УДК 004.056.

Белов Сергей Павлович
ФГБОУ ВПО «Московский государственный университет приборостроения и информатики»
Аспирант
E-Mail: Sergey.belov@list.ru

Нестандартное использование классов и свойств Windows Management Instrumentation для привязки программного обеспечения к комплектующим автоматизированного рабочего места без использования инсталлятора

Аннотация. Проблема нелегального использования программного обеспечения всегда была актуальной, усложнившейся с появлением программ побайтного копирования данных с накопителей. При их использовании виртуальная защита, встраиваемая в систему инсталлятором программного обеспечения, теряет практический смысл. В случае дорогостоящего программного обеспечения и оборудования - для его использования встает вопрос разработки иных методов защиты, даже если это требует ручной настройки для каждого оборудования. Для этого был изучен инструментарий управления Windows, произведен системный анализ его классов и свойств, выделены необходимые для работы с комплектующими и операционной системой. В статье рассматриваются данные классы и свойства в рамках защиты программного обеспечения (в том числе и их нестандартное использование).

Ключевые слова: защита; программное обеспечение; копирование; пиратство; автоматизированное рабочее место; инсталлятор; инструментарий управления windows.

При первоначальном изучении проблемы защиты программного обеспечения (далее - «ПО») автором была разработана методика, использовавшая Windows Management Instrumentation (далее - «WMI») для привязки ПО к автоматизированному рабочему месту (далее - «АРМ») **[1]**. У методики на тот момент был ряд недостатков:

- не все классы WMI (далее - «классы») и свойства классов WMI (далее - «свойства») были проанализированы (неполнота исследования);
- методика предназначена для использования разработчиком (недоступность для рядового персонала);
- не все свойства были опробованы на практике.

В данной работе количество изученных классов и свойств составляет более 10000 (пространство имен «root\CIMV2», основное пространство параметров комплектующих АРМ), из них отобраны свойства, позволяющие установить привязку (жесткую или мягкую) к операционной системе (далее - «ОС») или комплектующим АРМ. Жесткая привязка - любое изменение комплектующей или параметра ОС приведет к определению ее как чужеродной. Мягкая привязка - определенное изменение комплектующей или параметра ОС приведет к определению ее как чужеродной (например, к модели материнской платы или общему объему оперативной памяти). Количество классов пространства имен «root\CIMV2» изменяется от АРМ к АРМ (зафиксированное количество - от 331 до 575), поэтому количество отобранных свойств составляет всего 59 единиц. Отобранные свойства обеспечивают высокую вероятность обеспечения соответствующей привязки (тестирование проводилось менее чем на 100 АРМ).

На основе отобранных свойств было написано ПО, позволяющее рядовому персоналу выбирать их и генерировать файлы электронных ключей безопасности **[2]**. Механизм проверки ключей единоразово интегрируется программистом любой квалификации в разрабатываемое ПО. Рядовой персонал любой квалификации получил возможность диагностики комплектующих оборудования и ключей, получая коды ошибок ключа и расшифровывая их по инструкции к ПО.

Далее приводится таблица, содержащая отобранные свойства, принадлежность их к классу, комплектующие, тип привязки (М/Ж), особенности, нестандартное применение. Несколько мягких привязок могут формировать жесткую привязку. Коды экземпляра устройства - в большинстве своем уникальны и обеспечивают жесткую привязку.

