МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут комп`ютерних систем і технологій
"Індустрія 4.0" ім. П.М. Платонова
Факультет Комп`ютерної інженерії, програмування та кіберзахисту

XX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина І.

Одеса

21-22 квітня 2020 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XX Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Частина І. Одеса, 21-22 квітня 2020 р. - Одеса, Видавництво ОНАХТ, 2020 р. - 240 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані по секціях кафедри інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНАХТ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м. Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут».

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри КІ ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

СЕКЦІЯ № 1

Комп'ютерні науки

Тематичні напрями:

МАТЕМАТИЧНЕ І КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СКЛАДНИХ ПРОЦЕСІВ

УПРАВЛІННЯ, ОБРОБКА ТА ЗАХИСТ ІНФОРМАЦІЇ

НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ПРОГРАМНИХ КОМПЛЕКСІВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ

ОДЕСЬКОЇ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ХАРЧОВИХ ТЕХНОЛОГІЙ

Список
скорочень організацій, представники яких взяли участь у конференції

Таблиця 1

Скорочення	Повна назва організації
АУПРБ	Академия управления при Президенте Республики Беларусь
БГЄУ	Белорусский государственный экономический университет
ВНТУ	Вінницький національний технічний університет
ДДПУ	ДВНЗ «Донбаський державний педагогічний університет»
УДХТУ	ДВНЗ «Український державний хіміко-технологічний університет»
ДДТУ	Дніпровський державний технічний університет
ДДМА	Донбаська державна машинобудівна академія
ДНТУ	Донецький національний технічний університет
ДНУ	Донецький національний університет ім. Василя Стуса
ІФНТУНГ	Івано-Франківський національний технічний університет нафти і газу
ІІТЗН	Інститут інформаційних технологій і засобів навчання НАПН України
ІТТНАН	Інститут технічної теплофізики НАН України
КНУ	Київський національний університет імені Тараса Шевченка
НТУУ "КПІ"	Національний технічний університет «Київський політехнічний інститут»
КПАІТ	Коледж промислової автоматики та інформаційних технологій ОНАХТ
КДПУ	Криворізький державний педагогічний університет
НУ"ПП"	Національний університет «Полтавська політехніка імені Юрія Кондратюка»
НТУ «ХПІ»	Национальный технический университет "Харьковский политехнический институт"
ОНПУ	Одеський національний педагогічний університет ім.Ушінского
ОНАХТ	Одеська національна академія харчових технологій
ОНПУ	Одеський національний політехнічний університет
ОНУ	Одеський національний університет імені І. І. Мечникова
ПДАТУ	Подільський державний аграрно-технічний університет
РДГУ	Рівненський державний гуманітарний університет
СКХП	Сумський коледж харчової промисловості НУХТ
ТЛіАЛ	Технічний ліцей імені Анатолія Лигуна, Національний технічний університет «Дніпровська політехніка»
УАД	Українська академія друкарства
УДПУ	Уманський державний педагогічний університет імені Павла Тичини
ХНУ	Хмельницький Національний Університет
ХНУРЕ	Харківський національний університет радіоелектроніки
ЦУНТУ	Центральноукраїнський національний технічний університет
ЧНУ	Чорноморський національний університет ім. Петра Могили
IAE	Institute of Automation and Electrometry of the Siberian Branch Russian Academy
VNTU	Vinnytsia National Technical University

Список використаних джерел

1. Лимаренко В. В. Інформаційна система підтримки рішень для автоматизації створення технологічних процесів механообробки деталей високоточного обладнання: дисертація канд. техн. наук, Національний технічний університет «Харківський політехнічний інститут». Харків, 2019.
2. Харламов Ю.О., Романченко О.В., Міцик А.В. Міцність зчеплення детонаційно-газових покриттів на основі карбідів вольфраму та хрому. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2019, № 1 (249). С. 99-107.
3. Ворона Т.В. Підвищення зносостійкості сталевих газотермічних покриттів електроконтактною обробкою з використанням вуглецевовмісних наповнювачів: дисертація канд. техн. наук, Національна академія наук України, Інститут надтвердих матеріалів ім. В.М. Бакуля. Київ, 2016.

