# CS 5472 - Advanced Topics in Computer Security

## Topic 5: Deniable Encryption (1)

Spring 2022 Semester

Instructor: Bo Chen

bchen@mtu.edu

https://cs.mtu.edu/~bchen

https://snp.cs.mtu.edu

# The Grade for The First-round Presentation is OUT

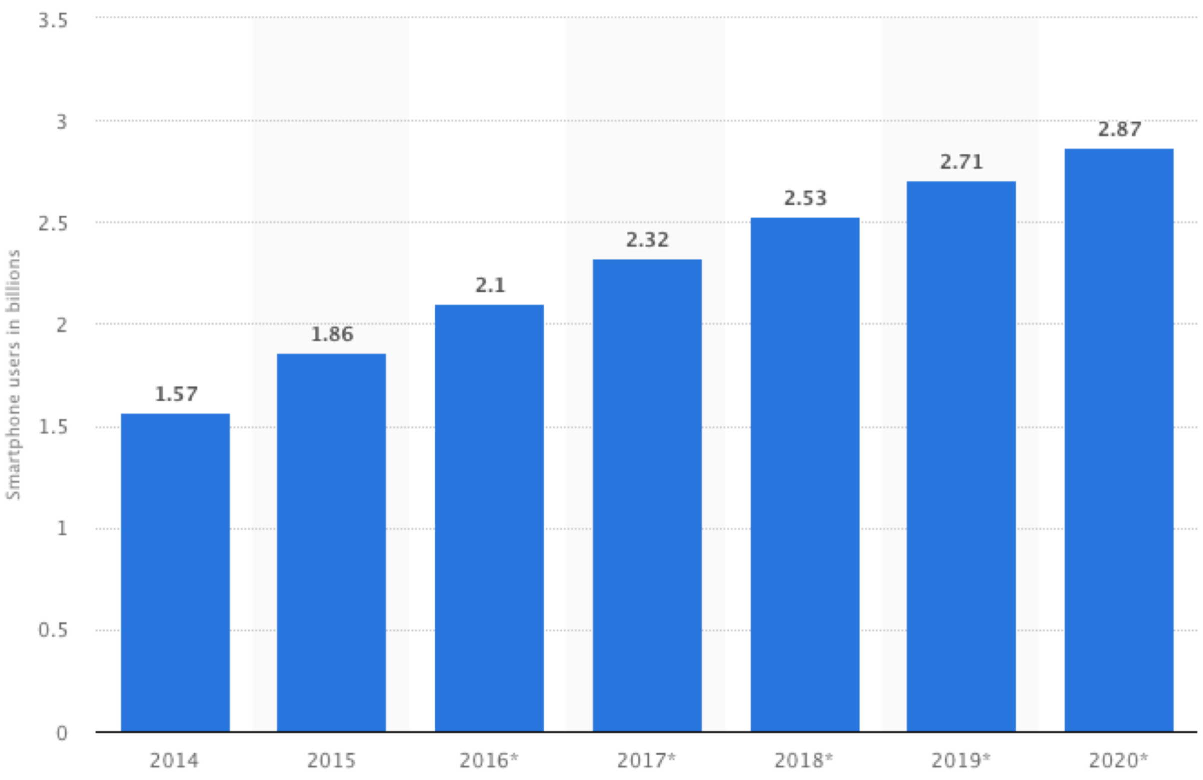
- You should be able to estimate your midterm grade based on your current performance in summary, presentation and project.