Таблица 1

Описание свойств классов WMI, используемых для привязки ПО к комплектующим АРМ

Свойство	Класс	Комплектующая	Привязка	Особенности	Особое применение
Материнская плата					
Manufacturer	BaseBoard	Производитель	М	В случае «пиратской» материнской платы может быть пустым	
Product	BaseBoard	Модель	М	Модель указывается без ревизии	
Name, Manufacturer, SerialNumber, Version, ReleaseDate	BIOS	Чип BIOS	М	Важны именно как комбинация свойств	Жесткая привязка к прошивке BIOS
SerialNumber	BaseBoard	Серийный номер**	М, Ж	В большинстве материнских плат содержит мусорную неуникальную информацию («пиратские», см. **[1]**).	Если серийный номер уникальный – получится жесткая привязка к нему
InternalReferenceDesignator	PortConnector	Интерфейсы (порты I/O, активные и неактивные)	М	Обычно интерфейсы вида «IDE», «USB», но встречаются вида «J2A2A», «J9A1 - TPM HDR»	
PNPDeviceID	FloppyController	Код экземпляра контроллера FDD***	Ж		
PNPDeviceID	IDEController	Код экземпляра контроллеров IDE***	Ж	Обычно число контроллеров IDE (ATA, PATA, Integrated Drive Electronics) кратно двум	
PNPDeviceID	InfraredDevice	Код экземпляра инфракрасного порта***	Ж	Колодки ИК-порта встречаются и на современных материнских платах	
PNPDeviceID	ParallelPort	Код экземпляра контроллера LPT***	Ж		

Свойство	Класс	Комплектующая	Привязка	Особенности	Особое применение
PNPDeviceID	PCMCIAController	Код экземпляра контроллера PCMCIA***	Ж		Полезен при привязке ПО к ноутбуку или нетбуку с поддержкой PCMCIA
PNPDeviceID	SCSIController	Код экземпляра контроллера SCSI***	Ж	Интерфейс Small Computer System Interface уступил место Serial Attached SCSI в 2000-х годах **[3]**	Определяет ли данный параметр и код экземпляра контроллера SAS - неизвестно
PNPDeviceID	1394Controller	Код экземпляра контроллера 1394***	Ж	Интерфейс IEEE 1394 (FireWire, i-Link) не уступает другим интерфейсам, обеспечивая пропускную способность до 3200Мб/с, применяется в зарубежной военной промышленности **[4]**	
PNPDeviceID	SerialPort	Код экземпляра контроллера COM***	Ж	RS232 является устаревшим, но не ушедшим с рынка комплектующих интерфейсом	
PNPDeviceID	USBController	Код экземпляра контроллеров USB***	Ж	Обычно каждый контроллер USB поддерживает один разъем на материнской плате (пара интерфейсов USB) или пару интерфейсов USB на задней панели	

Свойство	Класс	Комплектующая	Привязка	Особенности	Особое применение
PNPDeviceID	USBHub	Периферия: Код экземпляра концентратора в USB***	Ж	Не работает в Windows 2000. В список концентраторов USB будут входить подключенные к материнской плате внешние и внутренние кард-ридеры, концентраторы USB и флешки	Код экземпляра флешки уникален, поэтому данный параметр может использоваться в роли ключа eToken. Карты памяти таким свойством не обладают
Накопитель					
BytesPerSector	DiskDrive	Байт в секторе**	М	На большинстве накопителей – 512 байт. Кард-ридер и флешки также являются накопителями	
Model	DiskDrive	Модель	М		
InterfaceType	DiskDrive	Интерфейс	М	Иногда SATA определяется как IDE	
Partitions	DiskDrive	Число логических дисков	М		
PNPDeviceID	DiskDrive	Код экземпляра***	Ж	Уникален, за исключением кард-ридера	
Привод					
Caption	CDROMDrive	Модель	М		
PNPDeviceID	CDROMDrive	Код экземпляра***	Ж		
PNPDeviceID	FloppyDrive	Код экземпляра (FDD)***	Ж		
Оперативная память					
Capacity	PhysicalMemory	Общее количество	М		
SerialNumber	PhysicalMemory	Серийный номер**	М, Ж	Уникален, но практически всегда пуст	Если серийный номер уникальный – получится жесткая привязка к нему

Свойство	Класс	Комплектующая	Привязка	Особенности	Особое применение
SKU	PhysicalMemory	Идентификатор SKU**	M (Ж?)	Должен быть уникален, но пуст всегда.	Stock Keeping Unit - идентификатор товарной позиции, единица учёта запасов, складской номер, используемый в торговле для отслеживания статистики по реализованным товарам/услугам
Model	PhysicalMemory	Модель**	M	Практически всегда пуст	
Position	PhysicalMemory	Положение в слотах	M		
Сетевая карта					
Manufacturer	NetworkAdapter	Производитель чипа* **	M	Система не видит различия между физической сетевой картой и виртуальной.	
PNPDeviceID	NetworkAdapter	Код экземпляра* ***	Ж	Уникален только для физических сетевых карт	
MACAddress	NetworkAdapter	MAC-адрес* **	M	Уникален, но легко подделать	
Видеокарта					
Name	VideoController	Модель	M	Не уникален, но модель определяется однозначно	
AdapterRAM	VideoController	Объем памяти	M		
PNPDeviceID	VideoController	Код экземпляра***	Ж		
Процессор					
Name	Processor	Модель*	M		
ProcessorID	Processor	Серийный номер* **	M	Хаотичен, но не уникален	

