Security

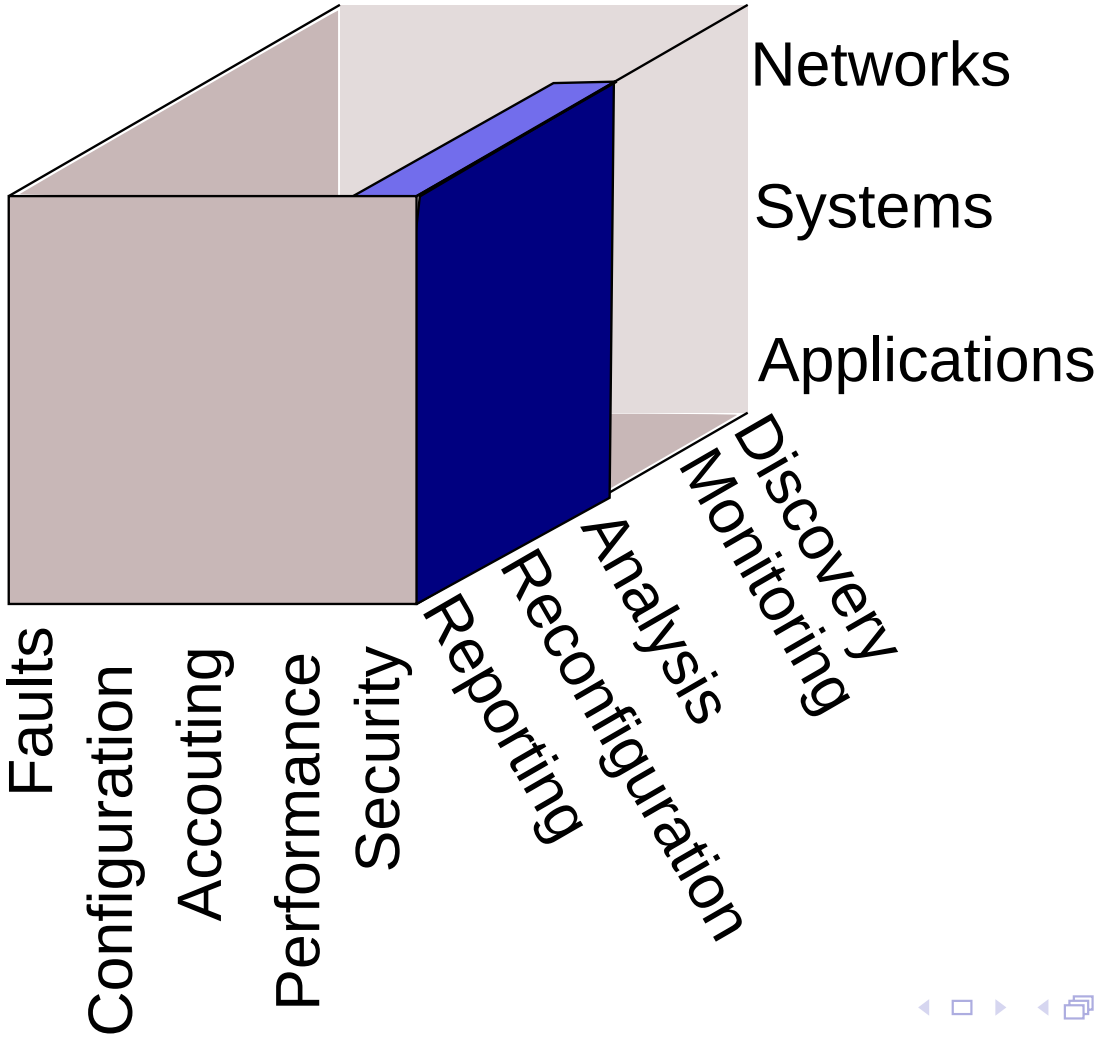
CGS - Hugo Miranda

08/05/2020

Ciências ULisboa

Faculdade de Ciências da Universidade de Lisboa

The Cube


Networks
Systems
Applications
Discovery
Monitoring
Analysis
Reconfiguration
Reporting
Security
Performance
Accouting
Configuration
Faults

Security Activities

- Authentication
- Confidentiality
- Integrity
- Non repudiation
- Availability

Security as a Compromise

- Race between security officers and hackers
- Trade-off between usability and security

  The most secure system is one that is disconnected

Examples

- VPN to access certain services
- Blocking switch ports to MAC addresses
- Password expiration/restrictions
- Time before locking the computer
- Store files where personal data is encrypted
- Impact on performance of antivirus software
- 2FA is slow/difficult

This Lesson

- Not a crash course on IT security
- Focus on a few key practical aspects on:
  - Authentication
  - Access Control
  - Non repudiation
  - Service and Data Availability

Hardware Authentication - Why?

- Because a device connected to the network can make damage
  - ARP poisoning
  - Network snooping
  - DHCP servers
  - MAC addresses can be faked

Hardware Authentication - How?

