PV204 Security technologies

Team projects

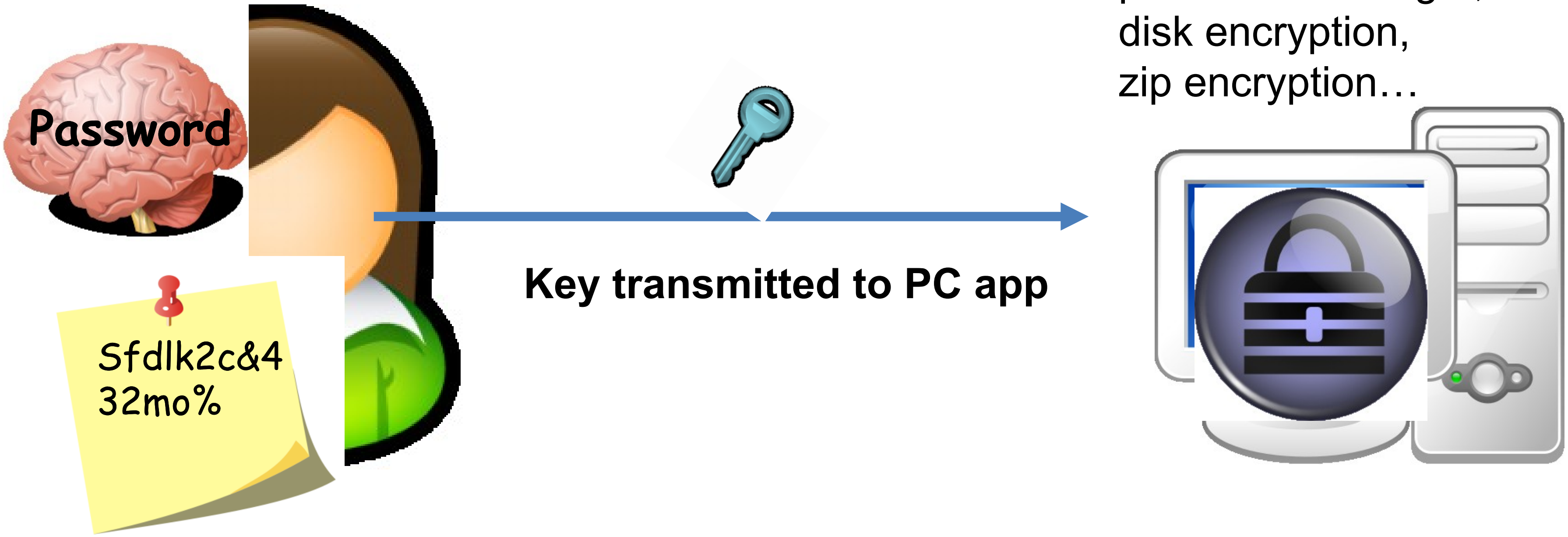
Petr Švenda
Faculty of Informatics, Masaryk University, Brno, CZ

