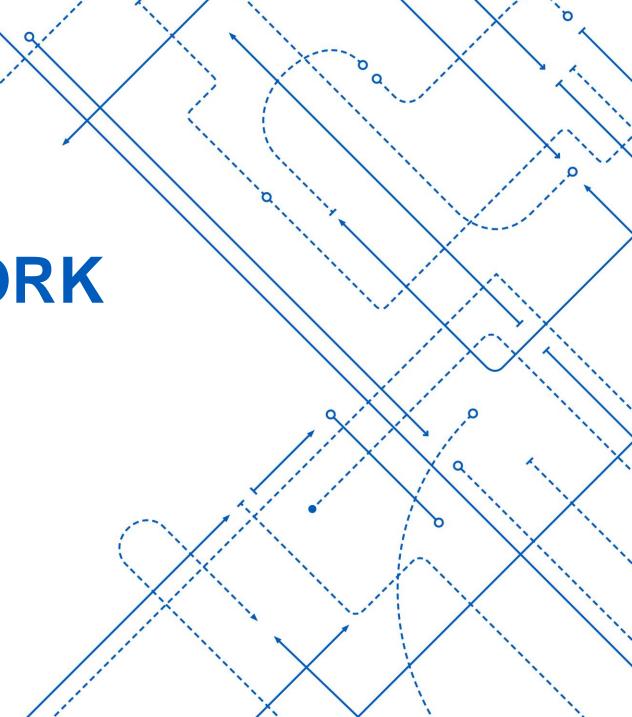
WIRELESS NETWORK AND SECURITY

Lecture 24: Revision

Instructor: Kui Ren







Introduction to Cryptography (Lecture 2)

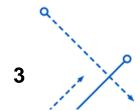
- Symmetric Cipher Model
 - Cryptography
 - Cryptanalysis and Brute-Force Attack
- Substitution techniques
 - Caesar cipher
 - Monoalphabetic ciphers
 - Playfair cipher
 - Polyalphabetic ciphers
 - One-time pad
- Transposition techniques
- Steganography





Symmetric-key Encryption (Lecture 3)

- Traditional Block Cipher Structure
 - Stream ciphers
 - Block ciphers
 - Feistel cipher
- The Data Encryption Standard (DES)
 - Encryption
 - Decryption
 - The strength of DES
- Block Cipher Design Principles
- Advanced Encryption Standard (AES)





Public Key Cryptography and RSA (Lecture 4)

- Public-key cryptosystems
- Requirements for public-key cryptography
- Public-key cryptanalysis
- The RSA algorithm
 - Description of the algorithm
 - Computational aspects
 - Security of RSA
- Diffie-Hellman Key Exchange
- ElGamal cryptographic system





Cryptographic Hash Functions (Lecture 5)

- Principles of pseudorandom number generation
 - The use of random numbers
 - TRNGs, PRNGs, and PRFs
 - PRNG requirements
- Applications of cryptographic hash functions
 - Message authentication
 - Digital signatures
 - Other applications
- Requirements and security
- Secure hash algorithm (SHA)





Message Authentication and Digital Signature (Lecture 6)

- Message authentication requirements
- Message authentication functions
- Requirements for message authentication codes
- Security of MACs
- HMAC authentication using a hash function
- CMAC authentication using a block cipher
- Digital signatures



Basics of Wireless Networking (Lecture 7 and 8)

- Wireless Transmission Basics
 - Electromagnetic (EM) waves
 - Frequency
 - Spectrum and Bandwidth
 - Capacity
 - Signal Propagation
 - Multiplexing
 - Modulation
 - Spread Spectrum
 - Orthogonal Frequency Division Multiplexing (OFDM)





Basics of Wireless Networking (Lecture 7 and 8)

- Medium Access Control (MAC) protocols
 - Channel Partitioning MAC protocols
 - Random Access MAC protocols
 - ALOHA
 - Slotted ALOHA
 - CSMA (Carrier Sense Multiple Access)
 - CSMA/CD (CSMA with Collision Detection)
 - CSMA/CA (CSMA with Collision Avoidance)
 - CSMA/CA with RTS/CTS



Wi-Fi Security Protocols (Lecture 9-11)

- Wired Equivalent Privacy (WEP)
 - WEP Encryption algorithms
 - Major Problems with WEP
 - Attacks on WEP
- Wi-Fi Protected Access (WPA)
 - Message Integrity Check: Michael Algorithm
 - TKIP Re-Key Mechanism
 - How to Negotiate a Passphrase
 - Attacks on WEP
- Wi-Fi Protected Access II (WPA2)
 - Phases of Operation
 - WPA2 Encryption
 - The Key Reinstallation Attack





Cellular Mobile Network (Lecture 12)

- GSM(2G)
 - Architecture
 - Security Measurement
 - Weakness
 - Popular Attacks
- UMTS(3G) vs GSM
- LTE(4G)
 - Networks
 - Threats



Smartphone Wireless Security (Lecture 13 - 15)

- Bluetooth technology basics
- Security and privacy protection for Bluetooth Low Energy (BLE)
- NFC basics
- Commercial NFC security mechanism
- NFC applications
- Secure distance bounding protocols
- Relay Attacks on PKES systems



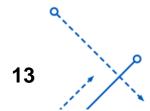
IoT Security (Lecture 16-18)

- Introduction to IoT
- IoT device risks
- DolphinAttack: Inaudible Voice Commands
- RFID basics, privacy problem, authentication protocol
- Security threats in connected vehicle
- Cybersecurity layers in connected vehicle
- Security and Privacy Vulnerabilities of In Car Wireless Networks



Biometrics and Heart-based Authentication (Lecture 19)

- Biometrics Basics
- Biometric Identification and Authentication:
 - Fingerprint
 - Vascular (Vein) Pattern Matching
 - Iris Recognition
 - Face Recognition
 - Voice Recognition
- Heart-based Authentication
 - Continuous User Authentication
 - Cardiac Motion Information
 - Doppler Effect





Eye Gaze and Voice Recognition (Lecture 20 and 21)

- Eye Gaze based Authentication
 - Eye tracking basics
 - Facial info processing:
 - Eye center detection
 - Iris detection
 - Authentication process
 - Evaluation
- Voice Authentication:
 - Attacks
 - Magnetic-based Detection
 - Voice Liveness Detection





Location and Social Networking Privacy (Lecture 22)

- Privacy Basics:
 - Privacy Definition
 - Privacy vs. Security
- Location Privacy
- Social Networking Privacy:
 - Contact Privacy
 - Attribute Inference Attack



3D Printing Side-Channel Attack (Lecture 23)

- 3D printing
- Side-channel attack
- Movement prediction based on signals
- Reconstruction results
- Defenses