ИНСТРУМЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЯЗЫКЕ GOLANG

С.М. Сацук, Д.В. Брынза

В последние годы происходит серьезное развитие языка программирования Go или Golang. Это компилируемый многопоточный язык программирования, разработанный внутри компании Google для совершенствования микросервисной архитектуры веб приложений, работы с большими базами данных, развития параллелизма (concurrency). В настоящее время Golang начинает использоваться во многих компаниях, позволяя переходить от монолитных приложений к микросервисам, быстрее осуществлять транзакции, обрабатывать больше данных и экономить на серверном оборудовании.

В связи с этим, одной из серьезных проблем, связанной с использованием языка программирования Go является защита web-приложений от взлома. Наиболее типичными способами взлома таких приложений являются: предсказуемое значение идентификатора сессии (Credential/Session Prediction); межсайтовая подделка запроса (CSRF); межсайтовое выполнение сценариев (Cross-site Scripting, XSS); внедрение операторов SQL (SQL Injection).
Для непосредственной защиты инструментариев языка можно использовать правильную защиту сессий и cookie с помощью технологии JSON WebTokens, CSRF (борьбу с межсайтовой подделкой запроса или CSRF атаками на сайт). С этой задачей в Go очень хорошо справляется библиотека NoSurf. На основе контекста запроса формируется токен, который впоследствии вставляется в необходимые поля и заголовки. Атака XSS или межсайтинговый скриптинг – это тип атаки на веб-систему, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода. Самый известный пример – это угон пользовательских cookies злоумышленником. Secure – небольшая прослойка для удобной настройки безопасных параметров сервиса. Secure умеет работать как с большим количеством фреймворков, так и со стандартным пакетом net/http. SQl-injection – один из распространенных способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SafeSQL – это статический анализатор кода для Go, который позволяет находить SQL injections.

Несмотря на то, что Golang довольно новый язык программирования, комьюнити очень быстро разрастается и реализует базовые решения, которые встречаются почти в каждом проекте, в том числе и решения, основанные на безопасности веб-приложения.

ОЦЕНКА ИНТЕНСИВНОСТИ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ, СОЗДАВАЕМОГО АБОНЕНТСКИМ ОБОРУДОВАНИЕМ СОТОВЫХ РАДИОСЕТЕЙ В МЕСТАХ С ВЫСОКОЙ ПЛОТНОСТЬЮ НАСЕЛЕНИЯ

А.С. Свистунов

В настоящее время в связи с увеличением территориальной плотности радиооборудования сетей сотовой связи и массовым активным пользованием различными услугами сотовой радиосвязи большой интерес представляет вопрос об электромагнитной безопасности сотовых радиосетей в часы наибольшей абонентской нагрузки в местах с высокой плотностью населения, особенно в местах скопления абонентов.

В работе выполнены оценки уровня суммарной интенсивности электромагнитного поля (ЭМП), создаваемого электромагнитным излучением абонентских устройств (АУ) сотовых радиосетей стандарта GSM на городских территориях. Результаты получены путем компьютерного моделирования распространения радиоволн (РРВ) с применением трехмерной модели РРВ (X3D-модель) и трехмерной модели фрагмента типовой городской застройки с высотой зданий 6–20 м. Моделирование проводилось при следующих системных параметрах сотовой радиосети: территориальная плотность АУ в активном состоянии $\rho_{MS} = 0{,}32$ АУ/м^2, территориальная плотность базовых станций (БС) $\rho_{BS} = 3$ БС/км^2, высота подвеса антенн $H_{BS} = 25$ м, высота антенны АУ над земной поверхностью $H_{MS} = 1{,}5$ м, значение отношения «несущая/помеха» на входе радиоприемника БС $C/I = 15$ дБ. Суммарная интенсивность ЭМП анализировалась на уровне 1,5 м от земной поверхности; минимальное расстояние от АУ до точки наблюдения составляет 0,4 м.

