Vasileios Gkioulos
IMT 6003
30/7/2016 to 6/8/2016

COINS summer school 2016, reflection report

Session 1: Mike Just, Heriot-Watt University, Edinburgh, UK: Usable security and authentication.

Professor Just initiated this session by presenting his earlier work and Heriot-Watt University/ Computer Science department. He proceeded presenting the field of Human-Computer Interaction arguing in respect to its necessity towards secure and usable applications, services and products. The main arguments were based on the need of analyzing human behavior and psychology when interacting with secure systems, in order to enhance the security design process and bypass intentional or unintentional harmful user behavior. As he mentioned:

> *"It is crucial for the efficient deployment of secure systems to understand the tricky balance between security and human behavior. Especially since users tend to perceive security as a secondary (If at all) task"*

The common status of security implementations was consequently discussed. In this section Professor Just highlighted the main elements that impede the enforcement of current security solutions, focusing in two specific elements, namely:

1- Usability of security solutions and the lack of user understanding over their necessity, since they tend to function as obstacles towards the achievement of a primary goal.
2- Complexity of current security implementations, with an abstract understanding of their benefits.

Following this analysis Professor Just presented a robust definition of Human Computer Interaction as:

"Human-computer interaction is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them. [ACM]"

and highlighted historical facts and fundamental aspects of the field.

The main focus of this session was on the analysis of developed models and design rules over the field of human computer interaction aiming at the aforementioned goals. The discussed models included Shneiderman's 8 Golden Rules (1987), Norman's 7 Principles (1988) and Nielsen's 10 Usability Heuristics (1994), highlighting seven usability principles with significant impact over security implementations, namely:

1. Enable (frequent) users to use shortcuts
2.Offer informative feedback
3. Help users recognize, diagnose and recover from errors
4. Permit easy reversal of actions
5. Allow users to minimize memory load
6. Make things visible
7. Offer help and documentation

These principles were analyzed in respect to their benefits over system evaluation during the design, use and after-use phases, while suitable methodologies were discussed. The presented techniques were consequently applied to established authentication techniques and applications such as fingerprints, facial scan, web security, file security and retina scan.

The second part of Professors Just lecture focused on password authentication. Various aspect of the domain were discusses both in theoretical and practical approach, including analysis of real life implementations, possible attacks and usability analysis. The main focus was on the usability analysis which included aspects in respect to human cognition, memory and behavior. Finally, research developed state of the art and best practices in respect to password authentication systems were presented and widely discussed. The discussion based on the lecture of Professor Just also focused on secondary and partial passwords as well as dual credential authentication. Finally, a developed mechanism for data driven authentication with use of mobile sensors was thoroughly presented, providing an opportunity for discussion over the applicability of the presented usability theory over real life applications.

Summary of questions asked
Question 1: What is your opinion in respect to Facebook connect, In terms of usability and credential delegation?
-It provides an easy way of authentication but users are commonly unaware of the risks as well as the privileges they delegate.
Question 2: What is the final practical use of the study?
-It aims at providing a data based authentication of mobile users, so device authentication requests are minimized.
Question 3: But it allows some error margin and a period of time that the machine can be exploited.
-Indeed, but the purpose of this approach is to increase security for the majority of users who prefer to not use authentication.

Session 2: Herbert Leitold, A-SIT, Austria: Federated identity management, STORK, eIDAS

The main focus of this lecture was on federated identity management and cross border authentication, within the scope of the STORK/ eIDAS projects. The presentation was initiated by Mr Leitold by highlighting the motivation and the necessity for the development of such systems. Early implementations of electronic identification systems were at a national level, with significant heterogeneity, which impedes their cross border interoperability. These notions were presented and analyzed, providing an understanding over the requirements and constraints of such systems. Following this short introduction over the topic, the presentation proceeded with the analysis of some national case studies from Austria, Estonia, Germany, Norway and UK. The focus was on technologies but also usage statistics, while commonalities and divergences were presented and discussed among the attendees.

The clarification of some fundamental terminology allowed the continuation of the presentation into more system-specific aspects, clarifying elements such as digital identity and its characteristics. This allowed the participants to identify discrete identity types and uses, but also to recognize their uses across various authentication mechanisms according to possible identification means such as appearance, social behavior, tokens or natural physiography. Consequently, the discussion focused on methods and technologies related to the attainment of identification, authentication and authorization.

