CIS 4360
Secure Computer Systems

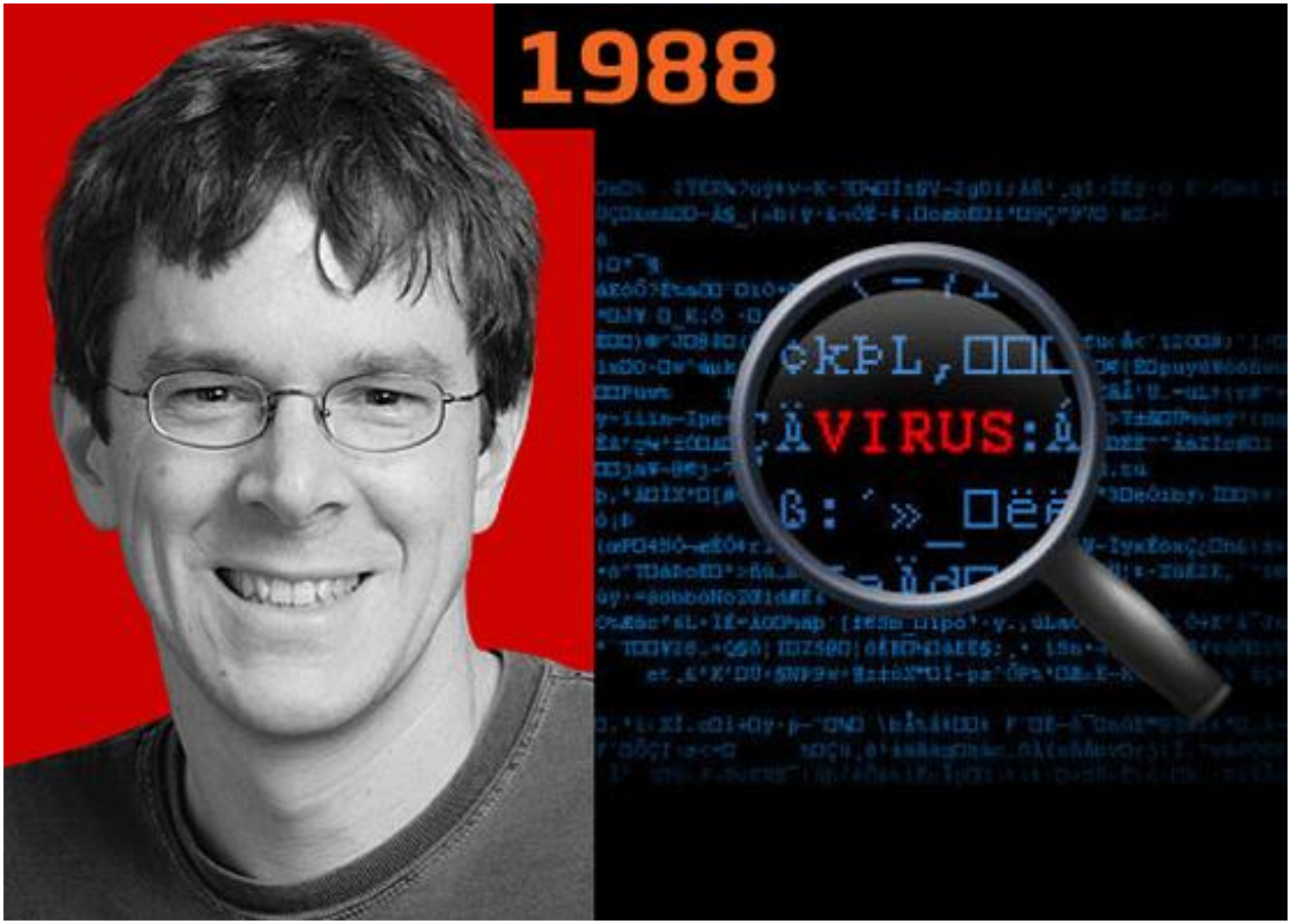
Introduction

Professor Qiang Zeng

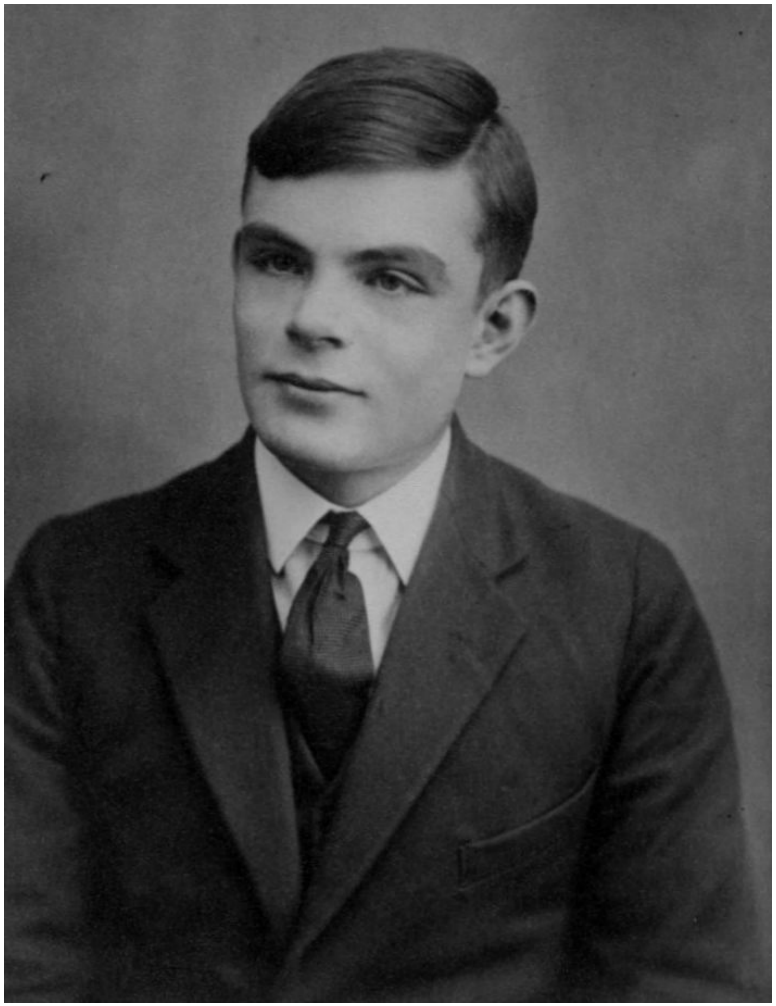
Spring 2017

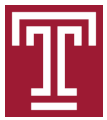
Story 1: Malware, *Stuxnet*, took down Iran's nuclear facilities (2009)

Story 2: Morris – the first worm in history



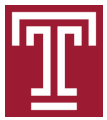
Story 3: Turing's cryptanalysis saved 14 million lives in WW2 (around 1940)





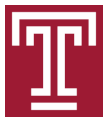
Story 4: Hackers remotely control 1.4 million Chrysler cars (2015)

Story 5: One billion Yahoo user accounts hacked (2016)



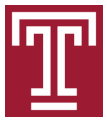
Stories in future

- Smart homes/buildings/hospitals
- Self-driving cars
- Drones
- Robots
- …



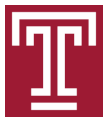
About me

- PhD in CSE, Penn State University
- Research interest: Systems Security
- Industry experiences:
  - IBM Watson Research Center
  - NEC Lab America
  - Yahoo
  - Symantec



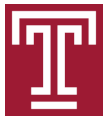
Goals of this course

- Students get to
  - understand important security principles and concepts
  - learn about commonly used attacks
  - assess threats to a given system
  - master methodologies to build secure systems
- Not a hacking course
  - How to write malware & launch attacks is not our goal



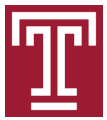
Ethics Statement

- This course will discuss various attacks and the technologies used. As an instructor, I oppose any abuse of those technologies and only advocate ethical use. Unethical use includes the act of circumventing existing security and privacy measures for any purpose, and disseminating or exploiting system vulnerabilities.
- Any violation will be reported to the proper authorities and may result in dismissal from the class or the college



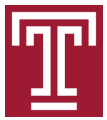
Example topics of this course

- Authentication and security policies
- Cryptography and its applications
- Memory corruption attacks, file system attacks,
- Trusted computing; sandboxing; virtualization
- Social engineering; biometrics; Web security



