SCIENTIFIC COLLECTION «INTERCONF»

№ 1 (37)

December, 2020

THE ISSUE CONTAINS:

Proceedings of the 1st International Scientific and Practical Conference

RECENT SCIENTIFIC INVESTIGATION

OSLO, NORWAY

6-8.12.2020

InterConf
Scientific Publishing Center

SCIENTIFIC COLLECTION «INTERCONF»

№ 1 (37) | December, 2020

THE ISSUE CONTAINS:

Proceedings of the 1st International Scientific and Practical Conference

RECENT SCIENTIFIC INVESTIGATION

OSLO, NORWAY

6-8.12.2020

OSLO
2020

UDC 001.1

S 40 *Scientific Collection «InterConf»*, (37): with the Proceedings of the 1st International Scientific and Practical Conference «Recent Scientific Investigation» (December 6-8, 2020). Oslo, Norway: Dagens naeringsliv forlag, 2020. 1151 p.

ISBN 978-82-7346-353-1

The recommended citation:
Surname N. (2020). Title of article or abstract. *Scientific Collection «InterConf»,* (37): with the Proceedings of the 1st International Scientific and Practical Conference «Recent Scientific Investigation» (December 6-8, 2020) in Oslo, Norway; pp. 21-27. Available at: https://interconf.top/...

This issue of Scientific Collection «InterConf» contains the International Scientific and Practical Conference. The conference provides an interdisciplinary forum for researchers, practitioners and scholars to present and discuss the most recent innovations and developments in modern science. The aim of conference is to enable academics, researchers, practitioners and college students to publish their research findings, ideas, developments, and innovations.

TABLE OF CONTENTS

MODELING AND NANOTECHNOLOGY

INFORMATION AND WEB TECHNOLOGIES

UDC 681.3

Голубничий Дмитро Юрійович
ORCID ID: 0000-0002-6873-7004
кандидат технічних наук, доцент, доцент кафедри Інформаційних систем
Харківський національний економічний університет імені Семена Кузнеця, Україна

Власов Андрій Володимирович
ORCID ID: 0000-0001-6080-237X
кандидат технічних наук,
старший науковий співробітник наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Третяк Вячеслав Федорович
ORCID ID: 0000-0003-2599-8834
кандидат технічних наук, старший науковий співробітник, доцент,
науковий співробітник наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Запара Денис Михайлович

начальник науково-дослідного відділу наукового центру Повітряних Сил
Харківський національний університет Повітряних Сил імені Івана Кожедуба, Україна

Жукова Ірина Юріївна
студентка
Харківський національний університет радіоелектроніки, Україна

ОЦІНКА СКЛАДНОСТІ МЕТОДІВ ВИЯВЛЕННЯ АТАК

Створення ефективних систем захисту інформаційних систем зіштовхується також з браком обчислювальної потужності. З самого початку розвитку комп'ютерів і комп'ютерних мереж спостерігаються дві тенденції відповідно закону Мура і закону Гілдера. Закон Мура говорить про щорічне подвоєння продуктивності обчислювачів, доступних за одну і ту ж вартість, а закон Гілдера – про потроєння пропускної спроможності каналів зв'язку за той же період. Таким чином, зростання обчислювальної потужності вузлів мережі

відстає від зростання об'ємів переданої по мережі інформації, що з кожним роком посилює вимоги до обчислювальної складності алгоритмів систем захисту інформації [1].

Методи виявлення атак в сучасних системах виявлення атак (СВА) недостатньо опрацьовані в частині формальної моделі атаки, і, отже, для них достатньо складно строго оцінити такі властивості як обчислювальна складність, коректність і т.д. Прийнято розділяти методи виявлення атак на **методи виявлення аномалій** і **методи виявлення зловживань**. До другого типу методів відносяться більшість сучасних комерційних систем (Cisco IPS, ISS RealSecure, NFR) – вони використовують сигнатурні (експертні) методи виявлення.

