На сегодняшний день разработан действующий прототип, который выставлялся на многочисленных национальных и международных выставках и завоевал высокие награды. Разработанные методики и алгоритмы защищены патентом. Исследовательская работа поддерживалась рядом государственных грантов.

Литература:

1. Forrest, S. Self-nonself discrimination in a computer / S. Forrest, A. Perelson, L. Allen, R. Cherukuri // In Proceedings of the IEEE Symposium on Security and Privacy, 1994. – P. 202–212.

2. Burnet, F. The Clonal Selection Theory of Acquired Immunity / F. Burnet. – Cambridge University Press, 1959.

3. Jerne, N. Towards a network theory of the immune system. Ann. Immunology (Inst. Pasteur), 125C / N. Jerne. – 1974. – P. 373–389.

4. Greensmith, J. The deterministic dendritic cell algorithm / J. Greensmith, U. Aickelin // In Proc. of the 7th International Conference on Artificial Immune Systems (ICARIS). – Springer, 2008. – P. 291–302.

5. Harmer, P. An artificial immune system architecture for computer security applications / P. Harmer, P. Williams, G. Gunsch, G. Lamont // IEEE Transaction on Evolutionary Computation, 2002. – 6(3). – P. 252–280,

6. Безобразов, С.В. Нейросетевая искусственная иммунная система для обнаружения вредоносных программ: принципы построения / С.В. Безобразов, В.А. Головко // Вестник БрГТУ. Физика, математика, информатика. – 2009.

7. Безобразов, С.В. Алгоритмы искусственных иммунных систем и нейронных сетей для обнаружения вредоносных программ / С.В. Безобразов, В.А. Головко // Научная сессия НИЯУ МИФИ «Нейроинформатика»: материалы Всеросс. науч. конф., МИФИ, Москва, 25–29 янв. 2010. – Москва, 2010. – С. 273–287.

8. Головко, В.А. Проектирование интеллектуальных систем обнаружения аномалий / В.А. Головко, С.В. Безобразов // Материалы международной научно-технической конференции «Открытые семантические технологии проектирования интеллектуальных систем OSTIS-2011». – Минск: БГУИР, 2011. – С. 185–196.

9. Golovko, V. Evolution of Immune Detectors in Intelligent Security System for Malware Detection / V. Golovko, S. Bezobrazov, V. Melianchuk, M. Komar // Proceedings of the 6th IEEE international conference on intelligent data acquisition and advanced computing system IDAACS-2011. – Prague: Technical university, 2011. – P. 722–726.

10. Головко, В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпьютеры и их применение: учеб. пособие. – М.: 2001. – 256 с.

11. Komar, M. Intelligent System for Detection of Networking Intrusion. / M. Komar, V. Golovko, A. Sachenko, S. Bezobrazov – In Proc. 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing System (IDAACS-2011). – Prague, Czech Republic, 2011. – P. 374–377.

Abstract

Artificial immune systems (AIS) and artificial neural networks (ANN) are very powerful technique for data mining and pattern recognition. Over the past few decades, application of these approaches has been growing rapidly in different domain. However, to date a consistent performance of AIS and ANN has not achieved. We sincerely believe that integration of these both techniques can allow constructing an intelligent system for information security. In this research we report a novel method for malicious code detection. It is based on main principles of AIS, which consist of different immune detectors and each immune detector represents counterpropagation neural network. The main goal of proposed approach is to detect unknown, previous unseen threat (malicious code, intrusion detection, etc.). It is achieved by the adaptation of the neural network immune detectors to the continually changeable computer environment. As a result the immune detectors have capability to evolve during a life. The evolution ability of neural immune detectors in artificial immune system is presented. The results of the experiments are shown the performance of the algorithm in increasing the quality of new, unknown threat detection.

Поступила в редакцию 18.05.2013 г.

