DOI: 10.18372/2410-7840.20.13079
УДК 004.773

МЕТОД ПРОТИДІЇ АТАКАМ ПОСЕРЕДНИКА У ТРАНСПАРЕНТНІЙ СИСТЕМІ ІНТЕРНЕТ ГОЛОСУВАННЯ

Володимир Чуприн, Володимир Вишняков, Олег Комарницький

Атака посередника, яку називають MITM (Man In The Middle), є однією з найбільш небезпечних загроз для систем Інтернет голосування (ІГ). Реалізація такої атаки може призвести як до розкриття таємниці голосів, так і до підміни результатів волевиявлення. Особливість атак посередника у транспарентних системах полягає в тому, щоб показувати контролюючим особам картину нормально функціонуючого сервера, а запити голосуючих непомітно для контролерів перехоплювати і обробляти завуальованим сервером, у якому закладені можливості для підробки результатів волевиявлення і розкриття таємниці голосів. Існуючі методи боротьби з MITM не забезпечують можливість кожному виборцю особисто упевнитись, що він спілкується зі штатним сервером, а не з підробкою зловмисників. Розглянуто метод протидії атакам посередника для транспарентних систем ІГ, у яких все без винятку програмне забезпечення є відкритим для перевірок та існує можливість в режимі реального часу контролювати відсутність модифікації штатного програмного забезпечення, а також перевіряти точність і своєчасність виконання штатних дій персоналом з боку необмеженої кількості активістів. З метою протидії атакам посередника запропоновано на сервері ІГ вести відкритий журнал обліку усіх запитів виборців на обслуговування під час здійснення актів волевиявлення. У цей журнал на початку кожного сеансу зв'язку виборця з сервером запропоновано заносити рядок з даними про час звернення разом з випадковим числом, яке генерується на сервері і відправляється виборцю. Виборець шляхом порівняння даних про момент часу свого звернення у журналі і значення випадкового числа може одразу впевнитись у тому, що він дійсно спілкується з цим сервером. Таким чином надається можливість кожному виборцю самостійно виявляти атаки посередника.

Ключові слова: *атака посередника, транспарентна система, Інтернет голосування, захист інформації, протидія атакам посередника..*

Вступ

Атака посередника, яку називають MITM (Man In The Middle), є однією з найбільш небезпечних загроз для систем Інтернет голосування (ІГ). Реалізація такої атаки, за умов відсутності або недостатньої ефективності механізмів захисту, може призвести, як до розкриття таємниці голосів, так і до підміни результатів волевиявлення.

Під транспарентною (відкритою або прозорою) системою ІГ ми будемо розуміти таку систему, у якій не тільки все без винятку програмне забезпечення, включаючи операційну систему (ОС), є заздалегідь відкритим для перевірок і експертиз, але є й можливість в режимі реального часу контролювати відсутність підміни або модифікації штатного програмного забезпечення, а також контролювати (з боку необмеженої кількості активістів) точність і своєчасність виконання штатних дій персоналом щодо управління системою ІГ. Принципи побудови транспарентних систем ІГ описані в роботах [1-4]. Особливість реалізації атаки посередника у таких системах ІГ полягає в тому, щоб показувати контролюючим особам картину нормально функціонуючого сервера системи ІГ, а запити виборців непомітно для контролерів перехоплювати і обробляти завуальованим сервером, у якому закладені можливості для підробки і розкриття таємниці голосів виборців. Враховуючи особливу значимість шкідливих наслідків від реалізації загрози MITM, вкрай бажано надати кожному виборцю можливість без зайвих зусиль проконтролювати той факт, що він спілкується зі штатним сервером, а не з підробкою зловмисників. Така можливість спрямована на надання виборцям впевненості у тому, що таємниця їх голосу буде збережена, а результати не будуть викривлені. Реалізації саме такої можливості присвячено цю статтю.

Аналіз опублікованих досліджень і постановка завдання

Декілька останніх десятиліть досвід створення систем ІГ активно обговорюється на міжнародних конференціях [5-6], а в деяких країнах, як, наприклад, в Естонії, системи ІГ вже набувають популярності [7-8], але існує також і протидія впровадженню ІГ з боку громадян, які не вірять в можливість створення прозорих систем ІГ [9]. Безумовно ІГ надає суттєві переваги виборцям щодо зручності, мобільності та економії часу, але недовіра буде існувати до того часу, поки громадяни не зможуть впевнитись у тому, що в електронних засобах для голосування не існує можливості для розкриття таємниці голосів та/або викривлення результатів волевиявлення. Відомо, що для подолання недовіри

треба надати можливість контролю всіх тих об'єктів і процесів, які викликають сумніви. Для досягнення беззаперечної довіри необхідно надати усім бажаючим можливість контролювати усі складові системи ІГ протягом усього часу її функціонування. Саме такий підхід запропоновано в роботах [1-4], де описані принципи побудови систем ІГ, у яких надається можливість масового дистанційного контролю з боку необмеженої кількості будь-яких осіб щодо усіх програмних засобів та процесів в режимі реального часу. В роботі [3] показано, що після проведення такого контролю не залишається підстав для недовіри, бо всі елементи системи і дії обслуговуючого персоналу, які можуть бути потенційно небезпечними, є відкритими для масового спостереження. Іншими словами, будь-яка спроба вчинення зловмисної дії у такій системі може бути виявлена та зафіксована контролюючими особами. Скоріш за все, неможливо досягти справжніх успіхів щодо впровадження ІГ без наявності такого контролю. Наведений в роботі [3], повний перелік загроз, які можуть стати причиною порушення таємниці голосів виборців або вплинути на вірність підрахунку, представлено у табл. 1 і табл. 2.

