CS 5472 - Advanced Topics in Computer Security

Topic 5: Deniable Encryption (1)

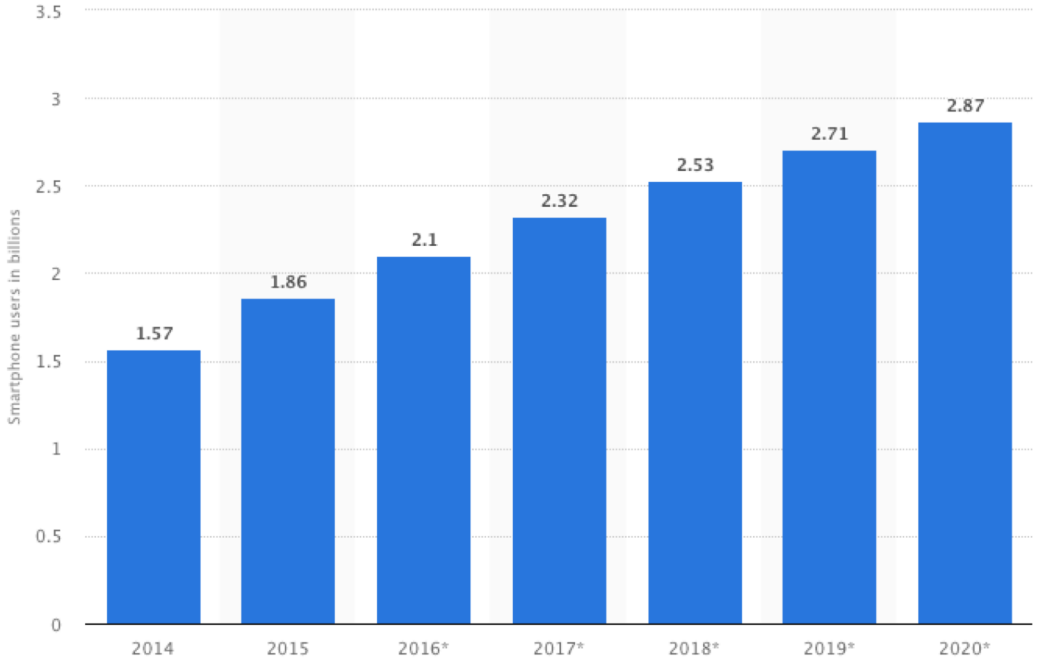
Spring 2018 Semester

Instructor: Bo Chen

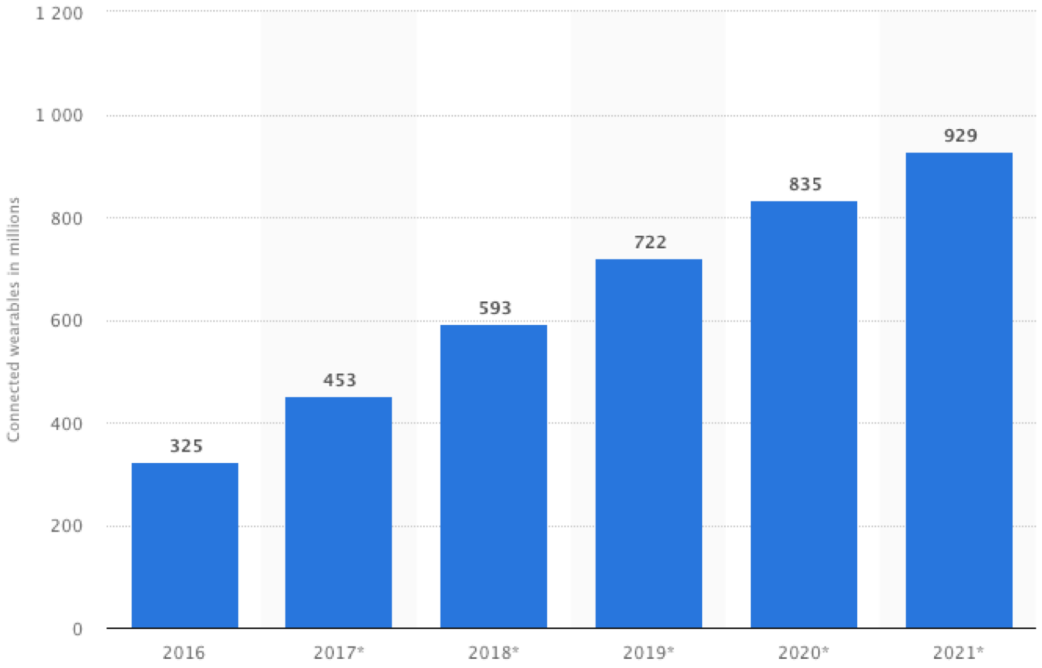
bchen@mtu.edu

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

Mobile Devices are Turning to Mainstream Computing Devices



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



