COINS: CySeP 2015 Report

B. Hale

Located just north of the center of Stockholm, the Kista KTH campus offered a central location for CySeP '15. While there were many excellent talks during CySeP, for conciseness only a few talk highlights from each day are presented in the following overview. Consequently, this is not an exhaustive summary and will certainly not address many interesting items of topic from CySeP, especially those talks with detailed technical content for the sake of conciseness. However, it underscores the value of CySeP in disseminating information and generating discussion related to cyber security and privacy in the modern and future world.

Day 1.
In his talk *Towards Privacy, Security* & *Trust in Cyberspace: Challenges and Solutions*, Jovan Golic discussed the distinction between cyber surveillance and cyber security – considering both necessary law enforcement and the threat to cyber security presented by uncontrolled surveillance. Essentially, the talk focused on issues of data privacy.

Day 2.
Day 2 of CySeP started with Eugene Spafford's talk on trust in security, *Truth and Consequences*. Fundamentally, this talk targeted the often-accepted phrase "no security in obscurity" under the argument that not only is obscurity necessary to some minimal degree for security (in the context of private keys, etc.), but obscurity in the form of active deception (obfuscation of true facts) has the potential to greatly enhance the security of a given system. Deception ultimately undermines trust – if we manage to undermine the trust of an attacker in the value of information they have obtained, we will weaken the power and potentially the success of such an attack. Examples of deception-for-security that were discussed include honey-trap stored passwords – which could allow for detection and possible response if an attacker attempts to use a stored fake password – and fake patches. Basically, the idea behind fake patches is that, in addition to a real patch, elements are put in place to fool an attacker into believing that the patch was not made, allowing for potential monitoring, tracking, identification, or other counter-responses against an attacker. Ultimately, knowledge of even the possibility of adoption of such systems undermines an attacker's trust in the success of an attack. Thus, modeling adversarial behavior, predicting it, and responding to it in an *obfuscated* way can increase the security of a system.

Jan Camenisch focused on means of achieving anonymity in his talk *Cryptography for People*. Particularly, he cross-compared the privacy concerns of x509 certificates, Open ID, and the Identity Mixer (developed at IBM Research, Switzerland). Unlike the other cases, the Identity Mixer method does not send actual credentials for verification, instead transforming the original certificate into a new one that is only used to verify essential information for the particular use-case.

Day 3.

During the third day of the summer school, Stephen Lechner from the Institute for the Protection and the Security of the Citizen, JRC, discussed the current status on the development of quantum computers and the issues in quantum-safe cryptography. With the European Commission backing quantum-safe methods as the future of cryptography, Lechner argued that the demand on this subfield is growing. After giving an overview of quantum computation (e.g. with qubits) and Shor's algorithm, Lechner outlined the quantum key distribution (QKD) performance and distance achieved to date, suggesting that actual realization is far from maturity. Current problems listed include the risk of protocol flaws, the sub-optimal effort vs. pay-off balance, and the lack of a quantum repeater (which implies that physical security of nodes is an absolute necessity).

Nasir Memon of the NYU Polytechnic School of Engineering gave an intriguing talk on media forensics – finding, organizing, searching, and attributing evidence in the digital age. In particular, Memon focused on the carving of fragmented files and image attribution, describing how PRNU (photo response non-uniformity noise) Based Sensor Fingerprints allow for the matching of images to the devices they were taken on (or other images taken on it), with high probability. Noise fingerprints can be used to successfully match a device to the corresponding image even if the image is seam-carved, as long as a 100x100 pixel area is untouched. For faster forensic analysis, the fingerprints of noise patterns can be combined, allowing for group-testing against a match within the group, thus easing the labor of image-by-image analysis.

Day 4.

Allison Mankin of Verisign Labs spoke on DNS privacy during Day 4 of the winter school. During her talk, Mankin gave an overview the DNS query paths, describing weaknesses and attack points for privacy compromise. Among the issues described, it was noted that 35% of server have only one client, while a full 75% of servers have 17 clients or fewer. Consequently, there can be little or no anonymity from a malicious server in the majority of cases. In order to gain privacy traction for DNS, several options were outlined, including DNS over TLS, qname-minimization, and DNSSEC, as well as several other more focused solutions for increasing privacy in DNS. DNS over TLS was a particular point as the method is nearing standardization, and the importance and process of standardization was a running theme throughout the presentation. It was noted that DNS queries through Tor is a research concept currently in exploration.

David Chaum finished the winter school talks with a discussion on random sample elections, drawing inspiration from the ancient Greek Kleroterion. In the context of modern society, Chaum argued that there is an increasing demand for government transparency as well as an increasing expectation by people of their own influence on government and law. It is with the need for encouraging and growing modern democracies that Chaum motivated Kleroterion 2.0.