Таблиця 1

Загрози, які можуть бути реалізовані поза сервером ІГ

Опис загрози	Метод протидії
1. Перехоплення даних під час передавання	Створення досконало захищених каналів
2. Заміна даних під час передавання	Використання протоколів, які досконало захищають цілісність даних
3. Проникнення до серверу через засоби дистанційного доступу	Усунення можливості проникнення до серверу з правами повного доступу
4. Заміна даних про результат голосування	Порівняння даних з довідками, отриманими через досконало захищений канал

Таблиця 2

Загрози, які можуть бути реалізовані персоналом, що обслуговує сервер ІГ

Опис загрози	Метод протидії
1. Фальсифікація операційної системи	Порівняння файлів ОС зі штатними
2. Виконання позаштатної команди управління	Контроль введення команд управління
3. Фізична заміна сервера	Контроль параметрів процесів ОС
4. Фальсифікація прикладного ПЗ	Порівняння текстів ПЗ зі штатними
5. Несвоєчасне виконання штатних дій	Перевірка дій за регламентом
6. Підключення позаштатних засобів з метою реалізації атаки посередника	Контроль характеристик трафіку

Загрози з табл. 1 можуть бути усунуті криптографічними, програмними та технічними засобами захисту інформації, а загрози з табл. 2, реалізація котрих пов'язана з помилками або зловмисними діями обслуговуючого персоналу, крім програмно-технічних засобів вимагають ще й адміністративних заходів. Методи, що наведені у табл. 2, дозволяють користувачам Інтернету виявляти і документувати загрози, але після цього треба приймати адміністративні рішення щодо порушників, бо інакше немає шансів на отримання бажаних чесних результатів волевиявлення. Іншими словами, якщо повідомлення про виявлені загрози будуть проігноровані, то виборцям залишається відмова від голосування і вихід на акцію протесту. Надалі припустимо, що зроблено все необхідне для того, щоб після виявлення загрози приймались правильні рішення. Проаналізуємо кожен з методів протидії на наявність слабких місць і можливих ускладнень під час їх реалізації. Протидія фальсифікації ОС шляхом порівняння файлів вимагає від контролюючих наявності додаткових комп'ютерів для встановлення такої ж ОС, як на сервері ІГ (в нашому випадку це OpenBSD). Порівняння файлів займає близько години, але для підтвердження справжності ОС достатньо двом-трьом незалежним групам активістів виконати таке порівняння і викласти в Інтернеті повідомлення про відсутність небезпечних розбіжностей, а також комусь із них опублікувати результат виконання команди *ps aux* у вигляді, який показано на рис. 1.

