АНАЛІЗ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ АРХІТЕКТУРИ КЛІЄНТ-СЕРВЕР

Колісник М.О.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Відомо, що перспективною технологією обробки даних на цей час є архітектура “клієнт-сервер”. До якості функціонування цих архітектур висуваються високі вимоги. Забезпечення таких вимог можливе за умов високої надійності апаратних засобів (як компонентів серверів, робочих станцій, так і ліній передачі даних та мережевого обладнання) та програмного забезпечення (системного та прикладного), а також їх високої стійкості при впливі зовнішніх та внутрішніх потенційних загроз.

До основних джерел уразливості цифрових систем передачі можна віднести дефекти програмного забезпечення й особливості передачі даних по каналах зв’язку, а саме: кодів операційної системи (ОС) (при переповненні пам’яті, при керуванні оновленнями ОС, в самих оновленням можуть бути вбудовані модулі програмних вкладень і т.і.); помилки в програмах користувача; при передачі інформації по протоколам різних рівнів моделі OSI (TCP, DNS, SMTP, ICMP); дефекти прикладних програм (firmware, наприклад, Apache); програми, вбудовані в апаратні засоби (в маршрутизатори, BIOS, контролери, процесори); підбір паролів; зловмисні програми з пристроїв, що підключаються до мережі (флеш-пам’ять, DVD, ноутбуки, планшети, смартфони); перехоплення повідомлень і керування в проводових та безпроводових мережах.

Для забезпечення захищеності цифрових систем від уразливостей необхідно своєчасно і вірно діагностувати вид зловмисної дії всередині пристрою (програмні закладки, що можуть перевести пристрій у несправний технічний стан або скопіювати інформацію і надіслати її зловмиснику) та зовнішні уразливості при передачі даних по мережі, та попередити або усунути її наслідки. Для цього доцільно провести аналіз видів можливих потенційних загроз та методів їх попередження й усунення.

Все більше серверів та робочих станцій потрапляють під дію DoS-атак (Denial of Service - відмова в обслуговуванні). Причиною таких атак часто стають боти. Боти і ботнети можуть проводити наступні шкідливі дії: організовувати масову спам-розсилку; брати участь в DoS і DDoS атаках (створювати умови, при яких доступ користувачам системи до надаваних системою ресурсів блокується або утруднюється); брати участь в brute-force атаках (за допомогою спеціальних “троянських” програм методом підбору обчислювати необхідні для проникнення в мережу паролі); завантажувати з командного центру і виконувати шкідливий код.

Слідуючи з вищесказаного, необхідною та актуальною задачею є забезпечення високої надійності реалізації архітектури клієнт-сервер. Високу надійність архітектури необхідно забезпечувати не лише методами підвищення надійності апаратних та програмних засобів серверів, робочих станцій та мережевих пристроїв, а і методами попередження й усунення наслідків різних видів уразливостей.