Mobile and Wireless Security
CSCE 496/896

Lecture # 5
Basics of cryptography and security

Instructor: Nirnimesh Ghose
Computer Science and Engineering

UNIVERSITY *of* NEBRASKA–LINCOLN

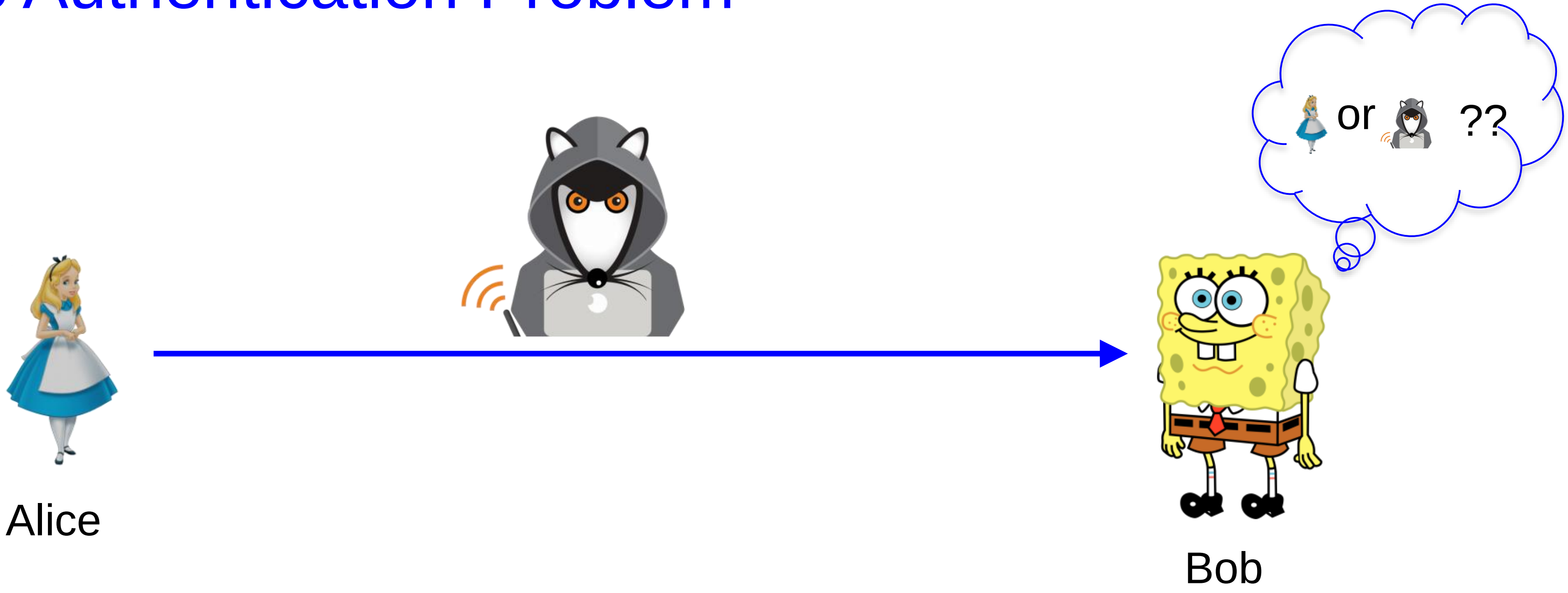
Lecture Set Overview

Access control and Authentication Basics

- Password based authentication

Wireless networks basics

Basic Authentication Problem



How do you prove to someone that you are who you claim to be?

Any system with access control must solve this problem

Who is Being Authenticated?

Authenticate a person to a server

Authenticate a machine to a machine

Authenticate both a person and a machine to a server

A machine stores high-quality secret; a person memorizes low-quality password

Cryptographic operations

Wireless:
Authenticate device to device, or device to a hub and vice-versa

Wireless specific properties + applied cryptography – efficient.

Many Ways to Prove Who You Are

What you know

- Passwords
- Secret key

Where you are

- IP address

What you are

- Biometrics

What you have

- Secure tokens

Password-Based Authentication

User has a secret password. System checks it to authenticate the user.

Vulnerable to eavesdropping when password is communicated from user to system

How is the password stored?

Store salted hash of password

How does the system check the password?

How easy is it to guess the password?