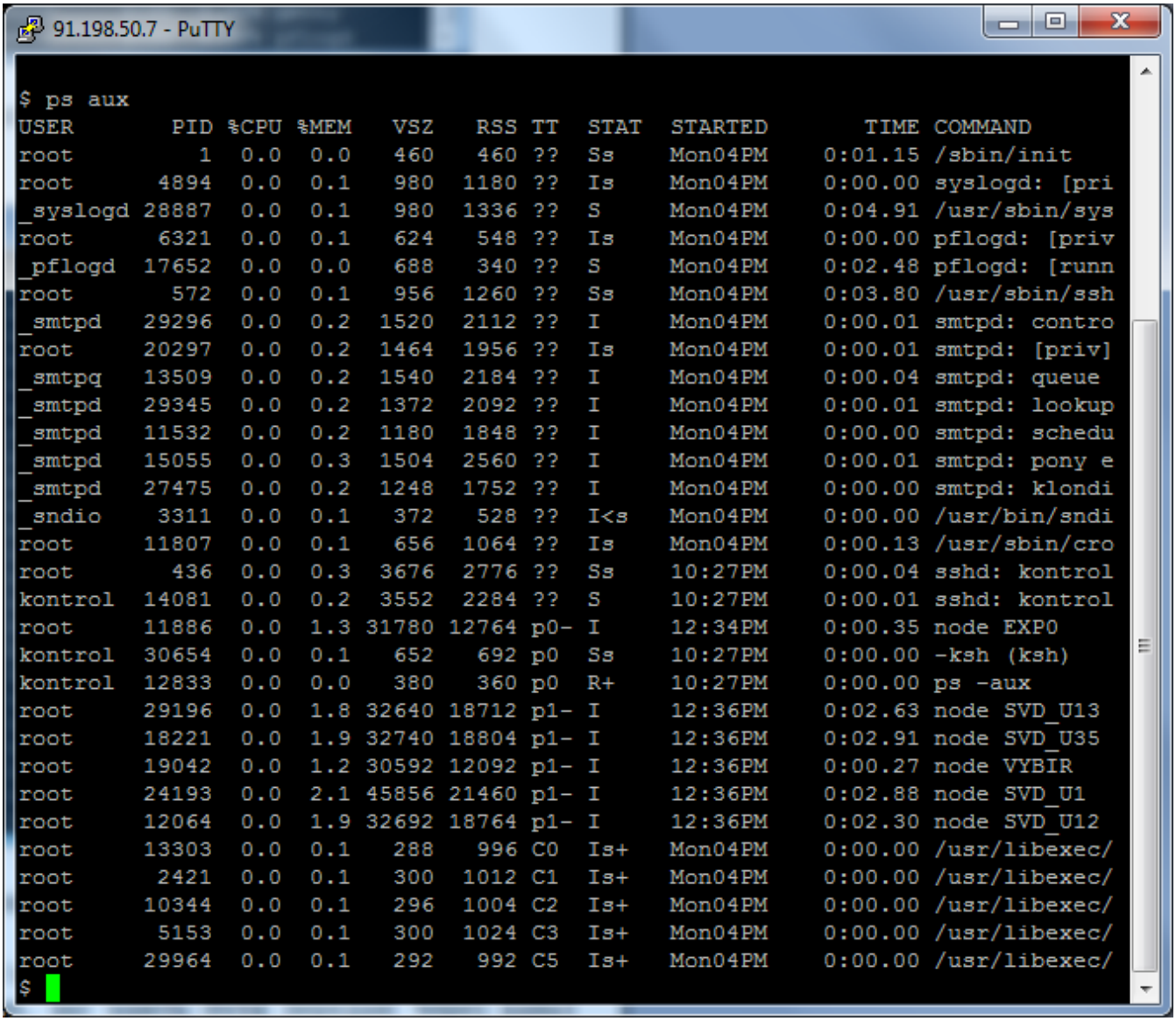

Рис. 1. Результат виконання команди *ps aux*

Виконання цієї команди дозволяє користувачам Інтернету впевнитись, що встановлена ОС на сервері ІГ є штатною, а також виявляти загрози, що описані у рядках 2-5 табл. 2. Для цього треба увійти на сервер ІГ з доступними для усіх правами контролера і виконати команду *ps aux*, після чого слід порівняти значення 20 чисел у стовпчику ідентифікаторів процесів PID між своїм і опублікованим результатами виконання даної команди. Ці 20 чисел знаходяться у рядках, які у стовпчику STARTED мають однакові значення (в нашому випадку Mon04PM). Протягом усього часу роботи сервера ці 20 цілих чисел не повинні змінюватись. Методи протидії загрозам, що описані у рядках 2-5 табл. 2, не потребують значних витрат часу і можуть бути виконані широким колом користувачів Інтернету. Наприклад, для тих, хто користується ОС Windows, достатньо встановити на своєму комп'ютері безкоштовне ПЗ типу *PuTTY* та/або *WinSCP* і виконувати нескладні дії зі спостереження за процесами на сервері ІГ у визначені моменти технологічного циклу, який представлено на рис. 2.

На рис. 2 сірим фоном виділено процеси на сервері ІГ, а також прийнято наступні скорочення:

ППД – період підготовки даних про претендентів на ІГ;

ППС – період підготовки сервера ІГ (встановлення ОС та програм загального користування);

ППЗ – прикладне програмне забезпечення для дистанційного голосування;

ПВЕБ – період введення електронних бюлетенів (в цей період запити виборців сервером не обслуговуються, а в списках виборців помічають тих, хто голосуватиме дистанційно, щоб не видавати їм паперові бюлетені).

Контроль введення команд управління розпочинають у наперед визначений організаторами голосування момент в межах періоду встановлення ППЗ. В цей момент у трьох рядках стовпчика *USER* з'явиться слово *admin*, а також з'явиться рядок зі значенням *sshd: admin* у стовпчику *COMMAND*, що означає початок роботи адміністратора, який повинен занести в директорію *home/admin* такі три файли ППЗ:

VDn.js – серверна прикладна програма;

VDn.DBT – дані про виборців для зчитування серверною програмою;

PWn.html – клієнтська програма введення паролів для голосування.

Замість букви *n* у назвах файлів проставляється номер виборчої дільниці. Конфіденційні дані про виборців у файлі *VDn.DBT* надаються у зашифрованому вигляді.

Після запуску сервера до початку роботи адміністратора повинно пройти достатньо часу, щоб активісти мали змогу (через порівняння файлів) впевнитись у відсутності будь-яких підробок серверного ПЗ. Після занесення перелічених вище трьох файлів до моменту запуску ППЗ також повинно бути достатньо часу для перевірки активістами змісту цих файлів. Запуск ППЗ супроводжується появою процесу, який відображується рядком з такими значеннями параметрів:

USER: *admin*;

PID: x (x – ціле число, яке не повинне змінюватись до кінця роботи сервера);

STARTED: ГГ:ХХ (час запуску ППЗ, ГГ – години; ХХ – хвилини);

COMMAND: *node VDn* (*n* - номер виборчої дільниці).

