



Symmetric-Key Authentication Services Revisited

B. Crispo, B. Popescu, A. Tanenbaum

Vrije Universiteit Amsterdam

crispo@cs.vu.nl <http://www.cs.vu.nl/~crispo>



Outline

- Motivation
- Related Work
- Approach proposed
- Analysis (Pros/Cons)
- Conclusion/Future Work



Motivation

- Technological changes
- Existing Symmetric-Key Authentication Schemes designed long time ago
- Alternative **in some cases** to Public-Key technology



Technological changes

- Moore's Law. Memory speed/density increases 30% every year (for at least another decade)
- MANET
 - Local versus global connectivity
 - *Ad-hoc* groups
 - Peer-to-peer



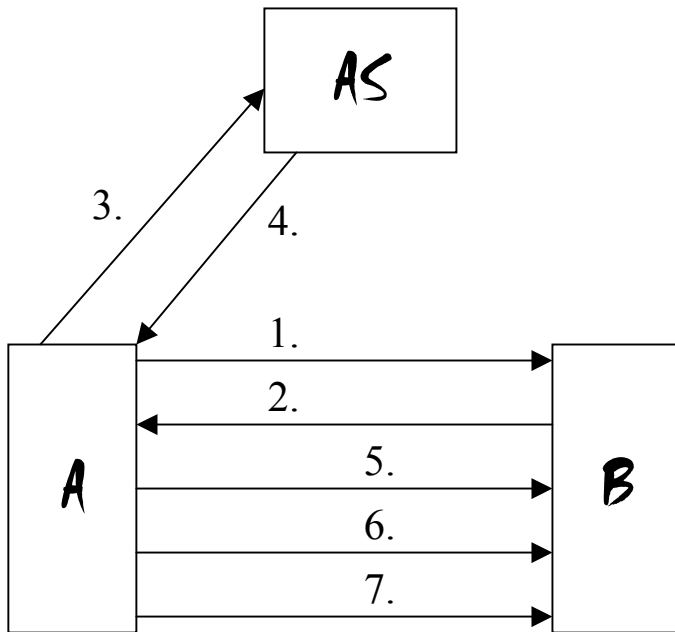
Existing SK schemes

- Needham-Schroeder (78, DS 81, 87) → Kerberos (88)

- Original assumptions
 - LAN
 - DoS attack
 - Dumb terminals (vt100)
 - Shared terminals
 - Memory against scalability



Needham-Schroeder



1. $A \rightarrow B: A$
2. $B \rightarrow A: \{A, NB_0\}_{K_{BAS}}$
3. $A \rightarrow AS: A, B, NA, \{A, NB_0\}_{K_{BAS}}$
4. $AS \rightarrow A: \{A, B, NA, K_{AB}\}_{K_{AAS}}, \{A, B, NB_0, K_{AB}\}_{K_{BAS}}$
5. $A \rightarrow B: \{A, B, NB_0, K_{AB}\}_{K_{BAS}}$
6. $B \rightarrow A: \{NB_1\}_{K_{AB}}$
7. $A \rightarrow B: \{f(NB_1)\}_{K_{AB}}$



Limitations

- Single point of failure (AS)
- Performance bottleneck (AS)
- AS is high sensitive target continuously exposed
- Too many keys
- Users cannot work offline
- Non repudiation not really possible



Freshness

- 2-phases protocol: Initial exchange

1. $A \rightarrow AS: A, B$

2. $AS \rightarrow A: \{A, B, K_s\}^{K_{AAS}}, \{A, B, K_s\}^{K_{BAS}}$

3. $A \rightarrow B : A, B, \{A, B, K_s\}^{K_{BAS}}, N_A$

4. $B \rightarrow A: [N_A]^{K_{AB}}, N_B$

5. $A \rightarrow B: [N_B]^{K_{AB}}$

where $K_{AB} = f(K_s, N_A, N_B)$



Keyed Hash Function: $f(.)$

- Easy to compute
- One way
- Collision resistance used for freshness
given K infeasible to find m_1 and m_2 such that
$$f(K, m_1) = f(K, m_2)$$
- As secure as encryption scheme used



Tokens

- AS tokens can be cashed and re-used
 1. $A \rightarrow AS: A, B$
 2. $AS \rightarrow A: \{A, B, K_s\}K_{AAS}, \{A, B, K_s\}K_{BAS}$
 3. $A \rightarrow B : A, B, \{A, B, K_s\}K_{BAS}, N_A$
 4. $B \rightarrow A: [N_A]K_{AB}, N_B$
 5. $A \rightarrow B: [N_B]K_{AB}$



Following exchanges

- 2nd phase of the protocol

1. $A \rightarrow B : A, B, N'_A$

2. $B \rightarrow A : [N'_A]K'_{AB}, N'_B$

3. $A \rightarrow B : [N'_B]K'_{AB}$

where $K'_{AB} = f(K_s, N'_A, N'_B)$



Uncovered issues

AS still needs to be on-line!!



