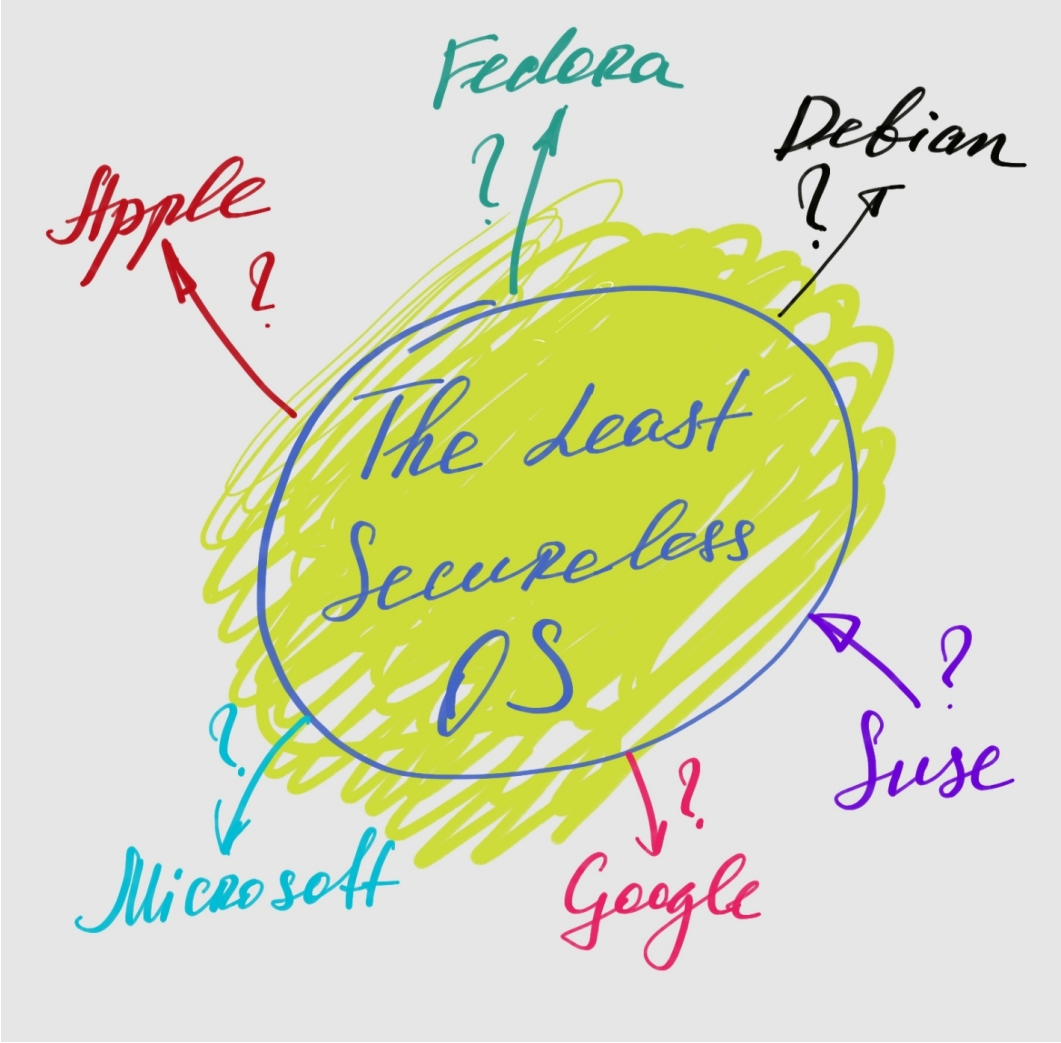
Наименее уязвимая ОС

(The Least Secureless OS)



В предыдущей статье мы рассмотрели уязвимости, обнаруженные в аппаратной части MacBook и других устройств Apple.

Если Вы захотите проверить эту информацию, можно, например, посмотреть в октябрьском номере журнала «Хакер» (№259) за 2020 год — статья «Взлом Apple T2». А также прочитать об этом в других изданиях и на англоязычных форумах по информационной безопасности.

В этой статье мы обсудим программную часть цифровых устройств, а именно — операционные системы (ОС).

