Faculty of Electrical Engineering
and Communication

Brno University of Technology
Technická 12, CZ-616 00 Brno, Czechia

http://www.six.feec.vutbr.cz

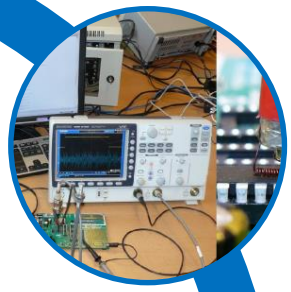
Stress Testing and Distributed Denial of Service Testing of Network Infrastructures

Lukáš Malina
Converged Systems, SIX
Department of Telecommunications, FEEC, BUT

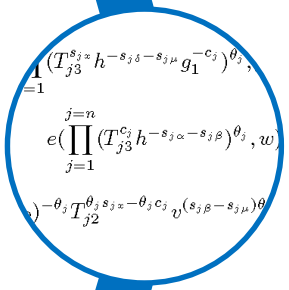
http://crypto.utko.feec.vutbr.cz
malina@feec.vutbr.cz

Our Research and Development Areas

Cryptology Research Group



Research and development in cryptology



Cryptographic design of new protocols, its implementation and optimization

Security and stress testing services

SIX research centre
sensor, information and communication systems

malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Our Security and Stress Testing Services

Capacity, security and performance testing

- Stress-testing of 10 Gbps network infrastructures and web applications using Spirent Avalanche equipment

Vulnerabilities and penetration testing

- Security evaluation of systems and infrastructures
- Testing of Distributed Denial of Service (DDoS) attack vulnerabilities

SIX research centre
sensor, information and communication systems

malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

About (D)DoS

- Denial of Service (DoS) attacks disrupt the ability of the machine to communicate with authorized users.

- Distributed DoS attacks are cyber attacks based on Denial of Service attacks but the origin of the attack is distributed among more sources.

