Postgraduate/Research Seminar on Security Autumn 2006

Introduction and Overview

N. Asokan, TML

Kaisa Nyberg, TCS

Agenda

- Welcome and introduction
- Introduction to the theme and example topics
- Administrivia
- Assignment presentation dates and review duties
- ESAS presentation dry run – Jukka Valkonen

Welcome

- Are you in the right place?
  - T-79.7001 Postgraduate Course in Theoretical Computer Science
  - T-110.7290 Research Seminar on Network Security
- About us
  - Kaisa Nyberg, Professor/TCS
  - N. Asokan, Professor/TML
  - Also affiliated to Nokia Research Center, Helsinki

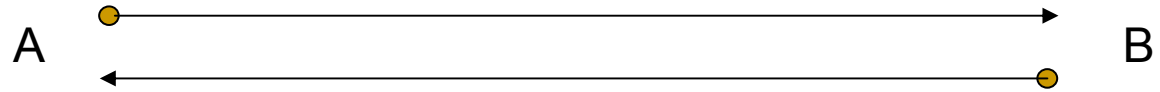
Introduction to the Theme and Example Topics

What is this seminar about?

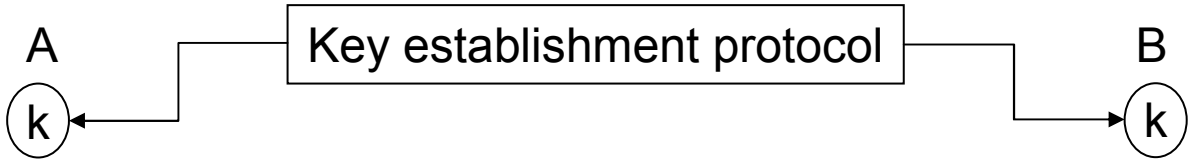
- New challenges in authentication and key establishment
- Authentication and key establishment (AKE) is a long-studied area
  - Starting from Needham-Schroeder in 1978
  - AKE protocols widely deployed: GSM security protocols, UMTS/AKA, TLS, Kerberos

Authentication and key establishment

Authentication: verifying the claimed identity of a principal



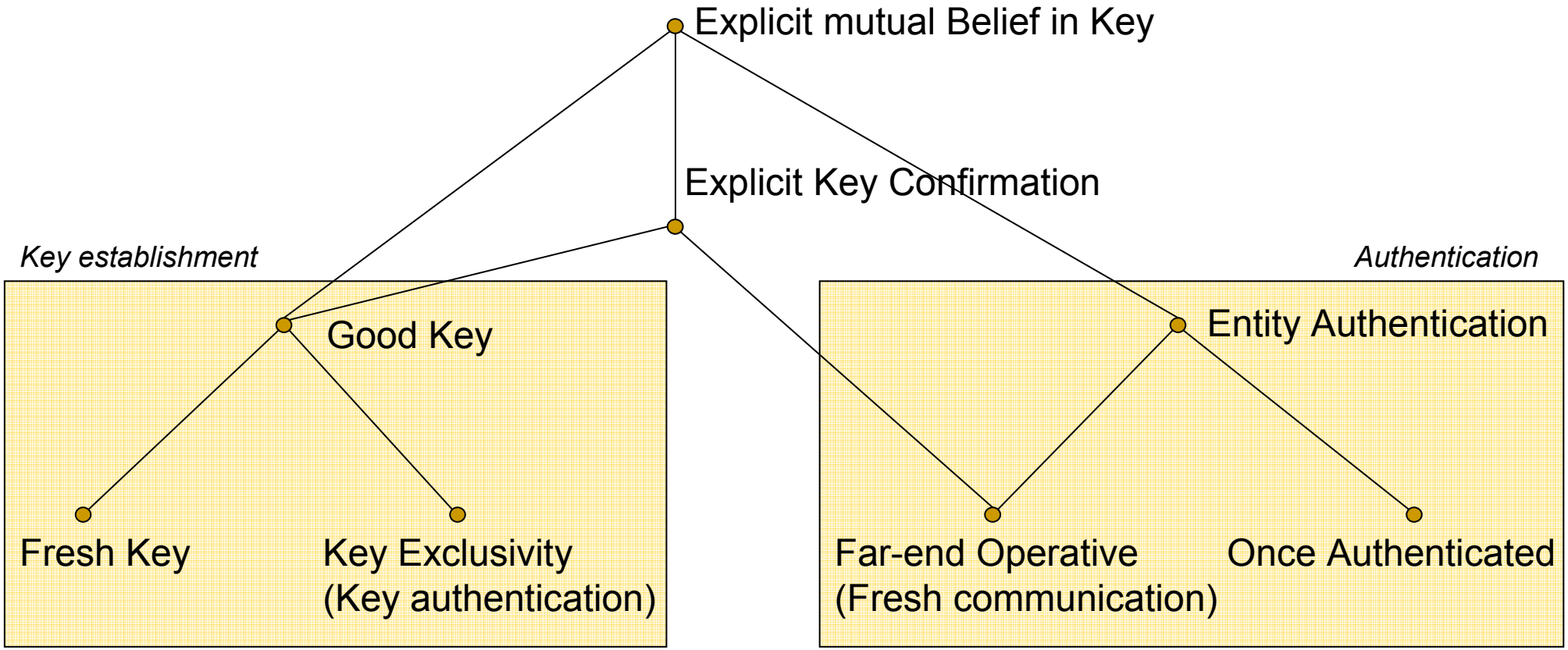
Key establishment: setting up a shared session key to protect subsequent communication



