Кузнецов Г.В., Бубнов А.О.
Національний гірничий університет, м. Дніпропетровськ

Модель обчислення загальної метрики довіри для підвищення рівня інформаційної безпеки регіонального сегменту грід

Темпи розвитку сучасних інформаційних технологій у більшості випадків значно випереджають темпи розробки адекватних заходів та засобів забезпечення інформаційної безпеки. Грід системи наразі є потенційними об'єктами атак зловмисників, а завдання забезпечення інформаційної безпеки ускладнюється через велику кількість користувачів, гетерогенний склад, різноманітність доступних ресурсів і високий ступінь розподіленості. Для забезпечення безпеки в більшості грід систем використовується "інфраструктура безпеки грід" (GSI), яка надає сервіси автентифікації, забезпечення конфіденційності передачі інформації і єдиний вхід в грід систему з використанням інфраструктури відкритих ключів (PKI). Технологія PKI має декілька слабких місць [1]. З урахуванням складності структури грід і постійної зміни складу користувачів, PKI архітектури часто недостатньо для забезпечення автентичної взаємодії всіх користувачів Грід мережі [2]. Ця проблема може бути вирішена шляхом впровадження гнучких механізмів оцінки довіри до кожного вузла як додаток до механізмів довіри інфраструктури PKI.

У доповіді запропоновано застосувати дворівневу модель довіри:

- рівень доменів – нижній рівень;
- рівень віртуальних організацій (ВО) – верхній рівень.

Така модель дозволяє використовувати різні метричні алгоритми оцінки довіри для доменів грід і віртуальних організацій, а також ефективно виконати інтеграцію в існуючу інфраструктуру системи безпеки. При цьому, довіра у віртуальній організації будується не тільки на підставі характеристик кожного члена (ідентифікатор, домен і так далі), але і на підставі мережевих шляхів, що дозволяє достатньо якісно відстежувати появу нових і відключення існуючих користувачів грід, чого не може надати лише політика безпеки [3].

Завдяки наявним механізмам сертифікатів в рамках GSI ми можемо точно ідентифікувати як вузли, так і їх домени. Кожному домену буде привласнена оцінка довіри до нього, яка дозволить оцінювати якість системи безпеки в цілому цього домену. Так само, кожен домен повинен буде підтримувати таблиці оцінок довіри щодо кожного вузла, який входить у цей домен.

У доповіді запропоноване аналітичне представлення оцінки довіри на рівні доменів та ВО, наведено приклади масштабування при застосуванні запропонованого підходу.

Гнучка модель довіри дозволяє реалізувати доповнення до вже існуючої системи безпеки, яке легко масштабується. Це дозволяє використовувати її в децентралізованих і розподілених системах. За рахунок розміщення її на верхньому рівні організації безпеки, досягається легкість впровадження її у вже наявну структуру безпеки без значних змін архітектури грід.

Література

1. C. Ellison, B. Schneier "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure" // Computer Security Journal, v 16, №1, 2000, pp. 1–7.
2. Г.В. Кузнецов, А.А. Бубнов, "Децентрализованная индивидуальная модель репутаций для организации доверительных отношений при взаимодействии в распределенных информационно-коммуникационных системах" // Материалы международной научно-практической конференции "ИНФОТЕХ – 2007", стр. 93–96, Севастополь, 2007.
3. Tuomas Aura. "Distributed Access-rights Managements with Delegations Certificates". Secure Internet Programming 1999: pp. 211–235.