Real-world (Cyber)Security with Kaisa Nyberg
A Personal Perspective

N. Asokan

https://asokan.org/asokan/
@nasokan
Kaisa Nyberg Fest

Half a day cryptology seminar in the honor of Prof. emerita Kaisa Nyberg’s work.
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

1. Set up a (server-authenticated) TLS channel
2. Run AKA
3. Do certificate enrollment via the (mutually) authenticated TLS channel
Bootsrapping certificate enrollment

1. Set up a (server-authenticated) TLS channel

2. Run AKA

3. Do certificate enrollment via the (mutually) authenticated TLS channel

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

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 $\mapsto$ 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
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

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

Key establishment

Key transport via OOB channel

Key agreement

Symmetric crypto only
- Authenticated
- Unauthenticated

Asymmetric crypto
- Authenticated
- Unauthenticated

Short keys vulnerable to passive attackers

Secure against passive attackers
Authentication by comparing short strings

A man-in-the-middle can easily defeat this protocol.
MitM in comparing short strings

**Diagram Description:**
- **A** and **B** are communicating parties.
- **C** is the MitM attacker.
- **PK_A** and **PK_B** are keys known to **A** and **B**.
- **PK_C1** and **PK_C2** are keys known to **C**.
- **v'_A** and **v'_B** are the expected outputs for **A** and **B**.

**Process:**
1. **A** computes **v'_A** using **PK_A** and **PK_C2**.
2. **C** intercepts the message and computes **v'_B** using **PK_C1**.
3. **B** computes **v'_B** using **PK_B**.
4. **C** compares **v'_A** and **v'_B**.
5. If **v'_A** and **v'_B** match, **C** forwards the message to **B**.
6. **B** verifies the message.

**Key Points:**
- **v'_A** = \( H(A, B, PK_A|PK_C2) \)
- **v'_B** = \( H(A, B, PK_C1|PK_B) \)
- 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

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

[LAN05] MANA IV, IACR report; [LN06] CANS ‘06
# Key establishment for secure pairing ~2008

<table>
<thead>
<tr>
<th>Unauthenticated Diffie-Hellman</th>
<th>Authenticated Diffie-Hellman</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>short-string comparison</td>
</tr>
<tr>
<td>WiFi Protected Setup</td>
<td>“Push-button”</td>
</tr>
<tr>
<td>Bluetooth 2.1</td>
<td>“Just-works”</td>
</tr>
<tr>
<td>Wireless USB</td>
<td></td>
</tr>
</tbody>
</table>

[AN10] “Security associations for wireless devices” (Overview, book chapter)
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 → 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!

Standardization

Applications

Cryptography