УДК 519.711

І.В. Коцюба, О.Є. Макаревич, г.Киев

ОБЕСПЕЧЕНИЕ КОНТРОЛЯ ДОСТУПОМ И ДИНАМИЧЕСКАЯ АВТОРИЗАЦИЯ ОСНОВАННАЯ НА МЕСТОПОЛОЖЕНИИ ПОЛЬЗОВАТЕЛЯ

Abstract. We propose the new form of authorization and location-based access control system, adding some new 3rd part factors to IT infrastructure with device independent approach.

Введение

Сохранение конфиденциальности пользовательских данных является одной из самых актуальных тем в области информационной безопасности. В последние годы сообщалось о выросшем количестве инцидентов торговли персональными данными пользователей, что заставляет регулировать эти вопросы с помощью стандартов и других законодательных инициатив, а также актуализирует инновационную деятельность в данной сфере. Существует огромное количество подходов, направленных на минимизацию потерь конфиденциальности и целостности данных при ее передаче. Наша работа посвящена последним методикам в данной области основанным на местоположении пользователей при попытке получить доступ к информации. Основным препятствием на пути внедрения данных инструментов безопасности, является то что физическое месторасположение человека есть не что иное как частная конфиденциальная информация, и несанкционированное овладение ею, может расцениваться как вмешательство в частную жизнь. Решения, обеспечивающие различные степени секретности в соответствии с предпочтениями пользователя или бизнес-потребностей - менее изучены. Например, можно рассмотреть метод запутывания, ухудшения точности измерения местоположения в связи с конфиденциальностью.

Стоит отметить, что точность определения местоположения во многом зависит от применяемой технологии. GSM/3G технологии широко распространены и в последние годы заметно улучшились возможности определения местоположения. 802.11 WiFi и AGPS / GPS, также могут быть использованы, хотя есть некоторые ограничения их применимости. WiFi имеет ограниченный охват и его использование ограничено в помещениях или в городских районах, охватываемых точками доступа. GPS, наоборот, не работает в помещении или в закрытых пространствах.

Контроль доступа основанный на местоположении

Обычные механизмы контроля доступа полагаются на то, чтобы во время запроса, полностью определить что данный профиль в праве делать. Тем не

менее, контекст информации и, в частности, физическое местоположение пользователя может также играть важную роль в определении прав доступа. Мы описываем интеграцию политик контроля доступа с расположением, то есть применение политик безопасности в зависимости от местоположения инициатора запроса и условий генерации запроса(например запрос должен быть сформирован внутри периметра определенной географической зоны при соблюдении других условий, таких как время суток, день недели и т.д.). Трудности возникают из самой природы информации о местоположении, которая является динамической, с большими погрешностями в измерении и требует специальной инфраструктуры. Быстрый прогресс в области беспроводных и мобильных сетей способствовали новому поколению устройств, пригодных для использования в качестве датчиков способных определить местоположение и перемещение пользователей. Политики контроля доступа должны реагировать и меняться в зависимости от контекста. Основные технологии которые помогут решить вопрос недоступности и отказа в доступе, это: Wi-Fi, Bluetooth, GSM, 3G, 4G, GPS, GLONASS, Galileo. Вне зависимости от конкретной технологии, проверка местоположения или доступности в одной из сетей, даст контекстуальную информацию о запросе, и предоставит доступ с требуемыми правами. В будущем для более тщательного анализа можно использовать менее значимую информацию, такую как, с кем находится пользователь во время получения запроса от него, стоит на месте или перемещается, какую информацию запрашивал до этого. Стоит отметить что предел используемого количества элементов этой системы не определен. Для этих целей можно также использовать вторичные характеристики пользователя, например, его автомобиль со встроенной системой навигации или с GPS меткой в связке с модемом передачи данных, второй мобильный телефон или планшетный компьютер, данные с системы контроля доступом периметром и помещениями(в какой комнате или на каком этаже пользователь находился перед запросом), данные с видеокамер или фотофиксирующих устройств с распознаванием лиц. Некоторые примеры приведены в таблице 1.1.

Чтобы гарантировать конфиденциальность местоположения пользователя, введем три основных метода запутывания, что изменит местоположение пользователя, чтобы уменьшить точность до заданного уровня.

