ECP – СИСТЕМА РАСПРЕДЕЛЕННОГО ХРАНЕНИЯ СВОЙСТВ ИНФОРМАЦИИ

Малинецкая Е.Г., Татузов А.А.

Московский государственный университет им. М.ВЛомоносова
Факультет вычислительной математики и кибернетики
119991, Москва, ГСП-1, Ленинские горы, МГУ, д. 1, стр. 52, 2-й учебный корпус,
Тел.: (095) 939-30-10, факс: (095) 939-25-96,
E-mail: ilerna@yandex.ru

Работая и общаясь в сети Интернет, пользователь сталкивается со следующими проблемами: информация в Интернете теряется, информация в Интернете портится. ECP предлагает пользователю некоторое решение описанных выше проблем, дает возможность больше доверять информации, выложенной на незащищенных серверах. ECP предоставляет пользователю:

- Возможность хранения вместе с основной информацией *m* некоторого свойства этой информации *dm*. Свойство *dm* должно быть в определенный момент легко проверяемо, и потом сообщение *m* не должно утрачивать этого свойства по истечении длительного времени. В существующей реализации ECP мы рассматриваем свойства авторство сообщения и метка времени.
- Возможность проверки и доказательства любым пользователем сети, обладает ли сообщение *m* свойством *dm* вне зависимости от места хранения сообщения.

Данные возможности реализуются при помощи набора сервисов, в числе которых:

- Генератор – Интернет-сервис, который получает на вход сообщение *m* и *dm*, проверяет, обладает ли сообщение *m* свойством *dm*, и если да, то выдаст в качестве ответа на запрос подписанное сообщение *m*+ *dm*+*ac*, где *ac* последовательность проверки, необходимая для последующей проверки свойства *dm*.
- Сервис проверки, который получает на вход подписанное сообщение *m*+ *dm*+*ac* и выдает ответ – корректно ли данное сообщение. Сервис проверки должен выдавать ответ о том, что подписанное сообщение корректно, тогда и только тогда, когда оно было сгенерировано генератором.

При проектировании ECP мы хотели создать общедоступную, доказуемо стойкую в некоторых естественных предположениях систему.

Стойкость. Требования стойкости можно неформально выразить двумя условиями. Имея сообщение *m*+ *dm* трудно не используя генератор найти такую последовательность проверки *ac*, чтобы сервис проверки признал сообщение *m*+ *dm*+ *ac* корректным. Если подать на вход сервису проверки сообщение *m*+ *dm*+ *ac*, сгенерированное генератором, то сервис проверки всегда ответит, что *m*+ *dm*+ *ac* корректны.

Общедоступность подразумевает открытость алгоритмов работы системы и минимизацию усилий, требующихся от пользователя для использования ECP.