The 8th BIU Winter School on Cryptography

Secure Key Exchange

Location: Kfar Maccabiah Conference Center, Ramat Gan, Israel

School organizers: Yehuda Lindell and Benny Pinkas

Sunday, February 11, 2018	**Introduction**
Lecturer: Hugo Krawczyk	
8:15 am to 8:45 am	***Registration***
8:45 am to 9:00 am	Opening remarks
9:00 am to 10:00 am	What Are Key Exchange Protocols?
10:00 am to 10:15 am	*Coffee break*
10:15 am to 11:15 am	Overview of Security Definitions
11:15 am to 11:45 am	*Coffee break*
11:45 pm to 12:45 pm	Diffie-Hellman Protocols and Authenticators
12:45 pm to 2:15 pm	*Lunch*
2:15 pm to 3:15 pm	STS, SIGMA and IKE (IPsec's Key Exchange)
3:15 pm to 3:30 pm	*Coffee break*
3:30 pm to 4:30 pm	Implicitly Authenticated KEPs
4:30 pm to 5:00 pm	*Coffee break*
5:00 pm to 6:00 pm	More on Implicit Authentication; Key Derivation
7:00 pm	*Bus to Tel Aviv*

Monday, February 12, 2018	**Advanced Definitions and Proofs**
Lecturer: Marc Fischlin	
9:00 am to 10:00 am	Bellare-Rogaway-Security of Key Exchange (passive adversaries)
10:00 am to 10:15 am	*Coffee break*
10:15 am to 11:15 am	Bellare-Rogaway-Security of Key Exchange (active adversaries)
11:15 am to 11:45 am	*Coffee break*
11:45 pm to 12:45 pm	Forward Secrecy
12:45 pm to 2:15 pm	*Lunch*
2:15 pm to 3:15 pm	TLS 1.3 and other protocols

3:15 pm to 3:30 pm	*Coffee break*
3:30 pm to 4:30 pm	Zero Round-Trip Time (0-RTT)
4:30 pm to 5:00 pm	*Coffee break*
5:00 pm to 6:00 pm	Universally Composable Key Exchange
7:00 pm	*Bus to Tel Aviv*

Tuesday, February 13, 2018 **Password-Based Key Exchange**	
Lecturer: David Pointcheval	
9:00 am to 10:30 am	Hash Proof Systems
10:30 am to 10:45 am	*Coffee break*
10:45 am to 11:45 am	Definitions and Models for Password-Authenticated Key Exchange
11:45 am to 12:00 pm	*Coffee break*
12:00 pm to 1:30 pm	Constructions of Password-Authenticated Key Exchange from Hash Proof Systems
1:30 pm	*Excursion*

Wednesday February 14, 2018 **Attacks and Automated Tools**	
Lecturer: Karthik Bhargavan	
9:00 am to 10:00 am	Man-in-the-Middle Attacks on Authenticated Key Exchange
10:00 am to 10:15 am	*Coffee break*
10:15 am to 11:15 am	Downgrade Attacks on Agile Real-World Protocols
11:15 am to 11:45 am	*Coffee break*
11:45 pm to 12:45 pm	Automated Symbolic Protocol Verification
12:45 pm to 2:15 pm	*Lunch*
2:15 pm to 3:15 pm	Mechanized Computational Protocol Proofs
3:15 pm to 3:30 pm	*Coffee break*
3:30 pm to 4:30 pm	Verified Cryptographic Libraries
4:30 pm to 5:00 pm	*Coffee break*
5:00 pm to 6:00 pm	Verified Cryptographic Protocol Implementations
7:00 pm	*Bus to Tel Aviv*

Thursday, February 15, 2018 **TLS and Secure Channels: Definitions and Attacks**	
Lecturer: Kenny Paterson	
9:00 am to 10:00 am	Overview of the TLS Handshake
10:00 am to 10:15 am	*Coffee break*
10:15 am to 11:15 am	Vulnerabilities in the TLS Handshake
11:15 am to 11:45 am	*Coffee break*
11:45 pm to 12:45 pm	From Key Exchange to Secure Channels
12:45 pm to 2:15 pm	*Lunch*
2:15 pm to 3:15 pm	Security Proofs for Fragments of TLS
3:15 pm to 3:30 pm	*Coffee break*
3:30 pm to 4:30 pm	Security Issues in Real-World Secure Channels
4:30 pm to 5:00 pm	*Coffee break*
5:00 pm to 6:00 pm	Modelling Secure Channels
6:00 pm	*Farewell*

This winter school is graciously sponsored by the European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013) / ERC Grant Agreement n. 615172 (HIPS), the BIU Center for Research in Applied Cryptography and Cyber Security in conjunction with the Israel National Cyber Bureau in the Prime Minster's Office, and Bar-Ilan University.

Prime Minister's Office
National Cyber Bureau

erc

Tradition of Excellence
Bar-Ilan University