УДК 004.492.2

АЛГОРИТМ АУТЕНТИФИКАЦИИ КОНЕЧНЫХ УСТРОЙСТВ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

Садикова А.А. (Университет ИТМО, Санкт-Петербург)
Научный руководитель – д.т.н., проф. Гатчин Ю.А.

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. Большинство 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 данной работе рассмотрены атаки и угрозы для киберфизических систем, построенных на основе периферийных вычислений, существующие методы и алгоритмы аутентификации конечных устройств подобных систем и приведен алгоритм аутентификации конечных устройств киберфизических систем.

Целями данной работы является классификация атак и угроз для киберфизических систем для дальнейшей разработки набора мер для противостояния им, выявление недостатков и ограничений существующих решений аутентификации конечных устройств киберфизических систем, а также разработка алгоритма аутентификации конечных устройств киберфизических систем для нивелирования части выявленных угроз.

Основные возможные атаки на безопасность и конфиденциальность приведены ниже:

1) Внедрение вредоносного оборудования и/или программного обеспечения.
2) Jamming Attacks.
3) Распределенные атаки типа «отказ в обслуживании» (DDoS).
4) Физические атаки или взлом.
5) Подслушивание или перехват.
6) Атаки по побочным каналам вне сети.
7) Атаки на информацию о маршрутизации.
8) Атаки подделки.
9) Несанкционированный доступ.
10) Атаки на целостность машинного обучения.
11) Replay Attack или Freshness Attacks.
12) Несущественные атаки журналирования.
13) Угрозы безопасности с / на IoT-устройствах.
14) Утечка конфиденциальности.

В рассмотренных работах других исследователей также наблюдается проблема необходимости значительных затрат ресурсов, что может привести к осложнениям при развертывании системы.

Отмечается, что технология Mobile Edge Computing (MEC) имеет ряд недостатков, в том числе проблема идентификации сервера MEC.

Таким образом, внутренние злоумышленники могут стереть следы доступа к чужим данным благодаря своим законным правам доступа. В связи с этим отмечается необходимость

разработки алгоритма аутентификации в периферийных вычислениях, чтобы защитить пользователей и решить проблемы конфиденциальности, минимизировав внутренние и внешние угрозы.

Садикова А.А. (автор)

Гатчин Ю.А. (научный руководитель)