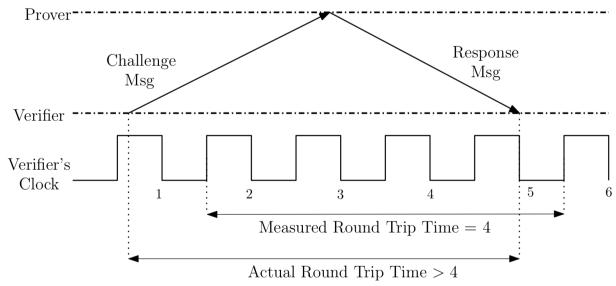
11
апреля
четверг

Коллоквиум факультета компьютерных наук НИУ ВШЭ

№80



Андрей Щедров

Пенсильванский университет / НИУ ВШЭ

Анализ кибер-физических протоколов безопасной передачи информации

Мы рассматриваем протоколы безопасной передачи информации, основанные на тех или иных предположениях о физических свойствах среды, в которой проводятся сессии протокола. Например, так называемые протоколы, ограничивающие расстояние (distance-bounding protocols), учитывают как точное время прохождения сообщений, так и скорость передачи, чтобы получить верхнюю оценку на расстояние между двумя участниками протокола.

Мы вводим общую вычислительную модель, основанную на логике переписывания, для формального анализа различных форм мошенничества на расстоянии, в том числе недавно обнаруженных атак на протоколы семейства Hancke-Kuhn. В рамках модели предлагается практический метод формального анализа, который призван помочь разработчикам систем преодолеть разрыв между концептуальными описаниями и низкоуровневыми конструкциями. Мы используем модель для определения новых стратегий атаки и количественных оценок их эффективности в реалистичных предположениях.

11 апреля, 18:10 – 19:30
Кочновский проезд, 3, ауд. 205

Регистрация:
https://cs.hse.ru/colloquium