Co-funded by the Erasmus+ Programme of the European Union

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant
N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

COURSE DEVELOPMENT PLAN – AN OVERVIEW

Information Security Services Education in Serbia (ISSES)

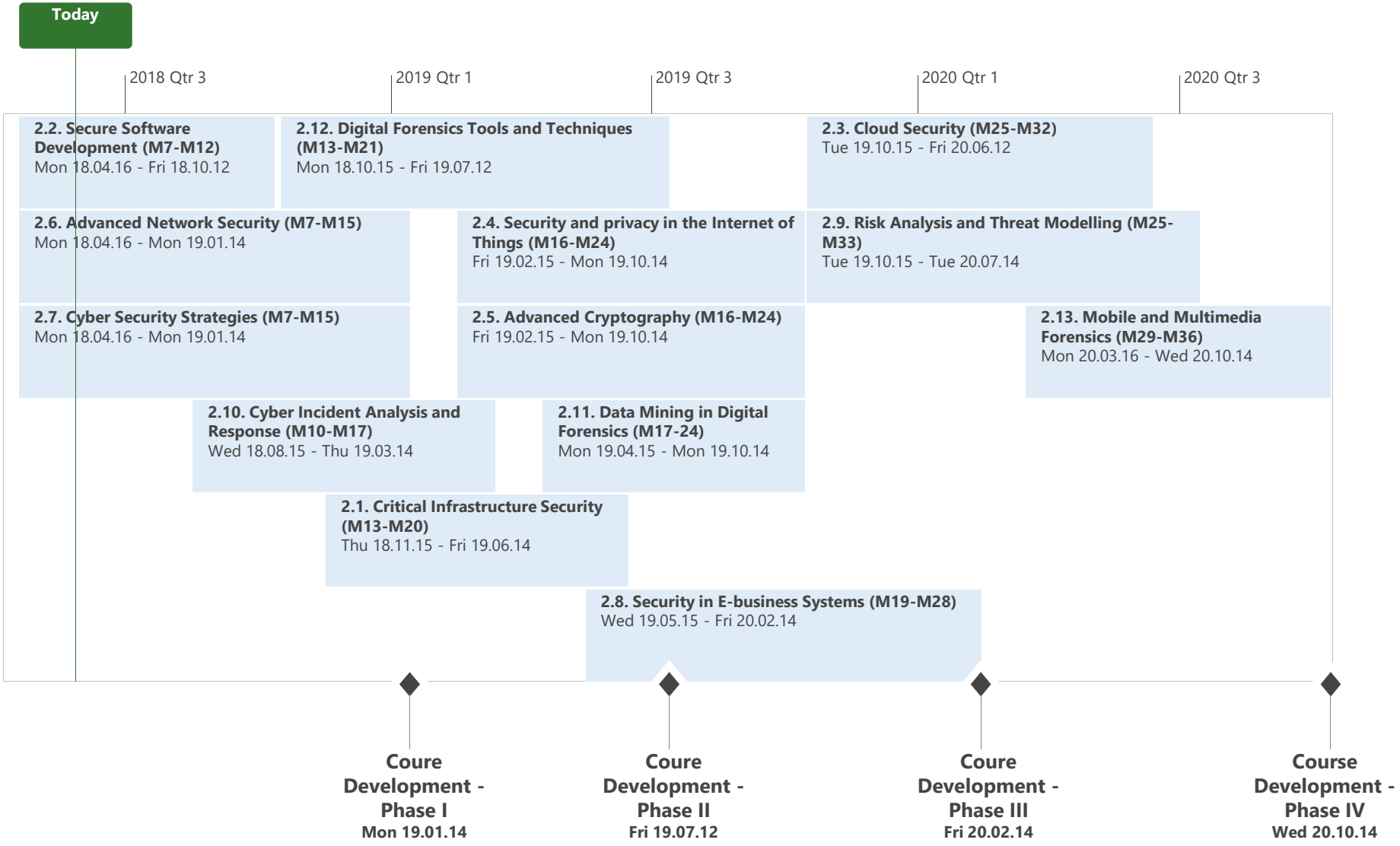
Erasmus+ Key Action 2 – Capacity Building in the field of Higher Education (CBHE)

ISSES 2017-2020
Novi Sad, Serbia

WP2 – Curriculum Development (UNS)