Assumptions

- New assumptions
 - WAN
 - DDoS and DoS attacks
 - Powerful computer as end node
 - Plenty of memory
 - Size of population known
 - Peer-2-Peer secure communications without the server



Initialization

- AS offline!
- N size of population
- AS generates N symmetric keys used as master keys with the users
- Master keys are assigned to user as they register



User Registration (AS)

Index	Key	User Name	Issue Time	Exp. Time
0	K ₀	J.Smith	03.12.03	03.12.04
1	K ₁	P.Brown	07.12.03	07.12.04
..				
I	K _I	R.Getty	25.12.03	25.12.04
I+1	K _{I+1}	--	--	--
I+2	K _{I+2}	--	--	--
..				
N-1	K _{N-1}	--	--	--

K₀ master key assigned to J. Smith

K_{I+1} reserved to user next user that will register



User Registration (User)

- User go to the AS
- Verification of credentials (conventional)
- User receives the master key assigned to him by the AS
- User receive a set of tokens that allows him to authenticate to all the other master keys
- ..also for master keys that have not being assigned yet



Our scheme

Registration

1. $A \rightarrow AS: A$
2. $AS \rightarrow A: I, K_I, T, (S_{IK_{IJ}}, IC_{IJ})_{J \in \{0, \dots, N\}, J \neq I}$



Tokens

$\{J, K_{IJ}, A, T\}_{K_J}$

Introduction Certificate (IC_{IJ})

K_{IJ}

Secure Introduction Key (SIK_{IJ})



User Registration (User)

User A, assigned index I

Key Index	Master Key	Introduction Certificate
0	SIK_{I0}	{0, A, SIK_{I0}, T}K₀
1	SIK_{I1}	{1, A, SIK_{I1}, T}K₁
	.	.
	.	.
	.	.
I-1	SIK_{I,I-1}	{I-1, A, SIK_{I,I-1}, T}K_{I-1}
I+1	SIK_{I,I+1}	{I+1, A, SIK_{I,I+1}, T}K_{I+1}
	.	.
	.	.
	.	.
N-1	SIK_{I,N-1}	{N-1, A, SIK_{I,N-1}, T}K_{N-1}



Sessions

User A (index I) and User B (index J)

1. $A \rightarrow B: I, N_A$
2. $B \rightarrow A: J, N_B, IC_{JI}$
3. $A \rightarrow B: [N_B]K_{AB}, IC_{IJ}$
4. $B \rightarrow A: [N_A]K_{AB}$

where $K_{AB} = f(SIK_{IJ}, SIK_{JI}, N_A, N_B)$



Our scheme

Memory requirements

$N * |\text{master key}|$

for the AS

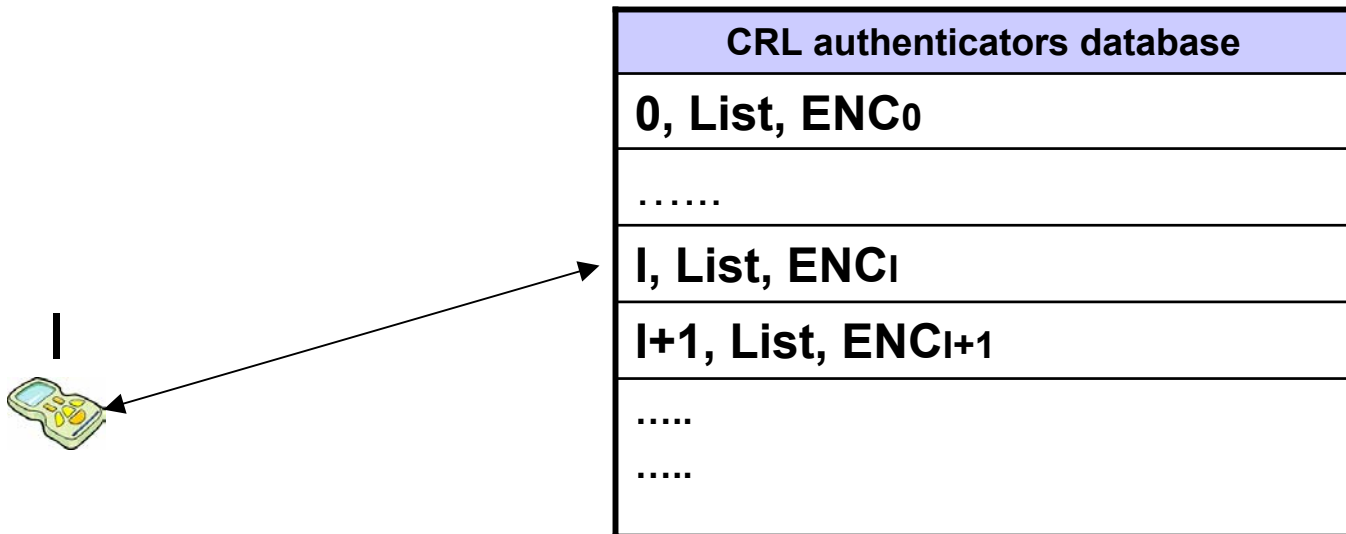
$N * |\text{SIK key} + \text{ticket}|$

for each user



Key Revocation

- Based on CRL
 - List of indices of revoked tickets (users)
 - Auth = [hash(list), T]
 - ENC_x = Auth, HMAC[K_x, Auth]



