

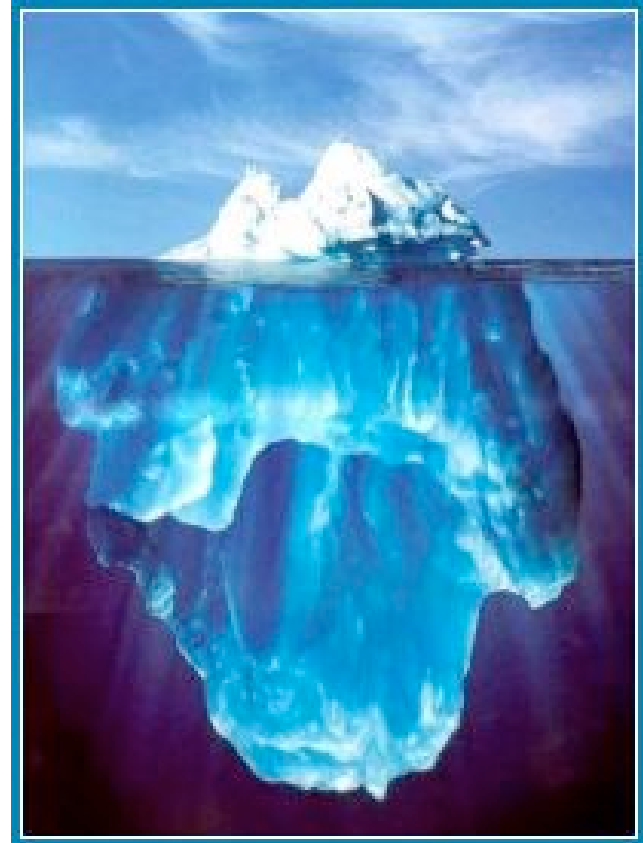
# Security Topics in Networking and Distributed Systems CS 590D

## **Lecture 23: Summary**

Department of Computer Sciences  
Purdue University

# This course ...

- Focused on network security
- The full picture:
  - Applications
  - Operating Systems
  - Write and verify secure code
  - Policies
  - Physical security

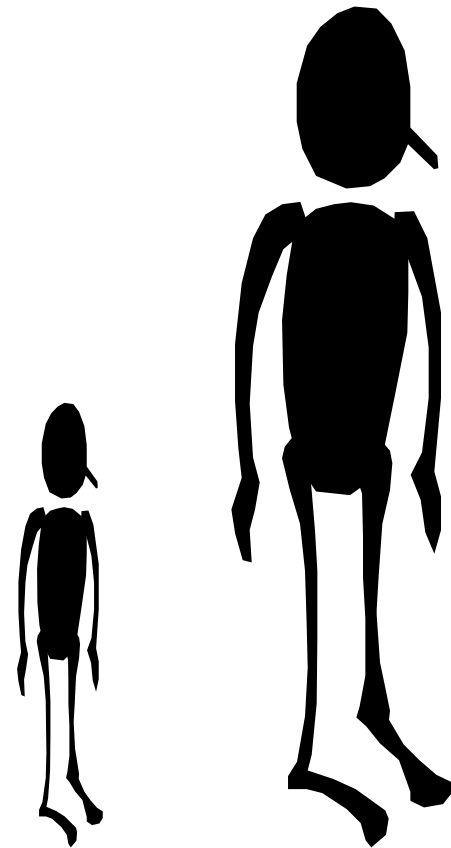


# Network Protocols and Services

- Span a wide range
  - Internet core services: DSN, BGP
  - Intra-domain communication: OSPF, RIPE
  - Major transport protocols: UDP, TCP and SSL
  - Wireless communication: 802.11
  - Severe resource constraint devices: sensors RFID
- Today's vs tomorrow's networks
- Theory vs. practice
- Mature protocols vs. protocols that are still evolving

# What Role Does Security Play?

- ESSENTIAL
- All the network protocols that we examined suffer from security flaws
- Mature protocols were not designed with security in mind and it is more difficult to consider it afterwards
- “Young” protocols (802.11 family, sensors) are still evolving, security should be considered in the design



# Root of Attacks

- Lack of Authentication
  - End-to-end
  - Hop-by-hop
- Authentication is most of the time tightly coupled with key management, requiring PKI
- Avoiding dynamic key management:
  - Pre-set keys
  - Methods that require tight-synchronization
- **HOW TO SECURELY BOOTSTRAP A SYSTEM?**



*"On the Internet, nobody knows you're a dog."*

# Limitations of Authentication

- Authentication does not solve all world problems
- **Faulty, selfish or malicious participants can not be prevented by using authentication**
- Defending against malicious participants: checking the reports vs. data reported by other participants
  - For sensors this seem natural
  - Also for sensors using different type of information there might be ways to distinguish between faulty and malicious



# PKI: Is It Ready for Use?

- Many security services and protocols require a PKI
- PKI technology is not perfect, but more mature than other technologies
- Remember, it's all a matter of trust:
  - “What do actually certificates provide (certify) and who do we actually trust when we accept a certificate”.
- **Revocation** is essential, but rarely implemented in practice.
- Scalability issues.
- Not easy to deploy.

