АРХИТЕКТУРА ЧИПА БЕЗОПАСНОСТИ

Зорин Виталий,
канд. техн. наук, системный аналитик ОАО «ЭЛВИС-ПЛЮС»

PC Week/RE № (493) 31`2005 от 23.8.2005

...Считаю самой приоритетной задачей для корпорации
и ИТ-индустрии на предстоящие десять лет создание
для пользователей защищенной информационной среды.

Билл Гейтс

Мы уже рассматривали на страницах нашего еженедельника инициативы некоммерческой международной организации Trusted Computing Group (TCG) по разработке и продвижению открытых спецификаций промышленного стандарта, определяющего доверенные модули, - Trusted Platform Module, TPM (см. PC Week/RE, № 12/2005, с. 27), а также практическое воплощение этих спецификации при реализации базового доверенного модуля (БДМ) “Мобильный клиент” (см. PC Week/RE, № 16/2005, с. 26).

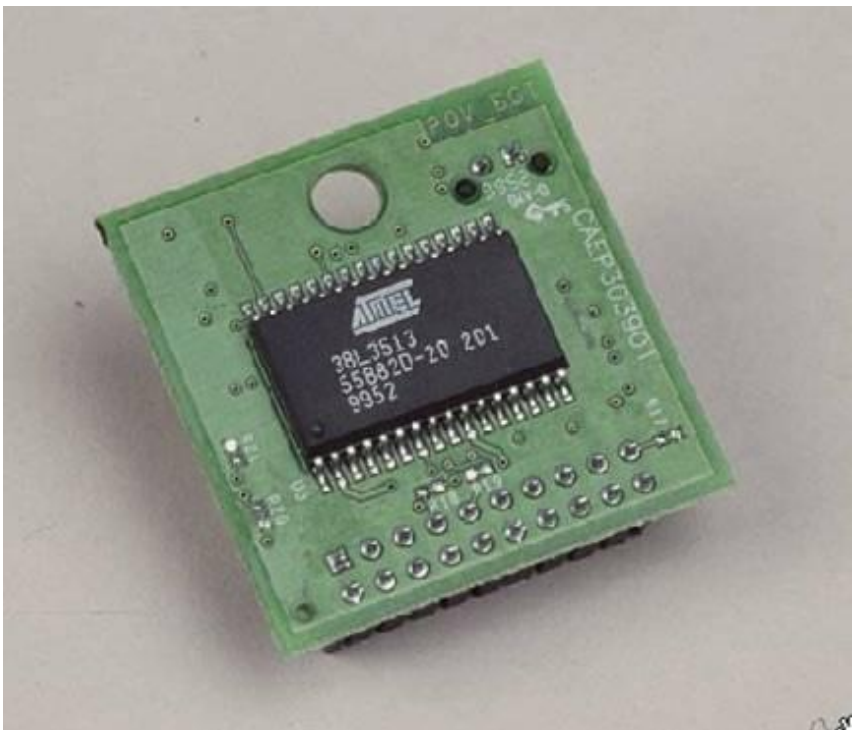

Рис. Чип безопасности

Модуль TPM представляет собой микроконтроллер, выполненный в виде интегральной микросхемы, которую принято называть чипом безопасности. Микроконтроллер хранит ключи, пароли и цифровые сертификаты. Обычно он встроен в системную плату компьютера, а потенциально может быть использован в любом устройстве, так как его размер не превышает размера мелкой монеты. Реализация чипа гарантирует, что хранимая в нем информация надежно защищена как от физического взлома, так и от атак со стороны внешнего программного кода. Защитные механизмы платформ способствуют разработке и применению сервисов безопасности. Технологии безопасности, основанные на открытом ключе (PKI), такие как ЭЦП и протоколы обмена ключами, защищаются посредством подсистем, реализованных по стандарту TCG. Доступ к данным и секретам платформы может быть запрещен, если параметры процесса загрузки ОС отклонятся от заданных значений. В силу этого критичные приложения и процессы, обеспечивающие защиту веб-доступа, электронной почты и локальных данных, при установке на доверенную платформу TCG становятся все более и более неуязвимыми.

