УДК 004.056: 004.73

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ КОМПОНЕНТІВ СПОЖИВАЦЬКОЇ ЕЛЕКТРОНІКИ

О. П. Войтович, к. т. н., доцент;
М. О. Губрій; Р. В. Шашков
Вінницький національний технічний університет
o_voytovych@mail.ru

На теперішній час *nix-системи використовуються як у класичних комп'ютерних системах, так і в різних компонентах споживацької електроніки. Часто останні не сприймаються користувачами як реальні інформаційно-комунікаційні системи, а тому до них не висувається всі ті вимоги безпеки, які є обов'язковими для класичних комп'ютерних систем. Проте треба пам'ятати, що по мірі того, як зростає кількість «розумних» пристроїв, якими користуються пересічні споживачі і комерційні компанії, росте і кількість «нових» загроз. Холодильник, що розсилає спам, телевізор, який бере участь в DDoS-атаці, заражений маршрутизатор, що перенаправляє будь-які запити на сервери, що належать кіберзлочинцям - це те майбутнє, яке вже наступило. Використання все тих же «розумних» пристроїв для кібершпіонажу - це вже не фантастика, а сьогодення. Вразливості компонентів споживацької електроніки спричинені в тому числі парадигмою інформаційної безпеки, що встановилась в сучасних інформаційних системах, де доступність (зручність використання для користувачів) переважає над конфіденційністю даних.

Отже виникла необхідність покращення безпеки інформаційно-комунікаційних систем у компонентах

споживацької електроніки, і в першу чергу необхідно розпочати з дослідження вразливостей, які для них характерні.

В споживацькій електроніці використовуються спеціалізовані операційні системи, більшість з яких дистрибутиви Linux різних версій. Спеціалізовані операційні системи для маршрутизаторів: Coyote Linux, Endian, Engrade Linux, Freesco, Ideco Internet Control Server, IPCop, IPFire, Kerio Control, Mikrotik RouterOS, m0n0wall, pfSense, SmoothWall, Untangle, Vyatta, Zentyal(eBox), Zeroshell. Cisco IOS - багатозадачна операційна система, що виконує функції маршрутизації, комутації і передачі даних, особливістю якої є її використання лише на відповідному обладнанні. Операційна система Maemo дистрибутив Debian призначений для смартфонів та інтернет-планшетів. На великій кількості споживацької електроніки (зокрема планшетних комп'ютерах та смартфонах) встановлено ОС Android, яка розроблена на базі ядра Linux. На телевізорах компаній LG та Samsung використовується технологія SMART TV, яка використовує міні-дистрибутив Linux.

Аналіз літературних джерел щодо вказаних операційних систем показав, що для більшості з них характерні однакові вразливості:

– погано написані програми (відсутність перевірки та фільтрації вхідних даних, використання небезпечних бібліотек, недотримання правил написання безпечного коду);

– наявність демонів (потенційно небезпечно через можливість активного дослідження, а також використання вразливостей демонів для атак);

– небезпека застосування атрибутів SUID/SGID (використання заданих по замовчуванню облікових записів та призначених їм прав);

– людський фактор.

Для дослідження вразливостей операційних систем використовується, в тому числі тест на проникнення, який моделює дії зовнішніх або внутрішніх зловмисників з взламу системи. При цьому використовуються моделі типу «чорна скринька» (відсутня інформація про внутрішні характеристики системи, найчастіше використовується) або «біла скринька» (забезпечується системна інформація про об'єкт).

Логічна послідовність виконуваних зловмисником дій, зазвичай, полягає в проникненні за допомогою віддаленого доступу, використовуючи будь-які вади в захисті служб, що знаходяться в стані очікування запитів, з наступним отриманням локального доступу до командної оболонки. Першим кроком зловмисника є дослідження операційної системи і складання схеми вразливих місць, тобто знаходження відповідності між певними атрибутами безпеки системи з відповідними явними або потенційними вадами. Можливими методами складання схеми вразливих місць можуть бути застосування загальнодоступних спеціальних інструментів або написання власного програмного коду, використання засобів, призначених для автоматичного сканування систем у пошуках вразливих місць, визначення вручну, як співвідносяться певні атрибути системи з інформацією про виявлені недоліки. Найбільш вживані засоби для дослідження операційних систем: Nmap, Zenmap, Nesus, Xspider, X-scan, OpenVAS, GFI LANguard, SAINT, Rapid 7 NeXpose. Основними методами для віддаленого проникнення є проникнення через службу, що знаходиться у стані очікування запитів, використання у якості плацдарму системи.

В подальшому планується розробити методологію дослідження вразливостей компонентів споживацької електроніки.