

Kerem Kocaer
Royal Institute of Technology
ICSS Program Description

Program Description

Master of Science in Information & Communication Systems Security

80 credits

Degree: 'Master of Science in Information Technology with specialisation in Information and Communication Systems Security'. ('Teknologie Magister i informationsteknik med inriktning mot informations- och kommunikationssäkerhet')

Description: 'After completing this programme, students should possess the knowledge, skills and attitude necessary to develop, plan, manage and perform, in a professional manner, necessary activities in the field of information and communication security in the public as well as the private sectors. Students will acquire a solid foundation for further development in the information and communication security field and for the extension of their own competence.'

University

KTH - Kungliga Tekniska Högskolan

Royal Institute of Technology

"KTH is Scandinavia's largest institution of higher education in technology and one of the leading technical universities in Europe." [wikipedia]

Web site: <http://www.kth.se>

Courses

- Introduction to Information Security and its Environment (10)
- Advanced Internetworking (6)
- Introduction to Cryptography (5)
- Network Security (5)
- Security for Java Environment and Electronic Commerce (4)
- Security in Mobile and Wireless Networks (4)
- Software Engineering and Security Architecture (5)
- Legal Aspects of Information Security (5)
- Security Management (10)
- Value Based Risk Management (5)
- Research Methodology and Scientific Writing (2)
- Master Thesis (20)

Introduction to Information Security and its Environment

10 credits

Course description

- A holistic approach to information and computer security
- Studying concepts and terminology commonly used in the area of IT security, to be unimpeded when reading articles written by professionals and researchers in the area. Critically analysing IT environments, identifying possible vulnerabilities and suggesting effective protective measures such as would alleviate those vulnerabilities.

Course topics

- General Systems Theory
- Cybernetics and Control Systems
- Living Systems Theory
- Introduction to information security (attacks/services/CIA/Threats/DAC-MAC)
- Security Models and Policies (La PaDula / BIBA / Clark-Wilson)
- Cryptography overview (Classical / Modern / Cryptanalysis)
- Security Architectures, Identification, authentication, access control.
- Malicious Software (Viruses, worms, trojan horses, Covert channels)
- Program Security
- Security Tools
- Assurance
- Law and ethics
- Privacy and Privacy Enhancement Tools

Books

- Schoderbek, Schoderbek, Kefelas: Management Systems. Conceptual Considerations
- Matt Bishop: Introduction to Computer Security

Projects

- System Holistic Approach: Application of Systems Theories to create a security policy for the Oregon University System.
- System Holistic Approach: Ethics in IT Security (nominated for best student project)
- Testing of security tools: Key loggers, Trojans, Nmap, Nessus, Dsniff, Ettercap, Ethereal, tcpdump, Snort, ...
- Exploiting vulnerabilities of the Microsoft Windows Operating System: RPC, WINS, IIS exploits. Utility usage: Netcat, nmap, tcpview, pskill, ntsan

Grade: 5

Advanced Internetworking

6 credits

Course description

- Deeper understanding of internetworking and routing protocols
- Design, operation, implementation and analysis of networking protocols

Course topics

- Bridging: Learning / Spanning Tree / Virtual LAN's
- Internetworking protocols: IP / IPX / Appletalk / CLNP / DECNET / IPv6
- Intradomain Routing Protocols: RIP / OSPF / IS-IS
- Network Layer Multicast (IGMP / DVMRP / PIM-SIM / Simple Multicast)

Books

- Radia Perlman: Interconnections: Bridges, Routers, Switches, and Internetworking Protocols

Projects

- ISP project: setting up of services necessary for running an ISP infrastructure: DNS servers (BIND), HTTP web server (ISC DHCP), FTP server (VSFTPD), SIP VoIP proxy server (Asterisk), OSPF Dynamic Inter-domain Routing (Zebra, Quagga).

Grade: 5

Introduction to Cryptography

5 credits

Course description

An advanced course about symmetric and asymmetric cryptography.

- mathematical foundations for cryptography
- symmetric and asymmetric cryptosystems

Course topics

- Classical Cryptography
 - Substitution & Transposition
 - Statistical analysis (Index of coincidence / Entropy)
- Stream Ciphers
 - LFSR / RC4 / A5 / Self-synchronisation
- Block Ciphers
 - Feistel Cipher / Key generation / Flaws
 - DES / AES
- Operational Modes (CBC / ECB / CTR / ...)
- Public Key Cryptography
 - RSA / El-Gamal / Diffie Hellman / Elliptic Curve
- Randomness (pseudo randomness, real randomness tests)
 - chi square, Frequency testing, Gap & run, Correlation
- Hashing (SHA-1 / MD5 / Collisions / birthday paradox)
- Authentication (Smartcard chall.resp. / NT Auth. / Unix Auth.)

