CSCD27

Computer and Network Security

Thierry Sans

Why security matters?

Back-to-school malware is hiding in those digital textbooks

Kaspersky warns that it found more than 100,000 textbook files with malware lurking inside.

BY RAE HODGE | SEPTEMBER 3, 2019 1:41 PM PDT

Researchers warn that malicious actors are targeting students seeking to escape rising textbooks costs via online alternatives.

Jeff Greenberg/Getty Images

C|NET
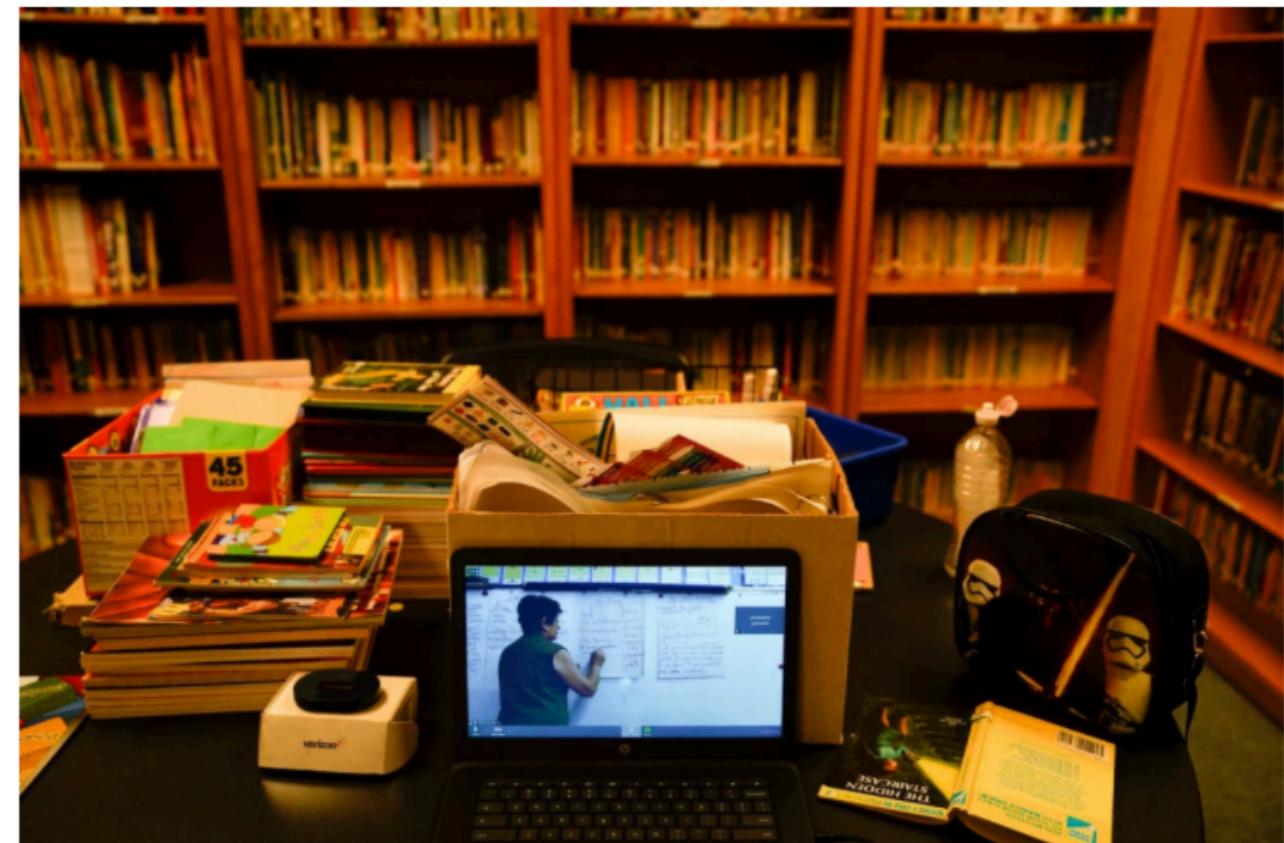
September 2019

New York Times

September 2020

Website Crashes and Cyberattacks Welcome Students Back to School

With many districts across the country opting for online learning, a range of technical issues marred the first day of classes.

Many of the nation's school districts faced technical challenges on Tuesday while starting the academic year remotely. Jae C. Hong/Associated Press

The University of Chicago Medicine Exposed 'Perspective Givers' Database With More Than A Million of Records

Security Discovery

June 2019

| 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

February 29, 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.

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 goo[d] threat, published contact information for 20,0[00] employees Monday afternoon, just one day a[fter] similar data on almost 10,000 Department of [Homeland] Security employees.

The hackers, tweeting from the account @Do[...] claim they obtained the details by hacking int[o a] Department of Justice database.

CNN

February 2016

CNET

January 2018

Homeland Security breach exposes data on 240,000 employees

Personally identifiable information was discovered in the possession of a former department employee.

