УДК 004.056.53

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ВЫЯВЛЕНИЯ ВНУТРЕННИХ НАРУШИТЕЛЕЙ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Палтусов Н.А., Дудкин А.С. (Военно-космической академии имени А.Ф.Можайского)
Научный руководитель – к.т.н. Дудкин А.С.
(Военно-космической академии имени А.Ф.Можайского)

Аннотация. Основной идеей настоящего исследования является разработка программно-аппаратного комплекса для выявления незарегистрированных устройств сотовой связи на объектах критической информационной инфраструктуры государственного назначения при помощи IMSI-ловушек, перехвата зашифрованного GSM-трафика, манипулируя параметрами MCC, MNC и LAC, на базе платформы OsmocomBB и одноплатного микрокомпьютера Raspberry Pi 3B+ и мониторинга состояния сети сотовой связи на предмет наличия компрометирующей и потенциально-опасной информации на объектах критической информационной инфраструктуры. Эксперименты с перехватом трафика и определением ключей шифрования, проводимые с использованием airprobe и Kraken, не наносят ущерб реальному оператору сотовой связи. В ходе работы применяется технология SDR (Software Defined Radio).
Основная цель разработанного программного средства – создание условий для анализа состояния сети сотовой связи на объекте КИИ и выявления потенциально-опасной информации на объектах критической информационной инфраструктуры, а также противодействия внутренним нарушителям без необходимости администрирования комплекса.

Введение.

Диапазон целей у злоумышленников в сетях сотовой связи может быть крайне широк: прослушивание телефонных переговоров, перехват вызовов и клонирование телефонных аппаратов. Принимая в расчет уровень и доступность современных технологий, а также количество сценариев проведения злоумышленником атак на конфиденциальность абонента в сети сотовой связи, становится очевидным, что проблемы безопасного использования технологий сотовой связи стандарта GSM в целом и, вопросы безопасности аутентификации абонентов сети GSM, в частности, в настоящий момент стоят достаточно остро.

Исследования уязвимостей алгоритмов GSM на сегодня не потеряли своей актуальности. Более того, учитывая факт повсеместного распространения сотовых телефонов, а значит и SIM - карт, среднестатистические (легальные) пользователи, не обладая достаточными знаниями о возможностях нелегального использования смарт - карт, часто не уделяют должного внимания их сохранности и процедурам вывода карт из обращения, давая тем самым возможность злоумышленникам для их беспрепятственного клонирования.

Кроме того, в силу использования закрытых алгоритмов шифрования и сопутствующих стандартов в GSM, задачи по теоретическим и практическим оценкам границ стойкости реализованных в GSM решений также требуют дополнительного изучения.

Основная часть.

Разработанный программно-аппаратный комплекс позволяет своевременно выявлять внутренних нарушителей на объектах критической информационной инфраструктуры и производить мониторинг состояния сети сотовой связи на предмет наличия компрометирующей и потенциально-опасной информации, перехватывать весь зашифрованный трафик, манипулируя параметрами MCC, MNC и LAC, на базе платформы OsmocomBB и одноплатного компьютера Raspberry Pi 3B+.

Программно-аппаратный комплекс выявления внутренних нарушителей на объектах критической информационной инфраструктуры государственного назначения обладает следующими свойствами: осуществление анализа большого объема трафика сети сотовой связи, обеспечивающего расширенную аналитику в реальном времени, определение источников угроз безопасности информации и оценка возможностей нарушителей по

реализации угроз безопасности информации, определение внутренних нарушителей на объектах КИИ и анализ информации на предмет потенциально-опасной и компрометирующей информации без необходимости администрирования.

Результаты

На сегодняшний день уже удается:

• производить мониторинг состояния сети сотовой связи;

• выявлять потенциально-опасную и компрометирующую информацию;

• дублировать комплекс на отечественное ПО (astra linux);

• перехватывать зашифрованный GSM-трафик;

• выявлять внутренних нарушителей на объектах КИИ;

• обеспечивать постоянную работу комплекса без необходимости администрирования.

Заключение

Информации, содержащийся и обрабатываемой в информационных системах на объектах КИИ государственного назначения, становится все больше. Контроль пространства в сетях сотовой связи, как методы сбора, изменения и разрушения информации организации, предприятий, государств и отдельно взятых личностей нестабилен, вместе с этим технический прогресс оказывает свое влияние на текущее состояние в области сотовой связи.

В связи с этим, данное устройство радиоконтроля и радиоперехвата, основанное на принципе IMSI-ловушки и инновационном подходе в области обеспечения защиты объектов КИИ государственного назначения, с использованием отечественных сертифицированных программно-аппаратных модулей, необходимо на предприятиях и объектах КИИ государственного назначения. Также необходим своевременный анализ состояния защищенности объектов КИИ МО РФ в сети сотовой связи на предмет потенциально-опасной и компрометирующей информации, основанный на принципе обработки GSM-трафика при помощи нейронных сетей.