CSC 580
Cryptography and Computer Security

Key Management and Distribution

Sections 14.1 - 14.2

April 12, 2018

Needham-Schroeder PK Protocol

Protocol designed in 1978. From the textbook:

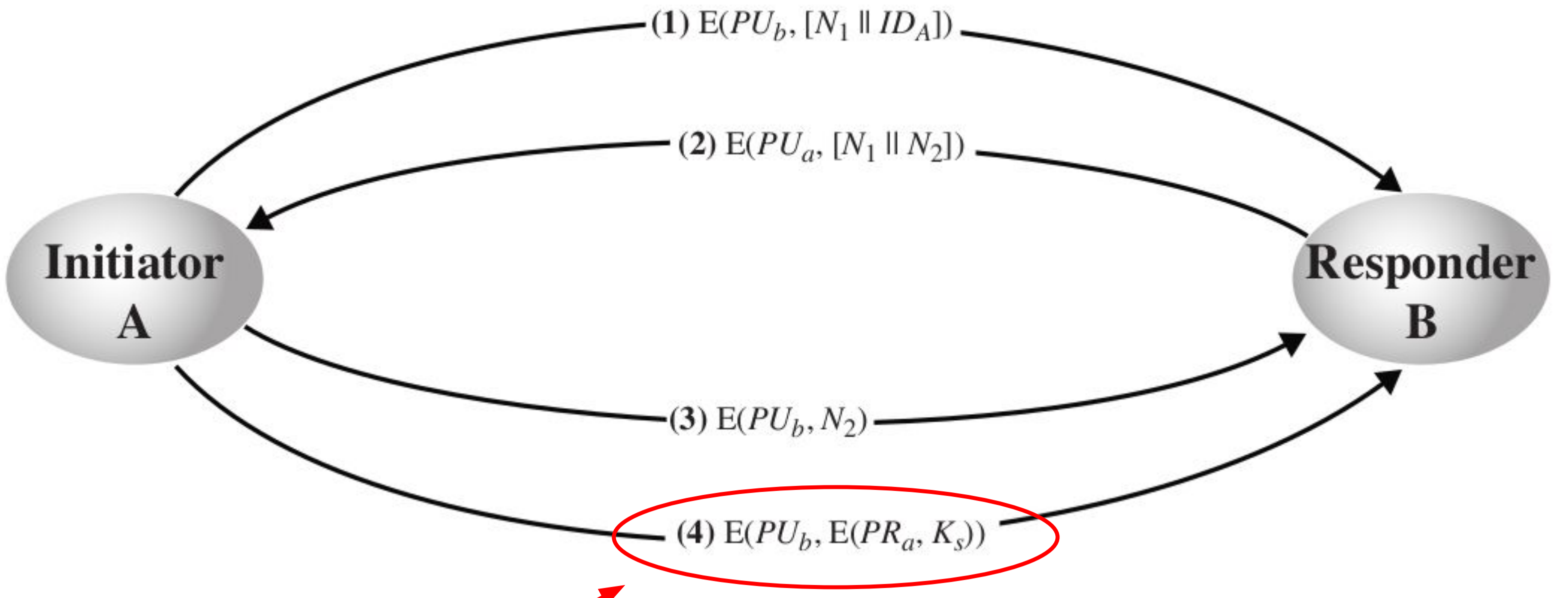

(1) $E(PU_b, [N_1 \| ID_A])$
(2) $E(PU_a, [N_1 \| N_2])$
Initiator
A
Responder
B
(3) $E(PU_b, N_2)$
(4) $E(PU_b, E(PR_a, K_s))$

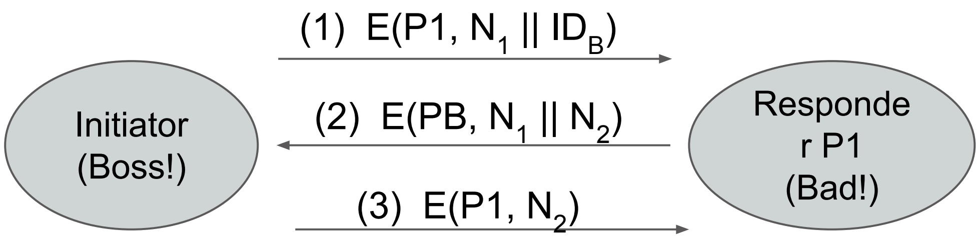
Figure 14.9 Public-Key Distribution of Secret Keys

Note: (4) is not in the actual Needham-Schroeder Protocol!

