Сколько безопасности требуется от встраиваемой в промышленное устройство ОС?

ФИО: Парьев Сергей Евгеньевич

Организация: Лаборатория Касперского

E-mail: tr-serge@mail.ru

Одним из применений встраиваемой ОС является создание на её основе промышленных устройств. Примерами таких устройств являются: ПЛК (программируемый логический контроллер); УСПД (устройство сбора и передачи данных), терминал РЗА (релейной защиты и автоматики); разнообразные медицинские приборы; бортовые системы транспортных средств; сетевое оборудование, используемое в промышленности и др.

Современная ситуация требует, чтобы эти устройства могли сохранять свою работоспособность в условиях воздействия на них компьютерных атак (более того, значительная часть таких устройств работают в составе объектов критической информационной инфраструктуры с повышенными требованиями к информационной безопасности). Поэтому разработчики промышленных устройств уделяют в настоящее время повышенное внимание информационной безопасности.

Для того, чтобы понять сколько безопасности требуется от встроенной в такое устройство ОС необходимо начать с модели угроз безопасности самого устройства и затем уже транслировать получающиеся угрозы к самой встраиваемой ОС.

В рамках доклада будет дана упрощенная модель угроз для типичного промышленного устройства: определены основные защищаемые информационные объекты, пользователи, типы нарушителей и далее угрозы информационной безопасности.

Будет также дан краткий обзор требований по информационной безопасности, релевантных для таких устройств: требования по критический информационной инфраструктуре (239-й приказ ФСТЭК России), МЭК 62443-4, МЭК 62351 и др.

По мнению автора встраиваемая ОС должна брать на себя основную роль при парировании угроз информационной безопасности на такое устройство. Для их парирования ОС должна иметь соответствующие встроенные механизмы защиты. Механизмы защиты условно можно разделить на две группы: 1) используемые для самозащиты ОС 2) используемые для защиты прикладного ПО, работающего поверх встраиваемой ОС и входящего в состав устройства.

Исходя из полученной модели угроз, а также типовых нормативных требований, будет рассмотрен ряд необходимых для парирования актуальных угроз безопасности механизмов защиты. Эти механизмы могут (а по мнению автора должны) быть встроены непосредственно в ОС. В рамках доклада будут рассмотрены необходимые механизмы защиты: доверенная загрузка; контроль целостности самой ОС и прикладного ПО; контроль сетевых потоков и защита от базовых сетевых атак; организация защищенных сетевых каналов; аудит безопасности и возможности отправки событий безопасности в централизованные системы сбора таких событий; аутентификация, идентификация и авторизация пользователей в ОС/устройстве; возможности централизованного управления пользователями и др.

В завершении доклада будет также дан обзор проблем, с которыми сталкиваются разработчики безопасных промышленных устройств при использовании имеющихся на рынке встраиваемых ОС.