УДК 004

МУЛЬТИФАКТОРНА МОДЕЛЬ ПОРУШНИКА З КОЛАПСОМ

О. В. Кіреєнко[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

В цій роботі представлено мультифаторну модель порушника, в якій допускається колапс. Описано різні підходи запобігання колапсу та відновлення системи після нього. Запропоновано сценарну модель із відновленням після колапсу.

Ключові слова: модель порушника, мультифакторна модель порушника, колапс моделі, відновлення після колапсу, зворотній зв'язок

Вступ

При розробці системи захисту інформації необхідно вирішити, від кого ми захищаємо інформацію. Порушники інформаційної безпеки суттєво відрізняються за рівнем знань, досвідом, ресурсами та іншими факторами. Згідно з НД ТЗІ 1.1-003-99 vодель порушника (user violator model) – абстрактний формалізований або неформалізований опис порушника. При розробці моделі порушника потрібно пам'ятати, що в першу чергу нас цікавить можливий вплив порушника на систему. Мультфиакторні моделі порушника є формалізованим описом, в якому встановлені зв'язки між факторами, що характеризують порушника, або в явному вигляді вказана відсутність таких зв'язків. У стандарті ISO/IEC 15408-1 «Evaluation criteria for IT security» вказано вимоги до оцінки IT-безпеки. Однією із вимог даного стандарту є зворотній зв'язок, що передбачає можливість модифікації моделі порушника на основі нових даних. В однофакторних моделях дані про порушника отримують із суджень експертів та/або на основі статистичних даних. Початковий набір даних в таких моделях може бути узгодженим, але імовірність виникнення помилок при їх оновленні вища. Мультифакторні моделі накладають додаткові обмеження на оновлення даних в моделі. Ці обмеження стосуються швидкості зміни факторів, їх максимальних та мінімальних значень, а також початкових значень.

1. Моделі порушника і критичні значення

Якщо мультифакторна модель містить лише фактори, що підсилюють одне одного, в ній може відбутися колапс. При колапсі значення факторів досягають деякого критичного рівня. В цей момент модель можна вважати виродженою. Колапс можна спостерігати і в однофакторних моделях. В загальному випадку колапс вказує на швидке, неконтрольоване зростання рівня загрози порушника, при якому будь-які засоби захисту втрачають ефективність. Допустимим є і протилежний випадок, при якому можливості порушника швидко знижуються до рівня, коли сторона захисту може його просто ігнорувати. Вироджена модель не несе цінної інформації для сторони захисту. Стороні захисту відомі критичні значення факторів. Прикладом критичних значень для апаратного забезпечення є:

- пропускна здатність каналів зв'язку;
- відмовостійкість обладнання;
- обсяг вільної пам'яті на жорстких дисках;
- наявність автономних джерел живлення;
- вартість обслуговування;
- вартість ремонту;
- вартість аренди.

Сторона захисту може виміряти пропускну здатність каналів зв'язку (якщо вони були встановлені самостійно) або визначити цю величину на основі тарифу на інтернет (якщо це розподілена система). Ця інформація дозволяє досить точно оцінити загрозу атаки на відмову в обслуговуванні. Якщо сторона захисту не використовує жодних додаткових засобів захисту від DOS-атак, критичним значенням буде пропускна здатність. Якщо порушник має досить ресурсів для генерації трафіку, що відповідає пропускній здатності каналів зв'язку, його рівень загрози буде співрозмірним рівню загрози порушника, який може згенерувати в 100 разів більше трафіку. В обох випадках канал зв'язку буде повністю зайнятий. Якщо розглядати цю проблему ізольовано, то будь-які значення в моделі, що перевищують критичні, практично не несуть корисної інформації. В якості прикладу із виродженням моделі та зниженням загрози від порушника можна розглянути придбання стороною захисту автономних джерел живлення в достатній кількості. Якщо єдиним засобом атаки для порушника є опосередкована атака через пошкодження електромережі, поступове нарощення кількості автономних джерел живлення зробить дану атаку не-

[a] kirealex12@gmail.com

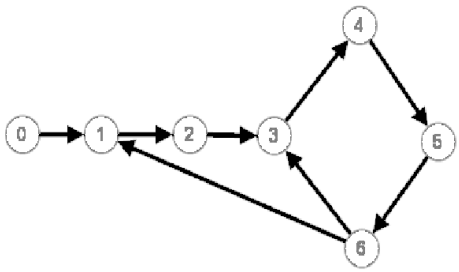

Рис. 1. граф мультифакторної моделі

ефективною. Критичним значенням в цьому випадку є кількість автономних джерел живлення.

