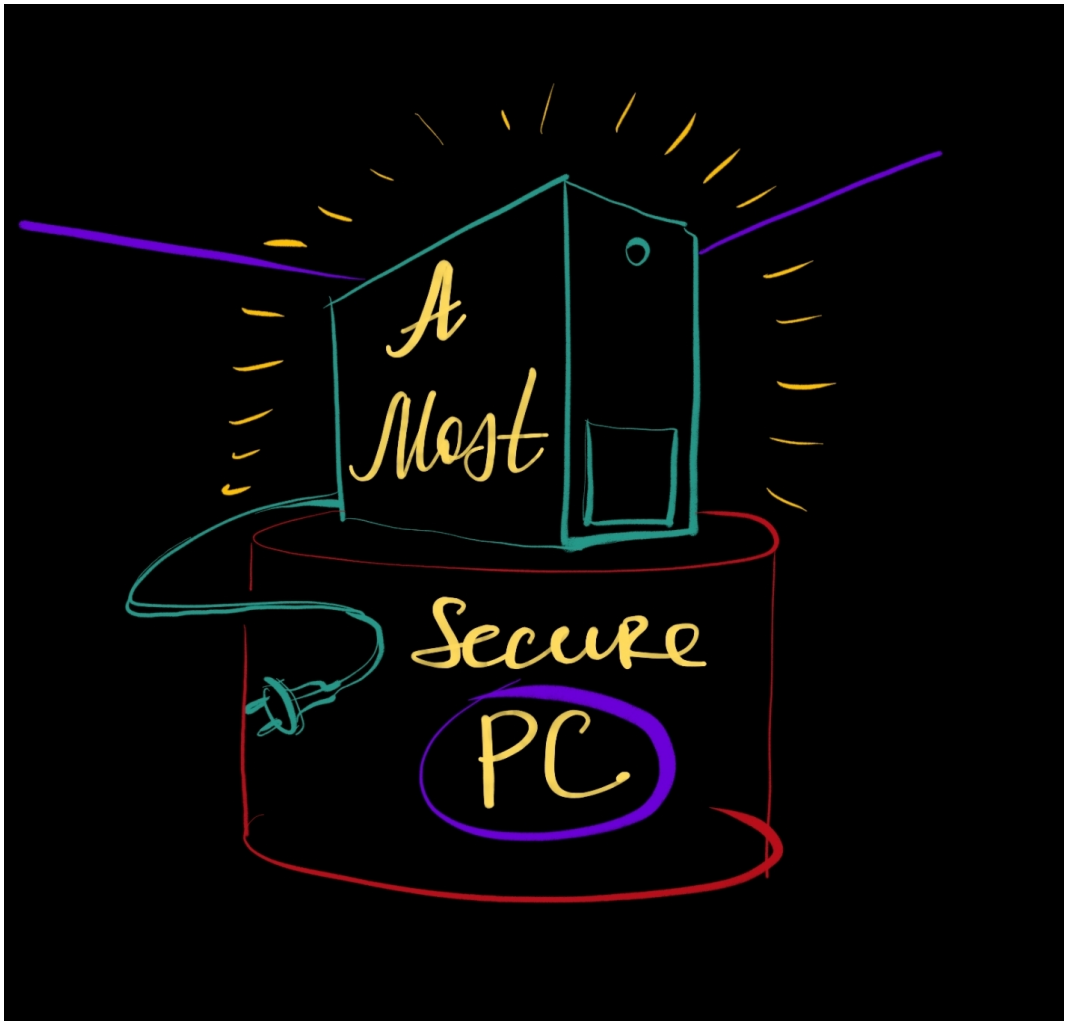
Самый безопасный компьютер

(A Most Secure Computer)



Единственный по-настоящему безопасный компьютер — это тот, который **выключен**, залит в **бетонный блок**, и помещен в герметичную **свинцовую комнату** под круглосуточной вооружённой **охраной** — но даже и в этом случае меня одолевают сомнения…

Так превосходно высказался ещё в 1989 году эксперт по интернет-безопасности Джен Спаффорд (Gene Spafford).

> *«The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards — and even then I have my doubt.»*

Безопасный компьютер не пьёт, не курит и не существует

Хотя высказывание от Джена Спаффорда и прозвучало более 30 лет назад, но до последнего времени оно воспринималась не более, чем шутка.

