Real-world (Cyber)Security with Kaisa Nyberg

A Personal Perspective

N. Asokan

https://asokan.org/asokan/

@nasokan

Aalto University

UNIVERSITY OF WATERLOO

Kaisa Nyberg Fest

Half a day cryptology seminar in the honor of Prof. emerita Kaisa Nyberg's work. T
Friday, **27 October** at 13:00-17:00 in Lumituuli, Dipoli, please register

Prof. emerita Kaisa Nyberg is a distinguished scholar renowned for her significant contributions to the field of cryptography. With a career spanning several decades across academia, industry, and military, Nyberg has made groundbreaking advancements in the development of cryptanalysis and cryptographic protocols. She is most notably recognized for her pioneering work in linear and differential cryptanalysis, which are nowadays fundamental concepts in provable security and the design of cryptographic algorithms. Nyberg's expertise and dedication have had a lasting impact on the world of cryptography, a testament to her prominence in the field.

Outline

- Reminiscences: collaborating on real-world protocols (that use cryptography)
  - Channel binding in protocol composition
  - Secure device pairing

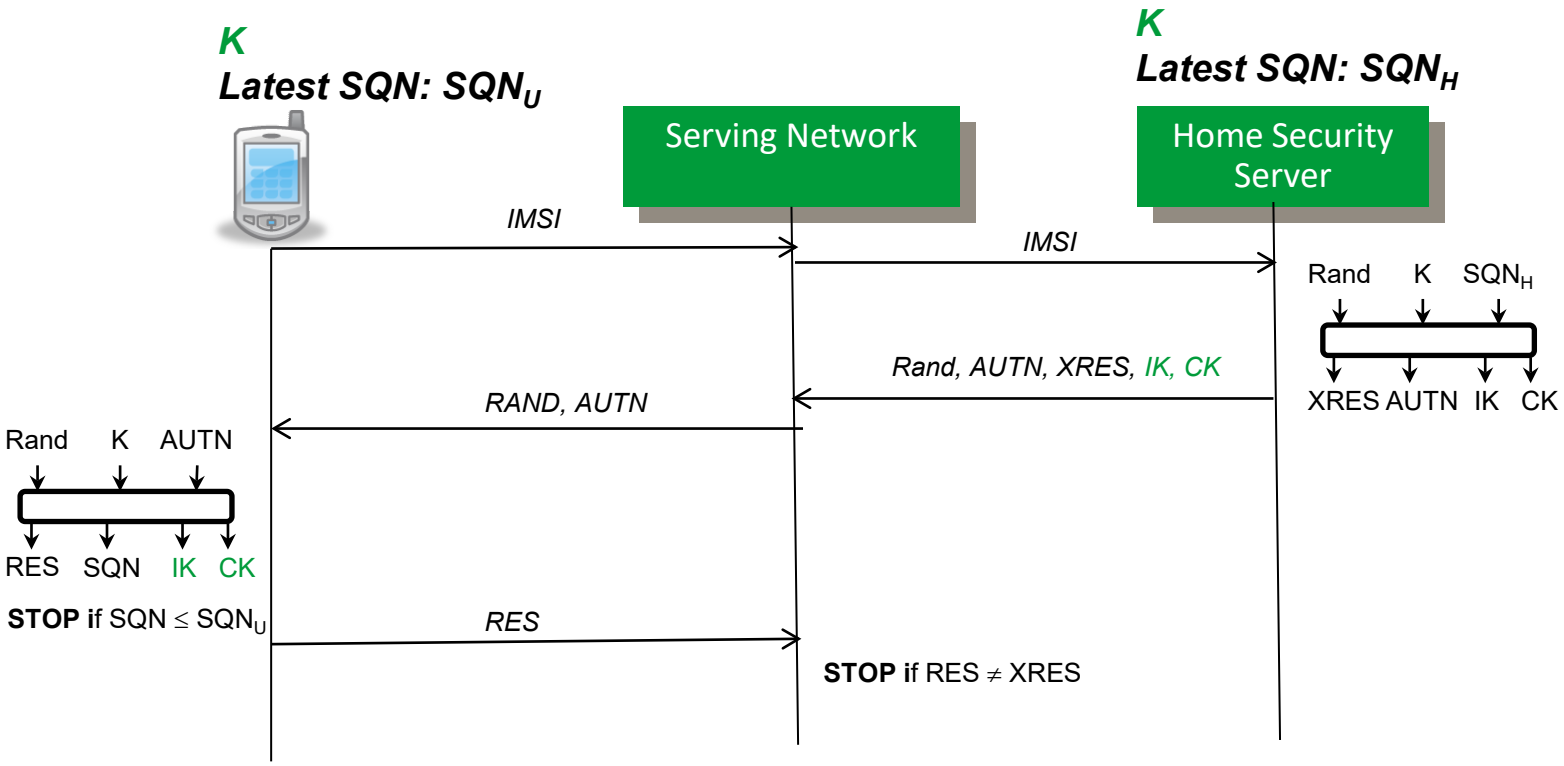
  (including lessons learned)
- More personal reminiscences about working with Kaisa

Channel Binding in protocol composition

Composing two secure authentication protocols carelessly can lead to a man-in-the-middle vulnerability

