Cryptographic Implementation Attacks

Check Point
June 25, 2010

Joseph Bonneau
Security Group
jcb82@cl.cam.ac.uk
Insecure MAC checking routine #1

```c
int check_MAC(u_char * test, u_char * correct) {
    return (strcmp(test, correct) == 0);
}
```
Insecure MAC checking routine #1

```c
int check_MAC(u_char * test, u_char * correct){
    return (strcmp(test, correct) == 0);
}

int strcmp(u_char *s1, u_char *s2){
    while (*s1 != '\0' && *s1 == *s2) {
        s1++;
        s2++;
    }

    return ((*s1 < *s2) ? -1 : (*s1 > *s2));
}
```
Insecure MAC checking routine #1

```c
int check_MAC(u_char * test, u_char * correct)
{
    return (strcmp(test, correct) == 0);
}

int strcmp(u_char *s1, u_char *s2)
{
    while (*s1 != '\0' && *s1 == *s2) {
        s1++;
        s2++;
    }

    return ((*s1 < *s2) ? -1 : (*s1 > *s2));
}
```

≈ |A| queries 😞
Insecure MAC checking routine #2

```c
int check_MAC(u_char * test, u_char * correct) {
    return (strcmp(test, correct, LEN) == 0);
}

int memcmp(u_char *s1, u_char *s2, size_t n) {
    while (n-- != 0) {
        if (*s1 != *s2)
            return 1;
        s1++;
        s2++;
    }
    return 0;
}
```
Insecure MAC checking routine #2

```c
int check_MAC(u_char * test, u_char * correct) {
    return (strcmp(test, correct, LEN) == 0);
}
```

```c
int memcmp(u_char *s1, u_char *s2, size_t n) {
    while (n-- != 0) {
        if (*s1 != *s2)
            return 1;
        s1++;
        s2++;
    }
    return 0;
}
```

\( \approx n \cdot |A| \) queries
MAC timing attack against Xbox 360

C:\Documents and Settings\Administrator\Desktop\360\DGTool>DGTool.exe 1 Infectus_5759#4_1888_build2.bin

Pairing Data 0x6DF3B8 01
Turn on your Xbox, press any key when the RRoD starts

H[0 00XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17821 A 17821 D 0 : 0 NEXT
H[0 01XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17817 A 17819 D -3 : 0 NEXT
H[0 02XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17822 A 17820 D 3 : 0 NEXT
...
H[0 1AXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17822 A 17819 D 3 : 0 NEXT
H[0 1BXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17831 A 17819 D 12 : 11 RPT
H[0 1BXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17830 A 17819 D 11 : 0 HIT!
H[1 1B00XXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17830 A 17830 D 0 : 0 NEXT
H[1 1B01XXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17829 A 17829 D -1 : 0 NEXT
...
H[1 1BFDXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17844 A 17830 D 14 : 8 RPT
H[1 1BFDXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17839 A 17830 D 9 : 0 HIT!
H[2 1BFD00XXXXXXXXXXXXXXXXXXXXXXXXX] M 17839 A 17838 D 1 : 0 NEXT
H[2 1BFD01XXXXXXXXXXXXXXXXXXXXXXXXX] M 17844 A 17841 D 4 : 0 NEXT
...
H[2 1BFDF0XXXXXXXXXXXXXXXXXXXXXXXXX] M 17856 A 17841 D 15 : 11 RPT
H[2 1BFDF0XXXXXXXXXXXXXXXXXXXXXXXXX] M 17851 A 17841 D 10 : 0 HIT!
...
H[15 1BFDF0625C214F67CD94DCA3FC47CA55] M 18014 A 17988 D 16 : 0 HIT!