Визначимо дві групи критеріїв: перша група характеризує власно методи виявлення атак і специфічні для них якісні і кількісні показники ефективності, тоді як друга група критеріїв характеризує реалізації цих методів в системах виявлення атак.

Критерії порівняння методів виявлення атак. Для порівняльного аналізу методів виявлення атак вибрані наступні критерії: рівень спостереження за системою (HIDS, NIDS, AIDS або Hybrid); верифікація методу (високий або низький); адаптивність методу (високий або низький); стійкість (глобальна або локальна). обчислювальна складність.

1. Рівень спостереження за системою: Даний критерій визначає рівень абстракції аналізованих подій в захищеній системі і визначає межі застосування методу для виявлення атак в мережах. Тому, розглядаються наступні рівні: HIDS – спостереження на рівні операційної системи окремого вузла мережі; NIDS – спостереження на рівні мережної взаємодії об'єктів на вузлах мережі; AIDS – спостереження на рівні окремих додатків вузла мережі; Hybrid – комбінація спостерігачів різних рівнів.

2. Верифікація методу: Даний критерій дозволяє оцінити, чи може людина (наприклад, кваліфікований оператор СВА або експерт) відтворити послідовність кроків по ухваленню рішення про наявність атаки, зіставляючи

вхідні і вихідні дані СВА. Наприклад, сигнатурні методи вважатимемо за верифіцируємими, а кластерні – ні. Верифікація дозволяє провести експертну оцінку коректності методу і його реалізації в довільний момент часу, зокрема в процесі експлуатації системи виявлення на його основі. Властивість верифікації методу важлива при експлуатації системи виявлення атак в реальній обстановці як засіб збору доказової бази про атаки. Можливі значення: висока (+) або низька (-).

3. Адаптивність методу: Оцінка стійкості методу до малих змін реалізації атаки, які не змінюють результат атаки. Адаптивність є єдиною істотною перевагою "альтернативних" методів виявлення атак перед "сигнатурними". Відсутність адаптивності не дозволяє системі захисту оперативно реагувати на невідомі атаки і вимагає організації системи регулярного оновлення баз відомих атак, по аналогії з антивірусними системами. Можливі значення: висока (+), низька (-).

4. Стійкість: Даний критерій характеризує незалежність виходу методу від захищеної системи – для одного і того ж входу метод повинен давати один і той же вихід, незалежно від захищеної системи. Проблема стійкості особливо гостро стоїть для статистичних методів, котрі аналізують абсолютні значення параметрів продуктивності і завантаженості ресурсів мережі і вузлів, що можуть істотно відрізнятися на різних вузлах і в різних мережах. Навчений в одній мережі розпізнавач може бути стійким в межах даної мережі і нестійким в решті всіх мереж. Таку стійкість називатимемо локальною. Оскільки процедура навчання зазвичай є "дорогою" – вимагає використання великої кількості ресурсів і часу – число процедур навчання бажано мінімізувати. Методи виявлення атак, які аналізують семантику введення, стійкіші, ніж статистичні. Можливі значення: глобальна (+), локальна (-).

5. Обчислювальна складність: Теоретична оцінка складності методу на основі інформації з відкритих публікацій. Це дозволяє оцінити тільки складність методу в режимі виявлення, без урахування можливих попередніх етапів настройки і навчання. Даний критерій є ключовим для завдання виявлення атак

в мережах і має набагато більше значення, ніж складність по пам'яті із-за випереджаючого зростання пропускної спроможності каналів передачі даних і здешевлення машинної пам'яті. Обчислювальна складність може мати наступну залежність: сублінійна – константа, логарифм; лінійна; квадратична і так далі

Критерії порівняння систем виявлення атак. Для порівняльного аналізу СВА були обрані наступні критерії: клас виявлених атак; рівень спостереження за системою; використовуваний метод виявлення; адаптивність до невідомих атак. управління і розподіленість; захищеність.