Books

- Bruce Schneier: Applied Cryptography

Projects

- Cryptanalysis of a simple substitution cipher: Frequency analysis, Index of Coincidence, Monograph statistics
- Cryptanalysis of the Mexican Army Cipher
- Analysis of 2 classic cipher machines (Enigma, Geheimschreiber) and 2 modern cipher systems (AES, Blowfish)
- Randomness: chi square, Frequency testing, Gap & run, Correlation

Grade: 5

Network Security

5 credits

Course description

An advanced course on security mechanisms in distributed information systems. The goals of the course are to familiarize the students with:

- secure communication over insecure networks
- different technologies for authentication in distributed systems

Course topics

- Digital signatures
- Public-Key Infrastructure (PKI) and Trusted Third Party (TTP)
- Message authentication
- Network authentication (Kerberos)
- Email security
- VPN technology (IPSec)
- WWW security (SSL/TLS/SET)
- Security in Web services

Books

- Scott Oaks: Java Security
- William Stallings: Network Security Essentials

Projects

- Implementation of the Diffie-Hellman key exchange protocol in Java.

Grade: 5

Security for Java Environment and Electronic Commerce

4 credits

Course description

Advanced, high specialization course in java security, with special emphasis on security for electronic commerce.

Course topics

- Security technologies in Java development/runtime platform
- Security protocols and architectures for Java applications
- Secure Electronic Transactions (SET) protocol and EC extensions
- Smart cards technologies and applications for security and electronic commerce

Books

- Scott Oaks : Java Security
- Jonathan Knudsen : Java Cryptography

Projects

- Smart Card Identification: Design and implementation of a personal identity verification system based on Java smart cards. The system consists of a Java smart card applet for storing identity information (coded with the Java Card development kit) and a Java application, with a user interface, for verifying this information.

Grade: 5

Security in Mobile/Wireless Networks

4 credits

Course description

- Comprehensive overview of all relevant aspects of security in mobile and wireless networks.
- Introduction to new, advanced research topics.

Course topics

- Introduction to wireless networks security
- Analysis of threats and application requirements
- Wireless networks security components
- Security services in wireless and mobile networks: authentication, authorization, data confidentiality, data integrity and access control
- Security infrastructure for wireless mobile networks: keys and certificate management
- Secure group applications
- Security of mobile code

Books

- Jon Edney, William A. Arbaugh: Real 802.11 Security - Wi-Fi Protected Access and 802.11i

Projects

- Wireless LAN traffic analysis, cracking WEP encryption.
- Captive Portals: Installation and configuration of the captive portal NoCatAuth to provide authentication to wireless networks.

Grade: 5

Software Engineering and Security Architecture

5 credits

Course description

This course focuses on methods, modelling, design, threats and vulnerabilities of software security solutions, Common Criteria/ITSEC, software security and some of their pitfalls (such as buffer overflow and race conditions), and the role of security personnel in project teams

Course topics

- Introduction to software security, and the role of security personnel in project teams
- Overview of software systems engineering and architecture principles for software security
- Overview of technology selection such as programming languages, operating systems and authentication
- System security analysis, attack trees and source-level security auditing tools
 - Buffer overflow, race conditions and other common threats for software solutions
 - Problems of randomness and determinism
- Common Criteria guest lectures:
 - Mats Ohlin: FMV Civil government agency, boosting overall capability of total defence organisation
 - Trust2You Consultant: Common Criteria specialist
 - Swedac: SWEDAC is the Swedish national accreditation body for CC
 - @sec: Information security provider, specialised in Common Criteria (Structure ST / PP)
 - CSEC: Swedish Certification Body for IT Security

Books

- John Viega, Gary McGraw: Building Secure Software - how to avoid security problems,

Projects

- Common Criteria - Evaluation of a Protection Profile: Mobile Phone Digital Rights Management Protection Profile. How threats are countered by objectives, how objectives are fulfilled by security requirements.
- Common Criteria: Practical software evaluation of the SnipSnap application
- Web Server C source code audit with Rough Auditing Tool for Security (RATS)

Grade: 4

Legal Aspects of Information Security

5 credits

Course description

An advanced course on the legal aspects involved in the work of information security professionals. The goals of the course are to familiarize the students with: the laws and regulations relevant for information security professionals comprising such concepts as privacy, freedom of information and intellectual property rights, privacy, intellectual property and digital rights.