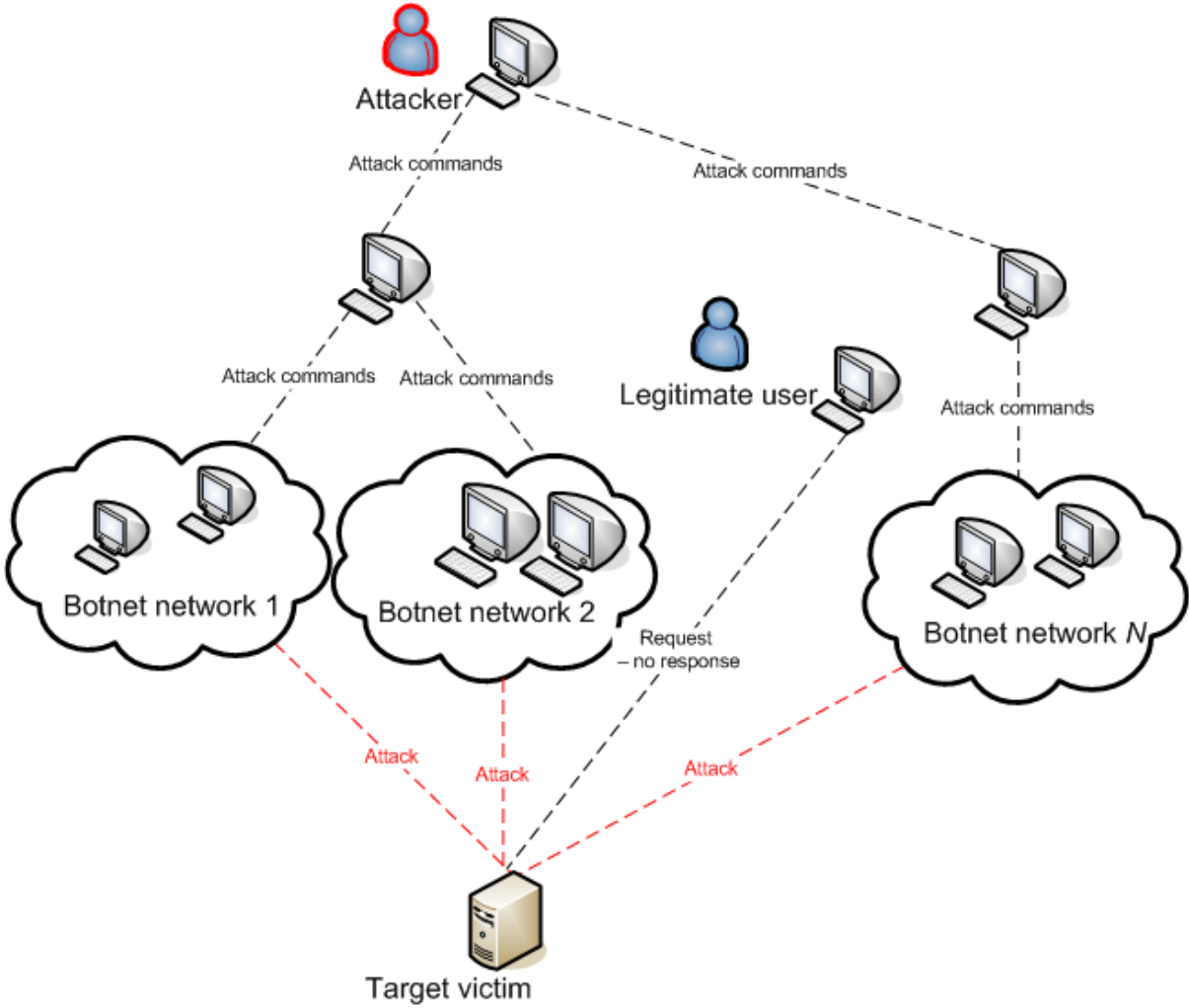
About DDoS

Motivation of DDoS attackers:

- Harm companies.
- Blackmailing.
- As a form of protest.

Some DDoS Atacks (CZ 2013):

- February 2013: an attack to viry.cz (TCP SYN Flood Attack from ca. 500 IP addresses on Apache Server)
- March 2013: massive attacks to several Czech news servers, bank servers and mobile operator servers(TCP SYN Flood attacks, thousands – millions packets/sec)



malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Types of Attacks (D)DoS

- Flooding attacks
  - Exhaust communications/memory/computing capacity of the target.
  - Exploit weaknesses in protocols.
  - For example: TCP-SYN flood, UDP flood, reflector attack...
- Logical attacks
  - Cause a crash of SW/OS.
  - Attacks on the logical weakness in SW programs/OS.
  - For example: Ping of death, Land attack...
- Other definitions: Volumetric and semantic attacks

Recent Worldwide Trends in DDoS

- Increase of DDoS attacks from Asian countries.
- Increase of DDoS attacks that are more stealthy and slower.
- Size of many DDoS attacks exceeds over 100 Gbps.
- Reflected amplification attacks become more popular.

Source> Prolexic Technologies, http://www.prolexic.com

DDoS Defense / Mitigation Techniques

- Robust and secure network infrastructure.
  - Employ firewalls, IDS systems, honeypots, redundant lines and servers.

- The protection by blacklisting and whitelisting.
  - Move the legitimate users to the backup line, and put them to the "white list".
  - Suspicious IP addresses insert on the "black list".

- Method of Defense attack.
  - Increase the number of packets from legitimate users.

Stress Testing with DDoS of Network Devices

- Equipment:
  - a stress tester/traffic and DDoS attacks emulator.