1. Клас виявлених атак. Даний критерій визначає, які класи атак здатна виявити дана система. Це один з ключових критеріїв. У зв'язку з тим, що на сьогоднішній день жодна система не здатна виявити атаки всіх класів, для повнішого покриття всього спектру атак необхідно комбінувати різні СВА. Тут використовується класифікація атак, заснована на розділенні ресурсів захищеної системи по типах. Клас атаки – це четвірка **<L,R,A,D>**, де **L**: розташування атакуючого об'єкту. Воно може бути або внутрішнім (li) по відношенню до захищеної системи або зовнішнім (le); **R**: ресурс, який атакується. Ресурси розділяються по розташуванню і за типом. По розташуванню: вузлові (rl), мережні (rn). За типом: призначені для користувача ресурси (ru), системні ресурси (rs), ресурси СУБД (rd), обчислювальні ресурси (rc), ресурси захисту (rp); **A**: цільова дія на ресурс: збір інформації (as), отримання прав користувача; ресурсу (ям), отримання прав адміністратора ресурсу (ar), порушення цілісності ресурсу (ar), порушення працездатності ресурсу (ad); **D**: ознака розподіленого характеру атаки: розподілені (dd), нерозподілені (dn).

2. Рівень спостереження за системою. Визначає, на якому рівні захищеної системи збирають дані для виявлення атаки. Розрізняються вузлові і мережні джерела. В межах вузлових джерел розділяються рівні ядра і додатку. Від рівня спостереження за системою залежить швидкість збору інформації, вплив системи на збирану інформацію, вірогідність отримання спотвореної інформації. Слід зазначити, що використання методу виявлення, що дозволяє аналізувати поведінку на всіх рівнях абстракції, не означає, що ця можливість реалізована в

конкретній системі. Часто реалізація володіє меншими можливостями, чим теоретичні можливості використовуваного нею методу: HIDS - спостереження на рівні операційної системи окремого вузла мережі; NIDS - спостереження на рівні мережної взаємодії об'єктів на вузлах мережі; AIDS - спостереження на рівні окремих застосувань вузла мережі; Hybrid - комбінація спостерігачів різних рівнів.

3. Використовуваний метод виявлення. Метод виявлення також є ключовим критерієм порівняння. Існує два класи методів: методи виявлення аномалій і методи виявлення зловживань. У приведеному нижче списку перераховані не окремі методи, але, в основному, сімейства методів, об'єднаних деяким єдиним підходом або теоретичною моделлю:

Виявлення зловживань: аналіз систем станів; графи атак; нейронні мережі; імунні мережі; SVM; експертні системи; методи, засновані на специфікаціях; MARS – Multivariate Adaptive Regression Splines; сигнатурні методи.

Виявлення аномалій: статистичний аналіз; кластерний аналіз (data mining); нейронні мережі; імунні мережі; експертні системи; поведінкова біометрія; SVM; аналіз систем станів.

4. Адаптивність до невідомих атак. Визначає здатність використовуваного методу виявляти раніше невідомі атаки.

5. Управління і розподіленність. До цього критерію відносяться три підкритерії: масштабованість, відкритість та формування відповідної реакції на атаку.

Масштабованість визначає можливість додавання нових аналізованих ресурсів мережі, нових вузлів і каналів передачі даних, зокрема можливість управління єдиною розподіленою системою виявлення атак. Управління може бути централізоване і/або розподілене.

Відкритість визначає наскільки система є відкритою для інтеграції в неї інших методів виявлення атак, компонентів сторонніх розробників і сполучення її з іншими системами захисту інформації. Це можуть бути програмні інтерфейси для вбудовування додаткових модулів і/або реалізація стандартів взаємодії

мережних компонентів.

Формування відповідної реакції на атаку визначає наявність в системі вбудованих механізмів реакції на атаку у відповідь, окрім самого факту її реєстрації. Прикладами реакції можуть бути розрив з'єднання з атакуючим об'єктом, блокування його на міжмережному екрані, відстежування шляху проникнення атакуючого об'єкту в захищену систему і т.д.