BY **STEVEN MUSIL** / JANUARY 3, 2018 6:20 PM PST

Equifax says number of Canadians affected by hack passes 19,000

Signage at the corporate headquarters of Equifax Inc. in Atlanta.

MIKE STEWART/AP

The Canadian Press

November 2017

CSO Online

May 2018

Air Canada locks down 1.7 million mobile app accounts after breach affects 20,000 customers

Aeroplan numbers, passport numbers, birth dates, nationalities and countries of residence could have been accessed
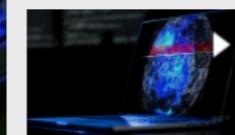

Financial Post

August 2018

19 million Canadians have had their data breached in eight months

CTV National News: Shocking data breach numbers

An exclusive investigation by the podcast 'Attention Control' hosted by Kevin Newman has uncovered disturbing data breach numbers.

CTV News

September 2019

913   913

FEATURED POLITICS »

Francesca Fionda, Investigative journalist, Attention Control
@francescafionda

Global News

October 2022

CANADA

Cybersecurity incidents affected 18% of businesses in Canada last year: StatCan

By Staff • The Canadian Press
Posted October 18, 2022 12:35 pm

Ontario's BORN birth registry breach sees data 'taken' from 3.4 million

By **Uday Rana** • **Global News**
Posted September 25, 2023 10:56 am · Updated September 25, 2023 12:49 pm

Global News

September 2023

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

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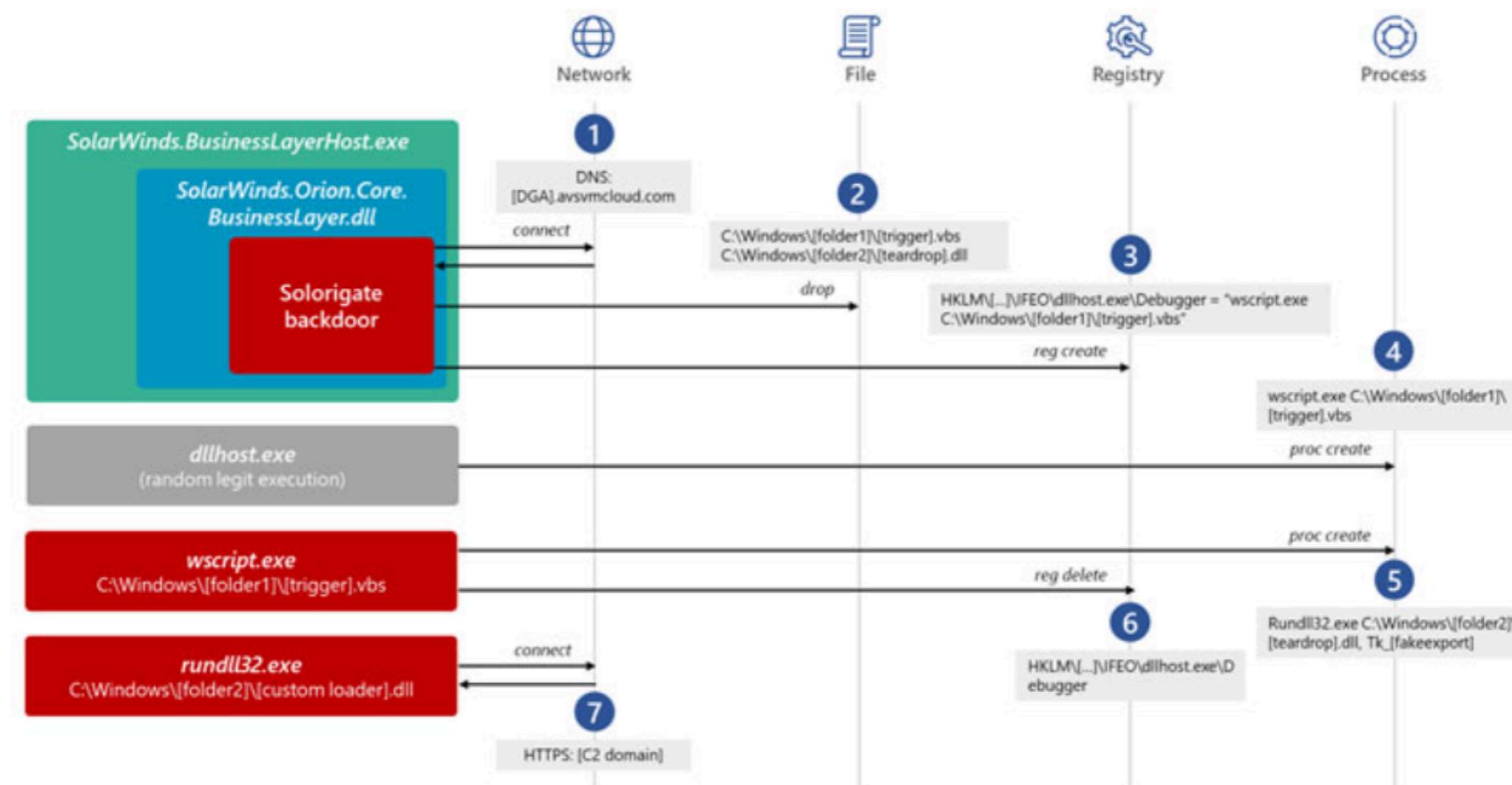
Dyn estimated that the attack had involved '100,000 malicious endpoints', and the company said there had been reports of an extraordinary attack strength of 1.2 terabits (1,200 gigabytes) per second. Photograph: Alamy

