UNIVERSITY OF TWENTE.

CYBER SECURITY SPECIALIZATION

Dr. Andreas Peter
Services, Cyber Security, and Safety Group
Why Cyber Security?

• Our world increasingly becomes digital and connected

• Cyber Security is BIG news: check the papers today

• Cyber Security is a BIG issue: 10% of our PCs are hijacked

• Cyber Security is BIG business: Patch Tuesday

• Graduates are in high demand!
Two Choices

- **3TU Cyber Security Specialization**
  - “High Tech, Human Touch”:
    Cyber Security Technology in context:
    Social, Psychological, Economical, and Legal
  - Industrial integration: courses, summer school, (optional) internships

- **EIT ICT Labs\(^1\) Master on Security & Privacy**
  - Double Degree (1\(^{st}\) or 2\(^{nd}\) year at an EU partner university)
  - 1\(^{st}\) year: technical basics, 2\(^{nd}\) year: specialization
  - Innovation & Entrepreneurship (I&E) basics

\(^1\) European Institute of Innovation & Technology
Cyber Security (Overview)

- Assessment of cyber risks and the design & implementation of countermeasures

- Three important Cyber Security measures
  - Prevention: for example using firewalls and awareness campaigns
  - Detection: for example using intrusion detection tools and data analytics
  - Recovery: for example using incident response methods and backups

- Cyber risk management: balancing the three measures to reach states of acceptable risk levels in various cyber domains.

- Multidisciplinary
  - Computer science core: for example cryptography, formal methods, secure software engineering, and machine learning
  - Supporting disciplines: for example law, economics, criminology, management, and psychology
Example (technical): Cyber Attacks

- What are cyber attacks and how do they work (e.g., hacking)?
- How can we prevent (e.g., firewalls), detect (e.g., data analytics), and recover from (e.g., backups) such attacks?
Attackers become more and more powerful, e.g., governments!

Edward Snowden
Example (socio-technical): Phishing

- What is phishing and how does it work (e.g., persuasion techniques)?
- How can we protect against it (e.g., awareness campaigns)?
Example (socio-technical): Phishing

- Phishing becomes more and more sophisticated, e.g., targeted attacks!

<table>
<thead>
<tr>
<th>Bank</th>
<th>Percentage of Phishing</th>
</tr>
</thead>
<tbody>
<tr>
<td>ING</td>
<td>41%</td>
</tr>
<tr>
<td>Rabobank</td>
<td>26%</td>
</tr>
<tr>
<td>SNS</td>
<td>21%</td>
</tr>
<tr>
<td>ABN Amro</td>
<td>8%</td>
</tr>
<tr>
<td>PayPal</td>
<td>4%</td>
</tr>
</tbody>
</table>

Targeted phishing on banks as reported to Fraudehelpdesk.nl.
In total (Oct 2014): 8850
UNIVERSITY OF TWENTE.
3TU CYBER SECURITY SPECIALIZATION

• Combines Cyber Security expertise of the 3 TUs
• Basic (core) courses (5 EC each, [TL] = tele-lectured)

<table>
<thead>
<tr>
<th>UT</th>
<th>TUD</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Cybercrime Science [TL]</td>
<td>[TL] Software Security (TU/e) –</td>
</tr>
<tr>
<td>– Computer Ethics</td>
<td>[TL] Cyber Risk Management –</td>
</tr>
<tr>
<td>– Machine Learning</td>
<td>[TL] Cyber Data Analytics –</td>
</tr>
</tbody>
</table>

• Joint elective courses (5 EC each, all tele-lectured [TL]):

<table>
<thead>
<tr>
<th>UT</th>
<th>TUD</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Biometrics</td>
<td>Economics of Security –</td>
</tr>
<tr>
<td>– Secure Data Management</td>
<td>Principles of Data Protection (TU/e) –</td>
</tr>
<tr>
<td>– Privacy-Enhancing Technologies</td>
<td>Software Testing and Reverse Engineering –</td>
</tr>
</tbody>
</table>

• Local elective courses (5 EC each):

<table>
<thead>
<tr>
<th>UT</th>
<th>TUD</th>
</tr>
</thead>
<tbody>
<tr>
<td>– Cyber Security Management [TL]</td>
<td>[TL] E-Law –</td>
</tr>
<tr>
<td>– Security Verification [TL]</td>
<td>[TL] Quantum Cryptography –</td>
</tr>
<tr>
<td>– ES and SCADA Security and Survivability</td>
<td>Applied Security Analysis “Hacking Lab” –</td>
</tr>
</tbody>
</table>

