Кібербезпека

УДК 004.056.5.057.4 (083.94)

Маркуця Віктор Григорович
студент факультету кібербезпеки,
комп'ютерної та програмної інженерії
Національного авіаційного університету
Маркуця Виктор Григорьевич
студент факультета кибербезопасности,
компьютерной и программной инженерии
Национального авиационного университета
Markutsya Victor
Student of Cyber Security, Computer and Software Engineering
National Aviation University

ДОСЛІДЖЕННЯ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ З ТОЧКИ ЗОРУ ЗАХИСТУ ІНФОРМАЦІЇ
ИССЛЕДОВАНИЕ ПРОТОКОЛОВ АУТЕНТИФИКАЦИИ С ТОЧКИ ЗРЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ
INVESTIGATION OF AUTHENTICATION PROTOCOLS FROM THE POINT OF VIEW OF INFORMATION SECURITY

Анотація. *У роботі розроблено методичні рекомендації щодо використання сучасних методів та засобів автентифікації до сучасних міжнародних стандартів з детальним відпрацюванням основних етапів проведення автентифікації, відпрацювання технології, запропонованої у стандартах Kerberos, SSL .*

Запропоновані підходи можуть бути використані при розробці, впровадженні та експлуатації комплексної системи захисту інформації на підприємствах та організаціях різних форм власності.

Можливі напрямки розвитку цієї роботи пов'язані з виконанням досліджень щодо удосконалення методів та засобів автентифікації взагалі, зокрема з використання криптографічних механізмів.

Ключові слова: *протоколи автентифікації, автентифікація, захист протоколів автентифікації, інформаційно-комунікаційні системи.*

Аннотация. *В работе разработаны методические рекомендации по использованию современных методов и средств аутентификации к современным международным стандартам с детальной отработкой основных этапов проведения аутентификации, отработки технологии, предложенной в стандартах Kerberos, SSL . Предложенные подходы могут быть использованы при разработке, внедрении и эксплуатации комплексной системы защиты информации на предприятиях и организациях различных форм собственности. Возможные направления развития этой работы связаны с выполнением исследований по совершенствованию методов и средств аутентификации вообще, в частности по использованию криптографических механизмов.*

Ключевые слова: *протоколы аутентификации, аутентификация, защита протоколов аутентификации, информационно-коммуникационные системы.*

Summary. *In this paper, developed guidelines for the use of modern methods and means of authentication to modern international standards with detailed testing of the main stages of authentication, testing technology proposed in the standards Kerberos, SSL. The proposed approaches can be used in the development, implementation and operation of a comprehensive system of information security in enterprises and organizations of various forms of ownership. Possible directions of development of this work are associated with the implementation of research on improving methods and means of authentication in*

General, in particular on the use of cryptographic mechanisms.

Key words: *authentication protocols, authentication, protection of authentication protocols, information and communication systems.*

Постановка проблеми. Особливу важливість останнім часом набуває забезпечення негласності і дистанційності роботи систем контролю доступу у різних сферах їх застосування (в авіації – диспетчери, оператори, енергетичних системах, банківській та інших сферах).

У зв'язку з цим можна зробити висновок, що тема статті, присвячена розробці рекомендацій щодо використання сучасних методів та засобів при проведенні ідентифікації та аунтентифікації в сфері інформаційної безпеки, є актуальної науковою задачею.

Формулювання цілей статті (постановка завдання) є виявлення особливостей побудови та використання сучасних методів і засобів автентифікації в сфері інформаційної безпеки.

Виклад основного матеріалу. Вивчався протокол автентифікації SSH-2.0, з метою аналізу стійкості останнього до загроз типу 31-39. У якості дослідного району виступала локальна мережа із 50 робочих станцій. У дослідженні «брало" участь дві робочі станції (зловмисник, клієнт), та сервер автентифікації.

Робоча станція клієнта знаходилась під управлінням операційної системи Microsoft Windows 2008, для проведення SSH сесій використовувався програмний пакет PuTTY v.052.

Робоча станція зловмисника знаходилась під управлінням операційної системи Microsoft Windows 2008, або FREE-BSD 4.5. Зловмисник використовував наступне програмне забезпечення: утиліта для формування TCP та ARP пакетів nemesis-tcp та nemesis-arp, аналізатор мереженого трафіку tcpdump, утиліта для повтору трафіку tcpreplay, аналізатор

мереженого трафіку "IRIS v3.8", програмний пакет XSpider.

Сервер автентифікації знаходився під управлінням операційної системи FREE-BSD 4.5.

- Реалізація загрози (модифікація та поміхи в обслуговуванні).