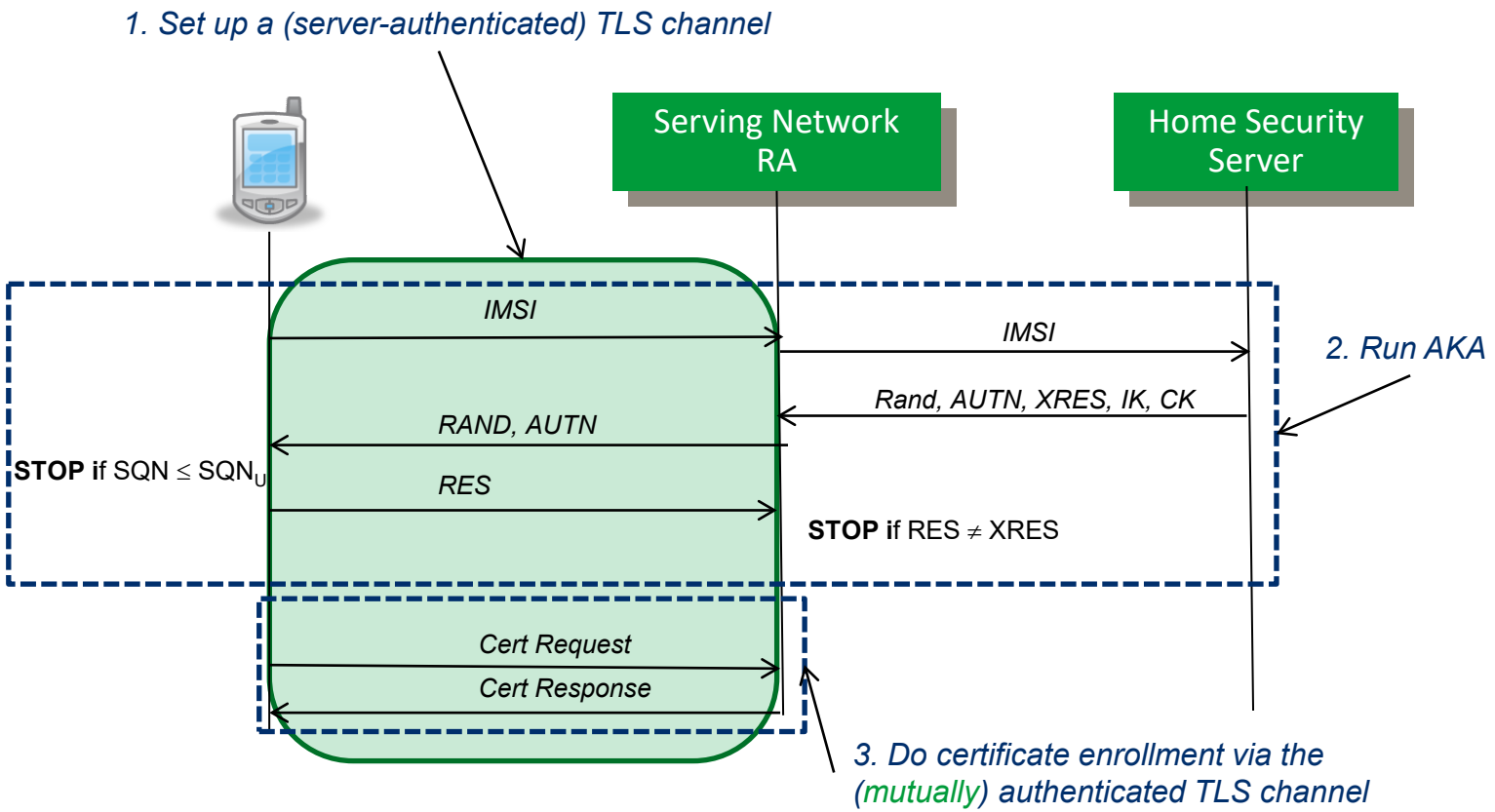
- Protocol composition can ease deployment
- Examples:
  - Server authentication using TLS + user authentication with password
  - Authentication for VPN access using legacy authentication protocol
  - Bootstrapping a “local PKI”