При относительно плохих условиях РРВ от АУ к БС (условиях затенения мест скопления абонентов зданиями) суммарная интенсивность ЭМП, создаваемая электромагнитным излучением АУ, может достигать 0,08 Вт/м^2. Предельно допустимый уровень ЭМП сотовой связи, ограничивающий вынужденный риск для здоровья населения, в Республике Беларусь составляет 0,1 Вт/м^2. При ρ_{MS} = 0,16 АУ/м^2 верхняя граница диапазона суммарной интенсивности ЭМП, создаваемого электромагнитным излучением АУ, составляет 0,06 Вт/м^2. В случае нахождения АУ в прямой видимости с ближайшей БС этот уровень снижается до 0,001 Вт/м^2.

Таким образом, при относительно плохих условиях РРВ от АУ к БС в местах скопления абонентов излучение АУ в активном состоянии может вносить существенный вклад в общий уровень ЭМП, создаваемый многими другими источниками электромагнитного излучения.

ПРОТОКОЛ ЗАЩИТЫ ТРАНСПОРТНОГО УРОВНЯ

М.А. Севостьянюк, А.С. Шелягович

Протокол TLS шифрует интернет-трафик любого вида, тем самым делая безопасными общение и транзакции в сети. Если ваши данные не шифруются, любой может проанализировать их и прочитать конфиденциальную информацию. Кроме веб-трафика, TLS также используется в почте и системах телеконференций. TLS использует самый безопасный метод шифрования – асимметричный. Так как в асимметричном шифровании применяются сложные математические расчеты, нужно много вычислительных ресурсов, поэтому TLS решает эту проблему, используя шифрование только в начале сессии, чтобы зашифровать общение между сервером и клиентом. Сервер и клиент должны договориться об одном ключе сессии, который они будут вдвоем использовать, чтобы зашифровать пакеты данных. Основной целью создания данного протокола являлось получение относительно безопасного канала для осуществления покупок или управления банковским счетом. В современном Интернете на TLS полагаются не только в коммерческой деятельности, но и при решении гораздо более общей задачи сохранения приватности и конфиденциальности важной информации. Одним из самых распространенных применений TLS является HTTPS. HTTPS стремительно вытесняет незащищенную версию (HTTP): доля зашифрованного веб-трафика растет, скорее всего, в скором будущем ожидается, что, практически весь веб-трафик будет зашифрован. Сегодня SSL/TLS – один из самых изученных, исследованных протоколов современного Интернета. Ключевым отличием TLS от SSL является наличие поддержки целого ряда расширений протокола, позволяющих реализовать современные методы защиты информации. На сегодняшний день TLS 1.2 является самой распространенной версией протокола. В новой версии TLS 1.3 будет совместимость с предыдущими версиями: например, соединение откатится до версии TLS 1.2, если одна из сторон не сможет использовать более новую систему шифрования в списке разрешенных алгоритмов протокола версии 1.3. Однако при атаке типа активного вмешательства в соединение, если хакер принудительно попытается откатить версию протокола до 1.2 посреди сессии, это действие будет замечено, и соединение прервется. Версия 1.3 протокола TLS, которая скоро будет выпущена, решает множество проблем с уязвимостями тем, что отказывается от поддержки устаревших систем шифрования [1, 2].

Литература

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на языке С. М.: ЗАО Компьютерное издательство «Диалектика», 2016. 221 с.

2. Бабаш А. Криптографические методы защиты информации. Т. 1. М.: Инфра-М, 2013. 124 с.

ОСОБЕННОСТИ ФОРМИРОВАНИЯ РЕЧЕПОДОБНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ НА КАЗАХСКОМ ЯЗЫКЕ

Е.Н. Сейткулов, А.В. Потапович, Г.В. Давыдов, В.А. Попов

Методы формирования речеподобных сигналов на русском и белорусском языках рассматриваются в работах [1–3]. Для формирования речеподобных последовательностей на казахском языке за основу можно использовать метод синтеза речеподобных сигналов