# SECURITY IN COMPUTING, FIFTH EDITION

## Chapter 13: Emerging Topics

# Chapter 13 Objectives

- Define the Internet of Things and discuss associated emerging security issues
- Discuss nascent efforts to financially measure cybersecurity to make sound investment decisions
- Explore the evolving field of electronic voting, which has been an important and open security research problem for over a decade
- Study potential examples of cyber warfare and their policy implications

# The Internet of Things (IoT)

- IoT refers to the connection of everyday devices to the Internet, making a world of so-called smart devices
- Examples:
  - Smart appliances, such as refrigerators and dishwashers
  - Smart home, such as thermostats and alarm systems
  - Smart health, such as fitness monitors and insulin pumps
  - Smart transportation, such as driverless cars
  - Smart entertainment, such as video recorders
- Potential downsides:
  - Loss of privacy
  - Loss of control of data
  - Potential for subversion
  - Mistaken identification
  - Uncontrolled access

# Smartphones

- Smartphones are the control hub of the IoT
- In 2013, Kaspersky Labs identified 143,211 distinct new forms of malware against mobile devices
- 98% targeted Android devices, far in excess of its market share
  - Android, unlike its competitors, does not limit the software users are allowed to install and is thus an easier target
- Apple, in contrast, only allows apps from its app store to be installed on its smartphones
  - All apps go through an approval process, which includes some security review
  - Once approved, apps are signed, using a certificate approach similar to that described in Chapter 2

# Economics

- Cybersecurity planning includes deciding how to allocate scarce resources for investing in security controls
- Making a business case:
  - A description of the problem or need to be addressed
  - A list of possible solutions
  - A list of constraints on solving the problem
  - A list of underlying assumptions
  - An analysis of the risks, costs, and benefits of each alternative
  - A summary of why the proposed investment is a good idea

# Influences on Cybersecurity Investment

| Categories of Influence | Average Percentage Across Organizations |
|---|---|
| Regulatory requirement | 30.1 |
| Network history or information technology staff knowledge | 18.9 |
| Client requirement or request | 16.2 |
| Result of internal or external audit | 12.4 |
| Response to current events, such as media attention | 8.2 |
| Response to compromised internal security | 7.3 |
| Reaction to external mandate or request | 5.0 |
| Other | 1.7 |

# Quantifying Security

- Cybersecurity threats are impossible to accurately quantify and estimate
  - How do you predict the likelihood that a hacker will attack a network, and how do you know the precise value of the assets the hacker will compromise?
- While many industrial surveys collect cybersecurity incident data, they are inconsistent on key issues:
  - No standards for defining or categorizing security incidents
  - Disagreements about sources of attack
  - Selection bias among respondents
- Useful data for decision making, such as rates and severity of attacks, cost of damage and recovery, and cost of security measures, are not yet known with any accuracy

# Electronic Voting

- Confidentiality
  - We want to be able to cast a ballot without revealing our votes to others.
- Integrity
  - We want votes to represent our actual choices and not be changed between the time we mark the ballot and the time our vote is counted. We also want every counted ballot to reflect one single vote of an authorized person. That is, we want to be able to ensure that our votes are authentic and that the reported totals accurately reflect the votes cast.
- Availability
  - Usually, votes are cast during an approved pre-election period or on a designated election day, so we must be able to vote when voting is allowed. If we miss the chance to vote or if voting is suspended during the designated period, we lose the opportunity to cast a vote in the given election.

# What Is a Fair Election?

- Each voter's choices must be kept secret.
- Each voter may vote only once and only for allowed offices.
- The voting system must be tamperproof, and the election officials must be prevented from allowing it to be tampered with.
- All votes must be reported accurately.
- The voting system must be available for use throughout the election period.
- An audit trail must be kept to detect irregularities in voting but without disclosing how any individual voted.

# Cyber Warfare

- Open questions:
  - When is an attack on cyber infrastructure considered an act of warfare?
  - Is cyberspace different enough to be considered a separate domain for war, or is it much like any other domain (e.g., land, sea, or air)?
  - What are the different ways of thinking about cyber war offense and defense?
  - What are the benefits and risks of strategic cyber warfare and tactical cyber warfare?

# Possible Examples of Cyber Warfare

- Estonia
  - Beginning in April 2007, the websites of a variety of Estonian government departments were shut down by multiple DDoS attacks immediately after a political altercation with Russia.
- Iran
  - The Stuxnet worm attacked a particular model of computer used for many production control systems, and all the infections could be traced back to domains within Iran linked to industrial processing.
- Israel and Syria
  - Missiles fired in 2007 by Israeli planes did not show up on Syrian radar screens because software had replaced live images with fake, benign ones.
- Canada
  - In January 2011, the Canadian government revealed that several of its national departments had been the victims of a cyber attack traced back to servers in China.
- Russia
  - According to the *New York Times*, Russian hackers infiltrated the computers of various national governments, NATO, and the Ukraine.

# Summary

- The IoT has resulted in a flood of new devices connecting our private and personal lives to the Internet but is far from mature from a security and privacy perspective
- Cybersecurity investment decision making remains challenged by our inability to accurately measure risk and vulnerability
- After over a decade of research and practice, electronic voting remains an unsolved research problem
- Cyber warfare continues to lack clear definition and presents critical challenges, including attribution