2. Типи колапсу

Для однофакторних моделей порушника найбільш характерним є колапс, що залежить від початкових умов. Так як в таких моделях відсутні зв'язки між факторами, будь-які висновки щодо можливого колапсу можна робити лише на основі занесених до моделі даних. В таких моделях ми можемо виявити «небезпечні» для сторони захисту значення факторів, але не тенденцію їх утворення. Під питанням залишається і виведення системи із стану колапсу. В мультифакторних моделях порушника можна виявити наближення системи до колапсу. Колапс найчастіше виникає в тих випадках, коли декілька факторів, що підсилюють одне одного, утворюють цикл із позитивним зворотнім зв'язком. Також причиною колапсу може стати досягнення критичного значення деяким фактором. Виведення системи із стану колапсу можливе, але потребує зовнішнього впливу. «Повільний колапс» – це особливий випадок, при якому запланований термін функціонування системи співрозмірний із терміном досягнення критичних значень факторів. Також може виникати ситуація із «гонкою озброєнь», коли сторона захисту та порушник одночасно прямують до критичних значень (швидке зростання можливостей або швидка деградація).

2.1. Колапс в мультифакторних моделях

Мультифакторну модель зручно представляти у вигляді орієнтованого графу. Вершини графу відповідають факторам, а дуги – зв'язкам між ними. В такому представленні однофакторна модель буде просто набором вершин.

На рис 1 представлено мультифакторну модель, в якій фактори 3, 4, 5 та 6 утворюють петлю зворотнього звязку. Якщо відповідні зв'язки між факторами є підсилюючими, виникає загроза колапсу. Дуга 6-1 може відповідати як виходу із колапсу за рахунок зовнішнього влпиву, так і бути частиною контуру 1-2-3-4-5-6-1. В другому випадку, дуга 6-1 має відповідати від'ємному зворотньому зв'язку. Представлення моделі за допомогою графу має наступні обмеження:

1) значення факторів (вершин графу) змінюються з деякою швидкістю;
2) перехід із вершини A у вершину B залежить від поточних значень факторів, яким відповідають дані вершини;
3) допускається одночасний вплив одного фактора на декілька інших факторів;
4) допускається одночасний вплив декількох факторів на один фактор;
5) правила вибору маршруту можуть спричиняти конфлікти.

Для того, щоб модель порушника могла коректно оновлюватися, необхідно розглянути кожне із цих обмежень вже в контексті прикладної задачі. В першу чергу нас цікавить «реакція» фактора на спробу змінити його значення зі швидкістю вищою, ніж це допускає модель. В найгіршому випадку порушення обмеження на швидкість зміни значення фактора призводить до колапсу, навіть якщо саме значення фактору ще не є критичним. Раптовий вихід з ладу значної частки обладнання може і не призвести до миттєвого краху всієї системи, але обмежить можливості по відновленню системи і запустить незворотні процеси. В роботі [1] автор розглядає системи із зворотніми зв'язками. Часто причиною появи позитивних зворотніх звязків, що руйнують систему, є прийняття симптоматичних рішень замість радикальних. Симптоматичні рішення допускають тимчасове покращення ситуації «зараз» за рахунок її різкого погіршення «потім». В контексті даної моделі порушника симптоматичному рішенню відповідатиме спроба виходу із колапсу (дуга 6-1) за рахунок неприпустимо сильного впливу на фактор 6 (вирішення проблеми «тут і зараз»). Радикальне рішення передбачає недопущення утворення конуру 3-4-5-6-3 (сторона захисту намагається впливати на кожен із факторів в моделі) або зниження рівнів підсилення факторів в контурі до прийнятного рівня (повільний колапс). Описана в [1] «пивна гра» є ілюстрацією колапсу системи. Хоча автор не називає жодного із учасників («продавець», «постачальник», «виробник») порушником, дії кожного із учасників ведуть до колапсу. Основною відмінністю між «пивною грою» та конфліктом між стороною захисту та порушником є злочинні наміри порушника. Учасники «пивної гри» можуть домовитися, а сторона захисту і порушник – ні. Метою порушника є отримання прибутку, а переведення системи в стан колапсу – один із способів досягнення цієї мети. Розглянемо проблему вибору маршруту на прикладі графу на рис 1. В мультифакторній моделі порушника може діяти одне або декілька правил із наступного списку:

1) перехід визначається поточним станом вершини, з якої виходить дуга;
2) перехід визначається значеннями вершин, в які входять дуги із поточної вершини;
3) перехід визначається величиною зміни поточного стану вершини, із якої виходить дуга;
4) перехід визначається величиною зміни значень вершин, в які входять дуги із поточної вершини.

На рис 1 з вершини 6 виходять дуги 6-3 та 6-1. Введемо функцію $S(V, E)$, що приймає в якості параметру граф мультифакторної моделі. V та E – множини

ребер та вершин графу із зазначенням поточних значень факторів (множина V). Дана функція повертає нову пару (V', E'), розраховану на основі приведених вище правил.

$$S(V_0, E_0) = \begin{cases} (V_1, E) & V_0[6] \leq 5 \\ (V_2, E) & \dfrac{V_2[3]}{V_0[3]} \leq 1 \end{cases}$$

В цьому прикладі модель переходить в стан V_1, якщо значення фактору 6 не перевищує 5(що є критичним значенням для цього фактору). Якщо дана умова не виконується, починається колапс, що буде продовжуватися, доки фактор 3 не почне знижуватися. Якщо жодна із умов не виконується або виконується більше ніж 1 умова, функція $S(V, E)$ має повертати значення V, E без жодних змін. Якщо в моделі не залишилося допустимих переходів і критичні значення факторів не були досягнуті, це є достатньою умовою встановлення рівноваги між порушником та стороною захисту. Рівновага може бути порушена зовнішнім впливом. Щоб врахувати зовнішній вплив, потрібно замінити функцію $S(V, E)$ на $S(V, E, c)$, де c – набір додаткових умов, лічильників і таймерів, що впливають на вже задані в $S(V, E)$ умови. Переведення системи в стан рівноваги є одним із способів запобігання колапсу або його відтермінуванню. Прикладом приведення системи до рівноваги є ситуація, коли порушнику потрібно одночасно використати деякий ресурс та атакувати деяку ціль. При цьому використання ресурсу зробить ціль не доступною, в той час як атака цілі знищує ресурс. Розглянемо ситуацію, при якій порушник збирається атакувати систему деякої організації. Дана атака неодмінно призведе до збитків для організації і відобразиться на працівниках у вигляді зниження зарплати та/або залученню їх до понаднормової роботи. В таких умовах завербувати спільника із цієї організації буде складніше (спільник постраждав від проведення атаки і може відмовити в допомозі або «погодитися» і зірвати наступну атаку). З іншого боку – вербувати спільника перед проведенням атаки теж ризиковано, тому що це може викликати підозри і можливість для проведення атаки буде втрачено. Так як деякі переходи залежать від поточного стану вершин, в які входять дуги, або від обмежень, що накладають на швидкість зміни цих значень, потрібно задати правила, за якими ці величини будуть порівнюватися. На рис 1 вершини $V[1]$ та $V[3]$ можуть відповідати знанням порушника про систему та його ресурсам відповідно. Якщо обмеження призводять до руху вздовж контуру 1-2-3-4-5-6-1, в порушника будуть змінюватися обидва фактори. Якщо замість цього рухатися по контуру 3-4-5-6-3 змінюватиметься лише фактор, що відповідає ресурсам. В роботі [2] описано способи приведення різних нематеріальних величин до єдиної шкали. Для моделі порушника можна використати аналогічний підхід і привести значення факторів до «вкладу» в проведення успішної атаки. У приведеному вище прикладі обмеження $\frac{V_2[3]}{V_0[3]} \leq 1$ стосується значення лише одного фактору. Це обмеження враховує лише 2 послідовні значення фактора $V[3]$. Особливу увагу потрібно приділяти обмеженням на приріст фактору. Навіть якщо приріст деякого фактору (або його вплив на інші фактори) зменшується, дані зміни потрібно враховувати. В [2, стор.29] це було показано на прикладі суми гармонічного ряду. Можливість виявляти подібні «контрінтуїтивні» результати була врахована в цій моделі.

