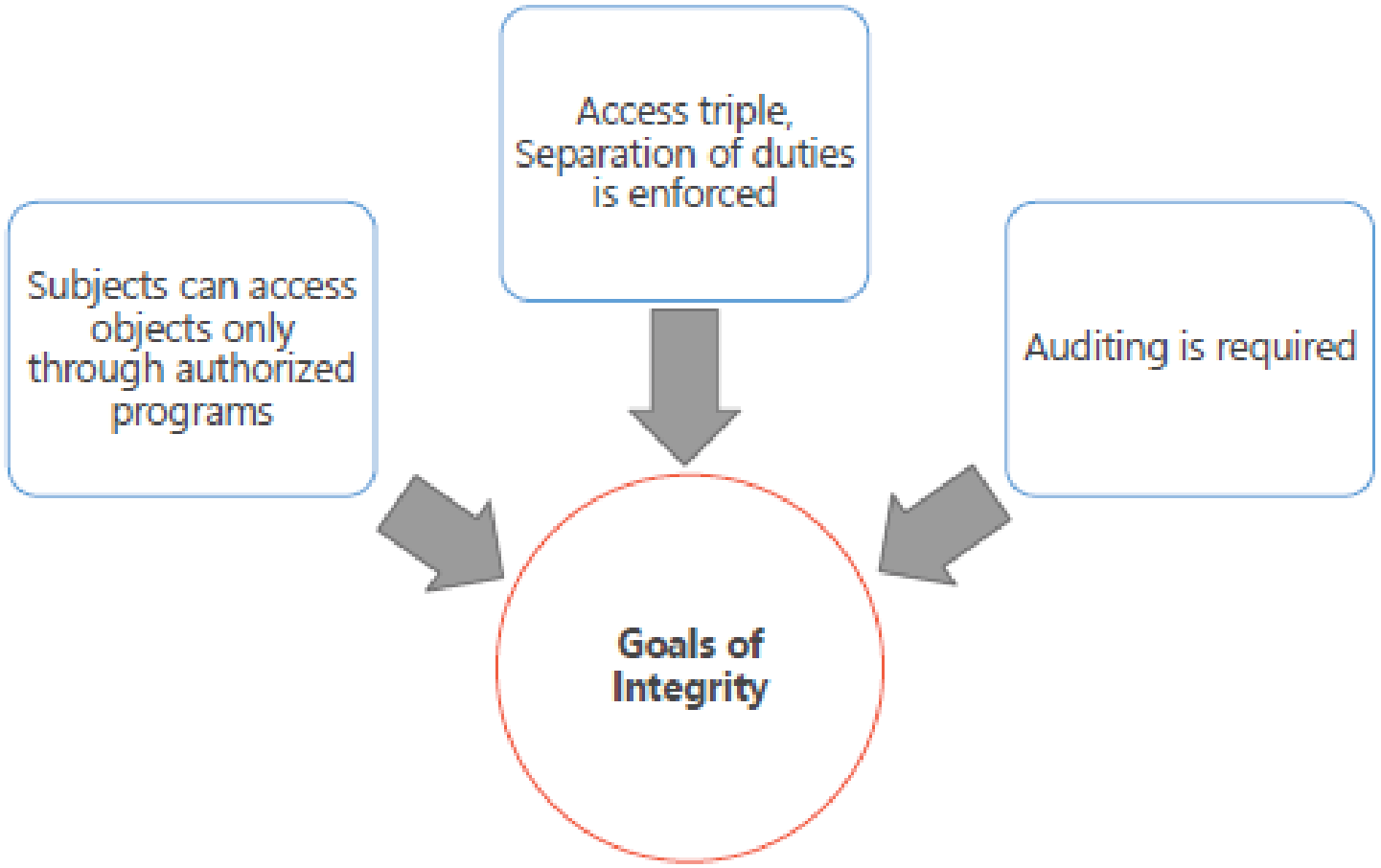
- It states that a subject cannot modify an object in a higher integrity level.
- This is called no write-up, or NWU (read as N-W-U).


Layer of Higher Secrecy
X
Contamination
Read
Write
Get Contamination
X
Layer of Lower Secrecy
Simple Integrity Property
Star Integrity Property

Clark Wilson Model

The Clark–Wilson model focuses on integrity at the transaction level and addresses the three major goals of integrity in a commercial environment.

- It provides a foundation for specifying and analyzing an integrity policy for a computing system.
- Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent.
- An integrity policy describes how the data items in the system should be kept valid from one state of the system to the next.


Access triple, Separation of duties is enforced
Subjects can access objects only through authorized programs
Auditing is required
Goals of Integrity

Security Matrix

	People	Physical	Networks	Computer Equipment
Prevention				
Detection				
Reaction				

The Security Matrix: uses

- Use the matrix to focus measures where they are needed, and to be aware of what measures are being (purposely) neglected.
- Drawing a threat/risk landscape. What areas are most at risk? Acceptable downtime.
- Define future measures, baselines, or project specific security

Examples

	People	Physical	Networks	Computer Equipment
	Users, managers, admins	Buildings, server rooms, laptops, diskettes, backups..	Telephone, fax, voicemail, IP tel., Internet , Intranet, VPN, SNA, Novel,I Dialup	Servers, workstations, laptops, routers, hubs, switches,

General measures

Prevention	Physical, technical, continual re-assessment, resource isolation, ...
Detection	Audits, looking for unusual behaviour
Reaction	Panic? .. disciplinary action, forensics/detective work

