O. O. Shelukha

MOBILE SURVEILLANCE SYSTEM OF DYNAMIC OBJECTS

The article describes a system of visual observation of dynamic objects. It highlighted the need to create a mobile surveillance system and also the mathematical apparatus for determining the position of the observed object. The first step shows the methodology for determining the coordinates of the observation of the object in the optoelectronic module frame. The second step shows the calculations of the coordinates of the object in of a rectangular coordinate system in the horizontal plane using angular coordinates. In the future, we propose the creation of an integrated system for the construction of three-dimensional model of the object the mobile surveillance system.

Keywords: *rectangular coordinate system, mobile tracking system, monitoring of dynamic objects.*

УДК 519.715

Ю. Б. Коваленко, к.пед.н.

Національний авіаційний університет, м. Київ

КОМП'ЮТЕРИЗОВАНА СИСТЕМА ЗАХИЩЕНОГО ЗАСТОСУВАННЯ НА ОСНОВІ ТЕХНОЛОГІЇ VOIP

Розвиток електронної комерції і зацікавленість технологією IP як єдиного транспорту для передачі інформації будь-якого виду, дали можливість зв'язати мережу Інтернет з традиційною телефонною мережею загального користування і запропонувати клієнтам персоналізоване обслуговування та зручний засіб спілкування. Розроблено захищений програмний застосунок, що на відміну від існуючих підтримує встановлення захищеного з'єднання та забезпечує захист медіа даних, при цьому ґрунтується на рекомендаціях RFC, а отже може вільно взаємодіяти з іншими апаратними і програмними технологіями VoIP. На додаток, у застосунку реалізовано керування доступом на основі ролей, що підвищує безпеку та удосконалює можливості моніторингу діяльності користувача.

Ключові слова : *контролер конференцій, технології VoIP, мережа SIP з проксі-сервером.*

Все більшої популярності серед користувачів в усьому світі набувають телекомунікаційні рішення на основі технологій VoIP. VoIP – система зв'язку, що забезпечує передачу мовного сигналу по мережі Інтернет або по будь-яким іншим IP-мережам. Сигнал по каналу зв'язку передається в цифровому закодованому вигляді з метою усунення надмірності.

Програми для VoIP використовуються для проведення по мережах, заснованих на протоколі IP, розмов подібних телефонним [1].

Деякі програмні VoIP-додатки включають в себе сервери для конференцій, системи внутрішнього зв'язку, віртуальні FXO і адаптовані телефонні додатки, що підтримують одночасно VoIP і ТМЗК, такі як системи IVR, сервери dial in dictation, утримання дзвінка і запису розмов.

Отже, можна стверджувати, що IP-телефонія не лише покращує ефективність ведення роботи, а й створює нові ризики. Залишаються проблеми безпеки інформації, адже навіть найбільш використовувані софтфони є вразливими для найпростіших атак. Отже актуальним є питання розробки програмного телефону з використанням захищених протоколів зв'язку.

Існує два основних фактори які впливають на голосовий трафік по захищених каналах IP. Перший – час, необхідний для шифрування змісту повідомлення і заголовків і створення нових заголовків. Другий – збільшення розміру пакета із заголовками доданими до вихідного пакету IP. Також існують проблеми стиснення даних Quality of service.

Зауважимо, перші VoIP методи, які використовували голосовий потік як прихований носій інформації, запропонував Діттманн.

Була запропонована оцінка існуючої стеганографії з особливим акцентом на рішеннях, які підходять для VoIP. Був описаний інструмент SteganRTP, використовуючи молодший біт (LSB) із кодеку G.711.

Ванг та Ву в роботі «Інформація, прихована у VoIP потоках» запропонували використовувати

молодші біти, але біти кодувалися з використанням кодеку Speex.

У праці «Оцінка загрози VoIP прихованого каналу» Такахаші і Лі запропонували аналогічний підхід, створивши прихований канал шляхом вбудовування та подальшого стиснення голосових даних у звичайному голосовому трафіку.

