cs261 Notes

Noah Johnson-Walls
11/09/09

Monday, November 09, 2009
10:51 AM

- No class on wednesday (holiday)
- HW 2 due tonight (11:59 pm)

Kerberos: schemes for securing

Nonces

$$\begin{tikzcd} A \arrow[r, shift right, "\{[N_B, m]\}"'] & B \arrow[l, shift right, "N_B"'] \end{tikzcd}$$

Timestamps

$$A \xrightarrow{\{[t, m]\}} B$$

sequence numbers

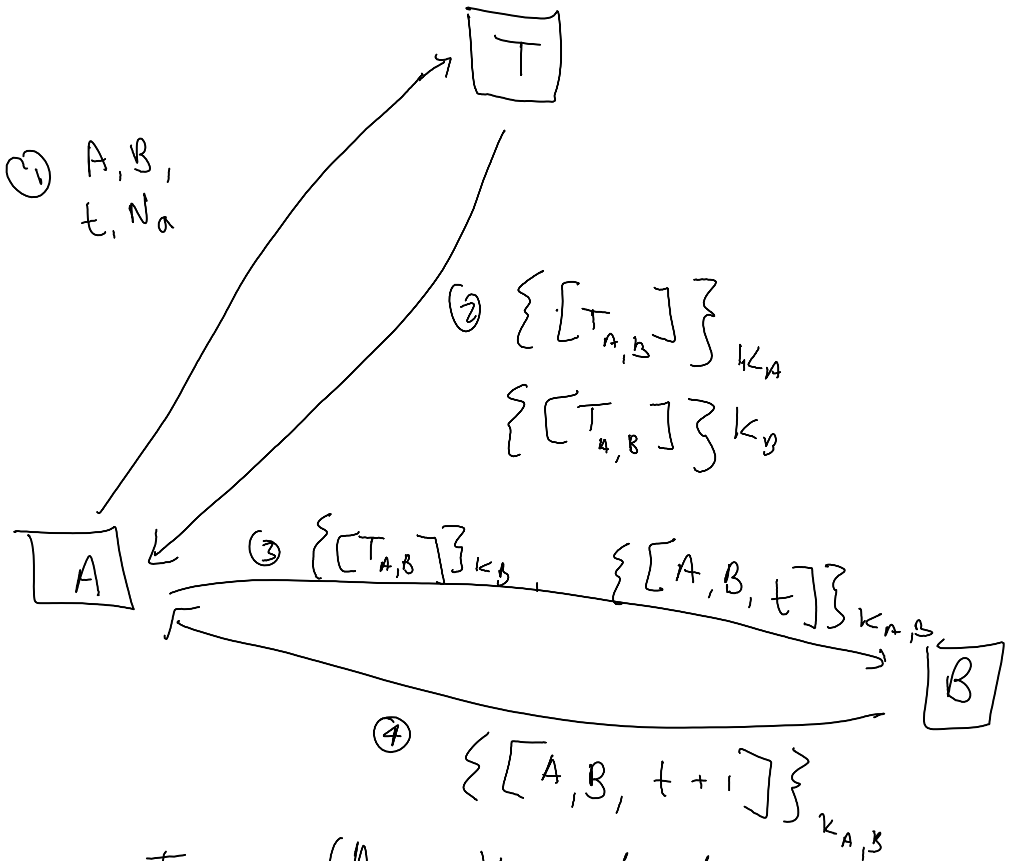
$$A \xrightarrow{\{[s, m]\}} B$$

	Nonces	Timestamps	Sequence
Replay	✓	✓	✓
Reflection	✓	maybe	✗
Deletion/Drop	✓	✗	✓
DoS	✗	✗	✗
Traffic Analysis	✗	✗	✗

Traffic Analysis X X X

Monday, November 09, 2009
11:05 AM

Diagram of Kerbros conversation


T
① A, B, t, N_a
② $\{[T_{A,B}]\}_{K_A}$
$\{[T_{A,B}]\}_{K_B}$
A
③ $\{[T_{A,B}]\}_{K_B}, \{[A, B, t]\}_{K_{A,B}}$
B
④ $\{[A, B, t+1]\}_{K_{A,B}}$

$$T_{A,B} = (A, B, K_{A,B}, t, t_{exp}, N_{a}, ipaddr_{A})$$

Note about notation used:

① "I, Alice, want a session key for use with Bob. It's now time t and here's a challenge: N_A"

$$A, B, t, N_A$$

Pros

- very consise and precise notation
- can be used in academic papers

Cons

- could mean something completely different
- two messages that could normally never collide could collide under condensed notation (this could enable attack)

Monday, November 09, 2009
11:27 AM

- from a security point of view, the Kerberos authentication server represents a huge security risk, since it stores everybody's password
- This system is subject to an offline brute force attack (if attacker sniffs an encrypted packet)

Weaknesses in Kerberos

- didn't use message authentication code to authenticate each message. A checksum is used, but this is not cryptographically secure..
- Random number generator is seeded with srand(time(0)) - the seed has a granularity of seconds, so it is easily guessable...
- System could benefit from public key
- could use SSL to establish encrypted channel

Strengths of Kerberos

- removing users (for example, if someone gets fired) is simple