3G AKA

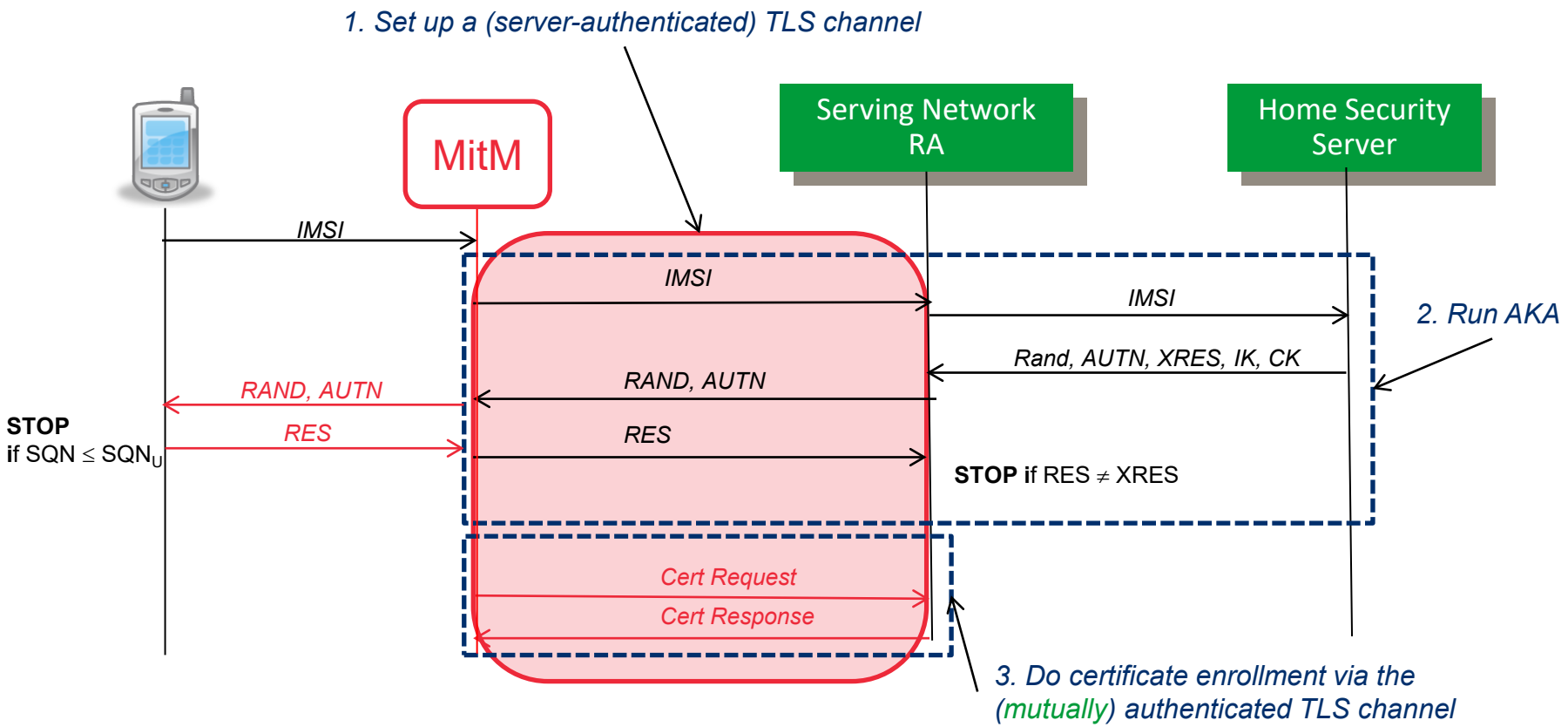


Provides mutual authentication

Bootstrapping certificate enrollment



Bootstrapping certificate enrollment



Channel binding: Use of **cryptographic binding** to compose two authenticated channels

[ANN03] "Man-in-the-middle in Tunnelled Authentication Protocols", Security Protocols, 2003

Channel binding: the aftermath

- Fiery reception at Security Protocols workshop!
  - "But you are using the worst rackets in industry as a justification for what you're doing. There are all sorts of people just generating garbage protocols, a couple of which you have already mentioned here. We're trying to reverse their work, whereas you're trying to advocate we use all these garbage protocols."
  - For an entertaining read, see transcript of discussion during my talk at SPW '03!
- Impact in IETF
  - Closing down of *ipsra* working group; channel binding in IKEv2
  - Continued attention: e.g., RFC 6813

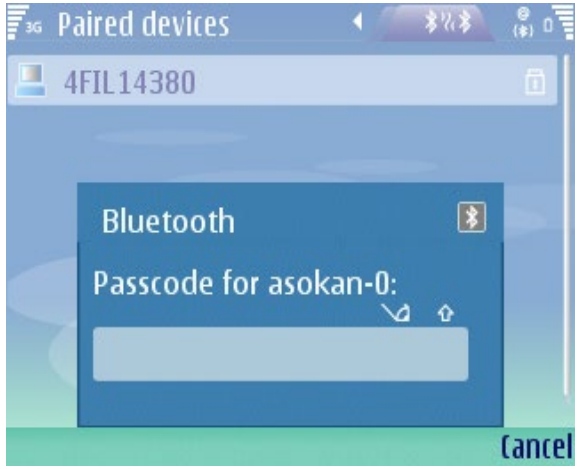
Channel Binding: lessons learned

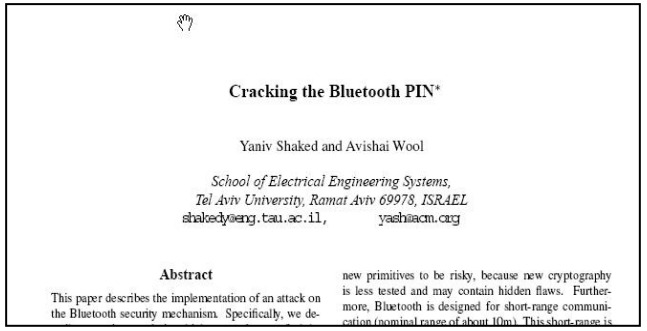
- Negative results are useful for security practitioners
- Standardization can make a good idea see light of day
- (Tech transfer) Impact $\not\rightarrow$ Capturing researcher interest

Secure Device Pairing

How can the process of pairing two devices be made easy to use without compromising security or adding to cost?

