Prof. Andre Scedrov (University of Pennsylvania, Philadelphia)

прочтет мини-курс из трёх лекций на тему

Анализ протоколов защиты информации

Лекции пройдут на факультете математики НИУ ВШЭ по адресу ул. Вавилова. д.7.

Расписание: 3.06, 18:30, ауд. 311; 4.06, 15:30, ауд. 317; 6.06, 15:30, ауд. 311

Для допуска в ВШЭ, пришлите заявку Д.С. Шамканову <daniyar.shamkanov@gmail.com>.

Analysis of Security Protocols

Protocols based on cryptographic primitives are commonly used to protect access to computer systems and to protect transactions over the internet. Relatively succinct but subtle protocols for authentication, key exchange, negotiation, authorization, and related tasks are the building blocks for secure distributed systems. Two well-known examples are the Kerberos authentication scheme, used to manage encrypted passwords on clusters of interconnected computers, and the Secure Sockets Layer, used by internet browsers and servers to carry out secure internet transactions.

Security protocol design and analysis is a difficult problem. Some of the difficulties come from subtleties of cryptographic primitives. Further difficulties arise because security protocols are required to work properly when multiple instances of the protocol are carried out in parallel, where a malicious intruder may combine data from separate sessions in order to confuse honest participants. Moreover, although the protocols themselves are often very simple, the security properties they are supposed to achieve are rather subtle and should be formulated with great care.

Many new protocols have been proposed and reviewed by Internet standards bodies in recent years, motivating substantial research efforts in networking, computer security, formal methods, and cryptographic communities. In this survey we will discuss foundations of protocol analysis as well as applications of analysis methods to selected protocols.