**Workshop in Information Security:**

**Building a Firewall within the Linux Kernel**

0368-3523, Winter 2019-2020

Lecturer: Reuven Plevinsky  
Time: Sunday 11:00-13:00    (you can ignore the "Lab" hours listed in the course list)  
Place: Kaplun building room 324

**Course overview**  
Firewalls control and monitor access to networks, and are found in every organization and personal computer. Emerging as an Israeli innovation two decades ago, modern firewalls perform sophisticated packet analysis tasks at a very high throughput.

In this workshop we will study the basic design of firewalls, and recreate the basic firewall functionality using just elementary building blocks of the GNU/Linux operating system. We will extend the Linux kernel with packet analysis capabilities, interface it with userspace programs, and experiment with using this firewall for blocking real-world attacks.

The workshop's goals:

* Become familiar with the Linux kernel, and how to extend it using kernel modules.
* Understand the TCP/IP protocol, and how it is processed in the Linux kernel.
* Understand concepts in packet inspection and parsing, and rule-based enforcement.
* Introduction to network attack techniques, detection and prevention.
* Gain experience in designing and implementing a modular system.

This workshop is offered in cooperation with industry experts from Check Point, offering a unique exposure to industry's capabilities and needs, and an opportunity for a real-world impact.

During the semester there will be 5-6 class meetings, and several assignments (serving as milestones towards the full project). The workshop projects will be done individually. The large, final assignment can be submitted by the semester's end; we will also allow extension into the summer if accompanied by a realistic work plan.

The assignments will be interesting and cool, but expect intensive and challenging work, and lots of self-learning. Students will be expected to read and learn on their own any concepts and systems that are unfamiliar and needed in order to carry out the project successfully.

Prerequisites:

* Operating systems (0368-2162)
* Software Project (0368-2161)

(Exception possibe for students with equivalent prior background.)

Recommended but not mandatory:

* Communication Networks (0368-3030)
* Any information security course