

CSC429 – Computer Security

LECTURE 1
COURSE OVERVIEW

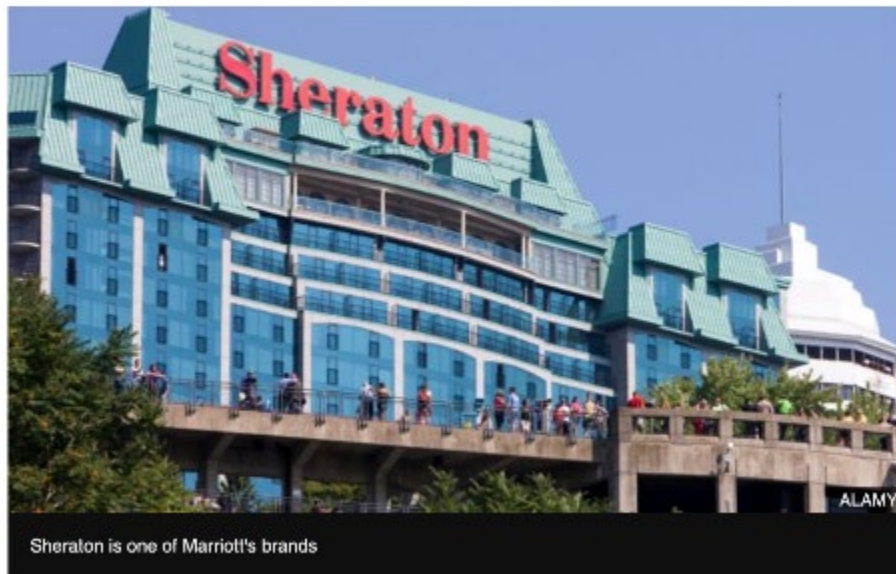
Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Why Security?

Marriott hack hits 500 million Starwood guests

🕒 30 November 2018

f 🗨️ 🐦 ✉️ ➦ Share



The records of 500 million customers of the hotel group Marriott International have been involved in a data breach.


Even Locally

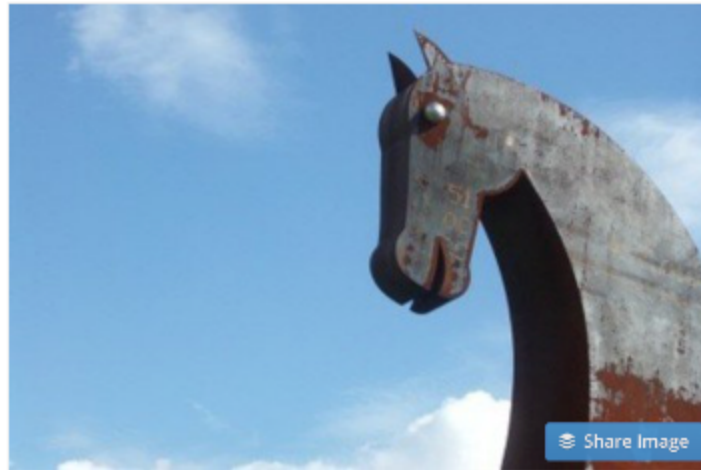
Security

Hack on Saudi Aramco hit 30,000 workstations, oil firm admits

First hacker-style assault to use malware?

By [John Leyden](#) 29 Aug 2012 at 09:18

4  SHARE ▼



Analysis Saudi Aramco said that it had put its network back online on Saturday, 10 days after a malware attack flooded 30,000 workstations at the oil giant.

Causes of Computer Security Incidents

- Buggy software and wrong configurations...
 - Complex programs
 - Security considered an add-on rather than fundamentally built-in.
- Lack of awareness and education
- Usability
 - Security sometimes makes things harder to use [a trade-off]
- Economic factors
 - Consumers do not care about security.
 - Security is difficult, expensive and takes time.
- Geo-political conflicts
- Human nature

Human Factors

- Who are the attackers?
 - Individual
 - Insiders, criminals, ..
 - Organizations
 - Espionage, surveillance, ...
 - Governments
 - Conflict, sabotage, ...
- Why systems are attacked?
 - Profit.
 - Information is power.
 - Everything is connected.

Security is Hard

- Security is not absolute
 - Is your car secure?
 - Can you be 100% secure?
- Security is relative to:
 - **Objectives.**
 - **Assumptions.**
- Defenders vs. attackers success criteria.

What is this Course About?

- Learn to think about security:
 - Threats, defenses, policies.
 - Software, human and environment factors.
- Think as an attacker:
 - Learn to identify threats.
- Think as a security designer:
 - Learn how to prevent attacks and/or limit their consequences.
 - Understand and apply security principles.
 - Learn tools that can defend against specific attacks, no silver-bullet solution.

