Аналитическое чтение тезисов с пленарных заседаний ACM CCS'13-14

Дедков Сергей

2015

Содержание

1 The Science, Engineering and Business of Cyber Security

Неоднозначый статус кибербезопасности сохраняется уже на протяжении 30 лет. И на протяжении этих 30 лет нет однозначного ответа кому принедлежит этот аспект развития информационных технологий - Бизнесу, Инженерии или Науке. Вообще развитие компьютерной науки отличается от развития традиционных и технических наук. Компьютеры и интернет проникли во многие сферы деятельности человека, что представить мир без них достаточно сложно. И хотя так есть, интеренет зачастую не удовлетворяет соответствующим требованиям кибербезопасности и конфеденциальности на уровне потребительского рынка. Среднестатистический пользователь комфортно себя чувствует и на текущем уровне обеспечения безопасности, об этом говорит масштабное принятие интернет-услуг по всему миру. Каждый сам решает насколько защищать свое киберпространство.

Хотя уже сейчас многие начинают задумываться на кого должна быть положена ответственность обеспечения бузопасности в сети. Вполне возможно при объединении средств науки, бизнеса и инженеров получиться обеспечить безопасность в сети интернет. Министерство обороны США публично признает киберпространство на одном уровне с пространством суши, моря, воздуха и пространства, внутри которого войн будет проводиться и облегчается. Таким образом должна существовать общественная организация, которая контролировала бы вмешаетльство правительства и большого бизнеса в развитие безопасности. Но и правительства должны на должном уровне обеспечивать безопасность во избежании кибертерорризма и кибервойн.

2 Exciting Security Research Opportunity: Next-generation Internet

Текущее состояние безопасности сети интернет не соизмеримы с его значением, т.к. интернет пронизывает многие сферы жизнедеятельности человечества. Даже короткие перерывы в работе сети могут оказать глубокое негативное влияние на правительственные, экономические и социальные операции, не говоря уже о простоях в минуту, час, день или неделю. Патчи по улучшению безопасности зачастую ограничены архитектурой сети интернет, бизнес-моделями и правовыми аспектами. Существующие фундаментальные решения текущей сети интернет, котоые усложняют беопасную эксплуатацию.

Другая важная задача - аутентификация субъектов в глобальной среде. Для решения подобных задач изучается конструкция последующих поколений сети Интернет. Предлягается единый дизайн, обеспечивая

тем самым стимул для перезода на новую арзитектуру, учитывая политические и жкономические аспекты на этапе пректирования. После того как будет понятно какой должна быть безопасная архитектура сети Интернет можно будет реализовывать ее внедряя в текущую реализацию Интернет и изучая сратегии перехода к сети Интернет следующего поколения.

3 The Cyber Arms Race

Разработчики решений сети Интернет во время ее повсеместного развития проигнорировали важность безопасности информации. В связи с этим в Интернет расцвела свобода в неограниченном мире онлайн. Люди создавали контент в различных целях - общение, переписка, хранение материалов. И все это в глобальных масштабах. Тогда политики поняли как важна сеть Интернет для целей наблюдения. Интернет и телефоны изменили мир. И они позволили провительствам осуществлять наблюдения за гражданими, при этом не только своих стран.

Летом 2013 года Эдвард Сноуден опубликовал утечку информации прогарммы АНБ США PRISM. Конечно, правильно было бы использовать сети Интернет для поиска преступников, просматривая их трафик по постановленю суда, но в полномочия PRISM входил шпионаж и за обычными гражанами, которые не подозревались в преступности. Они создавали досье, на людей невиновных. Эти досье могли рассказть очень многое из жизни этих людей на основе их Интернет активности. Помимо граждан США АНБ могли контролировать иностранных граждан, которые пользовались сервисами США. Они аргементировали двумя моментами:

- Налюдение ведется только в целях предотвращения террористов
- Другие страны делают то же самое.

Однако, большенство сервисов и продукции связанной с Интернет постаялется из Америки. Американцы не пользуются внешними программами, а вот как раз другие страны используют сервисы США. Возникает вопрос - почему? Ответ очевиден - на практике сложно избежать использования таких услуг, как - Google, Facebook, LinkedIn, Dropbox, Amazon Skydrive, ICloud, Android, Windows, IOS. Даже если продукт произведен не в США в скором времени Американские компании скупают его, например, Skype.

Данная проблема вызывает противоположные точки зрения. Например, если вы ничего плохого не делаете, то вам и не зачем беспокоиться. С другой стороны вы и не должны быть обескоены, вы должны быть возмущены. Мы не должны просто принимать тот факт, то иностранная разведка следит за нами.

4 Выводы

По моему мнению, вопрос безопасности в сети Интернет должен быть вынесен на более качественный уровень. В целях построения безопасной архитектуры сети Интернет вместе должны объедениться наука, бизнес и инженеры. Помимо этого для действительно глобальной безопасности, а сеть Интернет - сеть охватывающая большинство стран мира и они должны объединить усилия в целях решения данной проблемы. Уже сейчас многие страны обеспокоены защитой информации в сети.

Следует так же избегать монополии в данном впоросе, как например происходит сейчас, когда большинство людей пользуются сервисами расположенными в США. Пример отрицательной стороны этого ворпоса - государственная программа США PRISM.