InterMAClib: Beyond Confidentiality and Integrity in Practice

Torben B. Hansen @n_tbh
Joint work with
Martin R. Albrecht @martinarlalbrecht
Kenneth G. Paterson @kennyog

Information Security Group
Centre for Doctoral Training in Cyber Security

Real World Crypto 2018 January 12th
Motivation

InterMAC (lib)

OpenSSH InterMAC cipher modes
Performance

The next ~25 mins

We are here

InterMAC(lib)

BEGIN
Symmetric encryption

Modelling security

AE

C ← Enc_k(M) → C → M ← Dec_k(C)

Good approximation?

[BKN02] SSH CBC-mode is secure!

[APW09] SSH CBC-mode is not secure!
SSH packets contains a length field
Security notions

\[ C \leftarrow \text{Enc}_k(M) \]

\[ C \rightarrow \] Security notions

\[ C_1 \rightarrow \]

\[ C_2 \rightarrow \]

\[ M_1 \leftarrow \text{Dec}_k(C_1) \]

\[ M_2 \leftarrow \text{Dec}_k(C_2) \]

\[ M = M_1 \| M_2 \]

\[ \text{IND-CCA} \rightarrow \text{IND-sfCFA} \]

\[ \text{IND-CTXT} \rightarrow \text{IND-sfCTF} \]
Security notions

\[ C = \text{DJ@)%&6h} \]
\[ C' = \text{*s&FQOM"F} \]

SSH:
- Length field encrypted
- Random amount of padding
Security notions

(Open)SSH EtM cryptographic processing

Sequence Number 4
Packet Length 4
Pad Len 1
Payload
Padding ≥4

Enc

Packet Length
Ciphertext

Mac

MAC tag

[BDPS12] / [ADHP16]

[BDPS12]

IND-CCA
IND-CTXT
IND-sfCFA
IND-sfCTF

[ADHP16]

BH-sfCFA
n-DOS-sfCFA

Security notions

(BDPS12) / ADHP16 (Open)SSH EtM cryptographic processing

Sequence Number 4
Packet Length 4
Pad Len 1
Payload
Padding ≥4

Enc

Packet Length
Ciphertext

Mac

MAC tag

[BDPS12] / [ADHP16]

[BDPS12]

IND-CCA
IND-CTXT
IND-sfCFA
IND-sfCTF

[ADHP16]

BH-sfCFA
n-DOS-sfCFA
InterMAC

Achieve all 4 security notions

N - 1 | N - 1 | N - 1

Enc 0

Enc 0

Enc 1

IND$-CPA

Chunk counter: 0
Message counter: 0

Mac

Mac

Mac

PRF

[BDPS12]
InterMAC in practice

\[ N - 1 \quad N - 1 \quad N - 1 \]

- \( t = 1 \): no padding
- \( t = 2 \): padding

Chunk counter: 0
Message counter: C
InterMAC in practice

- **Nonce-based AE**
- **Chunk counter:**
  - Message counter:

- **t=1:** no padding
- **t=2:** padding

<table>
<thead>
<tr>
<th>0</th>
<th>0</th>
<th>t</th>
</tr>
</thead>
</table>

![Diagram](image-url)
InterMAClib

- C-implementation
- Aims to be "safe" to use
- Small API
- User-oblivious nonce-management
- Algorithm agility
- AES-GCM
- Chacha20-Poly1305
Nonce management

\[ \text{im_init(..., ae_cipher)} : \]

\[ \begin{align*}
\text{chunk counter} &= 0 \\
\text{message counter} &= 0 \\
\text{nonce} &= \begin{array}{c}
\vspace{0.5cm}
\text{32} \\
\text{64}
\end{array}
\end{align*} \]

InterMAC with ChaCha20-Poly1305

\[ K_{\text{mac}} \leftarrow \text{ChaCha20}(0, K, \text{nonce}, \text{block_counter} = 0) \]

\[ C \leftarrow \text{ChaCha20}(M, K, \text{nonce}, \text{block_counter} = 1) \]

\[ \text{Tag} \leftarrow \text{Poly1305}(K_{\text{mac}}, C) \]

InterMAC with AES-GCM

Initialise aes-gcm with nonce for each chunk
We implemented InterMAC-based cipher modes in OpenSSH (v7.4).

Performance of InterMAC-based cipher modes compared to existing cipher modes.

<table>
<thead>
<tr>
<th>Payload Packet Length</th>
<th>Pad Len</th>
<th>Padding ≥4</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
<td>≥4</td>
</tr>
</tbody>
</table>

Want cipher modes with all 4 security properties. No current cipher mode satisfy that...

im-aes128-gcm-N
im-chacha-poly-N

OpenSSH packet processing code: complex and buggy

Standalone code-path in the OpenSSH packet processing code

[APW09] [ADHP16] [PW10]

Throughput
Total bytes transmitted
Behavior relating to chunk length N
Implementations must cater for ciphertext fragmentation

We believe this feature should be reflected in the security models

[BDPS12] provides a security model for studying symmetric encryption schemes supporting ciphertext fragmentation

InterMAC satisfies all security notions from [BDPS12]

We modify InterMAC to make it usable in practice and create InterMAClib

OpenSSH want cipher modes that meets all security notions from [BDPS12]

We implement InterMAC-based cipher modes in OpenSSH using InterMAClib

InterMAC: SSH binary packet protocol done right, using modern primitives

We measured performance; indicates that greater security can be traded for only a minor performance hit

Finish line is in sight…
Hi Bob, I believe we can beat Eve!

CrApto...

Real World Class Alice!

Torben Hansen @n_tbh
Martin Albrecht @martinralbrecht
Kenny Paterson @kennyog