AIRS

April 2017

Here's How SolarWinds Hackers Stayed Undetected for Long Enough

January 21, 2021   Ravie Lakshmanan

Microsoft on Wednesday shared more specifics about the tactics, techniques, and procedures (TTPs) adopted by the attackers behind the SolarWinds hack to stay under the radar and avoid detection, as cybersecurity companies work towards getting a "clearer picture" of one of the most sophisticated attacks in recent history.

The Hacker News

List of Data Breaches and Cyber Attacks in 2023 – 8,214,886,660 records breached

👤 IT Governance   📅 5th January 2024

IT Governance

Global Data Breaches and Cyber Attacks in 2024

👤 IT Governance   📅 2nd May 2024

35,900,145,035 known records breached so far in

Top 10 biggest breaches of 2024 (so far)

	Organisation name	Sector	Location	Known number of records breached	Month
1	MOAB	Multiple	Multiple	>26,000,000,000	January
2	Discord (via Spy.pet)	IT services and software	USA	4,186,879,104	April
3	Far Eastern Research Center for Space Hydrometeorology (Planeta)	Public	Russia	2 PB	January
4	Baidu, Inc., Honor, Huawei, iFlytek, OPPO, Samsung Electronics, Tencent, Vivo and Xiaomi Technology	IT services and software	China	Up to 1,000,000,000	April
5	Indian mobile network consumer database (probably)	Telecoms	India	750,000,000	January
6	Zenlayer	Telecoms	USA	384,658,212	February
7	Unknown Brazilian organisation	Unknown	Brazil	>223,000,000	January
8	Telekom Malaysia	Telecoms	Malaysia	Almost 200,000,000	January
9	Pure Incubation Ventures	Professional services	USA	183,754,481	February
10	916 Google Firebase websites	Multiple	USA	124,605,664	March

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

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.
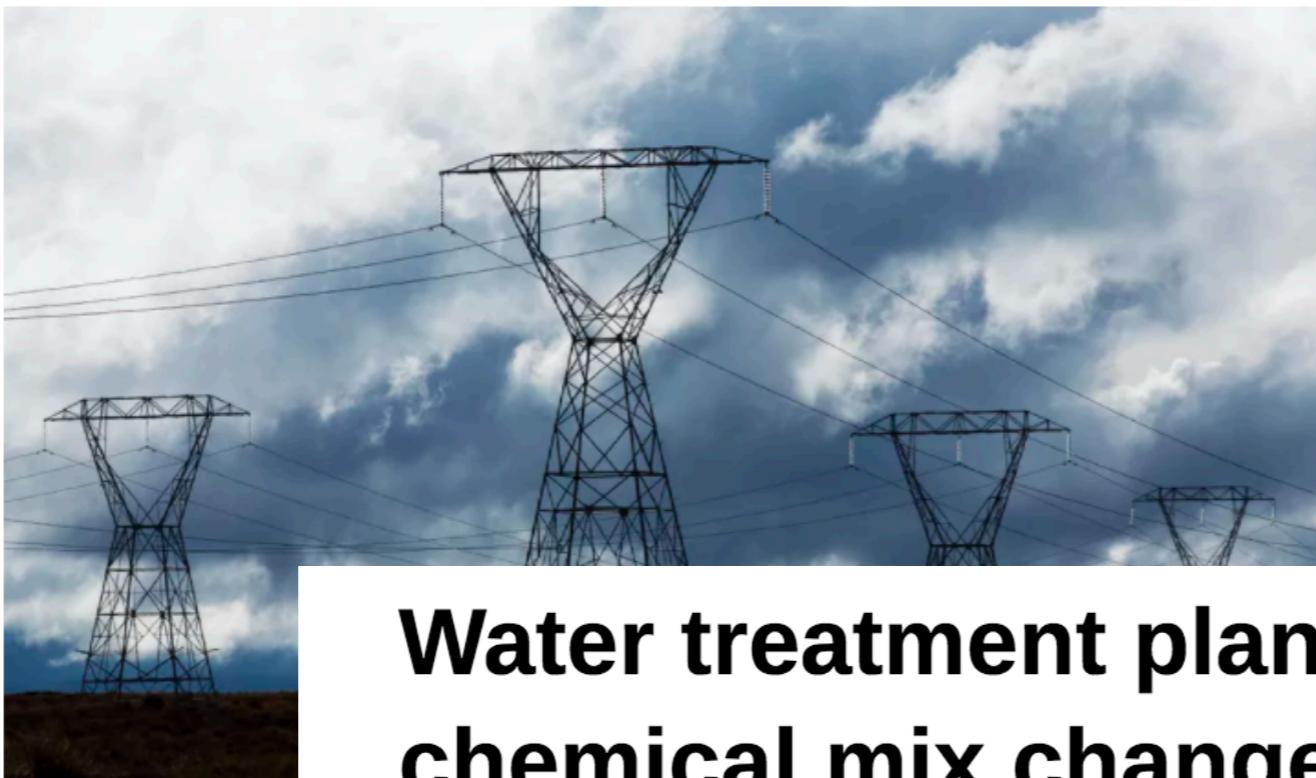
Security

