University of Nijmegen

The Ephemeral Pairing Problem

How to pay wirelessly, at the right counter

Jaap-Henk Hoepman
Security of Systems (SoS) group
Department of Computer Science
University of Nijmegen, the Netherlands
jhh@cs.kun.nl
www.cs.kun.nl/~jhh

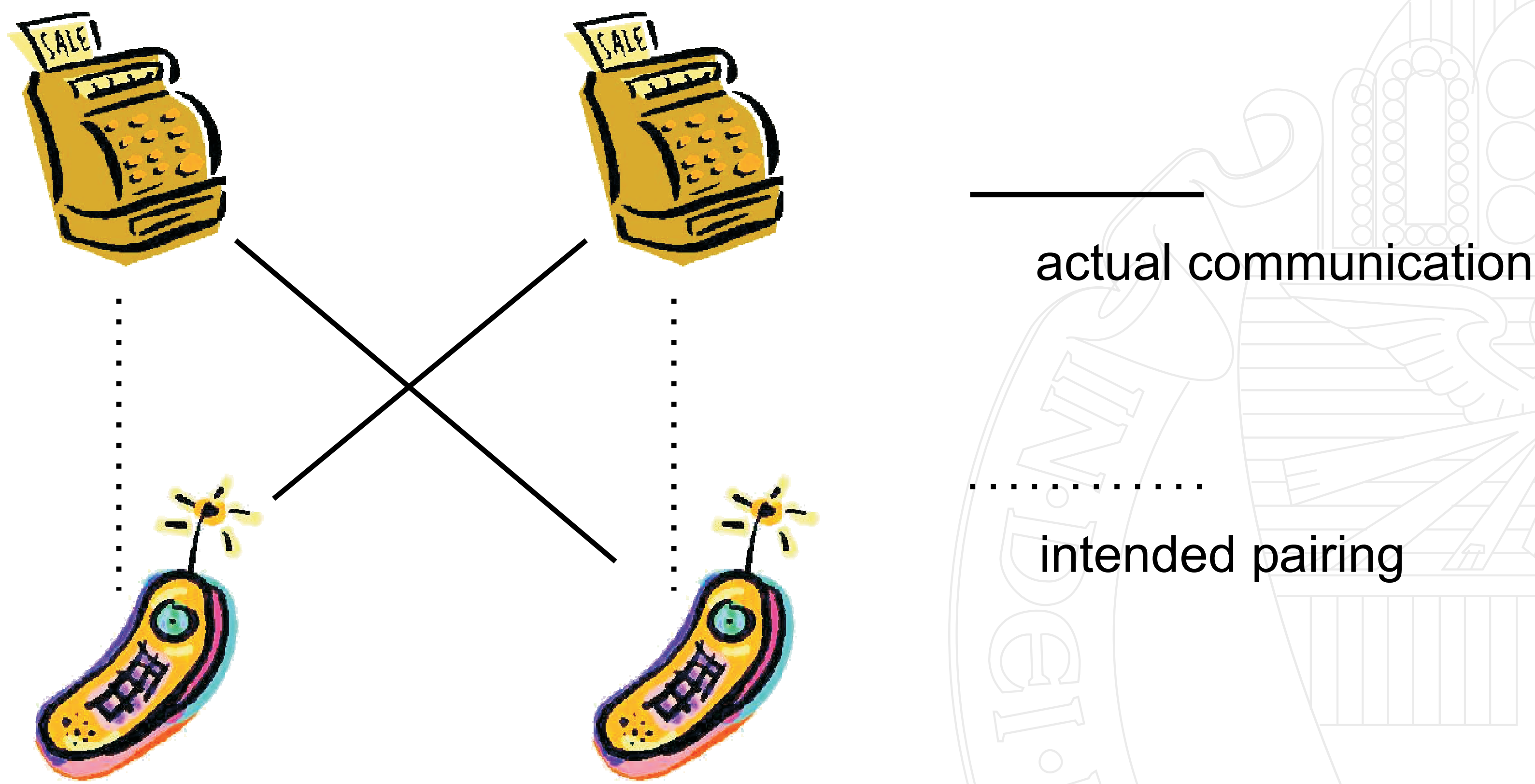
University of Nijmegen

Contents

- Introduction
- Model
- Background: EKE
- Protocols: φKE

University of Nijmegen

Introduction



The Ephemeral Pairing Problem

Given

- n physically identifiable nodes, human operated
- high bandwidth (anonymous) broadcast network
- simple point to point network (between operators)