# Wired Networks

- Core Internet Services:
  - DSN and BGP both can be attacked
  - Work to provide authentication DNSSEC and S-BPG
  - Some work on avoiding the inconsistencies in announcement non-crypto based
- Securing these services is CRITICAL
- Challenges:
  - How to bootstrap
  - Scalability
  - Changing them while Internet relies on them
  - Requires collaboration and coordination for deployment

# Wired Networks

- SSL is the main transport protocol, many web-based applications rely on it
- Suffers from all limitations that PKI suffers from
- Relies on TCP, therefore suffers from all TCP security flaws
- Unreliable communication: UDP, non-secure, no flow control

# Other Security Issues

- What users perceive today:
  - Denial of service
  - Worm spreading
  - Concerns about identify theft
- Challenges:
  - Involving ISP's (either by law or providing incentives)
  - It is not enough fixing the network, the end system is also responsible of the problem
  - Not enough understanding of the problem and solution
  - Testbed/metrics to evaluate impact and effectiveness of solution needed

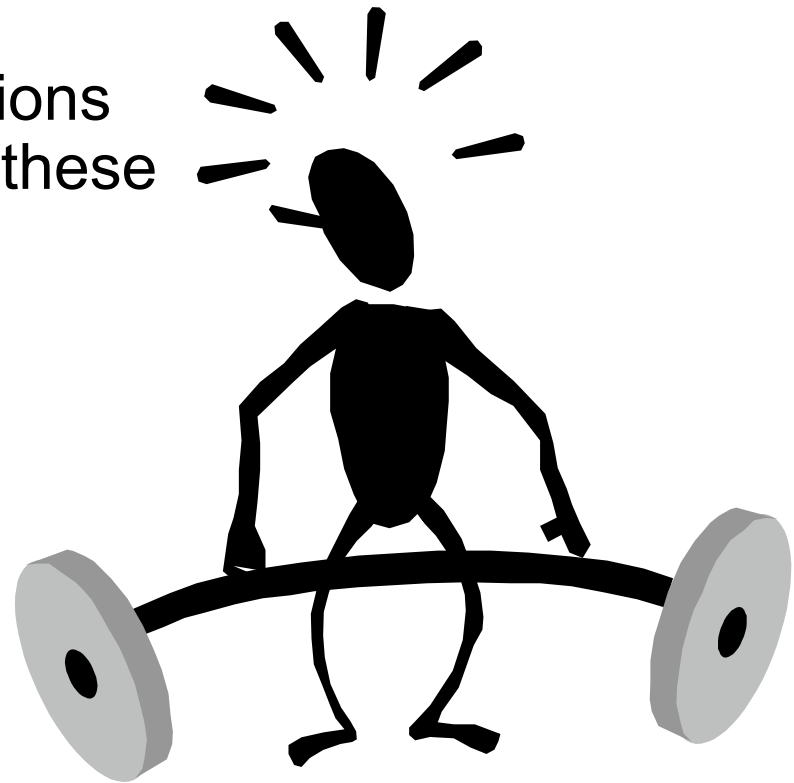
# Wireless Communication

- We have less established wireless communication protocols: 802.11 (still going through revisions and research): infrastructure and ad hoc
- Infrastructure: broken secure data link protocol
- Ad Hoc:
  - Routing and how to secure the routing protocols
  - PKI: distributed CA, or improved PGP
- **Challenges: mobility, limited battery, shared medium, easy eavesdropping, we do not understand all interactions between attacks/solutions**



# Severe Resource Constrained Devices

- Sensors and RFIDs
- How realistic are the solutions proposed today to secure these devices?
- **Challenges:**
  - Limited memory
  - Limited power
  - Limited computation
  - Limited bandwidth
  - Limited everything !!!



# How Will the ``Network'' Look in 10 years?

- Remember that 10 years ago first browser was out
- Most probably we will have sensors and actuators everywhere
- Pervasive computing will provide access to data anywhere, everywhere
- Design security keeping in mind that **“Your system is as secure as your weakest link”**
- **Minimize overhead without decreasing security**