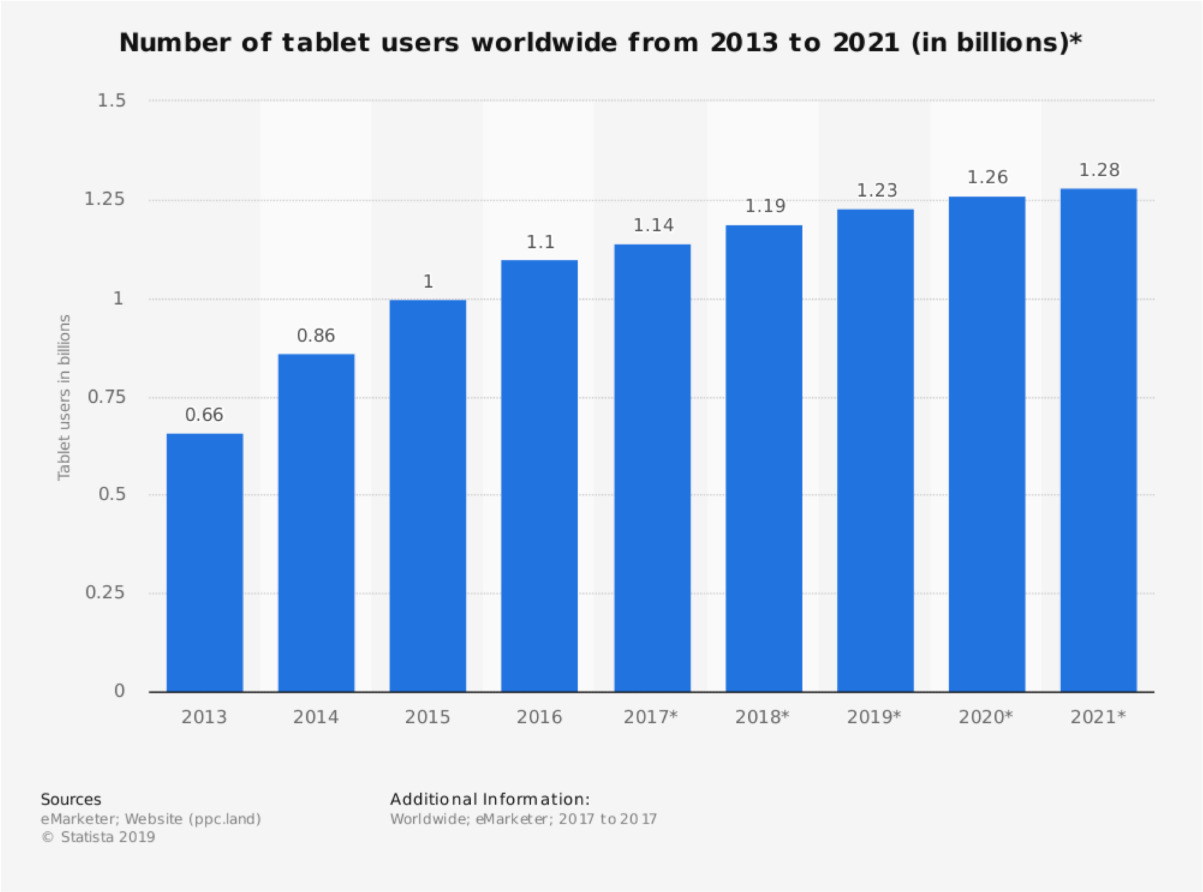
# Review: IoT Security

- Internet of Things (IoT)
- Smart home

IoT will not be possible without the mobile devices/IoT devices

# Mobile Devices are Turning to Mainstream Computing Devices




Number of tablet users worldwide from 2013 to 2021 (in billions)*

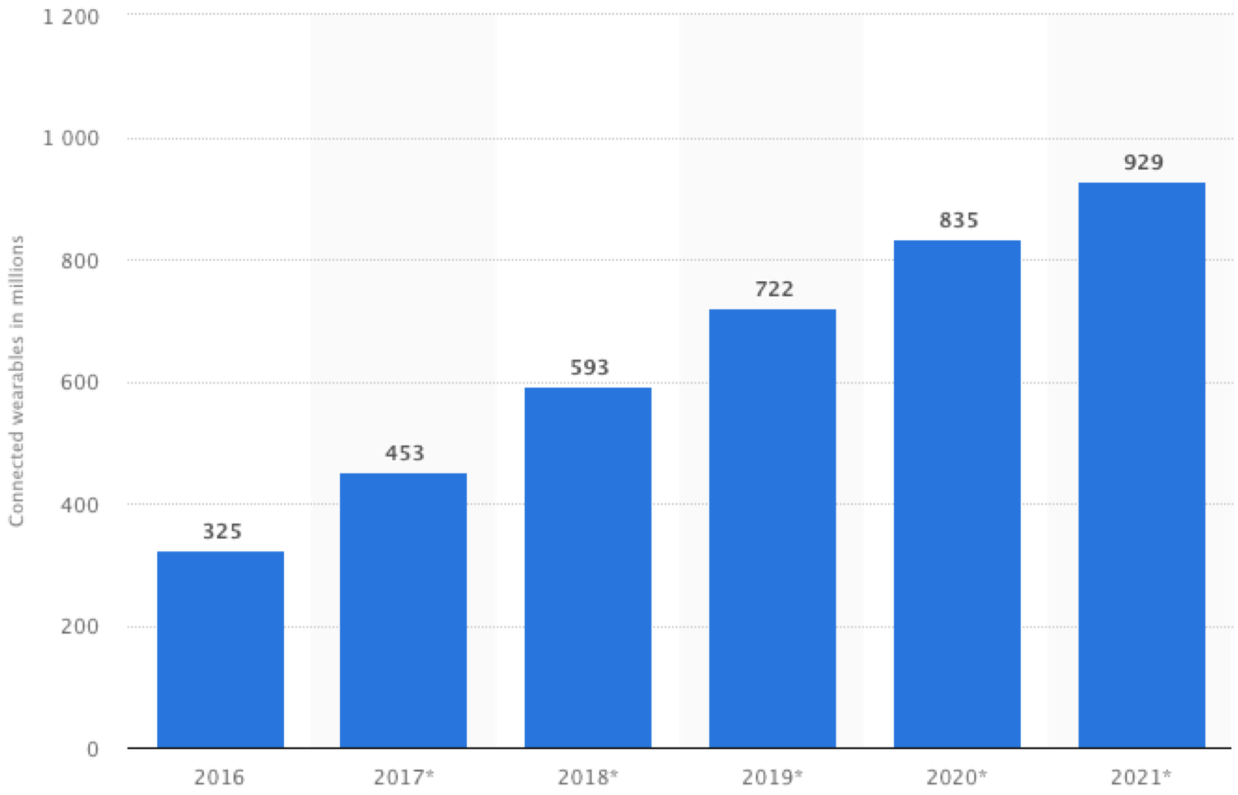
Sources
eMarketer; Website (ppc.land)
© Statista 2019

