



МИФЫ О НЕЗАЩИЩЕННОСТИ IP-ТЕЛЕФОНИИ

IP-телефония все чаще и чаще начинает применяться в компаниях. Она повышает эффективность ведения бизнеса и позволяет осуществлять многие до этого невозможные операции (например, интеграцию с CRM и другими бизнес-приложениями, снижение издержек на построение и эксплуатацию телекоммуникационной инфраструктуры, создание эффективных Call-центров, снижение совокупной стоимости владения системой и т.п.). Однако, активное развитие IP-телефонии сдерживается тем, что вокруг этой технологии циркулирует много слухов о ее низкой безопасности. Компания Cisco Systems доказала, что это не так и данная публикация призвана развенчать сложившиеся мифы о незащищенности IP-телефонии.

ВВЕДЕНИЕ

Сразу надо заметить, что Cisco - единственный производитель, обеспечивающий защиту инфраструктуры IP-телефонии на всех ее уровнях, начиная от транспортной среды и заканчивая голосовыми приложениями. Это достигается внедрением решений в рамках инициативы Cisco Self-Defending Network. Высокий уровень защищенности решений Cisco Systems подтверждается и независимыми тестовыми лабораториями. В частности, журнал NetworkWorld и лаборатория Micercom (<http://www.nwfusion.com/reviews/2004/0524voipsecurity.html>) протестировали несколько решений по IP-телефонии и только решению Cisco присвоил максимально возможный рейтинг "SECURE" («защищенный»).

IP-ТЕЛЕФОНИЯ НЕ ЗАЩИЩАЕТ ОТ ПОДСЛУШИВАНИЯ РАЗГОВОРА

Решения IP-телефонии компании Cisco используют несколько технологий и механизмов, обеспечивающих конфиденциальность проводимых телефонных разговоров. Во-первых, это выделение голосового трафика в выделенный сегмент сети и разграничение доступа к голосовому потоку путем использования правил контроля доступа на маршрутизаторах и межсетевых экранах. Во-вторых, весь голосовой трафик может быть защищен от несанкционированного прослушивания с помощью технологии построения виртуальных частных сетей (VPN). Протокол IPSec позволяет защитить телефонный разговор, осуществляемый даже через сети открытого доступа, например, Интернет. И, наконец, компания Cisco реализовала в своих IP-телефонах специально разработанный для обеспечения конфиденциальности голосового потока протокол SecureRTP (SRTP), не позволяющий посторонним проникнуть в тайну телефонных переговоров.

IP-ТЕЛЕФОНИЯ ПОДВЕРЖЕНА ЗАРАЖЕНИЮ ЧЕРВЯМИ, ВИРУСАМИ И ТРОЯНЦАМИ

Для защиты инфраструктуры IP-телефонии от заражения различными вредоносными программами компания Cisco предлагает целый ряд защитных мер, позволяющих построить эшелонированную оборону, препятствующую не только внедрению, но и распространению червей, вирусов, троянских коней и других типов вредоносной активности. Первой линией обороны является применение межсетевых экранов и систем обнаружения и предотвращения атак, наряду с антивирусами компаний-партнеров компании Cisco, для разграничения доступа к инфраструктуре IP-телефонии.

Вторая линия обороны строится на использовании антивирусов и систем предотвращения атак на оконечных узлах, участвующих в инфраструктуре IP-телефонии – Cisco IP SoftPhone, Cisco CallManager, Cisco Unity, Cisco IP Contact Center (IPCC) Express, Cisco Personal Assistant, Cisco IP Interactive Voice Response и т.д.



Последняя по счету, но не последняя по важности линия обороны – инициатива Network Admission Control, предложенная компанией Cisco Systems. В рамках этой инициативы все несоответствующие политике безопасности (в т.ч. и с неустановленным антивирусным программным обеспечением) рабочие станции и сервера не смогут получить доступ к корпоративной сети и нанести ущерб ее ресурсам.

