жим, что мы определили группу $G_l \simeq GL_2(p^{m_1})$ для $l \geq 1$. По условию насыщенности, конечная группа $< Z_{l+1}, L_{l+1}, G_l > \subset G_{l+1} \simeq GL_2(p^{m_{l+1}}) = GL_2(P^*_{l+1})$, где P^*_{l+1} подполе из P и $\left|P^*_{l+1}\right| = p^{m_{l+1}}$ по лемме (4). По построению

$$G_1 \subset G_2 \subset ... \subset G_l \subset G_{l+1} \subset ..., \bigcup_{i=1}^{\infty} G_l = G.$$

и $$P^*_1 \subset P ... \subset P^*_l \subset P^*_{l+1} \subset, \bigcup_{l=1}^{\infty} P^*_l = P.$$

Значит, $GL_2(P^*_1) \subset GL_2(P^*_2) \subset ... \subset GL_2(P^*_l) \subset ...$

и $\bigcup_{l=1}^{\infty} GL_2(P^*_l) = GL_2(P)$.

В силу изоморфизма $G_l \simeq GL_2(P^*_l)$, получаем, что $G = \bigcup_{l=1}^{\infty} G_l \simeq GL_2(P)$.

Теорема доказана.

Библиографические ссылки

1. *Шлепкин А. К.* Сопряженно бипримитивно конечные группы, содержащие конечные неразрешимые подгруппы // Сб. тезисов 3-й Междунар. конф. по алгебре. Красноярск, 1993. С. 363.

2. *Панюшкин Д. Н.* Группы Шункова, насыщенные прямыми произведениями различных групп : дис. ... канд. физ.-мат. наук. Красноярск, 2010.

3. *Shlyopkin A.* A Periodic groups saturated by the groups $GL_2(p^n)$ // Book of abstracts of the Intern. conf. on algebra. Kyiv, 2012. P. 144.

4. *Dichson L.* Linear groups. Leipzig : B. C. Neubner, 1901.

5. *Бусаркин В. М., Горчаков Ю. М.* Конечные расщепляемые группы. М. : Наука, 1968.

6. *Рубашкин А. Г., Филиппов К. А.* О периодических группах насыщенных $L_2 = (p^n)$ // Сиб. мат. журн. 2005. № 6. С. 1432–1438.

УДК 004.773.5

ЗАЩИЩЕННЫЙ ДОСТУП К СИСТЕМАМ ВИДЕОКОНФЕРЕНЦИИ*

К. Е. Шудрова[1], Р. В. Лебедев[2], В. Ю. Почкаенко[3]

[1]Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Россия, 660014, Красноярск, просп. им. газ. «Красноярский рабочий», 31. E-mail: shudrova87@mail.ru
[2]ОАО «Информационные спутниковые системы» имени академика М. Ф. Решетнева
Россия, 662972, г. Железногорск Красноярского края, ул. Ленина, 52
[3]Россия, Красноярск, ООО «НПП «Бевард»

Проводится анализ уязвимости «переполнение буфера» для программно-аппаратного комплекса «Метка привилегий». По методике CVSS строится вектор метрик, компоненты которого характеризуют уровень защищенности алгоритма. На основе полученных результатов авторами предлагается модифицировать существующий алгоритм.

Ключевые слова: видеоконференция, уязвимость, CVSS.

SECURE ACCESS TO VIDEO CONFERENCE SYSTEMS

K. E. Shudrova[1], R. V. Lebedev[2], V. Yu. Pochkaenko[3]

[1]Siberian State Aerospace University named after academician M. F. Reshetnev
31 “Krasnoyarskiy Rabochiy” prospect, Krasnoyarsk, 660014, Russia. E-mail: shudrova87@mail.ru
[2]JSC “Information Satellite Systems” named after academician M. F. Reshetnev
52 Lenin street, Zheleznogorsk, Krasnoyarsk region, 662972, Russia
[3] LLC “NPP” Bevard”, Krasnoyarsk, Russia

The authors present vulnerability analysis "buffer overflow" for software and hardware complex “The label of privileges”. By the CVSS procedure the metrics based vector is constructed, and its components characterize the level of security of the algorithm. Based on these results the authors suggest to modify the existing algorithm.

