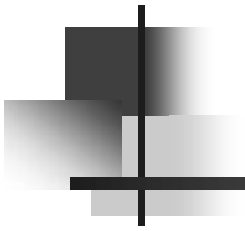

Inside Windows Product Activation

Fully Licensed GmbH
Berlin, Germany
July 2001
http://www.licenturion.com/xp/fully-licensed-wpa.txt
(Available as web manuscript August 2004)

Presented by Paul Mason

Article Summary

- Article about Windows Product Activation (WPA)
- Provides an in-depth description about the information Windows XP uses to activate it's product.
- Article based on ethical implications of WPA
  - "We strongly believe that every software vendor has the right to enforce the licensing terms governing the use of a piece of licensed software…"
  - "… each individual has the right to detailed knowledge about the full implications of the employed means and possible limitations imposed by it… "
- Article is thus written with these two statements in mind answering the questions:
  - "Exactly what information is transmitted during activation?"
  - "How do hardware modifications affect an already activated installation of Windows XP?"

Appreciative Comment

- Very precise well written article
  - Claims to be “a little vague at some points” however was still full of knowledge
- Accurately explained how to decode a Windows XP installation ID
  - The information that is sent for product activation
  - Provided verification of algorithms with tools and its corresponding source code
  - This article is slightly outdated due to SP1+ changing the Installation ID

Critical Comment

- Conclusion states that WPA "respects the user's right to privacy."
- Appears to have an ethical bias towards the developers rather than towards the users
- Direct mapping to Pfleeger's Universal Rules of Ethics
  - Right to Privacy vs Right to Knowledge
- How so?

Explanation

- When activating Windows XP msoobe.exe generates an Installation ID which it sends to Microsoft.
- Microsoft decodes this Installation ID and if successful returns a “Confirmation ID”.
- If the Confirmation ID is valid then the product will activate itself.

- The Installation ID is generated based on the activating PC’s hardware and product activation key.
- The article described in detail how to DECODE the Installation ID and find out what was sent.
  - This is where the Privacy vs Knowledge issue comes in to play….

The Installation ID

- The Installation ID is a string consisting of 50 decimal numbers in 6 digit groups
  - 002666-077894-484890-114573-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XX
- The rightmost digit in each group is a check digit to ensure that the numbers were entered (telephone method) or generated correctly
- Stripping the check digits leaves a 41 digit decimal number which corresponds to a 136-bit binary number (little endian format)
- The first 16 bytes are encrypted, the 17th byte is plaintext
- These 16 bytes are decrypted using a four-round Feistal cipher which leaves us with 16 bytes of plaintext and an unencrypted 17th byte.
  - Won't delve into how this is done here
- This corresponds to the following table:

Name	Size
H1	Double word
H2	Double word
P1	Double word
P2	Double word
P3	byte

- P1, P2 & P3 is the Product ID
  - Developer has right to know activating product…
    - Is this a biased opinion?
- H1 & H2 is the system's hardware configuration
  - Does the developer have a right to know this?

The Issue with the Hardware Information

- This contains information based on the hardware ID string of the: CDROM drive, graphics adapter, hard drive, SCSI host adapter, and IDE controller
- Contains information on the serial number string of the system volume and CPU (if present), the network MAC address string, the processor model string
- Also some more information on the value of the RAM size and whether the system is dockable or not (more leniency for hardware changes)
- The Hardware ID strings in the Installation ID are hashed to save space using:
  - Hash = (MD5(IDString) % MaxBitFieldLength) + 1
- Hashing may dissolve this "Unique ID" into a "hardware group"
  - Microsoft knows what hardware you have but does NOT know the exact brand. However, they may have an idea…. (e.g. popular hardware)
- This cut down information is sent to Microsoft in the Installation ID and it's full information is stored in a "snapshot" file "wpa.dbl" which stores the original and current snapshot of the hardware configuration (for reactivating on hardware change).
- The conclusion again: Windows Product Activation "respects the user's right to privacy."
  - Is this information necessary to be SENT to Microsoft? Perhaps in the sense of catching out people who pirate Windows. Even so, is this a naïve comment?

Summary

- The main reason for this paper being published was a reason of Ethics
  - Information "that Microsoft should have published long ago"
  - Justifies Microsoft's use of WPA
- Fits perfectly into an argument for Pfleeger's Universal Rules of Ethics
- Which leads me to my questions…

Questions

- Do you think that Microsoft is respecting the user's right to privacy & knowledge?
  - Taking into account that this article wasn't released by Microsoft
- Are we respecting Microsoft's right to privacy & knowledge?
  - Probably only going to use the collected information for catching piracy – not for misuse