System Security

Intro

Giovanni Russello

g.russello@auckland.ac.nz

http://www.cs.auckland.ac.nz/compsci725s2c/

First Part Coverage

- Basic notions
  - Authentication and Authorisation
  - Crypto primitives
- Research Topics
  - Smartphone security (very basic)
  - Security and Privacy in the Cloud

What are the Goals Software Security?

- Building a software system that is dependable and predictable when is:
  - Under malicious attacks
  - Under erroneous usage
  - Under unexpected circumstances

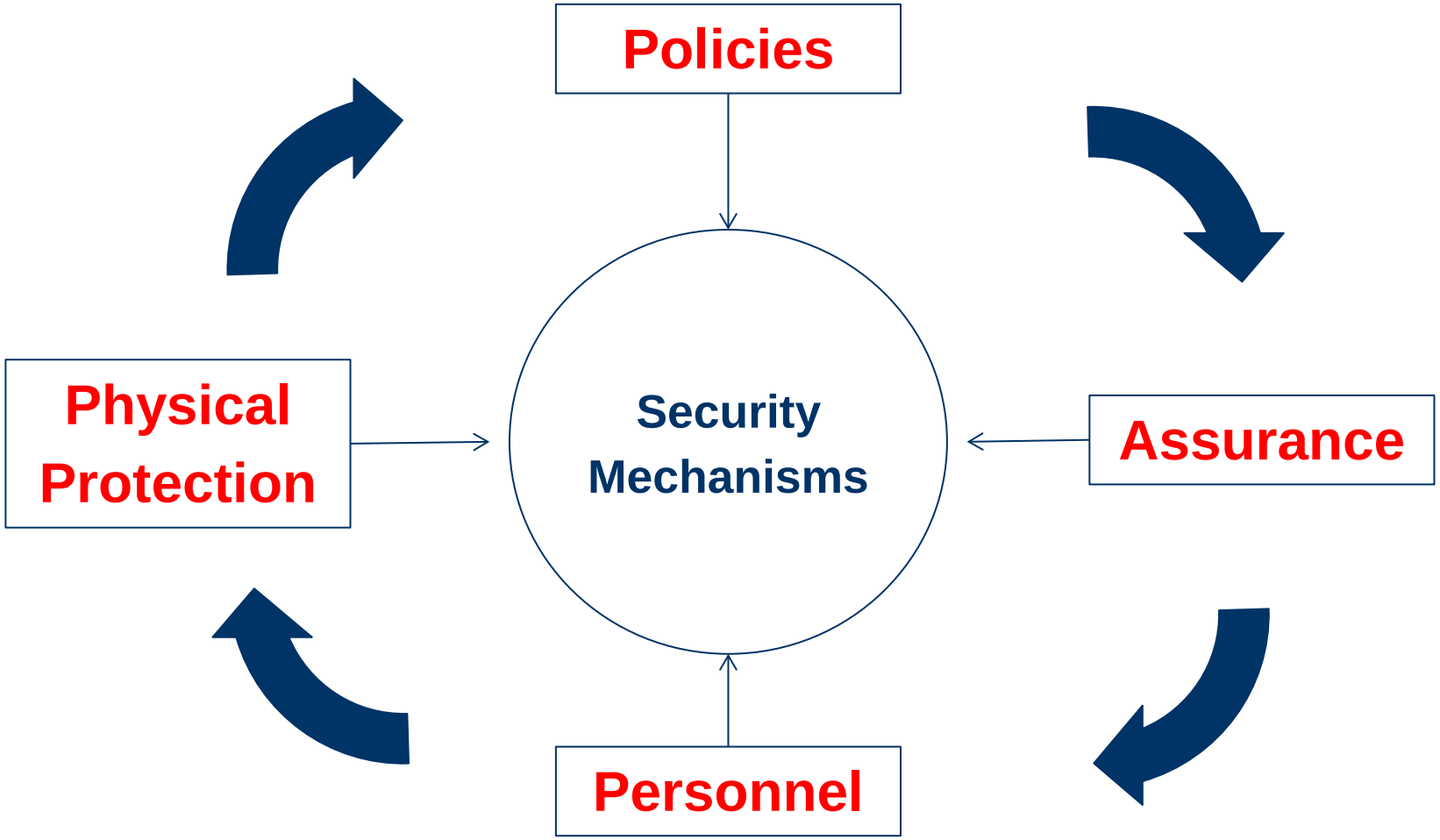
Multi Disciplinary Expertise

- Software Engineering only part of the game
  - Deals with errors and mischances
- Security Engineering needs to deal with malicious actions
- Requires knowledge of cryptography, tamper-resistant hardware, formal methods, applied psychology, economics, and laws

Satisfy Security Needs

- Analysis of the threats and requirements
- Identify right tools for the job:
  - Authentication, authorisation, integrity, fault-tolerance, data secrecy
  - Use correct/appropriate mechanism for each need
- Take into account USABILITY
  - Asking for SU permissions to connect to a WiFi might be over-killing

Security Framework



Weakest Link

- Technology is not the only factor
- Humans in the loop means:
  - Social Engineered attacks
  - Psychology
  - Personal reasons/motivations
- Attackers will target the most cost/effort effective vulnerability in your system

Resources

- Security Engineering – Ross Anderson
  - Available from the web
- Chapter 1: http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf
- Chapter 2: http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf