BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Introduction – Part-1

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement

- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Challenges in Computer Security

Challenges in Computer Security

List of security challenges

1. Computer security is not as simple as we might think
2. Constantly think about potential attacks on the security features
3. Procedures used to provide particular services are often counterintuitive
4. Physical and logical placement needs to be determined
5. No single protocol or algorithm
6. Computer security is a perpetual battle of wits between a perpetrator and the designer
7. Perceptions of no benefit from security investment
8. Security requires regular and constant monitoring
9. Security is too often an afterthought
10. Strong security viewed as an impediment

Challenges in Computer Security

Details

- 1) Computer security is not simple
  - The computer security requirements appear to be straightforward
  - For example, most of the major requirements for security services can be given self-explanatory one-word labels:
    - confidentiality, authentication, nonrepudiation, integrity
  - But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning
- 2) Potential attacks on security features
  - In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features
  - Most of the successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.

Challenges in Computer Security

Details

- 3) Procedures used to provide particular services are often counterintuitive
  - Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed
  - It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.
- 4) Physical and logical placement needs to be determined
  - Having designed various security mechanisms, it is necessary to decide where to use them
    - Physical placement
      - E.g., at what points in a network are certain security mechanisms needed
    - Logical placement
      - E.g., at what layer or layers of an architecture such as TCP/IP should mechanisms be placed

Challenges in Computer Security

Details

- 5) No single protocol or algorithm
  - Security mechanisms typically involve more than a particular algorithm or protocol
  - Security mechanisms also require that participants be in possession of some secret information (e.g., an encryption key)
    - This creates additional questions of creation, distribution, monitoring, and protection of that secret information
  - The *behavior of communications protocols* may complicate the task of developing the security mechanism
  - For example
    - If the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any unpredictable delays (due to network and communication protocols) may render such time limits meaningless

Challenges in Computer Security

Details

- 6) Computer security is a perpetual battle of wits between a perpetrator and the designer
  - Perpetrator – the one who tries to find holes
  - Designer – the one who tries to close them
  - Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security
- 7) Perceptions of no benefit from security investment
  - There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs

Challenges in Computer Security

Details

- 8) Security requires regular and constant monitoring
  - Constantly monitoring security would be difficult in today's short-term, overloaded environment
  - Think of security forces guarding our national borders 24/7
- 9) Security is too often an afterthought
  - Many times, security is incorporated into the system after the design is complete, rather than being an integral part of the design process
- 10) Strong security is viewed as an impediment
  - Many users, including security admins view strong security as an obstruction to smooth operation of an IS or information use


innovate
achieve
lead

BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
ज्ञानं परमं बलम्

Thank You!