Литература:
1. *Курако Е.А., Орлов В.Л.* Сервис-браузеры для информационных систем // Программная инженерия. – 2017. – Том 8. №9. – С. 413-421.
2. *Курако Е.А., Орлов В.Л.* Организация защиты информации в системах, использующих сервис-браузеры / Материалы 26-й Международной научной конференции «Проблемы управления безопасностью сложных систем» (Москва, 2018). – М.: ИПУ РАН, 2018. – С. 109-112.

DOI: 10.25728/iccss.2022.61.68.019

Исхаков А.Ю.

Анализ запросов в протоколах прикладного уровня при реализации усиленной проверки подлинности субъектов доступа

Аннотация: При реализации эшелонированной защиты для критически важных объектов особое внимание уделяется снижению коэффициентов ложноположительных срабатываний средств защиты информации. В этой связи эффективным решением является разработка адаптивных многофакторных алгоритмов проверки подлинности, учитывающих особенности индикаторов компрометации и векторов предполагаемых атак в том числе в ходе инспектирования протоколов прикладного уровня. В рамках данного исследования рассматриваются признаки, доступные в ходе проведения инспекции HTTP-запросов при реализации усиленной проверки подлинности субъектов доступа.

Ключевые слова: протокол прикладного уровня, анализ запросов, индикатор компрометации, усиленная проверка подлинности, кибератака

В настоящее время в ходе инструментального анализа кибербезопасности различных объектов критической инфраструктуры исследователи продолжают фиксировать большое количество уязвимостей, связанных с интерфейсами доступа,

функционирующих на прикладном уровне. Так, на рисунке 1 представлена выдержка из ежегодно публикуемого общедоступного отчета компании Positive Technologies [1].

В этой связи, при построении защищенного периметра необходимо особое внимание уделять обеспечению защиты веб-сервисов, а также других интерфейсов взаимодействия прикладного уровня [2].

Сервис	Высокий риск, эксплойт	Высокий риск	Средний риск, эксплойт	Средний риск	Низкий риск
Веб-сервисы	24	609	344	3659	1507
Удаленный доступ	110	192	234	452	441
Служба доменных имен	36	183	21	227	15
Электронная почта	—	10	102	598	437
VPN-сервисы	—	—	12	30	24
Файловые службы	—	—	4	49	19
Другие	—	7	14	72	51

Рисунок 1 – Распределение уязвимостей по сервисам и уровням риска

При разработке алгоритмического обеспечения для усиленной проверки подлинности субъектов актуальной является задача реализации адаптивного подбора дополнительно проверяемых факторов. Для реализации механизмов, осуществляющих адаптацию набора, типа факторов, а также подбора безопасных для конкретной операции технологии транспорта данных необходимо осуществлять автоматизированную оценку риска угрозы при нетипичном поведении субъекта в режиме времени, близком к реальному.

В ходе проведения данного исследования был проведен обзор возможных индикаторов компрометации, применяемых для решения данной задачи. Под индикаторами компрометации понимаются исключительно технические категории IOC [3], т.е. цифровые артефакты, явно указывающие на потенциальную вредоносность

описываемого запроса и/или факт компрометации защищаемого объекта. При этом, в качестве ограничения выступает соответствие протоколам прикладного уровня. В ходе инспекции предлагается осуществлять анализ всех запросов, поступающих от субъектов доступа, с целью проверки фактов:

– обращения к не содержащимся в WL (white list) списке доступа URL/URI, использование нелегитимных значений host и т.д.;

– несоответствия используемых токенов безопасности;

– наличия артефактов Slowloris атак [5];

– ограничений на список используемых методов HTTP;

– фактов превышения пороговых значений на длину HTTP-запроса;

– превышение общей длины всех HTTP-заголовков;

– время подготовки ответа по заголовкам и телу запроса.

Не менее важным является проведение глубокого анализа тела запроса, включая поиск индикаторов по наличию хеш-значений из TI-платформ, анализ по преднастроенным шаблонам регулярных выражений, выявление различных инъекций и т.д.

Использование вышеуказанных индикаторов в ходе анализа запросов в протоколах прикладного уровня позволяет реализовывать эффективные механизмы усиленной проверки подлинности субъектов доступа за счет обогащения анализируемых индикаторов в произвольном теле запроса с помощью автоматизированных проверок других его составных элементов.

Исследование выполнено при финансовой поддержке РНФ (проект №21-71-00125)

Литература:

1. Уязвимости периметра корпоративных сетей Результаты инструментального анализа защищенности. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ vulnerabilities-corporate-networks-2020-rus.pdf (дата обращения 15.10.2022).

2. *Баранова Е.М.* Анализ современных систем защиты Web-сервисов // Известия ТулГУ. Технические науки. – 2018. – №10. – С. 93-100.

3. *Дрянных Ю.Ю., Жуков В.Г.* Автоматизация сбора, проверки и загрузки индикаторов компрометации в платформу Threat

Intelligence / Актуальные проблемы авиации и космонавтики: Сборник материалов V Международной научно-практической конференции, посвященной Дню космонавтики. В 3-х томах. Том 2. – Красноярск: Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, 2019. – С. 225-227.

4. *Исхаков А.Ю., Мещеряков Р.В., Исхаков С.Ю.* Проблемы применения индикаторов компрометации для проактивного поиска угроз в работе робототехнических комплексов / Управление развитием крупномасштабных систем (MLSD'2021): Труды Четырнадцатой международной конференции (Москва, 27-29 сентября 2021 года) / Под общей редакцией С.Н. Васильева, А.Д. Цвиркуна. – Москва: Институт проблем управления им. В.А. Трапезникова РАН, 2021. – С. 1340-1347.

5. *Силаков Н.В*. Метод обнаружения аномальных вторжений в компьютерной сети, использующий критерий Фишера // Научно-образовательный журнал преподавателей и студентов «StudNet». – 2020. – № 10. – С. 1-13.

DOI: 10.25728/iccss.2022.17.30.020

Жарко Е.Ф.

Управление требованиями, верификация и валидация программного обеспечения АСУ ТП АЭС

Аннотация: Верификация и валидация важных этапов обеспечения безопасности и надежности программного обеспечения. Управление требованиями играет важную роль в рамках всех этапов верификации и валидации. В работе представлена схема управления требованиями для программного обеспечения систем, важных для безопасности АЭС, а также связь этого процесса с верификацией и валидацией.

Ключевые слова: программное обеспечение, верификация, валидация, управление требованиями, АСУ ТП АЭС

Системы верхнего уровня (СВУ) являются важной составляющей АСУ ТП АЭС. Верификация и валидация (V&V) [1] являются необходимыми этапами в обеспечении качества