РАСШИРЕННАЯ КЛАССИФИКАЦИЯ USB АТАК

Мамченко М.В.

Институт проблем управления им. В.А. Трапезникова РАН,
Россия, г. Москва, ул. Профсоюзная д. 65
markmamcha@gmail.com,

Сабанов А.Г.

Московский государственный технический университет им. Н.Э. Баумана,
Россия, г. Москва, ул. 2-я Бауманская д. 5 стр. 1
asabanov@mail.ru

Аннотация: В открытых источниках описаны классификации уязвимостей и угроз USB интерфейса, при этом кибератаки обычно рассматриваются в общем, и отдельно USB атакам практически не уделяется внимания. В статье рассматривается текущее состояние исследований в данной области и предлагается единая классификация USB атак.

Ключевые слова: USB, атаки, классификация.

Введение

В современных условиях обеспечение информационной безопасности – краеугольный камень стабильного роста организаций, высокого уровня репутации, доверия со стороны пользователей/клиентов, а также гарантии сохранности сетевой ИТ-инфраструктуры и конфиденциальных данных.

В настоящее время постоянно выявляются все новые и новые способы совершения кибератак, зачастую с готовым программным решением в рамках подтверждения гипотезы (proof-of-concept). Кроме того, активно проводятся исследованию по поиску новых способов применения уже известных атак. В связи с этим возникает необходимость их обобщения, анализа и классификации. Это позволяет сформировать (уточнить) требования к системам защиты и, возможно, сократить их

стоимость и издержки на развертывание. Более того, в случае совершения несанкционированных действий злоумышленником тщательный анализ атаки позволяет сделать вывод об уровне подготовки злоумышленника, его цели и принадлежности к какой-либо преступной группе.

В данной работе внимание уделяется исключительно USB интерфейсу. Цель работы заключается в том, чтобы проанализировать известные системы классификации кибератак и USB атак, оценить их эффективность и применимость и предложить собственную единую систему классификации USB атак.

1 Анализ текущего состояния в области классификация USB атак

Описание и классификация атак обычно осуществляется в рамках анализа и составления моделей угроз. В источнике [1] представлена универсальная модель киберугроз, составленная на базе уже известных (AVOIDIT Cyber Attack Taxonomy, Common Attack Pattern Enumeration and Classification, CNI Cyber Taxonomy, Common Language Security Incident Taxonomy, Military Activities and Cyber Effects Taxonomy). Частью данной модели является система классификации кибератак, проводимая по следующим основаниям: «по способу внедрения», «по используемым средствам», «по уровню автоматизации» и «по совершаемым действиям».

Ниже представлен список других рассматриваемых систем классификации кибератак:

1. В источнике [2] основное внимание уделяется оценке урона, наносимого атакой.
2. В исследовании [3] рассматриваются только внутренние атаки (атаки инсайдеров), их классификация осуществляется только по объекту воздействия.
3. В работе [4] представлена общая классификация кибератак по следующим основаниям: «намерения злоумышленника» и «используемые средства».

Кроме того, существуют работы, посвященные исследованию исключительно USB атак. Однако, например, в работе [5] система классификации содержит только одно основание – «по типу используемого оборудования». Другая группа исследователей рассматривает USB атаки исключительно как нарушения взаимодействия иерархических уровней: приложений, драйверов, порта (интерфейса) и устройств [6]. Схожим способом классифицируются USB атаки и в статье [7], при этом основное внимание уделяется их функциональным особенностям, так что основание классификации можно назвать «по вектору атаки»: уровень приложений, транспортный и физические уровни дополнены пользовательским, USB атаки рассматриваются как практическая реализация угроз со стороны инсайдеров и "внешних" злоумышленников.

На рисунке 1 представлены различные подходы к классификации кибератак (в целом) и USB атак (в частности). Очевидно, что основания классификаций не пересекаются. Однако существующие базовые классификации относятся ко всем кибератакам и не адаптированы под особенности атак USB интерфейса, а известные системы классификации USB атак имеют малое количество оснований. Таким образом, возникает необходимость создания обобщенной универсальной системы классификации USB атак, учитывая текущие результаты проделанных работ.

