# E-Safenet encryption

## Reversing and practical attacks

Jan Laan & Cedric Van Bockhaven

Supervisor: Armijn Hemel - Tjaldur Software Governance Solutions

# E-Safenet

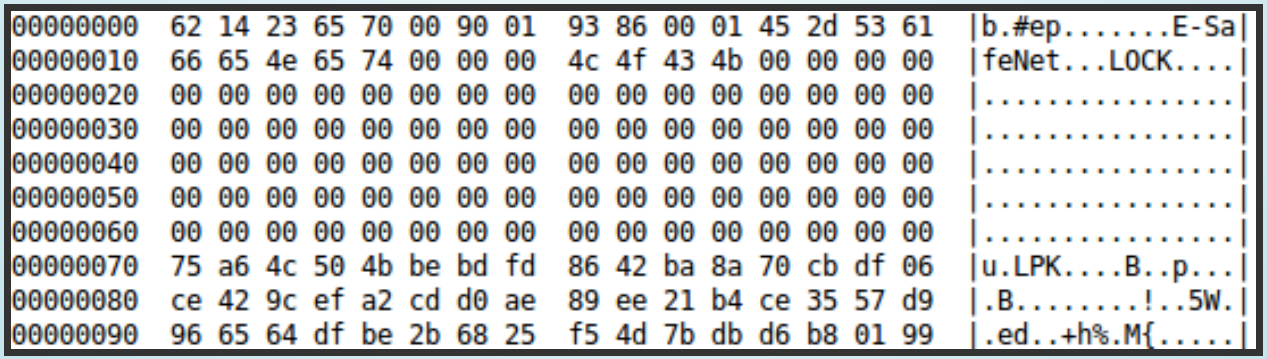
- Chinese company specialized in **data leak prevention**
- Smartphone manufacturers, government, ...
- Android (Linux kernel) released under GPL v2
- License compliance for Tjaldur

- E-Safenet encryption: How does it work, and can we decrypt it?

# E-Safenet

- Archives of encrypted source code

```
//////////////////////////////////////////////////////////////////////////////
/// @file  udp_client.c
///
/// @brief
///     UDP¿Í»§¶ËÄ£¿é
///
/// @author ÕÅ»ªÊ¤(wation)
/// @date 01/20/2011
///
/// @version 1.0
///
/// @details
///     ±¾Ä£¿éÌá¹©Ì×½Ó×ÖµÄ¸÷ÖÖÀà½Ó¿Ú£¬²¢°ÑÔBerkley½Ó¿ÚÖØÐÂ·â×°£¬Ìá¹©¸üÊÊºÏ
```



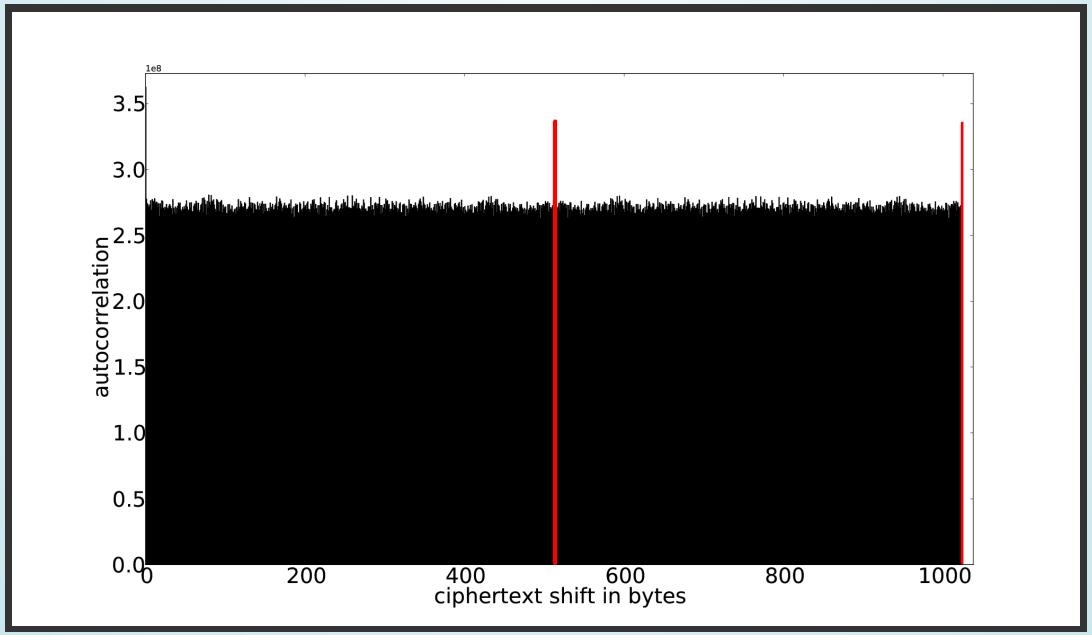
```
00000000  62 14 23 65 70 00 90 01  93 86 00 01 45 2d 53 61  |b.#ep.......E-Sa|
00000010  66 65 4e 65 74 00 00 00  4c 4f 43 4b 00 00 00 00  |feNet...LOCK....|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  75 a6 4c 50 4b be bd fd  86 42 ba 8a 70 cb df 06  |u.LPK....B..p...|
00000080  ce 42 9c ef a2 cd d0 ae  89 ee 21 b4 ce 35 57 d9  |.B........!..5W.|
00000090  96 65 64 df be 2b 68 25  f5 4d 7b db d6 b8 01 99  |.ed..+h%.M{.....|
```