In real protocol: After (3), A and B share secrets N_1 and N_2

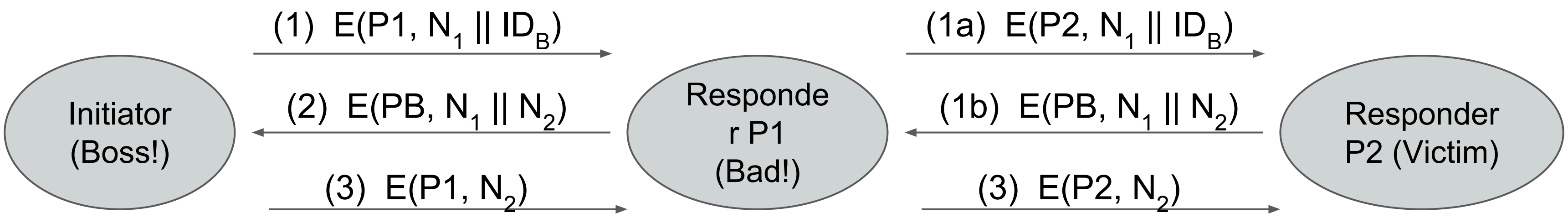
Needham-Schroeder PK Protocol - Oops!

But consider...



Needham-Schroeder PK Protocol - Oops!

But consider...



Initiator (Boss!)

(1) E(P1, N_1 || ID_B)

(2) E(PB, N_1 || N_2)

(3) E(P1, N_2)

Responde r P1 (Bad!)

(1a) E(P2, N_1 || ID_B)

(1b) E(PB, N_1 || N_2)

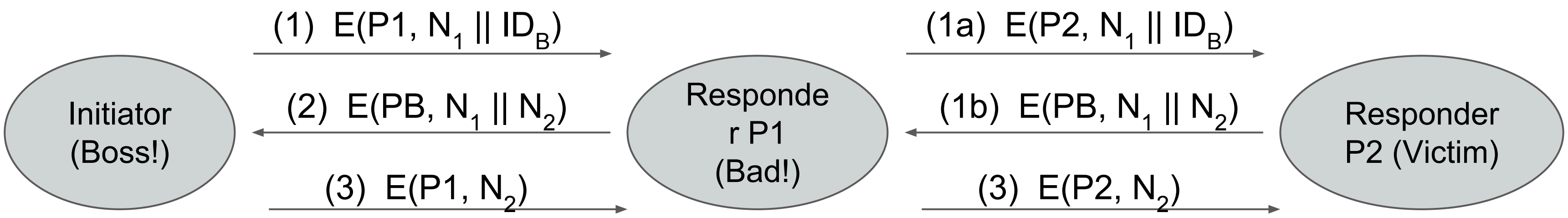
(3) E(P2, N_2)

Responder P2 (Victim)

As far as P2 is concerned, just did a key setup with the Boss!

Needham-Schroeder PK Protocol - Oops!

But consider...


(1) E(P1, N_1 || ID_B)
(1a) E(P2, N_1 || ID_B)
Initiator (Boss!)
(2) E(PB, N_1 || N_2)
Responde r P1 (Bad!)
(1b) E(PB, N_1 || N_2)
Responder P2 (Victim)
(3) E(P1, N_2)
(3) E(P2, N_2)