Measures

	People	Physical	Networks	Computers (OS + Applications)
Prevention	Policy, processes, responsibility, roles, education, goodwill.. Documentation: architecture/ services/ changelog. Good Programming. Continual re-assessment. Release mgt	Locks (several layers), logging.. cameras, security guards,	Network firewall, switches not hubs anti-spoofing content filtering strong authentication resource isolation encryption	Hardening local/personal firewall log analysis anti-virus & updates redundancy & backups resource isolation encryption
Detection	audits	Cameras, alarms Security guards	NIDS, logs, traffic changes Scanning	Log analysis integrity checker local/personal IDS
Reaction	Discipline Incident Response Team		Firewall rules Unplug networks	Unplug from network, shutdown, Reinstall, fix, ignore, Forensics

Computer Crime
Security and Privacy

Data communications capabilities provides new challenges

Keep data secure

- Destruction
- Accidental damage
- Theft
- Espionage

Keep data private

- Salaries
- Medical information
- Social security numbers
- Bank balances

Ways to secure data

- Locked servers
- Removable hard drives that are locked when not in use
- Hard disk drives requiring special tools for detachment
- Physical cages a s that prohibit access
- Passwording file

Security

System of safeguards designed to protect a computer system and data from deliberate or accidental damage

- Natural disasters
- Fire
- Accidents
- Vandalism
- Theft
- Theft or destruction of data
- Industrial espionage
- Hackers

Security
Identification and Access

- Provide access to authorized individuals only
- Uses one of more of the following systems
  - What you have
  - What you know
  - What you do
  - What you are

Security
Identification and Access

What You Have

- Key
- Badge
- Token
- Plastic card – magnetized strip
- Active badge – signals wearer’s location using infrared signals

Security
Identification and Access

What You Know

- Password
- Identification number
- Combination

Security
Identification and Access

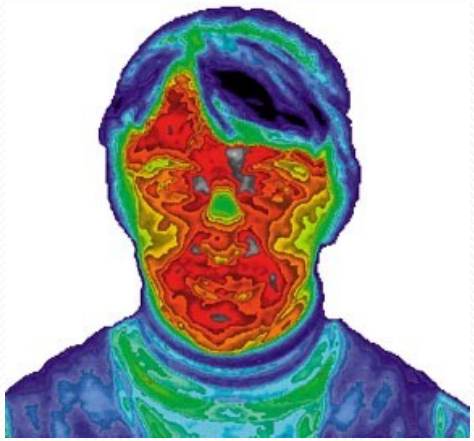
What You Do

- Verify signature – software verifies scanned and online signatures

Security
Identification and Access

What You Are

- Biometrics – science of measuring individual body characteristics
- Fingerprints
- Voice pattern
- Retina of the eye
- Entire face



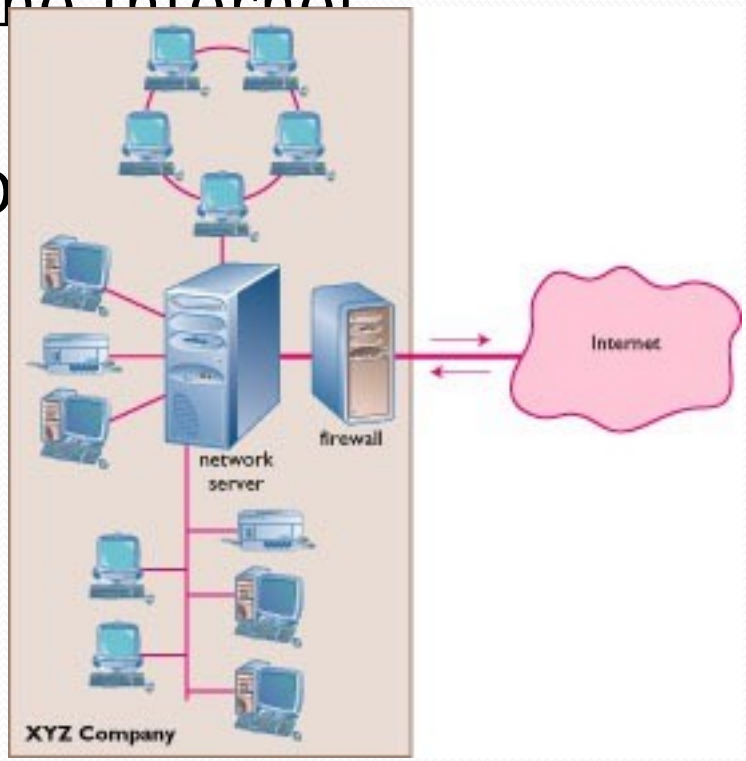
Security
The Internet

Firewall

Dedicated computer that governs interaction between internal network and the Internet

Encryption

Data Encryption Standard (D



Security
Personal Computers

- Physical security with locks and cables
- Surge protector
- Uninterruptible power supply (UPS)
- Backup files regularly and systematically

Privacy

- Where is my data?
- How is it used?
- Who sees it?
- Is anything private anymore?

Privacy

How Did They Get My Data?

- Loans
- Charge accounts
- Orders via mail
- Magazine subscriptions
- Tax forms
- Applications for schools, jobs, clubs
- Insurance claim
- Hospital stay
- Sending checks
- Fund-raisers
- Advertisers
- Warranties
- Military draft registration
- Court petition

Privacy

Your Boss is Spying on You!

Monitoring software

- Screens
- E-mail
- Keystrokes per minute
- Length of breaks
- What computer files are used and for how long

Privacy
Monitoring by Web Sites

Records:

- City
- Site you just left
- Everything you do while on the site
- Hardware and software you use
- Click stream
  - Series of clicks that link from site to site
  - History of what the user chooses to view

Privacy
Monitoring by Web Sites

Cookie

- Stores information about you
- Located on your hard drive
- Beneficial uses
  - Viewing preferences
  - Online shopping
  - Secure sites retain password in cookie
- Controversial use
  - Tracking surfing habits for advertisers
- Can set browser to refuse cookies or warn before storing
- Software available to manage cookies