6. Захищеність. Визначає ступінь захищеності СВА від атак на її компоненти, включаючи захист переданої інформації, стійкість до часткового виходу компонентів з ладу або їх компрометації.

Таким чином, "ідеальна" система виявлення атак повинна володіти наступними властивостями: покриває всі класи атак (система повна); дозволяє аналізувати поведінку захищеної КМ на всіх рівнях: мережному, вузловому і рівні окремих додатків; адаптивна до невідомих атак (використовує адаптивний метод виявлення атак); масштабується для КМ різних класів: від невеликих локальних мереж класу "домашній офіс" до крупних багатосегментних і комутованих корпоративних мереж, забезпечуючи можливість централізованого управління всіма компонентами СВА; є відкритою та має вбудовані механізми реагування на атаки; є захищеною від атак на компоненти СВА, зокрема від перехоплення управління або атаки "відмова в обслуговуванні".

Таким чином, аналіз публікацій показує (табл. 1), що для більшості методів виявлення аномалій характерна слабка верифікованість і слабка глобальна стійкість (або її відсутність).

Таблиця 1

Результати порівняння методів виявлення атак

Критерій / Метод	Рівень спостереження	Аномалії/ зловживання	Верифікованість	Адаптивність	Стійкість	Обчислювальна складність
Системи переходів	Hybrid	–/+	+	–	+	O(n)
Графи атак	Hybrid	–/+	+	+	+	NP
Нейронні мережі	NIDS, HIDS	+/+	–	+	–	O(n) і вище
Імунні мережі	NIDS, HIDS	+/+	–	+	–	O(n) і вище
SVM	NIDS, HIDS	+/+	–	+	–	ln(n)
Експертні системи	NIDS, HIDS	+/+	+	+	+	У загальному випадку NP
Специфікації	NIDS	–/+	+	–	–	ln(n)
MARS	NIDS, HIDS	–/+	–	+	–	O(n) і вище

Критерій / Метод	Рівень спостереження	Аномалії/ зловживання	Верифікованість	Адаптивність	Стійкість	Обчислювальна складність
Сигнатурні методи	Hybrid	–/+	+	–	+	ln(n)
Статистичні методи	NIDS, HIDS	+/–	–	+	–	O(n) і вище
Кластерний аналіз	Hybrid	+/+	–	+	–	O(n) і вище
Поведінкова біометрія	HIDS	+/–	–	+	–	O(n) і вище

Основна гідність методів виявлення аномалій полягає в їх адаптивності і здатності виявляти раніше невідомі атаки. Серед глобально стійких і верифікованих методів, що мають при цьому низьку обчислювальну складність, можна відзначити метод аналізу системи переходів і простий сигнатурний метод. Жоден з розглянутих методів не володіє одночасно адаптивністю, стійкістю і верифікованістю, маючи при цьому прийнятну обчислювальну складність.

Всі досліджені системи можуть виявляти атаки декількох класів. Тому для поліпшення читаності і скорочення об'єму тексту вводяться поняття об'єднання, перетини і вкладення класів атак. Для позначення об'єднання і перетину класів атак використовуватимемо символи "$\cup$" і "$\cap$" відповідно.

Частина систем орієнтована на виявлення вузлових атак, і використовує для аналізу такі джерела як журнали реєстрації додатків, ОС, журнали систем аудиту (OSSEC). Інші системи виявляють тільки зовнішні (мережні) атаки і використовують для аналізу інформацію, що отримується з каналів передачі даних в мережі (Bro, Snort). Решта систем є гібридними і виявляє як локальні, так і зовнішні атаки (STAT, Prelude).

Система Bro є мережною системою виявлення атак. Вона є набором модулів декомпозиції даних різних мережних протоколів (від мережного до прикладного рівня) і набором сигнатур над подіями відповідних протоколів. Сигнатури Bro фактично є регулярними виразами в алфавітах протоколів.