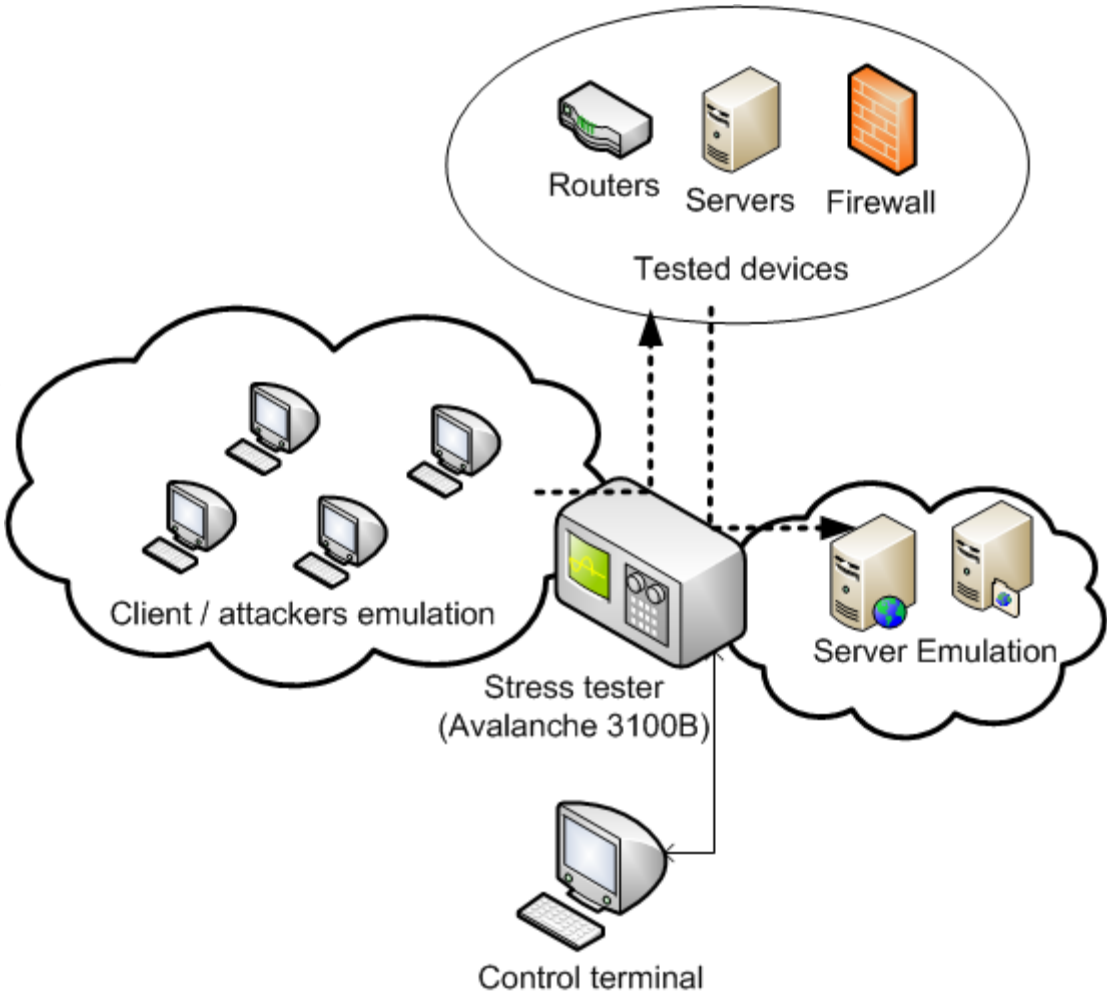
- Benefits:
  - Detection of device limits and weaknesses.
  - Detection of network bottlenecks.
  - Get feedback and optimal configuration.
  - Preparation of emergency and backup scenarios in the event of a real DDoS attack.

malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

General Test Scenario

Stress tester: **Spirent Avalanche 3100B**:

- Generating traffic to 40 Gb/s.
- Emulation of network clients and servers.
- L4-L7 Layers ISO-OSI.
- 15 DDoS attacks.
- Attack designer-custom definitions and design of attacks.



malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Test Results Visualization - Sample

Test of an Apache web server by using the Avalanche 3100B TestCenter:

Test Stages (Client)

