Information Security Technology
CSE – IST special master track

IST coordinators:
Boris Skoric
Berry Schoenmakers
Reasons for studying security ...
... and more reasons
TRU/e Master in Cyber Security

• New program, started 2015-2016
• Cooperation between TU/e and RU Nijmegen
  • Combines expertise in security
  • Wide variety of security courses
• Website: true-security.nl
• Successor of Kerckhoffs master (TU/e + RUN + Twente)

EIPSI = Eindhoven Institute for Protection of Information
www.win.tue.nl/eipsi/
• Combines security research at Math & CS
  – SEC group (CS)
  – Coding & Crypto group (Math)
TRU/e cybersecurity courses

**Mandatory**
- Software security
- Principles of Data Protection
- Security in Organisations
- Cryptology
- Advanced Network Security
- Verification of Security Protocols

**Electives (≥ 15 ECTS)**
- Law in Cyberspace
- Hackers Hut
- Hardware Security
- Cryptographic Protocols
- Cryptographic Engineering
- Physical Aspects of Digital Sec.
- Applied Crypto
- Privacy Seminar
- Seminar IST

*Security ≠ crypto
Crypto ≠ math*
# The curriculum – Q1 & Q2

<table>
<thead>
<tr>
<th>Time</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Q1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30-12:30</td>
<td>Principles of Data Protection (can also be done in Q5)</td>
<td>Cryptology</td>
<td>Cryptology</td>
<td>Security in Organisations</td>
<td></td>
</tr>
<tr>
<td>13:30-15:30</td>
<td>Cryptology</td>
<td>Principles of Data Protection (can also be done in Q5)</td>
<td>Law in Cyberspace</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:30-17:30</td>
<td>(Phys. Aspects of Digital Sec. in Q5)</td>
<td>(Phys. Aspects of Digital Sec. in Q5)</td>
<td>Software Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Q2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10:30-12:30</td>
<td>Applied Crypto (can also be done in Q6)</td>
<td>Hackers Hut</td>
<td>Hackers Hut</td>
<td>Security in Organisations</td>
<td></td>
</tr>
<tr>
<td>13:30-15:30</td>
<td>Hackers Hut</td>
<td>Applied Crypto (can also be done in Q6)</td>
<td>Law in Cyberspace</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:30-17:30</td>
<td></td>
<td></td>
<td>Software Security</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## The curriculum – Q3 & Q4

<table>
<thead>
<tr>
<th>Time</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:30-12:30</td>
<td>Hardware Security</td>
<td>Hardware Security</td>
</tr>
<tr>
<td>15:30-17:30</td>
<td>Cryptographic Engineering</td>
<td>Cryptographic Engineering</td>
</tr>
<tr>
<td>10:30-12:30</td>
<td>Cryptographic Protocols</td>
<td>Privacy Seminar</td>
</tr>
<tr>
<td>13:30-15:30</td>
<td>Verification of Sec. Protocols</td>
<td>Seminar TU/e</td>
</tr>
<tr>
<td></td>
<td>Verification of Sec. Protocols</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cryptographic Protocols</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## The curriculum – Q5 & Q6

<table>
<thead>
<tr>
<th>Time</th>
<th>Q5</th>
<th>Q6</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:30</td>
<td>(Princ. of Data Prot. Q1)</td>
<td>Physical Aspects of Digital Sec.</td>
</tr>
<tr>
<td>12:30</td>
<td></td>
<td>(can also be done in Q1)</td>
</tr>
<tr>
<td>13:30</td>
<td></td>
<td>Physical Aspects of Digital Sec.</td>
</tr>
<tr>
<td>15:30</td>
<td></td>
<td>(can also be done in Q1)</td>
</tr>
<tr>
<td>15:30</td>
<td>Physical Aspects of Digital Sec. (can also be done in Q1)</td>
<td>Applied Crypto (can also be done in Q2)</td>
</tr>
<tr>
<td>17:30</td>
<td></td>
<td>Applied Crypto (can also be done in Q2)</td>
</tr>
</tbody>
</table>

**Only electives. Opportunity for visits abroad**
Various registrations

• [Register for the "course" 2IMC91. Kickoff]

• Register as a “bijvak” student in Nijmegen
  • See TRU/e site for instructions.
    – You need “Bewijs Betaald Collegegeld”
      – Proof of paid tuition fee at TU/e
    – You need proof that you are qualified to follow the master courses at RU
      – e.g., because you have a Bachelors
  • Indicate if you don’t have an “OV kaart”

• Register at true-security.nl/admission/
Some IST graduates and their careers

- **Niels de Vreede**
  - Master’s project at TU Eindhoven
  - “Privacy-preserving biometric databases”
  - Afterwards: PhD student at TU Eindhoven

- **Eva Mwangi**
  - Master’s project at Philips Research Labs, Eindhoven
  - “Patient consent policies in XACML”
  - Afterwards: employed by ING bank, Amsterdam

- **Diego Ortiz Yepez**
  - Master’s project at IBM Zurich Labs
  - “Enhancing authentication in eBanking with NFC enabled mobile phones”
  - Afterwards: employed by IBM Zurich Labs

- **Ivo Pooters**
  - Master’s project at Fox-IT
  - “Forensic Data Acquisition from Symbian Smart Phones”
  - Afterwards: employed by Fox-IT
... IST graduates

• **Zhuo Chen**
  • Master’s project at Nedap
  • “Key Architecture and Updating Protocols in Large-scale Card-based Access Control Systems”
  • Afterwards: employed by Nedap

• **Henri Hambartsumyan**
  • Master’s project at Price Waterhouse Coopers
  • “Precise XSS Detection with Static Analysis using String Analysis”
  • Afterwards: employed by Deloitte

• **Simona Posea,**
  • Master’s project at Deloitte
  • "Renewal Periods for Cryptographic Keys"
  • Afterwards: employed by Deloitte
NOS journaal, 17 okt 2013:
"maar er is één sector waar de banen juist voor het oprapen liggen"

http://www.uitzendinggemist.nl/afleveringen/1374640
Circumvent Censorship By Using Bitcoin

(Ab)using Bitcoin for an anti-censorship tool

Media publicity

MSc thesis Krzysztof Okupski
Dec. 1, 2014

Student Aims to Boost Free Speech with
Bitcoin Messaging App

TU/e
Eindhoven University of Technology
Contact details

Boris Skoric
Security group / EIPSI
Dept. of Math. and CS
Office: MF 6.059
b.skoric@tue.nl

Berry Schoenmakers
Coding and Crypto group / EIPSI
Dept. of Math. and CS
Office: MF 6.103
berry@win.tue.nl
l.a.m.schoenmakers@tue.nl

ture-security.nl

www.win.tue.nl/eipsi/