

K. K. Kim, A. A. Tkachuk, D. O. Berkut, A. M. Zyryanov

Development of a System for Wireless Transmission of Induced Voltage from the Current in the Carrier Wire to Power the Lighting System of Passenger Platforms

Kim Konstantin Konstantinovich — Dr. Sci. in Engineering, Professor, Head of the Department “Theoretical Foundations of Electrical Engineering and Power Engineering”,

Tkachuk Anton Andreevich — PhD in Engineering, Associate Professor, Associate Professor of the Department “Theoretical Foundations of Electrical Engineering and Power Engineering”

Berkut Dmitrij Olegovich — 1st-Year Student of the Department “Automation and Telemechanics in Railway Transport”

Zyryanov Artemij Mikhailovich — 2nd-Year Student of the Department “Electric Traction”

Emperor Alexander I St. Petersburg State Transport University, Saint Petersburg, Russia

Abstract. A system for wireless power transmission from an AC overhead contact line's carrier cable is presented. This system serves as a power source for LED luminaires. The luminaires are located near passenger platforms and are activated at night. The key element of the wireless power transmission system is an inductive power take-off unit (IPU). This unit is a toroidal current transformer with a core. The operating principle of the IPU is discussed. Numerical calculations are performed using the ELCUT software package.

Keywords: carrier cable, current, electromagnetic field, lighting system, toroidal transformer, induction power take-off, AC contact network

УДК 004.056

Д. Д. Минеева, С. В. Корниенко

Разработка модели управления доступом на основе атрибутов со взвешенным принятием решений и оценкой риска

Минеева Диана Дмитриевна — студент группы КИБ-312

Корниенко Светлана Владимировна — кандидат технических наук, доцент кафедры «Информатика и информационная безопасность»

Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург, Россия

Аннотация. Классические модели управления доступом обладают ограниченной способностью учитывать контекстные факторы и уровень риска при принятии решений. В работе предложена гибридная риск-адаптивная модель контроля доступа, использующая механизм взвешенной оценки правил, динамический порог принятия решений и многофакторную оценку риска контекста. Модель учитывает характеристики субъекта, среды и ресурса, а также нелинейное взаимодействие факторов риска. Проведено экспериментальное исследование поведения модели при различных уровнях риска и конфликтующих политиках. Результаты показывают снижение количества ложных принятий решений и более устойчивое поведение системы в условиях неопределенности.

Ключевые слова: ABAC, контроль доступа, риск-адаптивная модель, RAdAC, AHP, информационная безопасность, конфликт политик, взвешенное принятие решений, оценка риска

Современные корпоративные информационные системы функционируют в условиях распределенной инфраструктуры, удаленного доступа и высокой динамики пользовательского контекста. Использование облачных технологий, мобильных устройств и удаленных рабочих мест значительно усложняет задачу обеспечения безопасного управления доступом к ресурсам.

Традиционные модели контроля доступа, такие как дискреционная (DAC), мандатная (MAC) и ролевая (RBAC), ориентированы преимущественно на статические правила принятия решений [1, 2]. Однако в условиях современных угроз подобный подход оказывается недостаточным, поскольку не учитывает изменение уровня риска, доверия к устройству, местоположения пользователя и других контекстных факторов.

Модель атрибутивного контроля доступа (ABAC) предоставляет более гибкий механизм за счет использования атрибутов субъекта, объекта и окружения [3, 4]. Несмотря на высокую адаптивность, классический ABAC также имеет ряд ограничений. Наиболее существенной проблемой является разрешение конфликтующих политик, при котором одновременно могут активироваться как разрешающие, так и запрещающие правила.

В большинстве существующих систем используются упрощенные стратегии разрешения конфликтов:

- запрет на переопределение;
- разрешение на переопределение;
- первое применимое;
- оценка на основе приоритетов.

Подобные механизмы не учитывают динамический риск контекста и могут приводить к ошибочным решениям типа «ложное разрешение» или «ложный запрет» [5, 6].

Целью данной работы является разработка гибридной риск-адаптивной модели контроля доступа, использующей:

- атрибутивный контроль доступа АВАС;
- многофакторную оценку риска;
- метод анализа иерархий (АНР);
- механизм взвешенного разрешения конфликтующих политик.

