CSCD27

Computer and Network Security

Thierry Sans

Why security matters?

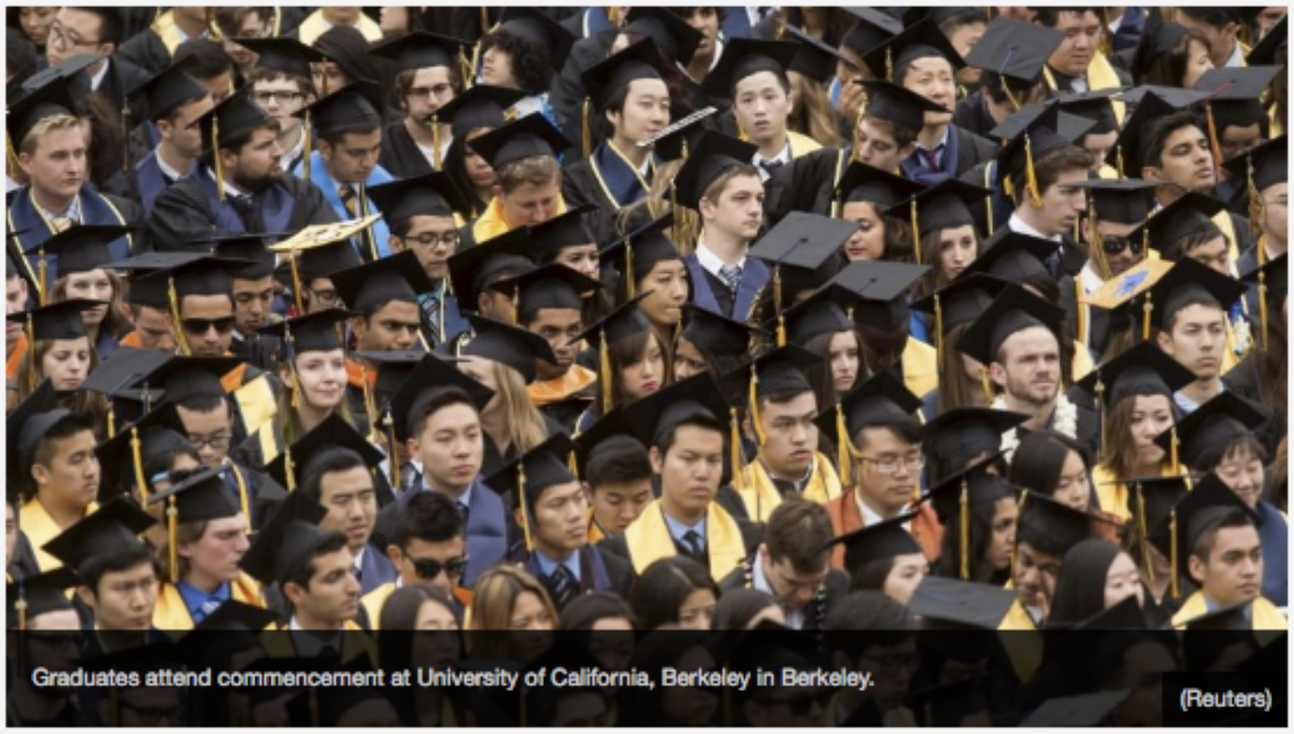
Dropbox hackers stole 68 million passwords - check if you're affected and how to protect yourself

The Telegraph

August 2016

Data breach affects 80,000 UC Berkeley faculty, students and alumni

Published February 28, 2016 · FoxNews.com



Graduates attend commencement at University of California, Berkeley in Berkeley. (Reuters)

A hacker broke into the University of California, Berkeley computer system holding financial data of 80,000 students, alumni, current and former employees, school officials said Friday.

witnessed Manson murder

face transplant dies

CREDIT RSS | Tue Dec 29, 2015 2:20pm GMT

Database of 191 million U.S. voters exposed on Internet: researcher

Signs are pictured during a voter registration drive for National Voter Registration Day outside Convention Center in Los Angeles, California September 22, 2015. REUTERS/Mario Anzuoni

By **Jim Finkle** and **Dustin Volz**

An independent computer security researcher uncovered a database of information on 191 million voters that is exposed on the open Internet due to an incorrectly configured database, he said on Monday.

