Information Security Conference (ISC 2015) Travel Report

Tetiana Yarygina
Department of Informatics
University of Bergen
Norway
tetiana.yarygina@ii.uib.no

September 24, 2015

Abstract

This report reflects on the presentations given during ISC 2015 with an emphasis on the topics of my personal interest. Attendance of the even was funded by COINS Research School.

1 ISC

The Information Security Conference (ISC) is an annual international conference dedicated to research on the theory and applications of information security. ISC 2015, the 18th in the series, was held in Trondheim, Norway, September 9-11, 2015. The event was organized by the Department of Telematics at the Norwegian University of Science and Technology (NTNU) in Trondheim.

The conference focus is on novel theoretical and practical results in access control, applied cryptography, authentication, biometrics, computer forensics, cryptographic protocols, digital right management, electronic frauds, embedded security, identity management, network security, privacy, security for Internet of Things, secure cloud computing, and others.

2 Featured papers

I was particularly interested in the following sections and papers:

- System and software security
  - Dynamically Provisioning Isolation in Hierarchical Architectures
  - Factors Impacting the Effort Required to Fix Security Vulnerabilities
  - Software Security Maturity in Public Organisations

- Cryptography II: Protocols
  - Oblivious PAKE: Efficient Handling of Password Trials
  - On the Efficiency of Multi-Party Contract Signing Protocols
  - On the Provable Security of the Dragonfly Protocol
- Network and cloud security
  - Multipath TCP IDS Evasion and Mitigation
  - Provenance based Classication Access Policy System based on Encrypted Search for Cloud Data Storage
  - Multi-User Searchable Encryption in the Cloud

The paper "Oblivious PAKE: Efficient Handling of Password Trials" introduces Oblivious Password based Authenticated Key Exchange (O-PAKE) and shows how ordinary PAKE protocols can be efficiently transformed into O-PAKE. O-PAKE allows a client that holds multiple passwords and is registered with one of them at some server to use any subset of the client's passwords in a PAKE session with that server. The term oblivious is used to emphasise that the only information leaked to the server is whether the one password used on the server side matches any of the passwords input by the client. The main drawback of this scheme discussed after the presentation is that overall security is limited by the weakest password in the set.

The existing network security infrastructure is not ready for future protocols such as Multipath TCP (MPTCP). The outcome is that middleboxes are configured to block such protocols. The paper "Multipath TCP IDS Evasion and Mitigation" studies the security risk that arises if future protocols are used over unaware infrastructures. In particular, the practicality and severity of cross-path fragmentation attacks utilizing MPTCP against the signature-matching capability of the Snort intrusion detection system (IDS) is investigated. Results reveal that the attack is realistic and opens the possibility to evade any signature-based IDS. To mitigate the attack, a solution is also proposed in the form of the MPTCP Linker tool. The work outlines the importance of MPTCP support in future network security middleboxes.

While Searchable Encryption (SE) has been widely studied, adapting it to the multi-user setting whereby many users can upload secret files and delegate search operations to some other users still remains an open problem. The paper "Multi-User Searchable Encryption in the Cloud" shows that the adversarial models used in existing multi-user searchable encryption solutions are not realistic as they implicitly require that the cloud service provider cannot collude with some users. The authors propose a stronger adversarial model, which is both practical and provably secure. The new solution combines the use of bilinear pairings with private information retrieval and introduces a new, non trusted entity called "proxy" to transform each user's search query into one instance per targeted file. As it was discussed after the presentation, this scheme involves one more party and, therefor, makes the system even more complicated and in some sense more fragile. The approach is definitely innovative.

3 Overall impression and other remarks

My main reason for attending this conference is personal interest in the above mentioned topics. I had a lot of useful discussions with other participants about web authentication and variations of PAKE, multipath TCP, and techniques for searchable encryption. After the conference in more relaxed setting homomorphic encryption and Bitcoin protocol were discussed.

The conference was well organized. All the scheduled activities were perfectly timed. Several presentations were held remotely over Skype, which was an interesting experience. Best paper and best student paper awards were presented.