UNIVERSITY OF AGDER

Formal Analysis about Security Requirements of a Group Authentication Protocol by Scyther

Huihui Yang, ICT, University of Agder

13/10/2014

Contents

- Background knowledge of Scyther
- Protocol introduction
- Protocol formalization
- Results

Scyther

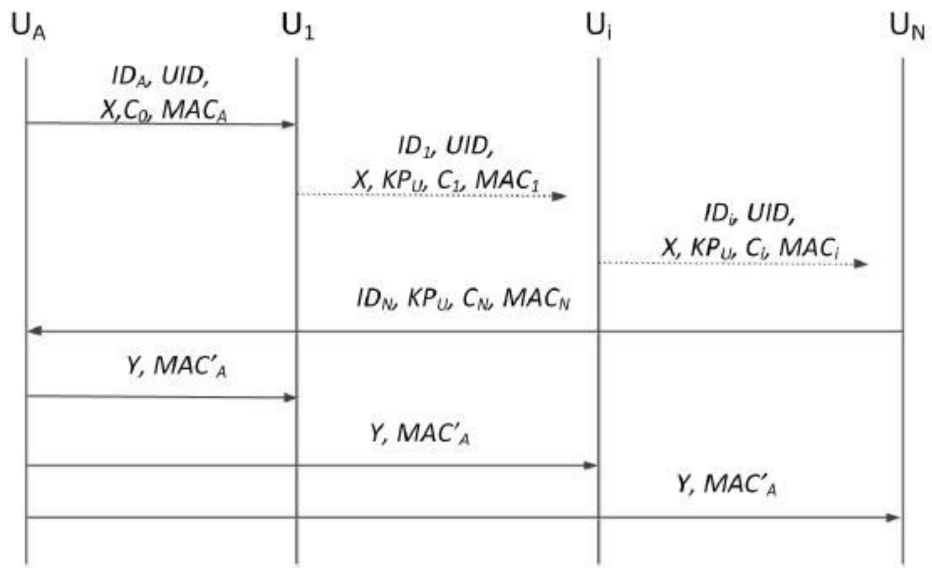
- Scyther is a tool for the automatic verification of sec
  - http://www.cs.ox.ac.uk/people/cas.cremers/sc
- Claims: claim(R, SKR, rt)
- Commitment: claim(R_1, Commit, R_2, rt)
- Match(p_1, p_2)

```
usertype SharedSecret;
hashfunction H;
protocol Example(A, B){
  role A{
    fresh x : SharedSecret;
    var y : nonce;
    send_1(A, B, {x}k(A, B));
    recv_2(B, A, {H(y)}sk(B));
  };
  role B{
    fresh y : nonce;
    var x : SharedSecret;
    recv_1(A, B, {x}k(A, B));
    send_2(B, A, {H(y)}sk(B));
  };
}
```

Adversary Model

- Adversary model: Dolve-Yao model
- Adversary ability: eavesdrop, delete message, learn knowledge, create and insert messages

Group Authentication Framework Introduction



1) $U_A \rightarrow U_1 : ID_A, UID, X, C_0, MAC_A.$

2) $U_i \rightarrow U_{i+1} : ID_i, UID, X, KP_U, C_i, MAC_i,$ where $1 \leq i \leq N-1.$

3) $U_N \rightarrow U_A : ID_N, KP_U, C_N, MAC_N.$

4) $U_A \rightarrow \mathbb{U} : Y, MAC'_A.$

Protocol Formalization (1)

- Discrete Logarithm Problem (DLP) and Elliptic Curve Discrete Logarithm Problem (ECDLP) based: Type 1 and Type 2
  - Only formalize DLP-based protocol of type 1
- Group member: 3
- Hard problems: type “hashfunction”
  - Diffie-Hellman problem, hash function, proxy encryption, MAC

Protocol Formalization (2)

- Security requirements: claims
  - Mutual authentication, implicit authentication, against impersonation attack, against passive adversaries

1) $match(h_i, H(U_A, U_i, x_a, t_i))$, where $1 \leq i \leq 3$.
5) $claim(U_A, Commit, U_i, V_i)$, where $1 \leq i \leq 3$.
6) $claim(U_R, SKR, K_G)$, where $R \in \{U_A, U_i\}$ and $1 \leq i \leq 3$.
7) $claim(U_A, SKR, h(g(n_i), m_i))$, where $1 \leq i \leq 3$.
8) $claim(U_i, SKR, h(g(m_i), n_i))$, where $1 \leq i \leq 3$.
9) $claim(U_i, SKR, h(g(n_j), n_i))$, where $1 \leq i, j \leq 3$ and $i \neq j$.

Results

Claim				Status		Comments
Group_authentication_DLP	UA	Group_authentication_DLP,UA1	SKR KG	Ok	Verified	No attacks.
		Group_authentication_DLP,UA2	SKR h(gn1,m1)	Ok	Verified	No attacks.
		Group_authentication_DLP,UA3	SKR h(gn2,m2)	Ok	Verified	No attacks.
		Group_authentication_DLP,UA4	SKR h(gn3,m3)	Ok	Verified	No attacks.
	U1	Group_authentication_DLP,U11	SKR KG	Ok	Verified	No attacks.
		Group_authentication_DLP,U12	SKR h(gm1,n1)	Ok	Verified	No attacks.
		Group_authentication_DLP,U13	SKR h(gn2,n1)	Ok	Verified	No attacks.
		Group_authentication_DLP,U14	SKR h(gn3,n1)	Ok	Verified	No attacks.
	U2	Group_authentication_DLP,U21	SKR KG	Ok	Verified	No attacks.
		Group_authentication_DLP,U22	SKR h(gm2,n2)	Ok	Verified	No attacks.
		Group_authentication_DLP,U23	SKR h(gn1,n2)	Ok	Verified	No attacks.
		Group_authentication_DLP,U24	SKR h(gn3,n2)	Ok	Verified	No attacks.
	U3	Group_authentication_DLP,U31	SKR KG	Ok	Verified	No attacks.
		Group_authentication_DLP,U32	SKR h(gm3,n3)	Ok	Verified	No attacks.
		Group_authentication_DLP,U33	SKR h(gn1,n3)	Ok	Verified	No attacks.
		Group_authentication_DLP,U34	SKR h(gn2,n3)	Ok	Verified	No attacks.

THANK YOU!