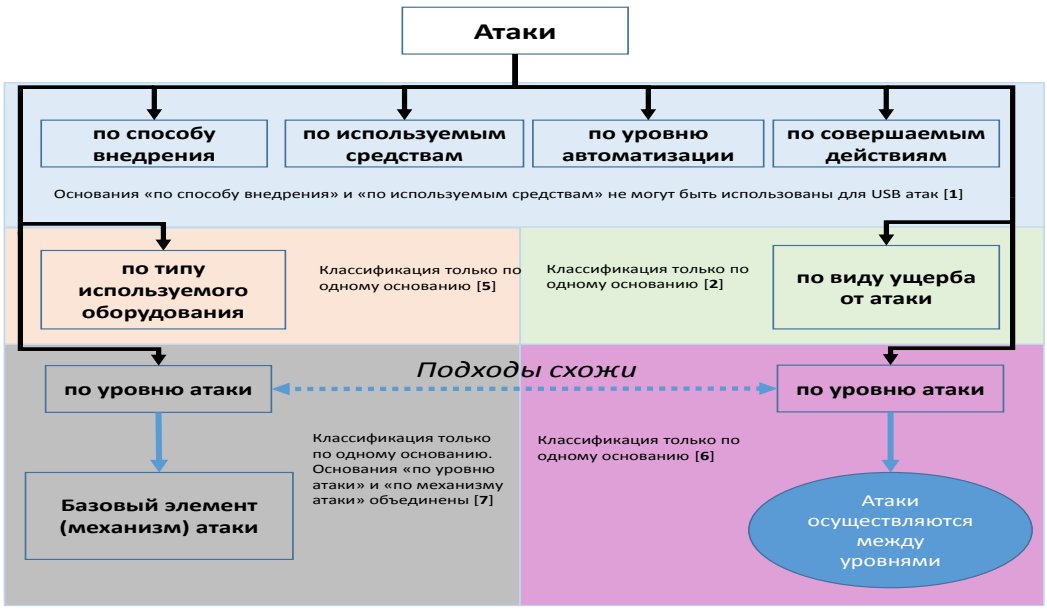

Рис. 1. Рассмотренные системы классификации кибератак и USB атак

2 Разработка единой системы классификации USB атак

Проанализировав вышеуказанные источники, содержащие различные системы классификации кибератак и USB атак, полагаем целесообразным внедрить в разрабатываемую классификацию следующие основания: «по механизму атаки», «по источнику угрозы», «по уровню воздействия» – из источника [7], «по используемым средства» – из работы [5], «по типу ущерба от атаки» – из статьи [2].

Кроме того, на данном этапе предлагается внести авторские измерения и дополнения в систему классификации:

добавить не описанные ранее основания: «по намерениям злоумышленника», «по объекту воздействия», «по уровню скрытности», «по уровню сложности атаки», «по серьезности последствий»;

дополнить известные примеры из основания «по используемым средствам» (программируемые микроконтроллеры; перепрограммируемое периферийное оборудование; периферийное оборудование без перепрограммирования; электрические устройства [5]) следующими: «специальное аппаратное оборудование» и «вредоносные программы». Использование этого основания делает возможным классификацию так называемых атак по сторонним каналам (например, перехват побочных электромагнитных излучений (ПЭМИ) и всех атак, связанных с программным обеспечением (вирусы, троянские программы и т.д.);

дополнить основание «по совершаемым действиям» [1] примерами «уничтожение оборудования», «осуществление перехвата» и «вызов неправильного функционирования/отказа в обслуживании». Например, устройство USB Killer просто уничтожает оборудование; регистрация и анализ ПЭМИ от USB устройств осуществляется за счет его перехвата; USB атаки на сервер RDP (RDP – Remote Desktop Protocol, протокол удаленного доступа) через службу «RemoteFX USB Redirection» с помощью устройства BadUSB может рассматриваться как целенаправленные действия по вызову отказа в обслуживании);

все основания предлагаемой классификации объединены к единую систему с учетом специфики USB атак.

На рисунке 2 представлена разработанная система классификации.

