

# Connect Now to MitM

Kaisa Nyberg

Helsinki University of Technology

Nokia Research Center

Finland

Crypto 06 Rump Session 22 August 2006

# Microsoft Windows Rally

- Allows easy and secure setup of networks of devices particularly for home users
- Windows Vista Connect Now-NET implements a snapshot of

**Simple Config** by WiFi Alliance

(work still in progress)

- Allows different configuration technologies, one method is

**Diffie-Hellman Key Agreement**

authenticated by a device password entered by the user and

**Device Password Proof-of-Possession (DPwPoP)**

protocol by Simple Config

- For more information, see

<http://www.microsoft.com/whdc/rally/>

# DPwPoP Protocol

Enrollee → Registrar:

$M1 = \text{Version} \parallel N1 \parallel \text{Description} \parallel \text{PKE}$

Enrollee ← Registrar:

$M2 = \text{Version} \parallel N1 \parallel N2 \parallel \text{Description} \parallel \text{PKR} \parallel \text{HMACAuthKey}(M1 \parallel M2^*)$

Enrollee → Registrar:

$M3 = \text{Version} \parallel N2 \parallel \text{E-Hash1} \parallel \text{E-Hash2} \parallel \text{HMACAuthKey}(M2 \parallel M3^*)$

Enrollee ← Registrar:

$M4 = \text{Version} \parallel N1 \parallel \text{R-Hash1} \parallel \text{R-Hash2} \parallel \text{ENCKeyWrapKey}(\text{R-S1}) \parallel \text{HMACAuthKey}(M3 \parallel M4^*)$

Enrollee → Registrar:

$M5 = \text{Version} \parallel N2 \parallel \text{ENCKeyWrapKey}(\text{E-S1}) \parallel \text{HMACAuthKey}(M4 \parallel M5^*)$

Enrollee ← Registrar:

$M6 = \text{Version} \parallel N1 \parallel \text{ENCKeyWrapKey}(\text{R-S2}) \parallel \text{HMACAuthKey}(M5 \parallel M6^*)$

Enrollee → Registrar:

$M7 = \text{Version} \parallel N2 \parallel \text{ENCKeyWrapKey}(\text{E-S2}) \parallel \text{HMACAuthKey}(M6 \parallel M7^*)$

Enrollee ← Registrar:

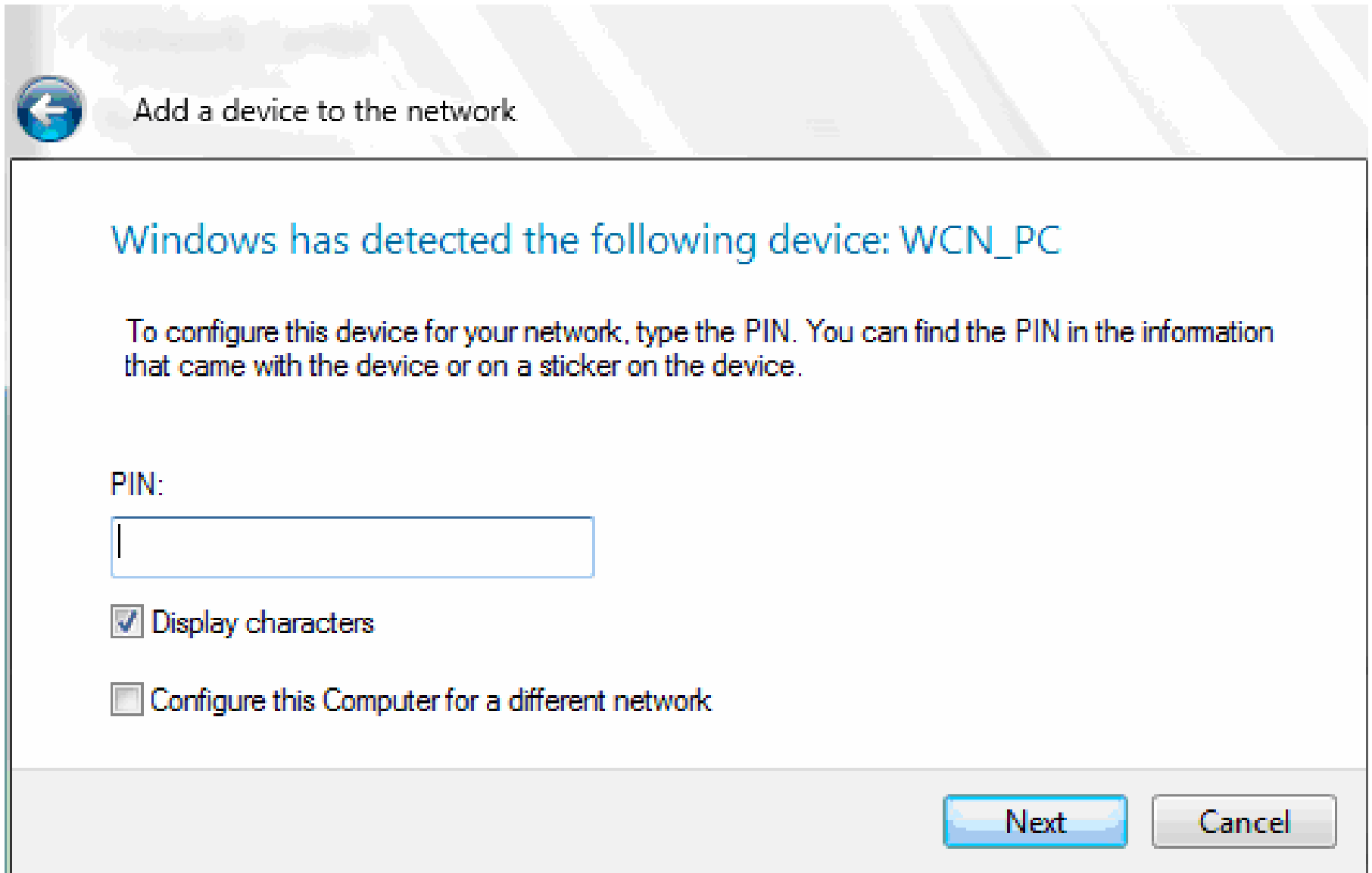
$M8 = \text{Version} \parallel N1 \parallel \text{HMACAuthKey}(M7 \parallel M8^*)$