Additional Information:
Worldwide; eMarketer; 2017 to 2017

Number of smartphone users worldwide from 2014 to 2020 (in billions)

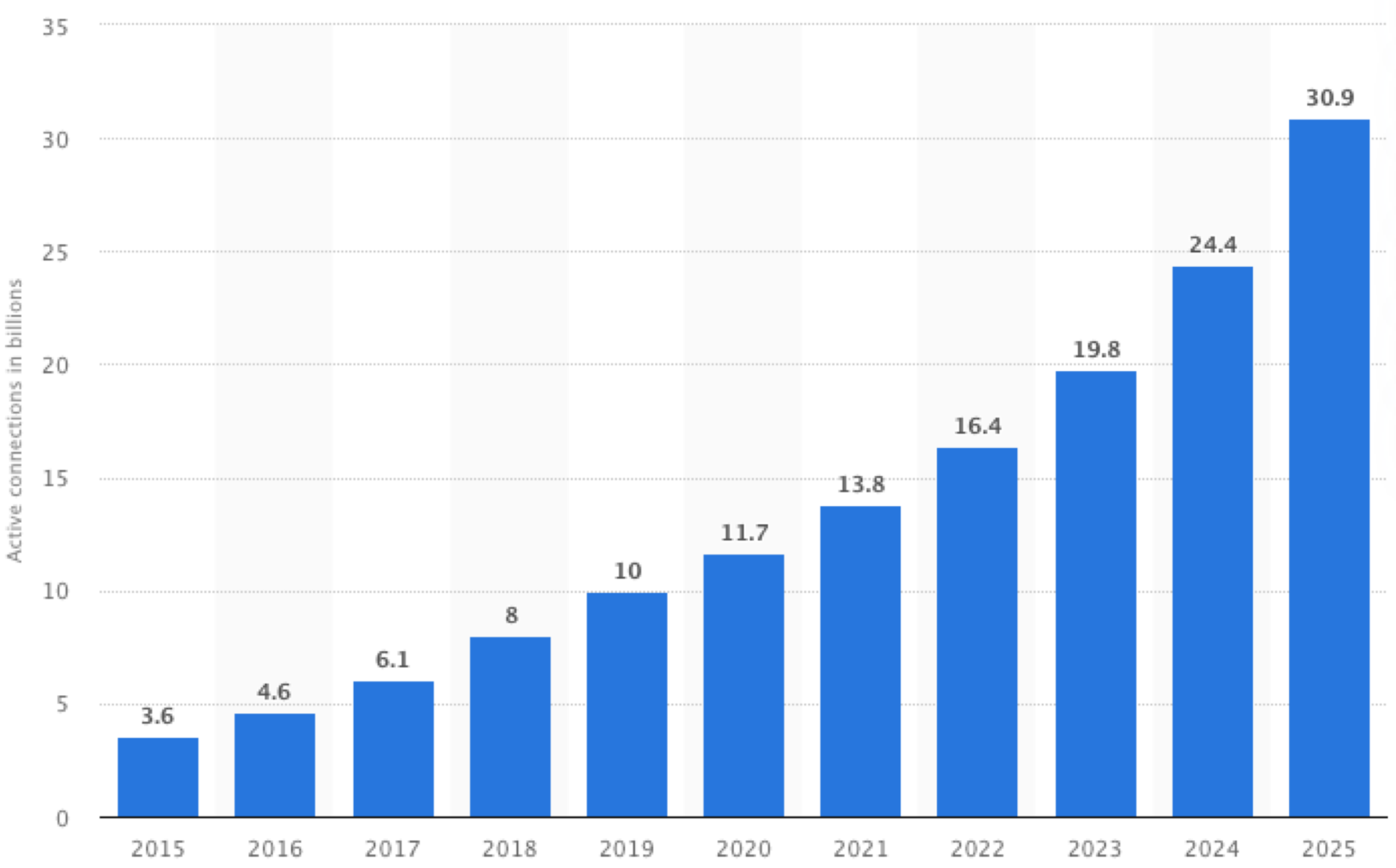
Number of tablet users worldwide from 2013 to 2021 (in billions)