ID	Title	Institution ?	Period
2.1	Critical Infrastructure Security	BME, Polimi, UNS	M13-M21
2.2	Secure Software Development	BME, UNS, UNI	M6-M12
2.3	Cloud Security	UNS, UB-ETF, VTS	M24-M32
2.4	Security and privacy in the Internet of Things	FOI, Polimi, BME, VTS, UNS	M16-M24
2.5	Advanced Cryptography	BME, UNS	M16-M24
2.6	Advanced Network Security	Polimi, UB/ETF, UNS	M7-M15
2.7	Cyber Security Strategies	BME, UB/FON	M7-M15
2.8	Security in E-business Systems	Polimi, UNS	M18-M28
2.9	Risk Analysis and Threat Modelling	Polimi, UB/FON, UNS	M25-M33
2.10	Cyber Incident Analysis and Response	FOI, UB/FON, UNS	M9-M17
2.11	Data Mining in Digital Forensics	FOI, Polimi, UB/FON, UNS	M17-M24
2.12	Digital Forensics Tools and Techniques	FOI, UB/FON, UNI, UNS	M13-M21
2.13	Mobile and Multimedia Forensics	FOI, UB/FON	M22-M30

WP2 Sub-project



Presentation Overview

- Introduction
- Phase I Courses
  - To be completed in 2018
  - 2.2, 2.6 & 2.7
- Phase II Courses
  - To start in 2018
  - 2.1, 2.5 (2.8), 2.12
- Phase III Courses
  - To start in Q1/Q2 2019
- Phase IV Courses
  - To end in 2020
- Next Steps & Summary

Collaboration Format

- Each course development (Task in the bullets below) is led by one (Serbian) HEI
- The Task leader (**Leader**) is responsible to implement the course
- The Leader creates the **course 'core'**, which is common for all HEIs
- A non-Leader participants might develop
  - part of the 'core' course content, or
  - their specific content, which does not become part of the course 'core'.
- The 'core' is at least **50%** of the course's (complete) content

Information Security Services Education in Serbia (ISSES)

COURSES – PHASE I

2.2 Secure Software Development

#	Lecture Topic
1	Overview of the secure software development lifecycle
2	Security requirements analysis
3	Security architecture, design patterns, and design principles
4	Security design analysis, threat modeling, and attack surface reduction
5	Risk assessment
6	Secure coding practices, static code analysis, and security code review
7	Security testing and dynamic application testing
8	Secure deployment configuration
9	Penetration testing
10	Software security metrics and assurance
11	Analysis of prominent risk and vulnerability sets (i.e., OWASP Top 10, SANS Top 25)

#	Laboratory Exercises
1	Security design analysis
2	Security code review and static code analysis
3	Security testing and dynamic application testing
4	Secure deployment configuration
5	Penetration testing 1
6	Penetration testing 2
7	Next-generation attack and defensive tools and techniques?
8	
9	
10	
11	

Check

Check

2.2 Discussion

- Possible content issues:
  - The penetration testing labs need to be more specific
  - Course should not overlap with Computer Security & Network Security content
  - Is Interactive Application Security Testing (IAST) missing as a topic?
  - Can we borrow a one-lecture Risk Analysis from another course? Who will work on that?

2.6 Advanced Network Security

#	Lecture Topic
1	Attack methodology and phases.
2	Gaining access - Network attacks
3	Gaining access - System attacks
4	Network defense tools
5	(D)DoS attacks, classification, botnets, Network DoS protection
6	Wireless, Bluetooth security
7	Anonymity, Tor, Onion routing
8	Mobile device security, threats and malware
9	Other types of attacks and vulnerabilities: Attack economics - Click frauds, phishing
10	Other types of attacks and vulnerabilities: Hardware Trojans
11	Penetration testing

#	Laboratory Exercises
1	Reconnaissance: packet capture, Wireshark, tcpdump, netstat, nmap
2	Network attack examples: ARP spoofing, DNS spoofing,…
3	System attack examples: SQL injections, EternalBlue and similar
4	Network protection: Firewall, IPS, IDS
5	DDoS attack/defense or Capture the flag
6	Penetration testing

2.6 Discussion

- Possible content issues:
  - The penetration testing lecture is at the end – isn't it too late considering that the labs should need that content as early as possible?
  - Lab #3: SQL injections are maybe a better fit in 2.2 (SSD)

2.7 Cyber Security Strategies

#	Lecture Topic
1	Cyberspace environment
2	Strategy and cyber security strategy in cyberspace
3	Security in Cyberspace
4	Risk Management in Cyberspace
5	Manage complex relationships in cyberspace
6	Cyber Security and Information Security Standards and Frameworks
7	Cyber Security Management Concepts
8	Contemporary conflict in cyberspace
9	Policy planning for the use of cyber space
10	Budget planning and implementing
11	Protection of civil rights and personal data
12	Physical Security and Environmental Risks and Events

#	Laboratory Exercises
1	Practical work on a cyber security related incident
2	Enterprise physical and environmental security standard, ISO IEC 17799 2000
3	Risk assessment tools and applications.
4	Designing a cyber defense exercise (steps, the attacker side and the defender side, the components of a cyber defense exercise: defender team, target system, infrastructure, attacker team, attacker system).
5	Planning the risk treatment actions and budget allocation

2.7 Discussion

- Possible content issues:
  - A 1-lecture Risk management + a 1-lecture Standards & Frameworks we might develop here and use elsewhere
    - Will depend on our decision related to 2.9 Risk – keep it or not?