3. Сценарна модель. Відновлення після колапсу

В сценарній моделі порушника кожному порушнику ставиться у відповідність множина атак A. Для будь-якої атаки із множини A можна знайти такий набір значень факторів, при яких цю атаку вважаємо успішною.

$$L_1^{min} \leq V[1] \leq L_1^{max},$$
$$L_2^{min} \leq V[2] \leq L_2^{max},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$L_n^{min} \leq V[n] \leq L_n^{max}.$$

Не всі значення факторів можуть бути суттєвими для конкретної атаки. Якщо для якогось значення $V[i]$ умови L_i^{min} та L_i^{max} не виконуються, атака може відбутися, але при цьому:

- знижується імовірність успіху;
- знижується прибуток від атаки у разі успіху;
- знижується тривалість атаки (якщо це атака на відмову в обслуговуванні);
- зростає тривалість атаки (атаки, що порушують цілісність та/або конфіденційність);
- зростають витрати порушника на проведення атаки;
- у випадку невдачі зростає час на підготовку до наступної атаки.

Перехід моделі до стану колапсу не означає крах системи. Система може функціонувати і після досягнення факторами їх критичних значень. Стан колапсу означає лише загальне зростання можливостей порушника до проведення атак, хоча для проведення конкретної атаки умови L_i^{min} та L_i^{max} можуть не виконуватися. Проведення атаки додатково змінює значення $V[i]$. Формуючи модель порушника, сторона захисту повинна вирішити, чи є прийнятним тимчасовий вихід із стану колапсу за рахунок симптоматичних рішень. В роботі [3, стор.58] конфлікт сторони захисту та порушника віднесено до «задач, які складно формалізувати». Основними причинами цього є прийняття рішень сторонами конфлікту в умовах невизначеності та деякими «пороговими» значеннями обізнаності сторін. Якщо розглядати конфлікт сторони захисту та порушника з точки зору теорії ігор, до моделі потрібно внести наступні зміни:

1) ввести обмеження на точність, з якою задані значення факторів (відоме точне значення / проміжок із розподілом імовірностей / проміжок без заданого розподілу / відсутність інформації);

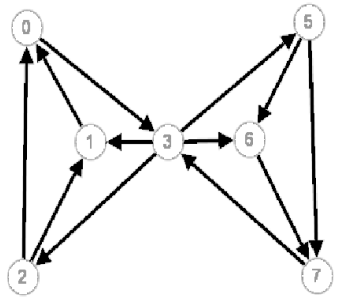

Рис. 2. симптоматичні рішення

2) ввести обмеження на час доступу до інформації про фактори (значення фактора відоме в довільний момент часу / значення фактора можна перевіряти через фіксовані проміжки часу / відоме лише початкове значення фактору);
3) ввести обмеження на сукупну кількість інформації про фактори (доступ до всієї інформації в межах перших двох пунктів цього списку / обмеженням є деяка кількість факторів при довільній кількості інформації по кожному з них / обмеженням є деяка кількість пам'яті, в якій зберігаються значення факторів);
4) обмеження інформації про зв'язки між факторами (характер зв'язку визначають за принципом «чорного ящику» по змінах значень у відповідних вершинах графу).

