Windows Genuine Advantage Registry Information

David Futcher

October 15, 2007

http://bobocanfly.wordpress.com
bobbocanfly@gmail.com

Document Version 1.0

1 Introduction

1.1 Abstract

This paper contains information about the data the Windows Genuine Advantage (WGA) application stores in the Windows Registry. it will also look at the possible uses of this data and whether the Windows Genuine Advantage program should be storing this data.

1.2 Testing

The results contained within this paper were gathered from the two Windows computers in my house:

Computer 1 (Desktop):

```
Manufacturer: Packard Bell
Processor: Intel Core 2 Duo
Graphics: NVidia GeForce
RAM: 1gb
```

Computer 2 (Laptop):

```
Manufacturer: Unknown
Processor: Intel Pentium 4
Graphics: Intel Onboard
RAM: 256mb (Stock), 512mb (Home Addition)
```

All registry information was gathered using 'regedit'.

1.3 Disclaimer

While I tried to be as fair as possible gathering this information, it may not be totally representative of all computers running Windows Genuine Advantage and may not be totally accurate due to the small amount of information available from Microsoft. Please do not use this data for anything mission critical as it may not fully represent the data stored by Windows Genuine Advantage.

2 Registry Keys

All information in this document is gathered from registry path:

```
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows Genuine Advantage\\
```

This seems to be the main place where WGA stores its registry data. In the data this is referred to as Path One. There is a small amount of data in

```
HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows Genuine Advantage\\
```

which I will include in the report. This is referred to as Path One.

A full list of Registry Keys is available in Section 5, Appendix I: List of Registry Locations.

3 Full Findings

```
Note: The characters information desribes the total amount
of characters stored in the Registry Key. The stripped
characters information describes the actual amount of data
stored in the key, minus the separation characters like
hyphens and colons etc.

In format, the * (star) symbol refers to a random
alphanumeric character.
```

3.1 MAC

Key Name: MAC

Path: Path One

Characters: Variable (Usually 18, 36 or 54)

Stripped Characters: Variable (Ususally 12, 24 or 36)

Format: **-**-**-**-**-**;

Format Notes: This pattern is repeated for each MAC address registered with your computers Network Cards. The key for a computer with 2 MAC addresses would look like **-**-**-**-**-**;**-**-**-**-**-**;

Key Type: REG_SZ

Possible Usage: Storing your computers MAC Addresses

3.2 UGD

Key name: UGD

Path: Path One

Characters: 39

Stripped Characters: 32

Format: {********-****-****-****-************}

Format Notes: Looks very much like a CD Key

Key Type: REG_SZ

Possible Usage: Unique ID Key for installation identification

3.3 HDSLN

Key name: HDSLN

Path: Path One

Characters: 8

Stripped Characters: 8

Format: ********

Key Type: REG_SZ

Possible Usage: N/A

3.4 GSSS

Key name: GSSS

Path: Path One

Characters: 13

Stripped Characters: 11

Format: *x******** (*)

Key Type: REG_DWORD

Possible Usage: N/A

3.5 Code

Key name: code

Path: Path Two

Characters: 13

Stripped Characters: 11

Format: *x********* (*)

Key Type: REG_DWORD

Possible Usage: N/A

4 Security

4.1 MAC Address Usage

Microsoft maintains that the WGA application gathers only required data from a users computer. From the Microsoft Website (http://www.microsoft.com/genuine/downloads/FAQ.aspx?displaylang=en):

```
The validation tools do not collect your name, address, e-mail address, or any
other information that Microsoft will use to identify you or contact you. The
tools collect such information as:

    * Computer make and model
    * Version information for the operating system and software using Genuine
Advantage
    * Region and language setting
    * A unique number assigned to your computer by the tools (Globally Unique
Identifier or GUID)
    * Product ID and product key
    * BIOS name, revision number, and revision date
    * Volume serial number
    * Office product key (if validating Office)
```

This makes absolutely no mention that Microsoft in any way reads your computers MAC Addresses. Nor does storing the MAC address fall under the category of the above headings. In fact the only mentions of MAC Addresses on www.microsoft.com is users asking for help to find it.

I make no assumption that WGA is sending this information back to Microsoft, along with the data mentioned above. In fact Microsoft could be collecting this information for a truly benign reason, like generating a Unique ID. But it does seem like a fairly strange way of generating an Identification Key.

4.2 Registry Storage

All of the information above is stored within the "public" registry, where any application running on the computer can access it. By storing semi-sensitive data like MAC Addresses in the Registry, WGA is making it much easier for malicious programs like Spyware, Viruses or Tracking Trojans to gather this data. While it is not a large security breach if a computer cracker knows your MAC Address, it can make things easier for them once in a network, as it can help bypass security measures like IP Spoofing.

4.3 Circumvention

This system should not be too difficult to circumvent. All it should require is a MAC Spoofing application to run before the WGA Application is installed. In theory this should stop WGA collecting the proper information, though it could cause WGA to invalidate your Windows Installation.

5 Appendix I: List of Registry Locations

Registry locations where WGA stores data:

```
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows Genuine Advantage\\MAC
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows Genuine Advantage\\UGD
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows Genuine Advantage\\HDSLN
HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows Genuine Advantage\\GSSS
HKEY_CURRENT_USER\\SOFTWARE\\Microsoft\\Windows Genuine Advantage\\code
```