Keywords: video conferencing, vulnerability, CVSS.

* Исследование выполнено при поддержке Министерства образования и науки Российской Федерации, соглашение 14.132.21.1800 «Разработка алгоритмов и программных решений организации доступа к мультимедиа конференциям различных типов».

Увеличение пропускной способности каналов передачи информации сделало видеоконференции удобным средством общения. Видеоконференции проводятся для обмена опытом специалистами в различных областях, проведения корпоративных совещаний, также видеосвязь широко используется в образовательных целях. Видеоконференцсвязь – это технология, обеспечивающая обмен аудио- и видеоинформацией в режиме реального времени между участниками территориально распределенной группы. Начало распространения ВКС относится к 1980-м гг. – от телевизионных систем, обеспечивающих интерактивные контакты между удаленными партнерами [1]. Многие видеоконференции предназначены для узкого круга лиц, поэтому необходимо сделать доступ к видео защищенным, исключив возможность несанкционированного доступа (НСД).

Существует большое количество различных систем видеосвязи, обладающих своими достоинствами и недостатками, в данной работе рассматривается программно-аппаратный комплекс (ПАК) «Метка привилегий» [2].

«Метка привилегий». Особенностью ПАК является функция передачи конфиденциальной информации, встраиваемой в стандартный видеопоток стеганографическими методами. Программная часть комплекса представляет собой клиент-серверное приложение, аппаратная часть представлена в виде электронных ключей. В основе работы лежит добавление в пакеты специализированных меток. Модификации происходят на транспортном уровне: протокол TCP. Для внедрения меток в заголовок TCP пакета используется не обязательное поле опций (расположено со 160 по 192 бит) [3]. Добавляются метки трех типов: метка начала специального режима, метка специального пакета, метка последнего пакета.

В обычном режиме пакеты передаются непосредственно от источника адресату, минуя сервер. Перед предполагаемым началом специального режима администратор запускает службу на сервере, сеть переходит в режим ожидания. Принятый пакет проверяется на наличие метки начала специального режима, при положительном результате проверки сеть переходит в специальный режим.

В специальном режиме происходит проверка аутентификационной информации. Если она верна, осуществляется проверка метки специального пакета, при положительном результате пакет доставляется адресату. Затем происходит проверка метки последнего пакета, она означает, что необходимо снять метку начала специального режима, доставить последний пакет и перейти к обычной работе сети. Если аутентификационная информация неверна, пакеты отклоняются.

Клиент запускает службу на своем компьютере и с помощью аппаратного ключа переходит в режимы «источник-сервер» и «сервер-адресат». При отправке сообщений в пакет добавляется информация о пользователе и метка привилегии, скрытые данные, затем пакет отсылается. Принятое сообщение записывается в буфер. Согласно таблице стеганографических преобразований выделяются пакеты со скрытой информацией. Происходит сборка конфиденциальной информации.

На начальном этапе работы программы создается дуплексный канал (сокет), соединяющий два процесса – отправки и передачи данных. На стороне отправителя происходит накопление видеоданных и конфиденциального текста, затем происходит отправка видеоданных с пометкой в первом байте, указывающей тип данных – «видео», после этого отправляются текстовые данные с пометкой в первом байте – «текст». На стороне получателя осуществляется сборка информации и вывод пользователю на экран. Для кодирования видео используется технология MJPEG, после сжатия кадра скрытая информация встраивается путём замены отдельных байтов [4]. Позиции заменяемых байтов вычисляются с помощью секретного ключа.

Видеокодеки MPEG2 и MPEG4 обладают большей степенью сжатия, но занимают большее количество процессорного времени [5]. В разрабатываемой системе необходимо кодировать видео в реальном времени, а встраивание скрытой информации увеличивает время кодирования. Поэтому скорость работы алгоритма является важным параметром при выборе технологии кодирования. Стоит отметить, что MJPEG имеет меньшую степень сжатия, чем MPEG2 или MPEG4 [6], однако преимуществом видеокодека является скорость кодирования. Еще одно преимущество MJPEG перед MPEG2 и MPEG4 – свободная лицензия, она позволяет разрабатывать собственные алгоритмы на основе MJPEG без необходимости лицензирования. По перечисленным выше причинам в качестве основы для разработки собственного алгоритма стегокодирования был выбран MJPEG.

