CS408
Cryptography & Internet Security

Reza Curtmola
Department of Computer Science

CS408
Cryptography & Internet Security

Lecture 1:
Introduction

Symantec.com > Business > The Stuxnet Worm

The Stuxnet Worm

Stuxnet is a computer worm that targets industrial control systems that are used to monitor and run large scale industrial facilities like power plants, dams, assembly lines and similar operations.

Free Assessment for Qualifying Enterprises

How Stuxnet Worm Works

Stuxnet looks for industrial control systems and then changes the code in them to allow the attackers to take control of these systems without the operators knowing. In other words, this threat is designed to allow hackers to manipulate real-world equipment, which makes it very dangerous.

It's like nothing we've seen before – both in what it does, and how it came to exist. It is the first computer virus to be able to wreak havoc in the physical world. It is sophisticated, well-funded, and there are not many groups that could pull this kind of threat off. It is also the first cyberattack we've seen specifically targeting industrial control systems.

The worm is made up of complex computer code that requires lots of different skills to put it together. Symantec security experts estimate it took five to ten people to work on this project for six months. In addition, knowledge of industrial control systems was needed along with access to such systems to do quality assurance testing; again indicating that this was a highly organized and well-funded project.

"We've definitely never seen anything like this before," said Liam O'Murchu, Researcher, Symantec Security Response. "The fact that it can control the way physical machines work is quite disturbing."

guardian.co.uk

News | Sport | Comment | Culture | Business | Money | Life & style | Travel | Environment

News > Media > WikiLeaks

The US embassy cables

Operation Payback cripples MasterCard site in revenge for WikiLeaks ban

Hackers attack credit card company and Swedish prosecution authority as 'censorship' row escalates

Follow the latest on our WikiLeaks live blog

Tweet 697 Share 7668

Esther Addley and **Josh Halliday**
guardian.co.uk, Wednesday 8 December 2010 17.28 GMT
Article history

A larger | smaller

Internet traffic was routed via Chinese servers

U.S. military sites included

By Shaun Waterman - The Washington Times 8:45 p.m., Monday, November 15, 2010

Nearly 15 percent of the world's Internet traffic, including that of many U.S. government and military sites, was briefly redirected through computer servers in China in April, according to a congressional commission report due out this week.

It is not clear whether the incident was deliberate, but the capability could enable severe malicious activities including the diversion of data and the interception of supposedly secure encrypted Internet traffic, the U.S.-China Economic and Security Review Commission states in a report to Congress.

A draft copy of the report, which is to be released Wednesday but viewed by The Washington Times, reports for the first time that .gov and .mil websites were affected by the 18-minute-long April 8 redirection, including those for the Senate, all four military services, the office of the secretary of defense, the National Aeronautics and Space Administration, the Department of Commerce, the National

This screen shot provided by Yahoo Inc. shows the newly redesigned Yahoo site. (Associated Press)

Print Email

View 13 Comment(s)

Enlarge Text | Shrink

Share 178 retweet

BBC Mobile News | Sport | Weather | Travel | T

NEWS TECHNOLOGY

Home | US & Canada | Latin America | UK | Africa | Asia-Pac | Europe | Mid-East | South Asia | Business

28 July 2010 Last updated at 20:37 ET

Details of 100m Facebook users collected and published

By Daniel Emery
Technology reporter, BBC News

The torrent is attracting hundreds of downloads

Personal details of 100m Facebook users have been collected and published on the net by a security consultant.