IP-ТЕЛЕФОНИЯ НЕ ЗАЩИЩАЕТ ОТ ПОДМЕНЫ ТЕЛЕФОНОВ И СЕРВЕРОВ УПРАВЛЕНИЯ

Для защиты от устройств, пытающихся замаскироваться под авторизованные IP-телефоны или несанкционированно подключенных к сетевой инфраструктуре, компания Cisco предлагает использовать не только уже упомянутые выше правила контроля доступа на маршрутизаторах и межсетевых экранах, но и развитые средства строгой аутентификации всех абонентов инфраструктуры IP-телефонии (включая сервер управления Call Manager), для подтверждения подлинности которых используются различные стандартизированные протоколы, включая RADIUS, сертификаты PKI X.509 и т.д.

ЗЛОУМЫШЛЕННИК С АДМИНИСТРАТИВНЫМИ ПРАВАМИ МОЖЕТ НАРУШИТЬ ФУНКЦИОНИРОВАНИЕ ИНФРАСТРУКТУРЫ IP-ТЕЛЕФОНИИ

В CallManager предусмотрены расширенные возможности по наделению различных системных администраторов только теми правами, которые им нужны для выполнения своих обязанностей. К таким правам могут быть отнесены - доступ к конкретным настройкам только на чтение, полное отсутствие доступа к ним, доступ на изменение и т.д.). Кроме того, все производимые администратором действия фиксируются в специальном журнале регистрации и могут быть проанализированы в любой момент в поисках следов несанкционированной активности.

Управление конфигурацией IP-телефонов и взаимодействие их с CallManager осуществляется по защищенному от несанкционированного доступа каналу, предотвращая любые попытки прочтения или модификации управляющих команд. Для защиты канала управления используются различные стандартизированные протоколы и алгоритмы – IPSec, TLS, SHA-1 и т.д.

CALLMANAGER НЕЗАЩИЩЕН, ПОТОМУ ЧТО УСТАНОВЛЕН НА ПЛАТФОРМЕ WINDOWS

Несмотря на то, что сервер управления инфраструктурой IP-телефонии CallManager установлен на платформе Windows, он не имеет присущих этой платформе слабых мест. Это связано с тем, что CallManager работает под управлением защищенной и оптимизированной версии Windows в которой:

- отключены все ненужные сервисы и учетные записи,
- установлены все необходимые и регулярно обновляемые «заплатки»,
- настроена политика безопасности.

Кроме того, CallManager дополнительно защищается специальными скриптами, входящими в дистрибутив и автоматизирующими процесс повышения уровня защищенности сервера управления инфраструктурой IP-телефонии. Дополнительный уровень защиты CallManager от вирусов, червей, троянских коней и других вредоносных программ и атак достигается за счет применения антивируса (например, McAfee, Symantec или TrendMicro) и системы предотвращения атак Cisco Secure Agent, которые блокируют все попытки злоумышленников вывести из строя основной компонент сегмента IP-телефонии.

IP-ТЕЛЕФОНИЮ ЛЕГКО ВЫВЕСТИ ИЗ СТРОЯ

Несмотря на то, что различные компоненты IP-телефонии потенциально подвержены атакам «отказ в обслуживании», решения компании Cisco Systems предлагают целый ряд защитных мер, предотвращающих как сами DoS-атаки, так и их последствия. Для этого можно использовать как встроенные в сетевое оборудование механизмы обеспечения информационной безопасности, так и дополнительные решения, предлагаемые компанией Cisco Systems:

- Разделение корпоративной сети на непересекающиеся сегменты передачи голоса и данных, что предотвращает появление в «голосовом» участке распространенных атак, в т.ч. и DoS.
- Применение специальных правил контроля доступа на маршрутизаторах и межсетевых экранах, защищающих периметр корпоративной сети и отдельные ее сегменты.
- Применение системы предотвращения атак на узлах Cisco Secure Agent.
- Применение специализированной системы защиты от DoS и DDoS-атак Cisco Guard и Cisco Traffic Anomaly Detector.
- Применение специальных настроек на сетевом оборудовании Cisco, предотвращающих подмену адреса, часто используемую при DoS-атаках, и ограничивающих полосу пропускания, не позволяющую вывести из строя атакуемые ресурсы большим потоком бесполезного трафика.