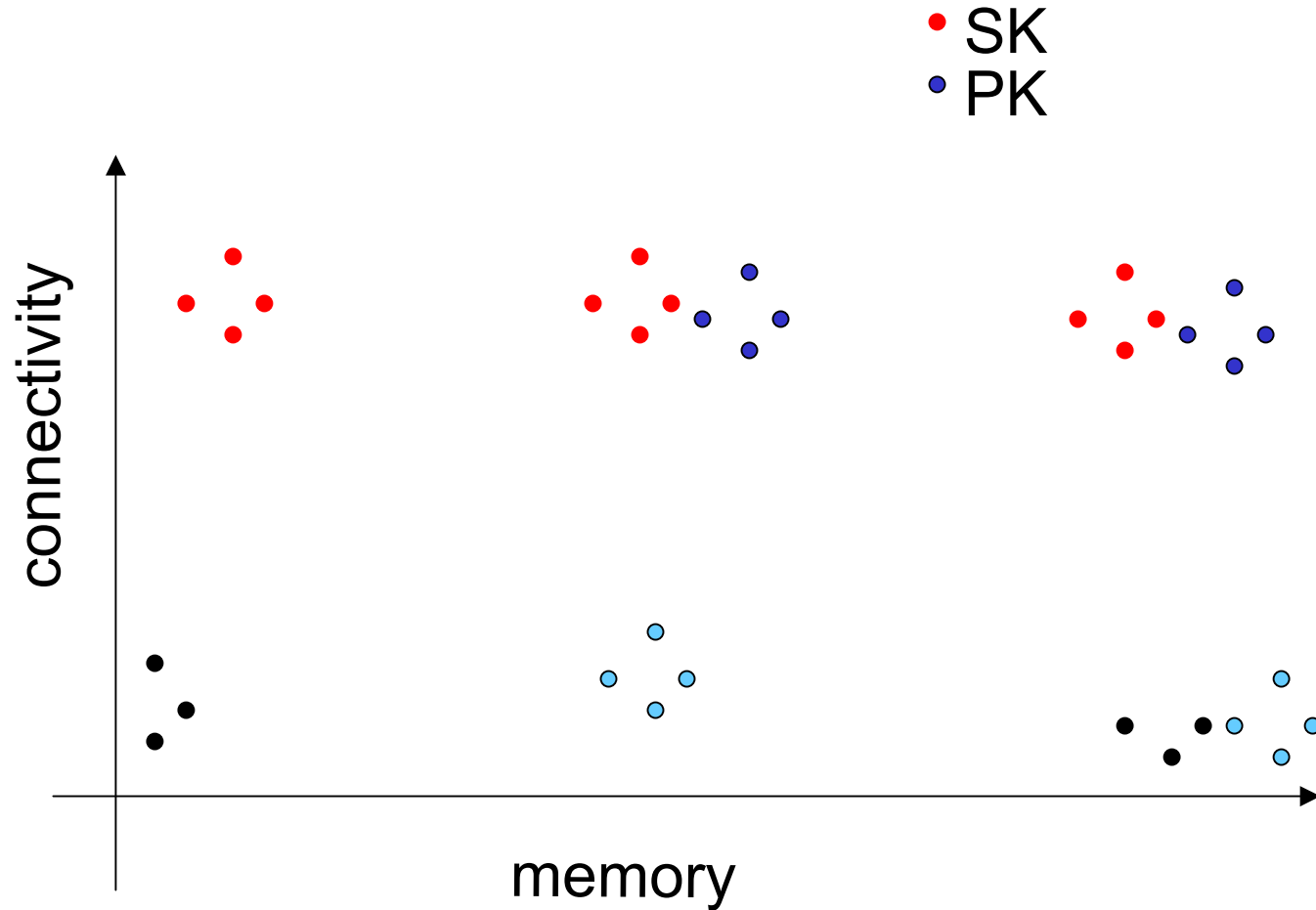


Advantages

- AS off-line
 - No single point of failure (or at least not critical as before)
 - No performance bottleneck
 - AS is not exposed to remote attacks (DoS)
 - Users can work offline
- Support mobility
- Non repudiation not really possible



Advantages





Limitations

- High memory requirements
- Size of population known *a-priori*
- AS workload
- Suitable only for some types of MANET
- Certificates with very different lifetimes
- Only where non-repudiation is not required



Future Work and Conclusions

- Implementation soon available
- What was impossible is becoming practical
- Many claimed shortcomings of SK authentication schemes are not due to SK but to the design of the systems
- Choose PK for the correct reasons!