CS 5472 - Advanced Topics in Computer Security

Topic 5: Deniable Encryption (1)

Spring 2019 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu
Review: IoT Security

• Internet of Things (IoT)
• Authentication and access control in home IoT
• Key sharing in home IoT
Mobile Devices are Turning to Mainstream Computing Devices

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 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
  – Authentication
  – Access control
Coercive Attack against Confidentiality

- To protect confidentiality of 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
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
Storage System in a Mobile Device

Applications layer

Files, APPs

Mobile file system layer

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

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

Block device layer

Flash memory layer

etc
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


Paper Presentation

• On Implementing Deniable Storage Encryption for Mobile Devices

• Presented by Vishnu Kamaraju