Meeting Format

- Overview of course content for each phase 1-by-1
  - Start with Phase I courses and work until list of topics is clarified and finalized, work is divided and responsible persons are named
  - Short break after each phase
- **Plan A:** Break-out session(s) of involved parties to overview course content (one person to take notes and report)
  - 2.2: BME, UNS, UNI – Rapporteur: Nikola (?)
  - 2.6: ETF, BME, UT – Rapporteur: Žarko (?)
  - 2.7: FON – Rapporteur: Prof. Simić (?)
- **Plan B:** Joint discussion of each course within a phase

Information Security Services Education in Serbia (ISSES)

COURSES – PHASE II

2.1 Critical Infrastructure Security

#	Lecture Topic
1	Types of critical infrastructures and key resources
2	Historical overview of failures and attacks
3	Equipment, communication infrastructure and processes
4	Traditional CI security architectures
5	Novel CI security architectures
6	Physical and personnel security
7	CI protection against cyber threats and cybercrime
8	Network theory and its implementation in CI protection
9	Vulnerability and risk analysis
10	Cyber incident analysis and response
11	Standards and specifications in CI protection

#	Laboratory Exercises	
1	Penetration testing in IP networks	
2	Penetration testing in traditional industrial networks	Check
3	Penetration testing in state-of-the-art industrial networks	Check
4	Next-generation attack tools and techniques	Check
5	Next-generation defensive tools and techniques	Check
6	Red vs Blue Team exercise in a CI setting	
7		
8		
9		
10		
11		

2.1 Discussion

- Possible content issues:
  - It will be tricky to develop lab exercises which are (sufficiently) different from the Network & IoT laboratory exercises

- Possible solutions:
  - Closely follow the development of the Network Security course and ensure that the labs & lectures will be different
  - Alternatively, we might turn this into a hybrid NS & CIS course, with 50% content pure NS and 50% content specific CIS content → remove the NS course from the UNS specialization → problems in 2019 with too few courses ready to enroll students

2.10 Cyber Incident Analysis and Response

#	Lecture Topic
1	Introduction to Incident Response and Handling
2	Risk management processes, application Security Risks
3	Basics of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy
4	Cybersecurity and privacy principles, cyber threats and vulnerabilities
5	Basics of computer networking concepts and protocols, and network security methodologies
6	Network security architecture concepts including topology, protocols, components, and principles
7	Incident categories, incident responses, and timelines for responses
8	Intrusion detection methodologies and techniques for detecting host and network-based intrusions
9	Network traffic analysis methods, packet-level analysis
10	Different classes of attacks, behavior of cyber attackers, cyber attack stages
11	Basics of malware analysis concepts and methodologies

#	Laboratory Exercises
1	Networking Security Monitoring
2	Penetration testing in IP networks Concepts: packet capture, Wireshark, tcpdump, netstat, nmap
3	Network investigation tools and Windows Events, Firewall, Logs, Processes, and Registry introductions
4	Actual attack and defensive tools and techniques
5	Static Malware Analysis/Dynamic Malware Analysis
6	Analyzing Malicious Windows Programs

2.10 Discussion

- Possible content issues:
  - If we remove a separate Risk subject, can this course be used to cover risk systematically?

2.12 Digital Forensics Tools and Techniques

#	Lecture Topic
1	Forensic objectives and principles
2	Forensic Media Preparation
3	Write blockers
4	Acquisition of media
5	Digital chain of custody
6	Basic forensic document analysis
7	Internet and web artifacts analysis
8	Forensic recovery
9	Mobile device forensic
10	Documents and reports
11	Presenting evidence
12	Disclosure/unused material

#	Laboratory Exercises
1	Investigating data streams
2	File storage dates and times
3	File deletion/recovery
4	Recovering Internet Usage Data
5	Recovering: Swap Files/Temporary Files/Cache Files
6	Preservation and safe handling of original media
7	Making bitstream copies of original media
8	Word document forensics and password cracking
9	Use tools such as Encase Forensic Edition, X-Ways Forensic Addition, Forensic ToolKit (FTK), Linux dd, etc.