# Mobile Devices are Turning to Mainstream Computing Devices (cont.)



Number of connected wearable devices worldwide from 2016 to 2021 (in millions)

# Mobile Devices are Turning to Mainstream Computing Devices (cont.)



Internet of Things (IoT) connected devices

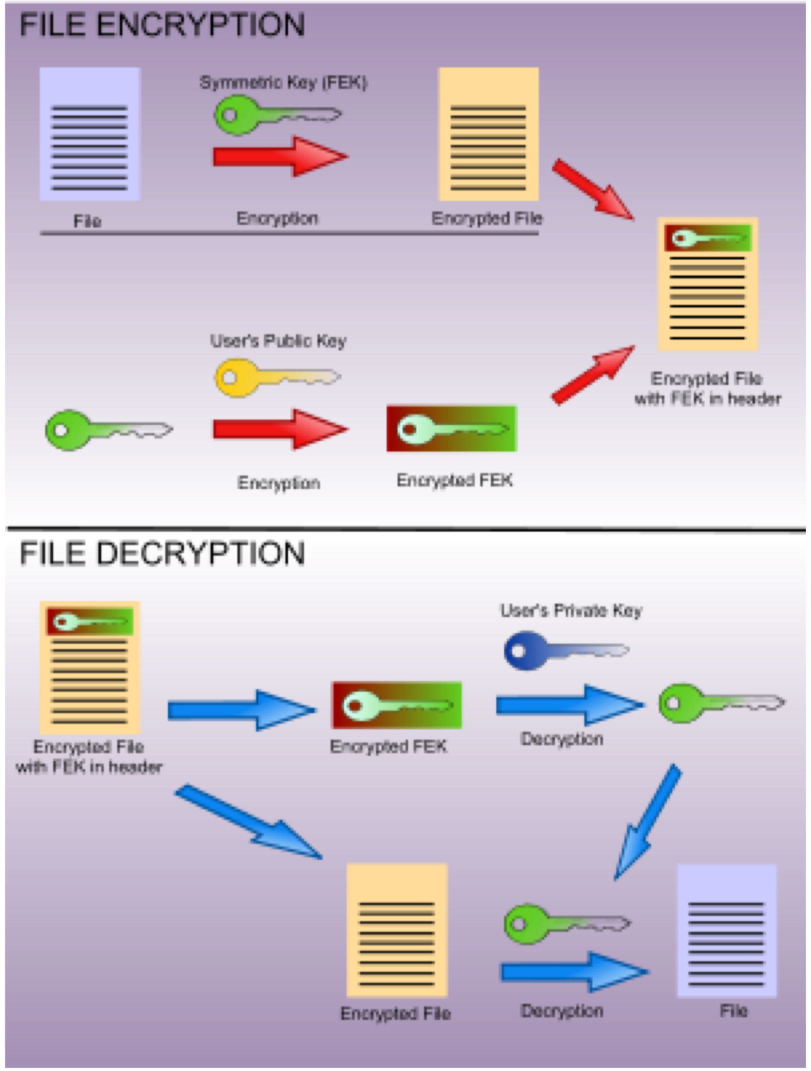
# Mobile Devices are Increasingly Used for Critical Applications

- Mobile devices are increasingly used to handle sensitive data
  - Online banking
  - Ecommerce
  - Cryptocurrency/stock trading
  - Naked photos
  - A human rights worker collects evidence of atrocities in a region of oppression
  - Etc.

