Засоби та стратегії для захисту від шкідливих програм і вірусів

Грищенко Юрій, ПЗС-2

Три ступені захисту

1) **Не завантажувати** шкідливі програми

2) **Не запускати** шкідливі програми

3) **Ізолювати** шкідливі програми

Хто відповідальний за безпеку?

Безпеку комп’ютерної системи забезпечує:

Сама система

Користувач системи

Хто відповідальний за безпеку?

Безпеку комп’ютерної системи забезпечує:

Сама система

- Верифікація
- Ізолювання
- Прозорість

Хто відповідальний за безпеку?

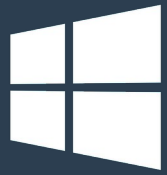
Безпеку комп’ютерної системи забезпечує:

Сама система

- **Windows**
- **macOS**
- **Linux**
- **Android/iOS**
- **Веб-застосунки**

Різні моделі безпеки!

Модель безпеки «Windows/MS-DOS»



Класична модель

- Будь-хто може скомпілювати програму
- Користувач обирає будь-яку програму
- Будь-хто може запустити програму
- Програма може робити будь-що*

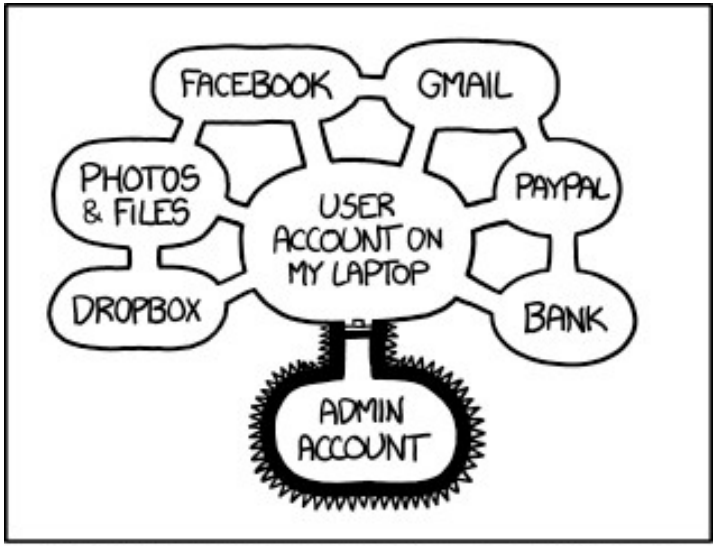
* грубо кажучи

Модель безпеки «Windows/MS-DOS»

Класична модель

- Будь-хто може скомпілювати програму
- Користувач обирає будь-яку програму
- Будь-хто може запустити програму
- Програма може робити будь-що*

* грубо кажучи



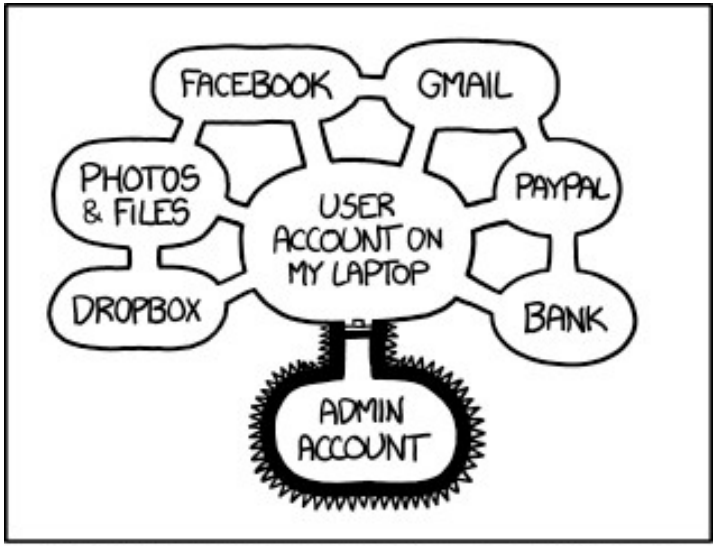
Модель безпеки «Windows/MS-DOS»

Класична модель

- Будь-хто може скомпілювати програму
- Користувач обирає будь-яку програму
- Будь-хто може запустити програму
- Програма може робити будь-що*

  * грубо кажучи

- Можливо, антивірус виявить шкідливу програму



Модель безпеки «macOS»

Централізована перевірка

- Apple перевіряє програми
- Користувач обирає програму **переважно з App Store**, якому **переважно довіряють**
- **Неперевірену програму запустити складніше**
- Програма може робити будь-що, грубо кажучи
- Можливо, антивірус виявить шкідливу програму

Модель безпеки iOS

Централізована перевірка **+ ізоляція**

- Apple перевіряє програми
- Користувач обирає програму **тільки з App Store**
- Сторонню програму **запустити вкрай складно**
  - Jailbreak...?
- Вірогідно, **ізоляція обмежить шкідливі дії**
- **Прозорість:** чіткі дозволи

Модель безпеки Android

Централізована перевірка + ізоляція

- Google перевіряє програми в Google Play
- Користувач обирає програму **переважно з Google Play**
- Сторонню програму **запустити трохи складно**
  - Можливе встановлення APK: F-Droid, itch.io...
- Вірогідно, ізоляція обмежить шкідливі дії
- Прозорість: чіткі дозволи

Модель безпеки веб

Ізоляція

- Будь-хто може створити веб-застосунок
  - Скажімо, на адресі накшталт `mircosoft.com...`
- Користувач заходить на будь-який веб-сайт
- Веб-застосунок миттєво запускається
- Вірогідно, ізоляція обмежить шкідливі дії
- Прозорість: чіткі дозволи