Secure Device Pairing: ca. 2005





Cracking the Bluetooth PIN*

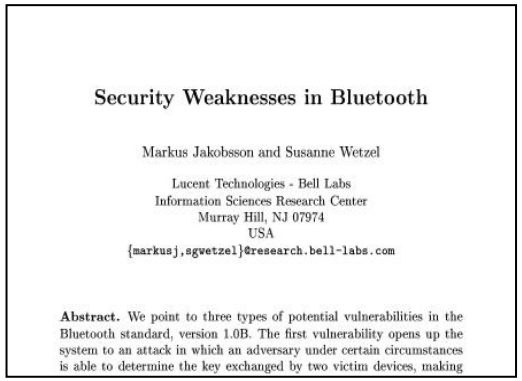
Yaniv Shaked and Avishai Wool

School of Electrical Engineering Systems,
Tel Aviv University, Ramat Aviv 69978, ISRAEL
shakedy@eng.tau.ac.il, yash@acm.org

Abstract

This paper describes the implementation of an attack on the Bluetooth security mechanism. Specifically, we de-

new primitives to be risky, because new cryptography is less tested and may contain hidden flaws. Furthermore, Bluetooth is designed for short-range communication (nominal range of about 10m). This short-range is



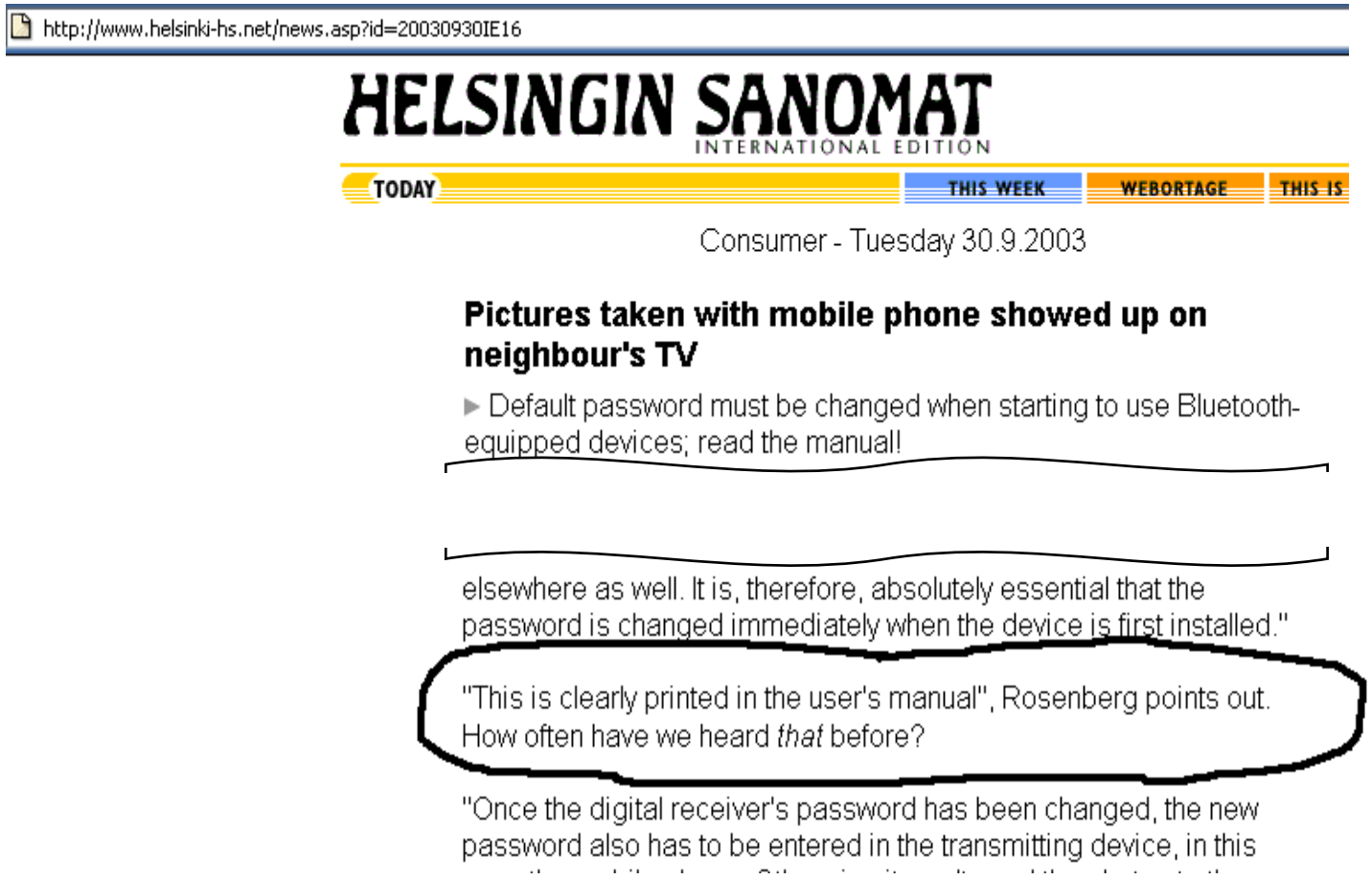
Security Weaknesses in Bluetooth

Markus Jakobsson and Susanne Wetzel

Lucent Technologies - Bell Labs
Information Sciences Research Center
Murray Hill, NJ 07974
USA
{markusj,sgwetzel}@research.bell-labs.com