# Reversing

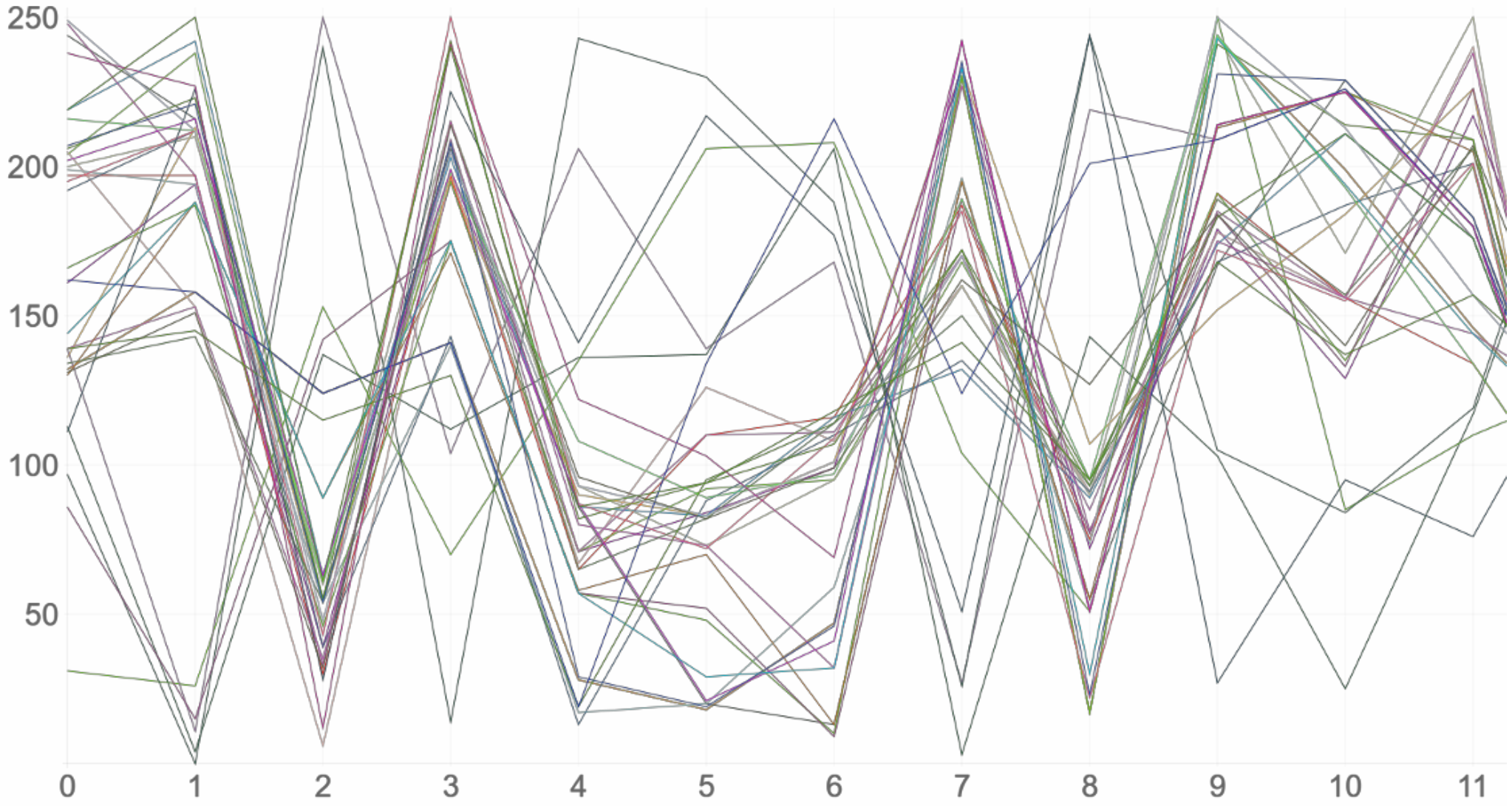
- Cryptanalysis / Autocorrelation
- E-Safenet data format research
- Attacks?

