Internet voting topics for crypto seminar

Sven Heiberg, Jan Willemson {sven,janwil}@cyber.ee

September 8th 2014

Attack tree based risk analysis of i-voting

- Attack tree is a method of structured attack presentation
- In 2014, two MSc theses presenting attack tree based analysis of Estonian Internet voting solution were defended
  - Tanel Torn, Tallinn University of Technology, Estonia, *Security analysis of Estonian i-voting system using attack tree methodologies*
  - Ruud Verbij, University of Twente, Netherlands, *Dutch e-voting opportunities*
- Both also attempt quantitative analysis of the proposed trees
- The task is to work through the relevant parts of the theses, compare the parameter assessment methodologies and, if possible, unify the results

End-to-end verification in remote electronic voting

- There exist several implementations of individually and universally verifiable remote electronic protocols, e.g.
  - Helios (`https://vote.heliosvoting.org/`) and
  - UniVote (`https://www.univote.ch/voting-client/`)
- The student would have to work with one of these protocols/implementations – understand its details and assess the degree of E2E provided by the solution using the method provided by Popoveniuc et al. (Performance Requirements for End-to-End Verifiable Elections, `https://www.usenix.org/legacy/event/evtwote10/tech/full_papers/Popoveniuc.pdf`)