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:

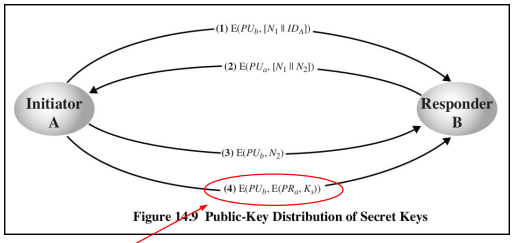
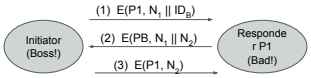


Figure 14.9 Public-Key Distribution of Secret Keys

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...

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

Needham-Schroeder PK Protocol - Oops!

But consider...

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

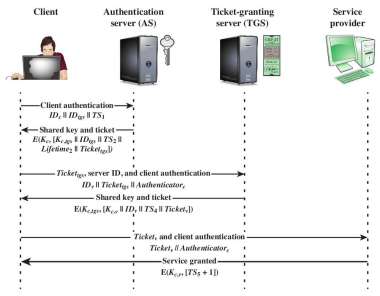


Figure 15.3 Kerberos Exchanges

Kerberos

Demo!