CROCS
Centre for Research on
Cryptography and Security

Situation before your project

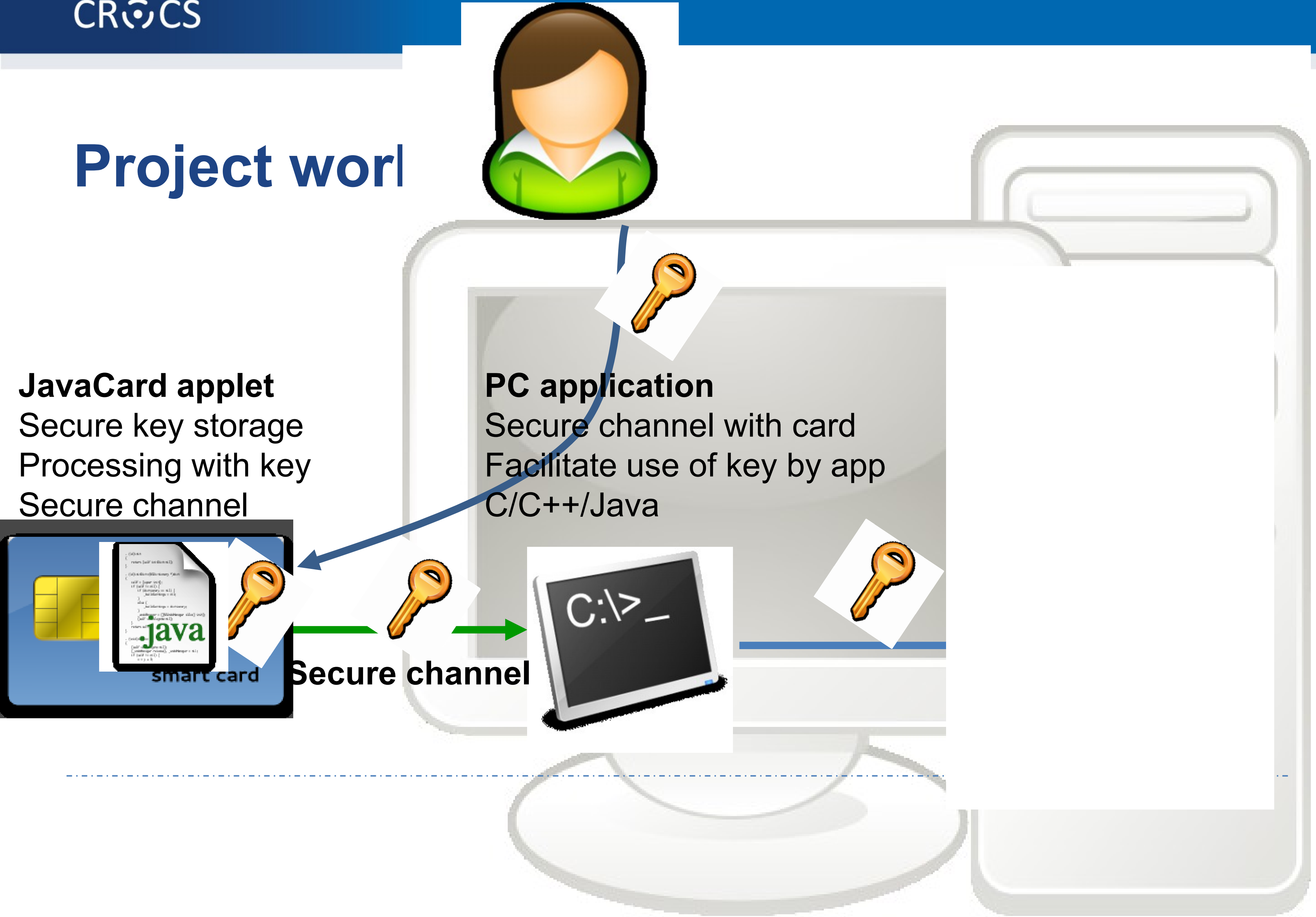
User stores keys
Memory, paper…

Open-source application
password manager,
disk encryption,
zip encryption…



Key transmitted to PC app

Project worl



JavaCard applet
Secure key storage
Processing with key
Secure channel

PC application
Secure channel with card
Facilitate use of key by app
C/C++/Java

Project

1. Identify suitable target scenario with need for cryptographic keys (disk encryption, remote authentication, DRM app…)
   - Open-source application
2. Design and implement JavaCard smart card applet
   - Storage and processing of secrets (keys)
   - Authentication and secure channel with PC application
   - Source code and installation scripts provided to other teams (code review)
3. Design and implement PC-based counterpart application
   - Establish secure channel with smart card applet
   - Transmit key from card or transmit data for processing by other team
   - Provide full dump of communication to other teams (reverse engineering)
4. Review implementations of other teams
   - Source code review of other team applet
   - Reverse-engineer of other team application dump

Teams

- 3 people per team
  - Assigned by us (within group), available in IS
- Start working early, especially with implementation
  - Distribute work load between all members
  - Use GitHub platform frequently (push often, your evaluation will be partially based on your participation)
- Teams may use own existing code from previous assignments (SimpleApplet etc.)

Projects - timeline

1. Identify target scenario, design of applications
   - 7 points (before 15th of April)
   - Report (max. 2 pages A4)
2. Write code (GitHub)
   - 13 points (before 5th of May)
   - JavaCard application, PC-based application
   - Design, code + presentation (5.5.2016, your seminar group, random team member)
3. Review and attack implementations
   - 10 points (before 19th of May)
   - Review and attack implementations of other teams
   - Report + presentations (19.5.2016, random team member)

- At least 15 points from project are required