Systems & Network Security

Introduction

What do we mean by security

- A good definition:
  - "[…] *processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction"*
  - ***"Computer security also includes protection from unplanned events and natural disasters"***

Source: https://en.wikipedia.org/wiki/Computer_security

What are we trying to protect

- Infrastructure
  - Routers, switches, and associated data
- Hosts, services
  - Mail, DNS, …
- Data
  - Files, databases, …
- Users
  - Passwords, privileged accesses

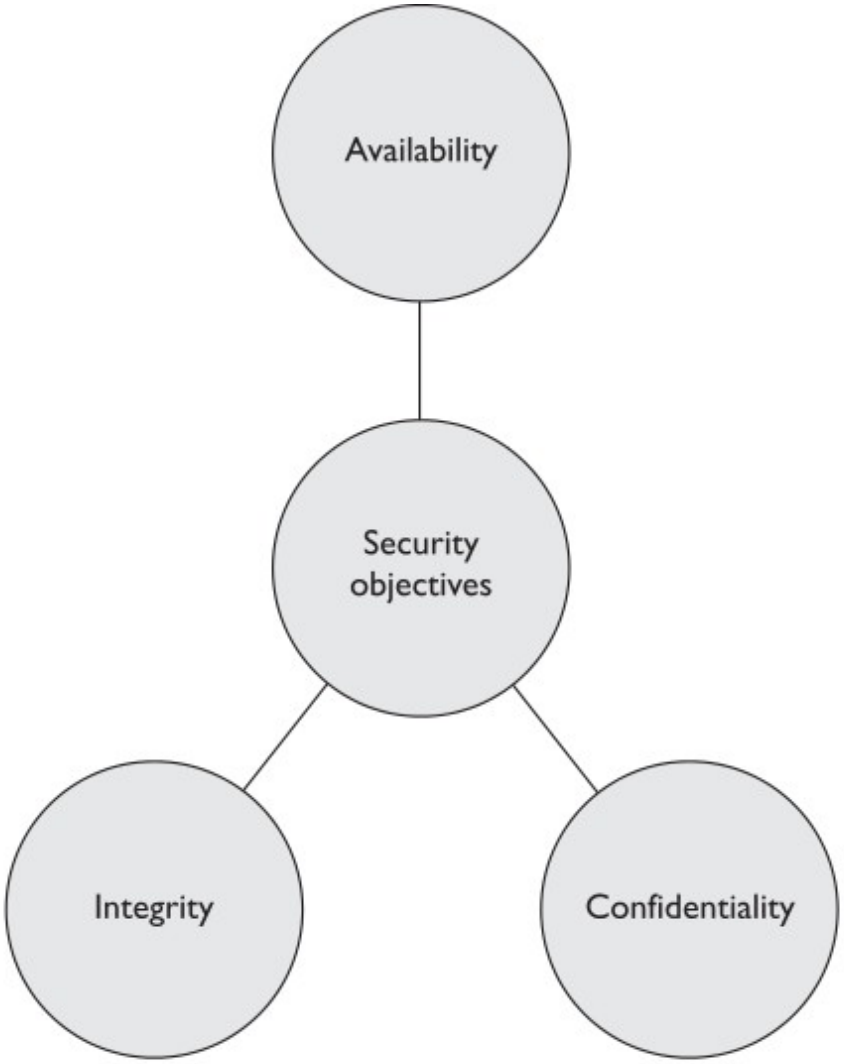
In other words…

- Host security
  - Remember, everything is a host
  - Protect the infrastructure as well as the hosts running services
- Data security
  - Mitigating what “they” have access to, once they’re inside
- Intrusion Detection
  - Try and detect malicious behaviour

Our approach

1. Prevent and protect
2. Detect
3. Mitigate

Fundamental Principles of security



Availability

Ensures reliability and timely access to data and resources to

authorized individuals.

Network devices/Computers & Applications availability.

Networks have so many pieces that must stay up and running (routers, switches, DNS servers, DHCP servers,proxies, firewalls)

Software - operating system, applications, antimalware software.

Integrity

Integrity is upheld when the assurance of the accuracy and reliability of information and systems is provided and any unauthorized modification is prevented.

The systems and network should be protected from outside interference and contamination.

Strict access controls, intrusion detection, and hashing can combat these threats.

System-criticalfiles should be restricted from viewing and access by users. Applications should provide mechanisms that check for valid and reasonable input values. Databases should let only authorized individuals modify data, and data in transit should be protected by encryption or other mechanisms

Confidentiality

Confidentiality ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure.

Confidentiality can be provided by encrypting data as it is stored and transmitted,enforcing strict access control and data classification, and by training personnel on the proper data protection procedures.

Security threats and trends

- Threats

  [excerpts from Arbor Network's yearly security report]
- Some clear threats emerge:
  - DDoS - http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet
  - Data Breach / theft of customer databases – (SONY, Citigroup, RSA, Evernote,)
    - More and more reports every month of compromised companies
  - Defacement (usually harmless, but poor image)
  - Malware (infected software, viruses, malicious documents – PDF, Flash, Java)
- Motivations for DDoS (upwards of 100 Gbps is not unheard of nowadays)
  - Political / Ideological
  - Gaming (!)
  - Vandalism
  - Social networking related
  - Revenge / disputes between groups
  - Extortion (less than people think)

http://www.arbornetworks.com/research/infrastructure-security-report

Questions

?