Target estimates breach affected up to 110 million

Ben Popken, NBC News

Jan. 10, 2014 at 8:21 AM ET

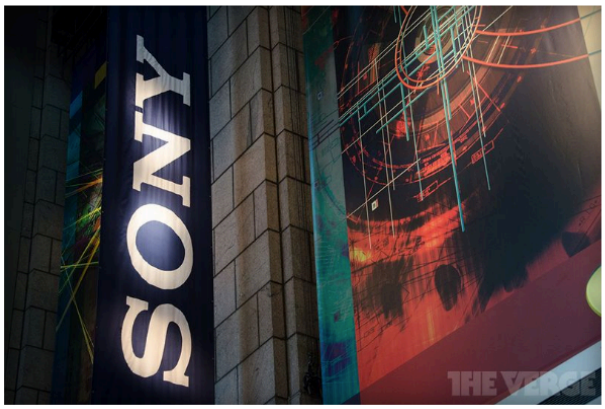
US & WORLD NATIONAL SECURITY

17 COMMENTS

Everything you need to know about the Sony hacks

By Russell Brandom on December 18, 2014 12:06 pm Email @russellbrandom

DON'T MISS STORIES FOLLOW THE VERGE Like Follow Subscribe Follow



- Information Security is an area that is full of open problems that have an impact on every day life
- Who's gonna fix them?

YOU !

Course Information

- When and where?
  - Tuesday 4:00 - 5:25 CKB 220
  - Friday 4:00 - 5:25 CKB 220
- Course webpage (general information):
  http://web.njit.edu/~crix/CS.408
- Course material (lecture slides, assignments etc):
  http://web.njit.edu/~crix/CS.408/content
- Professor contact info:
  - Office: GITC 4301
  - Email: crix@njit.edu
  - Office hours:
    - Tuesday 3-4pm, Friday 1:30-2:30pm
    - also by appointment (email me to set up a suitable time if you can't make it during the above times)

Class Attendance

- Lecture slides will be made available online, but they should not serve as a substitute for the lectures as they do not include all details
  - **class attendance is strongly recommended**
- Email me if you must miss lectures
- If you miss a lecture it is your responsibility to find out what happened in class
- You are advised to take notes

Emails

- For class-related announcements, I will use your NJIT email address
  - You can access your NJIT email address at:

    http://webmail.njit.edu

- Please include "CS.408" in the Subject line of all your emails related to this class

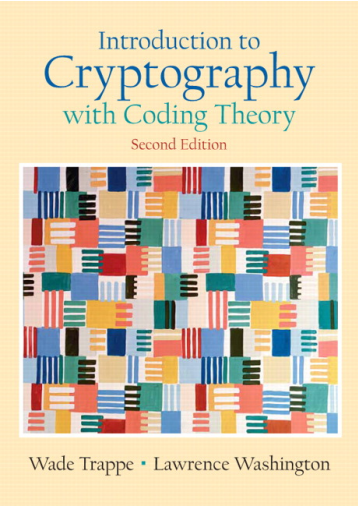
Prerequisites

- MATH 226 (Discrete Analysis)

or

- CS 241 (Discrete Mathematics)

Reference Material: Textbook



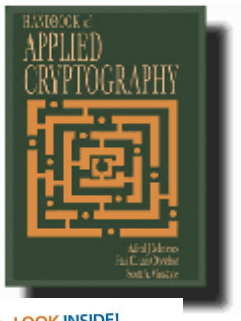
"Introduction to Cryptography with Coding Theory (2nd edition)"

by Wade Trappe and Lawrence Washington

published by Prentice Hall 2006

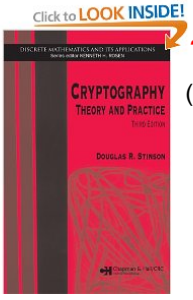
ISBN 0-13-186239-1

Reference Material: Additional resources



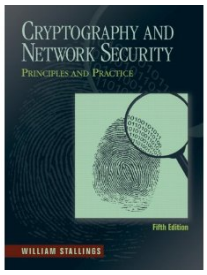
"Handbook of Applied Cryptography"

(a good reference book, available for free online at http://www.cacr.math.uwaterloo.ca/hac)



"Cryptography, Theory and Practice"

(by D. Stinson)



"Cryptography and Network Security"

(by W. Stallings)

Grading Policy

- Written Assignments (2) 22%
- Quizzes (in class) (2) 22%
- Midterm Exam 22%
- Final Exam 34%
- Programming Project (optional) 10%
- Class Participation (extra credit) 10%

