

A trace has been found.

## Abbreviations

$$\begin{aligned} \sim X_1 &= (\text{Auth2}(\text{h}(\sim M_1), a_1, a_2, \text{spk}(a_3)), \text{sign}(\text{Auth3}(\text{Auth2}(\text{h}(\sim M_1), a_1, a_2, \text{spk}(a_3)), \text{hash}(\text{Client1}(\sim M_1, \sim M_2))), \\ &\quad a_3), \text{Client1}(\sim M_1, \sim M_2)) \\ &= (\text{Auth2}(\text{h}(\text{rp\_id}_4), a_1, \\ &\quad a_2, \text{spk}(a_3)), \text{sign}(\text{Auth3}(\text{Auth2}(\text{h}(\text{rp\_id}_4), a_1, a_2, \text{spk}(a_3)), \text{hash}(\text{Client1}(\text{rp\_id}_4, \text{challenge}_3))), a_3), \\ &\quad \text{Client1}(\text{rp\_id}_4, \text{challenge}_3)) \end{aligned}$$

## Honest Process

Attacker

```
{1}new rpid_4
```

```
{2}new clientid_1
```

```
{3}new pinAuth_3
```

```
{4}new wk_2
```

```
{5}new aaguid_4
```

```
{6}new username_4
```

```
{7}new skA_2
```

```
{9}insert rp_record(username 4,aaguid 4,senc(Auth1(
    username 4,rpId 4,skA 2),wk 2),spk(skA 2))
```

```
{10}insert auth_record(senc(Auth1(username_4, rpid_4,
                               skA 2), wk 2))
```

Beginning of process RP\_Auth

Beginning of process **Client\_Auth**

Beginning of process **Auth\_Auth**

```
~M = username_4
```

```
~M = username 4
```

```
{22}get rp_record(username 4,aaguid 4,senc(Auth1(
  username 4,rpid 4,skA 2),wk 2),spk(skA 2))
```

---

{13}new challenge\_3

$$(\sim M_1, \sim M_2, \sim M_3) = (\text{rp\_id}_4, \text{challenge}_3, \text{senc}(\text{Auth1}(\text{username}_4, \text{rp\_id}_4, \text{skA}_2), \text{wk}_2))$$
 $\sim X_1$ 

```
{20}event Server_Finish_Auth(username_4, rpid_4,  
a_1, a_2, spk(a_3))
```