оброблюваних даних. Наслідком даного ефекту є той факт, що для певного діапазону розмірів вхідних файлів, починаючи з деякого значення, може бути заданий один і той же параметр, що є оптимальним в сенсі скорочення часу обчислень.

Висновки

В результаті проведеного дослідження може бути зроблено висновок про те, що процедура шифрування, що реалізовується на кластерах грід-мережі із застосуванням технології MPI, добре розпаралелюється і дозволяє досягти високих показників ефективності для широкого діапазону значень інтенсивності потоку даних без зміни основних параметрів обчислювального процесу.

Як результат даної статті можна також розглядати описаний досвід створення паралельних програм із застосуванням відповідного інструментального забезпечення, який може виявитися корисним для дослідників у різних наукових галузях.

1. *Антонов А.С.* Параллельное программирование с использованием технологии MPI: Учебное пособие. – М.: Изд-во МГУ, 2004. – 71 с.
2. *Шпаковский Г.И., Серикова Н.В.* Программирование для многопроцессорных систем в стандарте MPI. - Минск: Изд-во БГУ, 2002. – 323 с.
3. *Немнюгин С.А., Стесик О.Л.* Параллельное программирование для многопроцессорных вычислительных систем. – СПб.: БХВ-Петербург, 2002. – 400 с.

Поступила 22.02.2010р.

УДК 621.3

С.О.Нікулін

МЕТОДИ ФОРМУВАННЯ ОСНОВНИХ ІНФОРМАЦІЙНИХ ЗАСОБІВ СИСТЕМИ ЗАХИСТУ

Важливою компонентою довільної системи захисту являються дані про загрози. Останні представляють собою певні властивості об’єкту, що охороняється, який в даному випадку є системою управління спеціалізованим об’єктом. Виходячи з загально прийнятої інтерпретації поняття загрози [1] остання є негативною характеристикою системи. Тому при проектуванні системи передбачається не допускати в рамках останньої існування загроз. Практично, загрозами в інформаційній системі являються такі способи реалізації програмних засобів, які дозволяють або надають можливість використовувати відповідні фрагменти для несанкціонованого втручання в

роботу системи. На сьогоднішній день відомо цілий ряд засобів реалізації такого втручання [2]. Для запобігання таким способам фрагменти, що при цьому використовуються повинні проектуватися таким чином, щоб відповідний спосіб несанкціонованого втручання в роботу несанкціонованих факторів був неможливим. Прикладом класичної загрози, що може існувати в інформаційній системі може служити загроза, що дозволяє реалізувати зовнішнім чинникам переповнення буфера вводу даних [3]. У процесі проектування системи досить важко передбачити, яким чином треба сформулювати окремі фрагменти програмних засобів, щоб останні не могли бути використані несанкціонованими факторами для втручання в роботу системи. Очевидно, що відповідні вимоги до програмних засобів в частині всіх фрагментів можуть привести до того, що відповідний програмний продукт буде надмірним. Це обумовлюється тим ,що додаткові вимоги по відношенню до основних функціональних вимог, які визначаються необхідністю протидії можливим атакам, проводять збільшення об'єму програми. Але завдяки цьому відповідна загроза цим додатковим фрагментом нівелюється. Тому можлива атака уже не зможе використати відповідний фрагмент програми для втручання в роботу системи. Такий спосіб проектування системи, крім того, що приводить до виникнення надмірностей у програмі, що проектується, можливий лише в тому випадку, якщо відомі всі можливі атаки на об'єкт управління. Переважно такі дані у проектанта у необхідній мірі відсутні, оскільки небезпека може формувати нові атаки, які ще не використовувалися, і тому не можуть бути відомими проектантам системи управління. Для розв'язку проблеми, що виникає з приведених суперечливих вимог, що полягають у вимогах до створення оптимальних програмних засобів для розв'язку основних функціональних задач та вимог, що полягають у забезпеченні стійкості програмних засобів проти атак, формується система захисту, яка є окремою компонентою, співпрацює з системою управління спеціалізованого об'єкту. Формування системи захисту (SZ) таким чином, щоб вона представляла собою сукупність всіх необхідних засобів розпізнавання та засобів протидії сукупності можливих атак, недоцільно. Такий підхід приводить до недопустимого збільшення самої SZ, і, відповідно, до споживання великої кількості ресурсів обчислюваних засобів. Тому в рамках даної роботи реалізується підхід, в якому основними засобами захисту являються мобільні компоненти Zhi, які мігрують в середовищі об'єкту захисту в залежності від величини ризику виникнення в тому чи іншому місці інтруза. Завдяки цьому кількість Zhi буде в кожний момент ti скупчуватися в тих місцях середовища системи, в яких найбільше може виявитися інтрузів. Щоб уникнути необхідність формування різних типів Zhi, кожний з яких відповідав би різним типам атак, функціонування Zhi буде реалізовуватися на основі технології honeypot. Це дозволить використати наступні можливості:

- процес розпізнавання чи ідентифікації атаки реалізовувати в рамках елемента типу honeypot, яким являється Zhi, що дозволяє небезпеку, що

реалізує атаку нейтралізувати, перевіривши останню на Zhi;

- оскільки Zhi формально описується у вигляді автомату U(A, Q, B, φ, ψ, q0), то існує можливість останній адаптувати до відповідного типу атаки, який описується певним вхідним словом і може розпізнавати U(A, Q, B, φ, ψ, q_0)

З приведеного вище видно, що описи атак, які представляють собою послідовність подій можна представити у вигляді абстрактного слова мови M, яке може розпізнаватися автоматом Zhi. Оскільки такого абстрактного опису недостатньо, то необхідно використовувати словники опису атак, які дозволили б переводити їх абстрактний опис на прикладну мову користувача або проектанта. У цьому випадку слово {ai1, .., ain}мови M можна представити у вигляді {ai1, .., ain}=> <Σi11 , ..., Σi11k>|…|< Σin1, .., Σinm> де Σiki — окреме слово прикладної мови проектанта або користувача, < Σik1, .., Σikm> — фраза φi, яка описує окремий символ ai з абстрактного боку опису атаки {ai1, .., ain}CM. Оскільки атаки різного типу можуть мати однакові складники в алфавіті A, то словник опису атак можна представити в наступному вигляді: Sc={[a1=< Σ11, .., Σ1k>], [a2=< Σ21, .., Σ2m>], .., [an=< Σn1, .., Σnj>]}. У скороченому вигляді словник Sc записувати у скороченій формі: ai=j(ai), де j(ai) — текстова інтерпретація вхідного символа ai автомата U на природній мові споживача. Використання природної мови обумовлюється не тільки розв'язком задачі відображення інтерпретацій компонент системи у вигляді, який є приязним для споживачів, а для використання j(ai) або j(xi), де xi — довільна компонента системи опису інтерпретації для проведення більш глибокого аналізу чи перетворень. Доцільність у використанні j(xi) для розширення можливостей аналізу атак, небезпек та засобів захисту обумовлюється тим, що j(xi) представляє собою більш повне відображення інформації про об'єкт дослідження. Це означає, що використання j(xi) для аналізу та аналітичних перетворень дозволить не тільки отримати більш повну інформацію про об'єкт досліджень, а також дозволить розв'язувати нові задачі, що пов'язані з проблемами захисту інформаційних систем.