Extra Days

- **Every student has 3 extra days throughout the semester** for all the written assignments and the programming project
  - This does not mean that you have 3 extra days for each assignment. You have 3 days IN TOTAL
  - For example, you may use 1 extra day for Assignment #1, then 1 extra day for Assignment #2, and 1 extra day for the project
- YOU DECIDE HOW TO USE THEM
- Email me with name and number of extra days used for an assignment
- 1 minute late counts as 1 extra day
- After using your extra days, no late homework or project will be accepted

Written Assignments

- Must by TYPED. IF IT'S NOT TYPED, IT WILL NOT BE GRADED
- Are due in the beginning of class. If you use extra days, you must email it (use PDF or Word format)
- You **must work individually** on the written assignments (unless indicated otherwise)

Exams

- Midterm exam - March 13, 2015
- Final exam - one day between May 8-14, 2015
- We will have a review of the material before midterm and final exams
- Final exam covers all the material studied throughout the entire semester

Programming Project

- One programming project
- You can work alone or in pairs of two students
- More information will come
- Purpose of the project is to become familiar with cryptographic libraries and to offer a glimpse of what it means to design and implement secure protocols
- Programming will be in JAVA

- Programming project is OPTIONAL
  (counts for 10% of grade)

Academic integrity

- Honor code
  - Can find detailed information at http://www.njit.edu/academics/honorcode.php

Honor Code and Behavior

NJIT has a zero-tolerance regarding cheating of any kind and student behavior that is disruptive to a learning environment. Any incidents will be immediately reported to the Dean of Students. In the cases the Honor Code violations are detected, the punishments range from a minimum of failure in the course plus disciplinary probation up to expulsion from NJIT with notations on student's permanent record. Avoid situations where honorable behavior could be misinterpreted. For more information on the honor code, see http://www.njit.edu/academics/honorcode.php

No eating or drinking is allowed at the lectures. Cellular phones must be turned off during lectures - if you are expecting am emergency, leave it on vibrate. No headphones can be worn in class.

Important dates

- Course withdrawal deadline: March 30
- Reading days: May 6, May 7
- Final exam: one day between May 8-14

Important dates

02/10/15	Assignment 1 out
02/20/15	Assignment 1 due
03/03/15	Quiz 1 (in class)
03/13/15	Midterm exam (in class)
03/24/15	Programming project out
04/07/15	Programming project due + Assignment 2 out
04/17/15	Assignment 2 due
04/21/15	Quiz 2 (in class)
May 8-14	Final exam (one day in this time interval)

(dates for the assignment are tentative)

WHAT WILL YOU LEARN
IN THIS CLASS?

Course Overview (1)

- Concepts and principles of cryptography: security services, attacks and mechanisms
- Classical cryptographic systems: shift cipher, Vigenere and Vernam ciphers, Jefferson wheel cipher and the Enigma machine
- Block ciphers: DES, Blowfish, RC5, IDEA, AES
- Stream ciphers: RC4, SEAL

Course Overview (2)

- Definitions of security
- Random number generation
- Basic number theory notions
- Public-key encryption: RSA,Diffie-Hellman, ElGamal, Rabin
- Data integrity: cryptographic hash functions (MD5, SHA1), message authentication codes (HMAC)
- Digital signatures: RSA, ElGamal, DSA, Schnorr
- Public key infrastructure, PGP
- Authentication protocols
- Key establishment protocols
- Kerberos

Course Overview (3)