The available means (Such as appearance, name, bio-dynamics) have been identified and discussed, in respect to their characteristics but also suitability. Identity management and identity lifecycle have been identified as critical parameter of the system, and as so were analyzed regarding the credential creation, usage, governance and maintenance. The presentation also focused on the security threats and challenges related to identity management, such as identity theft, manipulation, trust and disclosure. This topic was discussed vividly in respect to attainment of privacy and data control, while maintaining interoperability across platforms.

The presentation proceeded by the analysis of existing architectures, protocols, systems and system components. The main focus was on STORK, STORK 2.0 and eIDAS. The systems have been thoroughly presented, including analysis of stakeholders, pilot implementations as well as the main program milestones and outcomes.

Summary of questions asked

Question 1: Did the projects analyzed the feasibility of implementing existing policy reconciliation solutions, for resolution of the interoperability problem?

-At that stage we resolved the issue with the incorporation of an overlay mechanism, as an additional layer on top of the cooperating systems.

Session 3 – Ravi Borgaonkar: Authentication and related threats in 2G/3G/4G networks

Dr Ravi Borgaonkar's presentation focused on cellular communication security. The initial topic was a thorough analysis of the characteristics of the SIM (Subscriber

Identity Module), referring both to hardware design, functionalities, architecture and stored/handled data. Concurrently, existing attacks against the SIM have been presented and analyzed. These include:

1. SIM cloning
2. SIM toolkit attacks
3. Cracking SIM update keys

The presentation proceeded with an in depth analysis of the architectures, of cellular communication systems. Following their development from 2G (GSM) to 3G (UMTS) and finally 4G (LTE). The main components of each system have been presented and analyzed, including their functionalities and cooperative operation. This section was followed by a thorough analysis of known security vulnerabilities of these systems. The discussed topics included:

1. GSM
    a. Lack of mutual authentication
    b. Unencrypted transmission of IMSI
    c. Possible unencrypted transmission of IMEI
    d. Encryption mechanisms are only employed within a part of the wireless channel (Up to the BS)
2. UMTS
    a. Unencrypted transmission of IMSI
    b. Possible unencrypted transmission of IMEI
    c. Lack of end to end encryption
    d. Privacy vulnerabilities

The introduction of earlier technologies was followed by a thorough presentation of LTE and LTE-advanced networks. The requirements that led to the development of these systems, were primarily the need for higher data rates and improved QoS, but also significant effort was required for the enhancement of the security solutions. The architecture and security features have analyzed in depth, including the new network components and security related processes (e.g. key exchange, encryption algorithms)

A significant element of this presentation was the reference and analysis of the security evolution, regarding the implemented solution in conjunction with the identified threats. The main focus of the parallel discussion was the enforcement of authentication, availability, confidentiality and data integrity, along with system weaknesses that allow denial of service attacks and data interception. A variety of practical and low cost attacks have been presented, while some were demonstrated with the use of suitable equipment.

This session concluded with a discussion in respect to the current development of fifth generation, cellular communication systems. The required security features have been presented, along with the ongoing design processes and requirements.

Summary of questions asked

Question 1: Is it correct to claim that the development of early systems had as a primary goal the provisioning of services, while security (although a concern) has not been prioritized?

-Indeed in early systems security has been a requirement. Yet, given the capabilities of technology and the expected threat model, the main focus has been on quality of service.

Session 4 - Yong Guan, Iowa State University, USA: Network Forensics – Challenges and Open Problems.

Professor Guan initiated this session by presenting Iowa State University and the Center for Statistics and Applications in Forensics evidence. Through the first section of his presentation professor Guan analyzed the motivation, challenges and requirements for research over the field of forensics and cybercrime analysis/prevention, since as he mentioned:

“Cyber-criminal activity is growing, not steadily but exponentially,
both in frequency and complexity”

Consequently, the presentation proceeded with an overview of digital forensics, focusing on the characteristics of cyber-crime and how forensics can be utilized in order to prevent, impede and analyze such events. These elements where further discussed according to a given use case scenario, focusing on the specifics of IP trace-back, such as current solutions and methodologies.

One of the main focus of this presentation was the use of modern forensics within the field of cryptocurrency. Recent BitCoin events have been presented and analyzed, focusing on the history, structure and processes involved within such systems. Finally, the presentation concluded with a discussion over the topic of accountable anonymity and how it can be preserved while enforcing non-repudiation.