ПОДХОД К ПОСТРОЕНИЮ СРЕДСТВ ЗАЩИТЫ «ОБЛАЧНЫХ» СИСТЕМ

УДК 004.3'2

В.И. Хведчук, В.В. Буслюк, С.С. Дереченник,
БрГТУ, г. Брест

Аннотация

В работе предлагается подход к хранению личных данных в корпоративной системе, базирующейся на «облачной» технологии. Проводится обзор известных решений в данной области. Рассмотрены базовые решения на базе протокола NFC. Выделены, в качестве основных, решения фирм Inside Secure и Texas Instruments. Предложена структура устройства на базе протокола, используемого в стационарных линиях связи с использованием отечественной элементной базы. В результате получается защищенная среда, позволяющая обеспечить доступ к «облачным» ресурсам и обеспечивающая мобильность корпоративных систем, построенных на современной основе. При этом необходимо решение дополнительно проблем с обслуживанием такого рода структур, связанных, прежде всего, с человеческим фактором. Здесь, конечно же, важную роль должно сыграть обучение кадров. Предполагается к использованию в корпоративной среде университета.

Введение

В настоящее время информационные технологии проникают в различные сферы деятельности человека, общества, государства. Происходит изменение обычных для нас процессов и объектов. Меняются способы оплаты услуг и

товаров, идентификации, обмена информацией. Не редкость сейчас идентификационная или банковская карта. Со временем этот процесс продолжится, Примером может служить введение мобильных технологий. Пока еще привычным является платеж в банке, но звонок по стационарному телефону уже не является единственным средством online-коммуникации. Массовая информатизация охватывает все новые сферы деятельности, появляется все больше «облачных» услуг. Но этот количественный рост требует качественно иного подхода к обеспечению надежности и безопасности базовых механизмов подобных сервисов и услуг. И не последнюю роль здесь может сыграть задача обучения современным технологиям защиты информации. Причем как сотрудников компаний, представляющих данные сервисы и услуги, так и их клиентов. При этом важной остается задача обеспечения защиты при доступе к «облачным» технологиям с помощью стационарных коммуникаций ввиду их надежности.

Обзор решений по защите «облачных» систем. Современные облачные технологии предполагают переход к новой парадигме вычислений, хранения данных, управления доступом, вводят такие понятия, как шина служб, кэширование. Присутствуют возможности доступа к удаленному рабочему столу, безопасная доставка по защищенному SSL-соединению. Появляется и проблема хранения личных данных [1].

Имеются сведения и об аппаратной защите данных у Google. Предлагается использовать миниатюрные криптографические карты Yubico. Установленные в USB-порт позволят зарегистрироваться на новом сайте или войти в аккаунт Google, не набирая паролей (причем достаточно сложных, состоящих из случайных букв или цифр). Такой способ аутентификации аналогичен открытию двери ключом. Возможен переход на беспроводные протоколы и усиление защиты введением одноразового кода [2].

Отмечается, что современные средства обеспечения безопасности по своей функциональности вышли за рамки защиты ПЭВМ от вирусов. Речь идет об интернет-сервисах, онлайн-платежах, социальных сетях, мобильных устройствах, облачных хранилищах. Появились новые функции – резервное копирование, хранение и синхронизация паролей, безопасные онлайн-платежи, родительский контроль. Имеются также функции генерации паролей достаточной сложности. Такого рода функции включены в новую версию пакета CRYSTAL от Kaspersky Lab, NORTON 360 [3]. Пока неизвестно о наличии защиты в «облаках» в белорусском антивирусе ВирусБлокАда.

Развиваются также средства защиты и на десктопах, в том числе и на базе операционной системы [4, 5].

Аппаратная платформа. В качестве аппаратных платформ для реализации средств обеспечения безопасности с учетом облачной природы объекта защиты используются чаще всего решения на базе протокола NFC.

Реализации в данной области предлагают многие фирмы, но наиболее широким спектром в области защищенных решений обладает компания Atmel [6]. Известна

