Crypto 101
A “no crazy maths” guide to breaking crypto

Benjamin Kearns – Technical Team Leader
Event – OWASP Day 2015
Date – 27th February 2015
Company Overview

Company
- Lateral Security (IT) Services Limited
- Founded in April 2008 by Nick von Dadelszen and Ratu Mason (Both Directors)
- Auckland, Wellington, Melbourne: ~20 highly specialised security consultants

Services
- Security testing (design & architecture, penetration testing, configuration, code reviews, security devices & controls, mobile apps)
- Security advisory (Lifecycle compliance & audit – ISO, PCI-DSS, NZISM, policy process development, threat modeling and risk assessment)
- Regular ongoing technical testing and assurance programs
Overview

- Introduction
- XOR
- Stream ciphers
- Block cipher modes
  - Electronic Codebook (ECB)
  - Cipher Block Chaining (CBC)
- HMAC
XOR (Exclusive Or)

0 XOR 0 = 0
1 XOR 0 = 1
0 XOR 1 = 1
1 XOR 1 = 0

\[
\begin{array}{c}
\text{0000 1011 (P)} \\
\oplus \\
\text{1100 1110 (K)} \\
\hline \\
\text{1000 0101 (C)}
\end{array}
\]

\[
\begin{array}{c}
\text{1000 0101 (C)} \\
\oplus \\
\text{1100 1110 (K)} \\
\hline \\
\text{0100 1011 (P)}
\end{array}
\]
Plain text: Secret String
Key: a

Secret String XOR aaaaaaaaaaaaaa

0101 0011 0110 0101 0110 0011
0110 0001 0110 0001 0110 0001
0011 0010 0000 0100 0000 0010

32 04 02 13 04 15 41 32 15 13 08 0f 06
Stream ciphers

Key

Stream cipher

Keystream

Plaintext
Stream Ciphers

“Secret Session Key” → Stream Cipher → 492485C29AF129B...

492485C29AF129B...

uid=4;cart_items=[502,388,590,4]
But you’re safe, right?

WEP
Block ciphers

Block cipher

Plaintext

Key

Ciphertext
Electronic Codebook (ECB)
ECB example

AAAAAAAAABBBBBBBBBAAAAAA

AAAAAAAAA | BBBBBBBBB | AAAAAAAA

a49e184729a65b18 | 38f9c215972c28e3 | a49e184729a65b18
ECB Example
Exploiting ECB

```php
function process_session_cookie() {
    session_cookie = decrypt_cookie(COOKIES['Session'])
    variables = session_cookie.split(';
    foreach(session_variable in variables) {
        key_value_array = session_variable.split('=')
        session[key_value_array.first] = key_value_array.second;
    }
}
```

//...

```php
if(session['ADMIN'] != 0) {
    // Unlock awesome admin powers
    SESSION=0358f292249283bc49f28b20a3c3051d48a84d294c128a46193b48cff29ac493104d210c20a04882294859ac4980a5dd
}
```
But you’re safe, right?

Cipher cipher = Cipher.getInstance("AES");
Cipher.init(…)
Cipher Block Chaining (CBC) mode encryption
Cipher Block Chaining (CBC) mode decryption
But you’re safe, right?

CVE-2005-0039
HMAC

Message

Key

HMAC

Signature

{user_id=3,timestamp=1376773912};BA842C380DD11204BF
But you’re safe, right?
Cracking crypto
Happy Dance!!
Computers are hard
More crypto fun

http://www.matasano.com/articles/crypto-challenges/
Questions and Contacts

Lateral Security (IT) Services Limited

Wellington
38-42 Waring Taylor Street (level 7, Petherick Tower)
PO Box 8093, Wellington 6143, New Zealand
Phone: +64 4 4999 756
Email: sas@lateralsecurity.com

Auckland
187 Queen Street (level 8, Landmark House)
PO Box 7706, Auckland, New Zealand
Phone: +64 9 3770 700
Email: sas@lateralsecurity.com

Melbourne
200 Queen Street (level 13)
Melbourne, VIC 3000, Australia
Phone: +61 1300 554745
Email: sas@lateralsecurity.com

Presentation Download
www.lateralsecurity.com/presentations