АНАЛІЗ СПОСОБІВ ЗАХИСТУ ОБМІНУ ПОВІДОМЛЕННЯМИ В МОБІЛЬНИХ ДОДАТКАХ

Соловйов Е.Г., студент 556 гр.,
Керівник: Шестопалов Сергій Вікторович, к.т.н., доцент
Одеська національна академія харчових технологій

В епоху коли конфіденційність комунікації, як ніколи важлива, нема нічого дивного в бажанні користувача залишити анонімною свою переписку або навіть анонімною свою ідентичність.

Одним із способів захисту обміну повідомленнями є шифрування. Більшість сучасних мобільних додатків за для комунікації в інтернеті мають достатньо потужний захист від хакерів і, навіть, деякі мають заявлене наскрізне шифрування. Але найчастіше на одному із рівнів воно не повне.

Методів шифрування дуже багато. Найбільш розповсюдженими серед сучасних розробників є: наскрізне (*End to end encryption – E2EE)*, на стороні клієнта(*Client-side encryption*), із точки в точку (*Point to point encryption).*

Розглянемо найбільш надійний спосіб серед перерахованих – це наскрізне шифрування. *E2EE* є різновидом асиметричного шифрування, тобто взаємодія відбувається між двома особами одна з яких володіє публічним ключом, яким шифрує дані, а інша закритим ключом, яким розшифровує. Навіть якщо припустити, що усі месенджери реалізували повністю *E2EE*, це не гарантує захист від професіональних хакерів, для яких залишаються такі інструменти інтернет атаки, як людина по середині(*man in the middle – MITM*). Також ніхто не гарантує захищеність кінцевого вузла від крадіжки ключів дешифрування. Деякі розробники намагаються підтвердити, що користувач є самим собою покладаючись на організації, що займаються веб безпекою і видають

сертифікати. Таким чином компанія, яка має сертифікат, може бути тим третім а́ктором, який підтвердить правильність даних. Інший спосіб – це генерувати хеш на основі публічного або спільного секретного ключа та відбитку пальця, звіряючи відбитки за іншим каналом, який гарантує безпечність але не обов'язково секретність.

Тобто *E2EE* як система забезпечення захисту комунікації в цілому виконує свою роботу але ніяк не захищає метадані користувача. Навіть в ідеальному випадку, коли передані дані були приховані від злочинця, організації або держави, то *IP*-адреса, інформація про місцезнаходження, пристрій і додаток, який був використаний, залишилася.

Рішень приховування метаданих є кілька. Їх можливо умовно поділити на приватні й на багатокористувацькі. Приватні рішення приховування метаданих це використання *VPN*(*Virtual private network*) та ланцюга проксі серверів. Багатокористувацькі базуються на «створенні» мережі, в якій майже неможливо визначити хто є кінцевим користувачем. Прикладами таких рішень є *Tor*(*The Onion Router*), *I2P*(*Invisible Internet Project*), *Freenet*, та *Bitmessage* [1], який має деякі відмінності. Останній на відміну від інших має *peer-to-peer* з'єднання та специфічний обмін повідомленнями.
Розглянемо рішення *Tor* як найбільш розповсюджене (рис. 1 [2]).