Correct hash: 1BFDF0625C214F67CD94DCA3FC47CA55
Result: BOOT
MAC timing attack against Xbox 360

C:\Documents and Settings\Administrator\Desktop\360\DGTool>DGTool.exe 1 Infectus_5759#4_1888_build2.bin

Pairing Data 0x6DF3B8 01
Turn on your Xbox, press any key when the RRoD starts
H[0 00XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17821 A 17821 D 0 : 0 NEXT
H[0 01XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17817 A 17819 D -3 : 0 NEXT
H[0 02XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17822 A 17820 D 3 : 0 NEXT
... H[0 1AXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17822 A 17819 D 3 : 0 NEXT
H[0 1BXXXXXXXXXXXXX] M 17831 A 17819 D 12 : 11 RPT
H[0 1BXXXXXXXXXXXXX] M 17830 A 17819 D 11 : 0 HIT!
H[1 1B00XXXXXXXXXXXXXXXXXXXXXXXXXX] M 17830 A 17830 D 0 : 0 NEXT
H[1 1B01XXXXXXXXXXXXXXXXXXXXXXXXXX] M 17829 A 17829 D -1 : 0 NEXT
... H[1 1BFDFXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17844 A 17830 D 14 : 8 RPT
H[1 1BFDFXXXXXXXXXXXXXXXXXXXXXXXXXX] M 17839 A 17830 D 9 : 0 HIT!
H[2 1BFD00XXXXXXXXXXXXXXXXXXXXXXXXX] M 17839 A 17838 D 1 : 0 NEXT
H[2 1BFD01XXXXXXXXXXXXXXXXXXXXXXXXX] M 17844 A 17841 D 4 : 0 NEXT
... H[2 1BFDF0XXXXXXXXXXXXXXXXXXXXXXXXX] M 17856 A 17841 D 15 : 11 RPT
H[2 1BFDF0XXXXXXXXXXXXXXXXXXXXXXXXX] M 17851 A 17841 D 10 : 0 HIT!
... H[15 1BFDF0625C214F67CD94DCA3FC47CA55] M 18014 A 17988 D 16 : 0 HIT!

Correct hash: 1BFDF0625C214F67CD94DCA3FC47CA55
Result: BOOT

≈ 2,000 queries
int check_MAC(u_char * test, u_char * correct){
    return (strcmp(test, correct, LEN) == 0);
}

int safecmp(u_char *s1, u_char *s2, size_t n){
    int result = 0;
    while (n-- != 0) {
        if (*s1 != *s2)
            result = 1;
        s1++;
        s2++;
    }
    return result;
}
Insecure MAC checking routine #3

```c
int check_MAC(u_char * test, u_char * correct){
    return (strcmp(test, correct, LEN) == 0);
}

int safecmp(u_char *s1, u_char *s2, size_t n){
    int result = 0;
    while(n-- != 0) {
        if (*s1 != *s2)
            result = 1;
        s1++;
        s2++;
    }
    return result;
}
```

≈ n · |A| queries
Secure MAC checking routine?

```c
int check_MAC(u_char * test, u_char * correct) {
    return (strcmp(test, correct, LEN) == 0);
}

int safercmp(u_char *s1, u_char *s2, size_t n) {
    int result = 0;
    while (n-- != 0) {
        result &= (*s1 ^ *s2);
        s1++;
        s2++;
    }
    return !result;
}
```
Rule #0: Attackers will always cheat

A CRYPTO NERD'S IMAGINATION:
His laptop's encrypted.
Let's build a million-dollar cluster to crack it.

NO GOOD! IT'S 4096-BIT RSA!
BLAST! Our evil plan is foiled!

WHAT WOULD ACTUALLY HAPPEN:
His laptop's encrypted.
Drug him and hit him with this $5 wrench until he tells us the password.

