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.