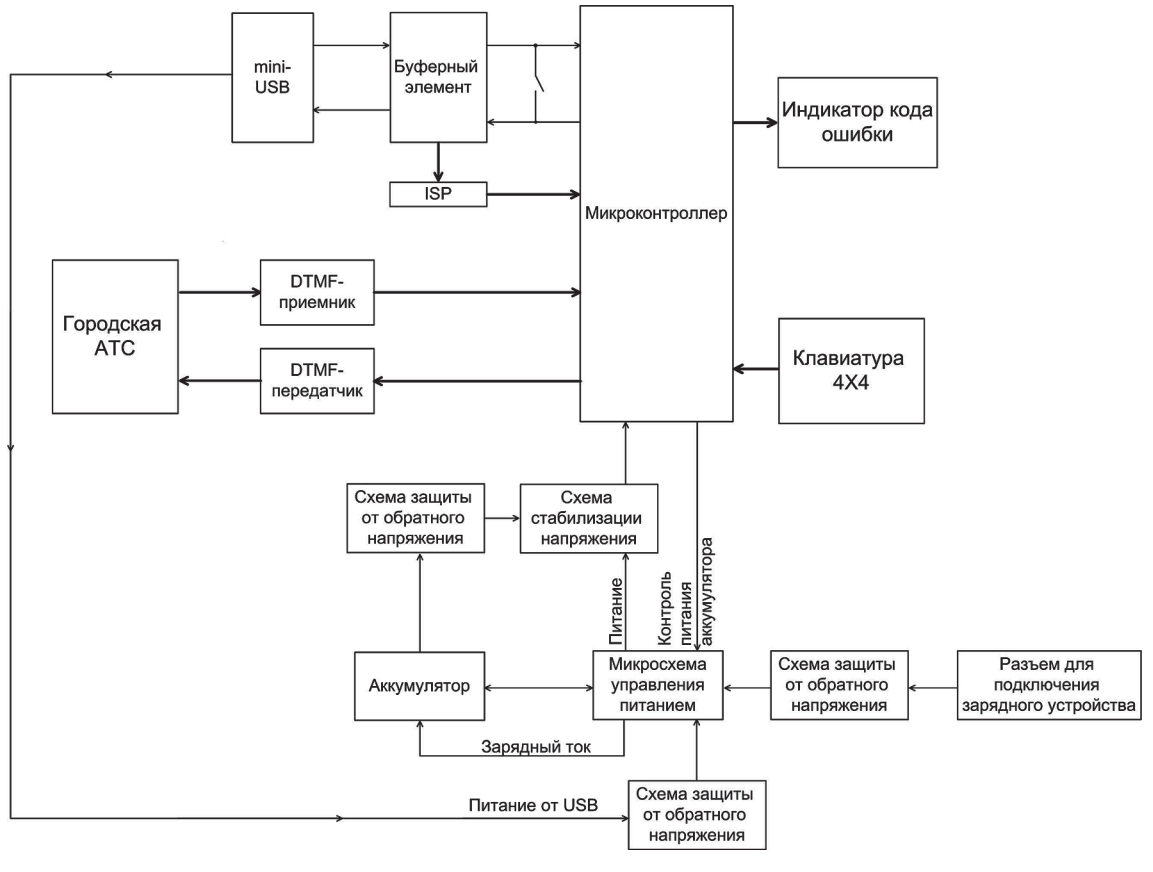

Рисунок 1

также своей проработкой вопросов построения закрытых приложений компания Inside Secure, которая приобрела в 2010 году подразделение Atmel, занимавшееся разработкой защищенных микроконтроллеров [7, 8]. Функции обеспечения информационной безопасности, реализуемые с помощью решений компании Inside Secure:

– аутентификация субъектов и объектов информационного взаимодействия (предоставление взаимодействующим сторонам возможности убедиться в том, что противоположная сторона действительно является тем, за кого себя выдает);

– шифрование информации (защита информации в случае перехвата ее третьими лицами);

– контроль целостности (гарантия того, что информация не была искажена или подменена);

– управление доступом (разграничение доступа к информации различных пользователей);

– управление ключами (организация создания, распространения и использования ключей субъектов и объектов информационной системы с целью создания необходимого базиса для процедур аутентификации, шифрования, контроля подлинности и управления доступом).

Хорошая схемотехническая проработка реализации NFC от фирмы Texas Instruments имеется в [9–11], причем со ссылкой на соответствующие стандарты. Описана также необходимая программная поддержка.