Reuters

September 2015

Identity Force

February 2016

IRS Data Breach Update: More Taxpayers Affected

Last year's IRS data breach is continuing to make headlines as the true scope of its damage becomes clearer. The breach, which the IRS believes took place in February 2015, was first announced in May 2015; at the time, it was thought that more than 100,000 American taxpayers had their personal information compromised. However, in August 2015, the agency revealed the discovery of an additional 220,000 victims. Now, about one year since the initial breach, the IRS is saying that the current total number of victims is topping 700,000 — about seven times more than initial estimates.

JPMorgan Chase Hacking Affects 76 Million Households

By JESSICA SILVER-GREENBERG , MATTHEW GOLDSTEIN and NICOLE PERLROTH

OCTOBER 2, 2014 12:50 PM 528

The Manhattan headquarters of JPMorgan Chase, which securities filings revealed was attacked by hackers over the summer. Andrew Burton/Getty Images

Email

Share

Updated, 9:03 p.m. | A cyberattack this summer on JPMorgan Chase compromised the accounts of 76 million households and seven million small businesses, a tally that dwarfs previous estimates by the bank and puts the intrusion among the largest ever.

The New York Times

October 2014

Hackers publish contact info of 20,000 FBI employees

By Mary Kay Mallonee, CNN

Updated 8:34 PM ET, Mon February 8, 2016

Hackers 'stole a master key' to U.S. government 02:17

Story highlights

Hackers published contact information for 20,000 FBI employees Monday afternoon

The Justice Department is actively investigating the incident

Washington (CNN) — Hackers, making good on a threat, published contact information for 20,000 FBI employees Monday afternoon, just one day after posting similar data on almost 10,000 Department of Homeland Security employees.

The hackers, tweeting from the account @DotGovs, claim they obtained the details by hacking into a Department of Justice database.

CNN

February 2016

IPhone Users Urged to Update Software After Security Flaws Are Found

By NICOLE PERLROTH AUG. 25, 2016

SAN FRANCISCO — One of the world's most evasive digital arms dealers is believed to have been taking advantage of three security vulnerabilities in popular Apple products in its efforts to spy on dissidents and journalists.

Investigators discovered that a company called the NSO Group, an Israeli outfit that sells software that invisibly tracks a target's mobile phone, was responsible for the intrusions. The NSO Group's software can read text messages and emails and track calls and contacts. It can even record sounds, collect passwords and trace the whereabouts of the phone user.

Citizen Lab (UofT)

The New York Times

August 2016

DDoS attack that disrupted internet was largest of its kind in history, experts say

Posted by Eric Beaudoin

Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

AIRS

April 2017

8/29/2016
07:30 AM

Alex Campbell
Commentary

0 COMMENTS
COMMENT NOW

Critical Infrastructure: The Next Cyber-Attack Target

Power and utilities companies need a risk-centric cybersecurity approach to face coming threats.

The way we think about cyber attacks changed in December 2015, when Ukraine experienced the first recorded power outage caused by a cyber attack. It didn't last long—between one and six hours, depending on the area—but it showed the government, industry, and the public how these attacks could affect the physical world. It's not just personal information and other sensitive data that's at stake. Critical infrastructure is now under threat.

Dark Reading
August 2016

Cyber attack hits German train stations as hackers target Deutsche Bahn

share

1 Comment

Government under pressure after NHS crippled in global cyber attack as weekend of chaos looms

share

100 Comments

Screenshot of the suspected ransomware message on a GP's computer in the Greater Preston area
CREDIT: PA

ıan train station displays the ransomware message CREDIT:

The Telegraph

May 2017

Hackers gain access to hundreds of global electric systems

Researchers find that a cyberattack group has been quietly sneaking into the world's power grid control systems over the last six years.

