

■ Protecting Computer Applications

Wim Mooij



Protecting Tangible Items

- Diamonds, money, documents, valuables
- Owners want protection against damage and theft
- Store in protected container
 - safe, vault, strongbox
- Safe strength rating has various gradations
 - based on time needed, tools used and expertise of attacker

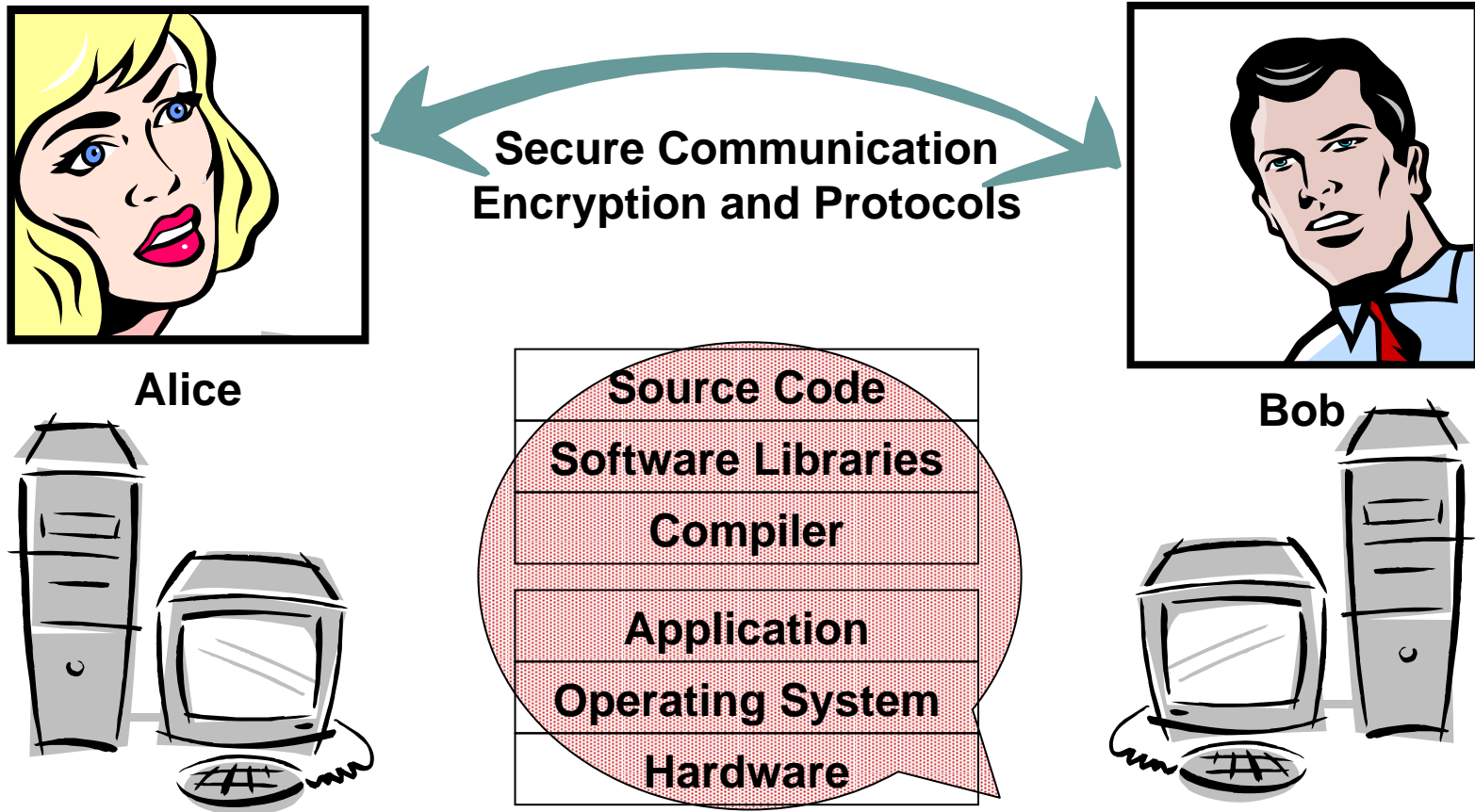
Protecting Electronic Items

- Files, Contracts, Static Data, Communication Links, Software Applications
- Owners want protection against tampering and theft
- Encrypt the digital information
 - DES, AES and many others
- Encryption Strength is binary property
 - broken or not yet broken
- Well understood and mature scientific field

Issues in Protecting Electronic Items

- Sharing Protected Virtual Items
 - Protected copy
 - Decryption means
- Sharing decisions for Protected Virtual Items
- Judgement on reliability of a person
 - People know how to do this
- Judgement on reliability of a computing infrastructure
 - A very hard problem
 - Many important commercial applications

Protecting Security Applications



Tamper Resistance

- Aims to create a reliable computing environment
- Equivalent to an “oracle” or a “black box”
 - Input and output
 - Some processing capability
- Protects applications against damage and theft
- Can be in hardware
 - smart cards, secure tokens
- Can be in software
 - white box crypto, obfuscation



Application Areas

- Protect applications from modifications and copying
 - games, banking, DRM, secure OS
- Provision of a reliable computing environment
 - embedded devices, Java Card
- Reliability extension
 - increase reliability of other applications that are in the same computing environment
 - trusted computing

Research Areas

- Hardware Tamper resistance
 - virtual smartcard design and attack environment
 - strength metrics for hardware tamper resistance
 - prove or disprove the existence of an unbreakable hardware “black box”
- Software tamper resistance
 - obfuscation methods and reverse engineering
 - whitebox cryptography
 - strength metrics for software obfuscation
- Reliable computing environments