Відмітимо, що використовування протоколів IP-телефонії, найбільш досліджені були спеціалістами із проблем мережевої безпеки Варшавського Технологічного Університету Войцехом Мазурчеком і Кжиштофом Джипйорским, які провели експерименти із використання VoIP сервісів для передачі таємних повідомлень, про що вони доповіли на четвертій міжнародній конференції з питань глобальної електронної безпеки в Лондоні. Деякі аспекти з цієї проблематики вивчав В. Орлов «Методи прихованої передачі інформації в телекомунікаційних мережах» та І. Корчак, Ю. Пирогова [1 – 4].

Отже, метою нашої роботи є організація захищеного зв'язку між клієнтом та сервером, а також безпосередньо між клієнтами, використовуючи методи автентифікації та авторизації, а також мережеві протоколи, які забезпечують шифрування, встановлення автентичності повідомлення, цілісності, захист від заміни даних.

Для досягнення мети вирішували наступні задачі: огляд технологій та їх застосування у сучасних рішеннях заснованих на технології VoIP; аналіз вразливостей VoIP, методів атак та захисту від атак; розробка захищеного програмного застосунку на основі технології VoIP.

Основні атаки на VoIP можна класифікувати наступним чином:

- атаки направлені на відмову в обслуговуванні;
- перехоплення голосового або сигнального трафіку;
- прослуховування дзвінка;
- перенаправлення голосового або сигнального трафіку.

Мережа побудована згідно рекомендації H.323 [5], має зонну архітектуру (рис. 1). Контролер зони виконує функції управління однією зоною мережі IP-телефонії, в яку входять термінали, шлюзи, пристрої керування конференціями, зареєстровані у даного контролера зони. Окремі фрагменти області мережі H.323 можуть бути територіально рознесені і з'єднуватися один з одним через маршрутизатори [6] (рис. 2).

