

CSCD27

Computer and Network Security

Kc Udonsi

# Why security matters?

SECURITY

# 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 textbook costs via online alternatives.

Jeff Greenberg/Getty Images

# CNET

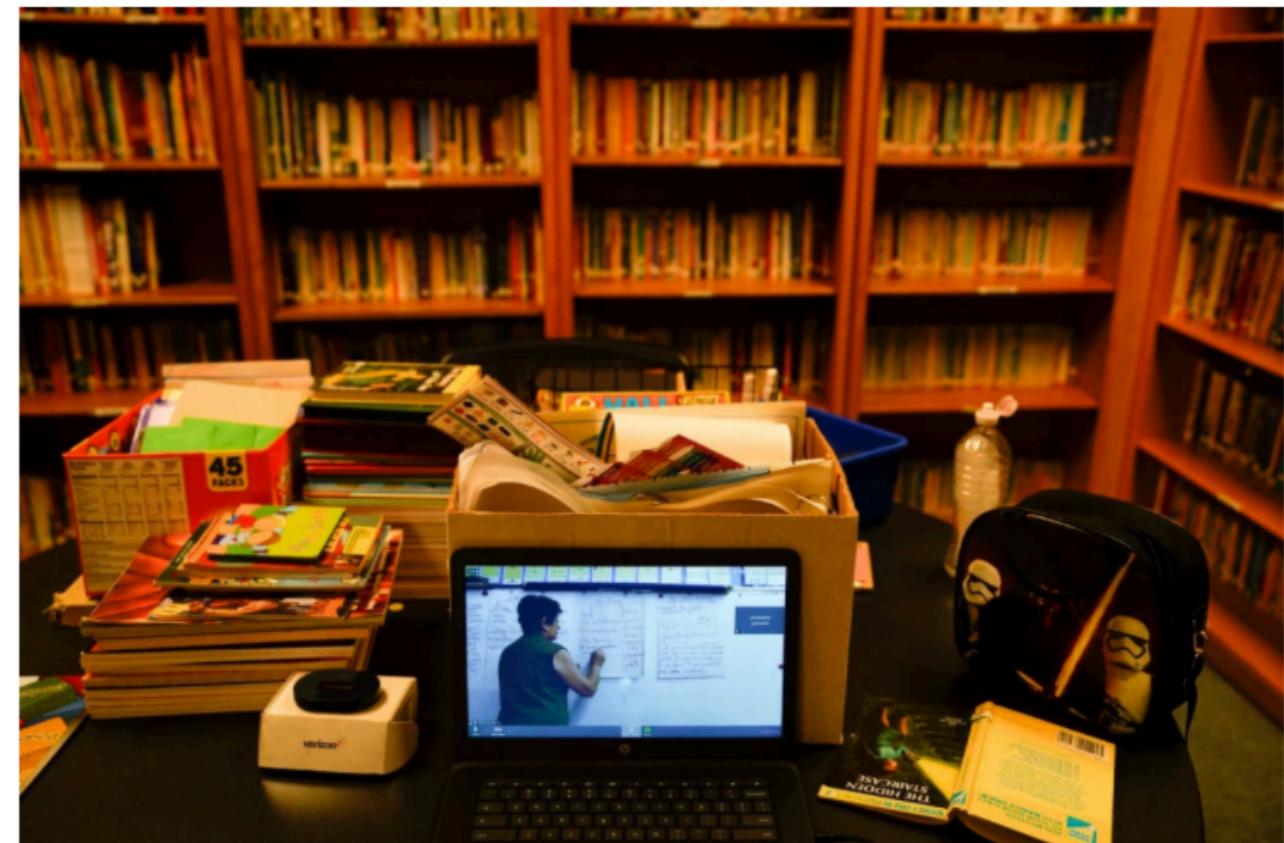
September 2019

# 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



# Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



February 01, 2022

Alert Number  
**I-020122-PSA**

Questions regarding this PSA  
should be directed to your  
local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)

## Scammers Exploit Security Weaknesses on Job Recruitment Websites to Impersonate Legitimate Businesses, Threatening Company Reputation and Defrauding Job Seekers

The FBI warns that malicious actors or 'scammers' continue to exploit security weaknesses on job recruitment websites to post fraudulent job postings in order to trick applicants into providing personal information or money. These scammers lend credibility to their scheme by using legitimate information to imitate businesses, threatening reputational harm for the business and financial loss for the job seeker.