Abstract. We point to three types of potential vulnerabilities in the Bluetooth standard, version 1.0B. The first vulnerability opens up the system to an attack in which an adversary under certain circumstances is able to determine the key exchanged by two victim devices, making

Naïve usability measures damage security



http://www.helsinki-hs.net/news.asp?id=20030930IE16

HELSINGIN SANOMAT
INTERNATIONAL EDITION

TODAY | THIS WEEK | WEBORTAGE | THIS IS

Consumer - Tuesday 30.9.2003

Pictures taken with mobile phone showed up on neighbour's TV

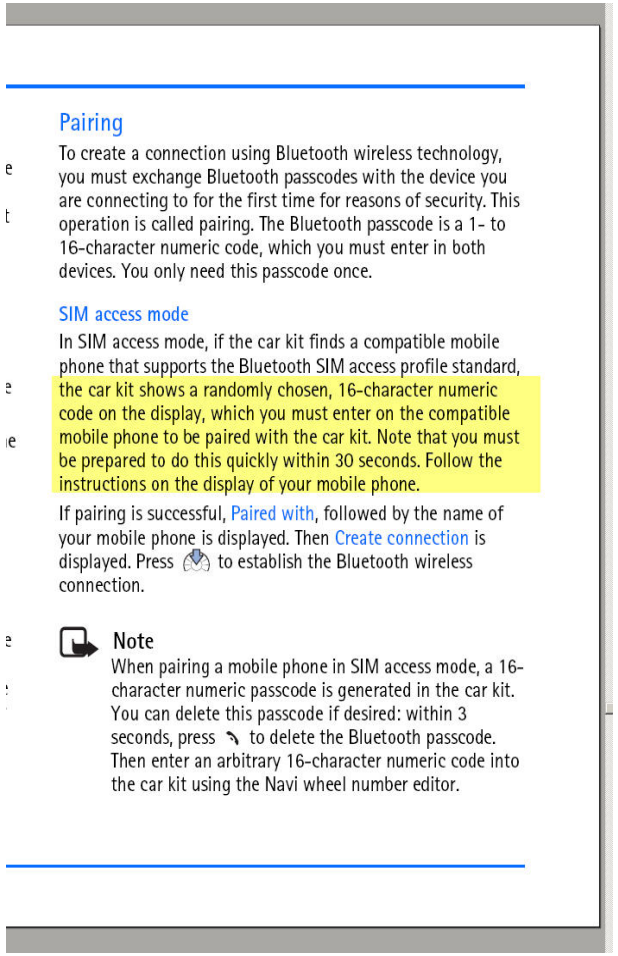
▶ Default password must be changed when starting to use Bluetooth-equipped devices; read the manual!

elsewhere as well. It is, therefore, absolutely essential that the password is changed immediately when the device is first installed."

"This is clearly printed in the user's manual", Rosenberg points out. How often have we heard *that* before?

"Once the digital receiver's password has been changed, the new password also has to be entered in the transmitting device, in this

Naïve security erodes usability



Pairing

To create a connection using Bluetooth wireless technology, you must exchange Bluetooth passcodes with the device you are connecting to for the first time for reasons of security. This operation is called pairing. The Bluetooth passcode is a 1- to 16-character numeric code, which you must enter in both devices. You only need this passcode once.

SIM access mode

In SIM access mode, if the car kit finds a compatible mobile phone that supports the Bluetooth SIM access profile standard, the car kit shows a randomly chosen, 16-character numeric code on the display, which you must enter on the compatible mobile phone to be paired with the car kit. Note that you must be prepared to do this quickly within 30 seconds. Follow the instructions on the display of your mobile phone.

If pairing is successful, Paired with, followed by the name of your mobile phone is displayed. Then Create connection is displayed. Press to establish the Bluetooth wireless connection.

Note

When pairing a mobile phone in SIM access mode, a 16-character numeric passcode is generated in the car kit. You can delete this passcode if desired: within 3 seconds, press to delete the Bluetooth passcode. Then enter an arbitrary 16-character numeric code into the car kit using the Navi wheel number editor.

