Mobile Security Technologies

Chapter 9

Topics

- Encryption methods used in mobile devices to secure data in-transit and at-rest
- Including applications of encryption, such as:
  - full disk encryption
  - file encryption
  - folder encryption
  - encrypting removable media.
- Access control methods

Encryption Basics

- Encryption goal: protect data confidentiality.
- Encryption involves two components, algorithm and key.
- The algorithm is the mathematical construct or theory that is used to manipulate the human readable data (called plaintext) into something that is unreadable (called ciphertext).
- Crypto goals authentication, non repudiation and integrity.

- Algorithms are also publicly known to ensure compatibility between applications and systems.
- Key is the unknown or variable piece that introduces uniqueness and secrecy into the process of encryption that the algorithm performs.
- Reverse is called decryption.

- Encryption keys can come in the form of PINs, passwords, passphrases, or even electronic keys stored in digital certificates.
- Should be constructed so as to be cryptographically strong.
- Keys should be complex and be of sufficient length as to resist attempts to crack them.

- Key space contributes to complexity .
- A complex key would use a large key space, such as numerals 0 through 9, lowercase alphabetic characters a through z, uppercase alphabetic characters A through Z, and special characters, such as !, %, #, &, (,), and so on.
- Large key space, combined with key length, ensures a cryptographically strong key.

- Two major categories, symmetric algorithms and asymmetric algorithms.
- Symmetric algorithms involve the use of only one key, which must be shared between any party that wishes to encrypt and decrypt communications.
- One other way to classify encryption algorithms is to categorize them as block or streaming algorithms. Block algorithms encrypt plaintext in defined chunks or sizes. For example, an algorithm may encrypt plaintext in 64-bit or 128-bit block sizes.
- A block algorithm encrypts a specified chunk of text, and then the next chunk, and so on until it encrypts the entire message.
- A streaming algorithm encrypts only one bit at a time of plaintext.
- The advantage to this is that it is faster than block ciphers, but a disadvantage is that streaming ciphers are typically easier to crack.

- One problem with symmetric cryptography is that this shared key, sometimes called a secret key, must be shared securely and not intercepted by any party that shouldn't participate in the communications session.
- Another problem in symmetric cryptography is that of scalability.
- The more parties you wish to securely communicate with separately, the more keys you must maintain in order to keep your communications with each and every one of them separate from the others.

- In asymmetric cryptography (also called public key cryptography), a pair of two keys is used for the encryption and decryption process. One key is a public key that anyone can have access to, and the other key in the pair is kept private or confidential by the individual that owns the key pair.
- Because anyone can have the public key, key exchange is typically not a problem.

- Encryption is primarily used to ensure data confidentiality and data integrity.
- Application of encryption is found in processes such as hashing, drive and folder encryption, certificate-based authentication, and other applications.

DES

- The Data Encryption Standard (DES) is an older block cipher encryption algorithm (implemented in 1977).
  - DES based upon Lucifer algorithm
- DES operates in five modes.
- Modes determine how plaintext is input and manipulated to produce the resulting ciphertext. modes operate on plaintext by manipulating it in specified size blocks of data (in the case of block ciphers), and introduce keys (variables) into the process to encrypt the data.
- The mode may also involve performing certain other mathematical functions on the data to more thoroughly encrypt it, sometimes repeating operations over several rounds (iterations).
- The modes also may manipulate the data and keys in different ways to produce stronger encryption.