Наразі існує ще багато способів використання клітинних автоматів, які не були вивчені та можуть мати велике значення у майбутніх криптографічних дослідженнях.

Список використаних джерел:

1. Toffoli T. Computation and construction universality of reversible cellular automata // Journal of Computer and System Sciences. 1977. 15, №2. pp. 213–231.
2. Wolfram S. Cellular Automata as Models of Complexity // Nature. 1984. 311. pp. 419–424.
3. Wolfram S. Universality and complexity in cellular automata // Physica D. 1984. 10. pp. 1–35.
4. Wolfram S. Computation theory of cellular automata // Commun. Math. Phys. 1984. 96. pp. 15–57.
5. Wolfram S. Cryptography with Cellular Automata // Advances in Cryptology: Crypto ‘85 Proceedings. Lecture Notes in Computer Science, vol. 218. Springer-Verlag, 1986. pp. 429–432.
6. Wolfram S. Theory and applications of cellular automata: Including selected papers 1983-1986. River Edge, NJ.: World Scientific Publishing Co., Inc., 1986.
7. Wolfram S. Cellular Automata and Complexity. – Addison-Wesley, Reading, 1994.
8. Wolfram S. A new kind of science. – Champaign, Ilinois: Wolfram Media Inc., 2002. 1280 p.

ПРОБЛЕМА КВАЗІ-ОДНОКОРИСТУВАЛЬНОГО РЕЖИМУ ПРИ ЕКСПЛУАТАЦІЇ ОПЕРАЦІЙНИХ СИСТЕМ СІМЕЙСТВА MICROSOFT WINDOWS

Бойко В.Д.

кандидат технічних наук, доцент, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія»

У доповідях [1] та [2] розглядалася можливість та практичні аспекти переходу академічної освіти на використання open source програмного забезпечення. Було обґрунтовано актуальність та необхідність переходу на відкрите програмне забезпечення[1]. Були розглянуті причини, через які навчальні процеси у вищих закладах виявилися насичені піратським (зламаним, або не ліцензованим явно) програмним забезпеченням, необхідність і невідворотність далі строго контролю за ліцензійною чистотою використовуваного програмного забезпечення. У [2] докладно розбиралися практичні аспекти переходу на відкрите програмне забезпечення: описаний перехід (відкрите ПЗ, відкриті формати даних) був організований поступово та послідовно. Як базова система використовувався, заснований на Debian GNU/Linux, дистрибутив операційної системи Ubuntu.

Перехід на нове програмне забезпечення дозволив вирішити ще одну проблему, а саме - питання роботи в квазі-однокористувальному режимі, поширеному в операційних системах сімейства Windows.

Управління користувачами та правами під Windows є досить заплутаною і незручною процедурою, тому серед користувачів поширений квазі-однокористувацький режим, коли більша частина роботи відбувається під одним налаштованим користувачем, при цьому найчастіше задля зручності цього користувача створюють (або виділяють йому права) адміністратора системи [3], [4].

Цей режим роботи є широко поширеним серед користувачів операційних систем сімейства Microsoft Windows, тому не дивно, що робота в такому режимі також набула поширення в комп'ютерних класах більшості навчальних закладів [5].

При цьому операційна система на робочих місцях комп'ютерного класу використовується в режимі "одна роль операційної системи для всіх працюючих за комп'ютером користувачів". Часто комп'ютерний персонал намагається поліпшити ситуацію встановлюючи різне обмежує функціональність стороне ПЗ, що саме собою представляє проблему.

Експлуатація операційної системи у згаданому вище режимі "один користувач (одна роль) операційної системи для всіх працюючих за комп'ютером користувачів" призводить до того, що комп'ютер у лабораторії може використовуватися як робоче місце відразу декількома студентами (найчастіше – різних курсів), при цьому, оскільки механізми поділу користувачів не використовуються, їх файли, системні налаштування та установки неминуче змішуються. Це призводить одразу до кількох негативних явищ.

Перше можна назвати "каузальним плагіатом" - вільний доступ до чужих робочих файлів провокує на їх часткове або повне використання у своїй роботі, яке може бути як імпульсною реакцією, так і заздалегідь спланованою поведінкою.

Такій поведінці найчастіше намагаються протистояти шляхом відмови від постійного зберігання файлів на робочому місці та переходу на використання сторонніх носіїв (найчастіше usb флеш-драйвів, або хмарних сервісів). При цьому робочий процес виглядає так: файли копіюються на робоче місце, з ними відбувається робота, далі вони зберігаються назад на флеш-драйв (або в хмару), після чого файли, що залишилися на робочому місці, видаляються.

Це вирішує проблему лише частково (використання файлів так чи інакше залишає слід, при запланованому заздалегідь плагіаті на комп'ютер може бути встановлено malware ПЗ з функціоналом запису дій користувача), при цьому в свою чергу створює додаткові проблеми. Наприклад, флеш-драйви дуже швидко перетворюються на переносники та розповсюджувачі шкідливого ПЗ. Крім того, копіювання файлів займає час і забирає енергію, "від'їдаючи" її у навчального процесу та працюючи таким чином як своєрідне "тертя" або "комп'ютерна бюрократія". Найчастіше використання таких заходів швидко сходить нанівець і

комп'ютер перетворюється на хаотичне нагромадження різних файлів, яке у системних адміністраторів отримало окремий термін - "файлопомийка".