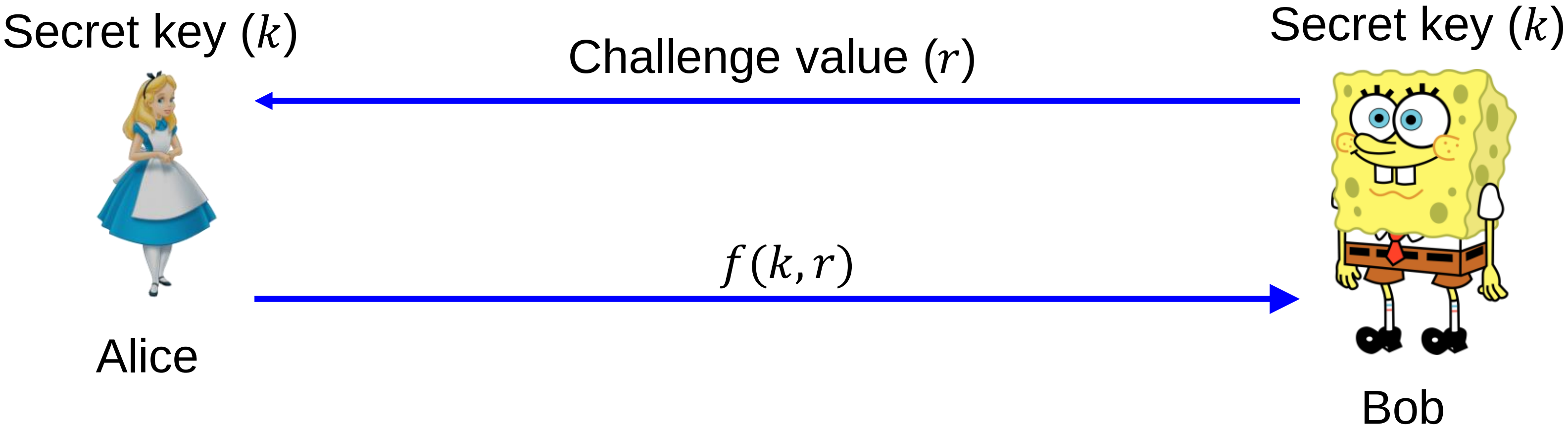
Easy-to-remember passwords tend to be easy to guess

Password file is difficult to keep secret

Problem: Prone to dictionary attack

Latest devices missing interface

Challenge-Response



Secret key (k)

Challenge value (r)

Secret key (k)

$f(k, r)$

Alice

Bob

Why is this better than a password over a network?

Secrecy: difficult to recover key from response

One-way hashing or symmetric encryption work well

Freshness: if challenge is fresh and unpredictable, attacker on the network cannot replay an old response