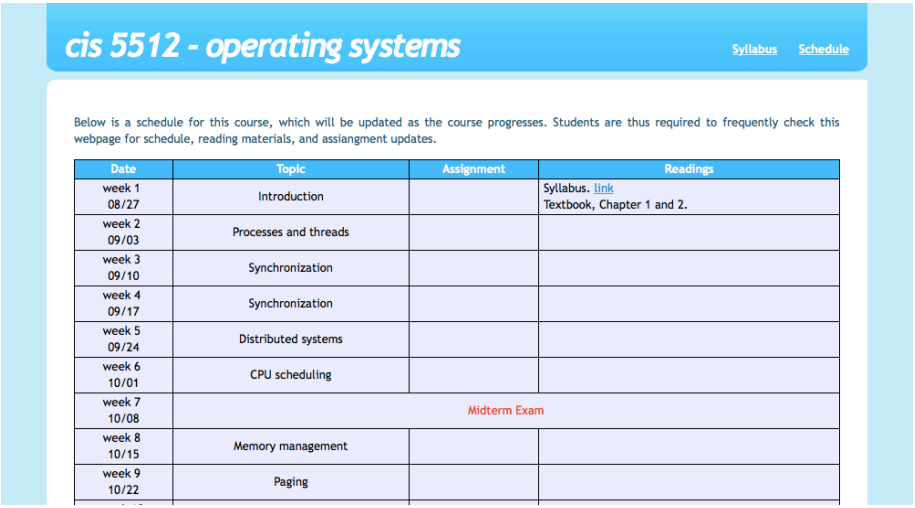
Course prerequisites

- Architectures and systems basics
  - CIS 3207 or CIS 5012
- C and Java programming



Course website

- http://cis.temple.edu/~qzeng/cis4360-spring17/
- Please check this website frequently for updates of assignments, readings, and slides
- Readings ahead of classes are required

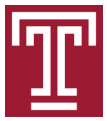


cis 5512 - operating systems

Syllabus Schedule

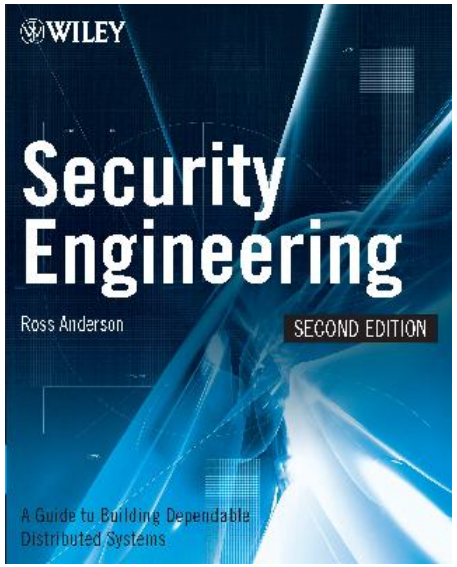
Below is a schedule for this course, which will be updated as the course progresses. Students are thus required to frequently check this webpage for schedule, reading materials, and assiangment updates.

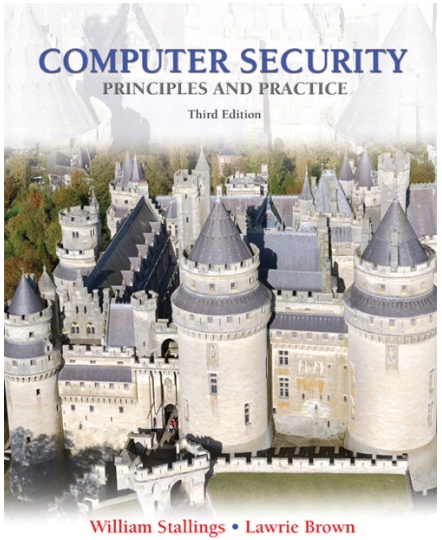
Date	Topic	Assignment	Readings
week 1 08/27	Introduction		Syllabus. link Textbook, Chapter 1 and 2.
week 2 09/03	Processes and threads		
week 3 09/10	Synchronization		
week 4 09/17	Synchronization		
week 5 09/24	Distributed systems		
week 6 10/01	CPU scheduling		
week 7 10/08	Midterm Exam		
week 8 10/15	Memory management		
week 9 10/22	Paging		



Textbooks

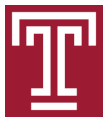
- Required
  - "Security Engineering", Ross Anderson, 2nd edition, 2008
    - Comprehensive content; many topics are touched but not deeply explained, though.
    - E-book: https://www.cl.cam.ac.uk/~rja14/book.html
- Recommended
  - "Computer Security: Principles and Practice", Stallings and Brown, 3rd edition, 2014
    - Interpret theories and concepts well





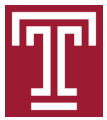
Grading

- Midterm (35%)
- Final (45%)
- Assignments (20%)
  - Two project assignments
  - Cheating will lead to “F” for the whole course
  - Late submission will be rejected directly; no excuse



Office Hours

- Tuesday and Thursday 2:30-3:30pm, SERC 328
- Feedback, comments, and in-classroom interaction are encouraged



Security objectives: the CIA Triad

Confidentiality

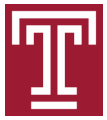
- No illegal read or unintended privacy disclosure

Integrity

- No illegal write (modification or destruction) or program execution (e.g., executing malicious code); and nonrepudiation (i.e., cannot deny)

