Stateful Authentication and AEAD Experiments: Constructing a Bridge in the Analysis of TLS

Based on joint work:

Colin Boyd[1] ***Britta Hale***[1]

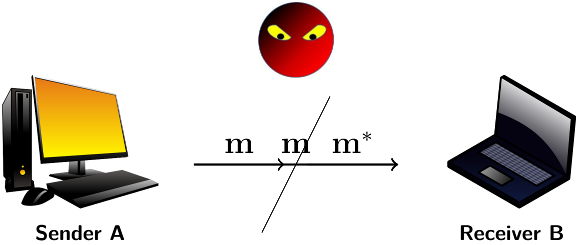
Stig Frode Mjølsnes[1] *Douglas Stebila*[2]

[1]Norwegian University of Science and Technology

[2]Queensland University of Technology

28 April 2016

What *is* data authentication?



Is $\mathbf{m}$ from **A**?

Has $\mathbf{m}$ been modified?

NTNU – Trondheim
Norwegian University of
Science and Technology

ACHIEVING AUTHENTICATION

- Message Authentication Code (MAC)
  - HMAC, etc...

- Signatures
  - DSA, Elliptic Curve DSA, etc...

- Authenticated Encryption with Associated Data (AEAD)
  - Galois Counter Mode (GCM), etc...

AUTHENTICATION HIERARCHY

Example		Sender		Receiver
TLS	Level 4	$m_0, m_1, m_2, m_3, m_4, m_5$	→	Auth., No Replays, Strictly Incr., No Drops $m_0, m_1, m_2, m_3, m_4, m_5$
802.11	Level 3	$m_0, m_1, m_2, m_3, m_4, m_5$	→	Auth., No Replays, Strictly Incr. m_0, m_2, m_3, m_5
DTLS*	Level 2	$m_0, m_1, m_2, m_3, m_4, m_5$	→	Auth., No Replays m_3, m_0, m_5, m_2
DTLS	Level 1	$m_0, m_1, m_2, m_3, m_4, m_5$	→	Authentication only m_3, m_5, m_3, m_2

SECURE CHANNEL VARIATIONS

Level 1
Canetti–Krawczyk 2001
Generic network channel protocol description

Level 4
Jager–Kohlar–Schäge–Schwenk 2012

Level 4
Bellare–Kohno–Namprempre 2002
INT-SFCTXT from INT-CTXT

Level 4
Krawczyk–Paterson–Wee 2013

Level 4
Canetti–Krawczyk 2001
Network authentication protocol

Level 1
Paterson–Ristenpart–Shrimpton 2011

HIERARCHY OF AUTHENTICATION

$\mathsf{Exp}^{\mathsf{auth}_i}_{\Pi,\mathcal{A}}()$:

$k \xleftarrow{\$} \mathrm{Kgn}()$
$st_{\mathrm{E}} \leftarrow \bot,\ st_{\mathrm{D}} \leftarrow \bot$
$u \leftarrow 0,\ v \leftarrow 0$
$\mathtt{r} \leftarrow 0$
$\mathcal{A}^{\mathsf{Send}(\cdot),\mathsf{Recv}(\cdot)}()$
return $\mathtt{r}$

Oracle Send(m):

$u \leftarrow u + 1$
$(sent_u, st_{\mathrm{E}}) \leftarrow \mathrm{Snd}(k, m, st_{\mathrm{E}})$
return $sent_u$ to $\mathcal{A}$

Oracle Recv(c):

$v \leftarrow v + 1$
$rcvd_v \leftarrow c$
$(m, \alpha, st_{\mathrm{D}}) \leftarrow \mathrm{Rcv}(k, c, st_{\mathrm{D}})$
if $(\alpha = 1) \wedge \mathsf{cond}_i$ **then**
  $\mathtt{r} \leftarrow 1$
  return $\mathtt{r}$ to $\mathcal{A}$
end if
return $\bot$

