Introduction to cryptography

2B. Intermezzo: authenticated encryption

Gilles Van Assche
Olivier Markowitch

INFO-F-405
Université Libre de Bruxelles
2020-2021

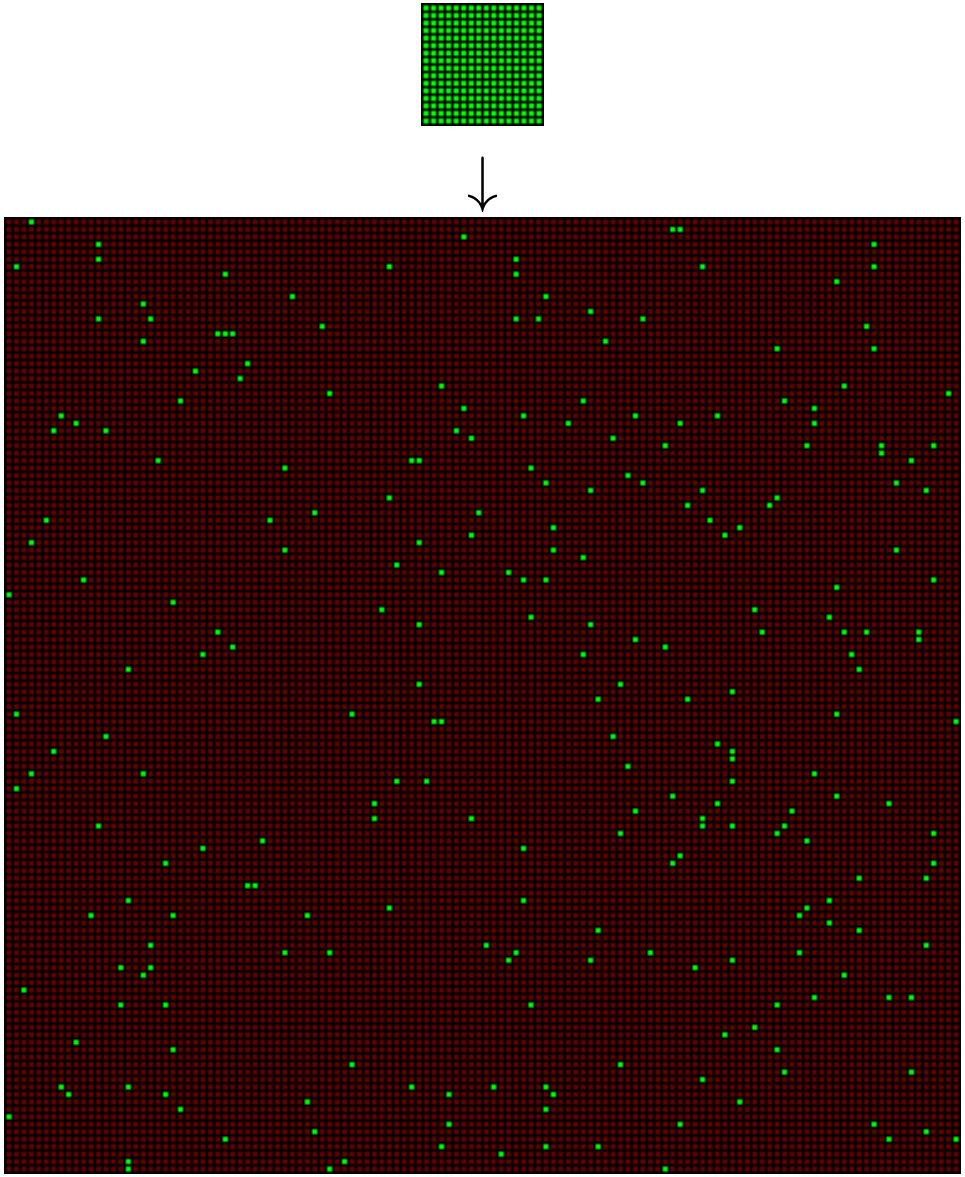
What is authenticated encryption (AE)?

