NordSec/CySeP 2015 Travel Report for COINS

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

1 Introduction

In October 2015 Stockholm has hosted three great IT security events in a row: COINS PhD student seminar, NordSec conference and CySeP winter school. COINS Research School of Computer and Information Security supported PhD students' participation in all these events.

The 20th Nordic Conference on Secure IT Systems (NordSec) was held at KTH Royal Institute of Technology, October 19-21. The conference addressed a broad range of topics within IT security with the aims of bringing together computer security researchers and encouraging interaction between academia and industry.

Cybersecurity and Privacy (CySeP) Winter School was held on October 20-23 at Kista KTH campus located northwest of Stockholm. The school was practically oriented and elaborated on the transition from research and teaching to solving real-world problems.

For conciseness the report highlights only several topics of the author's personal interest raised during these two events and leaves the comprehensive description and technical details out of scope. The report also covers organisation aspects of the events which can be of use for future reference.

2 NordSec keynote "Rethinking Cyber Security" by Eugene H. Spafford from Purdue University

The main ideas of this great visioning talk are:

- One size does not fit all
- Quality must be prioritized
- If you do not know what you are building, you are stuck with what you build
- Security must be designed in; adding it afterwards results in gaps

More detailed description of the main points follows.

Absolute security is unattainable and it always depends on context and available resources. The speaker referred to Robert Courtney's three laws:

- Nothing useful can be said about the security of a mechanism except in the context of a specific application and environment.
- Never spend more mitigating a risk than tolerating it will cost you.
- There are management solutions to technical problems but no technical solutions to management problems.

A problem of software design. Initial research in the 1970s and 1980s looked at system state. There is a set of states that are known to be allowed or safe. As a system executes, it changes state. Each valid operation results in a state of the system that is also defined as allowed. We also have "bad" states which we neither want to enter or to remain in.

The notion of allowed states is a match to the concept of system specification in software engineering. Execution of a state not in the specification is a "fault" that can result in a "failure". A failure in a protected system is a security failure.

We also have undefined states that are not documented. Entering undefined states is an error which may or may not lead to a fault. Undefined states are not necessary "bad" states since they might even lead back to allowed states, but we do not know that.

Most software today operates in the undefined state space because we have never defined its proper behavior. We have general requirements, but no specifications. Formal specifications are time-consuming and expensive. They also require expertise to define, and to build software to match. "A program that has not been specified cannot be incorrect; it can only be surprising."[1]

The speaker also mentioned bad feedback loop of increasing software and hardware complexity as well as open source issues.

Cyber security is the science and practice of protecting information and information processing components from misuse during their design, creation, transmission, storage, transformation, use, and disposal. Information assurance is the science and practice of increasing our confidence (trust) in the information security of a system.

Measuring security. Lord Kelvin (William Thompson) wrote: "When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is a meager and unsatisfactory kind; it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science".

The traditional view of security as a Confidentiality-Integrity-Availability triangle is not a proper model according to the speaker. The measures are not orthogonal: integrity overlaps availability, availability trumps confidentiality, and any one can be used to disable the third. Another approach is Donn Parker's Hexad which adds one more triangle (Control-Authenticity-Utility) to the traditional model. It gives better insight, but still is insufficient.

The question what properties are fundamental is still unanswered. Author believes each property should be well-defined, achievable in some context, limited, and its output should be measurable. The measures should be composable.

[1] Proving a Computer System Secure, W. D. Young, W.E. Boebert and R.Y. Kain, The Scientific Honeyweller (July, 1985), vol. 6, no. 2, pp. 18-27.

3 CySeP "Quantum-Safe Cryptography" by Stephan Lechner from Institute for the Protection and the Security of the Citizen, JRC

The talk gave a preview of a possible technology race between quantum-safe cryptography and quantum computing, with a suggested finish line after the year 2030. Quantum technology research has made significant progress in the recent years. Although a fully operational quantum computer is not yet created, such a computer would be far more powerful than any currently available supercomputer. Quantum computers will be capable of breaking cryptographic systems which are based on today's computational infeasibility of factoring big numbers (Shor's algorithm, for example) or calculating points on elliptic curves. Specifically designed mathematical algorithms could be safe against quantum attacks, but such technologies are not available today and far from being standardised.

4 CySeP "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" by Bruce Schneier

Bruce Schneier gave a very insightful talk on surveillance in modern society aimed to raise people awareness of the problem. The main idea is that much of the surveillance is voluntary: we cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection. The result is a mass surveillance society of our own making. But have we given up more than we have gained?

It was very unfortunate that Bruce Schneier was not able to be physically present during the event, although it was promised.

5 CySeP poster session

The poster session have showcases latest achievements and proposals for addressing important security and privacy challenges, such as privacy issues of Android OS, Internet key exchange for the IoT, ontology-based semantic obfuscation for medical data, etc.