Дана система виявляє атаки наступних класів (L,R,A,D): $L = \{li \cup le\}$ (внутрішні і зовнішні атаки); $R = \{rn\} \cap \{ru \cup rs\}$ (атаки на мережні призначені для користувача ресурси і системні ресурси); $A = \{as \cup au \cup ar \cup ad\}$ (збір інформації про систему, спроби отримання прав користувача, спроби отримання

прав адміністратора і порушення працездатності ресурсу); $D = \{dn \cup dd\}$ (нерозподілені і розподілені).

Система OSSEC, єдина з розглянутих в даній роботі, котра є спочатку орієнтованою на виявлення атак рівня системи (вузлових). Вона найбільш нова з розглянутих систем; її остання версія призначена, зокрема, для аналізу журналів реєстрації UNIX, типових застосувань (ftpd, apache, mail, etc), а також журналів міжмережних екранів і мережних СВА. OSSEC включає набір аналізаторів для різних джерел даних, контроль цілісності файлової системи, сигнатури відомих троянських закладок (rootkits) і ін.

Виявляються атаки наступних класів: $L = \{li\}$ (атакуючі об'єкти знаходяться усередині системи); $R = \{rl\} \cap \{ru \cap rs\}$ (вузлові призначені для користувача і системні ресурси); $A = \{au \cup ar \cup ai\}$ (спроби отримання прав користувача, спроби отримання прав адміністратора, порушення цілісності ресурсу); $D = \{dn \cup dd\}$ (нерозподілені і розподілені).

Система STAT є експериментальною університетською розробкою, і найбільш "старою" з даних систем - перші публікації по STAT датуються 1992 роком. Система включає набір компонентів виявлення атак різних рівнів – мережний (NETSTAT), вузловий (USTAT, WINSTAT), додатків (WEBSTAT), тобто є класичною гібридною системою.

СВА виявляє атаки наступних класів: (L,R,A,D), де: $L = \{li \cup le\}$ (внутрішні і зовнішні атаки); $R = \{rl \cup rn\} \cap \{ru \cup rs\}$ (атаки на вузлові або мережні призначені для користувача ресурси і системні ресурси); $A = \{as \cup au \cup ar \cup ad\}$ (збір інформації про систему, спроби отримання прав користувача, спроби отримання прав адміністратора і порушення працездатності ресурсу); $D = \{dn\}$ (нерозподілені).

Система Prelude, як і NETSTAT, є гібридною, тобто здатна виявити атаки як на рівні системи, так і на рівні мережі. Дана система спочатку розроблялася як самостійної СВА, але в даний час є високорівневою надбудовою над відкритими

СВА і системами контролю цілісності (AIDE, Osiris і тому подібне). Вузлова частина Prelude має достатньо широкий набір описів атак і, як джерело інформації, використовує різні журнали реєстрації: журнали реєстрації міжмережного екрану IPFW; журнали реєстрації NetFilter ОС Linux; журнали реєстрації маршрутизаторів Cisco and Zyxel; журнали реєстрації GRSecurity; журнали реєстрації типових сервісів ОС UNIX та інші.

СВА виявляє атаки наступних класів: (L, R, A, D), де: $L = \{li \cup le\}$ (внутрішні і зовнішні атаки); $R = \{rl \cup rn\} \cap \{ru \cup rs \cup rp\}$ (атаки на локальні або мережні призначені для користувача ресурси, системні ресурси і ресурси захисту); $A = \{as \cup au \cup ar \cup ad\}$ (збір інформації про систему, спроби отримання прав користувача, спроби отримання прав адміністратора і порушення працездатності ресурсу); $D = \{dn\}$ (нерозподілені).