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

Mobile Devices are 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.

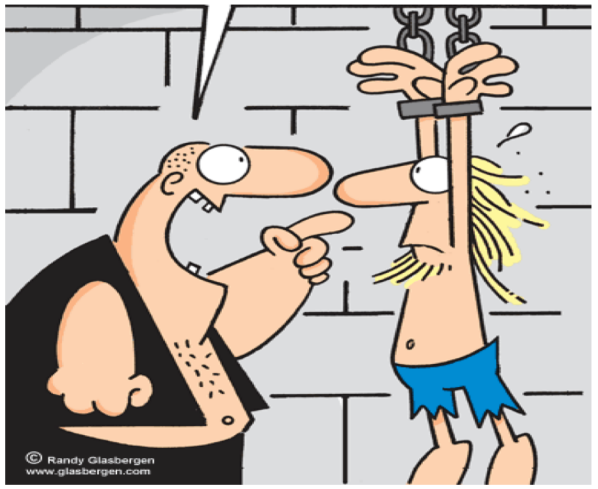
Coercive Attack

- To protect sensitive data, we can simply encrypt them
  - AES
  - 3DES

- Conventional encryption is vulnerable to a coercive attack

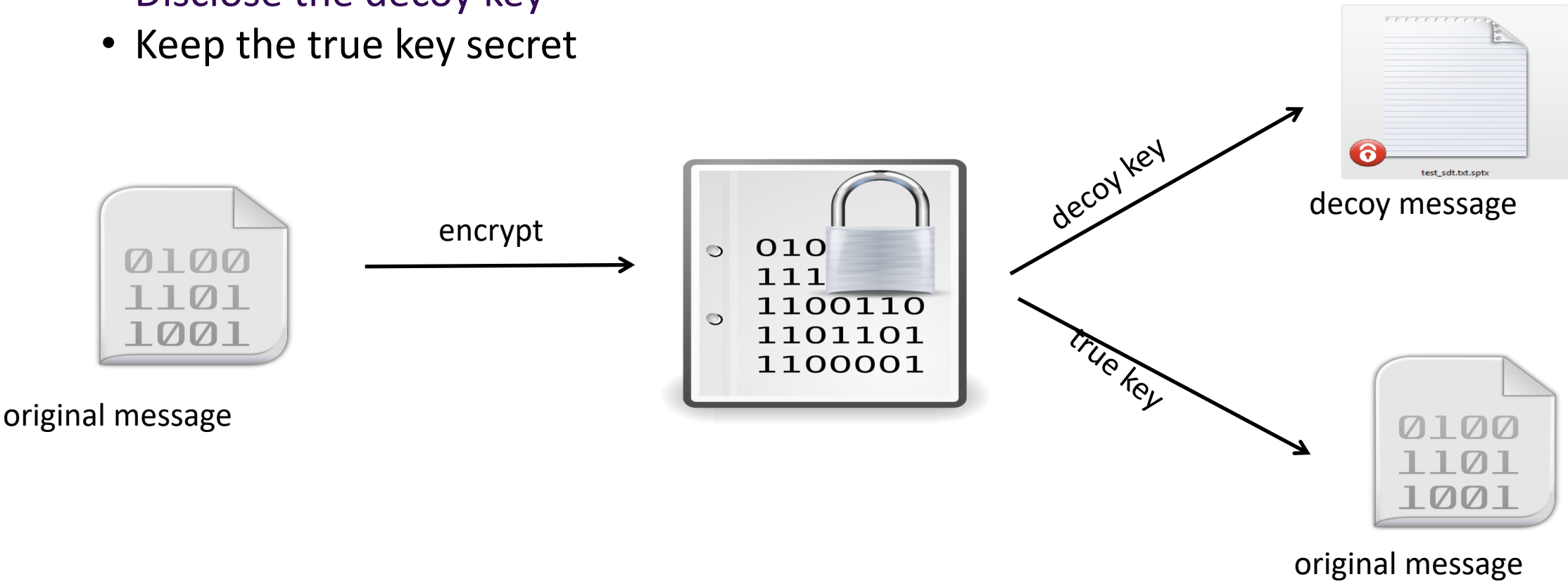
An attacker forces the device's owner to disclose the decryption key