GOT IT.
Crypto design processes ignore(d) cheating
Side Channels: whatever the designers ignored

\[ c = m^e \mod N \]

\[ T_0 = K_0 \oplus P_0 \]
Side Channels: whatever the designers ignored

Key \rightarrow \text{Encryption} \rightarrow \text{Ciphertext}

Plaintext
Side Channels: whatever the designers ignored
Side Channels: whatever the designers ignored

Key → Plaintext → Encryption → Ciphertext

- Time
- Power
- Noise
- Heat
- EM radiation
Definition

Side-channel cryptanalysis is any attack on a cryptosystem requiring information emitted as a byproduct of the physical implementation.
Related attacks
White box cryptanalysis: nothing is hidden

- Key
- Plaintext
- Encryption
- Ciphertext

```
int k[] = {0x1e, ...}
```

- Debugger
- Static analysis
- Memory dumps
TEMPEST: EM signals containing full secrets

Key -> Plaintext -> Encryption -> Ciphertext
Fault injection: inducing a telling error

Key → Encryption → Ciphertext

Plaintext
Hardware attacks: breaking the box open

Key → Plaintext → Encryption → Ciphertext
Covert channels: attack code running from within

Key -> Plaintext -> Encryption -> Ciphertext
Attacks against RSA
RSA: The original public key algorithm
RSA: The original public key algorithm

<table>
<thead>
<tr>
<th>Private Key:</th>
<th>p, q</th>
<th>(random primes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>d ≡ e^{-1} (mod φ(N))</td>
<td>(exponent)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Public Key:</th>
<th>N = p \cdot q</th>
<th>(modulus)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>e</td>
<td>(exponent)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Encryption:</th>
<th>c = m^e (mod N)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Verification:</th>
<th>m = c^d (mod N)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Signing:</th>
<th>s = m^d (mod N)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Verification:</th>
<th>m = s^e (mod N)</th>
</tr>
</thead>
</table>
RSA is implemented via square-and-multiply

\[
\begin{align*}
\text{b}^{65553} & \equiv \text{b}^{0x10011} \pmod{N} \\
\equiv \text{b}^{10000000000010001} \pmod{N} \\
\equiv \text{b}^{65536 \cdot b^{16} \cdot b^{1}} \pmod{N}
\end{align*}
\]

\(n\) digit exponentiation requires \(\log n\) squares, up to \(\log n\) multiplications.
RSA is implemented via square-and-multiply

```python
def power(b, e, N):
    result = 1

    for i in range(len(e)-1, -1):
        result = square(result, N)
        if bit_set(e, i):
            result = mult(result, b, N)

    return result
```

Simple power analysis of RSA
(Paul Kocher et. al 1999)
Simple power analysis setup

Key -> Plaintext -> Encryption -> Ciphertext
What does power consumption reveal?

Trace courtesy of Cryptography Research, Inc.
Each set exponent bit inserts a multiplication

```python
def power(b, e, N):
    result = 1

    for i in range(len(e)-1, -1):
        result = square(result, N)
        if bit_set(e, i):
            result = mult(result, b, N)

    return result
```
Multiplies can often be visually detected.

Trace courtesy of Cryptography Research, Inc.
Multiplies can often be visually detected.

Trace courtesy of Cryptography Research, Inc.
Secret exponent can be easily read out

Trace courtesy of Cryptography Research, Inc.
Secret exponent can be easily read out

1 encryption

Trace courtesy of Cryptography Research, Inc.
def power(b, e, N):
    result = 1
    b = mult(b, r, N)
    for i in range(len(e)-1, -1, -1):
        result = square(result, N)
        if bit_set(e, i):
            result = mult(result, b, N)
        else:
            result = mult(result, r, N)
    return mult(result, r_inverse, N)
Timing attack against RSA
(Paul Kocher 1996)
Timing attack setup

Key → Plaintext → Encryption → Ciphertext
def power(b, e, N):
    result = 1

    for i in range(len(e)-1, -1, -1):
        result = square(result, N)
        if bit_set(e, i):
            result = mult(result, b, N)

    return result
Timing of individual multiplies varies significantly

Kocher 1996
Need a model relating multiplication inputs to time

Example:

2345 \cdot 6789 \pmod{9997}

Multiply: \quad 2345 \cdot 6826 = 16006970

Reduce: \quad 16006970 - 9997 \cdot 1 \cdot 1000
\quad = 6009970 - 9997 \cdot 6 \cdot 100
\quad = 11770 - 9997 \cdot 0 \cdot 10
\quad = 11770 - 9997 \cdot 1 \cdot 1
\quad = 1773
def power(b, e, N):
    result = 1

    for i in range(len(e) - 1, -1):
        result = square(result, N)
        if bit_set(e, i):
            result = mult(result, b, N)

    return result
Attack exponent one bit at a time

\[ T = \text{observed timing of entire algorithm} \]

\[ M = \text{model for time of one multiplication} \]

Bit n-1: always 1
Attack exponent one bit at a time

$T = \text{observed timing of entire algorithm}$
$M = \text{model for time of one multiplication}$

Bit n-2:

Is $T(power(r, e, N)) \propto$
$M(mult(1, r, N)) +$
$M(square(r, N)) +$
$M(mult(r^2, r, N)) +$
$M(square(r^3, N))?$
Attack exponent one bit at a time

\[ T = \text{observed timing of entire algorithm} \]
\[ M = \text{model for time of one multiplication} \]

Bit n-2: \( \text{Is } T(\text{power}(r, e, N)) \propto M(\text{mult}(1, r, N)) + \]
\( M(\text{square}(r, N)) + \]
\( M(\text{mult}(r^2, r, N)) + \]
\( M(\text{square}(r^3, N)) \)?
Attack exponent one bit at a time

$T = \text{observed timing of entire algorithm}$

$M = \text{model for time of one multiplication}$

Bit n-3:

$\text{Is } T(\text{power}(r, e, N)) \propto$

$M(\text{mult}(1, r, N)) \cdot e[n-1] +$

$M(\text{square}(r, N)) +$

$M(\text{mult}(r^{2 \cdot e[n-1:n-1]}, r, N)) \cdot e[n-2] +$

$M(\text{square}(r^{e[n-1:n-2]}, N))$

$M(\text{mult}(r^{2 \cdot e[n-1:n-2]}, r, N)) +$

$M(\text{square}(r^{e[n-1:n-2]||1}, N))?$
Attack exponent one bit at a time

\( T = \) observed timing of entire algorithm

\( M = \) model for time of one multiplication

Bit n-3: \( \) Is \( T(\text{power}(r, e, N)) \propto \)

\[ M(\text{mult}(1, r, N)) \cdot e^{[n-1]} + \]

\[ M(\text{square}(r, N)) + \]

\[ M(\text{mult}(r^{2 \cdot e^{[n-1:m-1]}}, r, N)) \cdot e^{[n-2]} + \]

\[ M(\text{square}(r^{e^{[n-1:m-2]}}, N)) \]

\[ M(\text{mult}(r^{2 \cdot e^{[n-1:m-2]}}, r, N)) + \]

\[ M(\text{square}(r^{e^{[n-1:m-2]} || 1}, N)) \]?
Attack exponent one bit at a time

\[ T = \text{observed timing of entire algorithm} \]
\[ M = \text{model for time of one multiplication} \]

Bit \( n-i \):

Is \( T(\text{power}(r, e, N)) \propto M(\text{mult}(r^{2 \cdot e^{[n-1:n-i]}}, r, N)) + M(\text{square}(r^{e^{[n-1:n-i]}\|1}, N)) \)?
Attack exponent one bit at a time

\[ T = \text{observed timing of entire algorithm} \]

\[ M = \text{model for time of one multiplication} \]

Bit n-i: \[ \operatorname{Is} T(\text{power}(r, e, N)) \propto \]

\[ M(\text{mult}(r^{2e_{[n-1:n-i]}}, r, N)) + M(\text{square}(r^{e_{[n-1:n-i]}||1}, N)) \approx 2,500 \text{ encryptions} \]
More complicated attacks work across a LAN