Check

2.12 Discussion

- Possible content issues:
  - Last lab with too many tools for one exercise
  - Depending on the needs, we could add lectures on operating systems artifacts, network forensics, cryptanalysis, etc.
  - Prerequisites could be operating systems and data organization.
  - It would be useful to add a lecture about basic legal principles in criminal and civil proceedings (e.g. 2nd lecture) and cyber crime (e.g. 3rd lecture).
  - Should Media Preparation be combined with Acquisition of Media?
  - Incorporate write blockers (and disk duplicators) into data acquisition lecture – hard to talk about write blockers for two or three hours.
  - Chain of Custody & Disclosure might be merged in lecture 1
  - Lab 1 could be used to familiarize students with the DF Labs → this might be true for all hands-on labs (in other courses)

Information Security Services Education in Serbia (ISSES)

COURSES – PHASE III

2.4 Security and privacy in the Internet of Things

#	Lecture Topic
1	Introduction to IoT and security and privacy
2	IoT system architecture, components and technologies
3	Security and privacy requirements and challenges in IoT applications
4	Security threats and attacks in IoT
5	Data trustworthiness and privacy in IoT
6	Demonstration of IoT security issues and countermeasures using example systems and case studies
7	Security challenges
8	Security and Privacy Engineering for IoT Development
9	The secure IoT system implementation lifecycle
10	IoT Incident Response

#	Laboratory Exercises
1	Hands-on experience on IoT security through case studies and projects
2	Analyzing IoT security and privacy requirements for real-world use cases
3	Setting up development environment for lab exercise
4	Simulation of attacks and defensive tools and techniques
5	Realization of the authentication system.
6	Implementation of cryptographic techniques
7	Detection of attacks and recovery

2.5 Advanced Cryptography

#	Lecture Topic
1	History of cryptography
2	Stream ciphers, block ciphers, block encryption modes, attacks on CBC mode encryption
3	Random number generation and distributing public keys
4	Hash functions
5	Secure channels, message authentication and integrity protection
6	Key exchange protocols, public key encryption and digital signature schemes
7	WiFi security, Transport Layer Security (TLS), secure e-mail
8	Authentication in practice, passwords and one-time passwords
9	Protocols for resource constrained networks
10	Full disk encryption and beyond, cloud encryption, Digital Rights Management
11	Homomorphic encryption, perfect forward secrecy, post-quantum cryptography
12	Cryptoanalysis

#	Laboratory Exercises
1	Stream ciphers
2	Block ciphers
3	Hash functions and digital signatures
4	Creating, storing and using passwords
5	Authentication and authorization in practice
6	Cryptographic protocols in resource constrained networks
7	Perfect forward secrecy
8	Homomorphic algorithms
9	Cryptoanalysis tools & techniques

2.8 Security in E-business Systems

#	Lecture Topic
1	Overview of computer security
2	Symmetric and asymmetric cryptography
3	Cryptographic protocols and standards
4	Cryptanalysis
5	Digital signatures
6	Public key infrastructure and certificates
7	Network security
8	Smart cards
9	XML security
10	Authentication
11	Authorization
12	Information security

#	Laboratory Exercises
1	Cryptographic API
2	Symmetric and asymmetric cryptography
3	Hashes, message authentication codes and digital signatures
4	Certificates, CRL, OCSP
5	TLS and HTTPS
6	Passwords
7	OAuth
8	Single-Sign-On
9	RBAC authorization
10	Selected topic from OWASP Top 10
11	Selected web framework security

2.8 Discussion

- Possible content issues:
  - Considerable overlap with 2.4 Advanced Cryptography
  - Both developed at the UNS → no need to duplicate the efforts

- Possible solutions:
  - Merge 2.8 into 2.4
  - Substitute with a different course → Which?