Свойство	Класс	Комплектующая	Привязка	Особенности	Особое применение
ExtClock	Processor	Внешняя частота*	M		Уникален в случае, если значение было изменено пользователем в BIOS вручную и используется совместно с параметром модели процессора
MaxClockSpeed	Processor	Тактовая частота* ** ****	M	В случае автоматического определения в BIOS данный параметр использовать нельзя, так как имеются флуктуации частоты ±1Гц	В случае ручного определения в BIOS может стать уникальным параметром, если используется совместно с параметром модели процессора
АКБ					
DeviceID	Battery	Код экземпляра	M	Не уникален, иногда совпадает с названием оборудования, которое ее использует	Использование этих трех свойств позволяет запускать ПО на портативных ПК. Параметры батареи активны только тогда, когда батарея присутствует в оборудовании
Name	Battery	Модель****	M	Нестабильный параметр на некоторых ноутбуках - требуется до 30-ти раз перевыбирать модель, убедившись в ее неизменности	

Свойство	Класс	Комплектующая	Привязка	Особенности	Особое применение
BatteryStatus	Battery	Батарея: Режим работы	М	«От сети», «от батареи» – 2 стабильных вида данного свойства	
Периферия					
Name	Printer	Принтеры**	М	Позволяет получить привязку к принтеру, подключенному к конкретному порту	
PNPDeviceID	Keyboard	Код экземпляра клавиатуры	М	Уникален только как комбинация модели клавиатуры и порта ее подключения (только для портов USB)	
PNPDeviceID	PointingDevice	Код экземпляра мыши	М	Уникален только как комбинация модели мыши и порта ее подключения (только для портов USB)	
PNPDeviceID	TapeDrive	Код экземпляра стримера (Tape Drive)	Ж	Технологии размещения информации на ленточных накопителях в настоящее время конкурентоспособны с традиционными технологиями накопителей ЭВМ **[5]**	
PNPDeviceID	DesktopMonitor	Периферия: Код экземпляра монитора	М		

** - получение информации по свойству занимает более 1 секунды;*

*** - свойство с высокой вероятностью неуникальности и ненадежности;*

**** - уникальность наиболее вероятна;*

***** - нестабильное свойство.*

Заключение

Системный анализ WMI позволил точно определить свойства классов WMI, необходимые для решения проблемы нелегального копирования ПО, а именно привязку ПО к конкретному АРМ. Часть отобранных признаков позволяют осуществить жесткую привязку ПО к комплектующим АРМ, предотвращая негативное воздействие программ побайтного копирования данных.

Было разработано ПО, позволяющее осуществить данную задачу посредством создания электронных ключей безопасности. Оно легко интегрируется в защищаемое ПО программистом любой квалификации, создание и обслуживание ключей доступно сотруднику любой квалификации.

Основные методы нестандартного использование свойств классов WMI:

- код экземпляра концентраторов USB (свойство PNPDeviceID класса USBHub) может быть использован для привязки ПО к флешке (независимо от ее размера, фирмы и наполнения) как к ключу eToken, запретив загрузку ПО при ее отсутствии. Уникальность данного параметра тестировалась на 20 флешках, из них 10 - одного производителя, марки, модели и объема;
- в системе присутствуют виртуальные сетевые карты, получаемые при помощи свойств класса NetworkAdapter (Manufacturer, PNPDeviceID, MACAddress);
- внешняя и тактовая частота процессора (класс Processor: MaxClockSpeed, ExtClock), в случае ручного изменения в BIOS, могут стать уникальными параметрами, если используются совместно с параметром модели процессора;
- Stock Keeping Unit оперативной памяти (класс PhysicalMemory: SKU) мог бы использоваться для отслеживания статистики отказов комплектующих определенного поставщика, если бы не был всегда пуст;
- возможна привязка к батарее ноутбука/нетбука/планшета, позволяющая запускать ПО только на этих портативных устройствах (класс Battery: DeviceID, Name, BatteryStatus);
- возможна привязка к модели монитора как наименее очевидной для взлома защиты (свойство PNPDeviceID класса DesktopMonitor).