• Off-site Summer School (1.5 EC) where students solve a real cyber security problem

➢ Required is a minimum of 20 EC of core courses + Computer Ethics (5 EC)!
➢ Otherwise, free choices! Courses that are not listed can also be attended (→ program mentor)
### Sample Timetable

<table>
<thead>
<tr>
<th>Year 1 (60 EC)</th>
<th>Year 2 (60 EC)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Q1</strong></td>
<td><strong>Q1</strong></td>
</tr>
<tr>
<td>Cyber Risk Management</td>
<td>Software Security</td>
</tr>
</tbody>
</table>

- Individual timetables (→ program mentor: Pieter Hartel)
- Individual Final Degree Projects (socio-/purely technical, optional internship)
- Students can start in September or in February

*Bold = core course
Italic = socio-technical*
Overview

- Double Degree Master (1st or 2nd year at an EU partner university)
- Entry year: technical basics; exit year: specialization
- Innovation & Entrepreneurship (I&E) basics
- Mandatory Internship

Partner Universities

Entry + Exit: UNIVERSITY OF TWENTE.

**Cyber Security:**
High Tech, Human Touch

UNIVERSITY OF TRENTO - Italy

**Applied Security**

Exit Only:

**System Security**

TECHNISCHE UNIVERSITÄT DARMSTADT

**Information Security and Privacy**

UNIVERSITÄT DES SAARLANDES

**Advanced Cryptography**
Entry Year

- Mandatory courses (5 EC each)
  - Network Security
  - Security and Cryptography
  - Privacy Enhancing Technologies
  - I&E Business Development Lab (7 EC)
  - Elective courses (5 EC each):
    - Biometrics
    - Secure Data Management
    - Cyber Security Management
    - Security Verification
    - ES and SCADA Security and Survivability
    - Applied Security Analysis “Hacking Lab”
- Summer School on Security & Privacy after 1st year (3-6 EC)

Exit Year (Specialization: Cyber Security – High Tech, Human Touch)

- Mandatory courses (5 EC each)
  - Embedded System and SCADA Security and Survivability
  - Elective courses (5 EC each):
    - Biometrics
    - Secure Data Management
    - Cyber Security Management
    - Security Verification

**UNIVERSITY OF TWENTE.**  
**EIT ICT LABS SECURITY & PRIVACY MASTER**  
Sample Timetable (1st year OR 2nd year at UT)

<table>
<thead>
<tr>
<th>Year 1 (60 EC)</th>
<th>Year 2 (60 EC)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Q1</strong></td>
<td><strong>Q1</strong></td>
</tr>
</tbody>
</table>

- Individual timetables (→ program mentor: Pieter Hartel)  
  (→ program coordinator: Andreas Peter)

- Individual Final Degree Projects (socio-/purely technical)

**Bold = mandatory**  
**Italic = I&E part**
Examples (technical):

- “C&C botnet detection over SSL” (at Security Matters)
- “Drone Security” (at KPMG)
- “Detecting botnets using file system indicators” (at NHTCU of Dutch police)

Examples (socio-technical):

- “The Impact of Cyber Security on SMEs” (at Bicore)
- “Secure and privacy-preserving national eID systems with Attribute-based credential technologies” (at NXP)
- “Cognitive Cryptography: Planting a Password into a Person’s Brain without Him Having Any Conscious Knowledge of the Password” (local)
Typical job titles of graduates would be:

- Computer and network security specialist
- Developer
- Digital expert police
- Entrepreneur and security consultant
- Entrepreneur and developer
- Ethical hacker
- Information security advisor
- Lead engineer
- Management consultant
- PhD student
- Researcher IT-innovations
- Security & privacy consultant
- Security analyst
- Senior analyst and test consultant
- Software engineer
- Teacher
- Technical consultant
UNIVERSITY OF TWENTE.
SECURITY MASTER

Interested?

http://www.utwente.nl/en/education/master/

- 3TU Cyber Security Specialization
  http://www.3tu.nl/cybsec/en/course-program/

- EIT ICT Labs Master on Security & Privacy
  http://www.masterschool.eitictlabs.eu/programmes/sap/