Erroredemic. Заражение микросхем людскими ошибками

Мы уже давно научились делать качественное железо, но код всё-равно пишут люди. А людям всегда свойственно ошибаться. Поэтому мы будем исходить из того, что не бывает абсолютно безопасных операционных систем и программных продуктов.

Рейтинг уязвимости

Наталья Касперская на лекции в Вятском государственном университете (23 апреля 2019 г.) представила рейтинг уязвимостей от компании Positive Technologies.

Positive Technologies давно работает в сфере информационной безопасности, и мы склонны доверять её аналитическим материалам.

«Дивный новый мир: риски и возможности цифровой экономики» (https://youtu.be/9m0_G4nXeZg)

Слайд на временной отметке — 22:50 (мин:сек)

Существуют и другие рейтинги уязвимостей от различных компаний и ИБ-специалистов. Но общая картина распределения выглядит примерно одинаково.

Нам, к сожалению, не удалось найти первоисточник графика с этой картинки. Поэтому будем использовать этот слайд из видео.

Вот что нам удалось разглядеть на этом слайде. Мы специально подписали колонки более чётко. Возможно, что какие-то цифры и значения мы указали не совсем точно.

На графике видно, что в лидерах по уязвимости — Adobe, Microsoft и Google. Это сразу бросается в глаза.

Важно здесь отметить, что количество уязвимостей также напрямую связано с популярностью того или иного программного обеспечения. А также с масштабом экосистемы: чем больше программ завязано на определённого производителя, тем больше уязвимостей.

Для бóльшей наглядности мы выписали значения из графика в таблицу с сортировкой по убыванию. Цветом выделены строки, имеющие отношение к операционным системам:

1383	Adobe	
1325	Microsoft	
695	Google	
611	Apple	
596	Redhat	GNU/Linux
535	Novell	
≈300	Debian	GNU/Linux
280	Oracle	
278	Canonical	GNU/Linux
≈217	≈Linux	
205	Mozilla	
120	Fedoraproject	GNU/Linux
107	PHP	
95	≈Wireshark	
91	≈Qemu	
75	Phpmyadmin	
63	Suse	GNU/Linux

В хвосте списка оказались представители ОС из семейства GNU/Linux: **Debian**, **Canonical**, **Fedoraproject**, **Suse**.

Fedora — это ветка Linux-версии Red Hat, созданная для домашних пользователей.

Canonical — компания, создающая ОС Ubuntu. Ubuntu в свою очередь изначально основан на ОС Debian.

S.u.S.E (Gesellschaft für **S**oftware- **u**nd **S**ystem-**E**ntwicklung) — немецкая компания, выпускающая ОС OpenSUSE. OpenSUSE создана на базе дистрибутива Slackware, который некоторые фанаты называют «настоящим Linux».

Если Вы собираетесь заниматься чем-то серьёзным, переходите на Linux

Мы неоднократно слышали этот совет от разных людей, сведущих в информационной безопасности, но относились к нему скептически. Но когда уже сами столкнулись с проектами, где требовалось проявлять особое внимание к безопасности проектных данных, то в полной мере оценили на себе пользу и обоснованность этого совета.

В операционные системы семейства GNU/Linux изначально закладывался наиболее безопасный подход в функционировании всей ОС. Поэтому представителей семейства Linux всегда можно встретить в нижних строчках рейтингов уязвимостей.

Меньше уязвимостей – не значит безопасно

Чтобы взломать систему, уязвимости достаточно всего одной. И плюс несколько миллисекунд.

Конечно, 120 уязвимостей, это на порядок меньше, чем 1200. Но и удовлетворительным этот результат нельзя назвать. Поэтому в среде ИБ-специалистов говорят, что безопасность — это процесс. Процесс постоянного улучшения, безостановочное выявление и исправление уязвимостей.

==

В следующих своих статьях мы рассмотрим наиболее безопасную конфигурацию из нескольких операционных систем для выполнения различных задач.

Очевидно, что полностью перейти, к примеру, на Linux и отказаться от Windows, Google и прочего — невозможно.

У каждой операционной системы есть свои сильные и слабые стороны, а также своё соотношение критических и допустимых уязвимостей.