Цей рядок повинен залишатись незмінним до кінця роботи сервера ІГ.

Після запуску ППЗ адміністратор повинен завершити свою роботу командою *exit*. Після цього управління сервером буде виконувати виключно прикладна програма. Задача активістів в цей період полягає у тому, щоб виявляти появу нештатних процесів і у разі їх появи засвідчувати цей факт. При цьому можуть виникати в будь-якій кількості процеси з параметрами:

USER: *kontrol*;

COMMAND: *sshd*: *kontrol*.

Ці процеси слід залишати поза увагою, бо вони пов'язані з початком роботи активістів, які через обмеженість прав доступу не можуть утворювати загрози.

В період введення електронних бюлетенів на час занесення в директорію *home/admin* файлу *AVn.html* (це клієнтська програма голосування електронними бюлетенями) також повинні з'явитись чотири процеси з параметрами:

USER: *admin* (3 рядки);

COMMAND: *sshd*: *admin* (1 рядок).

Ці процеси свідчать про виконання адміністратором своєї штатної дії. Файл *AVn.html* також підлягає перевірці. Ніяких інших процесів на сервері ІГ за весь час спостереження не повинно з'являтись. Оскільки будь-яке зловмисне втручання в роботу сервера обов'язково потребує встановлення і запуск додаткової програми, а це не може бути невідображеним, як у файловій системі, так і в переліку активних процесів. Тому відсутність позаштатних процесів протягом усього періоду спостереження свідчить про те, що сервер працював виключно у штатному режимі і ніяких вдалих спроб втручання в його роботу не було. У разі виявлення позаштатного файлу або процесу до моменту запуску ППЗ існує можливість виправлення небезпечної ситуації шляхом повторного виконання усіх дій на сервері ІГ. При цьому період введення паролів, який має тривалість близько двох тижнів (оскільки він збігається в часі з періодом уточнення списків голосуючих [10]), може бути скорочено на декілька годин (або навіть на добу) без суттєвого впливу на процес голосування в цілому. Також можливо подібним чином виправити ситуацію у разі виявлення порушень на початку періоду введення паролів. У разі виявлення порушень у більш пізні часи, залишається тільки відміняти результати волевиявлення щодо конкретної групи учасників ІГ і проводити для цієї групи повторне голосування. Слід зауважити, що складнощі у роботі активістів під час спостереження за роботою сервера ІГ можуть бути усунені шляхом автоматизації. Дії контролерів не є складними, але потребують постійної уваги, бо через тимчасову неуважність активістів загроза може залишитись непоміченою. За допомогою автоматизації процесу спостереження цілком можливо створення таких засобів перевірки, коли жодна із загроз, що описані у рядках 1-5 табл. 2, не буде мати шансів залишитись непоміченою. Але відносно загрози *MITM*, яка описана у рядку 6 цієї таблиці, процедура виявлення не виглядає простою. Для реалізації цієї загрози зловмисники можуть скористатись тим, що запити контролерів відправляються на *TCP* порт 22, а запити виборців на інший *TCP* порт, наприклад, 8000. Розглянуту в роботі [3], схему підключення обладнання для реалізації загрози *MITM* показано на рис. 3.

За допомогою обладнання, що відокремлює, потік запитів від контролерів, який позначено цифрою 1, цей потік відправляють на сервер зі штатним програмним забезпеченням, де адміністратор точно і своєчасно виконує усі потрібні дії, а потік запитів від виборців, який позначено цифрою 2, відправляють на позаштатний сервер. При цьому у спостерігачів може скластись враження, що ніяких загроз не існує. В цей самий час на другому сервері, який недосяжний для спостерігачів, може бути встановлена програма, яка дозволяє порушувати таємницю голосів. Виявлення даної загрози пов'язане з необхідністю аналізу трафіка на сервері, який демонструє штатну роботу системи ІГ, за допомогою команди *netstat*, але такий аналіз залишає для зловмисників можливість розкриття таємниці окремих голосів, наприклад, з обраних *IP*-адрес. Тому бажано надати кожному виборцю можливість самостійно контролювати факт спілкування з реальним сервером ІГ, а не з підробкою зловмисників, що усуває можливість створення непомічених загроз з використанням *MITM*. Розробка засобів, які дозволяють усім виборцям самостійно впевнитись в тому, що їх звернення потрапляють дійсно на штатний сервер ІГ, і є завданням даної статті.