- Definition
  - $M = (A, P)$ message with associated data and plaintext
  - $M_c = (A, C)$ cryptogram with associated data and ciphertext
  - **wrapping**: M to M_c
  - **unwrapping**: M_c to M
    (*symmetric cryptography*: same key used for both operations)
- Authentication aspects
  - unwrapping includes **verification** of M_c
    $\Rightarrow$ if not valid, it returns an error $\perp$
  - wrap operation adds *redundancy*: $|C| > |P|$
    $\Leftrightarrow$ often coded as *tag* at the end $C = C' || T$

What is authenticated encryption (AE)?

- Definition
  - $M = (A, P)$ message with associated data and plaintext
  - $M_c = (A, C)$ cryptogram with associated data and ciphertext
  - **wrapping**: M to M_c
  - **unwrapping**: M_c to M
    (*symmetric cryptography*: same key used for both operations)
- Authentication aspects
  - unwrapping includes **verification** of M_c
    $\Rightarrow$ if not valid, it returns an error $\perp$
  - wrap operation adds *redundancy*: $|C| > |P|$
    $\Leftrightarrow$ often coded as *tag* at the end $C = C' \| T$

Why is there expansion?



Limitation of AE: traffic analysis

- Traffic analysis:
  - length of messages
  - number of messages
- Solution
  - creating dummy messages
  - random-length padding of plaintext
  - to be done on higher layer

    $\Rightarrow$ *AE scheme security should be independent from this layer*

Limitation of AE: traffic analysis

- Traffic analysis:
  - length of messages
  - number of messages
- Solution
  - creating dummy messages
  - random-length padding of plaintext
  - to be done on higher layer

    $\Rightarrow$ *AE scheme security should be independent from this layer*

Limitation of AE: need for message uniqueness

- Concrete AE proposals are deterministic

$$M = M' \Leftrightarrow M_c = M'_c$$

  - information leakage
  - concern of replay attacks at unwrapping end

- Solution is to use a **nonce** (=number used only once)
  - impose that A is unique for the given key K
  - often presented as a separate field: (A, N)
  - wrapping engine shall ensure (K, N) is unique
    - wrapping becomes stateful
    - a simple message counter suffices