Для того, щоб з'явилася можливість використовувати j(xi), що в загальному випадку описується як j(xi)= < Σi1n, .., Σi1m> |…|< Σik1, .., Σikn> |<Pi1, ..., Pik>, де Pij — параметри, що відображають числові величини, тих чи інших компонент або характеристик xi, що описуються, як мінімум, фразою < Σij1, .., Σijm>. Тому можна стверджувати, що між φi Є j(xi) і Pij можуть існувати декларативні взаємозв'язки. Наприклад, φi(Σi1, .., Σik)= Pij. Приймаючи до уваги, що всі j(xi) представляють нормалізовану форму, можна прийняти, що φi(Σi1, .., Σik) являється семантичною одиницею, а це дозволяє достатньо точно ідентифікувати кожний параметр Pij з конкретною семантичною одиницею. Система перетворень j(xi), яку будемо позначати Ξ, реалізується таким чином, щоб вона вкладалася в систему синтаксичних граматичних правил природної мови Г. Такі правила в більшості випадків обмежуються вимогами до певного впорядкування слів різних граматичних

типів в межах фази чи в межах речення. Таким чином, всі слова Σij з природної мови Ωi поділяються на граматичні типи, які в рамках словника Sc складають окремі класи. Для реалізації правил з Ξ необхідно певним чином індетифікувати або описувати відповідні слова, щоб в залежності від такої ідентифікації можна було виконувати перетворення Σi над (φi, φj). Оскільки природна мова має лінійну структуру, то розміщення Σi і Σj в рамках φi, φi і φj, в рамках речення φi описується однією базовою операцією «*», яку прийнято називати конкатенацією тому перетворення з Ξ можуть полягати в наступному:

- перестановці або реконфігурації слів Σi у фазі φi, або в реконфігурації фаз φi у межах речення,
- у додаванні до φi до нових слів,
- в елімінації слів з фаз і речень,
- у формуванні нових фраз на основі їх побудови з деякої групи слів {Σi1, .., Σik},
- у формуванні нових речень з групи фраз {φi1, .., φim}чи з групи окремих слів {Σi1, .., Σin}.

Очевидно, що можливі перетворення, які являються комбінаціями приведених вище перетворень. У зв'язку з можливістю здійснення відповідних перетворень виникає необхідність у виборі таких слів для здійснення рекомбінацій, розширень чи елімінацій, які відповідали б вимогам граматики Г. Оскільки словник Sc описує предметну область інтерпретації задач, що розв'язуються по відношенню до об'єкта в цілому, то j(xi) описує допустимі варіанти представлення відповідної компоненти, допустимі можливості, що визначають значимість та значення кожної з компонент та ряд характеристик, що визначають можливість або неможливість використання фрагменту j(xi) для здійснення перетворень у відповідності з правилами Σi. Це дає змогу при формальному підході до перетворень в середовищі {j(xi).., j(xm)} уникнути класичних семантичних суперечностей, які є допустимими в рамках формальних синтаксичних правил граматики Г. Прикладом, що ілюструє такий факт, може служити фраза, яка є синтаксично допустима, але семантично суперечлива в рамках відповідної області інтерпретації ,що виглядає наступним чином Ξ. Тому перетворення будемо здійснювати не на рівні окремих слів, а на рівні окремих елементарних фраз, що визначаються в межах j(xi) в рамках Sc. Очевидно, що елементарною фразою може бути окреме слово.

Завдяки тому, що перетворення Ξ виконуються на основі елементарних фраз φi j(xi) або Sc, то вдається уникнути семантичних суперечностей, що пов'язані з недотриманням обмежень, які визначаються предметною областю Wi, приклад якої приведено вище.

Реалізація довільного перетворення j(xi) обумовлюється певною ціллю, яка досягається елементарними перетвореннями, що описані вище. Використання кожною з перетворень лише в рамках синтаксичних правил може призвести до виникнення синтаксичної суперечності, до виникнення

семантичного конфлікту і т. д. Тому необхідно ввести семантичні параметри, які дозволили б узгоджувати семантичні особливості окремих фраз чи фрагментів речень таким чином, можна було б досягнути наступне:

- щоб перетворення не приводили до появи семантичних аномалій, які можуть появлятися в рамках Wi,
- щоб можна було б формувати нову j(φi), яка описує нову інтерпретацію фрази, що семантично допустила б Wi і не викликає появи невизначеності,
- щоб можна було елімінувати аномалії семантичного характеру, якщо остання в силу різних причин проявляється в Wi.
- Такими семантичними параметрами є:
- семантична значимість, яка може встановлюватися, обраховуватися або декларуватися в межах предметної області розв'язування задач W різними способами (λ),
- семантична суперечність (η), яка визначається на основі уявлень про λ,
- семантичний конфлікт (μ),
- семантична надмірність (σ),
- перевищення семантичних повноважень (χ) та ряд інших семантичних параметрів, що будуть вводитися по мірі необхідності.

Однією з найбільш поширених інтерпретацій семантичної суперечності являється інтерпретація, яка ґрунтується на уявленнях про узгоджене використання слів. У вузькому сенсі цього поняття вузька узгодженість визначається або базується на одному з параметрів. Прикладом такого параметру може служити семантична значимість окремого слова λ. Це означає ,що доцільно при формуванні певної фрази слова семантичних різниць значимість яких знаходиться у певному діапазоні Δλi. Очевидно, що така пара слів формується у відповідності з правилами семантики Г, що мають місце для відповідної мови. Це означає, що використання двох слів для формування з них фрагмента фрази не призведе до синтаксичної суперечності навіть в тому випадку, якщо вибрані слова по своїй семантичній значимості достатньо споріднені, що визначається Δλi(Σi, Σj).

Розглянемо формальний опис правил семантичних перетворень текстових описів інтерпретації компонент: φi(Σ1, .., {[η(Σi+1, Σi)≤δη]& [μ(Σi+1, Σi)≤δμ]}, .., Σn)→[φi(Σi, .., Σn) →φi* (Σi, .., Σi-1, Σi+1, .., Σn)]. Приведене правило виводу будемо називати правилом реконфігурації слів у фразі φi, або скорочено PRS. Правило реконфігурації фраз записується аналогічно, його можна розглядати як розширення PRS і будемо скорочено його позначати PRF. Правило додавання слів на фазі φi слова Σi або їх елімінація будуть описуватися наступними правилами: φi(Σ1, .., {[η(Σi-1, Σi+1)≤δη]& [μ(Σi-1, Σi+1)≤δμ]}, .., Σn)→[φi(Σi, .., Σn) →φi* (Σi, .., Σi-1, Σi+1, .., Σn)].

Правило додавання слова до фрази записується аналогічно. Правило елімінації слова будемо позначати PES, а правило додавання слова будемо позначати PDS.

Правило формування нових фраз можна розглядати як семантичний генератор фраз. Скорочено будемо його позначати буквами SGF, формально воно записується у вигляді наступного співвідношення: {[η(Σi, Σi)≤δη]& [μ(Σi, Σi)≤δμ] & [σ(Σi, Σi)≤σμ] & [χ(Σi, Σi)≤δχ]}→{[Σ1, .., Σi, Σj, .., Σn)]→ [(Σi*Σj)= φi*(Σi, Σj)]., «*» — знак конкатенації двох слів Σi і Σj в рамках однієї фази формула. Очевидно, що фаза φi*(Σi, Σj) являється новою Wi. В цьому випадку виникає задача виявлення доцільності формування такої фрази та її семантичного змісту в рамках предметної області Wi. Розглянемо наступне твердження.

Твердження 3.1 Генератор SGF формує коректну фразу в W_i і, відповідно, в S_c, якщо така загроза φ^* семантично не суперечна, не породжує конфлікт, не приводить до семантичної надмірності, предметна область неповністю відображається в S_c.

Перш ніж розглядати доведення твердження на якісному рівні, розглянемо уявлення про коректну фразу φ_i. Під коректною фразою будемо розуміти фразу, яка формується за допомогою правил PRF, PES і PDS. Якщо фраза φ_i описує деяку компоненту x_i з S_c або подію, що має місце в W_i, то елімінація слова Σ_i з φ_i приведе до звуження $\omega_i \in W_i$, яке описувала φ_i. Оскільки $W_i=\{\omega_1, .., \omega_n\}$, а звуження означає, що існують в W_i такі $\omega_1, .., \omega_k$, з яких може складатися правило PES, приводить до формування φ^*, яке описує частину фрагмента ω_i.