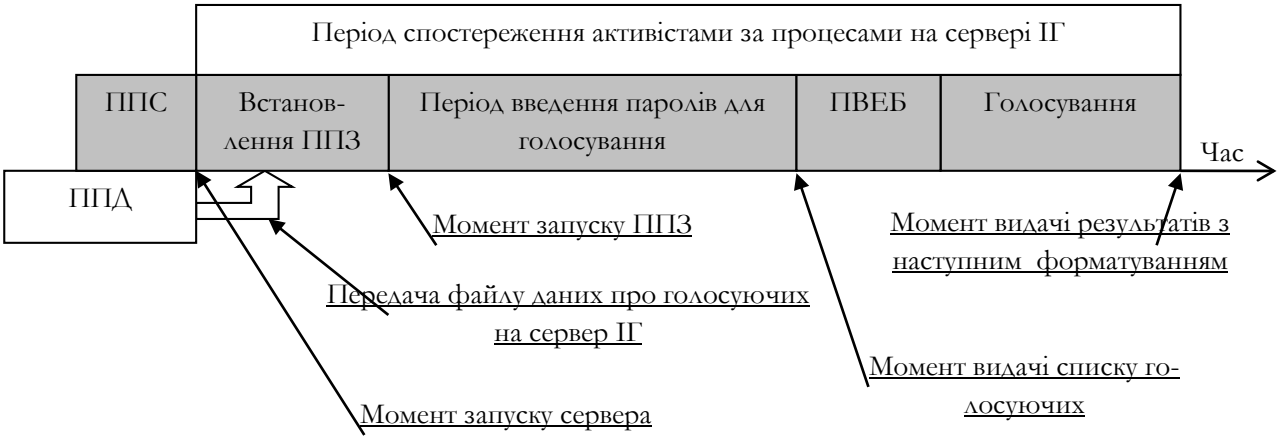

Рис. 2. Технологічний цикл функціонування системи голосування

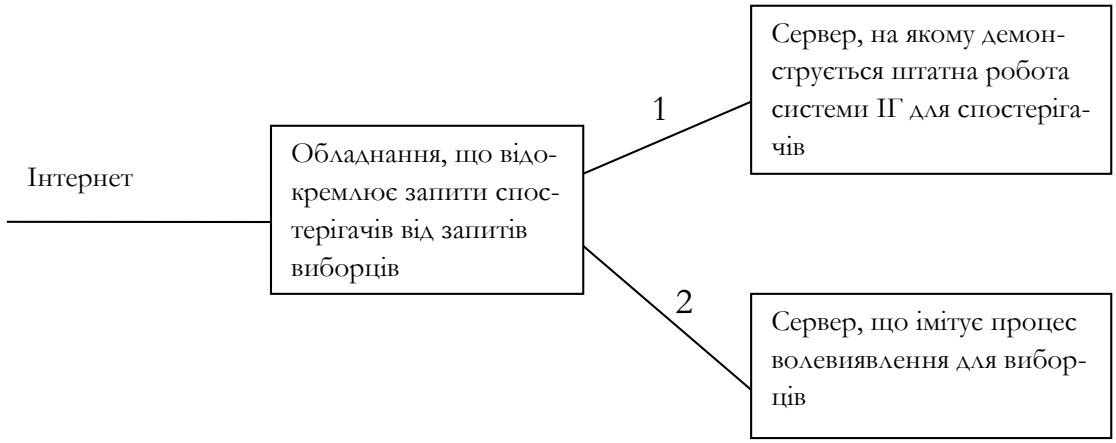

Рис. 3. Схема підключення обладнання для здійснення атаки посередника

Мета даної роботи полягає в розробці методу протидії атакам посередника у відкритій системі ІГ, який би дозволив кожному виборцю перед здійсненням акту волевиявлення без особливих ускладнень самостійно впевнитись у тому, що він дійсно спілкується зі штатним сервером ІГ, а не з підробкою зловмисників.

Основна частина дослідження

Проаналізуємо доцільність реалізації загрози *MITM* в ті чи інші періоди технологічного циклу функціонування системи ІГ. Реалізація загрози *MITM* протягом всього часу функціонування системи ІГ не є доцільною, бо в цьому випадку спостерігачі можуть ще на початку періоду введення паролів виявити загрозу за допомогою команд *netstat* або *tcpdump*. через відсутність або неточність підробки потоку пакетів між виборцями і сервером, який демонструє штатну роботу системи ІГ. Слід зауважити, що підробка цього потоку з абсолютною точністю неможлива через те, що на