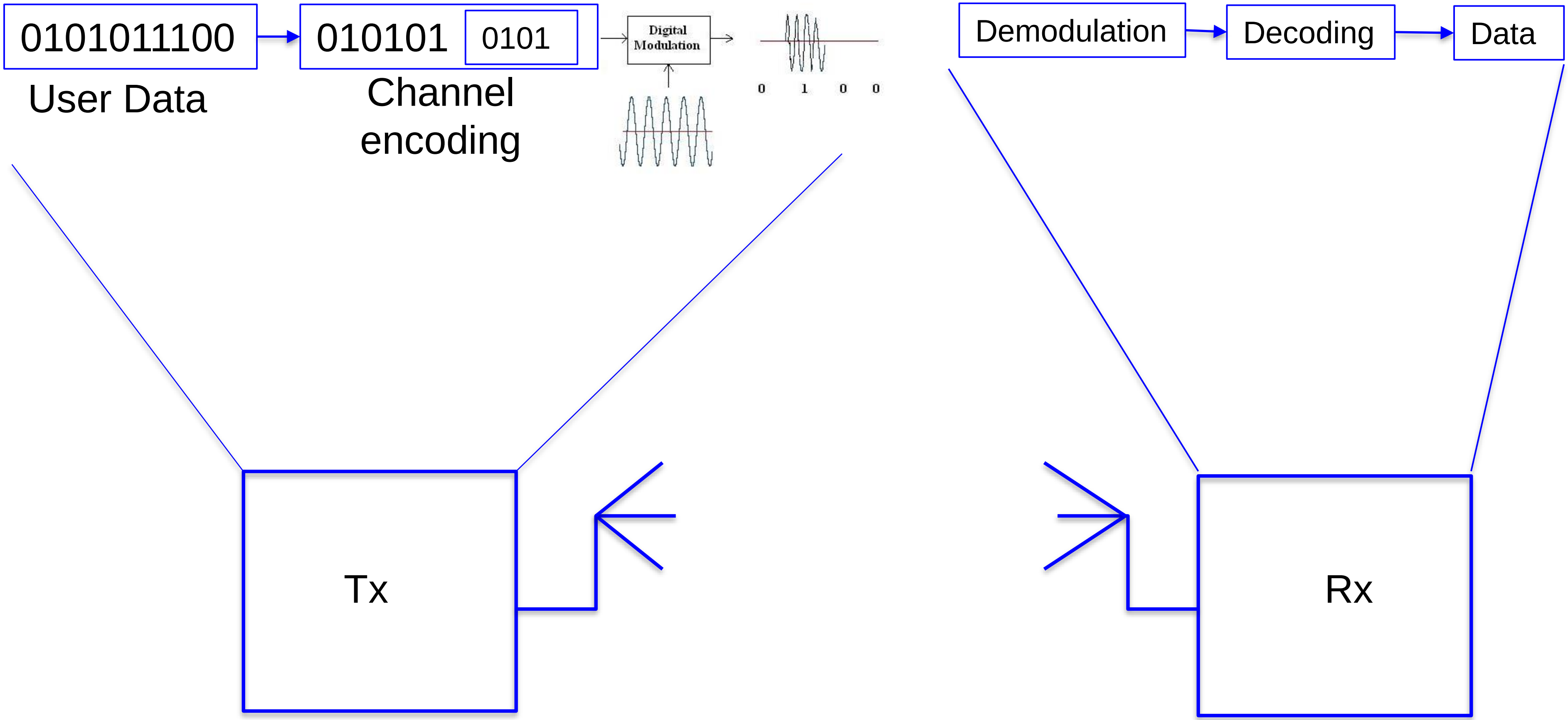
For example, use a fresh random number for each challenge

Good for systems with pre-installed secret keys

Layers of Network and Security

OSI Model	TCP/IP Model	Data Unit	Security
Application	Application	Data	S/MIME, Kerbos, HTTPS, SSH
Presentation		Data	
Session		Data	
Transport	Transport	Segments	SSL,TLS
Network	Network	Packets	IPSec
Data Link	Data Link	Frames	MAC Layer Sec
Physical	Physical	Bits	PHY Layer Sec

Wireless Network Basics



0101011100

User Data

010101 0101

Channel encoding

Digital Modulation

0 1 0 0

Demodulation

Decoding

Data

Tx

Rx

Why is security more of a concern in wireless?

No inherent physical protection:

- Physical connections between devices are replaced by logical associations.
- Sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.).

Broadcast communications:

- Wireless usually means radio, which has a broadcast.
- Transmissions can be overheard by anyone in range.
- Anyone can generate transmissions,
  - which will be received by other devices in range
  - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)

Why is security more of a concern in wireless?

Eavesdropping is easy due to broadcast nature

Injecting bogus messages into the network is easy due to ease of access

Replaying previously recorded messages is easy due to broadcast nature

Illegitimate access to the network and its services is easy due to ease of access

Denial of service is easily achieved by jamming

Node compromise is also relatively easy

Wireless communication security requirements

Confidentiality, Authenticity, Integrity

- Messages sent over wireless links must be encrypted
- Origin of messages received over wireless link must be verified
- Replay detection
- Modifying messages on-the-fly (during radio transmission)
- Integrity of messages must be verified

Access Control

- Network access should be provided only to legitimate entities

Availability

- Protection against jamming

Privacy

Accountability……

Wireless Networks Classification

One-hop wireless networks

- Cellular networks
- Wireless LAN
- PAN, BAN, Bluetooth
- RFID
- Pervasive computing environment

Multihop wireless networks

- Mobile ad hoc networks
- Sensor networks
- Vehicular networks
- Wireless mesh networks….

Many Ways to Prove Who You Are

Crypto	Wireless
What you know	
Passwords	Device fingerprints - PUF
Secret key	Channel state information
Where you are	
IP address	Proximity analysis
	Wireless fingerprint mapping
What you are	
Biometrics	Hardware fingerprint
What you have	
Secure tokens	Pre-loaded secrets