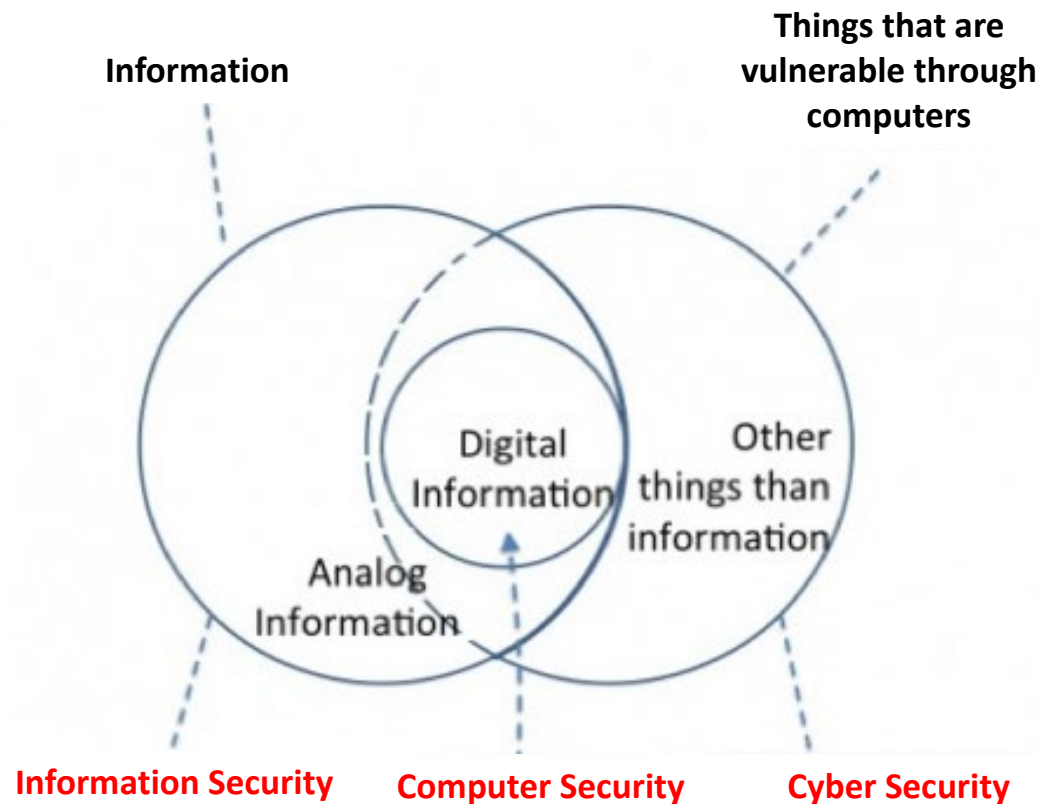
Course Outline

- Cryptographic tools.
- Security Protocols.
- Network Security.
- Software Security.
- Web Security.
- Operating System Security.
- Information Security Economics.
- Privacy.
- Legal and ethical issues surrounding security.
- Security Principles and Standards.

What is Security?

- Confidentiality
 - Only those authorized can know.
- Integrity
 - Only those authorized can successfully modify.
- Availability.
 - Ensuring those authorized to access can access.

Cyber Security vs. Computer Security vs. Information Security



Terminology

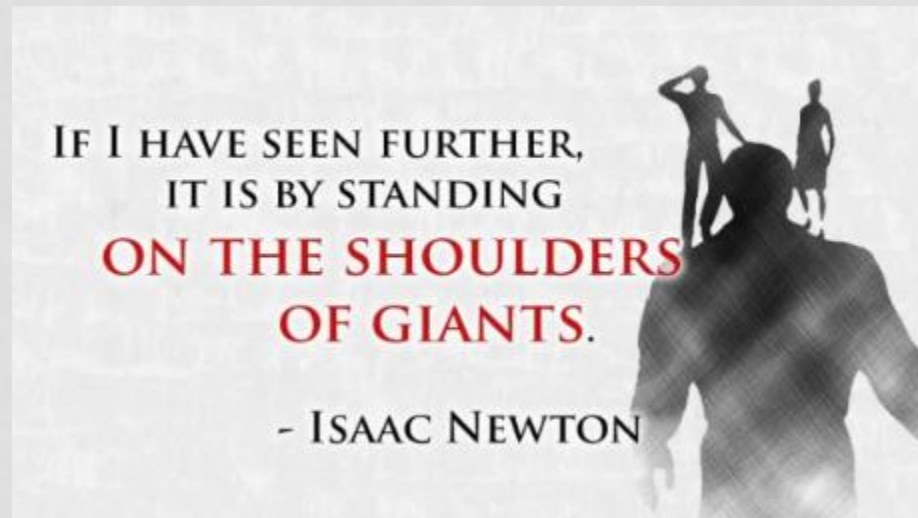
- Vulnerability
- Threat
- Risk
- Attack
- Security Control

Ethical Use

- We discuss vulnerabilities and attacks
 - Most vulnerabilities have been fixed.
 - Some attacks may still cause harm.
 - **Do not** try these at home.
- Purpose of this class
 - Learn to prevent malicious attacks
 - Use knowledge for good purposes

Acknowledgment

- Contents of these slides are based on:
 - Slides from Prof. Cristina Nita-Rotaru (Northeastren University) & Prof. Mikhail Atallah and Prof. Ninghui Li from Purdue University.
 - Slides from Prof. Keith Martin, Prof. Kenny Paterson and Prof. Jason Crampton from Royal Holloway, University of London.



Next Lecture

- Introduction to Cryptography.
- Readings:
 - For this lecture:
 - Anderson's Book – Chapter 1
 - <https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf>
 - For next lecture:
 - Anderson's Book – sections 5.1, 5.2.1, 5.2.2 and 5.2.3
 - <https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c05.pdf>