К IP-ТЕЛЕФОНАМ МОЖНО ОСУЩЕСТВИТЬ НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП

Сами IP-телефоны содержат целый ряд специальных настроек, препятствующих несанкционированному доступу к ним. К таким настройкам можно отнести, например, доступ к функциям телефона только после предъявления идентификатора и пароля или запрет локального изменения настроек и т.д.

С целью предотвращения загрузки на IP-телефон несанкционированно модифицированного программного обеспечения и конфигурационных файлов, их целостность контролируется электронной цифровой подписью и сертификатами X.509.

CALLMANAGER МОЖНО ПЕРЕГРУЗИТЬ БОЛЬШИМ ЧИСЛОМ ЗВОНКОВ

Максимальное число звонков в час на один сервер CallManager составляет до 100000 (в зависимости от конфигурации) и это число может быть увеличено до 250000 при использовании кластера CallManager. При этом в CallManager существуют специальные настройки, ограничивающие число входящих звонков необходимым значением. Кроме того, в случае потери связи с одним из CallManager'ов возможна автоматическая перерегистрация IP-телефона на резервном CallManager, а также автоматическая смена маршрута звонка.

В IP-ТЕЛЕФОНИИ ЛЕГКО СОВЕРШИТЬ МОШЕННИЧЕСТВО

Сервер управления инфраструктурой IP-телефонии CallManager содержит ряд возможностей, позволяющих снизить вероятность осуществления телефонного мошенничества в зависимости от его типа (кража услуг, фальсификация звонков, отказ от платежа и т.п.). В частности, для каждого абонента можно:

- заблокировать звонки как на определенные группы номеров, так и с них,
- заблокировать возможность переадресации звонков на различные типы номеров – городские, мобильные, междугородные, международные и т.д.,
- отфильтровывать звонки по различным параметрам,
- и т.д.

При этом все эти действия осуществляются независимо от того, с какого телефонного аппарата абонент осуществляет звонок. Это реализуется путем аутентификации каждого абонента, получающего доступ к IP-телефону. Если пользователь не проходит процесс подтверждения своей подлинности, то он может звонить только по заранее определенному списку телефонных номеров, например, в скорую помощь, милицию или внутренний отдел поддержки.

ТРАДИЦИОННАЯ ТЕЛЕФОНИЯ БОЛЕЕ ЗАЩИЩЕНА, ЧЕМ IP-ТЕЛЕФОНИЯ

Это самый распространенный миф, который существует в области телефонии. Традиционная телефония, разработанная десятилетия назад гораздо менее защищена новой и более совершенной технологии IP-телефонии. В традиционной телефонии гораздо легче осуществить подключение к чужому разговору, подмену номера, «наводнение» звонками и множество других угроз, некоторым из которых нет аналогов в IP-телефонии (например, war dialing). Защита традиционной телефонии



обеспечивается гораздо более дорогими средствами и механизмами, чем в IP-телефонии, в которой эти средства встроены в сами компоненты этой технологии. Например, для защиты от прослушивания традиционная телефония использует специальные устройства – скремблеры, централизованное управление которыми невозможно; не говоря уже стоимости их приобретения и установки перед каждым телефонным аппаратом.

ДОПОЛНИТЕЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

IP Communications Security Solution

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_package.html

SAFE: IP Telephony Security in Depth

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_white_paper09186a00801b7a50.shtml

Securing Voice in an IP Environment

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns391/c654/cdccont_0900aecd800dfd34.pdf

Cisco IP Telephony Solution

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns268/networking_solutions_package.html

Voice and IP Communications

<http://www.cisco.com/en/US/products/sw/voicesw/index.html>



Cisco Systems
Россия, 113054 Москва
бизнес центр “Риверсайд Тауэрз”
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр “Самал 2”
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр “Горайзон Тауэрз”
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on
Cisco Connection Online Web site at <http://www.cisco.com/>
<http://www.cisco.ru/>

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems Inc. All rights reserved. Printed in Russia. Cisco IOS is the trademark; and Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.