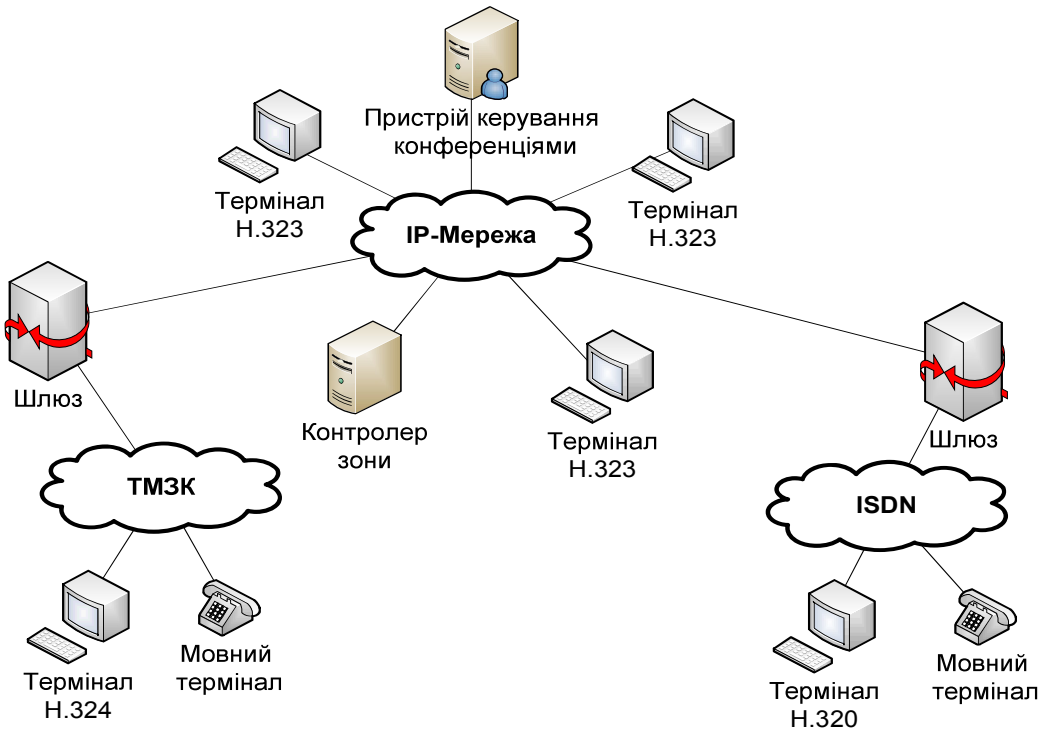

Рисунок 1 – Структура архітектури мережі H.323

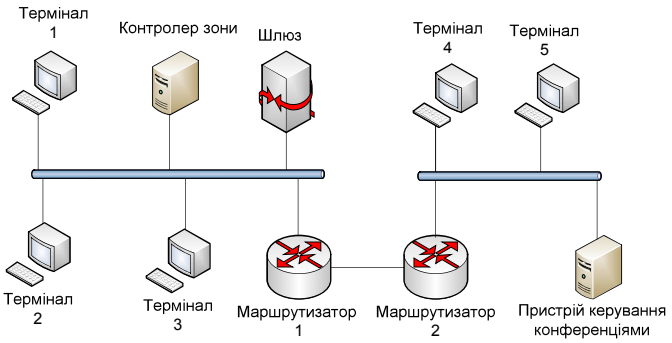

Рисунок 2 – Область мережі H.323

У сфері безпеки комп'ютерних систем, управління на основі ролей доступу (RBAC) – це підхід до обмеження доступу до системи тільки для авторизованих користувачів. Він використовується в більшості підприємств з великою кількістю співробітників.

В організації на підприємстві, ролі створюються для різних робочих функцій.

Дозволи для виконання певних операцій присвоюються конкретній ролі. Користувачам або персоналу (або іншим користувачам системи) призначаються певні ролі і через ці ролі їм надаються дозволи на виконання конкретних дій. Так як користувачам не призначаються дозволи безпосередньо, а тільки через ролі, управління індивідуальними правами користувача стає простим привласненням відповідних ролей облікового запису користувачу. Це спрощує загальні операції, такі як додавання користувача або зміна відділу користувача.

Для роботи з розробленим застосунком була обрана СУБД Microsoft SQL Server 2008.

Розроблена схема бази даних зображена на рис. 3.

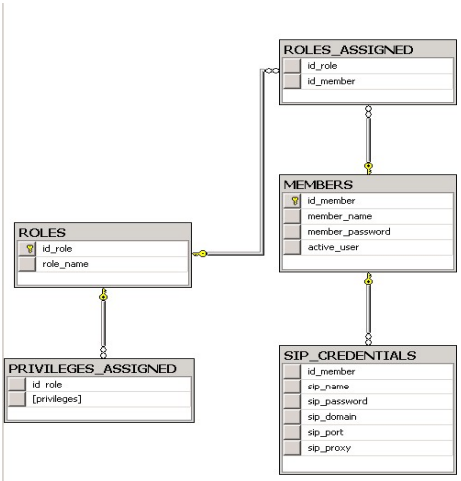

Рисунок 3 – Схема бази даних

Відповідно до окреслених завдань, а також визначених технологій та засобів реалізації було розроблено алгоритм роботи програми та написано програмний код.

Отже, програма налічує три форми для управління: форма автентифікації, головна форма, форма вхідного виклику.

Головна форма з її елементами зображена на рисунку 4. На ній містяться головні елементи управління програмою, такі як: поле для вводу номера абонента; меню; кнопка для початку виклику; кнопка для завершення виклику; регулятор гучності звуковідтворюючих пристроїв; регулятор гучності звукозаписуючих пристроїв; поле з відтворенням у текстовому режимі дій SIP-клієнта.

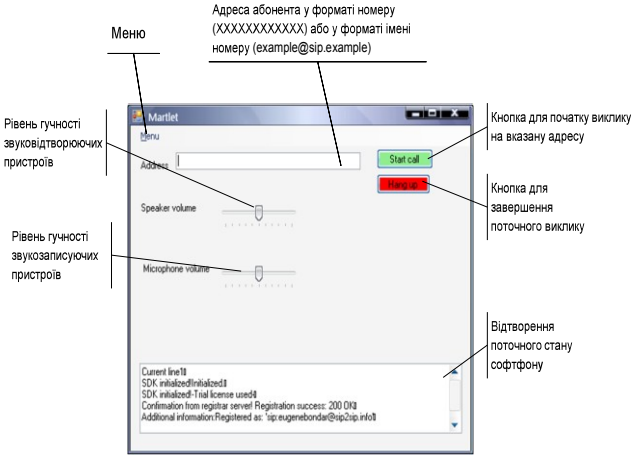

Рисунок 4 – Головна форма розробленого клієнта

При отриманні вхідного виклику з'являється форма зображена на рисунку 5, яка повідомляє про абонента який здійснює виклик, а також дозволяє прийняти чи відхилити дзвінок.