1 2 3 4 5

Test Stopped

Transactions

Attempted: 87 252
Successful: 23 775
Unsuccessful: 63 477
Aborted: 0

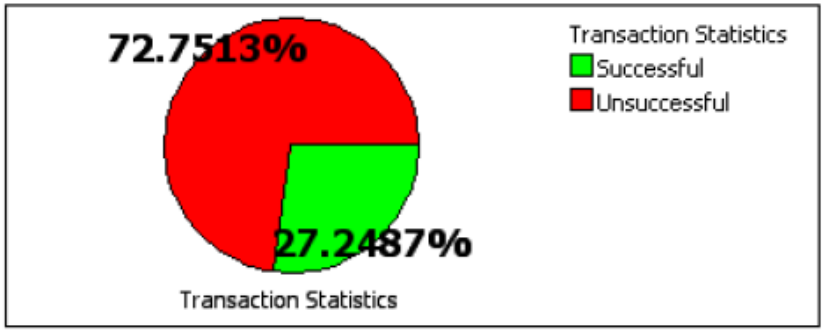
Time

Elapsed: 00:00:24
Remaining: 00:00:00

Layer 2 / Ethernet

Packets sent:	583 737
Packets received:	664 967
Bytes sent:	68 267 668
Bytes received:	727 871 402
Current sent packets per second:	25 353
Max sent packets per second:	27 641
Avg sent packets per second:	23 447
Current received packets per second:	27 511
Max received packets per second:	35 502
Avg received packets per second:	27 657

Test Results Summary	Transactions			Time (ms)						TCP Connections	
		Total	Rate Per Second		Page Response	URL Response	To TCP SYN/ACK	To First Data Byte	Est. Server Response		Total
	Attempted	87252	3635	Minimum	1.0	1.0	0.089	0.479	0.0	Attempted	87252
	Successful	23775	990	Maximum	9104.0	9104.0	6004.092	3288.192	3287.359	Established	86528
	Unsuccessful	63477	2644	Average							
	Aborted	0	0								



SIX research centre
sensor, information and communication systems

malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Example of Stress Test with the DDoS Attack

- Device tested:
  - Firewall CISCO ASA5510 (1.6 GH, 1024 MB RAM bandwidth up to 300 Mb/s).

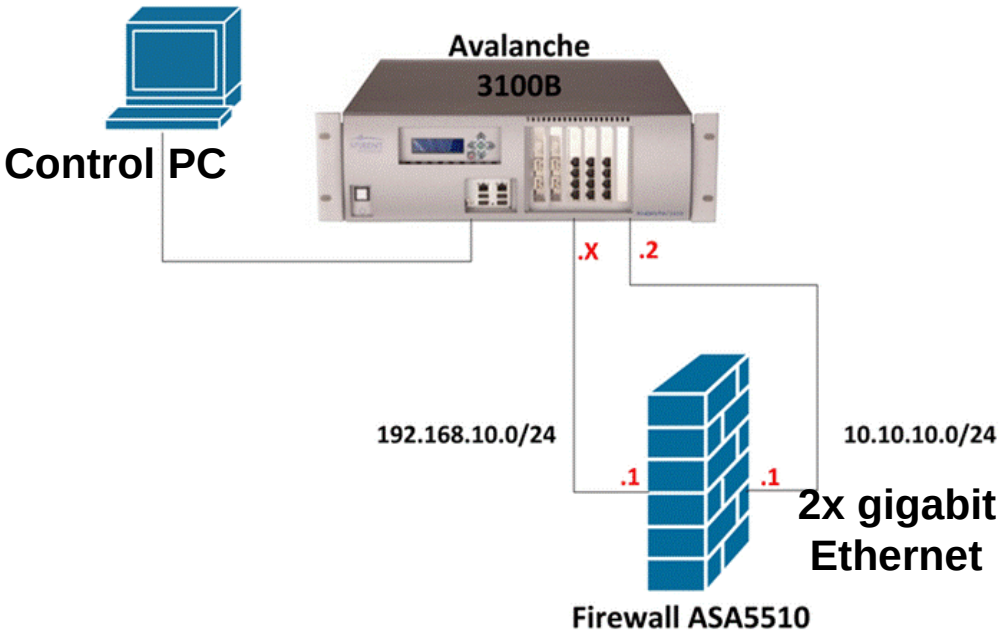
- DDoS attack chosen:
  - TCP-SYN flood attack.