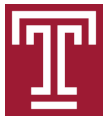
Availability

- Ensuring legal read, write, and execution



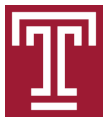
Questions

- In the case of “Snowden”, what did the NSA (National Security Agency) fail to achieve among the CIA triad?
  - Confidentiality
  - But do you know why Snowden disclosed the “mass surveillance” project?
- In the case of “Stuxnet”, what was violated among the CIA triad in the perspective of Iran?
  - Integrity: the integrity of the industrial control system was ruined
  - Confidentiality: private information was transmitted to the US
  - Availability: their nuclear facilities could not run as expected
- In the Morris attack, the Internet traffic jams were caused (for transmitting the worm code). How did it affect the security of uninfected computers?
  - Availability: they could not access the Internet as usual



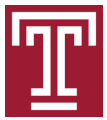
Threats

- A threat is a potential means or incident that may cause security breach or harms
  - A computer may be infected with virus when you insert a USB drive (so, virus infection is a threat)
  - Your laptop may be stolen when you leave it in the lib
  - An earthquake may destroy all the storage in a data center
  - Your telephone my be tapped and lead to eavesdropping
- A risk is to describe the consequences (and sometimes the likelihood) due to a realized threat
  - A risk exists due to threats



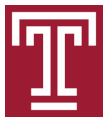
Vulnerabilities

- A vulnerability is a security flaw
- What are the sources of vulnerabilities?
  - Hardware or software bugs
  - Bad design: e.g., magnetic stripe credit card
  - Bad policies: e.g., allowing USB at nuclear facilities
  - Configuration: e.g., router password as “admin”
  - Human



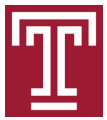
Attack

- An attack is an attempt to cause security breaches or harms; for example,
  - Password Guessing
  - Sending a large volume of requests to a service to attain Denial of Service (DoS)



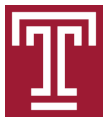
Categorization of attacks

- In the context of communication, we have Passive attacks and Active attacks
  - Passive attacks: eavesdropping or monitoring without interfering with the system operations
  - Active attacks affect the system operations by, e.g., forging, replaying, or modifying messages
- Insider attacks vs. Outsider attacks
  - Insider attacks are launched by authorized system users (typically, the employees), e.g., Snowden



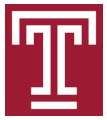
Compromises and Countermeasures

- A compromise occurs when some resource is taken over or altered when *an attack succeeds*
- A countermeasure is a measure (e.g., *action, device or policy*) used to discover or prevent attacks or to mitigate the harms due to attacks



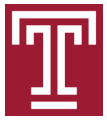
Attack Vectors

- An attack vector is the route or method to deliver an attack
  - A USB drive containing virus is “left” on the road; the USB drive is the attack vector in the attack
  - When emails are used to disseminate virus, sending emails is the attack vector
  - In the case of DoS attacks, sending (the large volume of) requests is the attack vector



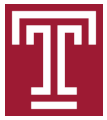
Exploits and Payload

- An exploit is specially crafted code or input that takes advantage of one or multiple vulnerabilities
  - E.g., a PDF file may contains some code used to hijack the control flow of the PDF reader
- An exploit usually contains a payload that is executed to achieve the attacker's goal after a system is compromised, e.g., sending back private info to attackers or destroying all the files
  - Q: What is the payload in the Stuxnet attack?
  - A: Malicious code that controls the speed of cetrifuge machines



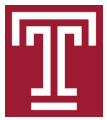
Attack Vectors, Exploits, vs. Payloads

- An attack vector is used to deliver an attack
- An exploit is used to deliver the payload
- Q: Does an attack always rely on some exploit?
- A: No, an attack may or may not make use of an exploit; for example,
  - Some DDoS attacks do not contain exploits
  - When you manually try passwords for password guessing attacks, there is no exploit



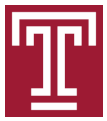
Example

- In the Stuxnet attack, what is the attack vector?
- Worm propagation through Internet and USB
- What is the exploit?
- Worm (will be covered in this course)
- What is the payload?
- Code that identifies and controls the Iran nuclear facilities