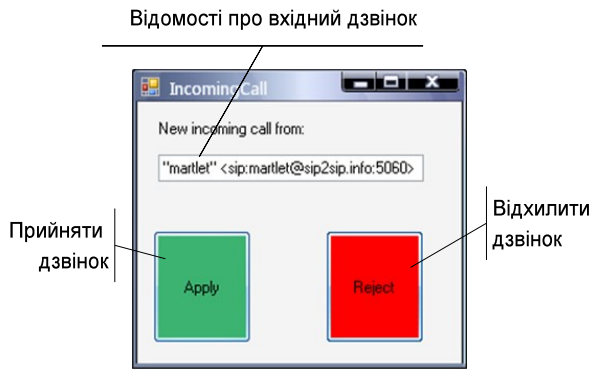

Рисунок 5 – Спливаюча форма при вхідному виклику

Зауважимо, новизна розробленого застосунку полягає у комплексному підході до захисту інформації. В розробленому програмному застосунку «Martlet» використовуються відкриті протоколи шифрування засновані на стандартах RFC. Це надає можливість взаємодіяти з програмним та апаратним забезпеченням сторонніх виробників. Також, у застосунку реалізована політика керування доступом на основі ролей (RBAC)

Захист IP-телефонії можна умовно поділити так: захист на рівні встановлення з'єднання, захист на рівні передачі медіа даних, розподіл прав користувачів. Зокрема, дані протоколу SIP, захищаємо за допомогою протоколу TLS. Використання протоколів TLS забезпечить конфіденційність адресата, та унеможливить відслідковування дзвінків. Передачу медіа даних захищаємо шляхом використання протоколів SRTP, SRTCP та ZRTP. Протокол ZRTP забезпечить узгодження ключів шифрування, SRTCP використовується для контролю медіа сесії, а SRTP відповідає за аутентифікацію, шифрування та пересилання медіа даних. Загальна схема роботи застосунку зображено на рис. 6.

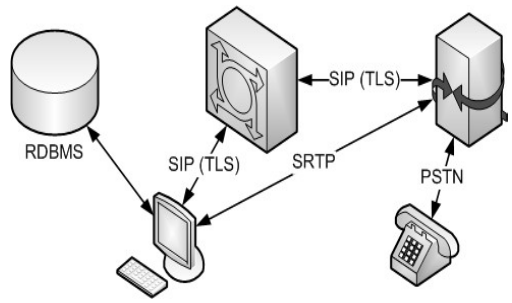

Рисунок 6 – Схема захищеного телефонного зв'язку

Як результат ми отримуємо захищене з'єднання, надзвичайно мобільну організацію зв'язку, можливість інтеграції з іншими мережевими та системними сервісами, можливість робити аналіз здійснених дзвінків та керувати доступом та правами клієнтів.

Список використаних джерел

1. Wendell Odom CCIE Routing and Switching Exam Certification Guide, 4th Edition / Wendell Odom, Rus Healy, Denise Donohue. – Cisco Press, 2009. – 1081 p.

2. Mazurczyk W. On Steganography in Lost Audio Packets [Електронний ресурс] / Wojciech Mazurczyk, Józef Lubacz, Krzysztof Szczypiorski// Warsaw University of Technology – Режим доступу: http://arxiv.org/ftp/arxiv/papers/1102/1102.0023.pdf.

3. Mazurczyk W. LACK – a VoIP steganographic method [Електронний ресурс] / Mazurczyk Wojciech, Lubacz Józef // Warsaw University of Technology. – Режим доступу: http://cygnus.tele.pw.edu.pl/~wmazurczyk/art/LACK_journal_final.pdf.