- Two testing scenarios:
  - Sending HTTP requests and responses from/to the emulated Web server from/to the emulated clients without the DDoS attack.
  - Linear amplification of DDoS attack until the congestion of the Web server (number of DDoS packets per second 0-4000).

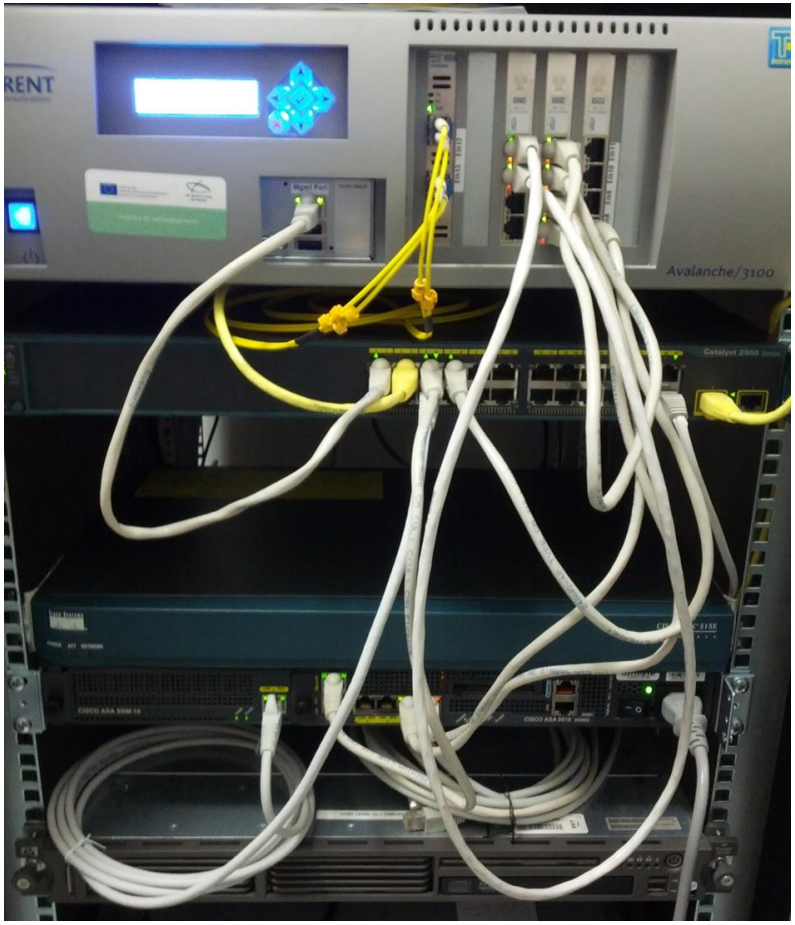
malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Test Topology