by **Alfred Ng**
6 September 2017 5:56 pm BST
@alfredwkng

Hundreds of po...

Water treatment plant hacked, chemical mix changed for tap supplies

Well, that's just a little scary

By John Leyden 24 Mar 2016 at 12:19   82 💬   **SHARE ▼**

Hackers infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water, we're told.

Hacker Tried Poisoning Water Supply After Breaking Into Florida's Treatment System

📅 February 08, 2021   👤 Ravie Lakshmanan

Hackers successfully infiltrated the computer system controlling a water treatment facility in the U.S. state of Florida and remotely changed a setting that drastically altered the levels of sodium hydroxide (NaOH) in the water.

The Hacker News

Ransomware Cyber Attack Forced the Largest U.S. Fuel Pipeline to Shut Down

📅 May 09, 2021   👤 Ravie Lakshmanan

Colonial Pipeline, which carries 45% of the fuel consumed on the U.S. East Coast, on Saturday said it halted operations due to a ransomware attack, once again demonstrating how critical infrastructure is vulnerable to cyber attacks.

The Hacker News

A cyber attack in Saudi Arabia failed to cause carnage, but the next attempt could be deadly

At a time when the world faces a dangerous escalation in cyber warfare, a series of assaults on petrochemical companies in Saudi Arabia – possibly backed by nation states – has caused alarm

Nicole Perlroth , **Clifford Krauss** | Wednesday 21 March 2018 06:00 |

Like   Click to follow The Independent

Computers crashed at sites including Sadara Chemical Company, a joint venture between the oil and chemical giants Saudi Aramco and Dow Chemical (*Sadara*)

Independent

March 2018

Energy producer Suncor admits 'cyber security incident'

HOWARD SOLOMON   JUNE 26, 2023

Image from Petro-Canada

Global News

June 2023

A Patient Dies After Ransomware Attack Paralyzes German Hospital Systems

📅 September 21, 2020   👤 Ravie Lakshmanan

German authorities last week disclosed that a ransomware attack on the University Hospital of Düsseldorf (UKD) caused a failure of IT systems, resulting in the death of a woman who had to be sent to another hospital that was 20 miles away.