Course topics

- Introduction to law in a digital environment
- Freedom of information and privacy protection
- E-government
- Intellectual property rights on the Internet
- Intellectual property law and ownership in employment relationships
- Designing a legal interface for contracting on the Internet
- E-procurement
- Electronic signatures in a legal context
- Dispute resolution on the Internet
- Criminal law in an internet environment

Books

- Cecilia Magnusson Sjöberg (Ed.): IT Law for IT Professionals: an introduction

Projects

- Pre-contract, negotiation, and contract agreement of IT contracts

Grade: 3

Security Management

10 credits

Course description

Organisational and managerial aspects of information security and operative risk, such as governance, risk and security management, and criminological and sociological aspects of IS/IT security in organisations.

Course topics

- Corporate and IT governance
- Operative risk
- Risk tolerance and risk appetite
- Risk analysis and vulnerability assessment
- Security standards and framework (ITIL, ISO17799, COBIT, OCTAVE)
- Cost/benefit analysis
- Acceptance Criteria
- Organisational behaviour
 - Actions and attitudes that people and groups exhibit in Organization
 - Ethical considerations
 - Motivation (MBO / Employee involvement / education / ...)
 - Decision Making
 - Leadership

Books

- Alberts, Christopher et al: Managing Information Security Risks
- Stephen P. Robbins: Essentials of Organizational Behaviour

Projects

I was chosen the 'security director' and leaded a group of 10 students working on the following projects:

- Managed Security Services
 - Threats to Ericsson's core business interests
 - Services offered by MSSP's
 - Advantages & Disadvantages of MSS
 - MSS Procurement details
 - Implications and side effects with procuring MSS
- A Qualitative Risk Analysis of the Business Area of Managed Security Services
 - Identification of critical resources
 - Identification of Value drivers and KPI's
 - Risk Analysis
 - Identification and creation of risk profiles
 - Risk prioritisation and impact analysis
 - Mitigation plan and strategy

Grade: 5

Value Based Risk Management

5 credits

Course description

This advanced course in IS/IT Risk Management focuses on the need of a shareholder perspective in order to cost-effectively secure shareholder value against IS/IT perils. The course focuses particularly on risk management in outsourcing and offshoring.

Course topics

- Introduction to the concept of Shareholder Value
- Overview of internal methods for promoting shareholder value
- Enterprise Security Architecture
- Outsourcing
- Offshoring
- Guest Lectures:
 - Kim Thomas, PriceWaterHouseCoopers: Outsourcing – a risk and security perspective
 - Jan Persson, SEB: Security Strategies – in an offshored business model
 - Electrolux

Books

- Sherwood et al: Enterprise Security Architecture – A Business Driven Approach
- C. Magnusson, the Confederation of Swedish Enterprise: “India and China – from an Information Security Perspective”

Projects

I was the project leader for the course assignment:

- Business Driven Security Architecture
 - Goal: Deliver a project proposal for a business driven security architecture. The assignment was based on an ongoing project to offshore a Fortune 100 company’s IT operations to an offshore supplier in Bangalore, India.
 - Problem: The company, heavily dependent on IT, was in urgent need of a security architecture to be able to communicate their businesses security requirements to their offshore partner.
 - Tasks:
 - Develop a business driven security architecture
 - Present the different layers of the architecture
 - Determine the security services that the supplier should provide
 - Determine the type and strength of security mechanisms

Grade: 5

Research Methodology and Scientific Writing

2 credits

Course topics

- Principles of science and research
- Thesis structure, format and report writing
- Problem definition
- Common thesis types
- Four levels of method and choosing a research method
- Finding and using literature

Grade: 4

Master Thesis

20 credits

Title: “Corporate Governance: From COSO-ERM to ISO 27001”

Abstract:

Following several high profile business collapses such as Enron and WorldCom, and consequently emerging compliance legislations such as the Sarbanes-Oxley Act, there has been a growing pressure on organizations to enhance the transparency of their internal control and financial reports, and the responsibilities of senior management have severely increased. This situation has led to a better understanding of the importance of - previously underestimated - corporate governance.

To facilitate the complicated issue of implementing corporate governance and closely related topics such as IT governance, IT security management and IT services management, a number of standards, frameworks and best practices have been created by international bodies. While these standards and frameworks provide guidance for their solo implementation, integrating them becomes a challenge since there is a lack of information when it comes to their collaborative use. This situation causes confusion and difficulties in most companies where several of these standards have to be in place together.

This master thesis investigates the problem by comparing and identifying the gaps and overlaps between COSO-ERM, ISO 20000, ISO 27001 and the Security Architecture Model. It then analyzes the COBIT framework as a potential facilitator for the integration, and discusses the possibilities of using it.