Since early 2019, the average reported loss from this scheme is nearly \$3,000 per victim, and many victims have also reported that the scheme negatively affected their credit scores.

**security.org**

March 2021



## Account Takeover Fraud: A Consumer's Guide to Protecting Yourself



By [Aliza Vigderman](#) | Published March 17, 2021

Account takeover fraud is a type of cybercrime or identity theft where a malicious third-party gains access to (or "takes over") an online account, such as an e-mail address, bank account, or social media profile. In fact, our research shows it's happened to about 1 in 5 adults. In this guide, we break down exactly what account takeover is, how it happens, and most importantly, how to prevent it. Account takeover is often abbreviated as ATO or called account fraud.

**FBI IC3**

February 2022

# Confluence Security Advisory 2022-06-02

Confluence Server and Data Center -  
CVE-2022-26134 - Critical severity unauthenticated  
remote code execution vulnerability

## Zero Day Initiative

June 2022

Atlassian  
Advisories

Still need help?

The Atlassian Community  
here for you.

Ask the community

SUBSCRIBE 

## CVE-2022-26937: MICROSOFT WINDOWS NETWORK FILE SYSTEM NLM PORTMAP STACK BUFFER OVERFLOW

June 08, 2022 | Trend Micro Research Team

## Security advisory - ADAudit Plus Unauthenticated Remote Code Execution Vulnerability

**CVEID:** CVE-2022-28219

**Severity:** Critical

**Affected Software Version(s):** All ADAudit Plus builds below 7060 [How to find your build number]

**Fixed Version(s):** Build 7060

**Fixed on:** March 30, 2022

**Details:** ManageEngine ADAudit Plus had some vulnerable API endpoints that allowed an unauthenticated attacker to exploit XML External Entities (XXE), Java deserialization and path traversal vulnerabilities. The chain could be leveraged to perform unauthenticated remote code execution. This issue has been fixed.

**Impact:** An unauthenticated attacker would be able to remotely execute an arbitrary code in the ADAudit Plus server.

*In this excerpt of a Trend Micro Vulnerability Research Service vulnerability report, Guy Lederfein and Jason McFadyen of the Trend Micro Research Team detail a recently patched code execution vulnerability in the Microsoft Windows operating system. The bug was originally discovered and reported to Microsoft by Yuki Chen. A stack buffer overflow vulnerability exists in Windows Network File System. A remote attacker can exploit this vulnerability by sending specially crafted RPC packets to a server, resulting in code execution in the context of SYSTEM. The following is a*

# ManageEngine Advisories

June 2022

## Cisco hacked by Yanluowang ransomware gang, 2.8GB allegedly stolen

By Sergiu Gatlan

August 10, 2022 04:05 PM 1



August 14th, 2022 update below. This post was originally published on August 10th.

Cisco confirmed today that the Yanluowang ransomware group breached its corporate network in late July. The actor tried to extort them under the threat of leaking stolen files online.

The company revealed that the attackers could only harvest and steal non-sensitive data from a Box folder on a compromised employee's account.

# Bleeping Computer

August 2022

## Bleeping Computer

June 2022

### Conti ransomware hacking spree breaches over 40 orgs in a month

By Ionut Ilascu

June 23, 2022 06:05 AM 0



The Conti cybercrime syndicate runs one of the most aggressive ransomware operations and has grown highly organized, to the point that affiliates were able to hack more than 40 companies in a little over a month.

Security researchers codenamed the hacking campaign ARMattack and described it as being one of the group's "most productive" and "extremely effective."

