Применение теории нечётких множеств в анализе рисков информационной безопасности

Хрипович Илья Сергеевич, НИИ ППМИ БГУ

Любая информационная система подвержена некоторому множеству угроз **T**, которые могут реализовываться посредством эксплуатации уязвимостей из множества **V** и т.о. наносить ущерб владельцам и пользователям систем. При создании системы защиты информации должна проводиться оценка возможного ущерба с учетом всевозможных комбинаций $\{t, v\} \in T \times V$. Наиболее популярным в настоящее время подходом оценки ущерба является оценка рисков. Существующие методики оценки рисков сложны тем, что требуют существенных временных затрат и надежных статистических данных, которые практически отсутствуют.

Поскольку важно уметь выявлять и быстро и эффективно реагировать на инциденты безопасности предлагаются и другие методы оценки. В настоящей работе исследуется возможность оценки критичности уязвимостей используются различные методы получения рейтинга уязвимости. Наиболее распространённой методикой является **CVSS** (Common Vulnerability Scoring System), разработанная **FIRST** (Forum of Incident Response and Security Teams). В крупнейших базах уязвимостей, таких как NVD и OSVDB, обязательно приводится рейтинг, вычисленный по данной методологии. CVSS позволяет по набору характеристик уязвимости получить её рейтинг на отрезке **[0..10]**, в ходе изучения данной методологии был выявлен следующий недостаток: значение рейтинга получилось отрицательным, при допустимых значениях параметров.

Был проведён более глубокий анализ используемых формул и значений параметров, в результате которого, были сделаны следующие выводы:

1. Распределение значений рейтингов оценок на множестве входных параметров является неравномерным.
2. Функциональная зависимость, используемая в формулах линейна, однако дискретная природа значений параметров приводит к ступенчатым функциям зависимости значения рейтинга от отдельного параметра.
3. Изменение коэффициентов или численных значений параметров приводит к нарушению области значения функции.

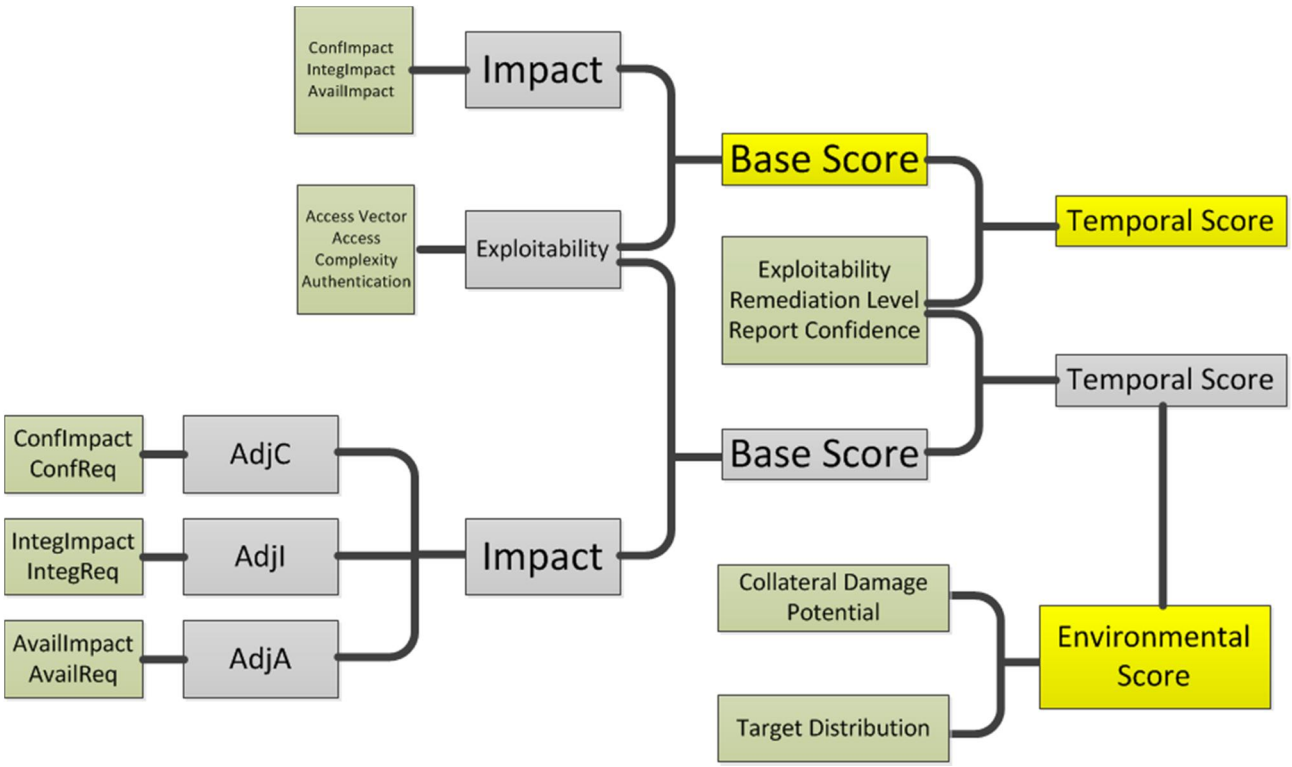
Для улучшения данных характеристик было принято решение использовать механизмы нечёткой математики.

В докладе рассмотрена система нечёткого вывода по алгоритму Мамдани.

На первом этапе группа экспертов формирует базу правил, составляющих нечёткую базу знаний. Фаззификация позволяет получить непрерывные значения, вместо дискретных, например требования могут быть «выше средних», затем происходит вычисление нечёткого

значения рейтинга, а на этапе дефаззификации вычисляется действительное число, отражающее рейтинг уязвимости.

Построение систем нечёткого вывода с большим количеством входных параметров сопряжено с проблемой экспоненциального роста количества правил нечёткой базы знаний, поэтому предлагается каскадная схема следующего вида.



Основной целью данной работы является построение такой системы нечёткого вывода, которая бы позволяла наиболее адекватно оценивать рейтинг уязвимостей и обладала следующими свойствами:

- Нелинейность зависимости результирующего рейтинга от входных параметров.
- Непротиворечивость оценок.
- Равномерность распределения значений рейтингов на множестве входных параметров.
- Гибкость в настройке веса параметров уязвимостей.

Результатом работы должна стать система оценки рейтинга уязвимостей, которая позволит получать более точные оценки по сравнению с существующей методологией.