Boneh and Brumley, 2003
More complicated attacks work across a LAN

\[ \approx 1,000,000 \text{ encryptions} \]

Boneh and Brumley, 2003
Blinded RSA provides generic defense

Private Key: \( p, q \) (random primes)
\( d \equiv e^{-1} \pmod{\varphi(N)} \) (exponent)

Public Key: \( N = p \cdot q \) (modulus)
\( e \) (exponent)

Signing: \( s = m^d \pmod{N} \)

Blind Signing: \( r_1 = r_0^e \pmod{N} \)
\( s = r_0^{-1} (r_1 \cdot m)^d \pmod{N} \)
Attacks against AES (aka Rijndael)
AES is cryptography's standard block cipher
AES is very complicated
AES is very complicated

SubBytes

Wikipedia
AES is very complicated

Wikipedia
AES is very complicated
AES is very complicated
AES is designed for very efficient implementation

\[
\begin{align*}
t_0 &= \text{Te0}[(s_0 >> 24)] \quad ^{\uparrow} \\
     &\quad \text{Te1}[(s_1 >> 16) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{Te2}[(s_2 >> 8) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{Te3}[(s_3) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{rk}[0]; \\
t_1 &= \text{Te0}[(s_1 >> 24)] \quad ^{\uparrow} \\
     &\quad \text{Te1}[(s_2 >> 16) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{Te2}[(s_3 >> 8) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{Te3}[(s_0) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{rk}[1]; \\
t_2 &= \text{Te0}[(s_2 >> 24)] \quad ^{\uparrow} \\
     &\quad \text{Te1}[(s_3 >> 16) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{Te2}[(s_0 >> 8) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{Te3}[(s_1) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{rk}[2]; \\
t_3 &= \text{Te0}[(s_3 >> 24)] \quad ^{\uparrow} \\
     &\quad \text{Te1}[(s_0 >> 16) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{Te2}[(s_1 >> 8) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{Te3}[(s_2) \& 0xff] \quad ^{\uparrow} \\
     &\quad \text{rk}[3];
\end{align*}
\]
AES utilises large pre-computed lookup tables

```c
static const u32 Te0[256] = {
    0xc66363a5U, 0xf87c7c84U, 0xee777799U, 0xf67b7b8dU,
    0xfff2f20dU, 0xd66b6bbdU, 0xde6f6fb1U, 0x91c5c554U,
    0x60303050U, 0x02010103U, 0xce6767a9U, 0x562b2b7dU,
    0xe7fefe19U, 0xb5d7d762U, 0x4dababe6U, 0xec76769aU,
    ...  
    0x824141c3U, 0x299999b0U, 0x5a2d2d77U, 0x1e0f0f11U,
    0x7bb0b0cbU, 0xa85454fcU, 0x6dbbbbd6U, 0x2c16163aU,
};
```
Lookups into shared cache are vulnerable
Lookups into shared cache are vulnerable

Plaintext → Key XOR → Lookup → Mix → Key XOR → Ciphertext

First round: $T[P_i \oplus K_i]$
Lookups into shared cache are vulnerable

First round: $T[P_i \oplus K_i]

Final round: $T[T^3[C_i \oplus K_i]]$
Simple power analysis of AES
(Bertoni et. Al, 2005; Bonneau 2006)
Cache hit/miss is very obvious in power trace

Bertoni et. al, 2005
Every miss yields many constraints

Plaintext

Key XOR

Lookup

Miss?
P_0 \oplus K_0 \neq P_1 \oplus K_1

Hit?
P_0 \oplus K_0 = P_1 \oplus K_1
Every miss yields many constraints

Plaintext

Key XOR

Lookup

Miss?

\[
\begin{align*}
P_0 \oplus K_0 &\neq P_1 \oplus K_1 \\
P_0 \oplus P_1 &\neq K_0 \oplus K_1
\end{align*}
\]

Hit?