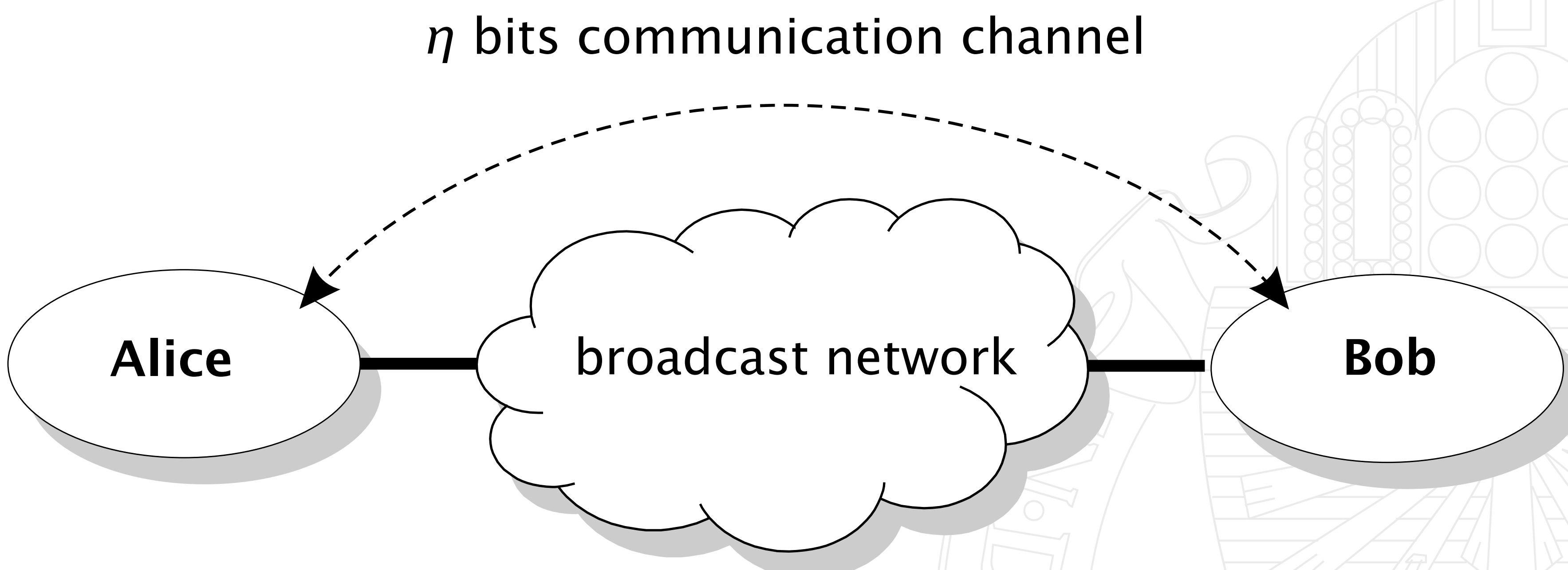
Goal: establish shared secret such that

(R1) both nodes are assured the secret is shared with the correct physical node,

(R2) no other node learns (part of) the shared secret, and

(R3) the operators need to perform only simple, intuitive steps.

Ephemeral Key Exchange (φKE)



Channel can be authentic (A) and/or private (P).

Goal: Alice and Bob must establish shared σ bits secret ($\sigma \gg \eta$).

Background: EKE (Bellovin & Merritt, 1992)

Goal: password authentication protocols, immune to off-line dictionary attacks.

Given: shared password P

Alice (client)		**Bob (server)**
generate key pair E_A, D_A	$\xrightarrow{A, P(E_A)}$	
decrypt and recover R	$\xleftarrow{P(E_A(R))}$	generate session key R
pick challenge c_A	$\xrightarrow{R(c_A)}$	decrypt, and
decrypt and verify	$\xleftarrow{R(c_A, c_B)}$	pick challenge c_B
	$\xrightarrow{R(c_B)}$	verify

Model

Encrypted key exchange model (Bellare, Pointcheval and Rogaway, 2000).