# Autocorrelation

- Used to find repeating patterns
- Comparison of text with a shifted copy of itself
- Peaks at 512 bytes



# Plot with blocksize 512 bytes

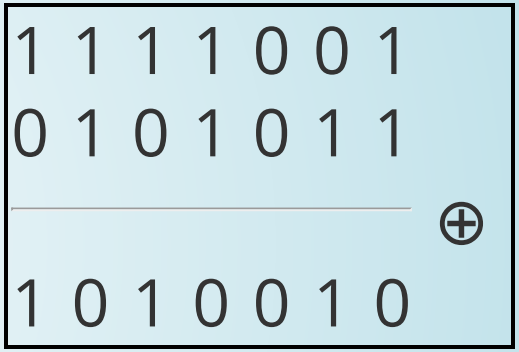


# XOR cipher

XOR truth table

| IN | | OUT |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 1 | 1 | 0 |

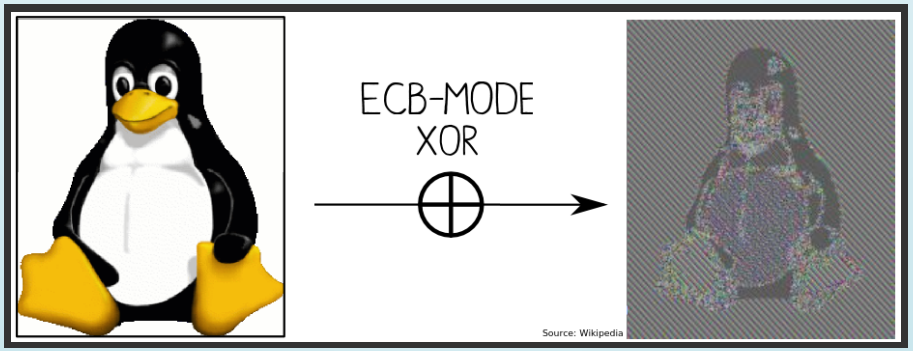
XOR example



# XOR cipher

- Every column has byte values from the same range
- Find key by XOR of an entire block with '/'
- Applying this key on the entire file revealed chunks of plaintext

```
\zF+X
}((
///g???HB4WZ^KD@??????????????????6;%4?}FlosGzsocket(void)
{
        UdpClientMgrStruct *pstSocket = &gstUdpCli6j /((
        t|B%hon-)d      \fij|{lm/VVdm_zB,>'4?$0>+,rtocc`}MGDBer_|????@?????H(
        ii
```