- Test topology>



How it look in practice>

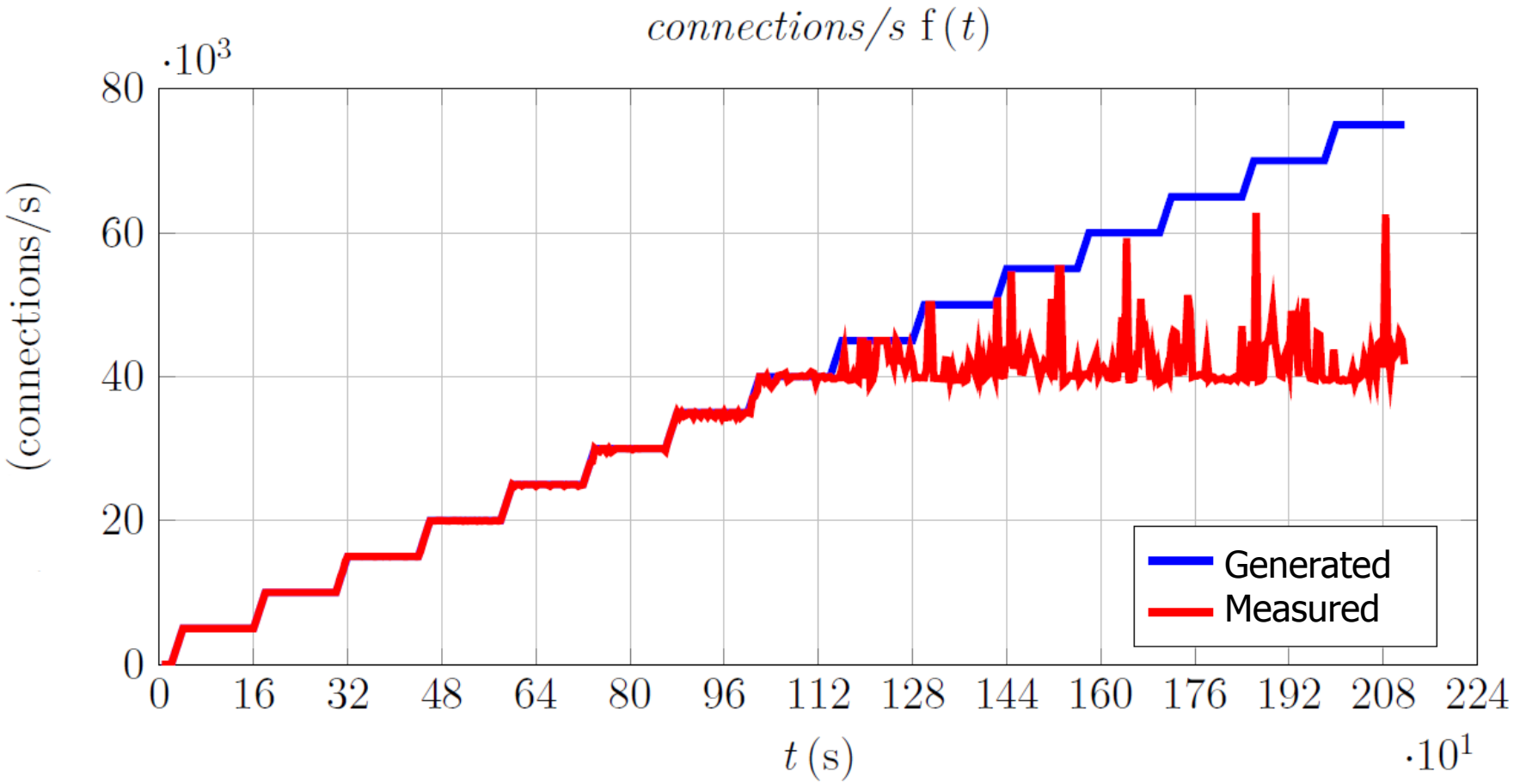


SIX research centre
sensor, information and communication systems

malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Test Results – Stress Test

