Методика формального проектування КСЗІ в ІТС

Роман Гвоздьов[1], Володимир Заболотний[2], Артем Бойко [3]

1. Кафедра Безпеки інформаційних технологій Харківський національний університет радіоелектроніки, Україна, м. Харків, пр. Науки, 14,
E-mail: roman.hvozdov@nure.ua
2. Кафедра Безпеки інформаційних технологій Харківський національний університет радіоелектроніки, Україна, м. Харків, пр. Науки, 14,
E-mail: volodymyr.zabolotnyi@nure.ua

3. Приватне акціонерне товариство "Інститут інформаційних технологій", Україна м.Харків, вул. Бакуліна, 12,
E-mail: boyko@iit.kharkov.ua

Коротка анотація – Formal methods enable reasoning from logical or mathematical specifications of the behaviors of computing devices or processes; they offer rigorous proofs that all system behaviors meet some desirable property. They are crucial for security goals, because they can show that no attack strategy in a class of strategies will cause a system to misbehave. Without requiring piecemeal enumeration, they rule out a range of attacks. They offer other benefits too: Formal specifications tell an implementer unambiguously what to produce, and they tell the subsequent user or integrator of a component what to rely on it to do. Since many vulnerabilities arise from misunderstandings and mismatches as components are integrated, the payoff from rigorous interface specifications is large.

Formal methods differ from other design systems through the use of formal verification schemes, the basic principles of the system must be proven correct before they are accepted. Traditional system design has used extensive testing to verify behavior, but testing is capable of only finite conclusions.

Ключові слова – SDL, Z.100, LOTOS, E-LOTOS, UML, UMLsec, РІВЕНЬ ГАРАНТІЙ, ІТС, ФПБ

I. Вступ

Зі стрімким збільшенням кількості послуг, що надають інформаційно-телекомунікаційні системи (ІТС), зростає складність архітектури ІТС. Недоліки при проектуванні таких систем можуть критично вплинути на їх функціонування, зокрема на безпеку. Оскільки системи ускладнюються, безпека стає важливим питанням, формальний підхід до проектування системи пропонує ще один рівень страхування. Якщо в ІТС планується оброблення інформації, порядок захисту якої регламентується законами України або іншими нормативно-правовими актами (наприклад, інформації яка становить державну таємницю або вимоги до захисту якої встановлено законодавством), обов'язковим є незалежне підтвердження (оцінювання) відповідності реалізованих засобів та заходів захисту встановленим вимогам та нормам[1].

В Україні як критерії оцінки використовуються критерії, встановлені в [2]. Згідно з цими вимогами, оцінюються реалізовані функції захисту (функціональні послуги безпеки, ФПБ) та рівень гарантій коректності їх реалізації (рівень гарантій).

Рівень гарантій коректності реалізації ФПБ містять вимоги до архітектури комплексу засобів захисту (КЗЗ), середовища розробки, послідовності розробки, середовища функціонування, експлуатаційної документації та випробувань КЗЗ. Зокрема, вводиться сім рівнів гарантій (Г-1 ... Г-7), які є ієрархічними. Ієрархія рівнів гарантій відображає поступово зростаючу впевненість у тому, що реалізовані в об'єкті експертизи (ОЕ) ФПБ дозволяють протистояти певним загрозам, а також, що механізми, які їх реалізують, у свою чергу коректно реалізовані та можуть забезпечити очікуваний споживачем рівень захищеності інформації під час її оброблення в ОЕ [1].

Наприклад, для заявленого рівня гарантій Г-4 і більше реалізованої КЗЗ оцінюваного ОЕ необхідно викладати опис проекту архітектури у формалізованому вигляді, тобто використовуючи формальну нотацію. На даний момент часу не існує чітко визначеної методики для формального проектування КСЗІ в ІТС.

II. Вимоги до методики розробки

До методики розробки формального проектування КСЗІ в ІТС можна ввести наступні критерії:

1) орієнтованість на опис процесів обробки інформації;
2) орієнтованість на опис політики безпеки інформації;
3) однозначність та легкість сприйняття;
4) наявність готових блоків з безпеки.

III. Огляд методів формального проектування

SDL (Specification and Description Language) – мова специфікацій з формальною семантикою, призначена для опису телекомунікаційних систем. Стандарт мови визначений Міжнародним консультативним комітетом з телефонії і телеграфії (МККТТ) та включає рекомендації з Z.100 по Z.109. SDL має концепції поведінки, опису даних та структурування (особливо для великих систем) [2]. Основною опису поведінки є розширені скінчені автомати, що передають повідомлення. Опис даних ґрунтується на типах даних для значень та об'єктів. Основою структурування є ієрархічна декомпозиція та ієрархія типів [2]. Основна область застосування для SDL – конкретизація поведінки процесів в системах реального часу та розробка таких систем. До застосування у галузі телекомунікацій належать[2]:

1) обробка дзвінків та з'єднань (наприклад, обробка дзвінків, телефонна сигналізація, вимірювання) в комутаційних системах;
2) технічне обслуговування та усунення несправностей (наприклад, тривоги, автоматичне усунення несправностей, звичайні випробування) у загальних телекомунікаційних системах;

3) системний контроль (наприклад, контроль за перевантаженням, модифікацією та розширенням);

4) функції експлуатації та обслуговування, управління мережею;

5) протоколи передачі даних;

6) телекомунікаційні послуги.