- Instance Π_p^i of principal p.
- Adversary can eavesdrop, modify, delete and insert messages. Modelled by oracles: Send(p, i, m), Execute(p, i, q, j), Reveal(p, i), and Test(p, i)
- Advantage of adversary attacking protocol P

$$\mathsf{Adv}_{\mathcal{A}}^{P} = 2\,\mathbf{Pr}\left[S_{\mathcal{A}}^{P}\right] - 1\ ,$$

  where $S_{\mathcal{A}}^{P}$ is event that adversary distinguishes session key from random.
- Bounded by small t (on-line) and large s (off-line) security parameter.

φKE: unidirectional $A + P$ channel

if client
  then $p \stackrel{R}{\leftarrow} \{0, \ldots, 2^t - 1\}$
    send p **on** pc
  else receive p **from** pc
$k :=$ EKE(p)

Analysis

- Authentic channel $\Rightarrow$ correct pairing.
- Private channel $\Rightarrow$ passwords independent.
- Hence at least as secure as underlying EKE protocol.
- But note that password is fresh for each EKE run.

φKE: bidirectional P channel

University of Nijmegen

$p \xleftarrow{R} \{0, \ldots, 2^t - 1\}$
send p **on** pc
receive q **from** pc
$r := p \oplus q$
$k := \mathsf{EKE}(r)$

Analysis

- Two private passwords combined $\Rightarrow$ correct pairing.
- Private channel $\Rightarrow$ passwords independent.

φKE: bidirectional A channel (1)

Four phases: commit, authenticate, exchange and validate.

Independent hashfunctions $h_1 \ldots h_5$.

Alice (client)		**Bob (server)**
Commit		
pick random x		pick random y
	$h_1(g^x)$ $\Longrightarrow$	receive α_B
receive α_A	$\Longleftarrow$ $h_1(g^y)$	
Authenticate		
	$h_2(g^x)$ $\longrightarrow$	receive β_B
receive β_A	$\longleftarrow$ $h_2(g^y)$	

φKE: bidirectional A channel (2)

Key exchange

$$\xrightarrow{g^x} \quad \text{receive } v \text{ if } h_1(v) = \alpha_B \text{ and } h_2(v) = \beta_B$$

$$\text{receive } u \text{ if } h_1(u) = \alpha_A \text{ and } h_2(u) = \beta_A \quad \xleftarrow{g^y}$$

Key validation

$$\xrightarrow{h_4(u^x)} \quad \text{receive } m$$

verify $m = h_4(v^y)$

$$\text{receive } m' \quad \xleftarrow{h_5(v^y)}$$

verify $m = h_5(u^x)$

$k := h_3(u^x)$ $\qquad$ $k := h_3(v^y)$

φKE: bidirectional A channel (1)

Commit

pick random x

broadcast $h_1(g^x)$ **on** bc

receive α **from** bc

Authenticate

send $h_2(g^x)$ **on** ac

receive β **from** ac

Key exchange

broadcast g^x **on** bc

receive m **from** bc

if $h_1(m) = \alpha$ and $h_2(m) = \beta$

then $u := m$

else abort

φKE: bidirectional A channel (2)

Key validation

$$j := \begin{cases} 0 & \text{if client} \\ 1 & \text{if server} \end{cases}$$

broadcast $h_{4+j}(u^x)$ **on** bc

receive m **from** bc

if $h_{5-j}(u^x) = m$

then $k = h_3(u^x)$

else abort

φKE: Analysis

Using the DDH assumption and the random oracle model [Boney '98]:

Proposition 0.1 *Let the order of G be at least 2^{2s}, and let $h_3 : G \mapsto \{0,1\}^s$ be a pairwise independent hash function. Then the advantage of any adversary distinguishing $h_3(g^{ab})$ from a random element of $\{0,1\}^s$, when given g^a, g^b is a most $O(2^{-s})$.*

Theorem 0.2 *The advantage of an adversary attacking the protocol using at most q_{send} send queries is at most*

$$O(1 - e^{-q_{send}/2^t}) + O(2^{-s}) \; .$$

Using

$$1 - (1 - 2^{-\eta})^{q_{\text{send}}} \approx 1 - e^{-2^{-\eta} q_{\text{send}}}$$

Implementing the low bandwidth channel

- Establishing physical contact.
- Using physical link properties.
  - *Aiming.*
- Using fixed visible identities.
- Using small displays.

Concluding remarks

- Future research:
  - *Unidirectional channels*
  - *Anonymous broadcast networks*
  - *Weaker assumptions*