1. **Basic authentication:**
   $\mathsf{cond}_1 = (\nexists w : c = sent_w)$
2. **Basic authentication, no replays:**
   $\mathsf{cond}_2 = (\nexists w : c = sent_w) \vee (\exists w < v : c = rcvd_w)$
3. **Basic authentication, no replays, strictly increasing:**
   $\mathsf{cond}_3 = (\nexists w : c = sent_w) \vee (\exists w, x, y : (w < v) \wedge (sent_x = rcvd_w) \wedge (sent_y = rcvd_v) \wedge (x \geq y))$
4. **Basic authentication, no replays, strictly increasing, no drops:**
   $\mathsf{cond}_4 = (u < v) \vee (c \neq sent_v)$

HIERARCHY OF AEAD

$\text{Exp}_{\Pi,\mathcal{A}}^{\text{aead}_i - b}()$:

$k \xleftarrow{\$} \text{Kgn}()$
$st_E \leftarrow \bot, st_D \leftarrow \bot$
$u \leftarrow 0,\ v \leftarrow 0$
$\text{phase} \leftarrow 0$
$b' \xleftarrow{\$} \mathcal{A}^{\text{Encrypt}(\cdot),\text{Decrypt}(\cdot)}()$
return b'

Oracle Encrypt(ℓ, ad, m_0, m_1):

$u \leftarrow u + 1$
$(sent.c^{(0)}, st_E^{(0)}) \leftarrow \text{E}(k, \ell, \text{ad}, m_0, st_E)$
$(sent.c^{(1)}, st_E^{(1)}) \leftarrow \text{E}(k, \ell, \text{ad}, m_1, st_E)$
if $sent.c^{(0)} = \bot$ or $sent.c^{(1)} = \bot$ **then**
  return $\bot$
end if
$(sent.ad_u, sent.c_u, st_E) := (\text{ad}, sent.c^{(b)}, st_E^{(b)})$
return $sent.c_u$

Oracle Decrypt(ad, c):

if $b = 0$ **then**
  return $\bot$
end if
$v \leftarrow v + 1$
$rcvd.c_v \leftarrow c$
$(\text{ad}, m, \alpha, st_D) \leftarrow \text{D}(k, \text{ad}, c, st_D)$
if $(\alpha = 1) \wedge \text{cond}_i$ **then**
  $\text{phase} \leftarrow 1$
end if
if $\text{phase} = 1$ **then**
  return m
end if
return $\bot$

1. **Basic authenticated encryption:**
   $\text{cond}_1 = (\nexists w : (c = sent.c_w) \wedge (\text{ad} = sent.ad_w))$
2. **Basic authenticated encryption, no replays:**
   $\text{cond}_2 = (\nexists w : (c = sent.c_w) \wedge (\text{ad} = sent.ad_w)) \vee (\exists w < v : c = rcvd.c_w)$
3. **Basic authenticated encryption, no replays, strictly increasing:**
   $\text{cond}_3 = (\nexists w : (c = sent.c_w) \wedge (\text{ad} = sent.ad_w)) \vee (\exists w, x, y : (w < v) \wedge (sent.c_x = rcvd.c_w) \wedge (sent.c_y = rcvd.c_v) \wedge (x \geq y))$
4. **Basic authenticated encryption, no replays, strictly increasing, no drops:**
   $\text{cond}_4 = (u < v) \vee (c \neq sent.c_v) \vee (\text{ad} \neq sent.ad_v)$

Level 1
Paterson–Ristenpart–Shrimpton 2011

MEE–TLS encoding – CBC
(message len.) $+$ (tag len.) $>$ (block len.) -8

} TLS satisfies **Level 1** AEAD

NTNU – Trondheim
Norwegian University of Science and Technology

SECURE CHANNELS WITH TLS

Authenticated and Confidential Channel Establishment (ACCE)

Level 4
Jager–Kohlar–Schäge–Schwenk 2012

Stateful length-hiding AEAD at **Level 4** } ACCE security for TLS (Suites: TLS-DHE)

Level 4
Krawczyk–Paterson–Wee 2013

Stateful length-hiding AEAD at **Level 4**
Constrained chosen ciphertext security } ACCE security for TLS (Suites: TLS-RSA, TLS-CCA, TLS-DH, TLS-DHE)

IMPLICATIONS BETWEEN AUTHENTICATION LEVELS

st'_{E} and st'_{D}:

- st'_{E} : st'_{E}.substate $:= st_{\mathrm{E}}$, where st_{E} is the state in Π, st'_{E}.counter
- st'_{D} : st'_{D}.substate $:= st_{\mathrm{D}}$, where st_{D} is the state in Π, st'_{D}.status, st'_{D}.sqnlist

---

$\mathrm{Kgn}'()$:

return $\Pi.\mathrm{Kgn}()$

$\mathrm{Snd}'(k, m, st'_{\mathrm{E}})$:

$(c, st'_{\mathrm{E}}.\mathsf{substate})$
$\quad \leftarrow \Pi.\mathrm{Snd}(k, \mathtt{Ecd}(st'_{\mathrm{E}}.\mathsf{counter}, m), st'_{\mathrm{E}}.\mathsf{substate})$
$st'_{\mathrm{E}}.\mathsf{counter} \leftarrow st'_{\mathrm{E}}.\mathsf{counter} + 1$
return (c, st'_{E})

$\mathrm{Rcv}'(k, c, st'_{\mathrm{D}})$:

if $st'_{\mathrm{D}}.\mathsf{status} = \mathsf{failed}$ **then**
$\quad$ **return** $(\perp, 0, st_{\mathrm{D}})$
end if
$(m_{\Pi}, \alpha, st'_{\mathrm{D}}.\mathsf{substate})$
$\quad \leftarrow \Pi.\mathrm{Rcv}(k, c, st'_{\mathrm{D}}.\mathsf{substate})$
if $\alpha = 1$ **then**
$\quad (\mathsf{sqn}, m, \alpha) \leftarrow \mathtt{Dcd}(st'_{\mathrm{D}}.\mathsf{sqnlist}, m_{\Pi})$
end if
if $(\alpha = 0) \vee \mathtt{TEST}i$ **then**
$\quad st'_{\mathrm{D}}.\mathsf{status} = \mathsf{failed}$
$\quad$ **return** $(\perp, 0, st'_{\mathrm{D}})$
end if
$st'_{\mathrm{D}}.\mathsf{sqnlist} = st'_{\mathrm{D}}.\mathsf{sqnlist} || \mathsf{sqn}$
return $(m, \alpha, st'_{\mathrm{D}})$

- **Basic authentication, no replays:**
  $\mathtt{TEST2} = (\exists j : \mathsf{sqn} = st'_{\mathrm{D}}.\mathsf{sqnlist}_j)$
- **Basic authentication, no replays, strictly increasing:**
  $\mathtt{TEST3} = (\exists j : \mathsf{sqn} \not> st'_{\mathrm{D}}.\mathsf{sqnlist}_j)$
- **Basic authentication, no replays, strictly increasing, no drops:**
  $\mathtt{TEST4} = (\exists j : \mathsf{sqn} \not> st'_{\mathrm{D}}.\mathsf{sqnlist}_j) \vee (\mathsf{sqn} \neq \max\{st'_{\mathrm{D}}.\mathsf{sqnlist}_j\} + 1)$

IMPLICATIONS BETWEEN AEAD LEVELS

st'_{E} and st'_{D}:

- st'_{E} : st'_{E}.substate $:= st_{\mathrm{E}}$, where st_{E} is the state in Π, st'_{E}.counter
- st'_{D} : st'_{D}.substate $:= st_{\mathrm{D}}$, where st_{D} is the state in Π, st'_{D}.status, st'_{D}.sqnlist

---

$\Pi'_i.\mathrm{Kgn}()$:

```
return Π.Kgn()
```

$\Pi'_i.\mathrm{E}(k, l, \mathtt{ad}, m, st'_{\mathrm{E}})$:

```
(ad_Π, m_Π) ← Ecd(st'_E.counter, ad, m)
(c, st'_E.substate)
    ← Π.E(k, m_Π, ad_Π, l, st'_E.substate)
st'_E.counter ← st'_E.counter + 1
return (c, st'_E)
```