Так как ПАК «Метка привилегий» предназначен для организации защищенного канала передачи конфиденциальной информации, необходимо оценить уровень защищенности системы [7].

Оценка уязвимостей ПАК «Метка привилегий». Оценка актуальных уязвимостей производится по системе CVSS. CVSS (Common Vulnerability Scoring System – Общая система оценки уязвимостей) представляет собой набор методов, позволяющих строить оценки уязвимостей компонент информационных систем (ИС) в едином пространстве мер. Объектом применения этих методов являются единичные (атомарные) уязвимости системного и прикладного программного обеспечения и связанных с ними протоколов взаимодействия. Получение в конечном итоге оценок в рамках единой шкалы делает возможным применять методы автоматизации при решении задач моделирования поведения злоумышленника при компрометации ИС и комплексной оценки информационных рисков для ее активов. Общие принципы построения оценок приведены ниже.

Всякому техническому ресурсу ИС ставится в соответствие абстрактный вектор v – вектор метрик.

$$v = (AV, AC, AU, C, I, A)$$

Этот вектор состоит из шести компонент, каждая из которых характеризует определенный параметр безопасности. Значения компонент приведены в таблице.

Компоненты вектора метрик

Компонента	Значения	Смысл значений
AV	*L* =0,395 *A* = 0,646 *N* = 1	Access vector: характер доступа для использования уязвимости. L (Local) – локально на целевой системе; A (Adjacent network) – изнутри сетевой зоны, в которой расположена целевая система; N (Network) – из любой сообщающейся сети. Чем «дальше» злоумышленник может находиться для совершения атаки, тем выше степень уязвимости
AC	*H* = 0,35, *M* = 0,61, *L* = 0,71.	Access complexity: уровень сложности использования уязвимости при условии успешного доступа злоумышленника к целевой системе. H (High) – высокий; M (Medium) – средний; L (Low) – низкий. Чем ниже уровень сложности, тем выше степень уязвимости ресурса
AU	*M* = 0,45 *S* = 0,56 *N* = 0,704	Authentication: параметр, характеризующий особенности аутентификации субъекта при доступе к уязвимому ресурсу. Данный параметр не отражает степень сложности аутентификации, а определяет необходимое количество раз проведения этой процедуры. M (Multiple) – многократная аутентификация, S (Single) – единовременная аутентификация, N (None) – без аутентификации. Чем меньше необходимое число процедур аутентификации требуется при использовании ресурса, тем выше степень его уязвимости
C	*N* = 0 *P* = 0,275 *C* = 0,66	Confidentiality impact: параметр, определяющий степень влияния уязвимого ресурса на конфиденциальность информационного актива (защищаемой информации, сетевого сервиса и пр.). N (None) – уязвимость не влияет на конфиденциальность; P (Partial) – частичное влияние; C (Complete) – непосредственное (полное) влияние на конфиденциальность. Чем выше степень влияния ресурса на конфиденциальность информационного актива, тем более уязвимым он считается
I	*N* = 0 *P* = 0,275 *C* = 0,66	Integrity ipmact: параметр, определяющий степень влияния уязвимого ресурса на целостность информационного актива. N (None) – уязвимость не влияет на целостность; P (Partial) – частичное влияние; C (Complete) – непосредственное (полное) влияние на целостность. Чем выше степень влияния ресурса на целостность информационного актива, тем более уязвимым он считается
A	*N* = 0 *P* = 0,275 *C* = 0,66	Availability ipmact: параметр, определяющий степень влияния уязвимого ресурса на доступность информационного актива. N (None) – уязвимость не влияет на доступность; P (Partial) – частичное влияние; C (Complete) – непосредственное (полное) влияние на доступность. Чем выше степень влияния ресурса на доступность информационного актива, тем более уязвимым он считается

Из таблицы видно, что каждая компонента вектора метрик *v* может принимать одно из трех различных значений. Из этого следует, что все множество векторов метрик *V* имеет конечную мощность |*V*|=3^6=729, которая характеризует количество различимых в рамках CVSS объектов ИС с точки зрения их уязвимостей [8].