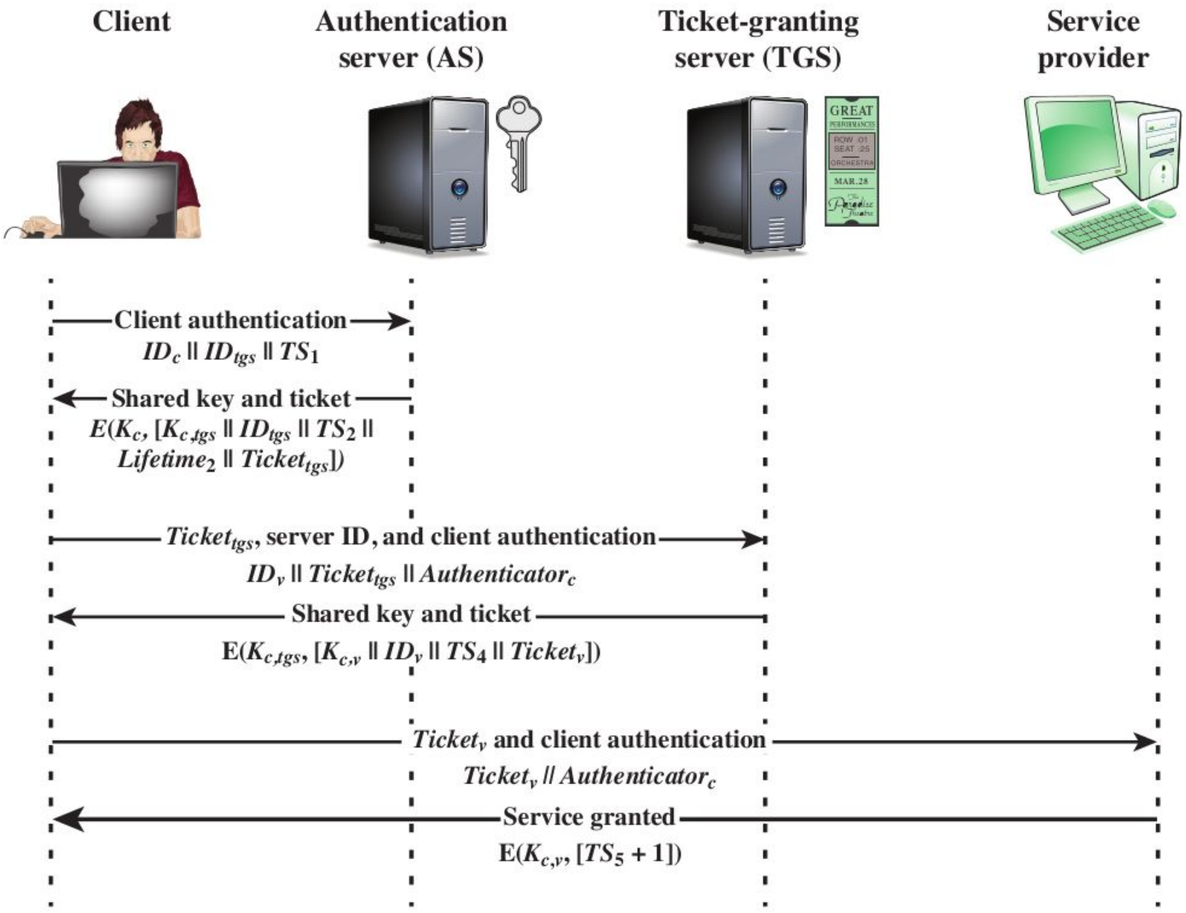
As far as P2 is concerned, just did a key setup with the Boss!

Some important points!

- N-S PK protocol “proved secure” in 1989
- Lowe found this attack in 1995
  - Simple solution: Add ID_{P1} in msg (2)

Humbling message for “provable security” people: Make sure you’re proving the right thing!

Kerberos



Client

Authentication server (AS)

Ticket-granting server (TGS)

Service provider

Client authentication

$ID_c \| ID_{tgs} \| TS_1$

Shared key and ticket

$E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs}$, server ID, and client authentication

$ID_v \| Ticket_{tgs} \| Authenticator_c$

Shared key and ticket

$E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_v$ and client authentication

$Ticket_v \| Authenticator_c$

Service granted

$E(K_{c,v}, [TS_5 + 1])$

Figure 15.3 Kerberos Exchanges

Kerberos

Demo!