На рис 2 представлено граф мультифакторної моделі, де враховано симптоматичні рішення. В цьому графі вершина $V[3]$ – єдиний фактор, від якого залежить успішність атаки порушника. Контури 1-0-3-1 та 5-6-3-5 відповідають радикальним рішенням сторони захисту та порушника відповідно. При наближенні значення $V[3]$ до інтервалу $[L_3^{min}, L_3^{max}]$, сторона захисту може прийняти симптоматичне рішення (перехід 3-2 може відбутися лише при неприпустимій швидкості зміни фактору $V[3]$), що повертає значення $V[3]$ до прийнятного рівня, але негативно впливає на фактори $V[0]$ та $V[1]$. Порушник теж може використовувати симптоматичне рішення (перехід 3-5). Яскравим прикладом симптоматичного рішення проблеми для сторони захисту є сплата викупу після зараження системи вірусом-шифрувальником (ransomware). Також до симптоматичних рішень можна віднести будь-яке скорочення штату та відмову від створення резервних копій/-зниження частоти резервного копіювання. Для порушника прикладом симптоматичного рішення буде відмова від залучення спільників (прибуток від успішної атаки не доведеться ділити, але множина допустимих атак скорочується)

Висновки

Колапс, який можна спостерігати при розробці/оновленні моделі порушника не є позаштатною ситуацією. Є два види колапсу – для сторони захисту та порушника. В стані колапсу (для сторони захисту) значення одного або більше факторів задовольняють умовам L_i^{min} та L_i^{max} і можна спостерігати тенденцію до збереження значень цих факторів на даному рівні. У випадку колапсу для порушника відповідні значення факторів будуть максимально віддалені від L_i^{min} та L_i^{max} і, як і в попередньому випадку, їх значення будуть зберігатися на поточному рівні. Проведення успішної атаки порушником потребує виконання всіх умов L_i^{min} та L_i^{max}. Відхилення від цих значень знижує ефективність відповідних атак. Для застосування мультифакторної моделі порушника з колапсом необхідно виконати наступні кроки:

1) визначити, від стану яких факторів залежать атаки порушника;
2) побудувати модель (на основі графу), що містить фактори із 1) та фактори, що на них впливають;
3) для даного графу визначити правила та обмеження впливу факторів одне на одного;
4) перевірити, чи знаходиться дана модель в стані колапсу, якщо так то:
   - знайти спосіб виходу із колапсу (симптоматичне або радикальне рішення; для конкретної системи може не існувати розв'язку);
   - ізолювати частину факторів, що спричиняють колапс, від решти (це дозволить зберегти контроль над рештою факторів, значення яких впливають на успішність атаки).
5) *додати одну або більше вершин(факторів), що відображатиме негативні наслідки від симптоматичних рішень;
6) на основі 3) згенерувати послідовність пар (V, E) за допомогою функції $S(V, E)$. (на цьому етапі ми дізнаємося, чи відбудеться колапс без будь-якого активного втручання порушника) Якщо послідовність прямує до колапсу, то додаткові активні дії порушника лише прискорять цей процес;
7) після необхідних змін, внесених до моделі на попередньому етапі, повторити крок 6) але з використанням функції $S(V, E, c)$.

*Даний пункт не є обов'язковим, так як симптоматичні рішення можуть бути недоступні та/або заборонені. Даний пункт можна реалізувати іншим способом, якщо замість вершин додавати нові ребра або дуги, але тоді граф не буде простим (без кратних ребер і петель).

Перелік використаних джерел

1. П. Сенге Пятая дисциплина — 2006. — С. 384 с. — Режим доступа: https://www.ozon.ru/context/detail/id/950887/.
2. Т. Саати Л. Принятие решений при зависимостях и обратных связях — 2008. — С. 360 с. — Режим доступа: https://www.twirpx.com/file/1898448/.
3. А. Росенко П. Внутренние угрозы безопасности конфиденциальной информации: Методология и теоретическое исследование — 2010. — С. 160 с. — Режим доступа: https://www.ozon.ru/context/detail/id/5045981/.