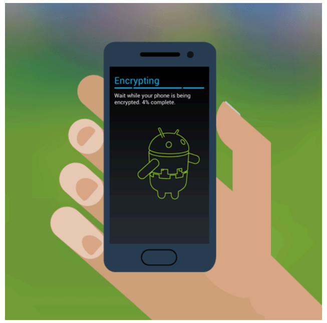
- Security issues in mobile computing devices
  - Confidentiality
  - Integrity and recoverability
  - Authentication
  - Access control
  - Malware detection and removal

# How to Ensure Confidentiality of Data in Mobile Devices

- File-based encryption
  - Encryption is performed by the user in files
  - Pros: the user can choose which files to be encrypted (fine-grained)
  - Cons: the user needs to get involved heavily in the encryption process



# How to Ensure Confidentiality of Data in Mobile Devices (cont.)



- Full disk encryption (FDE)
  - FDE at the system level
    - FDE is available in Android phones since Android 3.0
    - Since iPhone 3G S, Apple has consistently built 256-bit AES encryption into iOS devices
    - Other popular disk encryption tools: TrueCrypt/VeraCrypt, BitLocker (MicroSoft), FileVault (Apple), LUKS
  - FDE at the hardware level
    - A few SSDs (solid-state drives) have built-in hardware encryption
  - Pros: transparent to users, protect the data in the entire disk
  - Cons: everything stored in the disk will be encrypted automatically, causing a lot of extra overhead

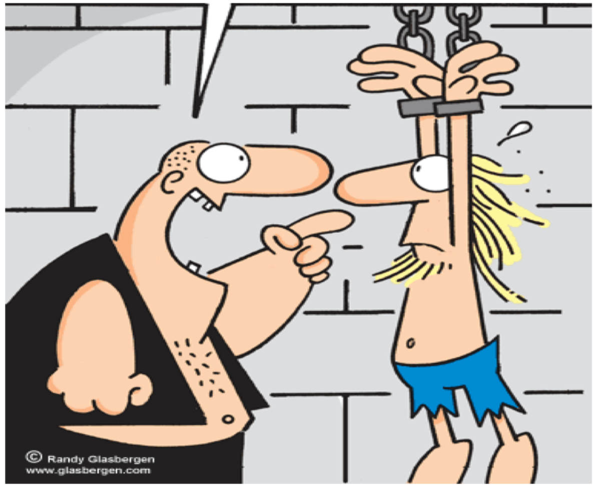
# Is Encryption Perfect for Ensuring Confidentiality of The Data in The Mobile Devices?

- Symmetric encryption is broadly used (rather than asymmetric encryption)
  - AES
  - 3DES

- Conventional encryption is vulnerable to a coercive attack

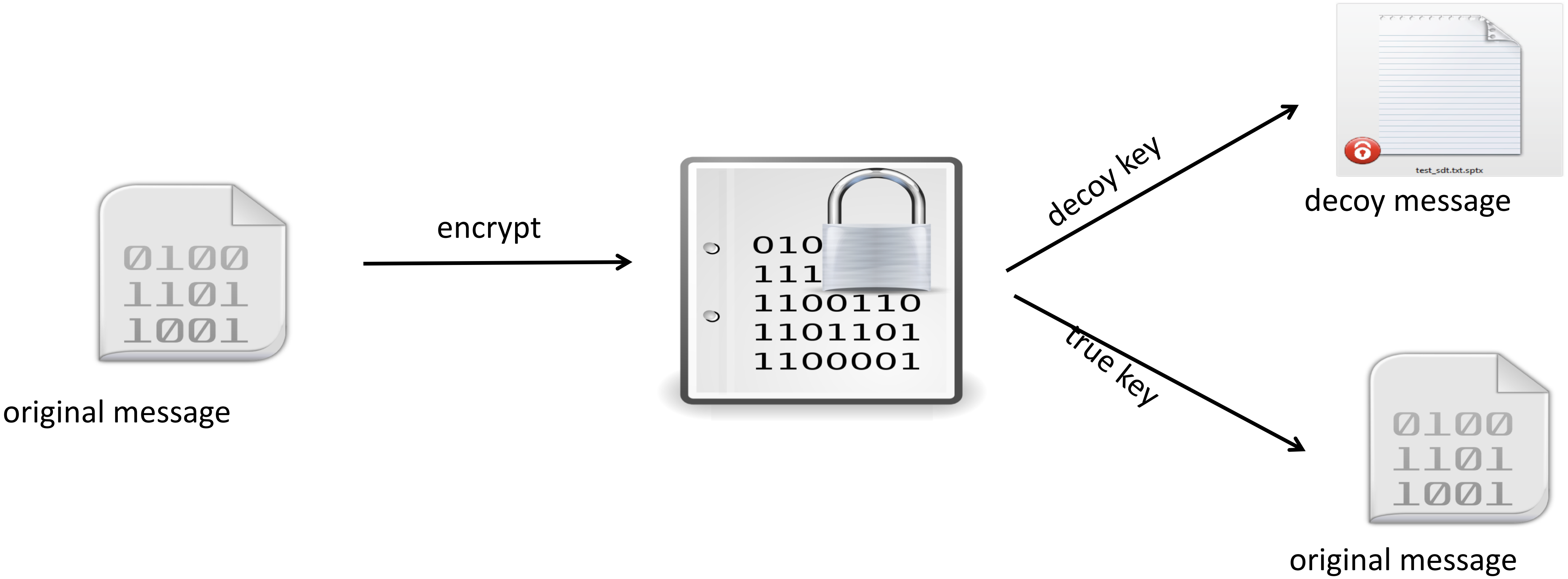
An attacker forces the device's owner to disclose the decryption key

TELL ME YOUR KEY!!!