початку кожного сеансу зв'язку відбувається обмін ключами з використанням випадкових бітових послідовностей. Зловмисник не може втручатись в роботу сервера, що імітує штатну роботу системи ІГ, через можливість бути виявленим, то ці бітові послідовності він змінювати не в змозі. Найбільші можливості для зловживань надає реалізація загрози *MITM* в період голосування. При цьому запити виборців будуть потрапляти на сервер, що імітує процес волевиявлення, де можливо розкрити усю інформацію, включаючи пароль для голосування. Це надає можливість зловмисникам голосувати на сервері, що демонструє штатну роботу систему голосування. Для цього може бути наданий дозвіл за відомими *IP*-адресами зловмисників для проходження їх *IP*-пакетів через обладнання, що відокремлює запити спостерігачів, у потік 1 (див. рис. 3). Щоб розкрити цю загрозу шляхом контролю характеристик трафіку необхідно дізнаватись *IP*-адреси виборців і перевіряти на сервері під час голосування наявність відповідного трафіку. Таку процедуру перевірки можливо виконати тільки для якоїсь частини виборців, що залишає певні можливості для шахрайства. З метою захисту кожного виборця від ризику потрапляння під розглянуту загрозу, ми пропонуємо на сервері ІГ вести відкритий журнал обліку усіх звернень виборців. На рис. 4 показано результат роздруківки сторінки цього журналу. У цей журнал на початку кожного сеансу зв'язку виборця з сервером слід заносити рядок з даними про час звернення разом з випадковим числом, яке генерується на сервері і відправляється виборцю у формі, яку показано на рис. 5. Виборець шляхом порівняння даних про момент часу свого звернення у журналі і значення випадкового числа може одразу впевнитись у тому, що він дійсно спілкується з цим сервером. Розбіжність у часі (в даному випадку на 19 секунд) пояснюється затримкою пакетів даних під час передавання від сервера до клієнта. Для полегшення доступу виборця до журналу можна автоматично дублювати зміст журналу на сайті виборчої дільниці. Оскільки втрутитись у роботу сервера ІГ без значного ризику бути поміченим спостерігачами, як було показано вище, неможливо, то ніяких шансів на те, щоб залишитись непоміченим під час реалізації загрози *MITM* у зловмисників не залишається.

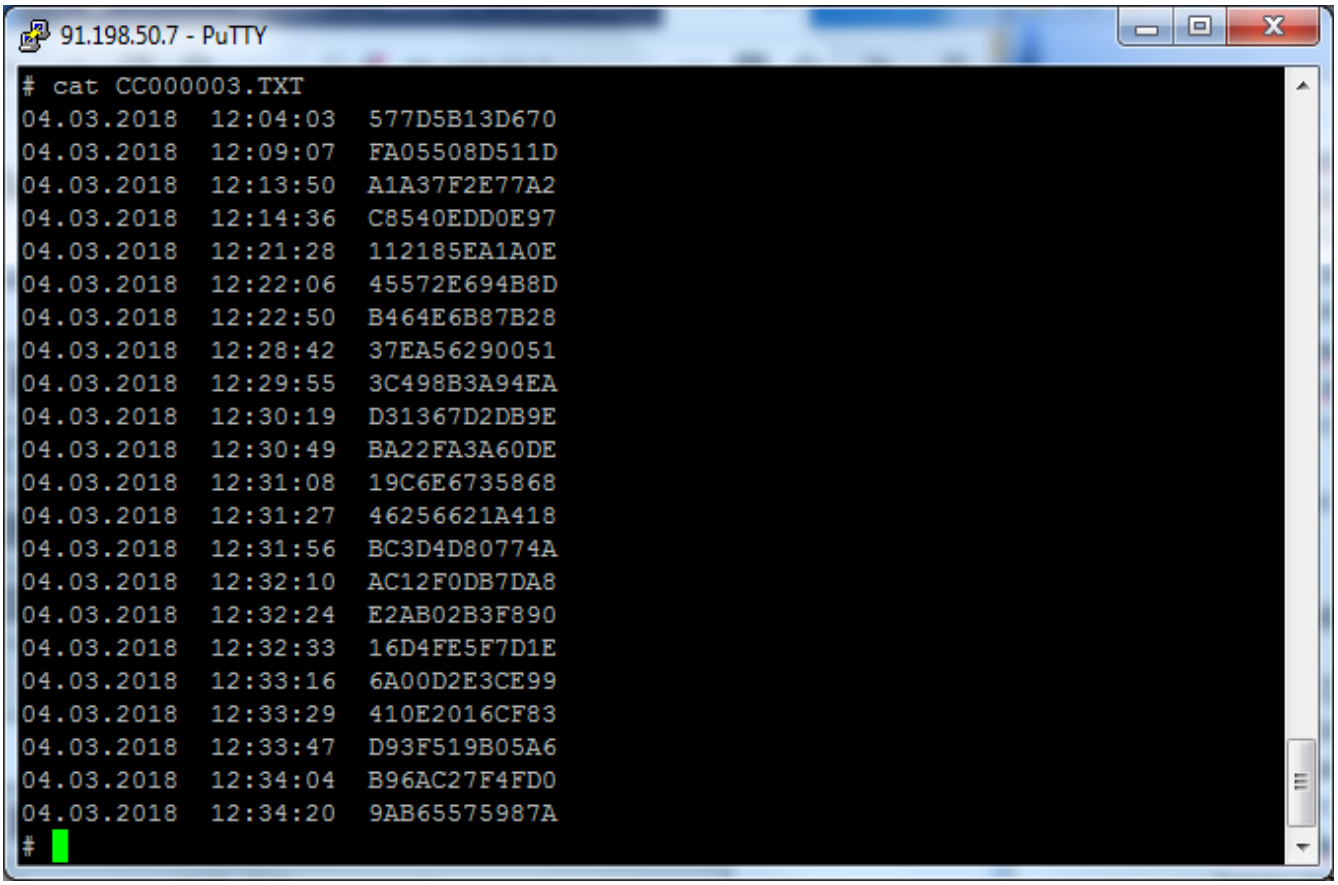

Рис. 4. Результат роздруківки сторінки журналу обліку звернень виборців за допомогою команди *cat*