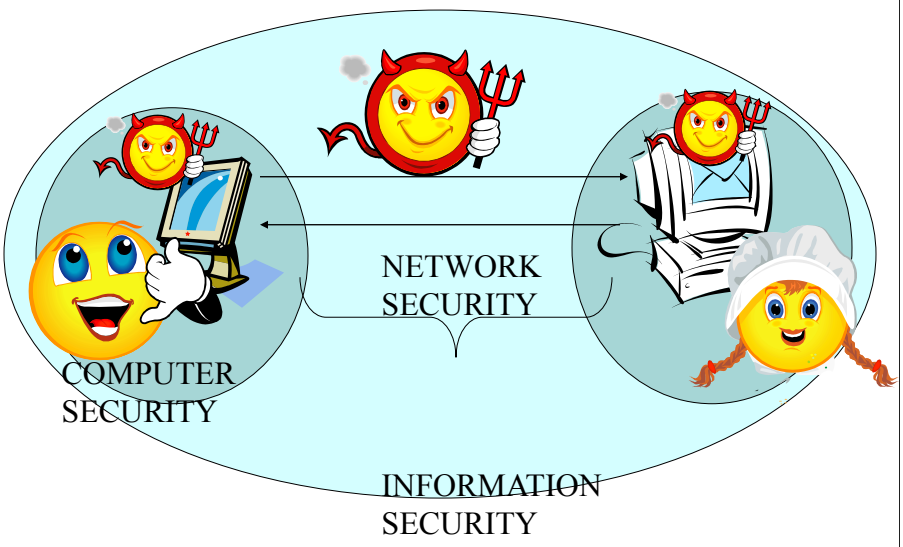
- Secure Sockets Layer (SSL)
- IPsec
- Zero-knowledge proofs
- Secure multi-party computation
- Identity-based cryptosystems
- Threshold cryptography
- Web and Internet security

Course Information

- Course webpage (general information):
  http://web.njit.edu/~crix/CS.408
- Course material (lecture slides, assignments etc):
  http://web.njit.edu/~crix/CS.408/content

Questions?

What's Crypto Got to Do with It?



Approaches to Secure Communication

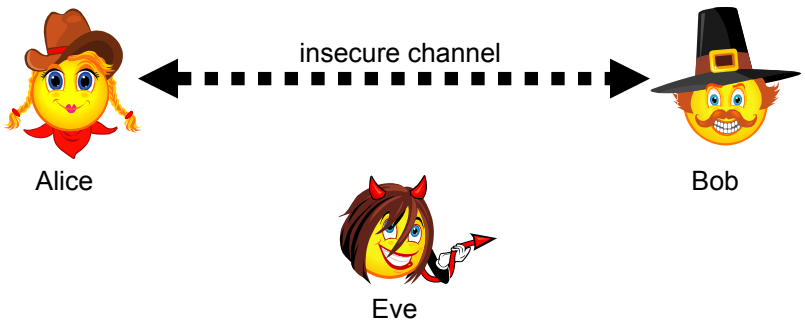
- Steganography
  - How to hide even the existence of a message
- Cryptography
  - How to hide the content of a secret message

Example: Making a purchase on amazon.com

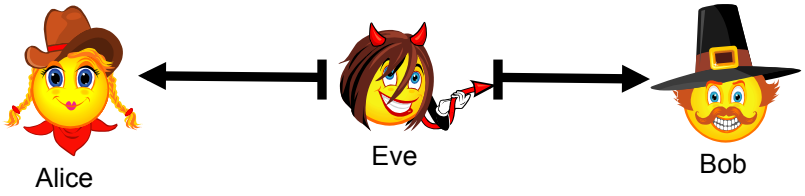
- amazon.com goals:
  - Make sure the right client is billed for the purchase
  - Only clients that paid get the goods
- Client goals:
  - Privacy, nobody can understand the communication (protects details of CC)
  - Not being charged for purchases of other people
- Cryptography can provide the tools to achieve these goals