Нехай фраза φ^* формується на основі PDS, якщо маємо φ_i, яка описує $\omega_i \in W_i$, і маємо, що представляє собою ідентифікацію компоненти x_i з S_c, то розширення φ_i визначає, або описує, наприклад, $\omega_{i1}, .., \omega_{ik}$, то розширення φ_i приведе до формування опису нової сукупності $\omega_{i1}, .., \omega_{ik}, \omega_i$. Така ситуація є допустимою, якщо S_c і $\{\varphi_1\ldots, \varphi_n\}$ є неповними в W_i. Припустимо, що $\{\varphi_1\ldots, \varphi_n\} \in W_i$ є певною системою фраз. Це означає, що в W_i не існує такого ω_i^*, яке б описувалося б у системі $\{\varphi_1\ldots, \varphi_n\}$. В цьому випадку для сформованого φ^* на основі PDS не повинна виконуватися умова $\varphi_i^* \le \delta\chi$. Якщо ця умова виконується і $\{\varphi_1\ldots, \varphi_n, \varphi_i^*\}$ повна, це означає, що має місце $(\varphi_i^*) \ge \delta\sigma$. В цьому випадку сформована фраза є некоректною.

У відповідності з формулою SGF, при формуванні φ* виконуються всі умови, що стоять у правій частині головної аплікації. Тоді Wi відображається в Sc, а нова φi* являється доповненням до {φ1…, φn, φi*}, яка описує (ω1…, ωn, ωi*) C Wi.

В рамках правила SGF існує можливість попередження описів нових компонент Wi, які при початковому формуванні Sc могли не бути сформульованими і в цьому сенсі невідомими інформаційній системі, що відповідний Sc використовує. Така властивість є особливо важливою, оскільки система безпеки може зустрічатися з новими типами атак, які є невідомими, а їх виявляти необхідно в першу чергу на етапах попередження атаки, поки остання не завершилася досягненням своєї цілі. Завдяки використанню автоматних моделей для опису Zhi, що реалізують принципи технологій honeypot, є важливим формувати нові фази, які описують,

відповідно, нові атаки. Формування такого типу атаки є неможливим на протязі одного року реалізації розширення φі та з використанням одного правила SGF. Тому формування нових фраз та речень φі, які б описували послідовність подій, що відповідали б новій невідомій атаці, необхідно використовувати більш розширену інформаційну компоненту, якою являється інформаційна модель Zhi, або mi (Zhi).

Правила побудови нових речень φі з групи фраз {φ1…, φn} формується аналогічно до правила SGF і позначати його будемо SGR. Різниця між правилом SGF і правилом SGR полягає в тому, що у другому випадку використовуються узагальнені семантичні параметри η, μ, δ та χ, які характеризують окреме не слово, а цілу фразу або групу фраз.

При формуванні нових текстових описів j*(xi*) в більшості випадків необхідно використовувати послідовність правил перетворень та правил виводу в цьому випадку виникає задача вибору необхідного чергового правила перетворень та задача вибору фраз та слів, що повинні бути використаними на черговому етапі перетворень.