Car kits

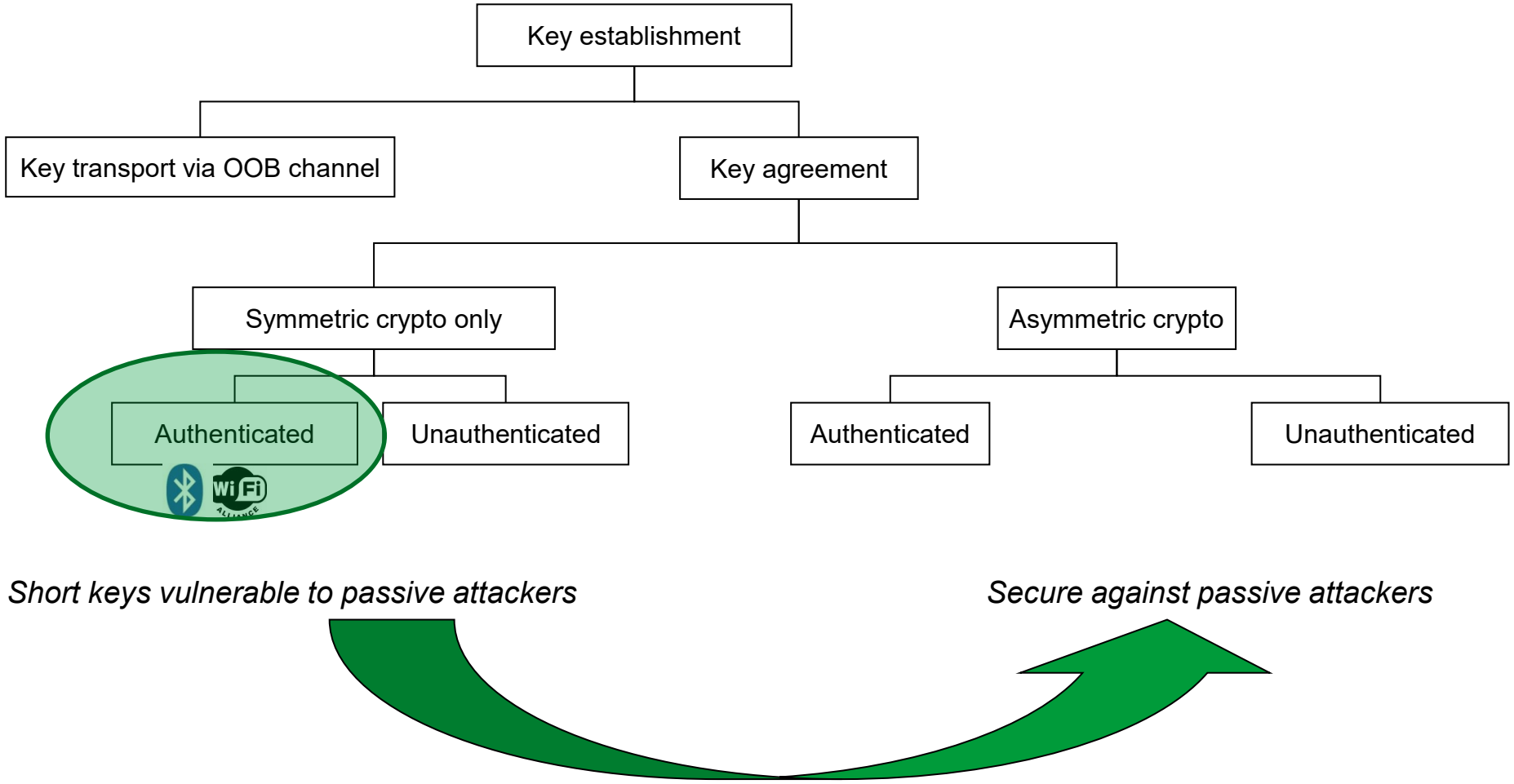
- Allow hands-free phone usage in cars
- Retrieve/use session keys from phone SIM
- require higher level of security

➢ users must enter 16-character passcodes

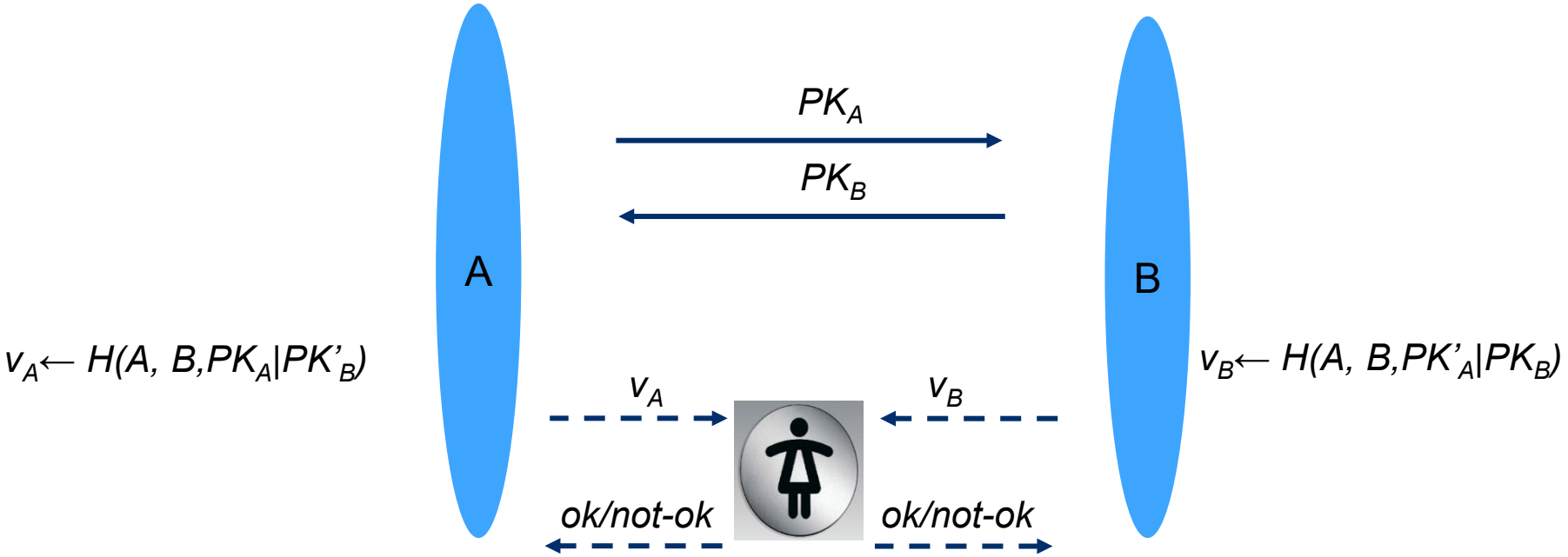
More secure = Harder to use?