Состав. Итак, чип безопасности представляет собой специализированную микросхему (см. рисунок) включающую:

- криптографический сопроцессор;
- связующую логику;
- специализированный интерфейс;
- генератор случайных чисел;
- логику защиты от атак по тактовой частоте;
- сенсоры: частоты, напряжения, температуры, освещения, импульсных помех.

Функции. В соответствии со спецификацией TPM чип должен выполнять, как минимум, следующий набор функций:

- хранение информации о статусе ОС;
- генерация и хранение закрытого ключа;
- хеширование (SHA-1) файлов;
- формирование ЭЦП;
- обеспечение цепочки доверия для ключей, сертификатов и других критичных данных.

Технология. Технологическими особенностями чипа безопасности являются:

- высокая степень интеграции элементов;
- энергонезависимая память;
- ППЗУ;
- скрытая структура ПЗУ.

Защитные механизмы. Использование новейших технологий производства ИС дает уверенность, что для взлома чипа хакеру потребуется очень дорогое оборудование и это ограничит число потенциальных нарушителей, понизит риски. Подделка такого высокотехнологичного чипа по сравнению с его взломом будет стоить еще дороже. В архитектуре чипа реализованы следующие механизмы:

- защищенное управление памятью;
- шифрование шины/памяти;
- тестирование режимов блокирования;
- активное экранирование.

Чтобы разобраться в системе встроенной детекции и получить результат ее срабатывания, взломщик должен исследовать хотя бы один чип. Например, активное экранирование означает, что чип может детектировать электрическое тестирование и в ответ предпринять необходимые меры вплоть до полного блокирования чипа. Большинство защитных механизмов связано с логикой работы чипа. В чип имплементированы алгоритмы асимметричной криптографии, обеспечивающие высокий уровень защиты. Некоторые элементы логического дизайна чипа являются нестандартными с точки зрения типовых методов проектирования интегральных схем (ИС). В частности, в чипе SLD 9630 TT компании **Infineon** вместо стандартного универсального процессора используется специализированный, обеспечивающий комплексную защиту. Применяются и специальные приемы проектирования ИС: “запутывание” топологии слоев ИС, усложняющее анализ функций элементов микросхемы, а также шифрование данных, хранящихся в памяти и передающихся по шинам. Всего этого нет в стандартном процессоре.

Ряд технологических особенностей чипов безопасности специально не разглашается компаниями-производителями, чтобы уменьшить вероятность взлома даже в том случае, когда для этого применяются современные методы анализа функционирования микросхем и дорогостоящее оборудование.

Чипы безопасности основных производителей. Рассмотрим особенности чипов безопасности различных поставщиков. Сравнительные характеристики чипов приведены в таблице.

Компания **Infineon** поставляет на рынок чип безопасности SLD 9630 TT, который представляет собой защищенный контроллер, включающий:

- защищенную перепрограммируемую память (EEPROM);
- аппаратный акселератор RSA криптоалгоритмов (вычисление ЭЦП, проверка ЭЦП, генерация ключей длиной до 2048 бит CRT);
- аппаратный акселератор хеш-функций (SHA-1, MD-5);
- генератор “правильных” случайных чисел;
- LPC-интерфейс, разработанный в соответствии со спецификацией Intel.

Чип характеризуется малой мощностью потребления, усовершенствованной защитой, в частности от SPA/DPA-атак, и легко интегрируется в известные PC-платформы.

ПО чипа безопасности SLD 9630 TT имеет ряд особенностей: встроенную защищенную ОС; программный стек TSS, созданный с учетом спецификации 1.1b комитета TCG; криптографический сервис-провайдер (CSP) спецификации TPM.

Дизайн и архитектура чипа отличаются следующими специфическими элементами и функциональными особенностями:

- нетиповой ЦП;
- применение скрытой топологии;
- ограниченный интерфейс;
- генератор случайных чисел;
- средства защиты от атак по питанию и тактовой частоте;
- защита управления памятью;
- шифрование данных, хранящихся в памяти и передающихся по шинам;
- блокирование режима тестирования.

