- System Security
- Reverse Engineering
- Security Testing
- Botnets + malware

(Unless you are really good and extremely motivated)

Herbert Bos
herbertb@cs.vu.nl
www.cs.vu.nl/~herbertb/
System Security

- Protecting + attacking programs
- Systems + networking perspective
- Examples:
  - BinArmor : USENIX’12
  - Minemu : RAID’11
  - Slower is Faster : USENIX’13
Reverse Engineering

- Rosetta project
- Start from data structures
- Examples
  - Howard : NDSS’11
  - MemPick : WCRE’13
  - MemBrush : WCRE’13
Security Testing

- New approach: Dowsing
- Find code likely to be vulnerable first
- Use symbolic execution to test this code
- Examples
  - Dowser : USENIX Security’13
Botnets + malware

- Reverse engineer, study, dismantle
- Focus on state of the art
- Examples
  - P2Pwned: Security & Privacy’13
  - Prudent Practices: Security & Privacy’12
  - Highly resilient botnets are here: Malware’13

- Project:
  - client-side honeypot for smartphones
  - [http://tracedroid.few.vu.nl/](http://tracedroid.few.vu.nl/)
External: Splunk

- Splunk: solution to make sense of lots of data
  - Write new applications against the API
  - Technical and less technical

- Company:
  - SMT (The Hague)
External: KPMG

- KPMG: pentesting etc.
- Looking for motivated students

- Company:
  - Amstelveen