Таким чином, SDL може використовуватися для опису:

а) вимог до об'єкта;

б) специфікацій системи;

в) технічних характеристик систем;

г) детальних технічних умов;

д) описи архітектури системи (як високого рівня, так і достатньо деталізованого для безпосереднього застосування реалізації);

е) описи системного тестування.

В сфері телекомунікацій SDL не має рішень з опису безпеки, а саме політик безпеки та готових блоків безпеки.

LOTOS (Language of Temporal Ordering Specification) – стандартизована мова специфікацій, призначена для опису комунікаційних та розподілених систем. LOTOS базується на CCS (Calculus of Communicating Systems, обчислення взаємодіючих систем) та CSP (Communicating Sequential Processes, комунікуючі послідовні процеси) для опису поведінки систем та на ACT-ONE для визначення абстрактних типів даних [3]. У LOTOS і E-LOTOS система, що підлягає специфікації, моделюється набором процесів, взаємодіючих між собою і їх оточенням. У LOTOS система описується сукупністю процесів. Процес може взаємодіяти з іншими процесами, що складають його середовище. Взаємодія між процесами базується на елементарних одиницях синхронізації, що називаються подіями або діями. Подія передбачає синхронізацію [4]: всі взаємодіючі процеси (два чи більше) беруть участь у події одночасно. Обмін даними може бути пов'язаний з цими синхронізаціями. Події є автономні, в тому сенсі, що їх виникнення відбувається миттєво, без тривалості. Вважається, що подія відбувається в точці взаємодії або в каналах подій (event gates). У разі синхронізації без обміну даними подія – це лише назва каналу подій[4].

UML (Unified Modelling Language) – мова графічного опису для об’єктного моделювання процесів. Модель UML складається з трьох основних категорій елементів моделі, кожна з яких може використовуватися для складання тверджень про елементи системи. Ці категорії [5]:

1) Класифікатор. Класифікатор описує набір об’єктів. Об'єкт - це елемент зі станом та стосунками до інших об’єктів. Стан об'єкта ідентифікує значення для цього об'єкта властивостей класифікатора об'єкта.

2) Подія. Подія описує набір можливих подій. Подія – це те, що відбувається, що має певний вплив на систему.

3) Поведінка. Поведінка описує набір можливих здійснень. Здійснення – це виконання набору дій (можливо протягом певного періоду часу), які можуть генерувати та реагувати на події, включаючи доступ та зміна стану об’єктів.

Також, існує UMLsec – це розширення до UML для інтеграції аспектів безпеки у специфікаціях UML. Опис аспектів безпеки реалізується за допомогою стереотипів (табл 3.1).

ТАБЛИЦЯ 3.1 – ПРИКЛАД UMLSEC СТЕРЕОТИПІВ (СКОРОЧЕНО)

Stereotype	Base Class	Description
Internet	link	Internet connection
encrypted	link	Encrypted connection
LAN	link, node	LAN connection
wire	link	wire
smart card	node	smart card device

Профіль безпеки UMLsec містить такі загальні ідеї[6]:

1) діаграма діяльності: безпечний потік управління, координація;

2) діаграма класу: обмін даними зберігає рівні безпеки;

3) діаграма послідовностей: взаємодія, яка критично важлива для безпеки;

4) схема діаграми стану: захищеність, що зберігається в об'єкті;

5) діаграма розгортання: вимоги фізичної безпеки;

6) пакет: цілісний погляд на безпеку.

Однак, UML з розширенням UMLsec не має в повному обсязі інструментів та визначень, які б дозволили в повному обсязі проектувати КСЗІ згідно з вимогами чинного законодавства.

Перераховані вище методи формального проектування, не задовільняють критеріям визначеними у пункті 2 цієї статті.

IV. Висновки

Актуальною задачею є розробка методики формального проектування КСЗІ в ІТС.

Література

[1] НД ТЗІ 2.7-010-09 «Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу»

[2] ITU-T Recommendation Z.100 (11/99) Specification and description language (SDL)

[3] Lisandro Zambenedetti Granville and Maria Janilce Almeida. «Specification of E-LOTOS Systems in the E-DART Environment»

[4] Luc Leonard, Guy Leduc. «An introduction to ET-LOTOS for the description of time-sensitive systems»

[5] OMG Unified Modeling Language (OMG UML)

[6] Jan Jurjens, “TU Munich: UMLsec – Presenting the Profile 22 Requirements on UML extension for security II”