В производстве чипа SLD 9630 TT используется передовая технология высокой степени интеграции, обеспечивающая изолированность ячеек ППЗУ и сокрытие структуры ПЗУ.

Чип SLD 9630 TT представляет собой специализированную ИС с заказными алгоритмами защиты, связующей логики и активным экранированием. Он содержит сенсоры частоты, напряжения, температуры, света, импульсных помех.

Подложка чипа имеет:

- экранирование слоев;
- неметаллический слой коммутации;
- плавкие перемычки;
- матричные ИС FPGA (перепрограммируемая пользователем вентильная матрица).

Чипы безопасности компании Infineon поставляются вместе с типовыми криптобиблиотеками MS CAPI и PKCS#11, обеспечивающими легкую интеграцию с функциями безопасности чипа существующих ОС и многих приложений.

Компания **Atmel** контролирует 95% рынка чипов безопасности (см. маркетинговые материалы Atmel за 2004 г.): с 1998 г. объем проданных чипов AT97SC3201 (TPM 1.1) достиг 5 млн. шт. С конца 2004 г. эта фирма производит чип AT97SC3202, совместимый со спецификацией TPM 1.2.

Новая микросхема AT97SC3202 имеет электронную защиту, которая детектирует и предотвращает попытки чтения внутреннего содержимого чипа. Также чип содержит в себе металлические экранирующие слои над внутренними электрическими цепями; выполняет шифрование данных, передаваемых по внутренним шинам; имеет специальные процедуры для тестирования защиты; противодействует timing-атакам и атакам по электропитанию.

Чип поставляется вместе с драйверами для ОС Linux и Windows 98, 2000, XP. Новые возможности AT97SC3202 обеспечивают: транспортные сессии, функционирование часов реального времени, локализацию, сохранение и восстановление контекста, DAA-аттестацию (direct anonymous attestation), энергонезависимое хранение данных и механизм делегирования.

Транспортные сессии позволяют удостовериться, что чип AT97SC3202 выполняет определенные команды (шифрование, дешифрование, генерацию ключей и т. п.). Транспортные сессии могут быть полезны, например, для администратора безопасности ИТ-подразделения при отслеживании операций резервного копирования ключей или контроля ноутбука с точки зрения правильности конфигурации модуля TPM.

Встроенные в чип часы реального времени предназначены для подстановки текущей даты и времени в процедуру формирования ЭЦП. Данная возможность применима при электронном обмене коммерческими контрактами, финансовыми гарантиями, заказами и в других случаях, когда время является критичным параметром.

Локализация поддерживает расширенные защитные функции специализированных микропроцессоров и/или системных чипов.

Механизм сохранения и восстановления контекста обеспечивает поддержку многопоточных приложений. В TPM версии 1.1 нужно было завершить выполнение одной авторизационной сессии перед началом выполнения следующей. Управление контекстом позволяет привилегированным, критичным по времени процессам выгружать менее критичные и за счет этого повышать производительность.

Благодаря прямой анонимной аттестации (DAA) модуль TPM может создавать для Интернета идентификационные карты (Internet ID cards), аналогичные сертификатам, которые используются в механизмах ЭЦП. В настоящее время сертификаты могут быть заказаны третьей стороне, например компании Verisign. Данная функциональность обеспечивает защиту пользовательских данных.

Делегирование позволяет собственнику TPM получить выборочный доступ к другим объектам с целью выполнения модулем TPM специальных функций, требующих присутствия собственника, - например, при генерации идентификатора пользователя. Кроме того, механизм делегирования разрешает пользователям временно предоставлять третьей стороне возможность использования любых ключей или формирования ЭЦП.

В отличие от других производителей компания **National Semiconductor** предложила решение, объединяющее в одной СБИС контроллер ввода-вывода и чип безопасности. Данный подход не только устраняет необходимость решать задачу размещения чипа без внесения изменений в типовые системные платы компьютера, но и создает задел на будущее. Компания Intel, опираясь на новую технологию La Grande, обещает с помощью чипа безопасности обеспечить контроль типовых интерфейсов ввода-вывода. Такой контроль затруднит перехват ввода-вывода пользовательской информации через буфер клавиатуры, доступ к содержимому защищенной памяти через контроллер DMA и к USB-устройствам и соответственно повысит уровень защищенности конфиденциальных данных (паролей, ключей, идентификаторов, сообщений и документов).