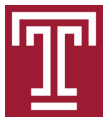
Summary

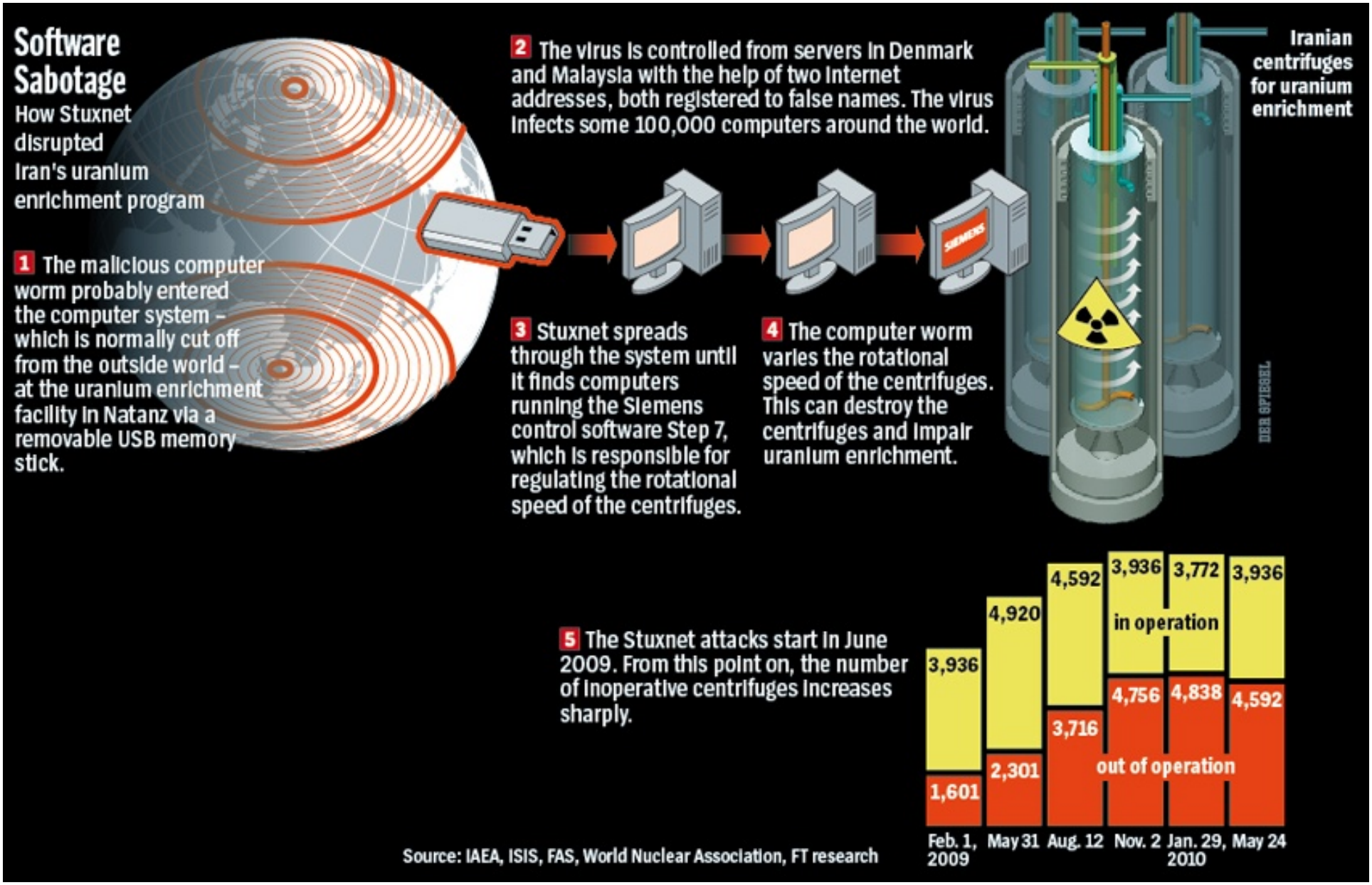
- The CIA Triad as security objectives
- Threat: *potential (means of incident)*
- Risk: *consequences*
- Attack: an *attempt*
- Compromise: *successful attacks*
- Attack Vectors vs. Exploits vs. Payloads



Writing Assignments

- Stuxnet and Morris are all famous attack examples
  - Please give another example of famous attacks you find interesting
  - Analyze which of the CIA objectives are violated in the example
  - Describe the Attack Vector, Exploit, and Payload in the example
  - Describe the Vulnerabilities exploited during the attack
- Compare Attack Vector, Exploits, and Payload




Software Sabotage
How Stuxnet disrupted Iran's uranium enrichment program
1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.
2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.
3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.
4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.
Iranian centrifuges for uranium enrichment
5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.
in operation
out of operation
3,936
4,920
4,592
3,936
3,772
3,936
1,601
2,301
3,716
4,756
4,838
4,592
Feb. 1, 2009
May 31
Aug. 12
Nov. 2
Jan. 29, 2010
May 24
Source: IAEA, ISIS, FAS, World Nuclear Association, FT research