УДК 004.42

Р.Н.Квєтний
К.Є. Шелест

АКТУАЛЬНІСТЬ БЕЗПЕЧНОГО ЗВ'ЯЗКУ IP-ТЕЛЕФОНІЇ

Вінницький національний технічний університет

Анотація

У даній роботі розглянуто актуальність та аспекти забезпечення і покращення безпеки зв'язку IP телефонії.

Ключові слова: *зв'язок, шифрування, IP, аутентифікація, безпека.*

Abstract

In this work the relevance and aspects of ensuring and improving the security of IP telephony communications are considered.

Keywords: *communication, encryption, IP, authentication, security.*

Вступ

IP-телефонія поступово заміняє минулі способи організації телефонного зв'язку. З впевненістю можна припустити, що через пару років традиційна телефонія буде повністю витіснена своєю більш сучасною та функціональною альтернативою, що працює за протоколом IP. Цей напрямок по суті не використовується навіть традиційними виробниками, оскільки всі їх зусилля спрямовані тепер на IP-телефонію.

Дійсно, при розробці протоколу IP не приділялося належної уваги питанням інформаційної безпеки, однак з часом ситуація змінювалася, і сучасні програми, що базуються на IP, містять достатньо захисних механізмів. Рішення IP-телефонії неможливі без заходів безпеки: реалізації стандартних технологій аутентифікації і авторизації, контролю цілісності та шифрування і т.д.

Аспекти безпеки IP-телефонії

1) Телефонний апарат

В IP-телефонії, перш ніж телефон пошле сигнал на встановлення з'єднання, абонент повинен ввести свій ідентифікатор і пароль на доступ до апарату і його функцій. Така аутентифікація дозволяє блокувати будь-які дії сторонніх і не турбуватися, що чужі користувачі будуть дзвонити в інше місто або країну за ваш рахунок.

2) Встановлення з'єднання

Після набору номера сигнал на встановлення з'єднання надходить на відповідний сервер управління дзвінками, де здійснюється цілий ряд перевірок з точки зору безпеки. В першу чергу засвідчується справжність самого телефону - як шляхом використання протоколу 8о2.1х, так і за допомогою сертифікатів на базі відкритих ключів, інтегрованих в інфраструктуру IP-телефонії. Така перевірка дозволяє ізолювати несанкціоновано встановлені в мережі IP-телефони, особливо в мережі з динамічною адресацією.

3) Телефонна розмова

Прослуховування: зловмиснику не складає труднощів перехопити голосові дані за допомогою жучка. В IP-телефонії рішення цієї проблеми передбачалося з самого початку. Високий рівень

конфіденційності телефонного зв'язку забезпечують перевірені алгоритми і протоколи (DES, 3DES, AES, IPSec і т. П.) При практично повній відсутності витрат на організацію такого захисту - всі необхідні механізми (шифрування, контролю цілісності, хешування, обміну ключами і ін.) вже реалізовані в інфраструктурних елементах, починаючи від IP-телефону і закінчуючи системою управління дзвінками. Однак з шифруванням пов'язаний ряд моментів, про які необхідно пам'ятати, впроваджуючи інфраструктуру VoIP. По-перше, з'являється додаткова затримка внаслідок шифрування / дешифрування, а по-друге, ростуть накладні витрати в результаті збільшення довжини переданих пакетів. І те й інше вирішується шляхом застосування протоколу SecureRTP (RFC 3711); який дозволяє забезпечити ефективний захист розмови без зниження її якості.

4) Невидимий функціонал

Найперше і найпростіше, що можна зробити для підвищення захищеності телефонних переговорів, коли вони передаються по тій же кабельній системі, що і звичайні дані, - це сегментувати мережу за допомогою технології VLAN для усунення можливості прослуховування переговорів звичайними користувачами. Механізм VLAN реалізується комутаторами локальної мережі. Залежно від виробника комутуюче обладнання дозволяє задіяти і безліч інших механізмів безпеки, вже вбудованих в придбане мережеве обладнання та підвищують захищеність передачі голосових даних по протоколу IP.

5) Спілкування із зовнішнім світом

Для захисту елементів голосової інфраструктури від можливих несанкціонованих впливів можуть застосовуватися спеціалізовані рішення - міжмережеві екрани (MCE), шлюзи прикладного рівня (Application Layer Gateway, ALG) і прикордонні контролери сеансів (Session Border Controller). Зокрема, протокол RTP використовує динамічні порти UDP, відкриття яких на межсетевом екрані призводить до появи зяючої діри в захисті. Отже, міжмережевий екран повинен динамічно визначати використовувані для зв'язку порти, відкривати їх в момент з'єднання і закривати по його завершенні. Інша особливість полягає в тому, що ряд протоколів, наприклад SIP, інформацію про параметри з'єднання розміщують не в заголовку пакета, а в тілі даних. Тому пристрій захисту повинен бути здатний аналізувати не тільки заголовок, а й тіло даних пакета, виокремлюючи з нього всі необхідні для організації голосового з'єднання відомості.

Висновки

По-перше, необхідно подбати про захист адміністративного інтерфейсу. У звичайної телефонії доступ до АТС відкриває практично безмежні можливості несанкціонованого зміни конфігурації, перехоплення дзвінків і т. П. У розвинених серверах управління передбачені розширені функції для наділення системних адміністраторів тільки тими правами, які їм потрібні для виконання своїх обов'язків.

По-друге, потрібно забезпечити доступність і захист від атак «відмова в обслуговуванні». З вирішенням цієї проблеми допомагають впоратися як спеціальні системи захисту від атак DoS і DDoS, так і вбудовані в мережеве обладнання механізми

І нарешті, найголовніше Для безпеки IP-телефонії - розуміння всіх ризиків, пов'язаних з нею. Тільки в цьому випадку можна побудувати високоефективну і недорогу систему захисту голосових даних, переданих по єдиному кабелю - разом з файлами, електронною поштою та сторінками Web. LAN

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. IP и протоколы [Електронний ресурс]. Режим доступу: https://habrahabr.ru/post/342234/. – Назва з екрану.
2. Винниченко И. В. Телефония и безопасность / И. В. Винниченко. – СПб. : Питер, 2005. – 203 с. : ил.
3. Телефонная связь [Електронний ресурс]. Режим доступу: https://habrahabr.ru/post/456987/. – Назва з екрану.

Шелест Катерина Євгеніївна – студентка групи 1СІ-15б, факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, м. Вінниця, e-mail: shelestkt@gmail.com

Науковий керівник: ***Квєтний Роман Наумович*** – д-р. техн. наук, професор, завідувач кафедри АІВТ, Вінницький національний технічний університет, м. Вінниця.

Shelest Kateryna Y. - student of the group 1SE-15b, faculty of computer systems and automatics, Vinnytsia National Technical University, Vinnytsia, e-mail: shelestkt@gmail.com

Supervisor: ***Kvyetnyy Roman N.*** – Dr. Sc. (Eng.), Professor, Head of the Chair of Automation and Information Measuring Devices, Vinnytsia National Technical University, Vinnytsia