Metochi Summer School 2016

Herman Galteland

Metochi is an annex to the monastery Limonos, which is located on the island called Lesvos, Greece. Metochi is rented by the University of Agder and has been a study center since 1993. COINS rented the study center from the university for a week to hold a summer school for the PhD students. The topic was "Authentication". Here is a summary of the lectures given.

Human-Computer Interaction Security (by Mike Just) What is a well-designed login interface? How could password restrictions influence the password strength? And how can our behavior be used for authentication? These are some topics which is covered in the study of Human-Computer Interaction (HCI) Security.

In HCI we want to understand the human factors of security and how to reduce security failures caused by us. The study uses; critical analysis, gathering and understanding context, designing new security techniques, and evaluate proposed techniques. Where these methods are used to analyze (for example); biometric authentication (i.e., fingerprints), file encryption, and web security.

Password strength is based on its length and to influence the users to pick better passwords we can use some different requirements or methods. Usually websites give some requirements which give incentive to use short and hard to remember password. Instead we could influence the user by suggesting a better password by inserting or swapping characters. We could also use "random password" where the website will gradually increase the length of the password by adding random characters and aid the user to remember them.

Federation Identity Management, STORK, eIDAS (by Herbert Leitold) Electronic identification (eID) is used for online authentication when accessing services provided by the government, banks or other companies – even for cross-border authentication. Types of eID include; smartcards, mobile eID, soft certificate, and username and password.

For cross-border authentication, when a citizen of country A tries to use the services provided by country B, we can use the STORK or eIDAS protocols. When accessing the service of B, the user will be asked to authenticate

using his eID from his country, A. The system used by country A and B may not be the same, hence country B need to send the authentication request to A to be processed. The request will then be sent through a chain of trusted servers that use a common protocol, which will end up at country A's authentication servers. The user can then be authenticated and given access to the services provided by country B.

Authentication and Related Threats on 2G/3G/4G Networks (by Ravishankar Borganonkar) To start a phone call, the mobile devise will first contact a basestation in order to authenticate itself and show that the user is a paying customer that wishes to make a phone call. The basestation itself will not process the authentication, instead it will send it through the core network to the home location registry (HLR).

Looking at the security history of the authentication protocols, we have that; *1G* offer no authentication and no security, *2G* offer no mutual authentication (only the mobile will authenticate itself), *3G* offer mutual authentication and integrity protection, and *4G* offer mutual authentication and deeper mandatory integrity protection. Even though the security has increased, there is still some issues. When receiving a call, the basestation will not authenticate itself to the receiver. Also, the basestation has the option of using a older, less secure, protocol and the user can not control this.

Network Forensics (by Yung Guan) The methodical approach to apprehend criminals by studying a crime scene started with Hans Gross and Criminalistics in 1891. Ever since, the study has been further developed and in since the late 1970's has included digital forensics. Where network forensics, which is a subbranch of digital forensics, investigates and gather information about network traffic.

To find the origin of some criminal activity on the network, an investigator can look at the information stored at different routers and compare timing and packet size to deduce where it came from, which might lead to the criminal. Similarly, when an investigator wishes to know the parties in a BitCoin transaction, or some other cryptocurrency, we would need an graph of the user's addresses. By gathering addresses and generating a graph the investigator can then observe the network and search through the graph to find the possible participants of an transaction.

An example of future direction within network forensics is to develop an accountable anonymity system. It is a concept where the system gives the user full anonymity under normal circumstances and has a failsafe if someone misuses the system. That is, if a user uses the system for a criminal activity, the system has means to deanonymize the criminal. As an additional requirement, no one should be able to impersonate and misuse an honest user's account.