Адам Шостак

ЗАЩИТА СИСТЕМ

ЧЕМУ «ЗВЕЗДНЫЕ ВОЙНЫ» УЧАТ ИНЖЕНЕРА ПО

БОМБОРА
ИЗДАТЕЛЬСТВО
Москва

УДК 004.056
ББК 32.973.2-018.2
Ш79

Шостак, Адам.

Ш79 Защита систем : чему «Звездные войны» учат инженера ПО / Адам Шостак ; [перевод с английского В. М. Беленковича]. — Москва : Эксмо, 2025. — 480 с. — (Мировой компьютерный бестселлер).

ISBN 978-5-04-199464-8

Гарантия безопасности программного обеспечения — одна из ключевых задач разработчиков в современном мире. Адам Шостак рассказывает об основах и практиках информационной безопасности с использованием идей вселенной «Звездных войн». В книге дан целый арсенал стратегий и методов защиты, которые применимы не только в фантастическом мире, но и в реальных работающих системах! Автор рассказал о закономерности проблем безопасности и предложил оптимальные решения, продемонстрировал практические модели.

УДК 004.056
ББК 32.973.2-018.2

ISBN 978-5-04-199464-8

Империя не считает однопилотные истребители угрозой для станции. Иначе бы они уплотнили оборону.

Генерал Додонна

Об авторе

Адам Шостак — ведущий эксперт по моделированию угроз. Он также является дизайнером игр, выступает в роли консультанта и судебного эксперта. Много лет он посвятил разработке безопасных продуктов и систем. В мире бизнеса диапазон его опыта охватывает самые разные области, от основания стартапов до почти десяти лет работы в Microsoft.

Ниже перечислены некоторые из его достижений.

- Помог создать CVE (Common Vulnerabilities and Exposures, база данных общеизвестных уязвимостей информационной безопасности); в настоящее время является почетным членом ее консультативного совета.
- Исправил автозапуск для Windows XP и Vista.
- Руководил разработкой и реализацией инструмента моделирования угроз Microsoft SDL (v3).
- Создал игру по моделированию угроз Elevation of Privilege и участвовал в создании игры Control-Alt-Hack.
- Автор книги Threat Modeling: Designing for Security («Моделирование угроз: проектирование для обеспечения безопасности») и соавтор книги The New School of Information Security («Новая школа информационной безопасности»).

Помимо консультирования и преподавания, Шостак выступает в качестве советника многих компаний и академических учреждений. Он является аффилированным профессором в Школе компьютерных наук и инженерии имени Пола Г. Аллена при Вашингтонском университете.

Подробнее о нем можно узнать на сайте shostack.org.

Благодарности

Эта книга была бы совершенно иной, если бы Джордж Лукас не придумал свой потрясающий и многогранный мир и если бы команда и актерский состав «Звездных войн» не воплотили его в жизнь. Если бы эта первая команда не вникала в детали, мы могли лишиться очень многого.

Эта книга — результат пятилетней миссии «Как объяснить инженеру, что такое безопасность». В 2017 году один джентльмен из Купертино задал мне простой вопрос: «Где я могу узнать больше об этих угрозах?» Я не записал его имя, но, если вы читаете этот текст, спасибо за вопрос, и извините, что так долго не отвечал.

В процессе исследований я говорил с сотнями людей о том, что «должен знать каждый инженер». Я хочу поблагодарить их всех за вклад в создание этой книги. А все ошибки, которые остались, принадлежат мне.

Моя замечательная команда преподавателей из Shostack + Associates (Валерий Берестецкий, Джейми Дикен и Кэролайн Эммотт) также прочитала весь черновик (иногда не по одному разу) и помогла убедиться, что многое из того, чему мы научились у наших студентов, вошло в книгу и что на многие вопросы, которые они задавали, даны ответы.

Параллельно с написанием книги я также работал над набором курсов в LinkedIn Learning. С командой, в которую в том числе входили Алисса Пратт, Рэй Хойт и Эндрю Проберт, у нас сложились теплые отношения, они поддерживали и наставляли меня на протяжении всего этого времени. Работа с ними над набором курсов по STRIDE одновременно с работой над книгой помогла улучшить и то и другое.

Лорен Конфельдер сделала больше, чем просто создала мнемоническую схему STRIDE (вместе с Преритом Гаргом), которая легла в основу этой книги. Она также прочитала бóльшую часть этой книги в черновом варианте, и я высоко ценю наши долгие беседы о деталях, а также о структуре.

Дин Триббл и Джонатан Шапиро напомнили мне о работе Марка Миллара «Власть» (Authority) как о способе выхода из беспорядочных размышлений о привилегиях и разрешениях. Этот ужас мог положить конец всей затее. Точно так же глава о синтаксическом анализе стала намного понятнее и богаче, когда я прочитал работу сообщества LangSec. Джефф Уильямс вдумчиво просмотрел первые черновики. Изар Тарандах внимательно прочитал текст, хотя его книга отчасти конкурирует с моей. Джим Белл объяснил, как космические аппараты на Марсе отслеживают время.

Некоторые из первых улучшений относились к тексту, который изменился настолько, что эти улучшения больше не видны. Я чрезвычайно благодарен этим людям, потому что они помогли книге не очень заметным, но очень важным образом: Майкл Ройтман предложил форматы дат для устойчивости канонизации, и их гораздо легче анализировать, чем мои примеры URL-адресов. Ким Вуйтс помог с определением предсказуемости и ее воздействии на неприкосновенность частной жизни.

