Protocol Issues

Cryptography

Ahto Buldas ahto.buldas@ttu.ee
Aleksandr Lenin aleksandr.lenin@ttu.ee
Jaan Priisalu jaan.priisalu@ttu.ee

September 18, 2018

Topics

Channel types

Channels are typed by security

- Unsecure
- Confidential
- Intrusion resistant
- Secure

Practical cryptosystems combine algorithms

Clock Based Pseudorandom

```
int main()
{   int i, n; time_t t; n = 5;

    /* Intializes random number generator */
    srand((unsigned) time(&t));

    /* Print 5 random numbers from 0 to 49 */
    for( i = 0 ; i < n ; i++ )
                    {    printf("%d\n", rand() % 50); }

    return(0);}
```

Netscape 1.1 Initialisation

```
RNG_CreateContext()
     (seconds, microseconds) = time of day; /* Time
     pid = process ID;   ppid = parent process ID;
     a = mklcpr(microseconds);
     b = mklcpr(pid + seconds + (ppid << 12));
      seed = MD5(a, b);

mklcpr(x) /* not cryptographically significant; sho
     return ((0xDEECE66D * x + 0x2BBB62DC) >> 1);

MD5() /* a very good standard mixing function, sour
```

Netscape 1.1 SSL session

```
RNG_GenerateRandomBytes()
    x = MD5(seed);
    seed = seed + 1;
    return x;
global variable challenge, secret_key;
create_key()
    RNG_CreateContext();
    tmp = RNG_GenerateRandomBytes();
    tmp = RNG_GenerateRandomBytes();
    challenge = RNG_GenerateRandomBytes();
    secret_key = RNG_GenerateRandomBytes();
```

Generating Good Random

- Hardware - test the quality
- Crypto library - check diagnostics!
- Collect entropy from environment - quantity is limited, combine with pseudorandom
- User Input - social attacks and habits.

NB! Random number generator can be backdoored

Nonce

Nonce is used to make messages unique

Prevent replay attacks - nonce should be unique

Should not be usable in other roles

DES is not a group

Permutations form a group

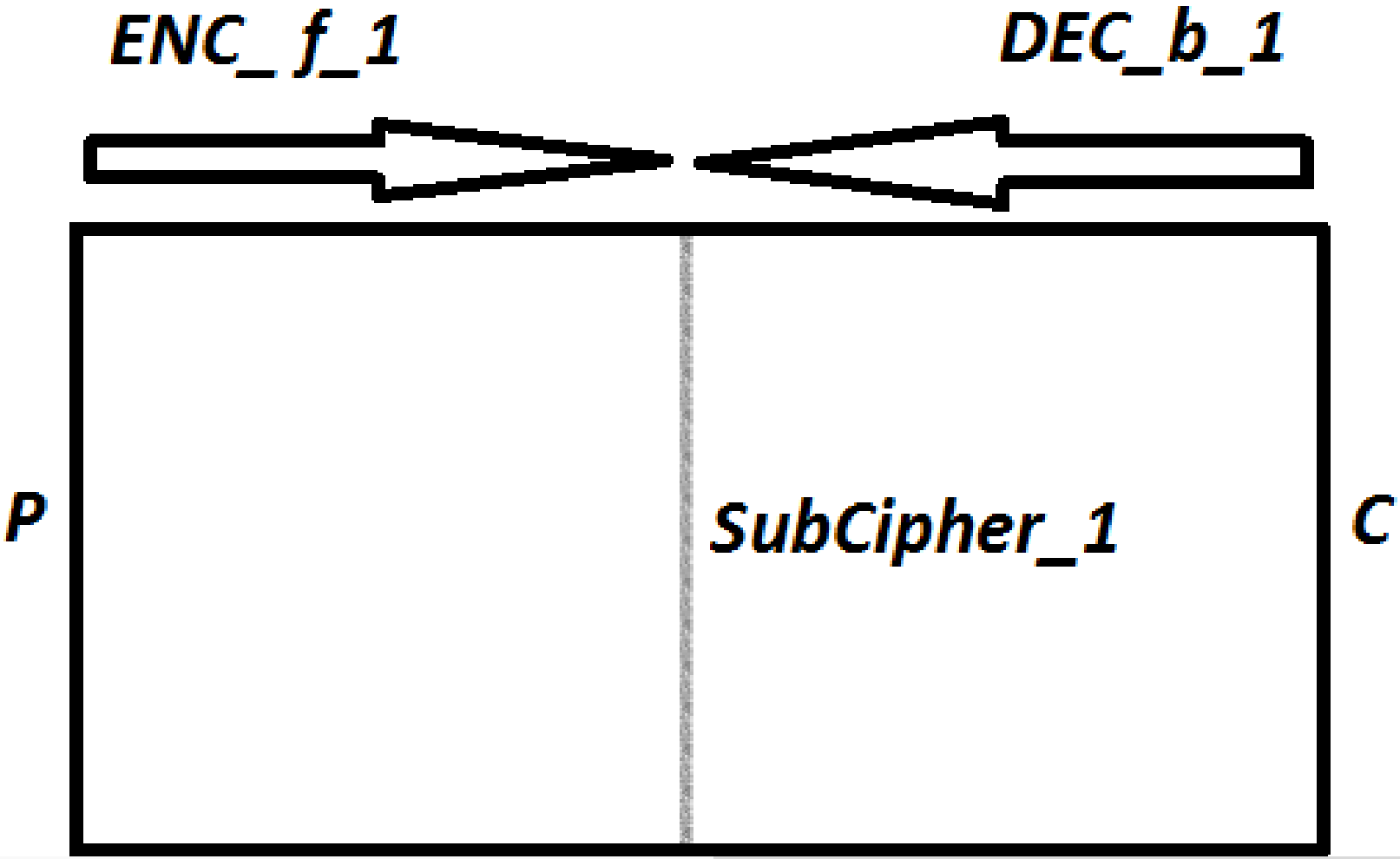
DES messages are 64 bits and keys 56 bits

There is $(2^{64})!$ permutations and 2^{56} keys

Searching for collison cycles

3DES

Meet in the middle attack



Traffic Analysis

When we cannot see the content, we still can measure the properties of traffic

- Identify communication parties
- Deduce casual relations from message order
- Infer content by message size
- Timing characterises the process generating the messages

Traffic padding and message routing randomisation

Sidechannels

Attacking multitasking

- Shared memory
- Free memory (ex Hartbleed)
- Swap file
- Processor cache
- Breaking buffer boundaries
- Shared processor - timing attacks

Physical attacks

- Microscoping and probing
- Reset
- Internal bus snooping
- Power analysis (ex DPA)
- Thermal signature
- Sound
- Electromagnetic emission

Fault injection