Presentation Master SNE

Security and Network Engineering

Master's Event

OS3 Team

University of Amsterdam

February 13, 2020

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
  - In Dutch: "Security- en NetwerkEngineering"
- 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

Outflow

- 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

Accreditation by the NVAO

In June 2013 the master education SNE has been visited by an accreditation panel. Most notable fact was that SNE got again, just as in 2008, an excellent evaluation for our didactic concept.

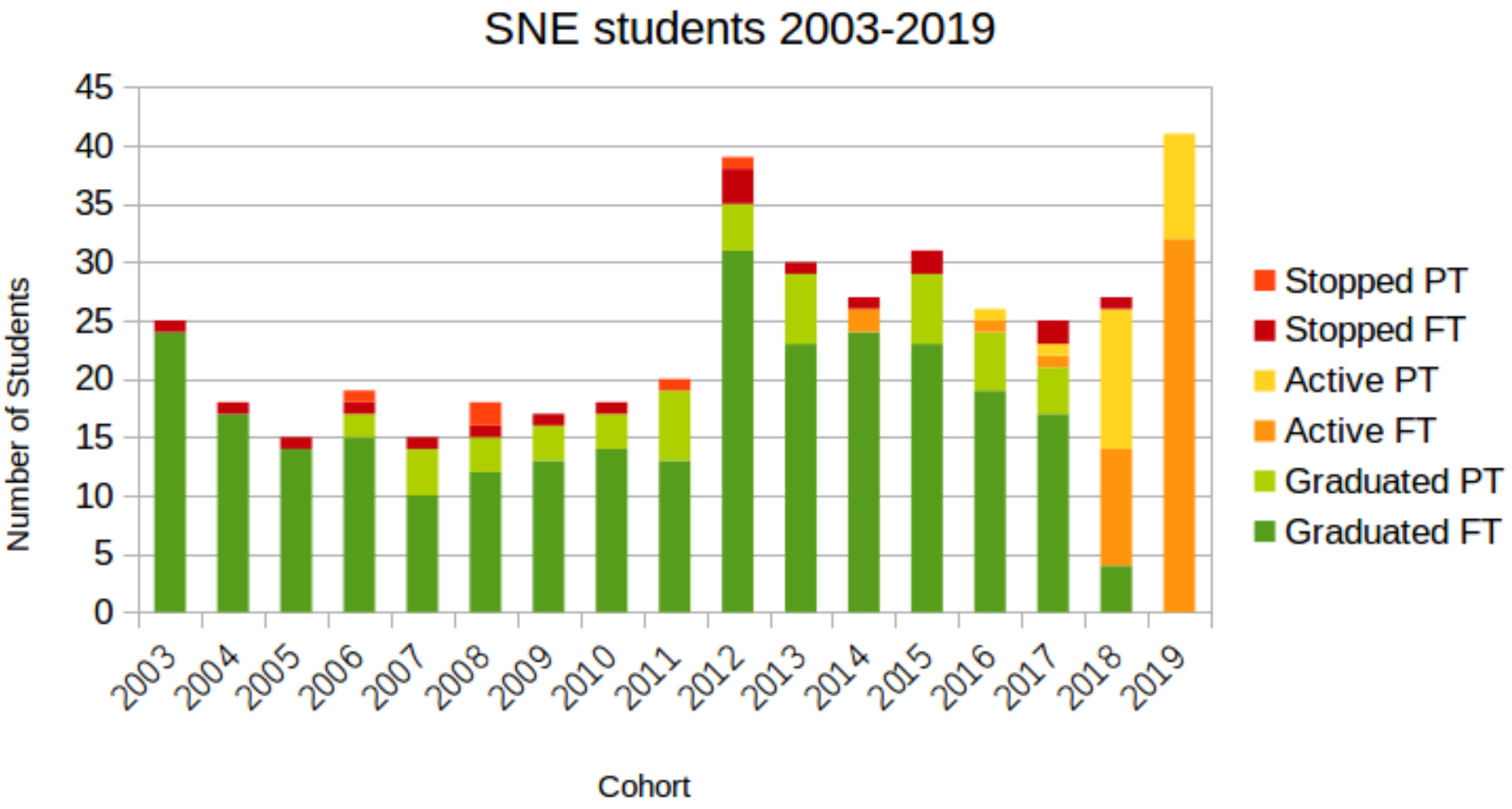
The official report of the NVAO ("Accreditation Organisation of the Netherlands and Flanders") is available at their site:

https://search.nvao.net/search-detail/55361

Top programme 2016 — 2018

http://www.keuzegids.org/

SNE students 2003-2019



Histogram

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 specialistic 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 protocols: DNS, SMTP, HTTP
  - Scaling techniques
  - Virtualization
  - Administration + DevOps
- Two specialistic courses
  - Classical Internet Applications
    - Foundations of the Internet
  - Large Systems

Semester 1

Month	Part-time year 1	Part-time year 2
Sep Oct	Security of Systems and Networks	Classical Internet Applications
Nov Dec	Large Systems	InterNetworking and Routing
Jan	Research Project 1	

Semester 2

Month	Part-time year 1	Part-time year 2
Feb Mar	CyberCrime and Forensics	Advanced Networking
Apr May	Offensive Technologies	Advanced Security
June		Research Project 2

“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.

Visit to CERN in October 2014

Visit to Paris in October 2015

Visit to Bletchley Park in October 2016

Visit to Paderborn in October 2017

SNE Lab production

- 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

SNE Lab experimental

- Experimental environment
  - Unix (Linux, BSD, macOS), Windows, ...
  - Hardware routers and software routers
  - Each student uses own backend server

    with virtualisation technology (Xen, containers)

SNE Lab at Science Park opened in August 2009

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
  - DNS(SEC)
  - Email
  - Web

Large Systems (LS)

- Large Systems
  - Design
  - Administration
  - Cloud Computing
  - Automation
  - Change Management
- Mini-project included

Offensive Technologies (OT)

- Offensive Technologies
  - Sniffing the network
  - 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 TCP
  - Software Defined Networking (SDN)
  - Fiber optics
  - Wireless technology
  - Build your own network!

CyberCrime and Forensics (CCF)

- 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

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)

News

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 a £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

Staff

- The Core Team
  - Director of education Karst Koymans
    - Also Networking Area coordinator
  - Security Area coordinator Jaap van Ginkel
  - Lecturers / Lab teachers Arno Bakker, Péter Prjevara, Vincent Breider
  - 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

Application and Admission (1)

- Check the deadlines at https://www.uva.nl/
  - Dutch students: **1 July**
  - EU/EEA students: **1 May**
  - Non-EU/EEA students: **1 February**
- Register in Studielink at https://www.studielink.nl/

Application and Admission (2)

- 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