Presentation Master SNE

Security and Network Engineering

UvA online Open House

OS3 Team

University of Amsterdam

November 16 and 20, 2020
1 History and Philosophy

2 Organisation

3 SNE Lab

4 Courses

5 People involved and more information
History of SNE

- Master of Science education, started in 2003
- Originally called System and Network Administration
  - In Dutch: “Systeem- en NetwerkBeheer”
- Now called Security and Network Engineering
- Moved to Science Park Amsterdam in 2009
  - Also part-time and international students
- Two focus areas
  - Networking and Security
  - Security includes Forensics
Inflow

- An interesting **mix** of bachelor educations
  - Bachelors of Science in Computer Science ("WO")
  - Bachelors of (Technical) Informatics (Polytechnic ("HBO"))
    - Belonging to the **best** polytechnic students
- *Intake* procedure (assessment) is required for all students
- You need to be well **motivated**
SNE master with an academic view

- Abstraction power
- Scientific knowledge
- Innovation power
- Presentation skills
- Reporting skills
- Research skills
Focus

- Open Technology
- OS3
  - Open Standards
  - Open Software
  - Open Security
- Security is omnipresent
- Technical orientation

Middle ground between abstract science and professional application
Accreditation by the NVAO

In March 2020 SNE has been visited by an accreditation panel.

“The panel is impressed about the educational concept and the teaching methods of the programme. Students are very intensively guided by lecturers and lab teachers and work together productively. As a result, students manage to acquire knowledge and skills at a very high pace.”

The official report of the NVAO (“Accreditation Organisation of the Netherlands and Flanders”) is available at their site:

https://www.nvao.net/nl/besluiten/uniwersiteit-van-amsterdam/m-security-and-network-engineering
Top programme 2016 — 2020

Top rated programme 2016
Top rated programme 2017
Top rated programme 2018

Best IT Master in Keuzegids 2020 (Dutch)

Keuzegids Masters 2020

masters
Career prospects

- Very good career perspectives
  - Companies are actively scouting for OS3 graduates
  - Almost 100% job guarantee
- Some sectors with many graduates
  - Networking organisations like AMS-IX and SURF
  - Security companies like Fox-IT and Secura
  - Research organisations like UvA and NLnetLabs
  - Government institutes like NCSC
  - Accountancy firms like KPMG and Deloitte
  - Many others
SNE students 2003-2020
Curriculum

- Total of 10 modules of 6 ECTS each
  - 60 ECTS == 1 year
  - 2 weeks == 3 ECTS
- Semester 1: 8+8+4 weeks
- Semester 2: 8+8+4 weeks
- Full-time or part-time (≡ full-time in 2 years)
Focus Area: Networking

- Focus on advanced networking
  - In-depth Routing and Switching (OSPF/IS-IS/MPLS/BGP)
  - In-depth TCP (high bandwidth/high latency)
  - Software Defined Networking (SDN)
  - Fiber optics
  - Wireless technology
- Two specialistic courses
  - InterNetworking and Routing
  - Advanced Networking
Focus Area: Security

- Focus on digital security, including forensics
  - Gather evidence in a way that will hold up in court
  - Malware
  - Security of radio-based technologies (GSM, BlueTooth, ZigBee)
  - Security of mobile operating systems
- Four specialist courses
  - Security of Systems and Networks
  - CyberCrime and Forensics
  - Offensive technologies
  - Advanced Security
Focus Area: Foundations and Complexity

- Focus on history, foundational aspects and complexity
  - History of Unix and the Internet
  - Basic Computer Architecture and Operating Systems
  - Basic protocols: DNS, SMTP, HTTP
  - Scaling techniques and Virtualisation
  - Administration and DevOps

- Two **specialistic** courses
  - Classical Internet Applications
    - Foundations of the Internet
  - Large Systems
### Semester 1

<table>
<thead>
<tr>
<th>Month</th>
<th>Part-time year 1</th>
<th>Part-time year 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep</td>
<td>Security of</td>
<td>Classical Internet Applications</td>
</tr>
<tr>
<td></td>
<td>Systems and Networks</td>
<td></td>
</tr>
<tr>
<td>Oct</td>
<td>Large Systems</td>
<td>InterNetworking and Routing</td>
</tr>
<tr>
<td>Nov</td>
<td>Research Project 1</td>
<td></td>
</tr>
<tr>
<td>Dec</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Semester 2

<table>
<thead>
<tr>
<th>Month</th>
<th>Part-time year 1</th>
<th>Part-time year 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb</td>
<td>CyberCrime</td>
<td>Advanced</td>
</tr>
<tr>
<td>Mar</td>
<td>and Forensics</td>
<td>Networking</td>
</tr>
<tr>
<td>Apr</td>
<td>Offensive</td>
<td>Advanced</td>
</tr>
<tr>
<td>May</td>
<td>Technologies</td>
<td>Security</td>
</tr>
<tr>
<td>June</td>
<td></td>
<td>Research Project 2</td>
</tr>
</tbody>
</table>
“Theoretical” courses

- 7 weeks (20 hours a week)
  - 2 * 2 hours lectures
  - 2 * 4 hours lab exercises and practical work
  - 1 * 8 hours private study
- 1 week examination
“Project” or “Practical” courses