Структура коммуникационного процессора. В структуре устройства (рисунок 1) выделяются следующие основные блоки: микроконтроллер; ISP; mini-USB; ключ «Режим отладки»; буферный элемент; DTMF-приемник; DTMF-передатчик; аккумулятор; схема защиты от обратного напряжения; схема стабилизации напряжения; разъем для подключения зарядного устройства (ЗУ); микросхема управления питанием; клавиатура 4×4; индикатор кода ошибки. Назначение блоков устройства:

– ISP – (In-System Programming – системное программирование) для программирования микроконтроллера;

– mini-USB – для связи с и прошивки микроконтроллера;

– ключ «режим отладки» – для отладки устройства при отсутствии компьютера и телефонной линии;

– буферный элемент – это приемопередатчик от разъема USB – устройство, которое обеспечивает обмен данными между несколькими устройствами по одной двухпроводной линии связи. Микроконтроллер осуществляет связь с компьютером для передачи и приема данных от устройства, отладки;

– DTMF-приемник (от англ. Dual Tone Multi Frequency – двухтональная мультичастотная посылка) – для приема зашифрованных данных от телефонной сети;

– DTMF-передатчик – для передачи зашифрованных данных в телефонную сеть;

– схема защиты от обратного напряжения – для электронной защиты при ошибочном подключении аккумулятора, ЗУ, mini-USB;

– схема стабилизации напряжения – экономичный преобразователь напряжения, необходимый для нормальной работы микросхем;

– микросхема управления питанием – осуществляет «умное» управление питанием, выбор необходимых источников питания, обеспечение безопасной зарядки аккумулятора и индикацию текущего состояния питания;

– клавиатура 4x4 – для ввода информации в устройство при отсутствии компьютера;

– индикатор кода ошибки – индикация текущего состояние устройства.

Заключение

Таким образом, возможно получить защищенную среду, позволяющую обеспечить доступ к «облачным» ресурсам и обеспечивающую мобильность корпоративных систем, построенных на современной основе. При этом решаются дополнительно проблемы с обслуживанием такого рода структур, связанных, прежде всего, с человеческим фактором. Здесь, конечно же, важную роль должно сыграть обучение кадров. Предполагается к использованию в корпоративной среде университета.

Литература:

1. Редкар, Т. Платформа Windows Azure / Т. Редкар, Т. Гвидичи. М: ДМК Пресс, 2012. – 656 с.

2. Пароли – это прошлый век // Хакер. – № 3. – 2013. – С. 8.

3. Защита и сохранение самого ценного // CHIP, № 4. – 2013. – С. 66–67.

4. Карп, Д. Хитрости Windows 7. Для профессионалов / Д. Карп. – Спб.: Питер, 2011. – 512 с.

5. Станек, У. Windows 7 для продвинутых / У. Станек. – Спб.: Питер, 2010. – 576 с.

6. AVR XMEGA microcontroller. – http://www.atmel.com/products/microcontrollers/avr/AVR_XMEGA.aspx, 09.02.2013.

7. Secure microcontroller. – http://www.insidesecure.com/eng/content/download/871/8385/version/3/file/FLYER-SecureMicrocontroller_BD.pdf, 09.02.2013

8. New NFC-based chip from Inside Secure protects luxury goods from counterfeiters and cloners. – http://www.insidesecure.com/eng/Media/Press-releases/NEW-NFC-BASED-CHIP-FROM-INSIDE-SECURE-PROTECTS-LUXURY-GOODS-FROM-COUNTERFEITERS-AND-CLONERS, 09.02.2013

9. Alexander Kozitsky, Josh Wyatt, Johannes Sturz, Juergen Mayer-Zintel. NFC and RFID Reader Ultra-Low-Power Card Presence Detection Using MSP430 and TRF79xxA. – http://www.ti.com/lit/an/sloa184/sloa184.pdf. 06.04.2013

10. Multi-protocol fully integrated 13.56-mhz rfid/near field communication (NFC) transceiver IC – http://www.ti.com/lit/an/sloa184/slos743f.pdf. 06.04.2013

11. Mixed signal microcontroller. – http://www.ti.com/lit/an/sloa184/slas518.pdf. 06.04.2013

Abstract

The paper proposes an approach to the storage of personal data in the corporate system based on the "cloud" technology. Provides an overview the prior art in this field. Describes the basic solutions based on NFC protocol. Solutions companies Inside Secure and Texas Instruments are selected key. Proposed the structure of a device based on the protocol fixed lines. Use national element base. The result is a secure environment, allowing secure access to the "cloud" resources and providing enterprise mobility systems based on a modern basis. Thus it is necessary to additionally maintenance problems such structures associated primarily with human factor. Here, of course, has an important role the training of service personnel. It is assumed to be used in the corporate environment of the university.

Поступила в редакцию 18.05.2013 г.