INNOPOLIS UNIVERSITY

Master program

“Security and Network Engineering”

What is SNE?

- Program started in University of Amsterdam in 2003
- Focus on the OS3
  - Open Standard
  - Open Software
  - Open Security
- Security oriented
- Industry based program
- Teamwork based
- Professional guest lectures and workshops

SNE Lab

- Workstations
- Servers
- Public IP addresses
- Embedded devices
- Network switches and routers
- Tea,coffee and cookies

Program

Focus on **cyber security** and **network engineering**:

- Classical Internet Applications
- InterNetworking and Routing
- Advanced Networking
- Security of Systems and Networks
- Large Systems
- Advanced Security
- CyberCrime and Forensics
- Offensive Technologies

Program structure / Semester schedule

Semester	September - October	November - December	January
1st	➢ Classical Internet Applications ➢ InterNetworking and Routing	➢ Security of Systems and Networks ➢ Advanced Networking	Research Project (RP1)

Semester	February - March	April - May	June - August
2nd	➢ Large Systems ➢ Advanced Security	➢ CyberCrime and Forensics ➢ Offensive Technologies	Industry-based Project (RP2)

Practice oriented courses

Many practical experience:

- Spending time in lab to perform hands-on work related to modern industry needs

Projects:

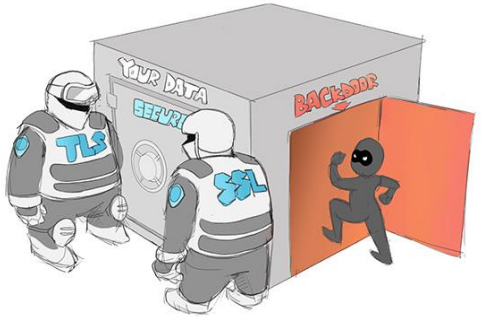
- Chance to get technical task from the real company
- Free choice to select technical problems you are interested in
- Teamwork skills
- Presentation skills
- Technical report writing skills

Research Projects 1

“Open-source Framework
for Security Event Logs Visualization “

“Probabilistic estimation
of honeypot detection “

“Backdooring Asymmetric Crypto Algorithms”



Classical Internet Applications (CIA)

- Booting
- Operating system structures
- DNS (Sec)
- Email
- Web

InterNetworking and Routing

- Basics of networking
- IPv4 and IPv6
- VOIP
- QoS
- Routing (OSPF, EIGRP, BGP)
- Advanced Routing and Traffic Engineering (MPLS,VPLS, VRF)

Advanced Networking

- SDN and CDN
- Network attacks
- VPN and IPsec
- Network segmentation and ACLs
- Network pivoting
- Network tools

Security of systems and networks (SSN)

- Cryptographic algorithms and related technology
- Secure Protocols (SSL, TLS, IPsec)
- Secure booting
- SSN Project

Large Installation Administration (LIA)

- Large Scale Virtualization
- Container Orchestration
- Continuous Integration and Continuous Delivery
- Data Centers
- Disaster Recovery
- High Availability Clusters
- IT service management
- Backup, Monitoring
- Storage Cluster

Advanced Security

- Wireless Security
- Database Security
- Web Security (web vulnerabilities discover and exploitation)
- Introduction to Reverse Engineering
- Debugging and disassembling
- Binary Exploitation
- IDS/ IPS systems and network evasion techniques

CyberCrime and Forensics (CCF)

- Law and regulations
- Acquiring of digital evidence
- Recovering information
- Anti-forensics
- File systems analysis
- Volatile information analysis
- Malware analysis
- Operating systems and network forensics artifacts
- Incidents Response
- Anonymity

Offensive Technologies (OT)

- Fuzzing, Scanning
- Advanced exploitation techniques
- Penetration testing techniques (blackbox vs whitebox)
- Vulnerability code assessment (OWASP and other methodologies)
- Offensive tools (Metasploit, Powershell Empire, NMAP, BurpSuite and so on)
- Physical security

Industry-based Projects (RP2)