\[
\begin{align*}
P_0 \oplus K_0 &\overset{?}= P_1 \oplus K_1 \\
P_0 \oplus P_1 &\overset{?}= K_0 \oplus K_1
\end{align*}
\]
Every miss yields many constraints

\[ P_0 \oplus P_2 \not= K_0 \oplus K_2 \land P_1 \oplus P_2 \not= K_1 \oplus K_2 \]
Table of possible key byte differences refined

<table>
<thead>
<tr>
<th></th>
<th>K0</th>
<th>K1</th>
<th>K2</th>
<th>...</th>
<th>K15</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0</td>
<td>00</td>
<td>{27,e0}</td>
<td>{35}</td>
<td>{23,70,c4}</td>
<td>{65}</td>
</tr>
<tr>
<td>K1</td>
<td></td>
<td>00</td>
<td>{32,45,89}</td>
<td>{5f,f3}</td>
<td>{0a,db}</td>
</tr>
<tr>
<td>K2</td>
<td></td>
<td></td>
<td>00</td>
<td>{86}</td>
<td>{17,64,9c}</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td>00</td>
<td>{42,d5}</td>
</tr>
<tr>
<td>K15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00</td>
</tr>
</tbody>
</table>
Table of possible key byte differences refined

<table>
<thead>
<tr>
<th></th>
<th>K0</th>
<th>K1</th>
<th>K2</th>
<th>...</th>
<th>K15</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0</td>
<td>00</td>
<td>{27,e0}</td>
<td>{35}</td>
<td>{23,70,c}</td>
<td>{65}</td>
</tr>
<tr>
<td>K1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>{0a,db}</td>
</tr>
<tr>
<td>K2</td>
<td></td>
<td></td>
<td>00</td>
<td>{86}</td>
<td>{17,64,9}</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td>00</td>
<td></td>
<td>{42,d5}</td>
</tr>
<tr>
<td>K15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>00</td>
</tr>
</tbody>
</table>
Cache observation attack
(Osvik et. al, 2006)
1) Attacker “primes” the cache with known data

```c
void * p = malloc(CACHE_SIZE);
while(i < CACHE_SIZE)
    p[i++]++;
```
1) Attacker “primes” the cache with known data

void * p = malloc(CACHE_SIZE);
while(i < CACHE_SIZE)
  p[i++]++;

RAM

AES

Attacker

Cache
2) Attacker triggers AES encryption

```
void * p = malloc(CACHE_SIZE);
while(i < CACHE_SIZE)
    p[i++]++;
aes_encrypt(random_p());
```
3) AES loads some cache lines

```c
void * p = malloc(CACHE_SIZE);
while(i < CACHE_SIZE)
    p[i++]++;
aes_encrypt(random_p());
```
4) Attacker can test which lines were touched

```c
void * p = malloc(CACHE_SIZE);

while(i < CACHE_SIZE)
    p[i++]++;

aes_encrypt(random_p());

while(i < CACHE_SIZE)
    t[i++] = timed_read(p, i);
```
5) All untouched lines yield constraints

\[ P_0 \oplus K_0 \notin \{ \text{Untouched lines} \} \]
5) All untouched lines yield constraints

\[ K_0 \notin \{\text{Untouched lines} \oplus P_0 \} \]
5) All untouched lines yield constraints

\[ K_0 \notin \{\text{Untouched lines } \oplus P_0\} \]
Cache timing attack
(Bonneau and Mironov, 2006)
Observation: self-collisions lower encryption time

\[ P_i \oplus K_i \equiv P_j \oplus K_j \]
Observation: self-collisions lower encryption time

Plaintext

Key XOR

Lookup

\[ P_i \oplus K_i \equiv P_j \oplus K_j \]

\[ P_i \oplus P_j \equiv K_i \oplus K_j \]
Internal collisions cause most timing variation
### Key byte differences ranked by average time

<table>
<thead>
<tr>
<th></th>
<th>K0</th>
<th>K1</th>
<th>K2</th>
<th>...</th>
<th>K15</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Key byte differences ranked by average time