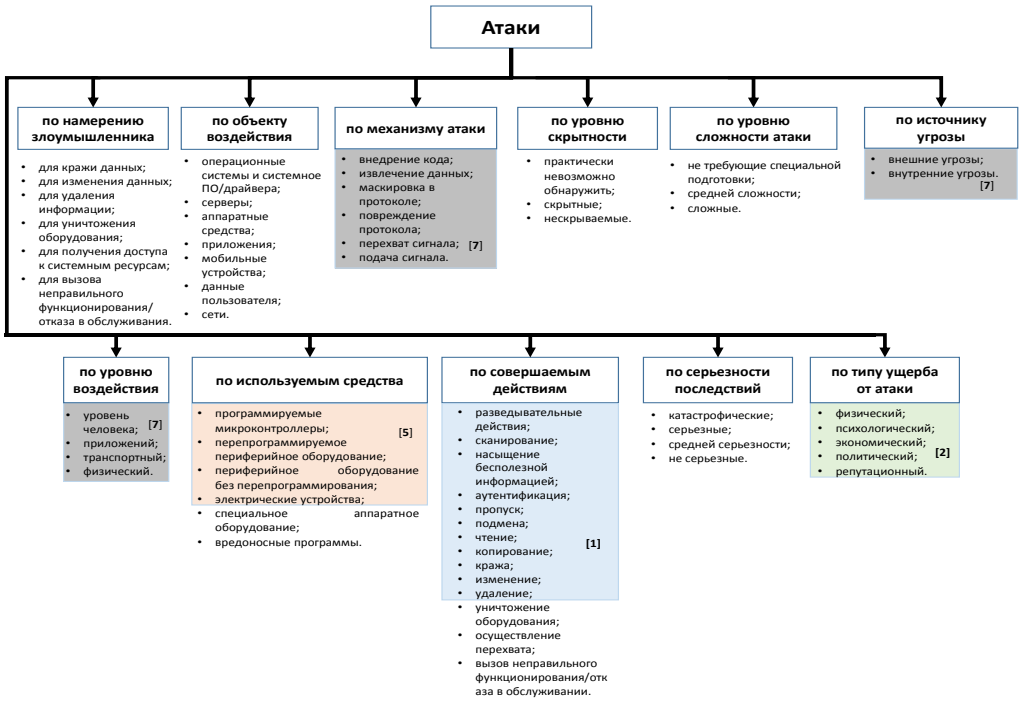

Рис. 2. Рассмотренные системы классификации кибератак и USB атак

Классификация любой из атак по всем вышеуказанным основаниям одновременно позволяет оценить уровень подготовки и оснащения злоумышленника (злоумышленников), спрогнозировать последствия атаки и оценить ее возможные векторы. В некоторых случаях появляется возможность выявить связь злоумышленника с определенной группой (с учетом особенностей атаки). Кроме того,

тщательный анализ и классификация атак позволяет наметить способы противодействия им и выявить недостатки в системе обеспечения информационной безопасности целевых объектов.

Литература

1. State-of-the-Art in Cyber Threat Models and Methodologies, March 2016, Bell, Canada, http://cradpdf.drdc-rddc.gc.ca/PDFS/unc225/p803699_A1b.pdf, last accessed 2019/06/15.

2. SWIFT Institute Working Paper NO. 2016-002. The Cyber Security Ecosystem: defining a Taxonomy of existing, emerging and future Cyber Threats. Jason Ferdinand, Richard Benham, https://swiftinstitute.org/wp-content/uploads/2017/10/SIWP-2016-002_Cyber-Taxonomy_-Ferdinand-Benham-_vfinal2.pdf, last accessed 2019/06/15.

3. Homoliak I., Toffalini F., Guarnizo J., Elovici Y., Ochoa M. Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures // ACM Computing Surveys. Vol. 52. 2019. – P. 30:1-30:40.

4. Reference Incident. Classification Taxonomy. Task Force Status and Way Forward. January 2018. European Union Agency For Network and Information Security, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/at_download/fullReport, last accessed 2019/06/15.

5. Nissim N., Yahalom R., Elovici Y. USB-based attacks // Computers&Security. Vol. 70. 2017. – P. 675-688.

6. Fu J., Huang J., Zhang L. Curtain: Keep Your Hosts Away from USB Attacks // Information Security. ISC 2017. Lecture Notes in Computer Science. Vol. 10599. 2017. – P. 455-471.

7. Tian J., Scaife N., Kumar D., Bailey M., Bates A., Butler K. SoK: “Plug & Pray” Today – Understanding USB Insecurity in Versions 1 Through C // 2018 IEEE Symposium on Security and Privacy (SP). Vol 6. 2018. – P. 1032-1047.