Модель безпеки Google Safe Browsing

Ізоляція + **деяка перевірка?**

- Будь-хто може створити веб-застосунок
  - **Google прослідковує шкідливі програми, соціальну інженерію...**
- Зайти на сайт, **відфільтрований через Safe Browsing, досить складно**
- Вірогідно, ізоляція обмежить шкідливі дії
- Прозорість: чіткі дозволи

Google

Модель безпеки Google Safe Browsing

Ізоляція + **деяка перевірка?**

- Будь-хто може створити веб-застосунок
  - **Google прослідковує шкідливі програми, соціальну інженерію...**
- Зайти на сайт, **відфільтрований через Safe Browsing, досить складно**
- Вірогідно, ізоляція обмежить шкідливі дії
- Прозорість: чіткі дозволи
- **Постають питання щодо приватності**

Google

Модель безпеки open-source

Відкритий код, «децентралізована перевірка»

- «при достатній кількості очей баги випливають на поверхню» - закон Лінуса
- Проекти мають сторонніх контрибуторів
- Користувач завантажує програми не напряму, а через довіреного посередника — **дистрибутив Linux**
- Дистрибутивів багато, незалежні один від одного

Модель безпеки open-source

Користувач завантажує програми не напряму, а через довіреного посередника — **дистрибутив**

- **Проте часто необхідно встановити безпосередньо**
- Встановити програму напряму — **можливо, але не рекомендовано**
- Інсталяція сторонніх програм часто складна (PPA, Arch User Repository, компіляція кода з GitHub...)
- **«Простий спосіб», але не дуже безпечний:**

```
> curl https://program.com/install.sh | sudo bash -
```

Панацеї немає!

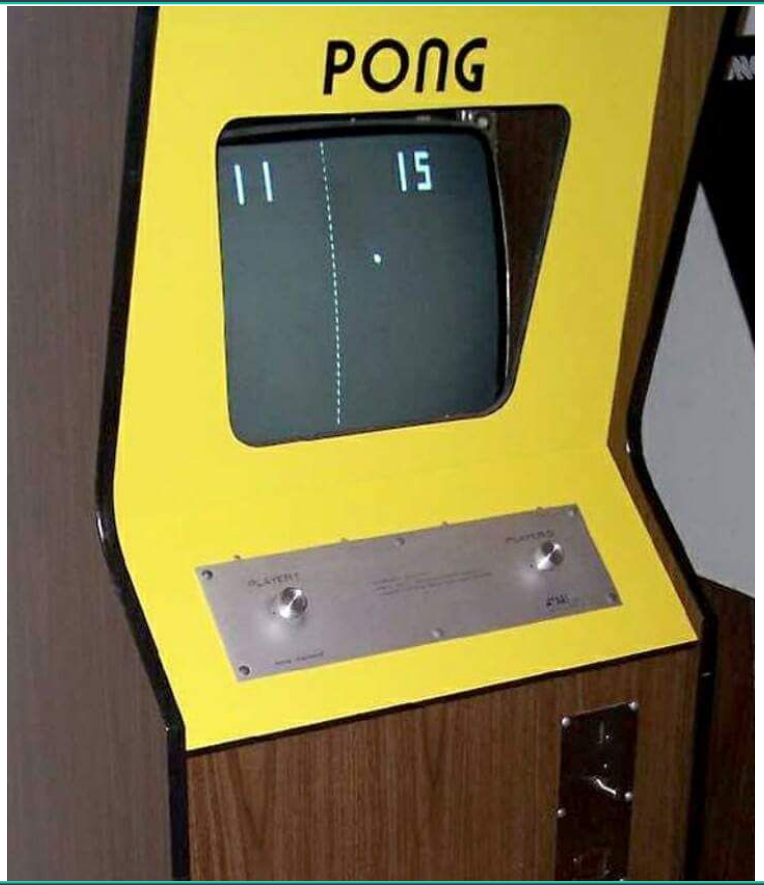
Ізоляція не є ідеальною!

«Перевірка» програм не завжди можлива або бажана!

Панацеї немає!

Система не гарантує захисту від шкідливих програм.

Єдина безпечна система — повністю ізольована, де нічого не можна встановити.



Хто відповідальний за безпеку?

Безпеку комп’ютерної системи забезпечує:

Сама система

Користувач системи

Хто відповідальний за безпеку?

- Обирайте довірені джерела
- Не довіряйте чужинцям (pop-ups, посилання)
- Встановлюйте оновлення

Користувач системи

Обирайте довірені джерела

- Користувачі Windows: знаходьте офіційні сайти
- Піратство несе великий ризик

Обирайте довірені джерела

- Використовуйте довірені платформи
  - «Нішеві» платформи — **security through obscurity**?
  - Користувачів macOS та Linux менше, ніж користувачів Windows
  - Тому macOS та Linux менш привабливі для хакерів
  - Але на це не варто розраховувати

Встановлюйте оновлення

- **Оновлення системи** забезпечують покращену роботу ізоляції, антивірусів, тощо.

Не довіряйте чужинцям

- **Оновлення системи** забезпечують покращену роботу ізоляції, антивірусів, тощо.
- Але не довіряйте чужинцям, наприклад, popup-вікнам.
- Перевіряйте URL посилань.

Для просунутих користувачів

Ізоляція програм: можна зробити власними руками

- Віртуальні машини: наприклад, для Windows XP
- Спеціальні інструменти: Docker, bubblewrap, Flatpak, ...
- The Amnesiac Incognito Live System (Tails)
  - Працює лише з оперативною пам’яттю, не записує дані на диск
  - Анонімність завдяки Tor
  - Максимальна ізоляція

Дякую за увагу!

Грищенко Юрій, ПЗС-2