З метою виведення із ладу сервера автентифікації (відмова в обслуговуванні), серверу автентифікації посилалась необмежена кількість TCP-пакетів, що ініціалізують запит на проведення автентифікації. При цьому проводилась підміна мереженої IP та MAC адреси відправника.

while true

do

nemesis-tcp -x 1464 -y 22 -f-fS/-w 16384 -a 0 -s 2137822097 -u 0 -S 10.101.1.34 -D 10.101.1.69 -t 00 -F O -T 255

-F 0 -d edO -H 00:02:44:32:49:E6 -M 00:02:B3:61:AA:FC

done

Спроба реалізації цієї загрози виявилась невдалою. У сервера залишилась можливість для подальшої нормальної роботи.

Атака проводилась в умовах повного контролю мереженого трафіку зловмисником. Зловмисник " вклинював" свій пакет підчас проведення процесу автентифікації. Через те, що довжина пакета була некоректною клієнт отримував відповідь сервера:

"Received disconnect from 10.101.1.34: Bad packet length 1718969195.**",** та зв'язок розривався. Отже атака виявилась успішною, що приводило до переривання процесу автентифікації.

Реалізація загрози 32 (розкриття змісту потоку інформації) виявилась успішною лише наполовину, а саме для уточнення значень чисел "Sequence number" і "Acknowledgement number", які предаються у TCP- пакстах при обміні автентифікаційною інформацією. Знання цих чисел, як виявилось раніше, є досить корисним.

Виявилось можливим перехоплення зашифрованих пакетів якоїсь конкретної сесії, що теоретично не дозволяє розшифрувати дані передані під час сесії, якщо тільки: їх можна розшифрувати без сесійного ключа (session key), який використовується для шифрування в даній сесії. Взагалі це було би еквівалентно взлому всього алгоритму шифрування,

Можна використати яку-небудь вразливість, присутню або на клієнті, або на сервері, для отримання session key. Далі використати його для розшифрування даних в прихваченій сесії, використовуючи конкретну реалізацію криптоалгоритма.

Взагалі поки-що не знайдено вразливостей у протоколі обміну ключами SSH-2.0. Вразливість знайдена у протоколі 1.5 (існує атака "Bleichenbacher" на протокол обміну ключами версії 1.5). Тобто успішна реалізація загрози типу 32, на даний час, еквівалентна взлому самого алгоритму шифрування.

З огляду на те, що протокол автентифікації «короткий" (тобто кількість кроків при реалізації автентифікаційного обміну є малою), в умовах у яких проводилось дослідження протоколу не вдалось реалізувати практично загрози: невизнання участі, відмова від авторства, відмова від одержання. Можлива практична реалізація цих загроз є більш реальною при критичній завантаженості мережі та самої дослідної ділянки.

Реалізація загрози типу фальсифікація.

Вдалось фальсикувати пакет у якому міститься пароль користувача у зашифрованому виді, так що сервер сприйняв його як пакет надійшовший від користувача, який якраз у цей момент проходив автентифікацію, при цьому клієнт отримував відповідь від сервера: " Access denied". Атака була реалізована наступним чином:

nemesis-tcp -x 1483 -y 22 -f-fA/-fP/-w 17168 -s 336247539 -a 1391757490 -S 10.101.1.34 -D 10.101.1.69 -d edO - H 00:02:44:32:49:E6 -M

00:02:B3:61:AA:FC

Найбільшою проблемою при такому виді атаки - це з'ясування чисел "Sequence number" і "Acknowledgement number", для цього необхідно мати можливість прослуховувати трафік між клієнтом та сервером.

Для реалізації можливості прослуховування мереженого трафіку доцільним є проведення ARP-атаки:

nemesis-arp -S 10.101.1.x -D 10.101.1.y -h yy:yy:yy:yy:yy:yy -т xx:xx:xx:xx:xx:xx -d edO -H yy:yy:yy:yy:yy:yy -M xx:xx:xx:xx:xx:xx;

Де 10.101.1.x та xx:xx:xx:xx:xx:xx - IP та MAC адреси «клієнта-жертви", а 10.101.1.y - адреса сервера автентифікації , yy:yy:yy:yy:yy:yy - MAC адреса зловмисника. Далі доцільним є використання проксі- сервера для найбільш ефективного втручання в сесії автентфікації. Проте реалізація ARP-атаки не є завжди можливою. Політика безпеки та налаштування мережі, де проводились досліди, це дозволяла.

- Реалізація загрози підміна після автентифікації є неможливою через відсутність сеансового ключа у зловмисника. Та навіть при наявності сеансового ключа через те, що мережеві адреси зловмисника та клієнта різні, зловмисник отримував повідомлення: "Network error: Software caused connection abort". За таких умов зловмиснику доведеться взагалі «викинути" клієнта із мережі та здійснити підміну мереженої адреси (IP та MAC). Тобто для успішної реалізації цієї загрози зловмисник повинен попасти в "ідеальні" для нього умови, а це означає, що протокол стійкий до загрози 39.

