CS 5472 - Advanced Topics in Computer Security

Topic 6: Deniable Encryption (1)

Spring 2023 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu
A Shift of Focuses

• Topic 1 to 5 are mostly about security of infrastructures
  • Blockchain
  • Cloud computing
  • Future Internet
  • Internet of things
  • Cyber-physical systems

• Next we will focus on security of terminal devices
  • Topic 6: safeguarding confidentiality of the sensitive data in mobile devices via plausibly deniable encryption
  • Topic 7: safeguarding confidentiality of the sensitive data in mobile devices via secure deletion
  • Topic 8: safeguarding integrity of the sensitive data by combating ransomware
Mobile Devices are Turning to Mainstream Computing Devices

Number of smartphone users worldwide from 2013 to 2028 (in billions)
Mobile Devices are Turning to Mainstream Computing Devices (cont.)

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

Sources:
enMarketer: Website (ppc.land) © Statista 2019

Additional Information:
Worldwide: enMarketer 2017 to 2017

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 2022 (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
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)
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)

![Diagram showing public volume and hidden volume with secret offset and random noise]
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.
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


Sponsored project

Hardware-assisted Plausibly Deniable System for Mobile Devices, US National Science Foundation, 10/01/2019 – 09/30/2023, $265K, Grant No. 1928349.
Paper Presentation

• On Implementing Deniable Storage Encryption for Mobile Devices

• Presented by Suruchi (bonus presentation)