Security

by **Alfred Ng**

6 September 2017 5:56 pm BST

@alfredwkng

Hundreds of power grids have been hacked in the United States, Turkey and Switzerland.

CNet

September 2017

CRUNCH NETWORK

The biggest threat facing connected autonomous vehicles is cybersecurity

*Posted Aug 25, 2016 by **Rob Toews** (**@_RobToews**)*

Rob Toews
CRUNCH NETWORK
CONTRIBUTOR

Rob Toews is jointly pursuing degrees at Harvard Business School and Harvard Law School. He is the co-

Connected, autonomous vehicles are around the corner. Many of the most innovative and deep-pocketed companies in the world are racing to bring them to market — and for good reason: the economic and social gains they will generate will be tremendous.

Techcrunch

August 2016

Why do have security issues?

- **Bugs**
  buffer overflows, cross-site scripting attacks …

- **Insecure configuration**
  improper authorization, incomplete mediation …

- **No security by design**
  most of network protocols running the internet

Why security should matters to you?

- Because **you** are going to build the next computer systems, networks and software

The Fast-Growing Job With A Huge Skills Gap: Cyber Security

Jeff Kauflin, FORBES STAFF
I cover leadership, management and careers. FULL BIO

Some experts predict there will be a global shortage of two million cyber security professionals by 2019.

Forbes

Mars 2017

Dark Reading

June 2017

CAREERS & PEOPLE

6/7/2017
06:10 PM

Dawn Kawamoto
News

Cybersecurity Faces 1.8 Million Worker Shortfall By 2022

(ISC)2 report shows the skills shortage is getting worse.

Over the next five years, the number of unfilled cybersecurity jobs will rise to a whopping 1.8 million, a 20% increase from 2015 estimates, according to a new (ISC)2 survey released today.

Welcome to CSCD27

Legacy

- CSCD27 Computer and Network Security
  Alan Rosselet
  University of Toronto Scarborough

- 15-349 Introduction to Computer and Network Security
  Iliano Cervesato, Khaled Harras and Thierry Sans
  Carnegie Mellon University Qatar

Course Objectives

CSCD27 is an undergraduate course that provides **a theoretical and technical overview** of the field of computer security

Learning goals

1. Acquire a **good understanding of basic concepts** such as
   - applied cryptography
   - networking security
   - software vulnerabilities analysis and defense

2. Acquire a **methodology to design and analyze the security of critical systems**

3. Acquire a **good practice to stay up-to-date** with the field

Course work, evaluation and grading

Tracks	Theory	Practice
Tutorials	Tutorials	Labs
Graded Work	Final Exam	CTF challenges
Grade weight	35%	65%

Course Topics

1. Applied Cryptography
2. Network Security
3. Computer Security

1. Applied Cryptography

- Classical crypto systems
- Modern crypto systems : symmetric vs asymmetric
- Hash functions and digital signatures
- Cryptography protocols for authentication and encryption

2. Network Security

Vulnerabilities and defense for the network stack

	Protocol	Secure Layer
Application	DNS	DNSsec
Transport	TCP	TLS (a.k.a. SSL)
Internet	IP	IPSec
Link	802.11	WPA2

3. System Security

- Operating Systems
- Programs
- Malicious code
- Web

Ethical Hacking

- You will be exposed to attack methods
- You should uphold to a high standard of **professional and personal ethic**
- **Your knowledge of attack methods does not imply permission to exploit them**

… even if it seems "harmful fun"

- **UofT policies** are strictly enforced
- **Canadian Criminal Code** is strictly enforced

Course website

https://thierrysans.github.io/CSCD27/

How to succeed in this course

- Come to lectures, tutorials … blah blah blah
- Do the work … blah blah blah
- Be curious, be stubborn and get your hands dirty