Швейцарская компания **STMicroelectronics** выпускает чип безопасности ST19WP18, совместимый со спецификацией TPM 1.2. Технологически чип наследует семейству ST19W-чипов для смарт-карт. За II квартал 2005 г. компания продала производителям системных плат для компьютеров более 1 млн. чипов ST19WP18. В частности, Intel применяет чипы безопасности STMicroelectronics в платах D945GNTLKR, D945GTPLKR, D945GCZLKR.

Чип безопасности по существу играет роль надежного встроенного сейфа для хранения “ключей” от дверей, за которыми хранится конфиденциальная информация в десктопах, ноутбуках и PDA-устройствах. Появление подобных чипов – естественная реакция на слабость существующих методов хранения таких “ключей”.

Неотделимость чипа безопасности от программно-аппаратной платформы обеспечивает возможность идентификации и аутентификации рабочих станций пользователей КПК и других устройств.

Наличие в чипе хеш-функции и функций ассиметричного криптопреобразования для поддержки ЭЦП позволяет контролировать целостность программно-аппаратной среды локальной рабочей станций, а также программно-аппаратных сред, входящих во взаимодействие с удаленными станциями и устройствами.

Сравнительные характеристики чипов безопасности

Характеристики	Atmel		Infineon		National Semiconductor	STMicroelectronics
	AT97SC3201	AT97SC3202	SLD 9630 TT 1.1	SLB 9630 TT 2.0[1]	PC8374T PC8392T[2]	ST19WP18
ЦПУ	8\16бит \ 16\33мГц	8\16бит \ 16\33мГц	16 бит \ 33мГц	16 бит \ 33мГц	16 бит \ 33 мГц	8 бит \ 33мГц
ОЗУ	8 Кб	8 Кб	8 Кб	12 Кб	8 Кб	4 Кб
ПЗУ	64 Кб	64 Кб	64 Кб	208 Кб	-	114 Кб
ППЗУ	16 Кб	16 Кб	16 Кб	68 Кб	128 Кб	18 Кб
Версия спецификации TPM	1.1	1.2	1.1	1.2	1.1b	1.1b / 1.2
Контроль загрузки BIOS MAD/MPD BIOS драйверы	+	+	+	+	+	+
Активное экранирование слоев	+	+	+	+	нет данных	нет данных
Сенсоры (частоты, напряжения, температуры, света, импульсных помех)	-	-	+	+	-	+
DAA	-	+	-	+	-	+
SPA\DPA	-	-	+	+	+	+
PCR[3]s	16	32	нет данных	нет данных	нет данных	нет данных
Защита от атак по питанию и тактовой частоте	+	+	+	+	+	+
Шифрование данных на шине	+	+	+	+	нет данных	+

[1] Планируется к выпуску в 2005 г.
[2] PC8392T – для ноутбуков; PC8387T – для десктопов
[3] Регистры конфигурации платформы ОС

Характеристики	Atmel		Infineon		National Semiconductor	STMicroelectronics
	AT97SC3201	**AT97SC3202**	**SLD 9630 TT 1.1**	**SLB 9630 TT 2.0[1]**	**PC8374T PC8392T[2]**	**ST19WP18**
Технология	0.18 мкм	0.18 мкм	0.24 мкм	0,22 мкм	нет данных	нет данных
ОС	Linux, Win 2000, WinXP	Linux, Win 2000, WinXP	Win2000, WinXP	Win2000, WinXP	Win2000, WinXP	Win2000, WinXP
Библиотеки PKCS#11, MSCAPI	-	-	+	+	+	+
Сертификат по Common Criteria	EAL3+	-	-	-	EAL3+	-
Питание	3.3 В	3.3 В	3.3 В	3.3 В	3.3 В; 5 В	3.3 В
Производитель	США	США	Германия	Германия	США	Швейцария