A summary of COINS Summer School on Authentication

by PhD Candidate Andrii Shalaginov
andrii.shalaginov@ntnu.no
Norwegian University of Science and Technology

August 31, 2016

Abstract

This report reflects a content of a COINS summer school that happen in August 2016 with s special focus on Authentication. In this work author also touches eID, mobile networks and network forensics. Below the summery of every day is given together with a defined questions related to the presentations.

Keywords: Authentication, Network Security, Network Forensics, Mobile Networks

1 Monday 01/8 Teaching

On the first day of school Mike Just discussed aspects of Human-Computer Interaction with corresponding security-related issues. Mike talked about causes of most probable causes of security failures such that attackers, system complexity causing likelihood of vulnerabilities and human factor like mistakes, etc. Another part of the lecture was devoted to password authentication. We learned about interaction patters such that screen or submission point, feedback or Validation point and feedback atomicity. In addition to this Mike described so-called partial password that are used by various organizations to authenticate without revealing complete passwords in one step.

In the second part of the day Herbert Leitold gave a very good and wide overview of the electronic initiatives (eID) that have been happening over Europe starting from 1999. He pointed out a need for a secure and reliable federation of eID that can be used across European nations and eliminated identity theft. Herbert discussed differences of various eID used by different governments such that nPA in Germany, Austria, Estonia, etc. These identity cars appeared in corresponding nations in early 2000th. Finally, it was mentioned SSO (Single Sign On) authentication method that has been widely used in many services considering development and spread of social network platforms. SSO allows customers to use a single set of credentials (e.g. Facebook) to access different services and on-line resources.

2 Tuesday 02/8 Teaching

In the beginning of the second day Ravi Borgaonkar made an overview of the authentication in 1G 4G mobile networks. Also we touched the case of IMSE catchers that were observed in Oslo during December 2014 causing big scandals because of hidden mobile surveillance. Also he mentioned so-called Silent SMS, a method used by law enforcement agencies to track location of a mobile phone. Such SMS does not trigger any system actives and does not show on the screen. Later, Herbert Leitold continued a lecture on eID. We learned more precisely about eIDAS[1], EU regulation on electronic identification and trust services for electronic transactions. It came into power in July 2014 for more secure internal market transactions. Then, Herbert described OAuth2 (open standard for authorization)[2] and SAML (security assertion markup language)[3]. The standard and data format are used to log in into the third-parties services using Identity Provided such that Facebook or Google. Also Herbert described STORK 2.0[4], a project aimed on making European eID platform that make easier and safer transactions and cooperation across countries in EU. Further, we discovered so-called eHealth and eJustice that used to enhance existing system together with electronic means with a special focus on data and privacy protection.

3 Tuesday 04/8 Teaching

On the 3rd day Ravi Borgaonkar continued with mobile network authentication aspects. We learned more specifically GSM network components starting from end-user terminals, base stations and ending with data networks. Ravi showed multiple aspects of 3G and 4G networks that are currently deployed by majority of mobile operators. He also presented a phone authentication in UMTS architecture and how new call is established. It was interesting to listed about the triangulation method to track a person using a signal from his phone delivered to radio access network nodes. After break, we learned about A5 algorithm, a stream cipher used from end of 1980th for over-the-air communication in GSM networks. he stated that UMTS and LTE has a vulnerability in authentication and key agreement protocols. The lecture was concluded with a state of the art in 5G networks, which can offer up to 10Gbps data transfer speed by 2020.

4 Friday 05/8 Teaching

On the last day of the Summer School Yong Guan made an overview of Network Forensics state of the art and human-centred security. In the first part of the lecture, we had a Q&A session on Digital Forensics and corresponding challenges. Yong presented several forensics-related organizations such that NW3C (National White Collar Crime Center)[5] IACIS (International Association of Computer Investigative Specialists)[6]. Many of us learned about ”Locard's exchange principle” (an assumption that a perpetrator anyhow leaves traces of himself on a crime scene as well as takes something from it), Hans Gross (who is a creator of a field of Criminalistics) and Alec Jeffreys (developed DNA profiling method). In addition to this we touched a set of rare file types that can be analysed by a Computer Forensics analyst such that .mpnt (Mac Paint Image) and .odg (OpenDocument Graphi), which can be used to conceal information inside it. Yong als talked on how an identity can be hidden in the Internet. He mentioned a famous work by David Chaum on untraceable electronic mail back in 1981 that proposed a scheme for anonymization in email system. In addition, Dining Cryptographers Network was described that used to preserve the privacy of the participants without revealing their identities. A the end SilkRoad 2.0 was mentioned as an online resource on darknet market.

[1] https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

[2] https://oauth.net/2/

[3] http://saml.xml.org/

[4] https://www.eid-stork.eu/

[5] https://www.nw3c.org/

[6] http://www.iacis.com/