Cryptography context

Cryptography algorithm definition A method or system for transforming given information in order to conceal its meaning

Cryptography system statistical building blocks since 1949
- Diffusion to thwart key discovery seeks to make the statistical relationship between plaintext and the cryptogram as complex as possible
- Confusion to thwart key discovery seeks to make the relationship between the statistics of the cryptogram and the value of the encryption key as complex as possible

Outline

1. Cryptography context
   - Cryptography definitions
   - Cryptography hardware
   - Cryptography major components
     - Asymmetric ciphers
     - Symmetric ciphers
     - Authenticators
     - Key management and key schedules
   - The ultimate prize
     - How MSFT Bitlocker works
     - Key discovery
     - Key schedule analysis
     - AESKEYFIND.C
   - Princeton cold boot attack
     - Memory without power
     - Memory statistics
   - Countermeasures

2. Countermeasures
   - References
DoD/NSA cryptography hardware

1. Link encryption KG-13, 75, 84, 175, 189, 192
2. Still in use, New technology emulates old
3. High Assurance IP Interoperability Specification

Outline

1. Cryptography context
   - Cryptography definitions
   - Cryptography hardware
2. Cryptography major components
   - Asymmetric ciphers
   - Symmetric ciphers
   - Authenticators
   - Key management and key schedules
3. The ultimate prize
   - How MSFT Bitlocker works
   - Key discovery
   - Key schedule analysis
   - AESKEYFIND.C
4. Princeton cold boot attack
   - Memory without power
   - Memory statistics
5. Countermeasures
6. References

Classification of cryptography major components

- Ciphers
  - Diffie-Hellman Key Exchange
  - Symmetric DES
  - Asymmetric RSA
  - Symmetric IDEA
  - Symmetric Blowfish
  - Symmetric AES
- Authenticators
  - SHA
  - MD5
- Key management and key schedules

Outline

1. Cryptography context
   - Cryptography definitions
   - Cryptography hardware
2. Cryptography major components
   - Asymmetric ciphers
   - Symmetric ciphers
   - Authenticators
   - Key management and key schedules
3. The ultimate prize
   - How MSFT Bitlocker works
   - Key discovery
   - Key schedule analysis
   - AESKEYFIND.C
4. Princeton cold boot attack
   - Memory without power
   - Memory statistics
5. Countermeasures
6. References

Asymmetric ciphers

Asymmetric Key Cryptography

Outline

1. Cryptography context
   - Cryptography definitions
   - Cryptography hardware
2. Cryptography major components
   - Asymmetric ciphers
   - Symmetric ciphers
   - Authenticators
   - Key management and key schedules
3. The ultimate prize
   - How MSFT Bitlocker works
   - Key discovery
   - Key schedule analysis
   - AESKEYFIND.C
4. Princeton cold boot attack
   - Memory without power
   - Memory statistics
5. Countermeasures
6. References
Cryptography context

Cryptography major components

The ultimate prize

Princeton cold boot attack

Countermeasures

References

Authenticators

Password Use of Hash Function

Key management and key schedules

Key distribution

- Manual delivery to both parties
- Use previous key to encrypt and transmit

AES CBC Key schedules

Outline

Cryptography context

- Cryptography definitions
- Cryptography hardware

Cryptography major components

- Asymmetric ciphers
  - Symmetric ciphers
- Authenticators
- Key management and key schedules

The ultimate prize

- How MSFT Bitlocker works
- Key discovery
- Key schedule analysis
- AESKEYFIND.C

Princeton cold boot attack

- Memory without power
- Memory statistics

Countermeasures

References

Outline

Cryptography context

- Cryptography definitions
- Cryptography hardware

Cryptography major components

- Asymmetric ciphers
  - Symmetric ciphers
- Authenticators
- Key management and key schedules

The ultimate prize

- How MSFT Bitlocker works
- Key discovery
- Key schedule analysis
- AESKEYFIND.C

Princeton cold boot attack

- Memory without power
- Memory statistics

Countermeasures

References

Outline

Cryptography context

- Cryptography definitions
- Cryptography hardware

Cryptography major components

- Asymmetric ciphers
  - Symmetric ciphers
- Authenticators
- Key management and key schedules

The ultimate prize

- How MSFT Bitlocker works
- Key discovery
- Key schedule analysis
- AESKEYFIND.C

Princeton cold boot attack

- Memory without power
- Memory statistics

Countermeasures

References

Outline

Cryptography context

- Cryptography definitions
- Cryptography hardware

Cryptography major components

- Asymmetric ciphers
  - Symmetric ciphers
- Authenticators
- Key management and key schedules

The ultimate prize

- How MSFT Bitlocker works
- Key discovery
- Key schedule analysis
- AESKEYFIND.C

Princeton cold boot attack

- Memory without power
- Memory statistics

Countermeasures

References
The ultimate prize

- Unlock encrypted full volume disks
- MSFT Bitlocker requirements
  - Disk sectors sizes 512, 1024, 2048, 4096, 8192
  - Sector number input to encryption/decryption
  - Maintains confidentiality of plaintext
  - Acceptable performance slow-down
  - Validated by public scrutiny
  - Attacker cannot predict plaintext if changes are made to ciphertext of a sector
- How MSFT Bitlocker works to balance security and performance

How MSFT Bitlocker works

- Balancing security and performance

Crypto key discovery

- Crypto key discovery methods
  - Exploit key management
  - Brute force
  - Source code analysis
  - Key schedule analysis
Princeton cold boot attack

- Memory remembers without power How long

<table>
<thead>
<tr>
<th>Memory Type</th>
<th>Chip</th>
<th>Memory Density</th>
<th>Model/Model</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>DDR4</td>
<td>1333</td>
<td>Dell Optiplex 9020</td>
<td>2015</td>
</tr>
<tr>
<td>B</td>
<td>DDR3</td>
<td>1600</td>
<td>Dell Optiplex 7020</td>
<td>2013</td>
</tr>
<tr>
<td>C</td>
<td>DDR4</td>
<td>2666</td>
<td>Dell Optiplex 7020</td>
<td>2013</td>
</tr>
<tr>
<td>D</td>
<td>DDR2</td>
<td>667</td>
<td>Dell Optiplex 7020</td>
<td>2006</td>
</tr>
</tbody>
</table>

- Error % at operating temp. Error % at ~50°C

<table>
<thead>
<tr>
<th>Memory Type</th>
<th>Temp</th>
<th>Error %</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>41</td>
<td>0.000001</td>
</tr>
<tr>
<td>B</td>
<td>50</td>
<td>0.000001</td>
</tr>
<tr>
<td>C</td>
<td>41</td>
<td>0.000001</td>
</tr>
<tr>
<td>D</td>
<td>50</td>
<td>0.000001</td>
</tr>
</tbody>
</table>

Countermeasures

- Intel AES instruction set extension
- Physical protection of memory
- Design DRAM to decay quickly
- Trusted Platform Module

References

References

- Feldman, aeskeyfind.c, 2008.