Розв'язок цієї задачі ґрунтується на наступних положеннях, які були сформульовані. Перше з них стверджує факт, відповідно до якого кожна атака реалізується на основі використання загроз, що існують в об'єкті охорони, яким у даному випадку являється інформаційна система управління. друге з цих положень стверджує, що кожна атака має певну ціль. Тому спосіб реалізації тієї чи іншої атаки суттєво залежить від цих обох положень. Розглянемо як ці фактори можна використати для формування опису можливої атаки. Очевидно, що в рамках системи управління і, відповідно в рамках системи безпеки існує інформація про поточний стан найбільш важливої інформації чи найбільш важливих факторів, що визначають величину рівня захисту. Такі фактори, що в даний момент мають високу вартість в рамках функціонального призначення системи, знаходяться певним чином локалізовані в системі, а також певним чином локалізована в Zhi інформація, що їх стосується. Оскільки структура управління відома, то SZ може визначити способи, якими можна до відповідних місць системи дійти. Таким чином, в SZ формуються траєкторії, що зв'язують зовнішнє оточення з відповідними факторами.

Наприклад, припустимо, що в системі знаходяться файли, що вміщують для об'єкту управління інформацію. Для того, щоб можна було цю інформацію зчитати та передати на зовні, необхідно виконати наступні дії, які будемо розглядати, починаючи від цілі атаки:

- визначити адреси файлів з необхідною інформацією, включаючи її носії,
- отримати повноваження в системі доступу на право читання відповідної інформації,
- ініціювати суб'єкт, котрий відповідні повноваження може прийняти на себе,
- щоб ініціювати такого суб'єкта, необхідно певним чином ініціювати систему управління процесами в системі управління зовнішніми

перериваннями процесу,

- оскільки першоджерелом таких ініціацій повинен бути зовнішній фактор, то необхідно виявити можливий в рамках даної системи управління спосіб вводу в систему відповідного фрагменту зовнішньої програми, що може бути ініціатором вище приведених дій.

Приведена вище послідовність подій, що починається від об'єкту атаки, являється одним з простих прикладів, який у певному наближенні ілюструє траєкторію реалізації можливої атаки. Кожний крок такої атаки використовує певну загрозу яка може бути більш або менш доступною для відповідного інтруза. Тому одним із головних критеріїв формування опису атаки у вигляді текстових описів інтерпретації її кроків, є міра доступності загрози на даному етапі відповідної траєкторії. Це означає, що на текучому кроці виводу опису, який в загальному вигляді записується наступним чином: {ψi= [φi1(Σ1i1, .., Σ1ik)* φij(Σji1, .., Σjim)* …* φik(Σki1, .., Σkin)]}, де φi1 відповідає фрагменту опису інформаційного середовища, яке вміщає адреси файлів, які повинен визначити потенціальний інтруз. У цьому випадку моделлю загрози являється алгоритм, який дозволяє відповідну ціль досягнути. Наприклад, якщо адреси файлів, що представляють собою для системи повишену цінність, є зашифрованими, то спосіб зламання такого шифру є описом моделі загрози, яка характеризує відповідний фрагмент системи управління. Рівень доступності такої загрози може підвищуватися шляхом заміни існуючого алгоритму шифрування більш стійким алгоритмом. Оскільки текстовий опис відповідної компоненти xi системи є найбільш повним, то j(xi)=φj1 використовується для перетворення речення φi шляхом розширення його функціональних можливостей.

Формування виводів описів можливих атак реалізується в рамках інформаційних моделей, які представляють собою програмні засоби, що наповнюють програмний honeypot, яким виявляється Zhi. Формування {ai1, .., ain} в рамках mi (Zhi) ініціюється лише тоді, коли на вхід автомату U, який являється зовнішнім описом Zhi, подається послідовність пакетів, в якій виявляється відхилення від очікуваних параметрів відповідної сесії зв'язку.

1. *Pierprryk K. L., Harjiono T., Seberry J.* Fundamentals of Computer Security. Springer — Verlad Berlin Htsdel, berg, 2003.

2. *Dhanjani N., Clarke L.* Network Security Tools. O'Relly Media, Inc., 2005.

3. *Лукацкий А. В.* Обнаружение атак. СПб.: БХВ — Петербург, 2001.

4. *Sarkar K., Sunolaralingam S., Balinsky A., Miller D.* Network Security without wire. Cisco Systems, 2005.

Поступила 18.01.2010р.