2.11 Data Mining in Digital Forensics

#	Lecture Topic
1	Introduction to data mining (motivation, case studies)
2	Exploratory analysis in data mining (K-means like clustering, and A-priori association rules)
3	Predictive analysis in data mining (Decision trees, Logistic regression)
4	Visualization (of data, data mining models, and parameters)
5	Documenting the data mining process (CRISP DM like methodologies)
6	Data preparation
7	Advanced evaluation of data mining models (silhouette plots, AUC, AUPRC, F Measure, Alpha, Beta, mistakes)
8	Advanced algorithms for clustering (DB SCAN, OPTICS, Spectral clustering)
9	Advanced algorithms for prediction (Ensemble algorithms, SVMs, NNs)
10	Advanced setting of data mining algorithms parameters
11	Case study: Using data mining tools for digital forensics

#	Laboratory Exercises
1	Introduction to Orange data mining software
2	Advanced options in Orange data mining software
3	Introduction to Python
4	Building your first predictive data mining models in Python
5	Building clustering models in Python
6	Visualization in Python

2.11 Discussion

- Possible content issues:
  - The topics listed are adequate for an introductory data science/engineering course
  - It might be useful to include more topics in information security
  - Change the title to Security Data Science → use at the UNS and UNI
  - Extend with additional 3-4 infosec topics, e.g. analysis of large volumes of PCAP data, credit card fraud analysis, etc.
    - Or keep current structure, but have hands-on exercises focus on infosec data, e.g. Linux & Windows logs, application logs, mobile audit logs, auditing in IoT systems (with low CPU/RAM), etc.

Information Security Services Education in Serbia (ISSES)

COURSES – PHASE IV

2.3 Cloud Security

#	Lecture Topic
1	Cloud computing introduction and history
2	Threat landscape in cloud computing
3	Cloud System Architecture – Concepts and Design
4	Cloud System Security - Platform and Infrastructure
5	Cloud-specific network security challenges
6	Cloud Data Security
7	Cloud Application Security
8	Cloud Service – Operations Management
9	Cloud Service – Legal and Compliance
10	
11	

#	Laboratory Exercises
1	NA
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	

2.3 Discussion

- Possible resource issues @ UNS
  - No experts to develop this course
  - Keep the lecture-only setup, i.e. no lab exercises
  - Closely align the content with the books and video courses for the ISC2'sCertified Cloud Security Professional (CCSP)
  - Jointly develop UNS & ETF & VTS with FOI/UT help
- Possible motivation issues @ UNS
  - Motivation = no space in UNS' envisaged MSc program → turn this into a PhD course at UNS similarly to UB-ETF

2.9 Risk Analysis and Threat Modelling

#	Lecture Topic
1	Risk
2	Risk management process
3	Risk assessment process
4	Vulnerabilities an weaknesses analysis
5	Atack
6	Threat analysis
7	Threat modeling:
8	Uncertainties and sensitivities in risk analysis
9	Risk analysis documentation, Monitoring and reviewing risk assessment, Application of risk assessment during life cycle phases
10	Standards related to risk assessment

#	Laboratory Exercises
1	Mapping Threats and Vulnerabilities
2	PASTA
3	OCTAVE
4	Threat Modeling Web Applications
5	VAST
6	Risk assessment tools and applications

2.9 Discussion

- Resource issues @ UNS
  - No experts to develop this course
- Motivation issues @ UNS
  - Motivation = no space in the envisaged MSc program

- Possible solutions:
  - Plan A: Inspect possibility to turn this into a PhD course
  - Plan B: Substitute with a different course more in line with the proposed specialization at the UNS about Cyber-physical systems (CPS) → maybe better to add CPS instead of 2.8, which might be merged into 2.5

2.13 Mobile and Multimedia Forensics

#	Lecture Topic
1	Introduction to Mobile Forensics
2	Introduction to Multimedia Forensics
3	Analysis of computer components
4	Analysis of computer digital storage devices
5	Mobile device analysis
6	Data in mobile device analysis
7	SIM / UICC card forensics
8	Properties of Multimedia
9	Multimedia data analysis
10	Multimedia device fingerprints
11	Watermarking
12	Reporting
13	Testimony

#	Laboratory Exercises
1	Performing a thorough computer analysis
2	Performing analysis of mobile computer
3	Performing multimedia data analysis
4	Practical exercises
5	Generating reports
6	Court case studies

Check

2.13 Discussion

- Possible content issues:
  - Mobile & multimedia forensics are quite dissimilar topics

- Possible solutions:
  - Put mobile forensics into 2.12
  - Separate mobile forensics into a separate subject
  - Remove or keep multimedia forensics? Turn it into a separate subject? PhD or MSc?

Information Security Services Education in Serbia (ISSES)

NEXT STEPS

Action items

- Continue with course content updates until finished
  - Incorporate updated course list and topics in the CDP
  - Inform the SC about the CDP changes

- Next training sessions
  - June 5-6, 2018: Network Security training in Budapest
  - June ??, 2018: Secure Software Development training in Budapest
  - Mid July 2018: Network Security training in Milano

Summary

- Introduction
- Course content in short
- Course-related issues
- Possible solutions
- Next steps

Thank you for your attention!