Symmetric Cryptography

February 1, 2017
Why Cryptography?

- Confidentiality - only intended parties can read contents
- Integrity - message tampering can be detected
- Authentication - the author is verified
- Non-repudiation - the author cannot deny being the author
Why symmetric cryptography?

- Fast (comparably less costly computation)
- Well suited for single user systems (encrypted files, etc.)
Why not symmetric cryptography?

- Requires a shared secret
- Non-repudiation requires third-party
Stream Ciphers

- Data stream is combined with the key stream (generally xor’d)
- Used for speed and ability to encrypt a data stream of variable length
- AS/1 (Cell Phones), RC4 (WPA TKIP)
Block Ciphers

- Operate on a fixed number of bits, partitioning the plaintext into blocks, utilizing a symmetric key (not keystream)
- Operate in modes that define how the blocks and the possible initialization vector interact
- Requires plaintext to be padded to be a multiple of the block size
- Most commonly used block cipher today is AES
- Can be used to ensure integrity and authentication*
Initialization Vector

- Random block use to randomize encryption, allowing the same plaintext to be encrypted with the same key multiple times
- Should NOT be reused
- Generally not considered secret
- Should not be able to be guessed at the time of encryption (BEAST Attack)
Padding

● Example Block Size: 8 bytes
● Plain text: 02 30 23 05
● PKCS#7: 02 30 23 05 04 04 04 04
● ISO/IEC 7816-4: 02 30 23 05 80 00 00 00
Message Authentication Codes

- Ensure integrity and authenticity
- Built as a function that takes a secret key and a message, and returns a tag
- Can be implemented many ways (Encrypt-then-MAC, MAC-then-Encrypt, Encrypt-and-MAC)
- Authenticity is needed for most communication
Encrypt-then-MAC
i.e. IPSec

Encrypt-and-MAC
i.e. SSH

MAC-then-Encrypt
i.e. SSL/TLS

https://en.wikipedia.org/wiki/Authenticated_encryption
Block Modes
Electronic Codebook

Electronic Codebook (ECB) mode encryption

Electronic Codebook (ECB) mode decryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
Electronic Codebook

- Not recommended (really bad)
- Doesn’t really provide confidentiality

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
Cipher Block Chaining

Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining (CBC) mode decryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
Cipher Block Chaining

- Well used
- Generally well liked
- Chain in single bit propagates across message (Allows for byte flipping attacks)
Breaking Block Ciphers (SSL/TLS)
Browser Exploit Against SSL/TLS

- BEAST
- CVE-2011-3389
- September 2011 (TLS v1.0)
- Attack against CBC, stemming from the ability for the attacked to know the IV at the time of encryption
- IV was negotiated at the start of the session to keep it secret
- This means every packet but the first will have a known “Initialization Vector”

Images following taken from:
http://commandlinefanatic.com/cgi-bin/showarticle.cgi?article=art027
Injected block: Kimberly

4B 69 6D 62 65 72 6C 79

CBC Residue (can't change this)

FE DC BA 98 76 54 32 10

B5 B5 D7 FA 13 26 5E 69

DES(password)

1D FD E2 97 8F EE E1 91

output
Plaintext block 1: Dearest

Initialization Vector

DES(password)

CBC Residue

output

Adjusted injected block

Injected block
Attack in Use

- Attempt to grab the session cookie
- Exploited a flaw in Java web applets
- Is made practical by splitting guessed segments across block boundaries, allowing each character to be guessed individually, instead of as a whole:

  If guessing an 8 digit number, guessing all digits together is at worst $10^8$
  Guessing them one at a time is at worst $10 \times 8$
Fixes:

- New unencrypted IV for each packet
- Not being encrypted is not a problem, as it is only good for that packet
- NOTE: The level of control an attacker needs to perform this attack makes it likely there is an easier way to exploit the user
Padding Oracle On Downgraded Legacy Encryption

- Poodle
- CVE-2014-3566
- September 2014 (SSL v3)
- Attack against CBC after a forced downgrade
- CBC MAC in SSLv3 does NOT cover padding, so an attacker can manipulate padding at will
- SSLv3 mandates padding is (# of bytes) - 1 in the final byte, and those bytes are completely ignored.
- Results in a padding oracle
POODLE Attack

- Attacker can send requests, but not see their plaintext
- Attacker forces the final block to be completely padding (message length is a multiple of the block size), so we know the final byte should be 15
- The byte to be guessed occurs in the final byte of a preceding block
POODLE Attack

Ciphertext = ... | $C_i$ | $C_n$

$|$ = Block boundaries

$C_i$ = Block to guess

$C_n$ = Known padding block

$C_n$ is replaced by $C_i$ and sent to the server to be decrypted
POODLE Attack

- To get the server to accept the request, we need to make $C_{i[15]} = 15$
- To do so, we replace $C_{i[15]}$ with 0 - 255 until we get a success
- A success means the server established $D(C_{i[15]}) + C_{n-1[15]} = 15$
- This means $P_{i[15]} = 15 + C_{n-1[15]} + C_{i-1[15]}$
Cipher Block Chaining

\[ D(C_i[15]) \oplus C_{n-1}[15] = 15 \]
\[ D(C_i[15]) = 15 \oplus C_{n-1}[15] \]
\[ P_i[15] \oplus C_{i-1}[15] = 15 \oplus C_{n-1}[15] \]
\[ P_i[15] = 15 \oplus C_{n-1}[15] \oplus C_{i-1}[15] \]

Cipher Block Chaining (CBC) mode encryption

Cipher Block Chaining (CBC) mode decryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
Fixes:

- Disable SSLv3
- Authenticate entire message
More Resources:

- [https://www.id0-rsa.pub/](https://www.id0-rsa.pub/) - Cryptography Challenges
- [https://www.youtube.com/watch?v=2aHkgB2-46k](https://www.youtube.com/watch?v=2aHkgB2-46k) - Cryptography Lectures
Questions?
Future Events

- Next week: Asymmetric Cryptography (Breaking RSA?)
- Introduction to Pentesting - Saturday, February 11th, 12 pm - 3 pm
- Coming Up (Most Likely): Binary Exploitation