Cost:
Calls to Customer Support

Key establishment for secure pairing ~2005



Authentication by comparing short strings

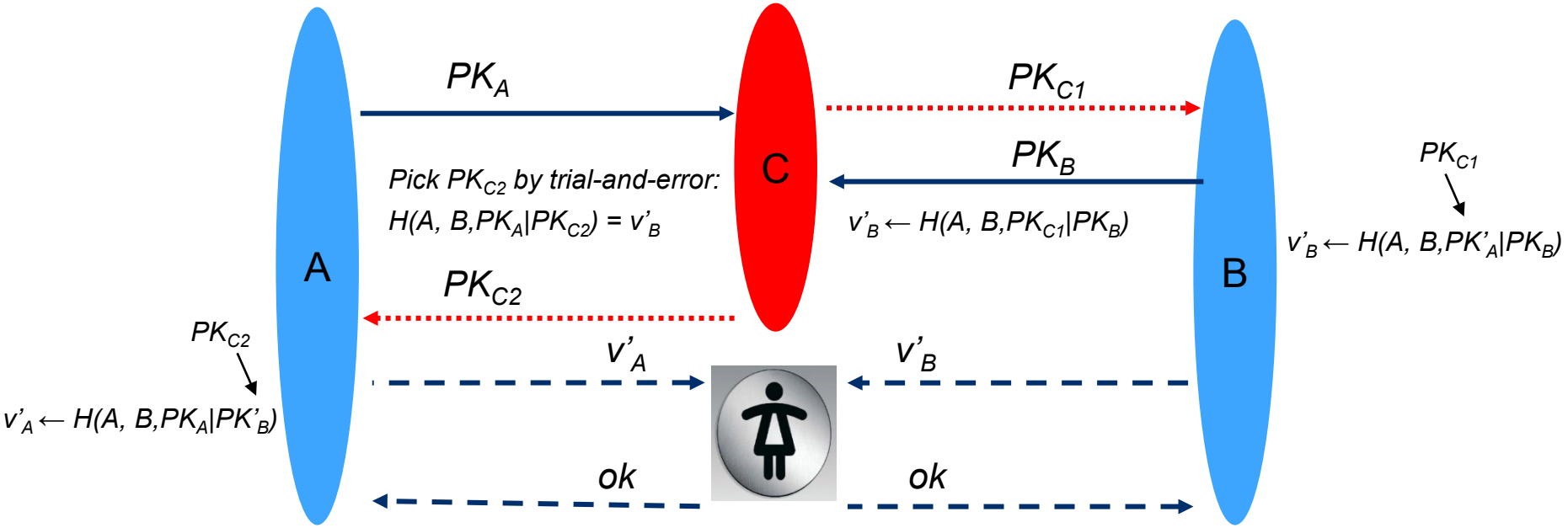


v_A and v_B are short strings (e.g., 4 digits),

User approves acceptance if v_A and v_B match

A man-in-the-middle can easily defeat this protocol

MitM in comparing short strings



Guess a value SK_{C2}/PK_{C2} until $H(A, B, PK_A|PK_{C2}) = v'_B$

If v'_B is n digits, attacker needs at most 10^n guesses; Each guess costs one hash calculation

A typical modern PC can calculate 100000 MACs in 1 second

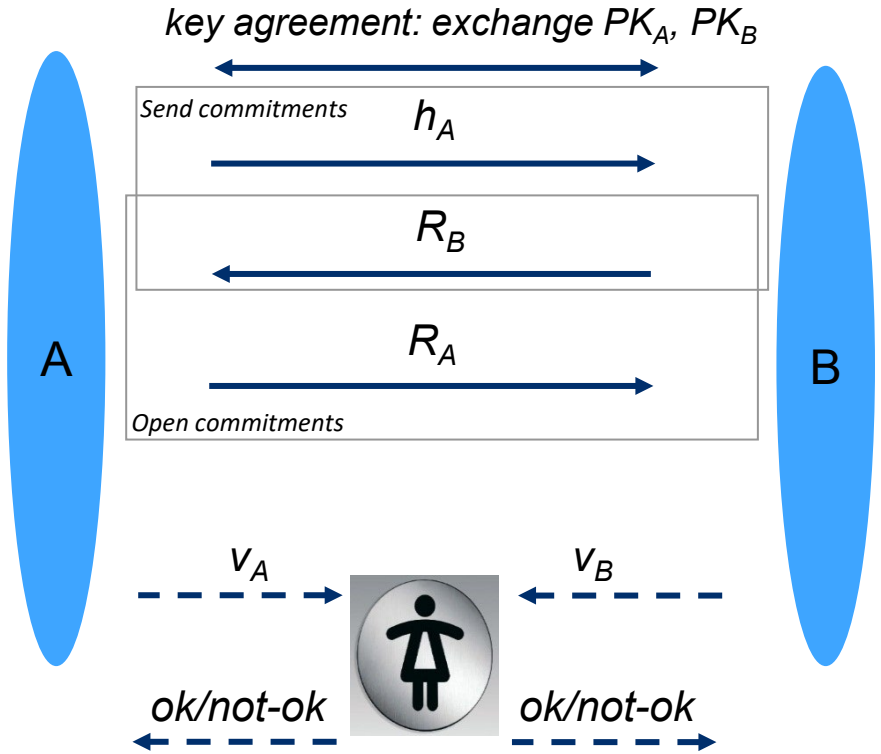
Authentication by comparing short strings