The Hacker News
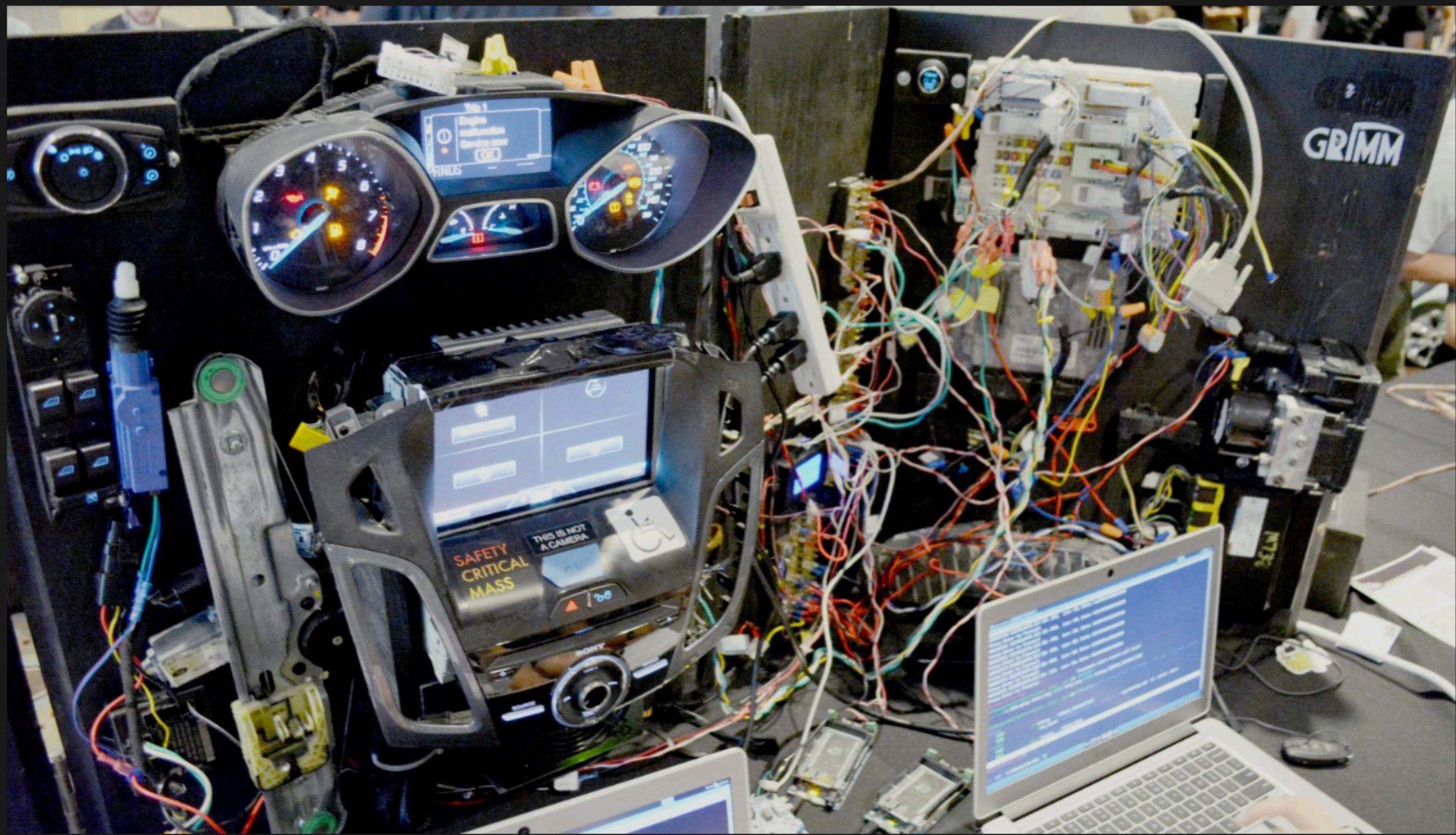
Hackaday

August 2018

FORBES > INNOVATION > TRANSPORTATION

Advanced Cars May Face Greater Risk Of Hacking, Cybersecurity Experts Warn

Ed Garsten Senior Contributor ⓘ

Follow

0

Apr 26, 2023, 08:26am EDT

As automakers add more technology to vehicles, they have become more vulnerable to cybersecurity ... [+] GETTY

Forbes

April 2023

Why GPS Is Under Attack

Satellite signals run the modern world. See just how vulnerable they are.

By SELAM GEBREKIDAN, K.K. REBECCA LAI, PABLO ROBLES and JEREMY WHITE

New York Times

July 2024

Why do we 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

Cybersecurity Jobs. PHOTO: Cybercrime Magazine.

Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021

350 percent growth in open cybersecurity positions from 2013 to 2021

Cybersecurity Ventures

Canada struggling to keep up with demand for cybersecurity talent: report

By Bradly Shankar   JUL 4, 2018   6:29 PM EDT   💬 0 COMMENTS

MobyleSyrup
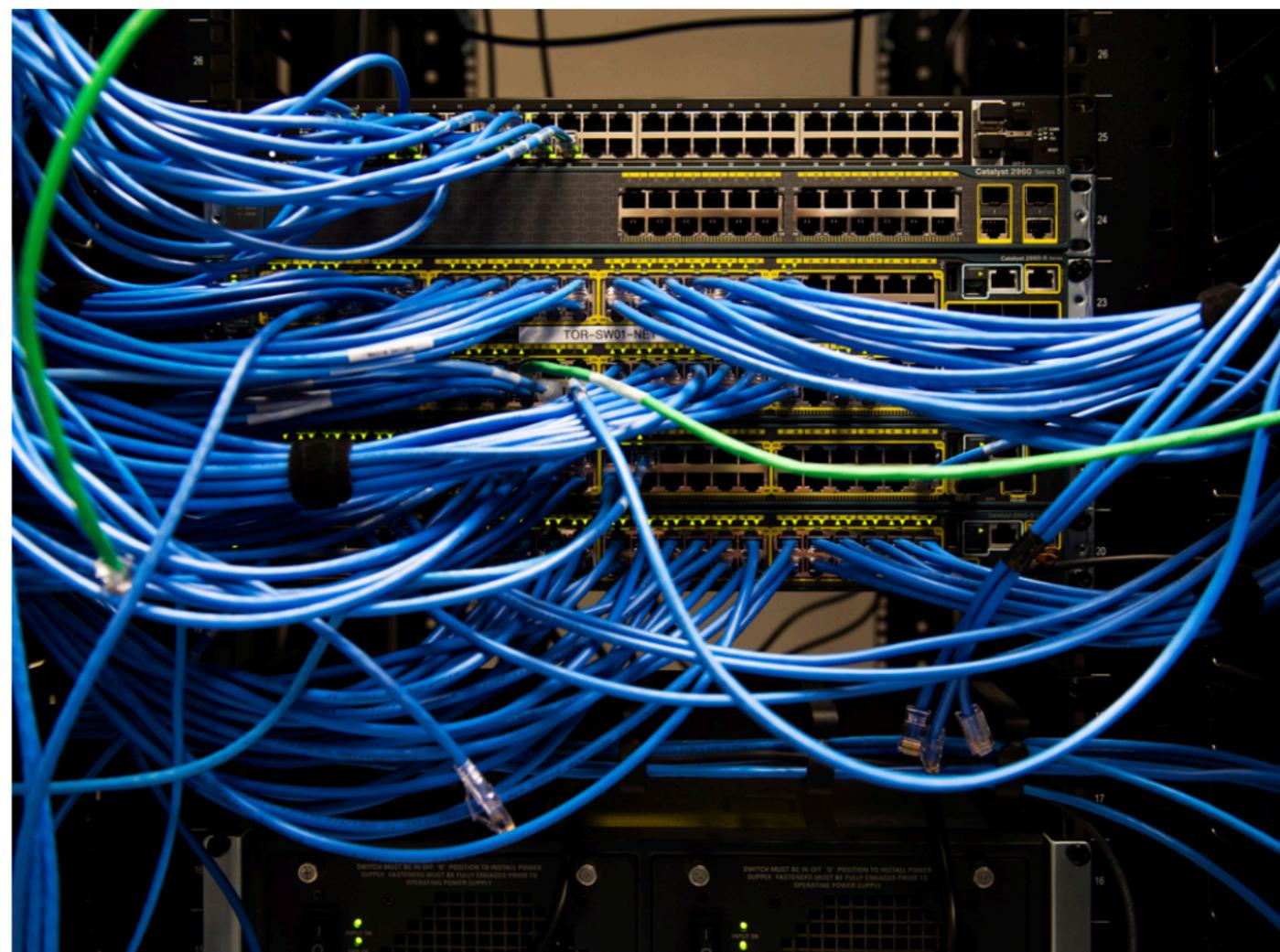
July 2018

Financial Post

July 2018

Canada facing a talent crunch when it comes to cybersecurity experts — and things look likely to get worse

The labour squeeze leaves companies at risk of serious cyberattacks that can go so far as to put them out of business

A new report from Deloitte says demand for cybersecurity professionals in Canada is growing by seven per cent annually, with 8,000 new workers needed by 2022. *Nathan Denette/The Canadian Press*

September 24, 2019

Cybersecurity Workforce Shortage In Canada

Introduction:

A cause-effect relationship is becoming increasingly evident within the cybersecurity world. A shortage of qualified candidates who are capable of tackling cybercrimes and preventing data breaches have resulted in both individuals and corporations being persistently vulnerable to cyber-attacks. As hackers on the dark web attack in waves, it is inevitable that the need for "white hats" to combat this global issue has elevated in importance.

Numbers Put Into Perspective

2.93 Million

Number of unfilled cybersecurity positions worldwide

8,000

Cybersecurity roles to be filled in Canada between now and 2021

Whitehorn Capital

September 2019

News & Events ›

One in Six Canadian Cybersecurity Roles Go Unfilled: New Report Explores Talent Shortage and Solutions

By ICTC · October 13, 2022

Share →

Ottawa, October 13, 2022—A shortage of cyber professionals in Canada sees one in six cybersecurity jobs go unfilled, which represents one of the country's biggest challenges for the digital economy.

The Information and Communications Technology Council (ICTC)

October 2022

Canada faces shortage of cybersecurity professionals amid rising demand

Demand is high amid surge in incidents

CSE | YouTube

The Big Read

Shortage of cybersecurity workers a 'crisis' at apex of federal government

By David Reevely Jun 6, 2023

FINANCIAL POST

Cybersecurity

Safety Net: Cybersecurity staff shortage looms if Canada fails to develop homegrown talent

Surging demand means firms need 10% more trained professionals a year for foreseeable future