# Plausible Deniable Encryption (PDE)

- Plausible Deniable Encryption (PDE) [Canetti et al., CRYPTO ’97]: a crypto primitive designed for mitigating coercive attacks
  - Disclose the decoy key
  - Keep the true key secret
  - The decoy message can be used to deny the existence of the original message (deniability)



original message

encrypt

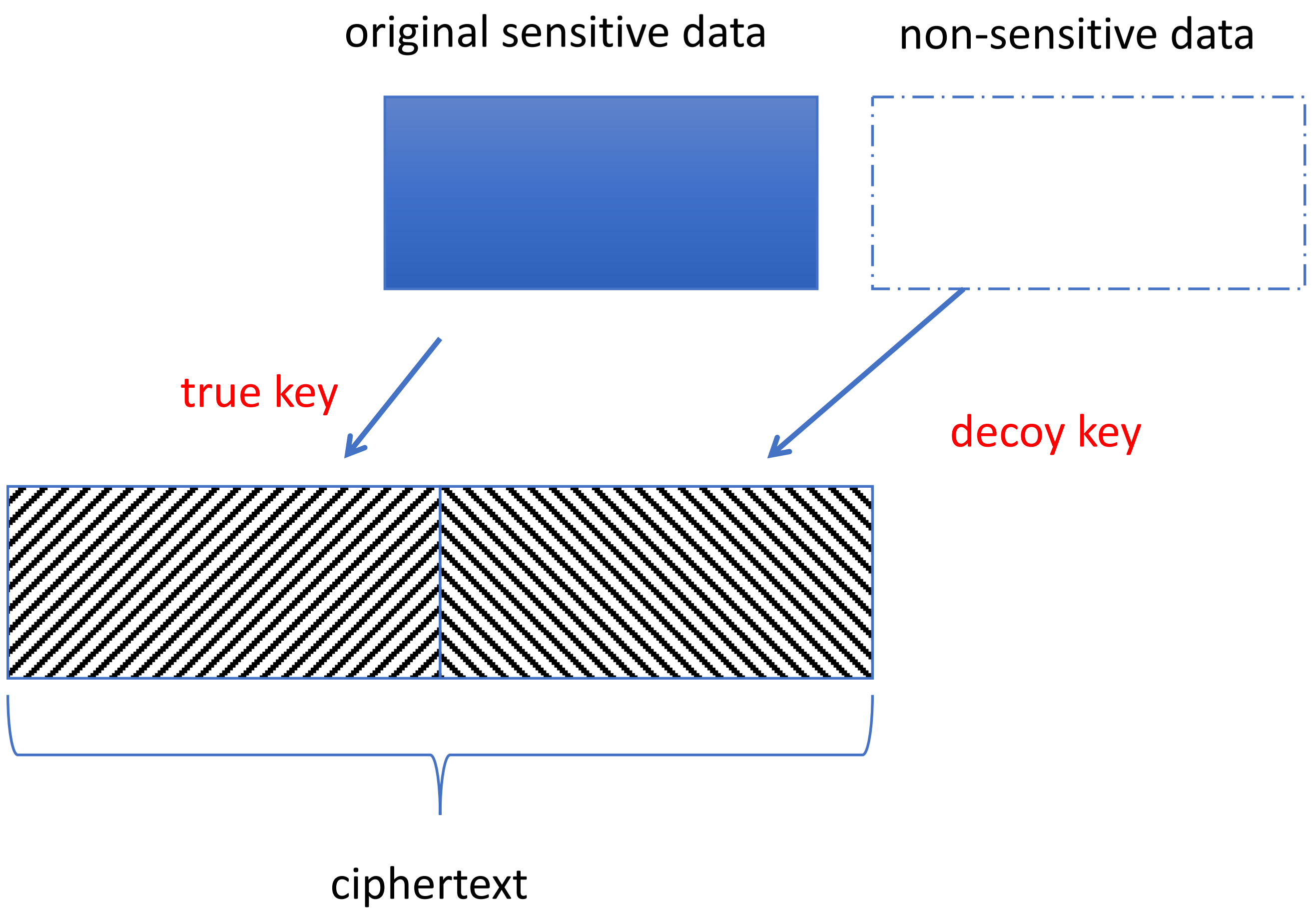
decoy key

true key

decoy message

original message

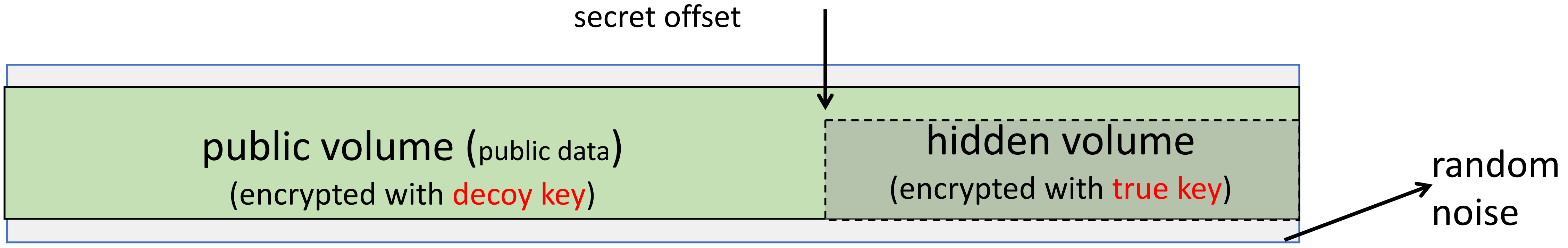
# Instantiate PDE in Cryptography



- Issues: the size of ciphertext is increased. Deniability is easily compromised

# Implementing PDE in Systems (1) - Hidden Volume

- Hidden volume [TRUECRYPT ’04] realizes the concept of PDE in systems
  - Only the decoy key will be disclosed