Attacks against communication

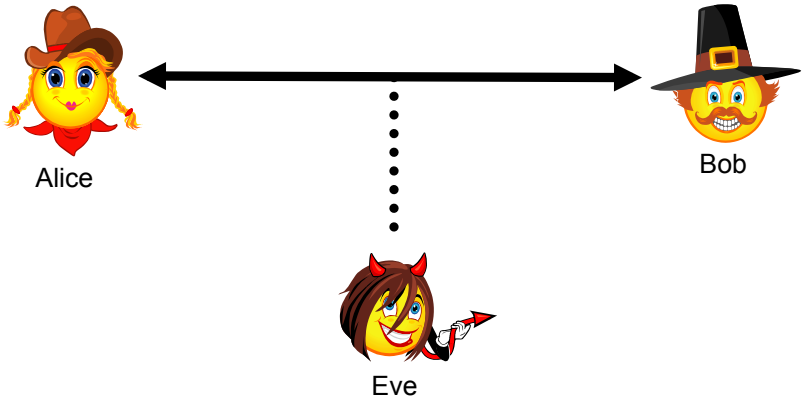
- Passive attacks
- Active attacks



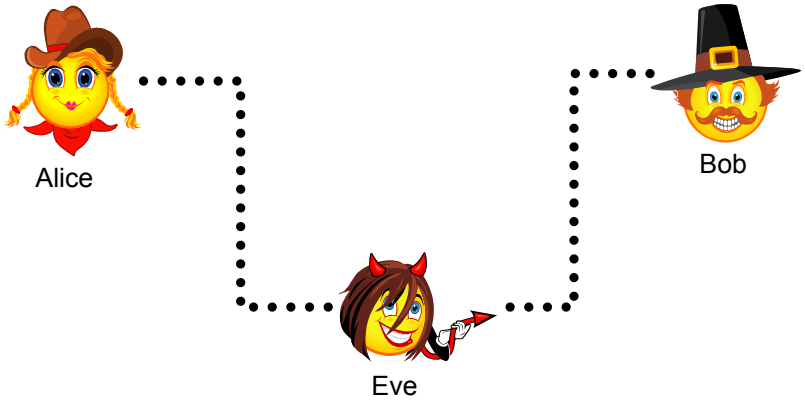
Attacks - interruption



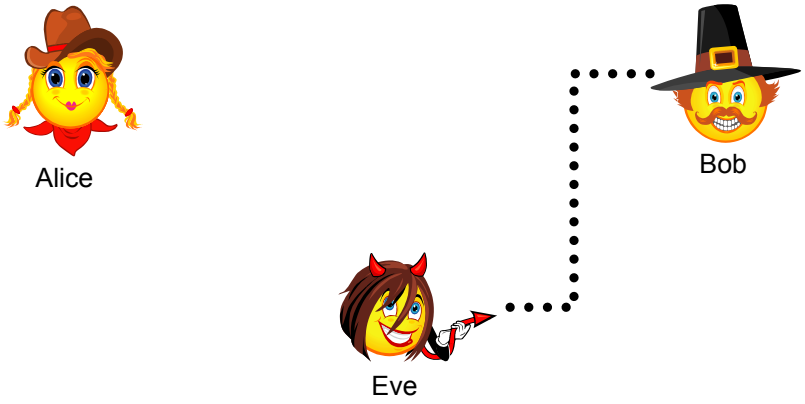
Attacks - interception



Attacks - modification



Attacks - injection



Basic security goals for data communication

- Confidentiality
  - Ensures secrecy of the message (only intended recipient can see the contents of communication)
- Integrity
  - Ensures data has not been altered in an unauthorized manner since the time it was transmitted
- Authentication
  - Ensures message really comes from the stated sender
- Non-repudiation
  - Ensures a party cannot deny the validity of the messages it creates

Security mechanisms

- Cryptography
  - Encryption
  - Digital Signatures
  - Message authentication codes
  - …
- Network security (firewall, IDS etc.)
- Hardware/Software protection
- Steganography
- Ad-hoc techniques
- …

Basic Terminology in Cryptography

- cryptography
- cryptanalysis
- cryptology
- plaintexts
- ciphertexts
- keys
- encryption
- decryption

What is Cryptography About?

- Constructing and analyzing protocols which enable parties to achieve objectives, overcoming the influence of adversaries.
  - a protocol (or a scheme) is a suite of algorithms that tell each party what to do
- How to devise and analyze protocols
  - understand the threats posed by the adversaries and the objectives (goals)
  - think as an adversary

Actually …

- **Cryptography**: the study of mathematical techniques related to aspects of providing information security services (construct)
  - Protect data
  - Provide techniques for secure communication over insecure channels
- **Cryptanalysis**: the study of mathematical techniques for attempting to defeat information security services (break).
- **Cryptology**: the study of cryptography and cryptanalysis (both).