John Chilibeck, Brunswick News, Special to Financial Post

Published Mar 15, 2023 • Last updated Mar 15, 2023 • 6 minute read

Financial Post

March 2023

EMERGING TECHNOLOGIES

The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap

Apr 28, 2024

The global cybersecurity industry is in need of 4 million more professionals.
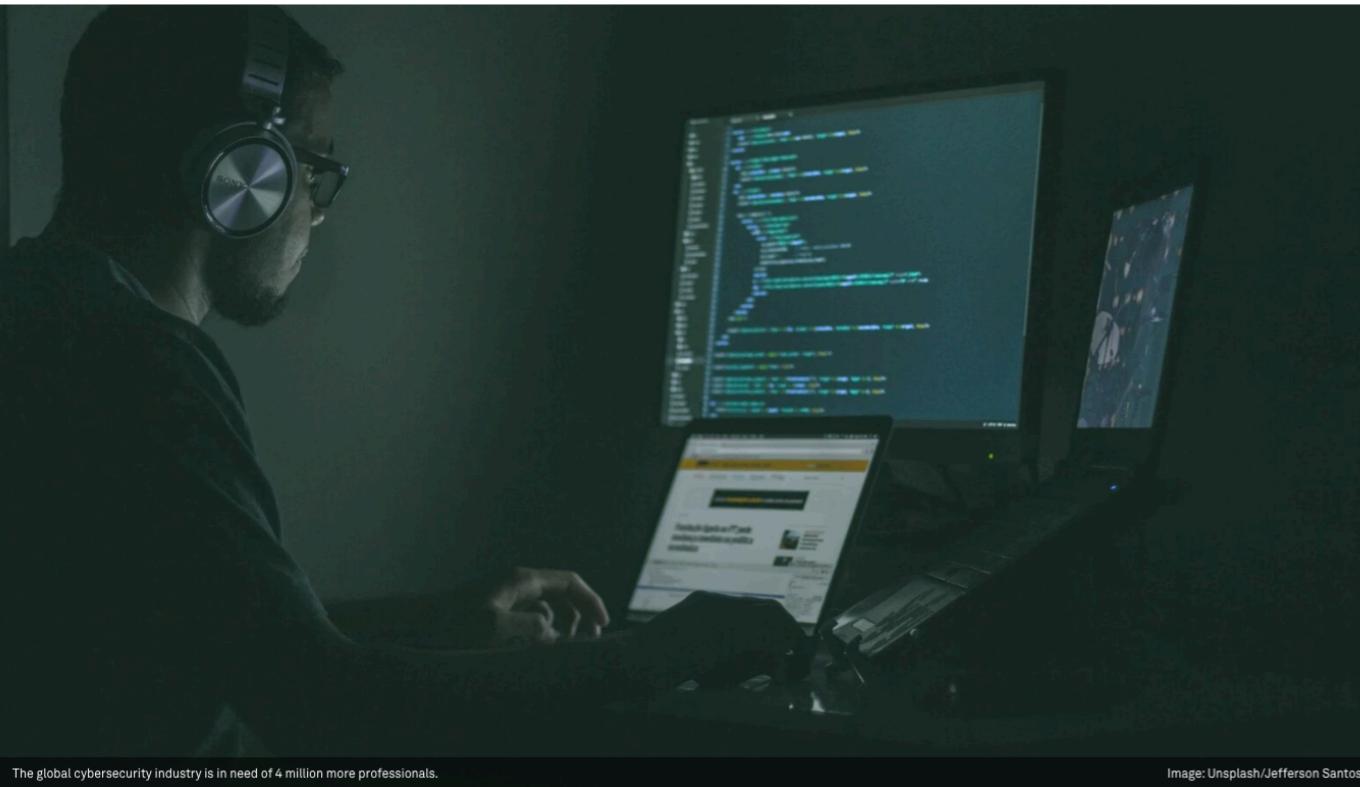
Image: Unsplash/Jefferson Santos

World Economic Forum

April 2024

HRD

May 2024

Cybersecurity industry short nearly 4 million professionals

New report shows global workforce shortage hitting cybersecurity sector

Welcome to CSCD27

Course Objectives

CSCD27 is an <u>undergraduate course</u> 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 security