<table>
<thead>
<tr>
<th></th>
<th>K0</th>
<th>K1</th>
<th>K2</th>
<th>...</th>
<th>K15</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

0) f2 1024.32
1) 37 1036.71
2) 7a 1036.84
3) 26 1036.91
...  
255) a2 1038.42
Key byte differences ranked by average time

<table>
<thead>
<tr>
<th></th>
<th>K0</th>
<th>K1</th>
<th>K2</th>
<th>...</th>
<th>K15</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

0) f2 1024.32
1) 37 1036.71
2) 7a 1036.84
3) 26 1036.91
... 3) 26 1036.91
255) a2 1038.42

0) 5d 1025.61
1) 10 1036.64
2) 46 1036.79
3) dc 1036.98
... 3) dc 1036.98
255) 03 1038.16
### Key byte differences ranked by average time

<table>
<thead>
<tr>
<th></th>
<th>K0</th>
<th>K1</th>
<th>K2</th>
<th>...</th>
<th>K15</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- 0) f2 1024.32
- 1) 37 1036.71
- 2) 7a 1036.84
- 3) 26 1036.91
- \(\ldots\)
- 255) a2 1038.42

- 0) 5d 1025.61
- 1) 10 1036.64
- 2) 46 1036.79
- 3) dc 1036.98
- \(\ldots\)
- 255) 03 1038.16

\[\approx 100,000\] encryptions
Final round is much better to attack

\[ C_i \oplus K_i = S[X] \]
\[ C_j \oplus K_j = S[Y] \]

\[ X = Y \Rightarrow C_i \oplus K_i = C_j \oplus K_j \]
\[ C_i \oplus C_j = K_i \oplus K_j \]
Final round is much better to attack

\[ C_i \oplus K_i = S[X] \]
\[ C_j \oplus K_j = S[Y] \]

\[ C_i \oplus C_j = K_i \oplus K_j \]

\[ \approx 32,000 \text{ encryptions} \]
Hardware countermeasures on the way

/*
AES-128 encryption sequence.
The data block is in xmm15.
Registers xmm0–xmm10 hold the round keys(from 0 to 10 in this order).
In the end, xmm15 holds the encryption result.
*/

pxor  xmm15, xmm0 // Input whitening
aesenc xmm15, xmm1 // Round 1
aesenc xmm15, xmm2 // Round 2
aesenc xmm15, xmm3 // Round 3
aesenc xmm15, xmm4 // Round 4
aesenc xmm15, xmm5 // Round 5
aesenc xmm15, xmm6 // Round 6
aesenc xmm15, xmm7 // Round 7
aesenc xmm15, xmm8 // Round 8
aesenc xmm15, xmm9 // Round 9
aesenclast xmm15, xmm10 // Round 10

Courtesy of Intel
Differential power analysis
(Kocher et. al, 1999)
Simple power analysis ineffective

Trace courtesy of Cryptography Research, Inc.
Hardware implementations don't use cache
Hardware implementations don't use cache

\[ S[P_0 \oplus K_0] \]
Guessing $K_0 = 00$, traces where high bit of $S[P_0 \oplus K_0]$ is set
Guessing $K_0 = 01$, traces where high bit of $S[P_0 \oplus K_0]$ is set
Partition traces by some predicted intermediate bit

Guessing $K_0 = 02$, traces where high bit of $S[P_0 \oplus K_0]$ is set
Partition traces by some predicted intermediate bit

\[ \approx 10,000 \text{ encryptions} \]

\[ K_0 = 02, \text{ traces where high bit of } S[P_0 \oplus K_0] \text{ is set} \]
Perfect countermeasures are very difficult
Even further down the rabbit hole...
Collects sounds which emanates from CPU

Capacitor emits sound from its foils due to fast pulse charging and discharging

Adi Purwono, 2008
Photon emissions

Sergei Skorobogatov, 2009
Lessons
Don't design or implement your own crypto

Foot-Shooting Prevention Agreement

I, ________, promise that once

Your Name

I see how simple AES really is, I will not implement it in production code even though it would be really fun.