- Authentication without key establishment is typically not useful (exception, e.g.: physical access control)
- Key establishment can be key transport or key agreement

Goals of AKE: an example hierarchy

- No commonly agreed set of goals for AKE
- Below is an example set (Boyd and Mathuria)

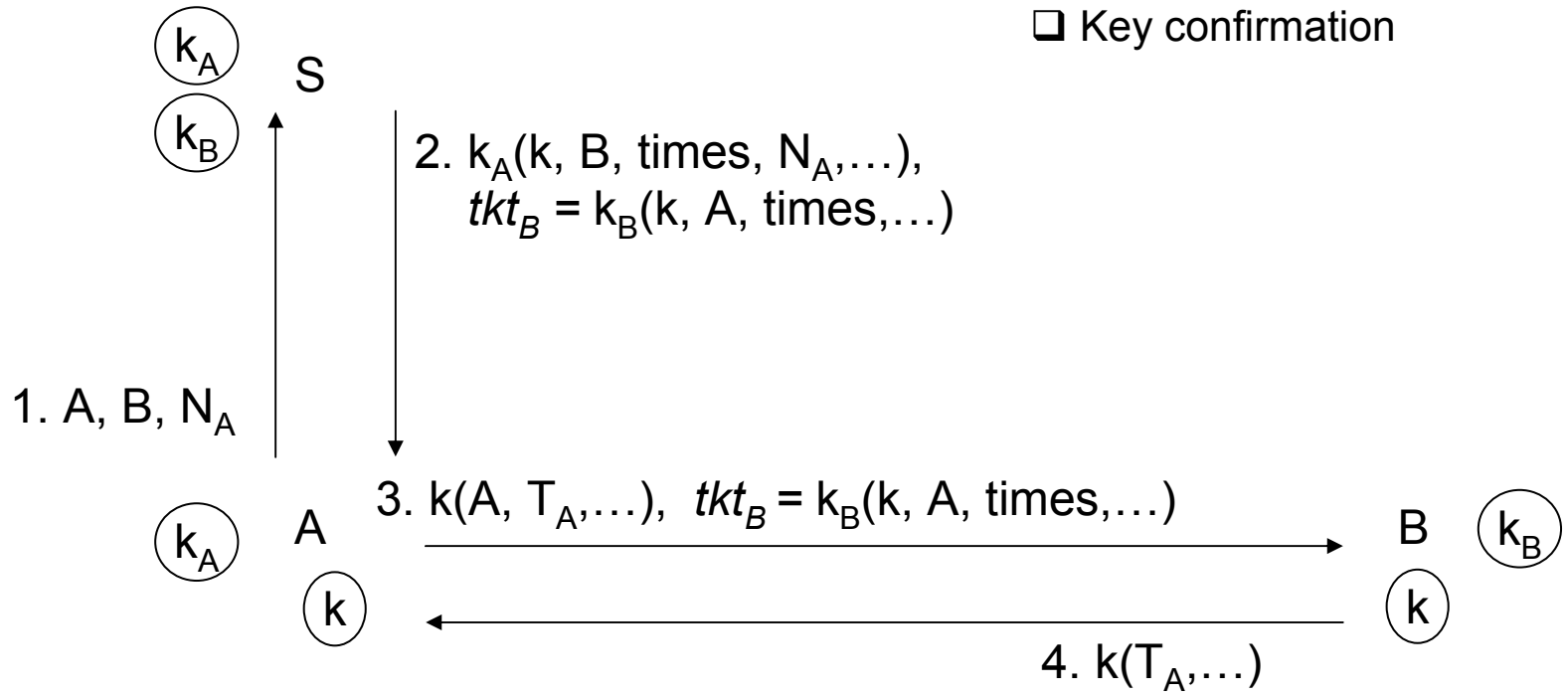


Further goals

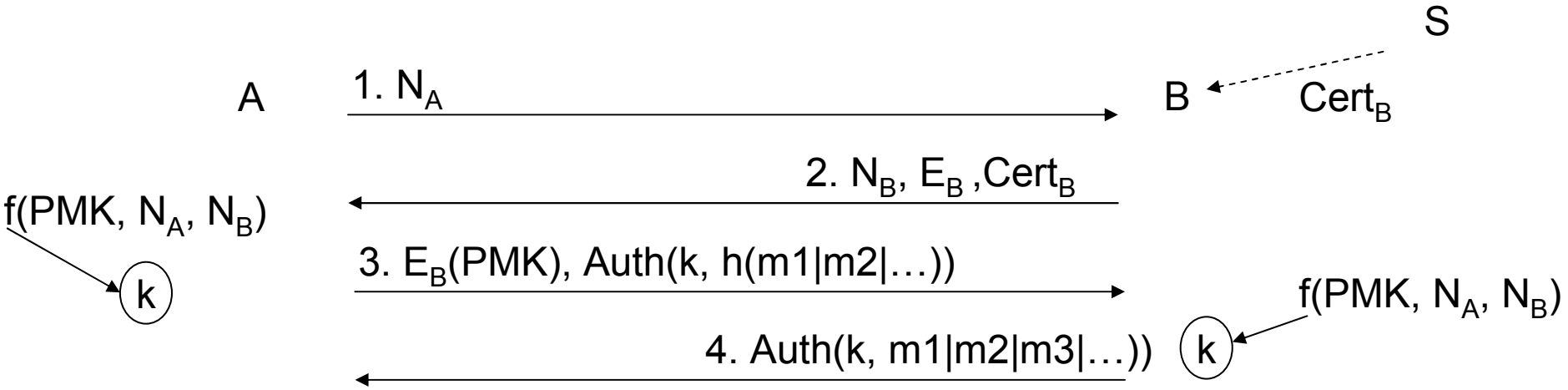
- Forward secrecy
  - Compromise of long term keys should not reveal past session keys
- Key separation and independence
  - Keys for different times and different purposes should be different and independent from one another

Example: Kerberos

- Prior enrollment with server
  - Basis for authentication and key exclusivity
- Timestamps to ensure freshness
- Key transport
  - Key confirmation



Example: Server-authenticated TLS



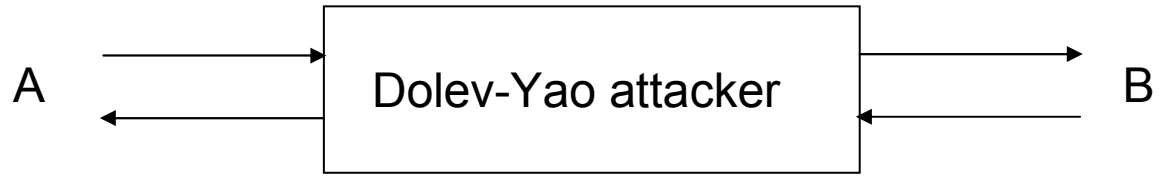
- Prior enrollment of public key E_B with a server,
- Prior initialization of server root public key in verifier
- Key agreement and key confirmation

Types of attacks

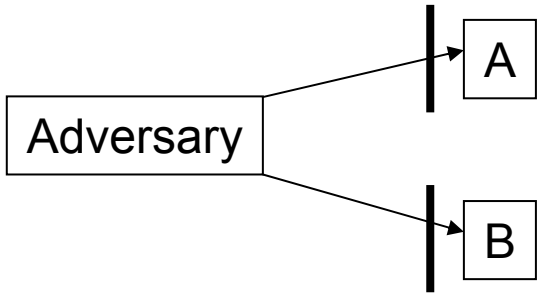
- Denial of service
- Replay, reflection, interleaving of whole messages
- Cut-and-paste of parts of messages
- Cryptanalysis
  - Using any combination of the above plus using honest players as oracles

Adversary models

- Passive vs. active adversary
- Dolev-Yao adversary: omniscient and omnipotent
  - can schedule/read/modify/insert messages between A and B



- Popular communication model for proofs



(New) Challenges in AKE

- Extending to groups
- Resource-constrained environments
- Revisiting attacker models
- The human factor
- Difficulty of formal analyses
- …

Key establishment in groups

- How to efficiently agree on a key?
  - *Group key agreement protocols*
- How to efficiently rekey when a member leaves or joins?
  - **Petri Jokela**: *Key agreement and key management for Secure multicast*
- What are the effects of interaction between key management schemes in different layers?
  - **Jukka Valkonen**: *Key agreement and key management for Secure multicast in practise, Case: WiMedia*

Resource constrained environments (1/2)