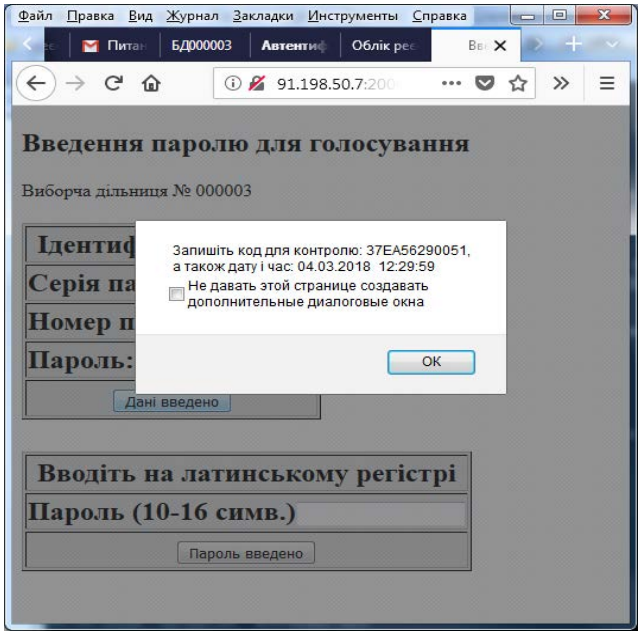

Рис. 5. Вигляд форми представлення виборцю даних для перевірки дійсності його звернення до сервера ІГ

ВИСНОВКИ

Атака посередника – цілком реальна загроза інформаційним ресурсам систем ІГ, яка за умов відсутності або недостатньої ефективності механізмів захисту, може призвести як до розкриття таємниці голосів, так і до підміни результатів волевиявлення.

У даній статті здійснено аналіз особливості реалізації цієї атаки для транспарентних систем ІГ, у яких все без винятку програмне забезпечення відкрите для перевірок та є можливість в режимі реального часу контролювати відсутність модифікації програмного забезпечення, а також перевіряти точність і своєчасність виконання штатних дій персоналом з боку необмеженої кількості спостерігачів. За результатами аналізу моделі атаки посередника в транспарентних системах ІГ запропоновано метод протидії цим атакам. А саме, запропоновано на сервері ІГ вести відкритий журнал обліку усіх запитів виборців на обслуговування під час голосування. У цей журнал на початку кожного сеансу зв'язку виборця з сервером слід заносити рядок з даними про час звернення разом з випадковим числом, яке генерується на сервері і відправляється виборцю. Виборець шляхом порівняння даних про момент часу свого звернення у журналі і значення випадкового числа може одразу впевнитись у тому, що він дійсно спілкується з цим сервером. Таким чином кожен виборець перед здійсненням акту волевиявлення може самостійно впевнитись у тому, що він дійсно спілкується зі штатним сервером ІГ, а не з підробкою зловмисників.

ЛІТЕРАТУРА

[1]. В. Вишняков, М. Пригара, О. Воронін, "Відкрита система таємного голосування", *Управління розвитком складних систем,* Вип. 20, С. 110-115, 2014.

[2]. В. Чуприн, В. Вишняков, М. Пригара, "Генерування випадкових чисел штатними засобами гостів мережі Інтернет", *Захист інформації*, Т. 18, №4, С. 323-335, 2016.

[3]. В. Чуприн, В. Вишняков, М. Пригара, "Захист операційного середовища систем Інтернет голосування", *Захист інформації,* Т. 19, №1, С. 56-66, 2017.

[4]. В. Чуприн, В. Вишняков, М. Пригара, "Метод протидії незаконному впливу на виборців у системі Інтернет голосування", *Безпека інформації,* Т. 19, №1, С. 7-14, 2017.

[5]. Lessons from the EVOTE 2014 Internation Conferens. [Electronic resource]. Online: http://eC/search?updated-min=2014-01-01T00:00:00-08:00&updated-max=2015-01-01T00:00:00-08:00& max-results=50.

[6]. C. Acemyan, P. Kortum, M. Byrne, D. Wallach, "Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II USENIX", *Journal of Election Technology and Systems (JETS)*, vol. 2, no. 3, pp. 26-56, 2014.

[7]. О. Савчук, *Системи електронних виборів процедури голосування та матеріально-технічні засоби. Міжнародний досвід.* [Електронний ресурс]. Режим доступу: http://euinfocenter.rada.gov.ua/uploads/documents/28966.pdf.

[8]. D. Springall, T. Finkenauer, Z. Durumeric, "Security Analysis of the Estonian Internet Voting System", *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '14)*, pp. 703-715, 2014.

[9]. Lombardi E. Electronic Vote & Democracy. [Electronic resource]. Online: http://www.electronic-vote.org.

[10]. Постанова Центральної виборчої комісії від 25 вересня 2015 року № 370 «Про роз'яснення щодо складання та уточнення списків виборців для підготовки і проведення голосування з місцевих виборів».