4. Mazurczyk W. Lost Audio Packets Steganography: The First Practical Evaluation [Електронний ресурс] / Wojciech Mazurczyk // Warsaw University of Technology. – Реж. доступу: http://arxiv.org/ftp/arxiv/papers/1107/1107.4076.pdf

5. Henning Schulzrinne, Jonathan Rosenberg, «A Comparison of SIP and H.323 for Internet Telephony» / Network and Operating System Support for Digital Audio and Video (NOSSDAV), Cambridge, England, July 1998.

6. Henning Schulzrinne, Jonathan Rosenberg, «Signaling for Internet Telephony»/ January, 1998.

7. Kundan Singh, Henning Schulzrinne, «Interworking between SIP/SDP and H.323» / Columbia University, May, 2000.

8. John Arquilla Networks and Netwars: The Future of Terror, Crime, and Militancy / John Arquilla, David Ronfeld. – RAND Corporation, 2001. – 376 p.

Надійшла до редакції 20.05.2016

Рецензент: д.т.н., професор Кваснікова В. П., Національний авіаційний університет, м. Київ.

Ю. Б. Коваленко, к.пед.н.

КОМПЬЮТЕРИЗОВАННАЯ СИСТЕМА ЗАЩИЩЕННОГО ПРИМЕНЕНИЯ НА ОСНОВЕ ТЕХНОЛОГИИ VOIP

Развитие электронной коммерции и заинтересованность технологии IP как единого транспорта для передачи информации любого вида позволили связать Интернет с традиционной телефонной сетью общего пользования и предложить клиентам персонализированное обслуживание и удобное средство общения. Разработано защищенное приложение, что в отличие от существующих поддерживает установку защищенного соединения и обеспечивает защиту медиа данных, при этом основывается на рекомендациях RFC, а значит, может свободно взаимодействовать с другими аппаратными и программными технологиями VoIP. В дополнение, в приложении реализовано управление доступом на основе ролей, что повышает безопасность и совершенствует возможности мониторинга деятельности пользователя.

Ключевые слова: *контролер конференций, технологии VoIP, сеть SIP с прокси-сервером.*

Yu Kovalenko, PhD

COMPUTERIZED SYSTEM IS PROTECTED APPLICATION TECHNOLOGY -BASED VOIP

The development of e-commerce and interest in IP technology as the only vehicle to transmit information of any kind made it possible to link the Internet with tradition-term public switched telephone network and offer customers personalized service and convenient means of communication. Developed protected software application that unlike existing supports establishing a secure connection and provides protection of media data, while based on the recommendations of RFC, and therefore can freely interact with other hardware and software technology VoIP. In addition, the application is implemented based access control roles, which increases safety and improves opportunities monitoring of the user.

Keywords: *Controller conferences, technology VoIP, network SIP proxy.*

УДК 004.89:531.7 (043.3)

Л. В. Кузьмич, к.т.н.

Національний університет водного господарства та природокористування, м. Рівне

СУЧАСНІ ТЕНДЕНЦІЇ СТВОРЕННЯ ПРИЛАДОВИХ СИСТЕМ ВИМІРЮВАННЯ МЕХАНІЧНИХ ВЕЛИЧИН

Обґрунтовано підходи щодо створення складних технічних виробів у вигляді приладових систем вимірювання механічних величин з застосуванням сучасних технології на основі теорії надійності, системного аналізу, штучного інтелекту, методів статистичного моделювання та ін. зі збереженням паритету між оптимальним рівнем експлуатаційної надійності даних виробів та їхньою економічністю.

Ключові слова: *виріб, приладова система, механічні величини, експлуатаційна надійність, інформаційно-вимірювальна система*

Постановка проблеми

Сучасні світові тенденції розвитку промисловості висувають на передній план питання забезпечення технічного рівня, якості, надійності та ефективності роботи складних технічних систем, яким властиві багатофункціональність, ієрархічність, складність конструкції.

В свою чергу, підвищення якості, надійності складає невід'ємну частину загальної задачі підвищення рівня промисловості та прискорення науково-технічного прогресу.

Одним з визначних факторів конкурентоспроможності складного виробу є створення нових наукових підходів щодо забезпечення якості виробу та забезпечення ефективного функціонування впродовж всіх етапів його життєвого циклу.

Сучасний рівень розвитку методологічних основ забезпечення якості, відповідного технічного рівня, надійності складних виробів