$\Pi'_i.\mathrm{D}(k, \mathtt{ad}, c, st'_{\mathrm{D}})$:

```
if st'_D.status = failed then
    return (⊥, 0, st_D)
end if
(ad_Π, m_Π, α, st'_D.substate)
    ← Π.D(k, ad, c, st'_D.substate)
if α = 1 then
    (sqn, ad, m, α) ← Dcd(st'_D.sqnlist, ad_Π, m_Π)
end if
if (α = 0) ∨ TESTi then
    st'_D.status = failed
    return (⊥, 0, st'_D)
end if
st'_D.sqnlist = st'_D.sqnlist||sqn
return (m, α, st'_D)
```

- **Basic authentication, no replays:**
  $\mathtt{TEST2} = (\exists j : \mathsf{sqn} = st'_{\mathrm{D}}.\mathsf{sqnlist}_j)$
- **Basic authentication, no replays, strictly increasing:**
  $\mathtt{TEST3} = (\exists j : \mathsf{sqn} \not> st'_{\mathrm{D}}.\mathsf{sqnlist}_j)$
- **Basic authentication, no replays, strictly increasing, no drops:**
  $\mathtt{TEST4} = (\exists j : \mathsf{sqn} \not> st'_{\mathrm{D}}.\mathsf{sqnlist}_j) \vee (\mathsf{sqn} \neq \max\{st'_{\mathrm{D}}.\mathsf{sqnlist}_j\} + 1)$

Computational Analysis:

Complexity-theoretic reduction proofs

- Protocol specification: MAC / AEAD / ...
- Adversary capabilities: network control / queries / ...
- Adversary winning conditions: experiment / advantage / ...

Security is reducible to that of
an underlying *hard* problem

Theorem

Let Π be a secure level-1 authentication scheme and `Coding` *be an authentication encoding scheme with collision-resistant encoding. Let $i \in \{2, 3, 4\}$. Then $\Pi'_i = P(\Pi, \texttt{Coding}, \texttt{TEST}i)$ is a secure level-i authentication scheme. Specifically, let $\mathcal{A}$ be an adversary algorithm that runs in time t and asks q_s* Send *queries and q_r* Recv *queries, and let $q = q_s + q_r$. Then there exists an adversary $\mathcal{B}$ that runs in time $t_\mathcal{B} \approx t$ and asks no more than $q_\mathcal{B} = \frac{1}{2} q_s(q_s - 1)$ queries, and an adversary $\mathcal{F}$ that runs in time $t_\mathcal{F} \approx t$ and asks $q_\mathcal{F} = q$ queries, such that*

$$\mathbf{Adv}^{\mathsf{auth}_i}_{P(\Pi,\texttt{Coding},\texttt{TEST}i)}(\mathcal{A}) \leq \mathbf{Adv}^{\mathsf{auth}_1}_{\Pi}(\mathcal{F}) + \mathbf{Adv}^{\mathsf{collision}}_{\texttt{Ecd}}(\mathcal{B}) \ .$$

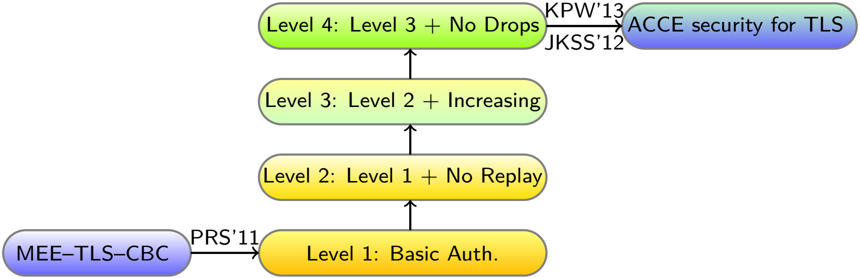
- Ecd security options: implicit or explicit sequence numbers?

Implications between Authentication Levels

- Level 4: Level 3 + No Drops — Received sqn is exactly the next expected one
- Level 3: Level 2 + Increasing — Received sqn is strictly greater than the last received
- Level 2: Level 1 + No Replay — Sequence number sqn does not repeat
- Level 1: Basic Auth.

Sequence number can be included **implicitly** or **explicitly**

AUTHENTICATION LEVELS APPLIED – TLS



AUTHENTICATION LEVELS APPLIED

- Protocol Analysis
  - Selection of appropriate authentication experiment
- Building Authentication Protocols
  - Encoding/checking sequence numbers to achieve desired level

Questions