# E-Safenet data format

```
00000000  62 14 23 65 70 00 90 01  93 86 00 01 45 2d 53 61  |b.#ep.......E-Sa|
00000010  66 65 4e 65 74 00 00 00  4c 4f 43 4b 00 00 00 00  |feNet...LOCK....|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000070  75 a6 4c 50 4b be bd fd  86 42 ba 8a 70 cb df 06  |u.LPK....B..p...|
00000080  ce 42 9c ef a2 cd d0 ae  89 ee 21 b4 ce 35 57 d9  |.B........!..5W.|
00000090  96 65 64 df be 2b 68 25  f5 4d 7b db d6 b8 01 99  |.ed..+h%.M{.....|
```

- b?#e??: begin and end of padding
- E-SafeNet LOCK literals
- Size of compressed data
- Checksum composed of addition of values of bytes 512-1023

# E-Safenet data format

- Encrypted file has same size as plaintext file
- First encrypted block has
  header and NUL-byte padding
- This doesn't add up, unless... compression

# Compression

## Original:

```
/* Copyright Statement:
 *
 * This software/firmware and related documentation ("MediaTek Software") are
 * protected under relevant copyright laws. The information contained herein
 * is confidential and proprietary to MediaTek Inc. and/or its licensors.
 * Without the prior written permission of MediaTek inc. and/or its licensors,
 * any reproduction, modification, use or disclosure of MediaTek Software,
 * and information contained herein, in whole or in part, shall be strictly prohibited.
 *
 * MediaTek
```

## Compressed:

```
/* Copyright Statement:** This software/firm` and rel@d docuxation ("MediaTek SÛ") P*
protected underevant copy¬laws.Pe inform¬contain@herein* PSfid[ialX/or its licensors.*
Without theYiD    prietary to 'Inc.` written permissjof(1i62,*M yL[ducl!, modific, use D
disclosurT)dô%   d;ý,T wholLPart, shall be strictlyHohibiH. .** MediaTek
```

# Compression

- Repeated occurences of data are backreferenced to the earlier copy
- Dictionary over a sliding fixed window size
- Characterizes Lempel-Ziv compression
- Many different algorithms: LZ77, LZ78, LZJB, LZRB, LZF, LZW, LZO, LZX, LZS, LZSS, LZ4, LZMA, LZP, ...

# LZO (Lempel-Ziv-Oberhumer)

- Best match of the LZ-family
- Only different in how previous data occurences are being referenced
- Many LZO versions, algorithms, compression levels
- Exhaustive search: LZO1X-1, compiled with LZO version 1.00

# Attacks

- Known-plaintext attack
- Probable-plaintext attack
- Ciphertext-only attack

# Known-plaintext attack

- `plain   ⊕ crypted = key`
  `crypted ⊕ key     = plain`
- Use a block of 512 bytes of known plain- and ciphertext to extract the key
- Result: Trivial decryption

# Probable-plaintext attack

- C files: returning probable keywords
  `const char, return, #define, sprintf, ...`
- Binary files (.doc, .xls): many `0x00` and `0xFF`
- Slide predefined set of keywords over the file
- If future offsets return plaintext, assume as correct
- Result: successful decryption given enough data (from 17kB, but results vary)

wrong offset

```
......return........
......□P□□6□........
......□□□~□□........
```

correct offset

```
........return........
........id mai........
........}\n  n........
```

# Ciphertext-only attack

- Decrypt a text file without knowledge of that file
- Assumed: Plaintext contains (mostly) printable characters, ASCII value 32-126
- For each column, try all possible key values, use the one that produces the most printable characters
- Result: similar to actual plaintext, can be fixed by manual inspection

| 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | L | j | c | e | n | s | e | | e | l | r | |
| H | P | F | x | c | e | l | | r | l | l | t | |
| | | # | | | * | / | | | # | # | | p |
| N | a | n | e | d | | r | a | n | d | f | s | |
| | @ | u | a | r | | b | o | o | o | | | * |
| M | L | G | a | t | a | = | N | U | O | O | ; | |
| | | | $ | t | h | i | s | - | = | \ | h | a |
| e | = | ' | C | e | r | t | i | f | j | ` | a | t |

# Conclusion

- E-Safenet encryption is extremely weak, can almost always be reversed
- Current checksum is useless
- E-Safenet encryption is made for speed
- Possible replacement: Bernstein's stream cipher Salsa20/12

# Questions?