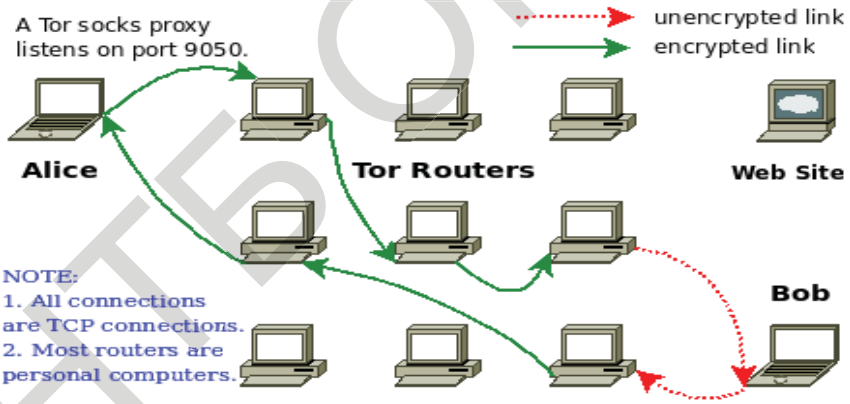

Рис. 1 – Архітектура *Tor*

Структура складається із першого і останнього користувача, випадково вибраного шляху, по якому передаються зашифровані дані. Вузол на якому розшифровуються дані називається кінцевим(*exit node*) і в більшості видів атак є вразливим місцем. Така архітектура є також вразливою до аналізу трафіка (*traffic analysis*). Якщо використовувати Tor для доступу до веб-серверу, то буде використовуватися стандарт *X.509*, який включає *HTTPS*. Цей стандарт був кілька разів скомпрометований. А *HTTPS* настільки надійний наскільки надійні сертифікуючі організації, а їх більше тисячі, варто тільки одній бути зламаною.

Напроти *Bitmessage* пропонує деякі кращі рішення, але з інших боків набагато гірші ніж в *Tor*. Децентралізація досягається за допомогою хешування публічних ключів, які також функціонують як адреси користувачів. Обмінятися

ними можливо наприклад через *QR-code* або інші канали. Механізм обміну повідомленнями є схожим на транзакції та блокову систему у *Bitcoin* [3] але с доказом роботи (*proof-of-work*). Доказ роботи – механізм, який наказує відправнику вирішити задачу, котру вибирає одержувач. Це допомагає боротись із спамом.

Цікавою річчю є те, що враховуючи цю систему усі користувачі отримують повідомлення але дешифрувати може тільки, той кому воно належить. Тим самим вирішується проблема із проміжним сервером, на якому треба тримати повідомлення, які ще не дійшли. Треба лише мати автоматичну систему, яка пересилає повідомлення відразу, як кінцевий отримувач з'являється онлайн. У *Bitmessage* дані у користувачів зберігаються два дні, а потім видаляються. Але це рішення не має багатошарового шифрування, як в *Tor* і масштабованість такої системи під питанням. Мається на увазі пропозиція самого розробника – після досягнення деякої кількості користувачів, почати їх організовувати в дерево вузлів. Або дослідники, які пропонують організовувати в вузли та супер вузли (*supernodes*) для взаємодії із сусідніми [4].

Виходячи з вищезазначеного, деяка комбінація описаних рішень може створити більш надійну систему.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Warren J. Bitmessage: A Peer-to-Peer Message Authentication and Delivery System [Електронний ресурс] / Jonathan Warren // Bitmessage. – 2012. – Режим доступу до ресурсу: https://bitmessage.org/bitmessage.pdf.
2. Haraty R. A Systematic Review of Anonymous Communication Systems / R. Haraty, M. Assi, I. Rahal // Proceedings of the 19th International Conference on Enterprise Information Systems / R. Haraty, M. Assi, I. Rahal. – Porto, Portugal: International Conference on Enterprise Information Systems, 2017. – С. 211–220.
3. BlockChain Technology: Beyond Bitcoin / [M. Crosby, V. Kalyanaraman, P. Pattanayak та ін.]. // Applied Innovation Review. – 2016. – С. http://scet.berkeley.edu/wp–content/uploads/AIR–2016–Blockchain.pdf.
4. Desmouceaux Y. Scalability of the BitMessage protocol [Електронний ресурс] / Y. Desmouceaux, M. Enguehard // de Télécom ParisTech. – 2013. – Режим доступу до ресурсу: https://perso.telecom-paristech.fr/drossi/teaching/inf570/projects/2013-report-04.pdf.

XX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

ОДЕСА
21-22 квітня 2020 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Артеменко С.В., Ольшевська О.В.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.