Choose long random R_A

Calculate commitment

$h_A \leftarrow h(A, R_A)$

$v_A \leftarrow H(A,B,PK_A|PK'_B,R_A,R'_B)$



Choose long random R_B

Verify commitment

$h'_A \stackrel{?}{=} h(A, R'_A)$

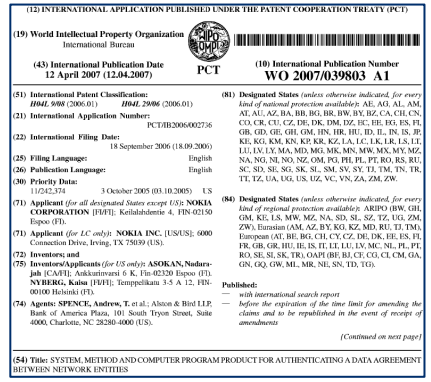
Abort on mismatch

$v_B \leftarrow H(A,B,PK'_A|PK_B,R'_A,R_B)$

User approves acceptance if v_A and v_B match

2^{-l} (“unconditional”) security against man-in-the-middle (l is the length of v_A and v_B)

h() is a hiding commitment; in practice SHA-256


(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

PCT

(43) International Publication Date
12 April 2007 (12.04.2007)

(10) International Publication Number
WO 2007/039803 A1

(54) Title: SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR AUTHENTICATING A DATA AGREEMENT BETWEEN NETWORK ENTITIES

[LAN05] MANA IV, IACR report; [LN06] CANS ‘06

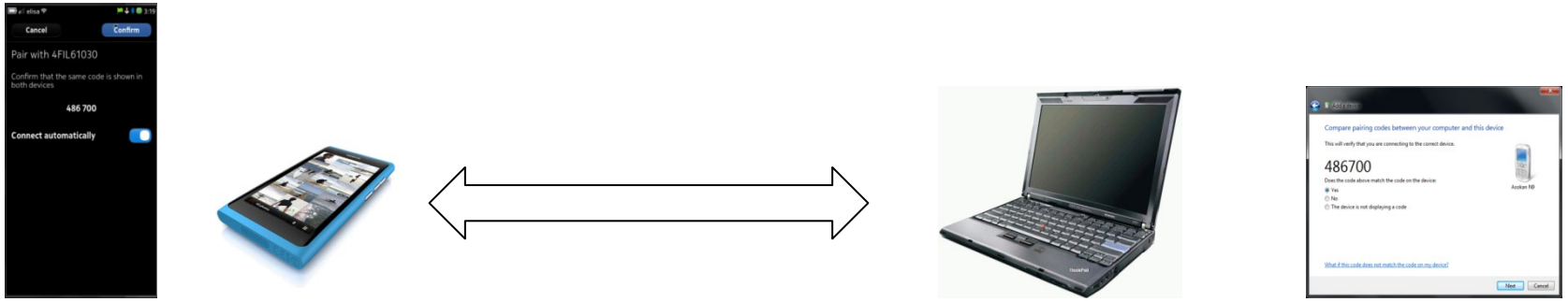
Key establishment for secure pairing ~2008

	Unauthenticated Diffie-Hellman	Authenticated Diffie-Hellman		
		short-string comparison	short PIN	Out-of-band channel
WiFi Protected Setup	“Push-button”		√	NFC
Bluetooth 2.1	“Just-works”	√	√	NFC
Wireless USB		√		USB Cable

[AN10] “Security associations for wireless devices” (Overview, book chapter)
[SVA09] “Standards for security associations in personal networks: a comparative analysis” IJSN 4(1/2):87-100 (survey of standards)

Secure Pairing: the aftermath

- Widely deployed (Bluetooth SSP, WiFi Protected Setup)
- Improving usability/security → fundamental protocol changes



[UKA07] "Usability Analysis of Secure Pairing Methods", USEC '07
[SEKA06] "Secure device pairing based on a visual channel", IEEE S&P '06

Secure Device Pairing: lessons learned

- Address pain points - builds credibility with stakeholders
- Don’t just guess security requirements; Ask stakeholders
- Desiderata for deployment and research can be different
- Standardization can make a good idea see light of day

Lessons Learned

- How to choose the “right” problems?
  - Don’t just guess security requirements; Ask stakeholders
  - Desiderata for deployment and research can be different
- How to identify “good” results?
  - Negative results are useful for security practitioners
  - (Tech transfer) Impact $\not\rightarrow$ Capturing researcher interest
- How to find paths to deployment?
  - Address pain points - builds credibility with stakeholders
  - Standardization can make a good idea see light of day

Personal reminiscences

Role model …

… in many dimensions!

Cryptography

https://toc.csail.mit.edu/cis

Applications

https://www.gizbot.com/mobile/news/nokia-6-nokia-5-nokia-3-nokia-3310-price-details-out-before-june-release-date-040591.html

Standardization

https://www.codepaltoolkit.com/2019/04/15/dealing-with-difficult-people/