ЛИТЕРАТУРА

1. Белов С.П. Разработка методики привязки программного обеспечения к комплектующим автоматизированного рабочего места без использования инсталлятора / Москва: МГУПИ, Сборник научных трудов VI Всероссийской научно-технической конференции «Мехатроника. Робототехника. Автоматизация», №7, 2014 г.
2. Свидетельство об официальной регистрации программы для ЭВМ №2014660899 (Защитник ПО v.1.0). Программа предназначена для привязки программного обеспечения к конкретным комплектующим системного блока (посредством создания и использования зашифрованных ключей) / Белов С.П. – 2014 г.
3. Википедия. SCSI / Сан-Франциско: Wikimedia Foundation, Inc., Свободная энциклопедия «Википедия», 2012 г. [Электронный ресурс] URL: https://ru.wikipedia.org/wiki/SCSI.
4. Уилф Салливан (Dy 4 Systems Inc.). Что заменит MIL-STD-1553 в роли сетевой магистрали военных систем следующего поколения? / Канада, Онтарио: журнал «Мир компьютерной автоматизации», №4, 1999 г.
5. Залужный Д. Ленточные накопители DAT/DDS. Настоящее и будущее формата / Москва: компания «NStor», 2008 г.

Sergey Belov
Moscow State University of Instrument Engineering and Informatics
Russian Federation, Moscow
E-Mail: Sergey.belov@list.ru

Non-standard use the classes and properties of Windows Management Instrumentation for fasten software to automation equipped working place without use installer

Abstract. The problem of the illegal use of software always was actual, complicated with appearance of the programs byte copying given with drives. Under their use virtual protection, built in system from software installer, loses the sense. In the event of high-priced software and equipment - for its use will get up the question of the development of other methods of protection even though this requires the manual setting for each equipment. For this was a studied Windows management instrumentation, is made system analysis of its classes and properties, are chosen required for work with completing. In article are considered given classes and properties within the framework of software protection (including their non-standard use).

Keywords: protection; software; copying; piracy; automated worker place; installer; windows management instrumentation.

REFERENCES

1. Belov S.P. Razrabotka metodiki privjazki programmnogo obespechenija k komplektujushhim avtomatizirovannogo rabochego mesta bez ispol'zovanija installjatora / Moskva: MGUPI, Sbornik nauchnyh trudov VI Vserossijskoj nauchno-tehnicheskoj konferencii «Mehatronika. Robototehnika. Avtomatizacija», №7, 2014 g.
2. Svidetel'stvo ob oficial'noj registracii programmy dlja JeVM №2014660899 (Zashhitnik PO v.1.0). Programma prednaznachena dlja privjazki programmnogo obespechenija k konkretnym komplektujushhim sistemnogo bloka (posredstvom sozdanija i ispol'zovanija zashifrovannyh kljuchej) / Belov S.P. – 2014 g.
3. Vikipedija. SCSI / San-Francisko: Wikimedia Foundation, Inc., Svobodnaja jenciklopedija «Vikipedija», 2012 g. [Jelektronnyj resurs] URL: https://ru.wikipedia.org/wiki/SCSI.
4. Uilf Sallivan (Dy 4 Systems Inc.). Chto zamenit MIL-STD-1553 v roli setevoj magistrali voennyh sistem sledujushhego pokolenija? / Kanada, Ontario: zhurnal «Mir komp'juternoj avtomatizacii», №4, 1999 g.
5. Zaluzhnyj D. Lentochnye nakopiteli DAT/DDS. Nastojashhee i budushhee formata / Moskva: kompanija «NStor», 2008 g.