Аналіз результатів досліджень. Основні результати досліджень

Загрози	Результат
Модифікація та завади в обслуговуванні	Загроза реалізована успішно двома способами за умов повного контролю трафіку, та за умови прослуховування трафіку зловмисником. Стійкість протоколу від даного типу загроз залежить від архітектури мережі, та додаткового «захисного" програмного забезпечення яке використовують робочі станції та сервер.
Розкриття змісту інформації	Загроза реалізована успішно тільки частково - вдалось одержати інформацію для подальшої реалізації загрози 31. Стійкість протоколу, від даного типу загроз, залежить від безпеки зберігання сесійного ключа на рівні робочої станції та сервера, а також від тих самих обставин, що і у попередньому випадку.
Невизнання участі	Стійкість протоколу до даного типу загроз була підтверджена для умов у яких проводились дослідження. Проте, можливо, протокол вразливий до даного типу загроз при критичній завантаженості мережі та самої дослідної ділянки.
Відмова від авторства	Стійкість протоколу до даного типу загроз була підтверджена для умов у яких проводились дослідження. Проте, можливо, протокол вразливий до даного типу загроз при критичній завантаженості мережі та самої дослідної ділянки.
Відмова від одержання	Стійкість протоколу до даного типу загроз була підтверджена для умов у яких проводились дослідження. Проте, можливо, протокол вразливий до даного типу загроз при критичній завантаженості мережі та самої дослідної ділянки.
Фальсифікація	Протокол виявився вразливим до атак такого типу. Стійкість протоколу від даного типу загроз залежить від архітектури мережі, та додаткового «захисного" програмного забезпечення яке використовують робочі станції та сервер.
Вимушена затримка	Загроза була реалізована успішно в умовах повного контролю зловмисником над мереженим трафіком.
Відбиття передачі	Аналогічно до попереднього випадку.
Підміна після автентифікації	Стійкість протоколу, від даного типу загроз, залежить від безпеки зберігання сесійного ключа на рівні робочої станції та сервера.

Стійкість протоколу до даного виду загроз при проведенні практичних досліджень на досліджуваній ділянці не підтверджена.

За результатами досліджень протокол протокол автентифікації SSH-2.0 можливо вважати безпечним лише за умов:

- При наявності додаткового "захисного" програмного забезпечення на кінцях автентифікаційного обміну (наприклад міжмережеві екрани);
- При певній архітектурі мережі, що унеможливлює пасивний чи активний контроль мереженого трафіку, без використання додаткових апаратних чи програмних засобів сервера та робочої станції;
- При використанні відповідного мереженого обладнання, що робить неможливим підміну мереженої адреси зловмисником.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі. Для проведення практичних досліджень було створено дослідний район для проведення випробувань протоколу SSH 2.0. У межах даного району практично реалізовано наступні загрози для протоколу: модифікація та поміхи в обслуговуванні, розкриття змісту потоку інформації, фальсифікація, вимушена затримка, відбиття передачі, підміна після автентифікації.

За результатами проведених теоретичних та практичних досліджень визначено, що використання в межах сучасних інформаційно-телекомунікаційних системах захищених протоколів мереженої автентифікації можливе за умов забезпечення комплексу вимог апаратного, програмного забезпечення робочих станцій, серверів системи, здійснення заходів щодо забезпечення безпеки ключів криптографічного захисту, які використовуються при реалізації криптоалгоритмів мережевої автентифікації.

Для подальших теоретичних та практичних досліджень пропонується розробити критерії оцінки протоколів автентифікації, та зайнятись дослідженням протоколів мережевої автентифікації, що використовуються у мережевому обладнанні фірми "Nortel", у межах дослідного району.• При реалізації загрози вимушена затримка протокол автентифікації повів себе досить "коректно". Затримці підлягала автентифікаційна інформація пароль

та логін. При затримці пакетів на час, більший порядку 3-ьох хвилин зв'язок із сервером обривався та клієнт отримував повідомлення: "Network error: Software caused connection abort". При затримці на менший час процес автентифікації проводився далі, та була можлива подальша коректна робота.

Під час реалізації загрози відбиття передачі зв'язок із сервером обривався, та клієнт отримував повідомлення: "Network error: Software caused connection abort".

Література

1. Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій. К.: ДУІКТ, 2006.
2. Галицький А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – аналіз технологий и синтез решений. М.: ДМК Пресс, 2004.
3. Глинских А. Мировой рынок систем електронного документооборота // Информационный бюллетень Jet Info. 2002. № 8.
4. Закон України "Про електронні документи та електронний документообіг" від 22 травня 2003 р. № 851-IV.
5. Закон України "Про електронний цифровий підпис" від 22 травня 2003 р. № 852-IV.
6. Информационная Безопасность открытых систем: учебник для вузов. В 2-х томах. Том 1 – Угрозы уязвимости, атаки и подходы к защите / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. М.: Горячая линия-Телеком, 2006.
7. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом ДСТЗІ СБ України від 26.07. 99 р. № 22.