Секція 1

ЗАСТОСУВАННЯ МОБІЛЬНИХ ОС У КРИТИЧНО ВАЖЛИВИХ СИСТЕМАХ

Литвинов О. А.
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник: Пєвнєв В.Я.

Актуальність. На даний момент у світі все переходить на керування з використанням ОС. Це приносить нові проблеми пов'язані с тим на якій саме ОС буде працювати та чи інша система. Найпоширеніші системи на так званому персональному комп'ютері Windows, Linux та її різновиди, також є macOS. Серед мобільних систем які використовують на даний час все сильно простіше: android та IOS, також нішевими є похідні дистрибутивів Linux, але вони використовуються значно рідше, android також є похідною, але все ж вважається як окрема система. Також системи поділяють по архітектурі центрального процесора x86 та ARM, не для всіх систем це має багато сенсу, бо наприклад Windows 11 працює на двох архітектурах, і може емалювати для запуску додатків протилежну архітектуру. Але в основі своїй комп'ютерні ОС працюють на першій архітектурі, а мобільні відповідно на другому типі. Але ця грань з кожним роком становиться більш розмитою. Як наслідок, компанії розглядають інтеграцію у свою систему нових ОС, включаючи мобільні, що привносить можливі проблеми з безпекою, тому перед інтеграцією, потрібно провести аналіз можливості використання ОС та її безпеку.

Мета. Метою роботи є аналіз можливості використання мобільних ОС та в цілому COTS пристроїв в критично важливих системах (КВС).

Основні положення. КВС – це комп'ютерні системи, які можуть призвести до травм, або загибелі людей у разі їх збою, або несправності, а також можуть завдати шкоди іншому обладнанню або навколишньому середовищу у разі несправності [1]. В першу чергу треба розглянути можливість загроз зараження пристроїв зловмисним ПЗ. Статистично на Android зловмисних програм на 744% більше ніж на Linux [2] який використовується як ядро у різних системах в тому ж числі критично-важливих. Частину загроз є можливість уникнути, обмеживши пристрою доступ до непотрібних для роботи сайтів та завантаження додатків. Згідно зі звітом про глобальні ризики Всесвітнього економічного форуму за 2022 рік, 95% проблем кібербезпеки пов'язані з людською помилкою [3]. Це є тривожним сигналом для всіх організацій. Тепер ці пристрої мають доступ до конфіденційних даних компанії та пряме підключення до корпоративної мережі. КВС можуть бути змішаними в випадках коли в цілому вся система не є критичною. Наприклад комерційний літак, він має управляючу

систему, та медійну, перша є КВС, а для другої сертифікування, як для першою, надмірне та затратне. Стандарти підтримують змішану критичність у випадках коли системи ізольовані одна від одної як фізично, так і логічно. Та така система повинна гарантувати що менш критична система не призведе до проблем с КВС [4].

Висновки. Проаналізовано можливість використання COTS пристроїв у КВС. Виявлено, що мобільні ОС, мають багато різних зловмисних програм. Небезпека використання мобільних ОС для контролю над критично важливими системами полягає в їх величині, що ускладнює їх сертифікацію та контроль за їх точністю. Це може призвести до помилок. COTS пристрої вже використовуються в КОС, але частіше всього вони не є мобільними ОС. COTS пристрої можуть бути лише частиною КОС, а не її цілком. Кожна система вимагає конкретних функцій, які повинні бути відлагоджені. У випадку мобільних ОС це означає додатковий час на відлагодження потрібних налаштувань.

Список літератури

1. W. Yeager, M. Leibham, J. Bartman. Safety-Critical Systems. *Web Archive* URL:https://web.archive.org/web/20201010000538/https://sites.google.com/site/cis115textbook/safety-critical-systems (дата звернення 26.10.2024).
2. Total amount of malware and PUA under Windows. *AV-ATLAS – Malware and PUA*. URL – https://portal.av-atlas.org/malware/statistics (дата звернення: 26.10.2024).
3. Зловмисне ПЗ для мобільних пристроїв у 2022 році. *КО IT для бізнесу*. URL:https://ko.com.ua/zlovmisne_pz_dlya_mobilnih_pristroyiv_u_2022_roci_142676 (дата звернення: 26.05.2024).
4. Jonsson E. Mobile Interaction with Safety Critical Systems : A feasibility study. 2015. URL: https://www.semanticscholar.org/paper/Mobile-Interaction-with-Safety-Critical-Systems-%3A-A-Jonsson/86fc8210c7da987327c96a24f87b7b4033f9a15c (дата звернення: 26.05.2024).

Відомості про авторів

Литвинов Олександр Андрійович, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», a.lytvynov@student.csn.khai.edu
Пєвнєв Володимир Яковлевич, професор кафедри комп'ютерних систем, мереж і кібербезпеки, НАУ «ХАІ», д.т.н., доцент, v.pevnev@csn.khai.edu