УДК 004.492.2

ОБЗОР СОВРЕМЕННОГО СОСТОЯНИЯ ЗАЩИЩЕННОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ, ПОСТРОЕННЫХ НА ОСНОВЕ ПЕРИФЕРИЙНЫХ ВЫЧИСЛЕНИЙ

Садикова А.А. (Университет ИТМО, Санкт-Петербург)

Быстрый рост объема данных, производимых датчиками и устройствами IoT, привел к появлению граничных вычислений, в которых данные обрабатываются в точке, в которой они находятся, или рядом с ними. Это способствует снижению задержки, а также безопасности и конфиденциальности данных за счет локализации данных на граничном узле. Однако из-за проблем, связанных с ограниченными ресурсами аппаратного и программного обеспечения, большинство периферийных вычислительных систем подвержены большому количеству атак.

В данной работе рассмотрены различные атаки и угрозы для киберфизических систем, построенных на основе периферийных вычислений.

Целью данной работы является классификация атак и угроз для киберфизических систем для дальнейшей разработки набора мер для противостояния им.

Хотя периферийные вычисления имеют множество преимуществ и используются в различных сценариях, они не лишены определенных угроз и проблем безопасности. Фактически, следующие факторы способствуют расширению поверхности атаки в случае граничных вычислений:
аппаратные ограничения: поскольку большинство периферийного вычислительного оборудования (периферийные устройства и даже пограничные серверы) имеют меньшую вычислительную мощность и емкость хранилища по сравнению с туманным или облачным сервером, они неспособны запускать выделенные системы предотвращения атак, такие как брандмауэры, и поэтому более уязвимы к атакам,
неоднородность программного обеспечения: большинство устройств и серверов, работающих на граничном уровне, обмениваются данными с использованием большого количества различных протоколов и операционных систем без стандартизированных правил. Это усложняет задачу создания единого механизма защиты.

Большинство этих угроз усугубляются из-за недостатков конструкции, ошибок реализации и неправильной конфигурации устройств на периферийных устройствах и серверах. Кроме того, отсутствие полноценных пользовательских интерфейсов во многих периферийных устройствах часто не позволяет распознать текущую или предполагаемую атаку.

В свете вышесказанного понимание угроз безопасности (и средств защиты) в пограничных вычислениях приобретает первостепенное значение. Отмечается необходимость разработки перечня мер противодействия атакам, направленным на киберфизические системы, построенные на основе периферийных вычислений.

Садикова А.А. (автор)