МЕТОД ПРОТИВОДЕЙСТВИЯ АТАКАМ ПОСРЕДНИКА В ТРАНСПАРЕНТНОЙ СИСТЕМЕ ИНТЕРНЕТ ГОЛОСОВАНИЯ

Атака посредника, которую называют MITM (Man In The Middle), является одной из наиболее опасных угроз для систем Интернет голосования (ИГ). Реализация такой атаки может привести как к раскрытию тайны голосов, так и к подмене результатов волеизъявления. Особенность атак посредника в транспарентных системах заключается в том, чтобы показывать контролирующим лицам картину нормально функционирующего сервера системы ИГ, а запросы избирателей незаметно для контролеров перехватывать и обрабатывать завуалированным сервером, в котором заложены возможности для подделки результатов волеизъявления и раскрытия тайны голосов избирателей. Известные методы борьбы с MITM не обеспечивают возможность

каждому избирателю лично убедиться, что он общается со штатным, а не фальшивым сервером. Рассмотрен метод противодействия атакам посредника для транспарентных систем ІГ, в которых всё без исключения программное обеспечение является открытым для проверок и существует возможность в режиме реального времени контролировать отсутствие модификации штатного ПО, а также проверять точность и своевременность выполнения штатных действий персоналом со стороны неограниченного числа активистов. С целью противодействия атаке посредника предложено на сервере ІГ вести открытый журнал учета всех запросов избирателей на обслуживание во время осуществления актов волеизъявления. В этот журнал в начале каждого сеанса связи избирателя с сервером предложено заносить строку с данными о времени обращения и случайным числом, которое генерируется на сервере и отправляется избирателю для ознакомления. Избиратель путем сравнения данных о моменте времени своего обращения в журнале и значения случайного числа может удостовериться в том, что он действительно общается с этим сервером. Таким образом предоставляется возможность каждому избирателю выявить атаку посредника.

Ключевые слова: атака посреднока, транспарентная система, интернет голосование, защита информации, противодействие атакам посредника.

METHOD OF COUNTERACTION OF ATTACKES OF MEDIATOR IN TRANSPARENT SYSTEM THE INTERNET VOTING

An attack of mediator, that is named by MITM (Man In The Middle), is one of threats for the systems of Internet-voting (ІГ). Realization of such attack can result both in opening of secret of voices and to the substitution of results of will. Feature of realization of attack of mediator - to show the picture of normally functioning server of the system of ІГ to the supervisory persons, and queries of electors unnoticed for inspectors to intercept and process the veiled server in that possibilities are stopped up for the imitation of results of will and opening of secret of voices of electors. The existent methods of fight from MITM do not provide possibility to every elector personally to ascertain, that he intermingles with a regular server, but not with the imitation of malefactors. The method of counteraction to the attacks of mediator is considered for the transparent systems of ІГ, in that all without an exception software is open for verifications and there is possibility real-time to control absence of modification of regular software, and also check up exactness and timeliness of implementation of regular actions a personnel from the side of unlimited amount of activists. With the purpose of counteraction to the attack of mediator it offers on the server of ІГ to conduct the open magazine of account of all queries of electors on service during realization of acts of will. In this magazine at the beginning of every session of connection of elector with a server to bring a line with data about time of appeal and random number that is generated on a server and leaves to the elector for an acquaintance. An elector by comparison of data about the moment of time of the appeal in a magazine and value of random number can make sure of that he really intermingles with this server. Possibility is thus given to every elector independently to find out the attacks of mediator.

Keywords: attack of mediator, transparent system, internet-voting, defence of information, counteraction to mediator attacks.

Чуприн Володимир Михайлович, кандидат технічних наук, професор кафедри телекомунікаційних систем Національного авіаційного університету.
E-mail: mega_chupr@ukr.net.
Чуприн Владимир Михайлович, кандидат технических наук, профессор кафедры телекоммуникационных систем Национального авиационного университета.
Chupryn Volodymyr, PhD in engineering, professor, Department of Telecommunication Systems, National Aviation University.

Вишняков Володимир Михайлович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп'ютерної інженерії Київського національного університету будівництва і архітектури.
E-mail: volodymyr.vyshniakov@gmail.com.
Вышняков Владимир Михайлович, кандидат технических наук, доцент, доцент кафедры кибербезопасности и компьютерной инженерии Киевского национального университета строительства и архитектуры.
Vyshniakov Volodymyr, PhD in engineering, associate professor, Department of Cyber Security and Computer Engineering, Kyiv National University of Construction and Architecture.

Комарницький Олег Олександрович, головний спеціаліст, Департамент інформаційно-комунікаційних технологій Київської міської державної адміністрації.
E-mail: komarnitskiy2012@gmail.com.
Комарницкий Олег Александрович, главный специалист, Департамент информационно-коммуникационных технологий Киевской городской государственной администрации.
Komarnitskiy Oleg, Chief Specialist, Department of Information and Communication Technologies of Kyiv City State Administration.