Архитектура модели

Архитектура предложенной модели включает следующие компоненты:

- модуль политик;
- модуль рисков;
- модуль оценки;
- AST-модель политик;
- модуль взвешенного принятия решений;
- журнал аудита.

На первом этапе выполняется оценка риска запроса на основе характеристик субъекта, окружения и ресурса. Затем вычисляются правила авторизации АВАС. На завершающем этапе результаты интегрируются с использованием механизма взвешенного принятия решений.

Общий процесс принятия решения может быть представлен следующим образом: запрос → оценка рисков → анализ правил → взвешенное суммирование → окончательное решение.

Для описания политик используется AST-представление логических выражений с поддержкой операций AND, OR, NOT и предикатов сравнения атрибутов.

Математическая модель

Оценка риска выполняется на основе трех кластеров:

- риск, связанный с объектом деятельности (R_s);
- риск, связанный с окружающей средой (R_e);
- риск, связанный с ресурсами (R_r).

Весовые коэффициенты вычисляются методом АНР на основе матрицы попарных сравнений Т. Л. Саати [7].

Для учета нелинейного взаимодействия факторов риска используется критерий взаимодействия:

$$R_{int} = \gamma \cdot R_s \cdot R_e \cdot R_r,$$

где γ — выбранный эмпирически калибровочный параметр (составляет примерно 5–15 % от общего риска при типичных значениях факторов).

Использование критерия взаимодействия позволяет учитывать ситуации, при которых совокупность нескольких умеренных факторов формирует высокий уровень риска.

Интегральная оценка риска определяется выражением:

$$R_{raw} = w_s R_s + w_e R_e + w_r R_r + R_{int},$$

где w_s, w_e, w_r — веса АНР.

Наибольший вклад в итоговый риск вносит субъект доступа, что соответствует современной концепции Zero Trust.

Для нелинейной нормализации используется сигмоидная функция:

$$R_{final} = \frac{1}{1 + e^{-k(R_{raw} - \theta)}},$$

где k — коэффициент крутизны;

θ — пороговая точка.

Сигмоидная нормализация обеспечивает плавный переход между низким и высоким уровнями риска и предотвращает резкие скачки итоговой оценки.

В отличие от классических стратегий разрешения конфликтов предложенная модель использует механизм взвешенного принятия решений.

Для каждого активированного правила вычисляется вес:

- разрешающие правила увеличивают итоговый вес;
- запрещающие правила уменьшают его.

Базовая функция оценки определяется как:

$$Score_{raw} = W_{allow} - W_{deny}.$$

Для учета уровня риска применяется риск-адаптивная корректировка:

$$Score = (W_{allow} - W_{deny}) \cdot (1 - 0,5R).$$

Динамический порог принятия решения определяется выражением:

$$T = 0,2 + 0,3R,$$

где коэффициенты 0,2 и 0,3 выбраны эмпирически таким образом, чтобы обеспечить устойчивое поведение системы при изменении уровня риска.

Итоговое решение формируется следующим образом:

$$Решение = \begin{cases} Разрешить, & Score > T \\ Запретить, & Score < -T \\ Запретить, & \text{иначе} \end{cases}$$

Таким образом, при росте риска системе становится сложнее принять разрешающее решение.

Экспериментальное исследование

Для проверки работоспособности модели был разработан программный прототип на языке Python с использованием библиотеки Streamlit.

В модели учитывались следующие факторы:

- уровень допуска пользователя;
- доверие к устройству;
- местоположение;
- время доступа;
- чувствительность ресурса;
- принадлежность к подразделению;
- роль пользователя.

Были проведены серии экспериментов с различными комбинациями параметров.

ТАБЛИЦА. Основные сценарии тестирования

Сценарий	Результат
Администратор инициирует запрос на удаленный доступ к высокочувствительному ресурсу более низкого уровня с неавторизованного устройства в рабочее время	Запретить
Менеджер инициирует запрос на удаленный доступ к низкочувствительному ресурсу более высокого уровня с авторизованного устройства в рабочее время	Разрешить

Особое внимание уделялось анализу конфликтующих политик. В ряде сценариев одновременно активировались правила разрешения и запрета. В отличие от традиционных стратегий разрешения конфликтов предложенная модель учитывала:

- вес правил;
- уровень риска;
- доверие к сессии;
- контекст доступа.