$\Rightarrow$ From now on we always include a nonce N

Limitation of AE: need for message uniqueness

- Concrete AE proposals are deterministic

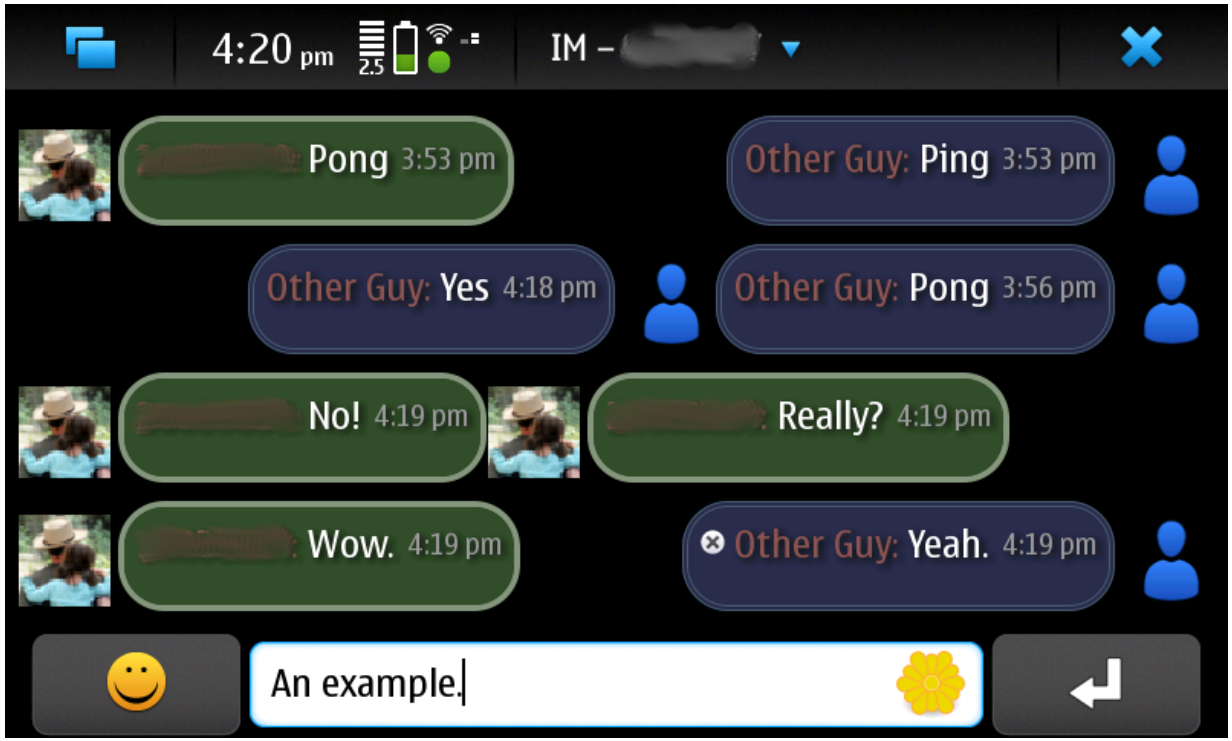
$$M = M' \Leftrightarrow M_c = M'_c$$

  - information leakage
  - concern of replay attacks at unwrapping end

- Solution is to use a **nonce** (=number used only once)
  - impose that A is unique for the given key K
  - often presented as a separate field: (A, N)
  - wrapping engine shall ensure (K, N) is unique
    - wrapping becomes stateful
    - a simple message counter suffices

$\Rightarrow$ From now on we always include a nonce N

Sessions



Picture by Alan Bruce

Sessions

Cryptogram authenticates full sequence so far

- Additional protection against:
  - insertion,
  - omission,
  - re-ordering of messages within a session
- Nonce per session
  - in case of unique session key: no nonce!
- Alternative view:
  - splits a long cryptogram in shorter ones
  - intermediate tags

[Bellare, Kohno and Namprempre, ACM 2003] [Bertoni, Daemen, Peeters and VA, SAC 2011] [Boldyreva, Degabriele, Paterson, Stam, EC 2012] [Hoang, Reyhanitabar, Rogaway and Vizár, 2015]

Sessions

Cryptogram authenticates full sequence so far

- Additional protection against:
  - insertion,
  - omission,
  - re-ordering of messages within a session
- Nonce per session
  - in case of unique session key: no nonce!
- Alternative view:
  - splits a long cryptogram in shorter ones
  - intermediate tags

[Bellare, Kohno and Namprempre, ACM 2003] [Bertoni, Daemen, Peeters and VA, SAC 2011] [Boldyreva, Degabriele, Paterson, Stam, EC 2012] [Hoang, Reyhanitabar, Rogaway and Vizár, 2015]

Sessions

Cryptogram authenticates full sequence so far

- Additional protection against:
  - insertion,
  - omission,
  - re-ordering of messages within a session
- Nonce per session
  - in case of unique session key: no nonce!
- Alternative view:
  - splits a long cryptogram in shorter ones
  - intermediate tags

[Bellare, Kohno and Namprempre, ACM 2003] [Bertoni, Daemen, Peeters and VA, SAC 2011] [Boldyreva, Degabriele, Paterson, Stam, EC 2012] [Hoang, Reyhanitabar, Rogaway and Vizár, 2015]

Sessions

Cryptogram authenticates full sequence so far

- Additional protection against:
  - insertion,
  - omission,
  - re-ordering of messages within a session
- Nonce per session
  - in case of unique session key: no nonce!
- Alternative view:
  - splits a long cryptogram in shorter ones
  - intermediate tags

[Bellare, Kohno and Namprempre, ACM 2003] [Bertoni, Daemen, Peeters and VA, SAC 2011] [Boldyreva, Degabriele, Paterson, Stam, EC 2012] [Hoang, Reyhanitabar, Rogaway and Vizár, 2015]