TELL ME YOUR KEY!!!

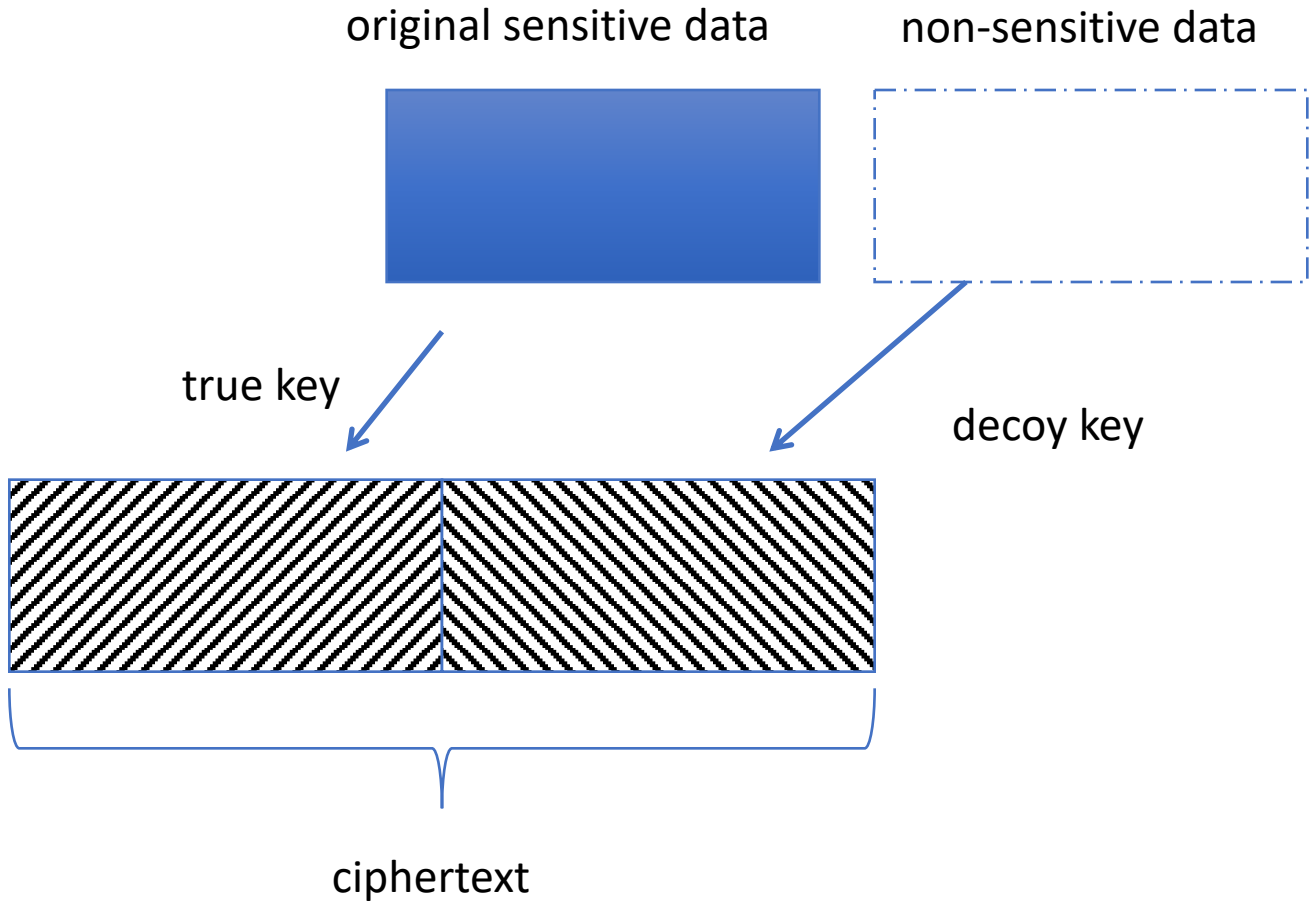


Plausible Deniable Encryption (PDE)

- 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



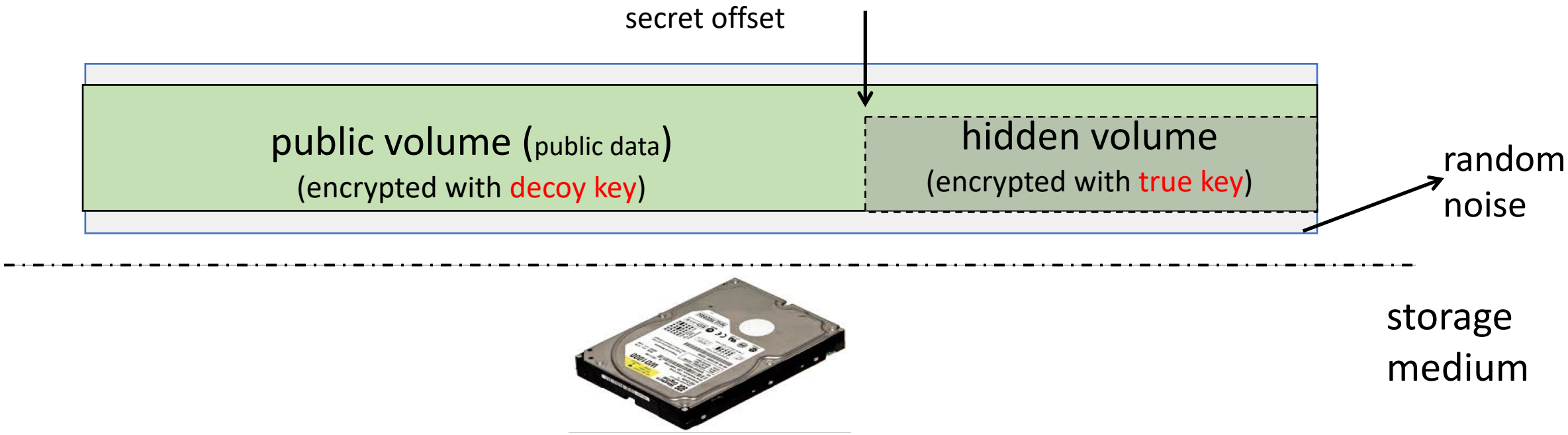
Instantiate PDE in Cryptography



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

Implementing PDE in Systems - 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



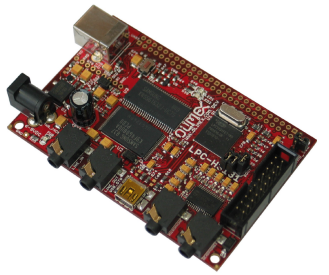
Research Problems

- 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

- 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. Under submission.
- 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.



Paper Presentation

- On Implementing Deniable Storage Encryption for Mobile Devices

- Presented by Manu Nandan Chemudupati