- Extremely resource constrained environments
  - Computational power, memory (sensors, RFID)
  - Bandwidth (sensor networks)
  - **Jan-Erik Ekberg**: *Key agreement between sensor network nodes*
  - *Authenticating communication between an external query/sink node and a sensor network node.*
  - *RFID authentication*

Resource constrained environments (2/2)

- Extremely resource constrained environments
  - Connectivity (Disruption-tolerant scenarios)
  - Processing time budget (packet-level authentication)
- Is it sensible to use identity-based key-agreement?
  - **Dan Forsberg**: *Identity-based authentication and key agreement*

Revisiting attacker models

- Is Dolev-Yao attacker model an overkill?
- Succesful examples of weaker models
  - Leap of faith
- Possibly covered in the sensor networks topic

The human factor (1/2)

- Secure First Connect
  - How can ordinary users set up AKE? Ease-of-use is paramount
  - No key management infrastructure: no server to enroll with
    - E.g., Bluetooth pairing, Home WLAN setup
  - **Nie Pin** *Key agreement protocols for First Connect*
  - **Jani Suomalainen** *Comparative survey of AKE in "First Connect" standard proposals, in terms of security, usability, and extensibility*.
  - **Vesa Vaskelainen**: *Theoretical bounds for human mediated data authentication protocols*

The human factor (2/2)

- End user access to remote services
  - Typically, based on just a short password
    - Other possibilities add cost: one-time passwords, h/w tokens
  - Attackers fool user into revealing password: phishing
  - What techniques can minimize risk of phishing?
    - Should be scalable, usable and affordable
    - Changing the whole world (e.g., deploying Single SignOn infrastructure) is difficult
  - **Kristiina Karvonen**: *Phishing-resistant authentication with human users*

Difficulty of formal analyses

- AKE Protocol design is notoriously error-prone
- No widely available, easy to use verification tool
  - But, *Analyzing security protocols with AVISPA* looks promising

Administrative Notes and other Trivia

Objectives of the seminar

- Understanding, evaluating current research
- Identifying and possibly shaping new research
- Effective peer reviewing

Approach

- Pick a topic and research it thoroughly
  - Some topics and starting pointers on course web page
- Write a paper and present it
- Revise paper based on feedback
  - Written review
  - Discussion during presentation
- Provide written review for two other papers
- Actively participate in discussions

What should your research aim for?

- At a minimum a good survey of state-of-the-art
  - Critical analysis: don't just summarize the papers
  - Reading between the lines: explain implicit assumptions or reasoning in the surveyed papers
- Ideally, aim for a publishable paper
  - Flaws in or improvements to previous work
  - The recommended topics have good potential for new results

How will you be evaluated?

- Quality of your own paper and presentation
  - Assessment by the co-ordinators
  - Reviews by assigned reviewers
- Quality of your own reviews
  - Constructive, detailed
- Participation in discussions

Credits and grading

- 3 Credits
  - Paper+presentation
- ½ Credit for each review
  - 2 reviews are mandatory
  - You earn an additional credit by doing **two extra** reviews. If you are interested in this, let the co-ordinators know the papers you want to review

Meetings

- Today: Introduction
- Sep 29: Lecture by Kaisa
- Student presentations: Starting October 13
  - We'll agree on the dates for presentations today
  - Review duties will be assigned by the co-ordinators
    - You can indicate any preferences you may have

Schedule

- Presenters make their papers available **1 week before** date of presentation (e-mail to reviewers and to co-ordinators who will post on web page)
- Reviews made available **2 days before** (Thursday 6:00 AM) presentation (e-mail to presenter, and to co-ordinators for web posting)
- Revised paper made available **1 week after** presentation (e-mail to co-ordinators for web posting)

Presentation schedule and review assignments

	Presenter
Oct 13	Jan-Erik Ekberg
Oct 20	Dan Forsberg
Oct 27	Nie Pin, Jani Suomalainen
Nov 3	Vesa Vaskelainen
Nov 10	Jan Hlinovsky
Nov 17	Petri Jokela, Jukka Valkonen
Nov 24	Maarit Hietalahti
Dec 1	Laura Takkinen
Dec 8	Kristiina Karvonen

Interested reviewers

- **Jan-Erik**: Jani, Dan
- **Jani**: Kristiina, Dan
- **Pin**: Vesa, Jukka
- **Vesa**: Jani, Jan-Erik [, Petri]
- **Petri**: Jan, Laura [, Dan]
- **Dan**: Maarit, Vesa [, Petri]
- **Jukka**: Pin, Kristiina
- **Kristiina**: Jan, Petri [, Jani]
- **Maarit:** Petri, Pin
- **Jan:** Laura, Maarit,
- **Laura:** Jan-Erik, Jukka