Phases in Cryptography's Development

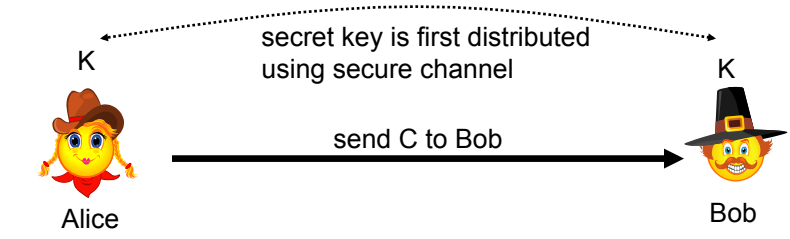
- Cryptography is driven by computing and communication technology
- First stage, paper and ink based scheme
- Second stage, using cryptographic mechanical devices
- Third stage, modern cryptography
  - relying on mathematics and computers
  - information-theoretic security
  - computational security

Cryptography vs. Coding Theory

- Cryptography seeks to provide secure communication over an insecure channel
- Coding theory deals with the problem of reliable communication over a noisy channel
  - Data may get lost over the channel. What to do?
    - Alice may retransmit the lost data
    - Alice may include redundant data in the first place!

Secret-key vs. Public-key Cryptography

- Secret-key cryptography (a.k.a. symmetric-key cryptography)
  - encryption & decryption use the same key (Alice and Bob have a trust relationship: they share a secret key)
  - key must be kept secret
  - key distribution is very difficult



generate ciphertext C
from message M using K

retrieve message M from
ciphertext C using K

analogy with a safe

Secret-key vs. Public-key Cryptography

- Public-key cryptography (a.k.a. asymmetric-key cryptography)
  - encryption key different from decryption key
  - cannot derive decryption key from encryption key
  - higher cost than symmetric cryptography
  - simplifies key distribution

  - Came into existence in 1976
  - Analogy with a mailbox

Some Applications of Modern Cryptography

- Pseudo-random number generation
- Non-repudiation: Digital signatures
- Zero-knowledge proofs
- E-voting
- Secret sharing

Symmetric key encryption

- A symmetric-key encryption scheme is a collection of three algorithms (G, E, D)
  - $\mathcal{K}$ (key space), $\mathcal{P}$ (plaintext space), $\mathcal{C}$ (ciphertext space)
  - Key generation algorithm G generates a key k
  - Encryption algorithm E : $\mathcal{K} \times \mathcal{P} \rightarrow \mathcal{C}$
    we use notation: $c = E_k(p)$
  - Decryption algorithm D : $\mathcal{K} \times \mathcal{C} \rightarrow \mathcal{P}$
    we use notation: $p = D_k(c)$

- The following should always hold true (correctness):
  - $D_k(E_k(p)) = p$, for all k and p
- A symmetric-key encryption scheme is also known as a symmetric-key *cipher*
- Provides: confidentiality
- Does not provide: authentication, integrity, non-repudiation
- It is a keyed cryptographic primitive
- Example: AES, DES, 3DES, Twofish, Serpent etc.

Kerchhoff's Principle

The security of a protocol should rely only on the secrecy of the keys, protocol designs should be made public (1883)

- **security by obscurity does not work** (there are many examples, WEP, voting machines, car immobilizers, etc.)

Dr. Auguste Kerckhoff (19 January 1835 – 9 August 1903) was a Dutch linguist and cryptographer who was professor of languages at the School of Higher Commercial Studies in Paris in the late 19th century.

How Do You Know a Cipher is Secure?

- Show that under the considered attack model, security goals are NOT achieved (break it)
- Show that under the considered attack model, security goals are achieved (evaluate/prove)

Recommended Reading for This Lecture

- Trappe & Washington
  - Chapter 1