  - The encrypted hidden volume cannot be differentiated from the random noise (the encrypted hidden volume is denied as the randomness filled initially)



secret offset

public volume (public data)

(encrypted with decoy key)

hidden volume

(encrypted with true key)

random noise

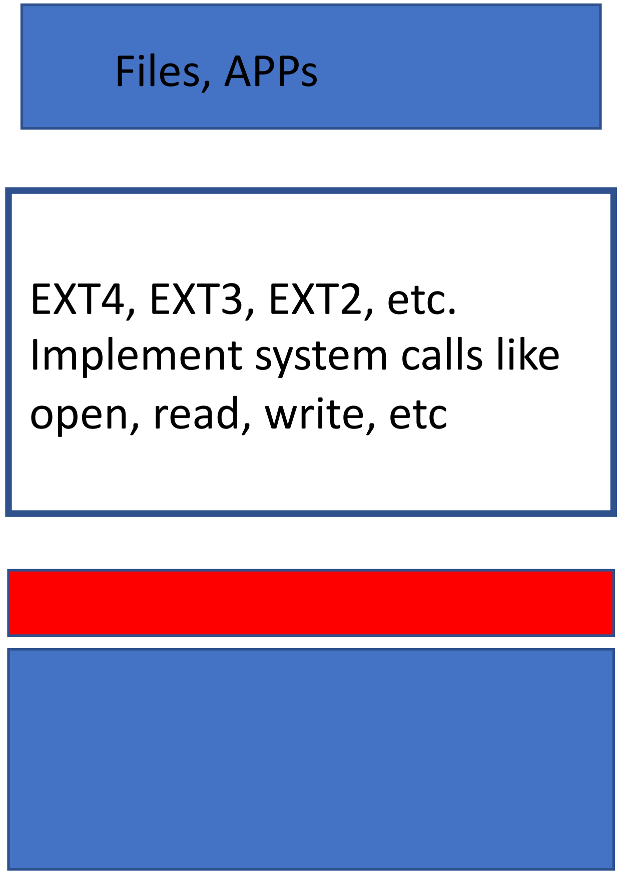
storage medium

# Implementing PDE in Systems (2) – Steganographic File Systems

- Option 1:
  - A few cover files in the systems, and the hidden file is an XOR of these cover files
  - Limitation: difficult to update the hidden file

- Option 2:
  - The file system is initially filled completely with blocks of random data. The file blocks of the hidden file are hidden amongst this random data
  - Limitation: the hidden file may be over-written by the regular files, and we need to store a few redundant copies across the disk.