Система Snort це найбільш популярна на сьогоднішній день некомерційна СВА. Вона активно і динамічно розвивається, оновлення бази відомих атак відбуваються з частотою, порівнянною з комерційними аналогами (зазвичай оновлення Snort випереджають комерційні). Snort є чисто мережний СВА і, окрім основної бази описів атак, має набір підключаємих модулів для виявлення специфічних атак або реалізовують альтернативні методи виявлення. Система здатна виявити атаки наступних класів (L, R, A, D): $L = \{li \cup le\}$(внутрішні і зовнішні атаки); $R = \{rl \cup rn\} \cap \{ru \cup rs \cup rp\}$ (атаки на локальні або мережні призначені для користувача ресурси, системні ресурси і ресурси захисту); $A = \{as \cup au \cup ar \cup ad\}$ (збір інформації про систему, спроби отримання прав користувача, спроби отримання прав адміністратора і порушення працездатності ресурсу); $D = \{dn \cup dd\}$ (нерозподілені і розподілені).

Таким чином, жодна з розглянутих систем не покриває всю множину класів атак. Слід також відзначити, що ці системи використовують неадаптивні методи виявлення атак. звідні результати порівняння розглянутих систем по вибраних критеріях наведені в табл. 2.

Таблиця 2

Результати порівняння відкритих СВА

	Класи атак	Рівень спостереження за системою	Метод виявлення	Адаптивність	Масштабованість	Реакція	Захист
Bro	$L = \{li \cup le\}$, $R = \{rn\} \cap \{ru \cup rs\}$, $A = \{as \cup au \cup ar \cup ad\}$, $D = \{dn \cup dd\}$	Системний	Сигнатурний	–	–	–	–
OSSEC	$L = \{li\}$ $R = \{rl\} \cap \{ru \cup rs\}$ $A = \{au \cup ar \cup ai\}$ $D = \{dn \cup dd\}$	Системний	Сигнатурний	+/–	+	–	–
STAT	$L = \{li \cup le\}$ $R = \{rl \cup rn\} \cap \{ru \cup rs\}$ $A = \{as \cup au \cup ar \cup ad\}$ $D = \{dn\}$	Системний, мережний	Сигнатурний, аналіз переходів станів	–	+	+	SSL
Prelude	$L = \{li \cup le\}$ $R = \{rl \cup rn\} \cap \{ru \cup rs \cup rp\}$ $A = \{as \cup au \cup ar \cup ad\}$ $D = \{dn\}$	Системний, мережний	Сигнатурний	–	+	+	SSL, Libsafe
Snort	$L = \{li \cup le\}$ $R = \{rl \cup rn\} \cap \{ru \cup rs \cup rp\}$ $A = \{as \cup au \cup ar \cup ad\}$ $D = \{dn \cup dd\}$	Мережний	Сигнатурний	–	–	+	–

На підставі проведеного порівняльного аналізу можна зробити вивід, що жодна з розглянутих вище відкритих СВА, не відповідає повною мірою критеріям "ідеальної" СВА. Основним недоліком є відсутність адаптивності до невідомих атак і неможливість аналізувати поведінку об'єктів КМ на всіх рівнях одночасний.

Список джерел:

1. Голубничий Д.Ю. Технології аудиту кібербезпеки інформаційних систем / Д.Ю. Голубничий, О.В. Коломійцев, В.Ф. Третяк, С.Г. Рязанін // Scientific Collection «InterConf», (36): with the Proceedings of the 7 th International Scientific and Practical Conference «Challenges in Science of Nowadays» (November 26 - 28, 2020) in Washington, USA: EnDeavours Publisher, 2020. – Pp. 333 – 342. вилучено із https://ojs.ukrlogos.in.ua/index.php/interconf/issue/view/26-28.11.2020/396.

SCIENTIFIC EDITION

BN 978-8-273463-53
9 788273 463531

SCIENTIFIC COLLECTION «INTERCONF»

№ 1 (37) | December, 2020

The issue contains:

Proceedings of the 1st International Scientific and Practical Conference

RECENT SCIENTIFIC INVESTIGATION

OSLO, NORWAY
6-8.12.2020

Contacts of the editorial office:

Scientific Publishing Center «InterConf»
E-mail: info@ interconf.top
URL: https://www.interconf.top

InterConf
Scientific Publishing Center