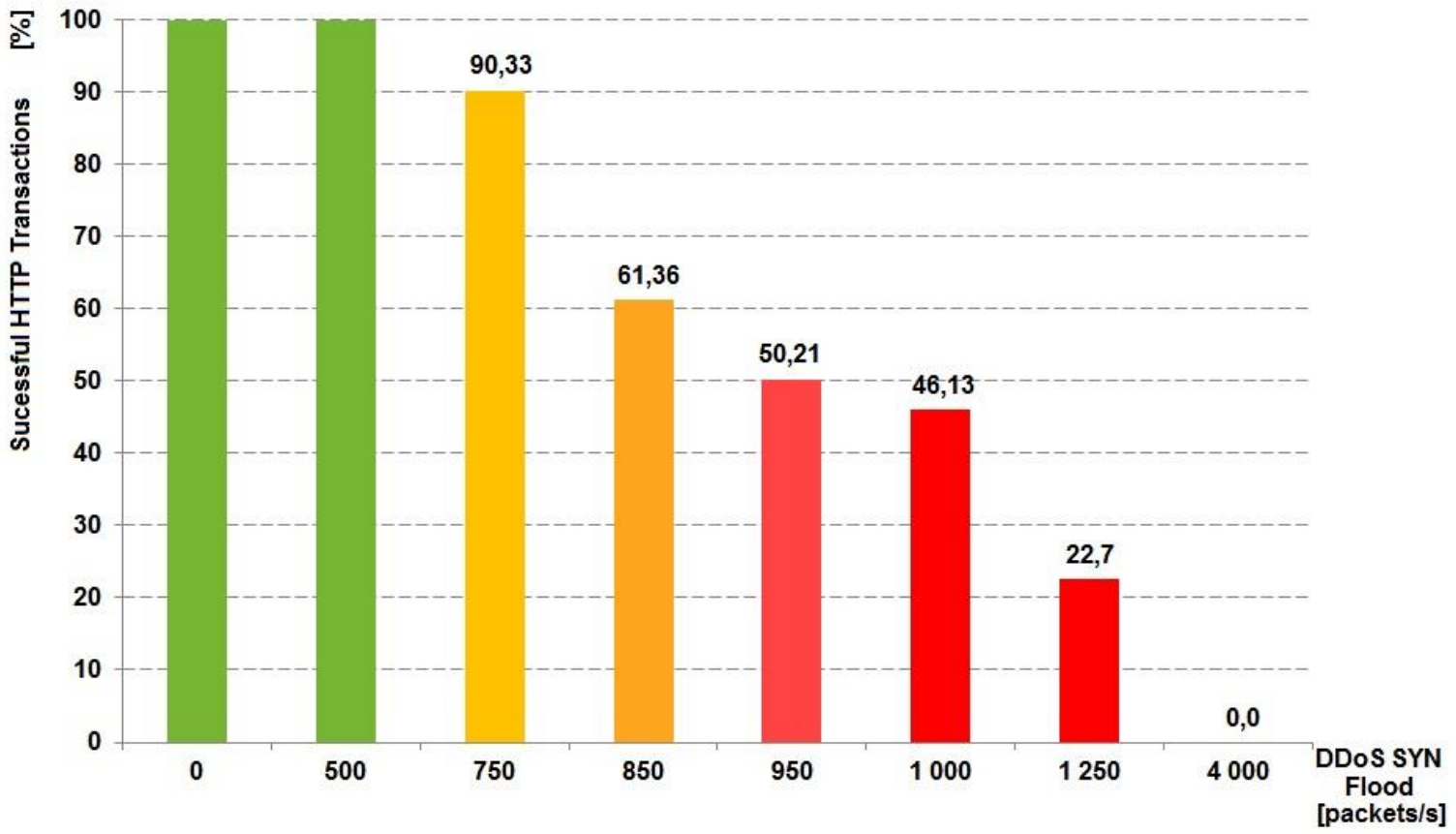
- TCP connection test (ASA 5510 provides max. 50000 connections/s):



malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Test Results – DDoS Test

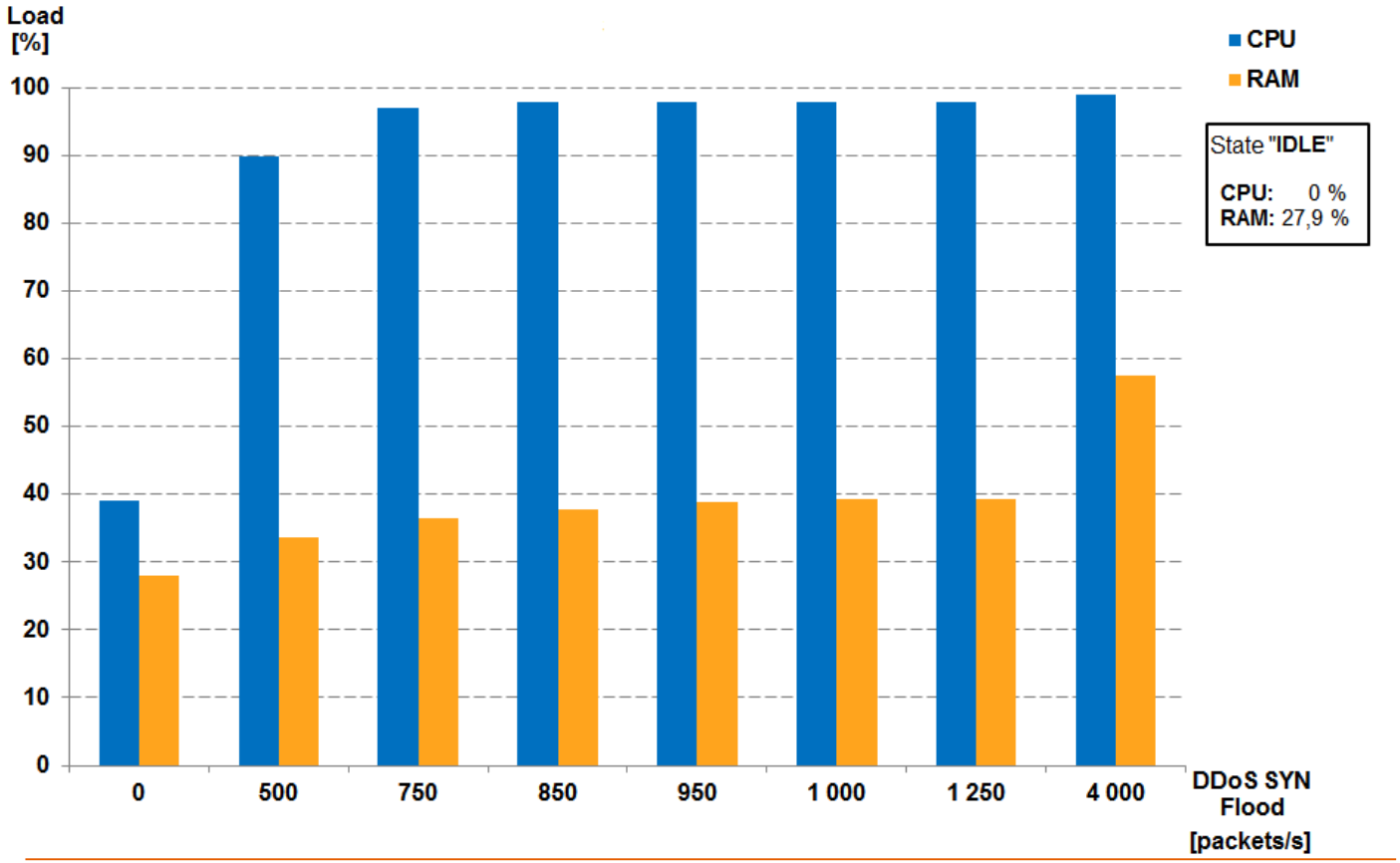
- The percentage of successful HTTP transactions during the TCP-SYN flood attack:



malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Test Results – DDoS Test

- Memory and CPU load on the ASA5510 Firewall during the TCP-SYN flood attack:



malina@feec.vutbr.cz, http://crypto.utko.feec.vutbr.cz

Conclusion

- DDoS protection and prevention:
  - Use active and passive security network devices, the backup lines.
  - Test network devices and infrastructures.
  - Create the crisis scenario.
- Benefits of stress and secure testing:
  - Recognition of the device behavior during the DDoS attacks.
  - Determine the limits of devices tested.
  - Detection the bottleneck of the network infrastructure.
  - Get the feedback.

Contacts

Thank you for your attention!

About author:
Ing. Lukáš Malina
malina@feec.vutbr.cz
+420 541 146 963

Our webs:
SIX:
http://www.six.feec.vutbr.cz/

Cryptology Research Group:
http://crypto.utko.feec.vutbr.cz/