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

Мартынов Семён

14 февраля 2015 г.

В материале The Cyber Arms Race финский эксперт с 20-летним опытом Mikko Hypponen обращает внимание на то, что на заре своего бурного роста в начале 90-х интернет не был особо интересен властям, и там сформировались определённая культура свободы. Но со временем, политики отметили важность интернета, в том числе и в целях наблюдения за гражданами. Интернет и мобильные телефоны изменили мир, в то же время стали отличным оружием слежки. Утечка о программе PRISM Агентства Национальной Безопасности США, устроенная Эдвардом Сноуденом, стала темой номер 1 в прессе. Автор принимает необходимость проведения расследований и наблюдений в интернет-среде, когда речь идёт о торговле наркотиками, стрельбе в общественном месте или терроризме, но всё это не относится к программе PRISM. PRISM отслеживает действия любого человека, вне зависимости от того, подозревается ли он в чём-либо. Результатом становится досье, дающее точную картинку каждого из нас. И в каждом таком досье, можно найти что-то подозрительное или неприятное на каждого. Спецслужбы США имеют полное законное право наблюдать за иностранными гражданами. Но все мы являемся иностранцами, по отношению к США, таким образом мы являемся объектом слежки, когда пользуемся интернет-сервисами, расположенными в Америке. Когда начались первые утечки, Агентства Национальной Безопасности США постаралось успокоить общественность заявив, что программа только выискивает признаки террористов, но дальнейшие утечки обнаружили следы этой программы в Европейской Комиссии и ООН, что дискредитировало Американские власти. Другой аргумент Американцев состоит в том, что кибер шпионажем занимаются все. Это действительно так, но тут следует учесть масштабы: большинство крупнейших интернет-сервисов (поисковые сервера, почтовые сервисы, социальные сети, облачные провайдеры...) находится в США, так что наблюдение оказывается не симметричным. Обыватель мог бы задаться вопросом, стоит ли ему об этом беспокоиться, если он не совершает ничего противозаконного? Автор предлагает свой ответ на этот вопрос - мне нечего скрывать, в то же время я не имею желания делиться какой-либо информацией о себе с Агентством Национальной Безопасности США. А если подобное наблюдение действительно необходимо, пусть этим занимаются национальные власти, а не большой брат из США. И когда автор получает вопрос о том, стоит ли волноваться по этому поводу, он отве-

чает, что тут стоит не волноваться, а возмущаться. Нельзя допускать чтобы весь контроль за всем глобальным пространством осуществляла одна страна.

В материале The Science, Engineering and Business of Cyber Security автор Ravi Sandhu делится своим опытом и оптимистичным взглядом на кибер-безопасность. Он полагает, что потребительский рынок и общественные усилия приведут к относительно низкому уровню потребности в безопасности и приватности. Масштаб использования интернет-сервисов по всему миру является одним из индикаторов того, что средний потребитель чувствует себя довольно комфортно при нынешнем уровне рисков. В то же время, автор разделяет уверенность в том, что многие ведущие национальные агентства безопасности на полном серьёзе рассматривают угрозу интернет-войн и интернет-терроризма. Министерство обороны США официально признало киберпространство таким же полем боя как земля, море и воздух. Многие другие национальные военные министерства готовят наступательные и оборонительные кибервозможности.

В Швейцарском Институте информационной безопасности, Adrian Perrig озабочен тем, какую важную роль интернет играет в современных фундаментальных процессах. В своей работе Exciting Security Research Opportunity: Next-generation Internet он указывает на то, что эта важности никак не соотносится с тем уровнем безопасности и надёжности, который может предоставить интернет в его нынешнем виде. Проблема кроется в самой архитектуре, при его разработке закладывались другие условия безопасности, таким образом все заплатки, которые сейчас применяются для повышения безопасности упираются в ограничения архитектуры, бизнес-модели и юридические аспекты. В качестве примера он приводит проблему масштабирования сервисов авторизации. В данное время широко распространена модель PKI (Public Key Infrastructure), но она совершенно не масштабируема, т.к. один субъект не может доверять другому субъекту, если их ключи подписаны различными Удостоверяющими центрами. Решением этой проблемы автор видит интернет следующего поколения, где безопасность, высокая надёжность и приватность будут доступны на уровне дизайна. Изучив все потребности в интернете нового поколения, можно будет перейти к его включению в существующие сети, либо разработать план перехода.