Queen Mary
University of London

BIRMINGHAM CITY
University

Information Security: Goals and Enabling Technologies

Ali E. Abdallah

Professor of Information Security

Birmingham City University

Email: Ali.Abdallah@bcu.ac.uk

With thanks to Professors Anne Flanagan and Ian Walden

Lectures are part of the project:

ConSoLiDatE
Multi-disciplinary Cooperation for Cyber Security, Legal and Digital Forensics Education

Funded by The Higher Education Academy

December 2014-March 2016

BIRMINGHAM CITY University

Queen Mary University of London

Enabling Technical Concepts and Mechanisms

Enabling technical concepts

- Cryptography
- Access control
- Security protocols
- Secure software
- Trust

The Cast of Characters

- Alice and Bob are "honest" players.

- Malory is a generic "intruder".

Bob's Online Bank

- Bob opens Bob's Online Bank (BOB)
- What are Bob's security concerns?
- If Alice is a customer of BOB, what are her security concerns?
- How are Alice and Bob concerns similar? How are they different?
- How does Malory view the situation?

Bob's Online Bank

- Bob opens Bob's Online Bank (BOB)
- What are Bob's security concerns?
- If Alice is a customer of BOB, what are her security concerns?
- How are Alice and Bob concerns similar? How are they different?
- How does Malory view the situation?

Confidentiality

- **Confidentiality:** prevent unauthorized disclosure of information
- BOB must prevent Malory from learning Alice's account balance

Integrity

- **Integrity:** prevent unauthorized writing of information
- Malory must not be able to change Alice's account balance
- Alice must not be able to improperly change her own account balance

Availability

- **Availability:** Data is available in a timely manner when needed
- BOB's information must be available when needed
- Alice must be able to make transactions
  - If not, she'll take her business elsewhere

Enabling Technology: cryptography

- How does Bob 's computer know that "Alice" is really Alice and not Malory?
- Alice's password must be verified
  - This requires some clever **cryptography**
- What are security concerns of passwords?
- Are there alternatives to passwords?

Enabling Technology: Protocols

- When Alice logs on, how does BOB know that "Alice" is really Alice?
- Unlike standalone computer case, network security issues arise
- What are network security concerns?
- **Protocols** are critically important and crypto plays an essential role defining these protocols

Enabling Technology: Authentication

Protocols are based on:

- Something you **know** (a PIN, or password).
- Something you **have**:
  - secureID card or other token, generating a one-time password.
  - a key imbedded in a `secure area' on host machine, in browser software, etc.
  - a smartcard (which may have keys imbedded and can perform cryptographic operations on behalf of a user).
- Something identifies **where** you are.
  - IP address
  - GPS
- Something you **are** (a biometric).
  - fingerprints,
  - retinal characteristics

Enabling Technology: *Authorization*

- Once Alice is *authenticated* by BOB, then BOB must restrict actions of Alice
  - Alice can't view Charlie's account info
  - Alice can't install new software, etc.
- Enforcing these restrictions is known as *authorization*
- **Access control** includes both authentication and authorization

Enabling Technology: secure software

- Cryptography, protocols, and access control are implemented in **software**
- What are security issues of software?
  - Most software is complex and buggy
  - Software flaws lead to security flaws
  - How to reduce flaws in software development?

Enabling Technology: Anti-Virus

- Some software is intentionally evil
  - Malware: computer viruses, worms, etc.
- What can Alice and Bob do to protect themselves from malware?
- What can Malory do to make malware more "effective"?

Enabling Technology: Trust?

- Operating systems enforce security
  - For example, authorization
- OS: large and complex software
  - Win XP has 40,000,000 lines of code!
  - Subject to bugs and flaws like any other software
  - Many security issues specific to OSs
- Can you **trust**:
  - An operating system? Hardware chips?
  - How about insiders, administrators or cloud operators?

Enabling Technology: Trust?

www.bbc.co.uk/news/technology-19585433

BBC Sign in News Sport Weather iPlayer TV Radio More... Search

NEWS TECHNOLOGY

Home World UK England N. Ireland Scotland Wales Business Politics Health Education Sci/Environment Technology Entertainment & A

13 September 2012 Last updated at 15:51

5.2K Share

Malware inserted on PC production lines, says study

Cybercriminals have opened a new front in their battle to infect computers with malware - PC production lines.

Several new computers have been found carrying malware installed in the factory, suggests a Microsoft study.

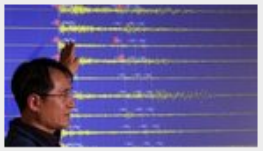
One virus called Nitol found by Microsoft steals personal details to help criminals plunder online bank accounts.

Microsoft discovered four factory fresh PCs that were pre-infected with malware

Microsoft won permission from a US court to tackle the network of hijacked PCs made from Nitol-infected computers.

Related Stories

Top Stories



North Korea nuclear devi

'Forced labour' claim wins on appea

Benedict vows 'not to interfere'

Barclays announces 3,700 job cuts

Minister calls second meat summit

Features

Radical decad

What happened in change the Pope?

Driving data

Think Like Malory

- Good guys must think like bad guys!
- A police detective
  - Must study and understand criminals
- In information security
  - We want to understand Malory's motives
  - We must know Malory's methods
- "It's about time somebody wrote a book to teach the good guys what the bad guys already know." — Bruce Schneier

Key questions

- Which information assets are we trying to protect?
- What are they worth to the business?
- What's the impact if we lost Confidentiality, Integrity or Availability of these?
- How do we mitigate the risk? – which controls
- What's the cost?

Security Journey

- An ongoing dynamic journey – never done must constantly tune program
- Must protect against current known threats as well as preparing for threats not yet.
- Security program must encompass defense in depth
- The cost of protection must align with value of asset
- Tension between security and usability

Investigations

- For each attack case study outlined in the lecture, investigate the following characteristics:
  - Which security goal was violated?
  - Source
  - Target
  - Means
  - Sophistication
  - Impact
- Comment on how the attack could have been avoided?

Questions???