# DPwPoP Protocol

- Simple protocol using commitments with interleaving opening
- Commitments are hiding, but not for short data that can be searched exhaustively (offline dictionary attack)
- Security against MitM achieved ONLY IF fresh random passkey used for each execution of the protocol.

BUT this does not always seem to be the case in Windows Rally... a recommended option is to use static password.

# Find 8-digit Password on Sticker



The image shows a Windows Network Setup dialog box. At the top left, there is a blue circular button with a white left-pointing arrow. To its right, the text "Add a device to the network" is displayed. The main content area has a light blue header that reads "Windows has detected the following device: WCN\_PC". Below this, a paragraph of text explains that the user should enter a PIN found on the device or its sticker. A text input field labeled "PIN:" is provided, with a single vertical cursor line at the beginning. Below the input field are two checkboxes: the first is checked and labeled "Display characters", and the second is unchecked and labeled "Configure this Computer for a different network". At the bottom right, there are two buttons: a blue "Next" button and a grey "Cancel" button.

← Add a device to the network

Windows has detected the following device: WCN\_PC

To configure this device for your network, type the PIN. You can find the PIN in the information that came with the device or on a sticker on the device.

PIN:

Display characters

Configure this Computer for a different network

Next Cancel

# DPwPoP Protocol & MitM (1)

## 1<sup>st</sup> Attempt:

Enrollee → MitM → Registrar:

$M1 = \text{Version} \parallel N1 \parallel \text{Description} \parallel \text{PKE}$

Enrollee ← MitM ← Registrar (†) :

$M2 = \text{Version} \parallel N1 \parallel N2 \parallel \text{Description} \parallel \text{PKR} \parallel \text{HMACAuthKey}(M1 \parallel M2^*)$

Enrollee → MitM → Registrar (†) :

$M3 = \text{Version} \parallel N2 \parallel \text{E-Hash1} \parallel \text{E-Hash2} \parallel \text{HMACAuthKey}(M2 \parallel M3^*)$

Enrollee ← MitM ← Registrar (†) :

$M4 = \text{Version} \parallel N1 \parallel \text{R-Hash1} \parallel \text{R-Hash2} \parallel \text{ENCKeyWrapKey}(\text{R-S1}) \parallel \text{HMACAuthKey}(M3 \parallel M4^*)$

Enrollee → Mitm → Registrar:

$M5 = \text{Version} \parallel N2 \parallel \text{ENCKeyWrapKey}(\text{E-S1}) \parallel \text{HMACAuthKey}(M4 \parallel M5^*)$

*Verification fails at the Registrar (with high probability)*

**Execution of the protocol is aborted.**

**MitM learns the first 4 digits of the password.**

(†) MitM uses different AuthKeys and KeWrapKeys with Enrollee and Registrar

# DPwPoP Protocol & MitM (2)

## 2<sup>nd</sup> Attempt:

Enrollee → MitM → Registrar:

$M1 = \text{Version} \parallel N1 \parallel \text{Description} \parallel \text{PKE}$

Enrollee ← MitM ← Registrar (†) :

$M2 = \text{Version} \parallel N1 \parallel N2 \parallel \text{Description} \parallel \text{PKR} \parallel \text{HMACAuthKey}(M1 \parallel M2^*)$

Enrollee → MitM → Registrar (†) :

$M3 = \text{Version} \parallel N2 \parallel \text{E-Hash1} \parallel \text{E-Hash2} \parallel \text{HMACAuthKey}(M2 \parallel M3^*)$

Enrollee ← MitM ← Registrar (†) :

$M4 = \text{Version} \parallel N1 \parallel \text{R-Hash1} \parallel \text{R-Hash2} \parallel \text{ENCKeyWrapKey}(\text{R-S1}) \parallel \text{HMACAuthKey}(M3 \parallel M4^*)$

Enrollee → MitM → Registrar (†) :

$M5 = \text{Version} \parallel N2 \parallel \text{ENCKeyWrapKey}(\text{E-S1}) \parallel \text{HMACAuthKey}(M4 \parallel M5^*)$

Enrollee ← MitM ← Registrar:

$M6 = \text{Version} \parallel N1 \parallel \text{ENCKeyWrapKey}(\text{R-S2}) \parallel \text{HMACAuthKey}(M5 \parallel M6^*)$

*Verification fails at the Enrollee (with high probability)*

**Execution of the protocol is aborted.**

**MitM learns the second 4 digits of the password.**

# DPwPoP Protocol & MitM (3)

**Third attempt:**

M1 ... M2 ... M3 ... M4... M5... M6 ... M7 ... M8 ...

**Third time lucky!**

**User finally succeeds connecting the devices ... to the Man-in-the-Middle!**