Оценочная мера *S* уязвимости объекта ИС вычисляется из значений компонент вектора метрик *v* согласно формуле (2). Диапазон ее значений ограничен интервалом чисел от 0 до 10 с одной значащей цифрой в дробной части.

$$S = (0{,}6*\text{Impact} + 0{,}4 \cdot \text{Exploitability} - 1{,}5) \cdot f(\text{Impact}),$$
$$\text{Impact} = 10{,}41 \cdot (1 - (1 - C) \cdot (1 - I) \cdot (1 - A)),$$
$$\text{Exploitability} = 20 \cdot AV \cdot AC \cdot AU, \qquad (2)$$
$$f(\text{Impact}) = 0, \text{ если Impact} = 0$$
$$\text{и } f(\text{Impact}) = 1{,}176, \text{ если Impact} <> 0$$

Таким образом, уязвимость всякого объекта ИС, описанная в форме вектора метрик, может быть оценена по единой шкале независимо от ее природы и свойств. Полученная оценка позволяет судить о степени уязвимости рассматриваемого объекта ИС в рамках анализа защищенности ИС в целом [9].

Анализ проводится отдельно для каждой уязвимости, в данной статье рассматривается уязвимость переполнения буфера сервера. По таблице вычисляются шесть основных характеристик, результаты приведены ниже:

1. Access vector: характер доступа для использования уязвимости (*AV*) – *N* (Network) – из любой сообщающейся сети. *N* = 1.

2. Access complexity: уровень сложности использования уязвимости при условии успешного доступа злоумышленника к целевой системе (*AC*) – *H* (High) – высокий. *H* = 0,35.

3. Authentication: параметр, характеризующий особенности аутентификации субъекта при доступе к уязвимому ресурсу. Данный параметр не отражает степень сложности аутентификации, а определяет необходимое количество раз проведения этой процедуры (*AU*) – S (Single) – единовременная аутентификация. *S* = 0,56.

4. Confidentiality impact: параметр, определяющий степень влияния уязвимого ресурса на конфиденциальность информационного актива (защищаемой ин-

формации, сетевого сервиса и пр.) (*C*) – *N* (None) – уязвимость не влияет на конфиденциальность. *N* = 0.

5. Integrity ipmact: параметр, определяющий степень влияния уязвимого ресурса на целостность информационного актива (*I*) – *C* (Complete) – непосредственное (полное) влияние на целостность. *C* = 0,66.

6. Availability ipmact: параметр, определяющий степень влияния уязвимого ресурса на доступность информационного актива. *C* (Complete) – непосредственное (полное) влияние на доступность. *C* = 0,66.

Для компонент вектора были получены следующие результаты: *AV* = 1; *AC* = 0,35; *AU* = 0,56; *C* = 0; *I* = 0,66; *A* = 0,66. Используя эти значения, произведем дальнейшие вычисления по формуле (2):

$$\text{Impact} = 10{,}41 \cdot (1 - (1 - C) \cdot (1 - \text{I}) \cdot (1 - A)) = 10{,}41 \cdot (1 - (1 - 0) \cdot (1 - 0{,}66) \cdot (1 - 0{,}66)) = 9{,}207,$$

$$\text{Exploitability} = 20 \cdot AV \cdot AC \cdot AU = 20 \cdot 1 \cdot 0{,}35 \cdot 0{,}56 = 3{,}92,$$

$$f(\text{Impact}) = 1{,}176, \text{ так как Impact} > 0$$

$$S = (0{,}6 \cdot \text{Impact} + 0{,}4 \cdot \text{Exploitability-1,5}) \cdot f(\text{Impact}) = 6{,}576,$$