- Same as theoretical courses, but with a small project as part of the practical work
  - Teamwork
  - Communication
  - Presentation
Research Project

- 4 weeks (full-time)
- Individual work (mostly)
  - Week 1: orientation and project definition
  - Week 2 and 3: research
  - Week 4: report writing
  - One day in week 5: presentation
The “fifth” day

- Lectures and lab exercises fill 4 full days every week
- The remaining day (mostly Wednesday) contains
  - Guest lectures
  - Colloquia
  - Site visits
  - Research preparation
  - Private study
Obligatory presence

- 10:00-16:00 on normal days
- On Wednesdays if there is an organized event
- Research projects: twice 1 month full time.
Corona times situation

- Lectures are online (09:00-10:45)
- Labs are, if possible, on-site in multiple groups
  - Labs may also be partially online
Visit to Bletchley Park in October 2016
Production environment

- x86-64 based PCs
- Running Ubuntu Linux on the desktop
- Using our own servers
- Using our own IP space 145.100.96.0/20
  - and our own IPv6 space 2001:610:158::/48
  - and our own AS AS1146
Experimental environment

- **Unix** (Linux, BSD, macOS), Windows, ...
- Hardware routers and **software routers**
- Each student uses own backend server
  with **virtualisation** technology (Xen, containers)
Security of Systems and Networks (SSN)

- Security of Systems and Networks
  - Crypto (traditional and modern)
  - Protocols (SSL, IPsec)
  - Authentication
  - Hacking tools
  - Passwords

- Mini-project included
Classical Internet Applications (CIA)

- Classical Internet Applications
  - History
  - Computer Architecture
  - DNS(SEC)
  - Email
  - Web
Large Systems (LS)

- Large Systems
  - Design
  - Administration
  - Cloud Computing
  - Scaling
  - Automation
  - Change Management
Offensive Technologies (OT)

- Offensive Technologies
  - Sniffing
  - Intrusion detection
  - Hacker mindset
  - Malware
  - Botnets

- Mini-project included
InterNetworking and Routing (INR)

- InterNetworking and Routing
  - Physical and logical structure of the Internet
  - Addressing (IPv4, IPv6)
  - Layer 2 and loop prevention
  - Layer 3 and routing
    - Interior (RIP, OSPF, IS-IS)
    - Exterior (BGP)
Advanced Networking (AN)

- Advanced Networking
  - In-depth transport layer (TCP)
  - Software Defined Networking (SDN)
  - Network Function Virtualisation (NFV)
  - Optical technology
  - Wireless technology
  - Carrier grade connectivity
  - Build your own network!
Cybercrime and Forensics

- Reliable gathering of digital information
- Recovering (partially) destroyed information
- Timelining
- Trap avoidance
- File systems
- Volatile information capture

- Mini-project included
Advanced Security (AS)

- Advanced Security topics
  - Wireless security
  - Mobile security
  - Internet of Things

- Mini-project included
Research Projects

- Research a problem of your own choice

Examples

- OV Chipcard
- Detection of peer-to-peer botnets
- Smart metering
- Wireless protocol analysis using GNUradio
- Industrial-Scale Software Defined Networking
- Optical Networks using Hollow Fibers
E-passport investigation (The Times)

Fatal flaw: How a baby became

The supposedly fail-safe system devised to foil terrorists and criminals can be easily turned to their advantage.

Steve Boggan reports

Jeroen van Beek takes the passport of a 16-month-old British boy and puts it on to an £40 smartcard reader the size of an iPod. He punches a code into his computer and, within seconds, the information contained in the passport's microchip appears on screen.

This is not supposed to happen, as communication between the chip and the reader uses powerful encryption, but a renowned British computer expert called Adam Laurie worked out how to crack the code 18 months ago.

Within seconds, in his university office in Amsterdam, Mr van Beek, 30, copies the contents of the microchip on to another chip, making a clone of the first. He launches some software called Golden Reader Tool — the International Civil Aviation Organisation (ICAO) standard kit for checking biometric passports — and the new chip is deemed to be authentic.
Staff

- **The Core Team**
  - Director of education **Karst Koymans**
  - Also Networking Area coordinator
  - Security Area coordinator **Jaap van Ginkel**
  - Lecturers / Lab teachers **Arno Bakker, Vincent Breider, Roy Vermeulen**
  - System Engineer **Niels Sijm**

- **Other lecturers**
  - **Jeroen van Beek, Paola Grosso**
  - **Cees de Laat**

- **Guest lecturers**
SNE information

- https://www.os3.nl/
- mailto:info@os3.nl
- “goto: Science Faculty, Science Park 904, Amsterdam”

for a visit and a personal introduction
Check the deadlines at https://www.uva.nl/

- Dutch students: June 30 23:59
- EU/EEA students: June 30 23:59
- Non-EU/EEA students: January 31 23:59

Register in Studielink at https://www.studielink.nl/
Receive your UvA-net ID and further instructions by email (check your spam folder)

Apply for the programme in Datanose **before the deadline**
Go to www.datanose.nl, log in with your UvA-net ID and upload all necessary documents

Pass SNE intake!
The Admissions Board will consider your request