Спасибо также Джону Калласу, Крису Энгу, Марку Френчу, Тому Гэлхагеру, Шону Эрнану, Джеффу Джармоку, Аррону Джонсону, Кристофу Клаассену, Лаки Манро, Даниэлю Остермайеру, Яну Пойнтеру, Джону Пулену, Моргану Роману, Ананту Шриваste, Пелеусу Ули, Таре Уилер и Чарльзу Уилсону.

Дуг Барнс, адвокат и киберпанк, был тем другом, который написал фразу «Включать в свои протоколы этап „а потом появляются полицейские“ — это сомнительная идея», цитируемую в главе об отказе от ответственности. Предложение и абзац были сложными, и поэтому я благодарю его здесь.

Неоднократно авторы использовали «Звездные войны» для иллюстрации своих теорий: The Ultimate Star Wars and Philosophy («Путеводитель по „Звездным войнам“ и философия») [Wiley, 2015], «Звездные войны. Психология киновселенной» (Star Wars Psychology) [Sterling, 2015] и «Мир по „Звездным войнам“» (The World According to Star Wars) [Sunstein, 2016]. Я многому научился у каждого из них и использую «Звездные войны» более целенаправленно и детально благодаря тому, что они указали мне путь. Келлман Мегу отметил, что в сцене перед появлением Дарта Вейдера имперские войска проводят довольно серьезное совещание по реагированию на вторжение, но я не нашел способа включить это в текст. И, говоря о содержании «Звездных войн», я особенно хочу поблагодарить читателей, которые не очень с ним знакомы: они отметили места, где я переусердствовал с погружением в тему. Они предпочли остаться анонимными, хотя ни в чем меня не подвели.

И последнее, но не менее важное: я хочу поблагодарить мою команду в издательстве Wiley. Джима Минателя за то, что он снова и снова задавал провокационные

вопросы, пока я не сообразил, что пишу что-то не то, а затем советовал, как написать книгу, которая опирается на любимую вселенную. Келли Тэлбот — фантастический редактор проектов, принимавшая все проблемы с юмором. Ким Уимпсетт тщательно отредактировала все, что было необходимо, и исправила то, что не стоит называть. Кстати, о неназванных: было много людей, с которыми мне так и не довелось встретиться. Подобно безымянным повстанцам, которые так часто появляются на заднем плане, вы помогли сделать общее дело.

Адам Шостак

Оглавление

Предисловие

Откуда R2-D2 знает, кто такой Бен Кеноби? Как он принимает решение воспроизвести запись принцессы Леи Бену, а не Люку? Как принцесса Лея сообщает R2 о своих намерениях? Эти три вопроса затрагивают фундаментальные аспекты безопасности: аутентификацию, авторизацию и дизайн пользовательского интерфейса (usability). (Фанаты узнают ответ на первый вопрос из приквелов, но Лея его не знает.) Более того, использование компьютеров и технологий в мире «Звездных войн» может стать знакомой основой для изучения работы технологий в нашем мире.

Я был фанатом «Звездных войн» до того, как написал первую строку кода, и задолго до того, как взломал первую систему. Когда я стал экспертом по компьютерной безопасности, мне стало ясно, что мы в силу своей деятельности много лучше пишем код, чем истории, и хотя так и подмывает сказать: «Потому-то у нас ничего не получается», рассказывать истории получше — не единственная наша надежда. Когда я думал о «Звездных войнах», я понял, что сразу после титров камера показывает нам корабль принцессы Леи, который преследуют из-за… украденной запись с данными! Я понял, что «Звездные войны» — это не только история героического путешествия Люка и его взросления, но также история

о раскрытии информации и последствиях этого. Последние десять лет я использовал «Звездные войны», чтобы рассказывать истории о компьютерной безопасности, потому что эпические истории дают нам опорные точки и иллюстрируют важные проблемы.

В этой книге почти все ссылки — на оригинальную трилогию. Есть материал, для которого я мог бы использовать и «Изгой-один», и приквелы, и сиквелы, и телевизионные сериалы, книги и так далее. Но я предполагаю, что большинство читателей смотрели и пересматривали только три эпизода оригинальной трилогии: «Звездные войны: Новая надежда», «Империя наносит ответный удар» и «Возвращение джедая».

Как Сила является свойством каждого живого существа, так и безопасность — это свойство всех технологических систем. И так же, как Сила имеет две стороны — светлую и темную, у безопасности есть защита и атаки. Эта книга в основном про атаки, угрозы, проблемы. Вы должны понимать, в чем угроза, прежде чем выберете подходящую защиту. Сцена, когда император Палпатин пускает в Люка Скайуокера фиолетовые молнии Силы, очень драматична, но, если бы Люк был лучше подготовлен, он бы мог распознать угрозу и понять, как лучше от нее защититься. Ни межсетевой экран, ни список доступа не блокируют молнии Силы.

Если вы хотите сделать свой дом безопасным, вам необходимо подумать о множестве вещей, которые могут причинить вред. Некоторые из них природного происхождения (наводнение), некоторые могут быть и природными, и рукотворными (пожар), а некоторые (воровство) являются действиями разумных существ.

У нас есть неявные модели того, что такое дом, типы домов и общие типы проблем. Эти проблемы могут