This agreement shall be in effect until the undersigned creates a meaningful interpretive dance that compares and contrasts cache-based, timing, and other side channel attacks and their countermeasures.

Signature

Date

Jeff Moser
Do break whatever you can

**Algorithms:**
- Elliptic curve DSS/DH
- Pairing-based algorithms
- AES-GCM authentication
- SHA-3 candidates

**Side-channels:**
- Motherboard sensors
- CPU debug registers

**Killer target:**
- Cross-VM key compromise
Thank you
Complication: cache lines
Complication: cache lines

Table lookup
Complication: cache lines

- Table lookup
- Cache
Complication: Table families

t0 = Te0[(s0 >> 24)] ^
Te1[(s1 >> 16) & 0xff] ^
Te2[(s2 >> 8) & 0xff] ^
Te3[(s3) & 0xff] ^
rk[0];

t1 = Te0[(s1 >> 24)] ^
Te1[(s2 >> 16) & 0xff] ^
Te2[(s3 >> 8) & 0xff] ^
Te3[(s0) & 0xff] ^
rk[1];

t2 = Te0[(s2 >> 24)] ^
Te1[(s3 >> 16) & 0xff] ^
Te2[(s0 >> 8) & 0xff] ^
Te3[(s1) & 0xff] ^
rk[2];

t3 = Te0[(s3 >> 24)] ^
Te1[(s0 >> 16) & 0xff] ^
Te2[(s1 >> 8) & 0xff] ^
Te3[(s2) & 0xff] ^
rk[3];
Final round is much better to attack
Final round is much better to attack

\[ C_i \oplus K_i = S[X] \]
\[ C_j \oplus K_j = S[Y] \]
Final round is much better to attack

\[ C_i \oplus K_i = S[X] \]
\[ C_j \oplus K_j = S[Y] \]

\[ X = Y \Rightarrow \]
\[ C_i \oplus K_i = C_j \oplus K_j \]
\[ C_i \oplus C_j = K_i \oplus K_j \]
Better approach-rank all possible pairs

<table>
<thead>
<tr>
<th></th>
<th>K0</th>
<th>K1</th>
<th>K2</th>
<th>...</th>
<th>K15</th>
</tr>
</thead>
<tbody>
<tr>
<td>K0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

0)  f2  1024.32
1)  37  1036.71
2)  7a  1036.84
3)  26  1036.91
... 
255) a2  1038.42
Better approach—rank all possible pairs
Fault injection: inducing a telling error
Normal RSA-CRT

Private Key: \( p, q \) (random primes)
\( d \equiv e^{-1} \pmod{\varphi(N)} \) (exponent)

Public Key: \( N = p \cdot q \) (modulus)
\( e \) (exponent)

Signing:
\[ s_p = m^d \pmod{p} \]
\[ s_q = m^d \pmod{q} \]
\[ s = \text{CRT}(s_q, s_p) = m^d \pmod{N} \]
Fault-injected RSA-CRT

Private Key: $p, q$ (random primes)
$d \equiv e^{-1} \pmod{\varphi(N)}$ (exponent)

Public Key: $N = p \cdot q$ (modulus)
$e$ (exponent)

Signing: $s_p = m^d \pmod{p}$
$x \neq m^d \pmod{q}$
$s = \text{CRT}(x, s_p) \neq m^d \pmod{N}$
Fault-injected RSA-CRT

Private Key: \( p, q \) (random primes)
\[ d \equiv e^{-1} \pmod{\varphi(N)} \] (exponent)

Public Key: \( N = p \cdot q \) (modulus)
\( e \) (exponent)

Signing:
\[ s^e = m \pmod{p} \]
\[ s^e \neq m \pmod{q} \]
\[ p = \text{GCD}(s^e - m, N) \]