Виникнення "файлопомийки" призводить до негативних явищ другої категорії, яке, за нашими спостереженнями, добре пояснюється "теорією розбитих вікон" (англ. broken windows theory) [6]. Відповідно до положень цієї теорії, дрібні порушення правил у суспільно-доступній системі (розбите вікно в будівлі), провокує все більше таких порушень (що характеризуються ємною фразою "іншим можна, а мені не можна?") в результаті система позбавляється більшої частини свого ресурсу (в будівлі не залишається жодного цілого вікна) [7]. Ця теорія спочатку використовувалася пояснення механізмів і динаміки криміногенної обстановки у межах і у цій ролі часто критикувалося, проте, її становища цілком можна поширити використання операційної системи без поділу на користувальницькі ролі.

Рідко виходить так, що всі користувачі, що працюють на робочому місці комп'ютерного класу, суворо дотримуються писаних і неписаних правил використання файлового простору, налаштування програмного забезпечення та конфігурацію операційної системи. Порушення правил одним користувачем, провокує порушення правил іншими користувачами. Такі порушення накопичуються, що призводить до того, що поведінка користувачів одного комп'ютера стає все менш щадною та поважною по відношенню один до одного. Іноді таке ставлення може спричинити ворожість між користувачами. При цьому дрібні порушення можуть переростати у цілеспрямований вандалізм. Це відбувається рідко, хоча автору кілька разів доводилося спостерігати розвиток конфліктів, які починалися з встановлення заставок на робочих столах провокуючого змісту і закінчувалися використанням шкідливого програмного забезпечення та викраденням особистих даних з кешу браузера (або просто з незакритої по забудьку сесії роботи).

Очевидні недоліки безпеки та незручності такого режиму використання операційної системи користувачі та адміністратори системи прагнуть компенсувати за рахунок встановлення додаткового ПЗ, що виконує функції як забезпечення безпеки, так і заборони доступу до налаштувань і ресурсів операційної системи. Однак таке "блокуюче ПЗ" не тільки має сумнівну ліцензійну чистоту і потенційно несе в собі додаткові загрози безпеці, але насамперед сильно ускладнює навчальний процес, оскільки для встановлення та оновлення необхідного програмного забезпечення (а також відкриття прав та доступу, яке це ПЗ вимагає) доводиться звертатися до системного адміністратора. Це негативно позначається як на самому навчальному процесі, так і на навичках, які студенти отримують, які часто втрачають ініціативу і самостійність. Замість дослідження операційної системи, її режимів роботи та налаштувань, студент опиняється у "дитячому манежі", будь-який вихід за межі якого вимагає звернення до сторонніх осіб.

Незважаючи на те, що "блокуюче ПЗ" створює помилкову ілюзію відносної безпеки операційної системи та навчального ПЗ, його механізми захисту та блокування розраховані на некваліфікованого користувача і досить просто обходяться, а крім того, створюють мінімальну перешкоду (або не створюють її зовсім) різного шкідливого ПЗ. Таке ПЗ не може завадити поширенню вірусів, троянів, хробаків тощо.

Можливості навести лад у такому сформованому процесі обмежені. У випадках вандалізму рідко вдається визначити конкретного порушника без складного та витратного за часом та ресурсами дослідження системних журналів. Наведення порядку у файлах та даних робочого місця також ускладнюється - кожен користувач вважає свої файли та налаштування цінними та активно пручається їх упорядкуванню.

За всієї зовнішньої незначності, такий режим експлуатації операційної системи та робочий процес у комп'ютерних класах загалом створює атмосферу безладу та хаосу та - згідно з "теорією розбитих вікон", знижує і якість навчального процесу та ентузіазм учнів, що є серйозною проблемою при підготовці кваліфікованих ІТ -Фахівців.

Список использованных источников:

1. Бойко В.Д. Вопросы перехода на свободное программное обеспечение в современном академическом образовании. In Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України), volume 1, pages 607--610, 2021.
2. В.Д. Бойко. Практические аспекты перехода на свободное программное обеспечение в современном академическом образовании. In О. В. Дикий, editor, Кібербезпека в сучасному світі : матеріали III Всеукр. наук.-практич. конф. (м. Одеса, 19 листоп., 2021 р.), page 148. Одеса : Видавничий дім «Гельветика», October 2021.
3. Add a work or school account as a separate windows user. URL: https://answers.microsoft.com/en-us/windows/forum/all/i-want-to-add-a-work-or-school-account-as-a/ee7caa6c-3b9a-43f0-b4eb-0f59f3fe26f7
4. The 21 worst tech habits - and how to break them – ARN. URL: https://www.arnnet.com.au/article/459900/21_worst_tech_habits_-_how_break_them/?fp=2&fpid=2
5. How (and Why) to Create a Separate Windows Account Just for School | PCMag URL: https://www.pcmag.com/how-to/how-and-why-to-create-a-separate-windows-account-just-for-school
6. Kelling G. L. et al. Broken windows //Atlantic monthly. 1982. Т. 249. №. 3. С. 29-38.
7. Harcourt B. E., Ludwig J. Broken windows: New evidence from New York City and a five-city social experiment //U. Chi. L. Rev. 2006. Т. 73. С. 271.