Экспериментальные результаты показали:

- снижение количества ложно сработанных решений;
- более устойчивое поведение системы при росте риска;
- уменьшение влияния конфликтующих политик;
- адаптивное изменение строгости контроля доступа.

Заключение

В работе предложена гибридная риск-адаптивная модель контроля доступа, объединяющая механизмы АВАС, АНР и взвешенного принятия решений. Разработанный подход позволяет учитывать динамический контекст доступа, уровень риска и конфликтующие политики при принятии решений.

Программный прототип подтвердил работоспособность предложенного подхода и показал более устойчивое поведение системы в условиях неопределенности и конфликтующих политик.

Список источников

1. Jin X., Krishnan R., Sandhu R. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC // IFIP Annual Conference on Data and Applications Security and Privacy. 2012.
2. Sandhu R., Coyne E., Feinstein H., Youman C. Role-based access control models // IEEE Computer. 1996.
3. Guide to Attribute Based Access Control (ABAC) Definition and Considerations / V. C. Hu [et al.] // NIST Special Publication 800–162. 2019
4. Servos D., Osborn S. Current Research and Open Problems in Attribute-Based Access Control // ACM Computing Surveys. 2017.
5. McGraw R. Risk-Adaptable Access Control (RAdAC) // NIST Privilege Management Workshop. 2009.
6. Kandala S., Sandhu R., Bhamidipati V. An Attribute Based Framework for Risk-Adaptive Access Control Models // Proceedings of the 5th International Conference on Availability, Reliability and Security. Vienna, Austria, 2011.
7. Saaty T. L. Decision Making with the Analytic Hierarchy Process // International Journal of Services Sciences. 2008.

D. D. Mineeva, S. V. Kornienko

Development of an Attribute-Based Access Control Model with Weighted Decision-Making and Risk Assessment

Mineeva Diana Dmitrievna – Student of the KIB-312 Group

Kornienko Svetlana Vladimirovna – PhD in Engineering, Associate Professor of the Department “Computer Science and Information Security”

Abstract. Classical access control models have a limited ability to account for contextual factors and risk levels in decision-making. This paper proposes a hybrid risk-adaptive access control model that employs a weighted rule evaluation mechanism, a dynamic decision threshold, and a multifactorial assessment of contextual risk. The model considers the

characteristics of the subject, environment, and resource, as well as the nonlinear interaction of risk factors. An experimental study was conducted to examine the model's behavior under various risk levels and conflicting policies. The results show a reduction in the number of false acceptances and more robust system behavior under conditions of uncertainty.

Keywords: ABAC, access control, risk-adaptive security, RAdAC, AHP, information security, policy conflicts, weighted scoring, risk assessment

УДК 629.42.077

А. Н. Попов, И. Д. Вершинин

Моделирование движения виртуально сцепленных поездов с учетом задержки в цифровом радиоканале

Попов Антон Николаевич — кандидат технических наук, доцент, доцент кафедры «Автоматика, телемеханика и связь на железнодорожном транспорте»

Вершинин Илья Дмитриевич — аспирант кафедры «Автоматика, телемеханика и связь на железнодорожном транспорте»

Уральский государственный университет путей сообщения, Екатеринбург, Россия

Аннотация. В статье рассмотрена задержка передачи информации в цифровом радиоканале при движении виртуально сцепленных поездов. Для оценки предельно допустимого времени задержки использована стохастическая модель движения с учетом длины поездов, скорости, тормозных характеристик, межпоездного расстояния и длины блок-участка. Моделирование методом Монте-Карло показало зависимость допустимой задержки от положения границы занятого блок-участка и расстояния между поездами.

Ключевые слова: виртуальная сцепка, цифровой радиоканал, блок-участок, задержка передачи данных, моделирование

Введение

Развитие технологий интервального регулирования движения поездов направлено на увеличение пропускной способности и сокращение межпоездного интервала. Одним из направлений является технология виртуальной сцепки поездов, которая предполагает информационное взаимодействие между ведущим и ведомым поездом посредством цифрового радиоканала [1, 2]. Такое взаимодействие создает новые эффекты, связанные с повышением скоростей движения при следовании на отличные