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 Topics

1. Applied Cryptography

2. Network Security

3. System 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
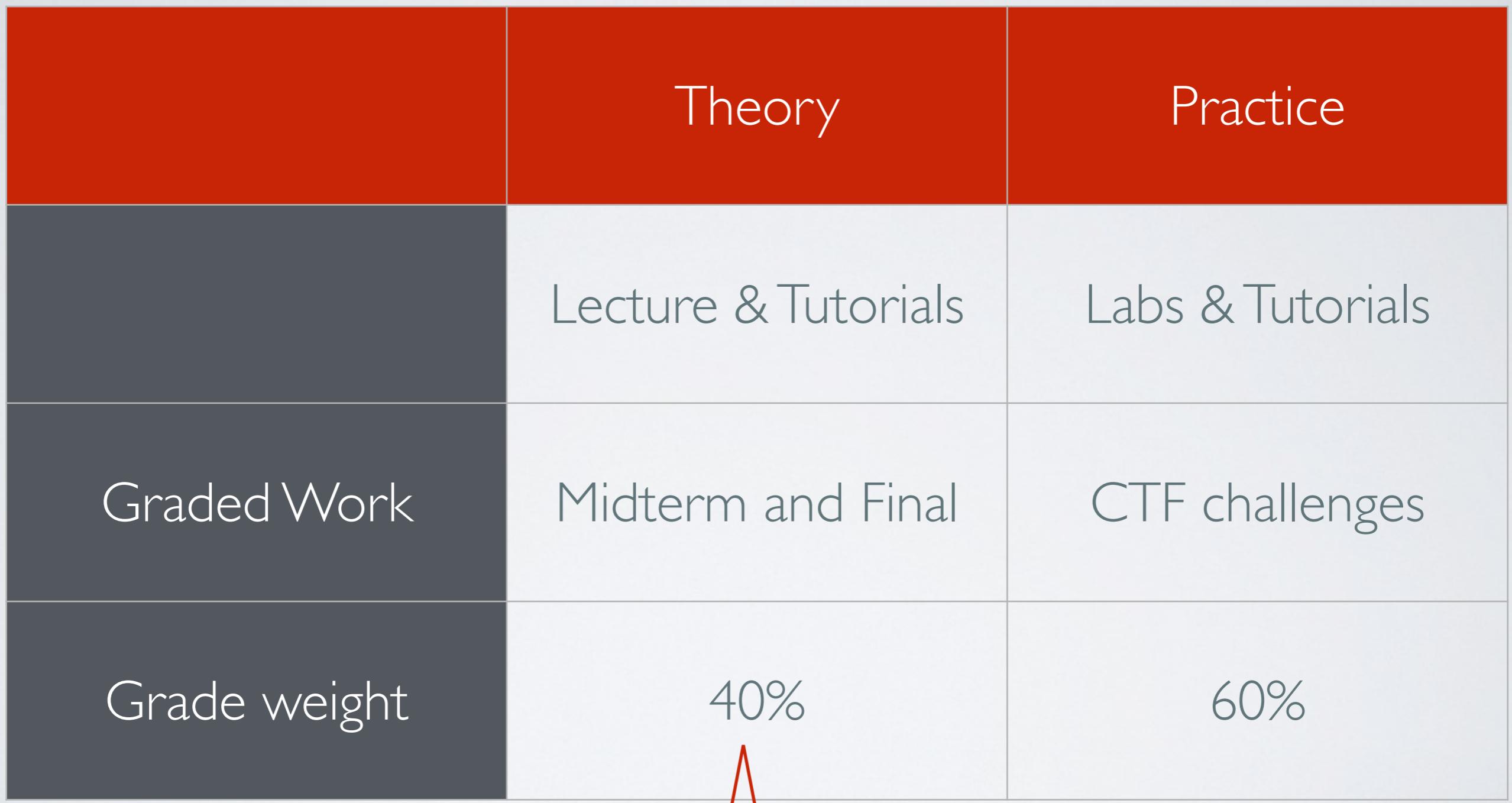
Vulnerabilities and defense for the network stack

	Protocol	Secure Layer
Application	DNS	DNSsec
Transport	TCP	TLS (a.k.a. SSL)
Internet	IP	IPSec
Link	802.11	WPA3

3. Software Security

- Operating Systems

- Programs

- Malicious code

- Web Security

Course work, evaluation and grading

	Theory	Practice
	Lecture & Tutorials	Labs & Tutorials
Graded Work	Midterm and Final	CTF challenges
Grade weight	40%	60%

A mark of at l**east 40% on the final exam is required** to pass the course

Academic Integrity

✓ For CTF challenges you are allowed to discuss problems with your classmates but not solutions

◉ For midterm and exams, you are not allowed to discuss problems and solutions with anyone

◉ You are not allowed to search online for the solution to the problem

✓ But you are allowed to search online for snippets of code that will help you write your solution

◉ You are not allowed to share snippets of code with anyone

◉ You are not allowed to publish online any snippet of code related this course even after the end of the semester

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 <u>strictly enforced</u>
- **Canadian Criminal Code** is <u>strictly enforced</u>

Course website

https://thierrysans.me/CSCD27/

How to succeed in this course

https://thierrysans.me/CSCD27/doc/howtosucceed/

You know the drill ...

- Come to lectures

- Tutorials are important … blah blah blah

- Start to work early … blah blah blah

.... but more specifically to this course

The important is **why** rather than *how*

The skills you must have

- Basic knowledge of computer systems (B09, B58 and C69)

- Good programming skills (especially Python and C)

- Good Linux skills (shell scripting)

➡ Be able to **seek for documentation** and **learn new materials** on your own

About the lectures

The slides are **not** lecture notes

About the tutorials

The important is **not the solution** to the problems **but the discussion**

About the CTF challenges

For each challenge, there will be a **fair amount of materials to learn and to understand** before being able to start working on a solution

Each challenge is **highly experimental**

Warning - the course load is significant

About the midterm and final exam

You will be tested on your understanding of:

- the content covered in **lectures**

- the content covered during **tutorials**

- the content covered in the challenges including the **handout**, **the commands, and the starter code**

- every **command and line of code** that you have used for producing and running **your solution**

Beyond the course

- Be curious

- Experiment with things (in an ethical hacking way)

- Get yourself up-to-date with the latest security news

Wishing you a fun semester