- 802.1x
  - Usable for users and devices
  - Link layer level
    - Popular in wifi
    - Unpopular in wired
- Homework
  - Read a description of the 802.1x protocol
  - See the role of the participants

Access Control

- We know who the user is... What can he do?

Approaches

A survey on "where's the list of who can do what"?

Access Control Lists (ACL)

The list is at the resource

- White list denied by default
- Black list permitted by default

Capabilities

The list is at the user

Approaches

Clearance Levels

- Users and actions/resources have levels (U_l and A_l)
- User U can do action A if $U_l \geq A_l$

Role Based

- Users belong to roles (groups)
- ACL for groups

Physical Access

- Prevent hard drives from being stolen
  - Physical access to a data center
- Proper destruction of hard drives/backup tapes/paper
  - Certified companies
  - Certified procedures

What about user devices?

- Encrypt files
- Encrypt partitions
- Self-destruction buttons
- Convince the user that this is important

The problem with encripted files

https://www.online-tech-tips.com/ms-office-tips/
how-to-remove-crack-or-break-a-forgotten-excel-xls-pas

How encrypted partitions work?

Non-Repudiation

- Prove that users did what they did
  - Asymmetric cryptography
    - Digital signatures
  - Login/password
    - Acceptable by law
  - Indisputable logs
    - Storage space
    - Prove they haven't been changed: Blockchain

Data availability

- Make sure that the data is there when we need it
- Not as easy as it sounds

Threats

- Ransomware
- Trojan/virus
- Hard drive physical damages/theft

Approaches

- RAID
  - For hard drive failures
- Data center replication
  - For catastrophic (data center) failures
- Backups / Version Control
  - To bring (part of) the system to some point in time in the past
  - To survive catastrophic failures

Backup Concepts

- A backup keeps a snapshot of the system status at some point in time
- Challenges
  - To preserve them
  - To make them without disturbing the system operation

Backup Metrics

RPO/RPA Recovery Point Objective/Actual

- **RPO** How long will my system have to rollback if a restore is needed in the worst case scenario
- **RPA** How long will my system have to rollback in "this" restore

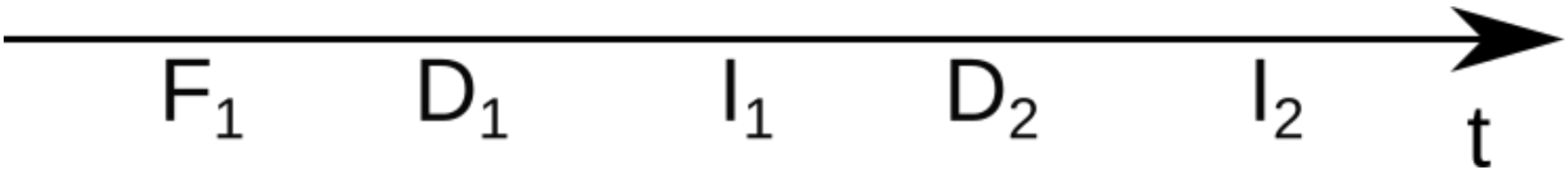
RTO/RTA Recovery Time Objective/Actual

- **RTO** How long will I take to recover the system in the worst case scenario
- **RTA** How long did I take to recover the system "this" time

Backup Types

Full	Create a snapshot of the full system state
Differential	Create a snapshot with the differences since the last full
Incremental	Create a snapshot with the differences to the last backup (any type)

Backups in a Timeline



- Impact on RPO?
- Impact on RTO?

Performing Backups

- System should be backed up in consistent state
  - Services should be stopped, state backed up, and resumed
  - What about system availability?

Staging

Stage 1 fast and expensive

- Backup to hard drives
- (Stop here if enough budget)

Stage 2 slow and cheap

- Copy backup to tapes
- Free storage space for next backup

Staging

Tapes

LTO Linear Tape-Open

Tape Robots

Tapes versions

LTO5

- 1.5Tb capacity
- 800m magnetic tape
- 140Mb/s
- writing 1Tb $\approx$ 2h10m

Tapes versions

LTO6

- 2.5Tb
- 160Mb/s
- writing 1Tb $\approx$ 2h

Tapes versions

LTO7/LTO8

- 6.0Tb/12.0Tb
- 300Mb/s

Backups: Software

- Schedules the backups
- Coordinates/cooperates with services their suspension/resume
  - VM hypervisor
  - Storage
- Coordinates the staging process
- Manages the robot
- Can be used to retrieve each individual file

Backups: Final Remarks

Tapes must be preserved

- Away from the public
  - Data protection
- Away from the data center where the data is
- In proper condition
  - Humidity
  - Magnetic fields

Backups: Final Remarks

Tapes fail when we most need them

- Random reading sampling

Backups: Final Remarks

Preserve history

- Problems may be found after several backups
- Keep historical backups

Services Availability

- Content Delivery Networks (CDNs)
  - Can be used for load balancing
    - Mitigating DDoS

Wrap Up

- Security
  - Far more than passwords and firewalls
  - The more you do, the less happy users are