**REPORT / PRESENTATION**

**Discipline "Computer Networks", Year I Master IVA engl.**

**General requirements**:

- Work in a group of maximum two people

- Presentation will be made in front of the class

- The choice and communication of the theme will be made in school weeks 3-4

- The elaboration and sending of the files with the report and the presentation are made in

weeks 5-8 and the oral presentation will be made in weeks 9-12

The entire achievement (report and oral presentation) will be graded and will represent 40%

from the final grade of the discipline.

**Technical requirements**:

THEME:

**To analyze a system from the point of view of its security, highlighting vulnerabilities, providing possible solutions**.

The report will provide:

- a presentation of the system, its mechanisms, evolution and performance

- investigation of possible defects that may occur, vulnerabilities, weaknesses, types of attacks

- solutions, possible remedies, improved variants will be offered.

System examples: OS, web, Internet, LAN, database, e-commerce, grid, management system, multilayer networks, wireless networks, mobile, etc.

Choose an assignment, send an email with the title of the assignment and the names of the students who collaborate for its realization; My answer (reply) will validate the theme. In your email insert a supposed table of contents, which may be the initial topic of discussion for our first meet

Write a report of maximum 10 pages IN ENGLISH (MS file Word, PDF) and send it by email

 Prepare a presentation (10-15 slides, .ppt, pdf) and send it by email; will constitute the

oral presentation support (maximum 10 minutes, in the last four weeks of school of the calendar year)

- Mailing address: vasile.dadarlat@cs.utcluj.ro. Please do not use my email address associated with the ‘campus user’, instead use the chat provided in the course’s associated team ‘RC Master an I’

It will be mandatory to present the bibliography / web resources used, correctly

referred in the text

The document should specify the contribution of each one (this will also be noted at your

oral presentation).

The last chapter will constitute the own conclusions on the theme (obtained by

comparative analysis, analysis of the evolution in the field, forecasts, etc.).

The general structure of the report will be based on chapters that will express (at least)

the following elements:

o Definition of the theme and elements of introduction (if the problem/theme is current state in the field, existing achievements)

o Detailed analysis of the chosen theme

o Proposals for solutions

o Results of the implementation of the proposals (if applicable) and your own conclusions

o Bibliography

Writing format as a scientific paper (survey, presentation of research activity) is encouraged.

For those who wish to conduct a more general study/presentation, they can choose the development of the following themes, (or others can be proposed):

**BIOMETRICS: Overview**

Introduction to biometric authentication

Technologies in biometrics

Cutting-edge achievements and existing applications (present a case study)

**SSL/TLS and SSH security protocols**

Security at the transport and application levels

Applications in e-commerce and remote administration

Comparisons with IPSec

**Implementing security in network management**

SNMP : Evolutionary presentation

Security features introduced

SNMPv3 analysis and problems to be solved

**Generalized MPLS (G-MPLS)**

Concept description

Architectures

Operation

**Multilayer Networks**

Mult-layer routing

Multilayer protection and restoration

Multilayer design and optimization

For those who want to study advanced topics in the field of computer security and computer networks security (higher degree of study difficulty):

You have at your disposal the following topics (possible bibliographic landmarks in the file

'Topics1-upadova.doc':

Topic 1: RFID Security

Topic 2: Captcha

Topic 3: Untrusted Storage

Topic 4: SmartPhone Security

Topic 5: Attacks on SmartPhone

Topic 6: Password Protection

Topic 7: Distributed Denial of Service Attacks

Topic 8: Sybil Attacks

Topic 9: Behavioural Biometrics

Topic 10: VoIP Security

Topic 11: Secure Content Delivery

Topic 12: Anonymous Communications

Topic 13: Keyloggers Detection

Topic 14: Anonymity in WSN

Topic 15: Botnet Detection

Topic 16: Trusted HW

Topic 17: Security of RFID ePassports

Topic 18: Node Replication Attack in WSN

Topic 19: Secure Data Aggregation in WSN

Topic 20: Privacy issues in Social Networks

Topic 21: Google Android smartphone security

Topic 22: Electronic Voting

Topic 23: P2P BotNet Detection

Topic 24: Specific aspects in IoT security

Topic 25: Browser Security

Topic 26: Privacy of Location Based Services

Topic 27: Named Data Networking Security

Topic 28: Named Data Networking Privacy

Topic 29: Cloud Security

Topic 30: Anonymity in Wireless Network

Topic 31: Smartphone User Profiling

Topic 32: SSL security issues in Android

More possible topics can be found in the articles about 'security in the Internet of Things'

in the 'topics-IoTsec.doc' file.