Наоборот считалось, что компьютеры, полностью изолированные от интернета и внутренних сетей, надёжно защищены и безопасны в использовании. И что информация на таких компьютерах абсолютно недоступна для посторонних.

По такому принципу во многих правительственных системах и коммерческих структурах хранятся секретные документы и разного рода информация с ограниченным уровнем доступа.

Но технологии не дремлют, они постоянно развиваются. И также постоянно развиваются *«технологии двойного использования»* новых технологий.

На протяжении последних лет исследователи по всему миру открывают новые способы получения данных даже с самых изолированных компьютеров.

Если работает, значит излучает информацию

Как можно получить данные с компьютера, который изолирован от всего? **Специалисты из израильского университета** имени Бен-Гуриона подошли к такой задаче творчески.

Исследователи рассуждали просто: если компьютер работает, значит он излучает электромагнитные волны. А раз это электромагнитные волны, то по ним можно передавать информацию.

Они взяли самый очевидный компонент, который есть в любом компьютере, — оперативную память (RAM — Random-Access Memory). И смогли превратить планку RAM в беспроводной излучатель для передачи данных «по воздуху» (атака AIR-FI).

Оказалось, что электромагнитные волны, которые генерирует RAM, такие же по частотам как и у Wi-Fi — 2,4 ГГц. И при определённой подготовке такой сигнал может принять любое устройство (от смартфона до умных часов), находящееся поблизости с изолированным компьютером.

При желании можно прочитать об этом подробнее: это исследование подробно описано в декабрьском номере журнала «Хакер» (№261, 2020 г.).

Ещё ранее учёные из того же Израиля обнаружили, что обычные сотовые телефоны могут получать от компьютеров двоичные данные. Подробнее об этом способе также можно найти в интернете.

А в 2013 г. Анг Цуй, студент из Колумбийского университета, смог снять подобный сигнал с «ножек»

микросхемы, с помощью которых крепятся к компьютеру. Цуй обнаружил, эти ножки могут колебаться уникальным образом, а значит передавать данные с помощью радиосигналов.

В радиотехнической разведке способны и на другие чудеса. Например, воспроизвести изображение на мониторе любого компьютера, воздействуя специальной антенной на крошечный источник электромагнитного излучения, находящейся внутри монитора. Метод называется — «телефонный хакинг Ван Эка».

Это потенциальное свойство всех цифровых устройств становиться антеннами назвали — **фантенна** (funtenna). Этот термин придумал Майкл Оссманн. Фантенна — это используемая злоумышленником антенна, которая не разрабатывалась в качестве таковой при создании системы.

Недостижимый идеал

Никто не может запретить мечтать о надёжном и безопасном компьютере. Ради достижения этого идеала компьютеры отключают от интернета, защищают данные стойким шифрованием, сворачивают внутреннюю сеть, создают уровни доступа и прочее, и прочее.

Но этот призрачный идеал всегда ускользает и порой вместе с важными данными…

Хорошо считает. Хорошо запоминает. Но ни черта не соображает.

На каком-то этапе развития компьютерных технологий всем нам казалось, что при определённых мерах безопасности компьютеру можно доверить хранение важной информации и выполнение ответственных задач.

Но компьютер лишь рычаг. Бессознательный инструмент, готовый выполнить задачу от любого, кто найдёт к нему правильный подход. Компьютер плохо определяет сигнал «свой — чужой», поэтому его легко обмануть.

Здесь важно понимать взаимосвязь между требованиями к безопасности и моделью угроз. Сложность мер безопасности зависит от того, кто заинтересуется данными на определённом компьютере.

Если пользователю нужен только поиск в интернете, то антивируса будет достаточно. Если пользователю предстоит работа над важным проектом, то нужно собирать конфигурацию из нескольких компьютеров, о которой мы поговорим в следующих статьях.

А если предстоит работа с секретными документами, то любые меры безопасности — это лишь вопрос оттягивания момента, когда эти данные будут похищены.

Потому что такой компьютер попадает в поле внимания — **target surveillance** (направленной слежки) — от которой практически нет способов защиты. И об этом будет тоже в следующих статьях…