# Storage Architecture in a Mobile Device



Applications layer

Files, APPs

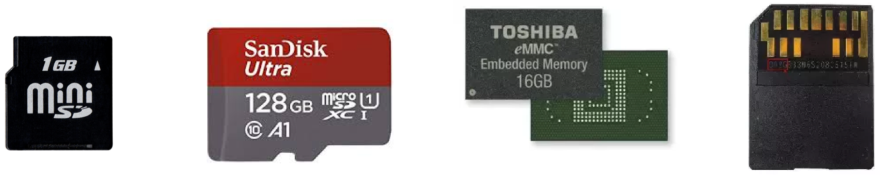
Mobile file system layer

EXT4, EXT3, EXT2, etc.
Implement system calls like open, read, write, etc

Block device layer

Flash memory layer

Manage the mappings between the applications' view and the block device's view



eMMC Chip

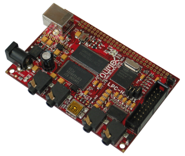
MMC Card

# Research Problems

- How to incorporate PDE concept into real-world mobile devices to allow the device’s owner to survive when facing coercive attacks?
    - Smart phones (e.g., Android phones)
    - Wearable devices (e.g., Android wear smart watches)

- What need to be achieved
    - Security: provide deniability against a coercive adversary who can capture the device owner and the device
        - No deniability leakages in memory/external storage media
        - Defend against a multiple-snapshot adversary
    - Multiple deniability levels: allow different levels of data protection
    - Fast mode switching: can fast switch to the hidden operating mode
    - Compatibility: compatible with different file systems
    - Efficiency: mobile devices are usually light-weight (limited computational power and battery)
    - Etc.

# The Efforts of My Research Group on Building PDE Systems for Mobile Devices



## Publications

- Jinghui Liao, **Bo Chen**, and Weisong Shi. TrustZone Enhanced Plausibly Deniable Encryption System for Mobile Devices. The Fourth ACM/IEEE Workshop on Security and Privacy in Edge Computing (*EdgeSP '21*), San Jose, CA, December 2021.
- Niusen Chen, **Bo Chen**, and Weisong Shi. MobiWear: A Plausibly Deniable Encryption System for Wearable Mobile Devices. The First EAI International Conference on Applied Cryptography in Computer and Communications(*AC3 '21*), Xiamen, China, May 2021.
- **Bo Chen**, and Niusen Chen. A Secure Plausibly Deniable System for Mobile Devices against Multi-snapshot Adversaries. 2020 IEEE Symposium on Security and Privacy (*S&P '20*), San Francisco, CA (online), May 2020 (extended abstract).
- Bing Chang, Fengwei Zhang, **Bo Chen**, Yingjiu Li, Wen Tao Zhu, Yangguang Tian, Zhan Wang, and Albert Ching. MobiCeal: Towards Secure and Practical Plausibly Deniable Encryption on Mobile Devices. The 48th IEEE/IFIP International Conference on Dependable Systems and Networks (*DSN '18*), June 2018.
- Qionglu Zhang, Shijie Jia, Bing Chang, **Bo Chen**. Ensuring Data Confidentiality via Plausibly Deniable Encryption and Secure Deletion - A Survey. *Cybersecurity* (2018) 1: 1.
- Bing Chang, Yao Cheng, **Bo Chen**, Fengwei Zhang, Wen Tao Zhu, Yingjiu Li, and Zhan Wang. User-Friendly Deniable Storage for Mobile Devices. *Elsevier Computers & Security*, vol. 72, pp. 163-174, January 2018.
- Shijie Jia, Luning Xia, **Bo Chen**, and Peng Liu. DEFTL: Implementing Plausibly Deniable Encryption in Flash Translation Layer. 2017 ACM Conference on Computer and Communications Security (*CCS '17*), Dallas, Texas, USA, Oct 30 - Nov 3, 2017.
- Bing Chang, Zhan Wang, **Bo Chen**, and Fengwei Zhang. MobiPluto: File System Friendly Deniable Storage for Mobile Devices. 2015 Annual Computer Security Applications Conference (*ACSAC '15*), Los Angeles, California, USA, December 2015.
- Xingjie Yu, **Bo Chen**, Zhan Wang, Bing Chang, Wen Tao Zhu, and Jiwu Jing. MobiHydra: Pragmatic and Multi-Level Plausibly Deniable Encryption Storage for Mobile Devices. The 17th Information Security Conference (*ISC '14*), Hong Kong, China, Oct. 2014.

## Sponsored project

Hardware-assisted Plausibly Deniable System for Mobile Devices, US National Science Foundation, 10/01/2019 – 09/30/2022, $265K, Grant No. 1928349.

# Paper Presentation

- On Implementing Deniable Storage Encryption for Mobile Devices
- Presented by prior student (recording)