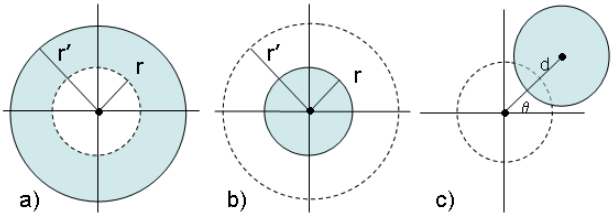

Рис. 1.1 Запутывание с помощью увеличения радиуса, уменьшения радиуса и смещения центра

Таблица 1.1

Примеры на основе определения местоположения

Тип	Характеристика	Описание
Местоположение	1.В периметре	1.Определить здание в котором находится пользователь.
	2. Вне периметра	2. Определить вне зданий где находится пользователь
	3. Удаленность от периметра	3. Определить расстояние пользователя от зданий и периметров.
Движение	Скорость	Определить попадание скорости пользователя в заданный предел, а также определить возможность изменения местоположения пользователя так быстро.
Взаимодействие	Плотность	Определить количество пользователей в данной географической области.
Данные смежных систем	Косвенные показатели	Определить какая дверь открывалась пользователем последней. Определить где находится автомобиль или второе устройство пользователя. Определить какая виде или фотокамера фиксировала пользователя последней.
Активность	Сфера интересов	Определить над каким проектом или данными может быть сосредоточен пользователь в настоящий момент, и не является ли запрашиваемая информация слишком несвязанной с текущей деятельностью.

Сокрытие области измерения местоположения путем увеличения ее радиуса (см. рисунок 1.1 (a)) является чаще всего используемым методом, местоположение при котором скрывается до нужных значений (город, страна, материк).

Другой возможный способ сокрытия местоположения пользователя состоит в уменьшении радиуса заданной окружности как показано на рисунке 1.1 (b).Эффект запутывания, заключается в том что при сравнении координат, они сдвинуты к центру заведомо определенной окружности.

Запутывание местоположения также может быть достигнуто за счет смещения центра области измерения. Очевидно, что эффект запутывания зависит от пересечения двух областей, чем меньше площадь наложения окружностей, тем больше эффект от данного типа запутывания.

Выводы

В данной работе мы обсудили требования для создания систем контроля доступа с применением данных о местоположении инициатора

запроса. Также описали важность обеспечения конфиденциальности данных о местоположении пользователя. В связи с этим очень важно найти баланс между точностью позиционирования для более точного определения прав и обеспечить в то же время неточность для запутывания в связи с сохранением конфиденциальности.

1. *Stuart Jacobs* ENGINEERING INFORMATION SECURITY / Stuart Jacobs – IEEE Press 2011. − 728 p.
2. *Sosinsky, Barrie* 2011 Cloud Computing Bible / *Sosinsky, Barrie* – Willey, 960p.
3. *Vic (J.R.) Winkler* Securing the Cloud / Vic (J.R.) Winkler– 2011 Elsevier Inc– 315 p.

Поступила 4.03.2013р.

УДК 648

А.А. Владимирский, И.А. Владимирский, И.П. Криворучко, А.А. Криворот, А.А. Безпрозванный, С.А. Молодых, г.Киев

РАЗРАБОТКА АППАРАТУРЫ КОНТРОЛЯ ВОЗНИКНОВЕНИЯ ИСКРЕНИЯ ЩЕТОЧНО-КОНТАКТНОГО АППАРАТА ТУРБОГЕНЕРАТОРОВ

Equipment for the control of brush sparking contactors powerful turbogenerators are presented

Группой “Технической диагностики” ИПМЭ им. Г.Е.Пухова НАН Украины разработана система контроля возникновения искрения щеточно-контактного аппарата (ЩКА) турбогенераторов (ТГ) “ИНИС-1”. В качестве информативного параметра для контроля искрения используется электромагнитное излучение. Чем интенсивнее искрение, тем выше уровень электромагнитного излучения. Проведенный анализ [1] позволил рассматривать выявление электромагнитных проявлений искрения наиболее перспективным методом для решения задачи своевременной регистрации искрения ЩКА.

Структура системы представлена на рис.1. В состав “ИНИС-1” входят два индукционных датчика, измерительное устройство, выносное устройство и соответствующее программное обеспечение.

Индукционные датчики предназначены для выделения высокочастотных сигналов искрения на ЩКА турбогенераторов. Они устанавливаются в непосредственной близости от силовых магистралей, подводимых к ЩКА. Применяется встречное включение двух дифференциальных датчиков - на