Попытаемся улучшить данный алгоритм с помощью введения многократной аутентификации. Из всех компонент вектора при этом изменится только параметр *AU* = 0,45. Показатели Impact и *f*(Impact) останутся прежними, Impact = 9,207, *f*(Impact) = 1,176. По формуле (2) вычислим остальные показатели:

$$\text{Exploitability} = 20 \cdot AV \cdot AC \cdot AU = 20 \cdot 1 \cdot 0{,}35 \cdot 0{,}45 = 3{,}15,$$

$$S = (0{,}6 \cdot \text{Impact} + 0{,}4 \cdot \text{Exploitability-1,5}) \cdot f(\text{Impact}) = 6{,}214,$$

Также улучшить защищенность можно с помощью изменения параметра *AV* – для этого сервер и клиенты должны располагаться в одной локальной сети, *AV* = 0,646. Оставим неизменной однократную аутентификацию и произведем вычисления по формуле (2):

$$\text{Impact} = 9{,}207,$$

$$\text{Exploitability} = 20 \cdot AV \cdot AC \cdot AU = 20 \cdot 0{,}646 \cdot 0{,}35 \cdot 0{,}56 = 2{,}532,$$

$$f(\text{Impact}) = 1{,}176, \text{ так как Impact} > 0$$

$$S = (0{,}6 \cdot \text{Impact} + 0{,}4 \cdot \text{Exploitability-1,5}) \cdot f(\text{Impact}) = 5{,}923.$$

Итак, рассмотрена оценка уязвимости переполнения буфера ПАК «Метка привилегий» по системе CVSS. При неизменном алгоритме для этой уязвимости *S* = 6,576 по шкале от 0 до 10. Этот показатель является относительным и рассматривается в сравнении. Анализ таблицы показал, что *S* можно улучшить двумя способами: введением многократной аутентификации (*S* = 6,214) и применением алгоритма для локальной сети (*S* = 5,923). Смысл параметра *S* сводится к следующему: чем ниже числовое значение параметра, тем больше система защищена от рассматриваемой уязвимости. По результатам проведенных вычислений можно сказать, что ПАК «Метка привилегий» по возможности лучше применять в локальной сети, в остальных случаях повышение защищенности от переполнения буфера достигается введением модификации – многократного проведения аутентификации клиентов. Ведется работа по анализу других уязвимостей и доработке ПАК в соответствии с полученными результатами.

Библиографические ссылки

1. *Синепол В. С, Цикин И. А.* Системы компьютерной видеоконференцсвязи. Серия изданий «Связь и бизнес», М. : ООО «Мобильные телекоммуникации», 1999.

2. Организация защищенного канала передачи информации // Программные продукты и системы. 2012. № 3. С. 142–147.

3. Протокол TCP: перевод RFC: 793 [Электронный ресурс]. URL: http://citforum.ru/internet/tifamily/tcpspec.shtml (date of visit: 08.03.2013).

4. *Cox I. J., Kilian J., Leighton T., Shamoon T. G.* Secure spread spectrum watermarking for images, audio and video // Proceedings of the IEEE International Conference on Image Processing. 1996. P. 243–246.

5. MPEG-2 Generic coding of moving pictures and associated audio information [Электронный ресурс]. URL: http://mpeg.chiariglione.org/standards/mpeg-2/mpeg-2.htm (date of visit: 08.03.2013).

6. MPEG-2 Overview [Электронный ресурс]. URL: http://www.erg.abdn.ac.uk/future-net/digital-video/mpeg2.html (date of visit: 08.03.2013).

7. *Шудрова К. Е., Томилина А. И.* Проблемы информационной безопасности при организации видеоконференций // Актуальные проблемы авиации и космонавтики : материалы XVI Всерос. науч.-практ. конф. В 2 т. СибГАУ. Красноярск, 2012. Т. 2. С. 693–694.

8. *Лебедев Р. В.* Исследование системы оценок уязвимостей объектов информационных систем // Актуальные проблемы авиации и космонавтики : материалы VIII Всерос. науч.-практ. конф. СибГАУ. Красноярск, 2012.

9. *Лебедев Р. В.* Методика формирования исходных данных для моделирования сетевых атак // Актуальные проблемы авиации и космонавтики : материалы XVI Всерос. науч.-практ. конф. В 2 т. СибГАУ. Красноярск, 2012. Т. 2. С. 663–665.