# 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.

# JOINT CYBERSECURITY ADVISORY

TLP:WHITE

FBI | CISA

Zeppelin actors gain access to victim networks via RDP exploitation [T1133], exploiting SonicWall firewall vulnerabilities [T1190], and phishing campaigns [T1566]. Prior to deploying Zeppelin ransomware, actors spend one to two weeks mapping or enumerating the victim network to identify data enclaves, including cloud storage and network backups [TA0007]. Zeppelin actors can deploy Zeppelin ransomware as a .dll or .exe file or contained within a PowerShell loader. [1]

Prior to encryption, Zeppelin actors exfiltrate [TA0010] sensitive company data files to sell or publish in the event the victim refuses to pay the ransom. Once the ransomware is executed, a randomized nine-digit hexadecimal number is appended to each encrypted file as a file extension, e.g., file.txt.txt.C59-E0C-929 [T1486]. A note file with a ransom note is left on compromised systems, frequently on the desktop (see figure 1 below).



Figure 1: Sample Ransom Note

The FBI has observed instances where Zeppelin actors executed their malware multiple times within a victim's network, resulting in the creation of different IDs or file extensions, for each instance of an attack; this results in the victim needing several unique decryption keys.

# Cybersecurity and Infrastructure Security Agency

August 2022

# Federal Bureau of Investigation

May 2022



May 04, 2022

Alert Number  
**I-050422-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)

## Business Email Compromise: The \$43 Billion Scam

This Public Service Announcement is an update and companion piece to Business Email Compromise [PSA I-091019-PSA](#) posted on [www.ic3.gov](http://www.ic3.gov). This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to December 2021.

### DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and

# Israeli government websites temporarily knocked offline by ‘massive’ cyber-attack

Jessica Haworth 15 March 2022 at 11:55 UTC

Israel DDoS Cyber-attacks



DDoS assault blamed on Iran, local media reports



A “massive” cyber-attack knocked several Israeli government websites offline last night (March 14).

The incident was confirmed online by the Israel National Cyber Directorate, which said that a DDoS services “for a short time”.

# The Daily Swig

May 2022

## Russia behind cyber-attack on satellite internet network KA-SAT that disrupted Ukrainian infrastructure – EU

Adam Bannister 10 May 2022 at 12:52 UTC

Updated: 11 May 2022 at 09:54 UTC

Russia Ukraine Cyber Warfare



Attack took place one hour before Russia invaded Ukraine



**UPDATED** The EU has blamed Russia for a powerful cyber-attack that disrupted satellite broadband services in Ukraine and “helped facilitate President Vladimir Putin’s invasion of the country”.

Thousands of modems were knocked offline by the attack on the KA-SAT network, which took place one hour before Russia’s invasion of Ukraine commenced on February 24.

The incident caused communication outages and other disruptions for government websites and banks in Ukraine, and affected several EU Member States that also use the KA-SAT network.

# The Daily Swig

March 2022

# Hundreds of companies potentially hit by Okta hack

⌚ 23 March



**Hundreds of organisations that rely on Okta to provide access to their networks may have been affected by a cyber-attack on the company.**

Okta said the "worst case" was 366 of its clients had been affected and their "data may have been viewed or acted upon" - its shares fell 9% on the news.

It says it has more than 15,000 clients - from big companies, including FedEx, to smaller organisations, such as Thanet District Council, in Kent.

Cyber-gang Lapsus\$ is behind the hack.

BBC

March 2022

MSRC

March 2022

March 22, 2022 • 17 min read

## DEV-0537 criminal actor targeting organizations for data exfiltration and destruction

Microsoft Threat Intelligence Center (MSTIC)

Detection and Response Team (DART)

Microsoft Defender Threat Intelligence



Share ▾

**March 24, 2022 update** – As Microsoft continues to track DEV-0537's activities, tactics, and tools, we're sharing [new detection, hunting, and mitigation information](#) to give you additional insights on remaining vigilant against these attacks.

In recent weeks, Microsoft Security teams have been actively tracking a large-scale social engineering and extortion campaign against multiple organizations with some seeing evidence of destructive elements. As this campaign has accelerated, our teams have been focused on detection, customer notifications, threat intelligence briefings, and sharing with our industry collaboration partners to understand the actor's tactics and targets. Over time, we have improved

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.

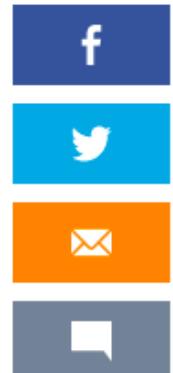
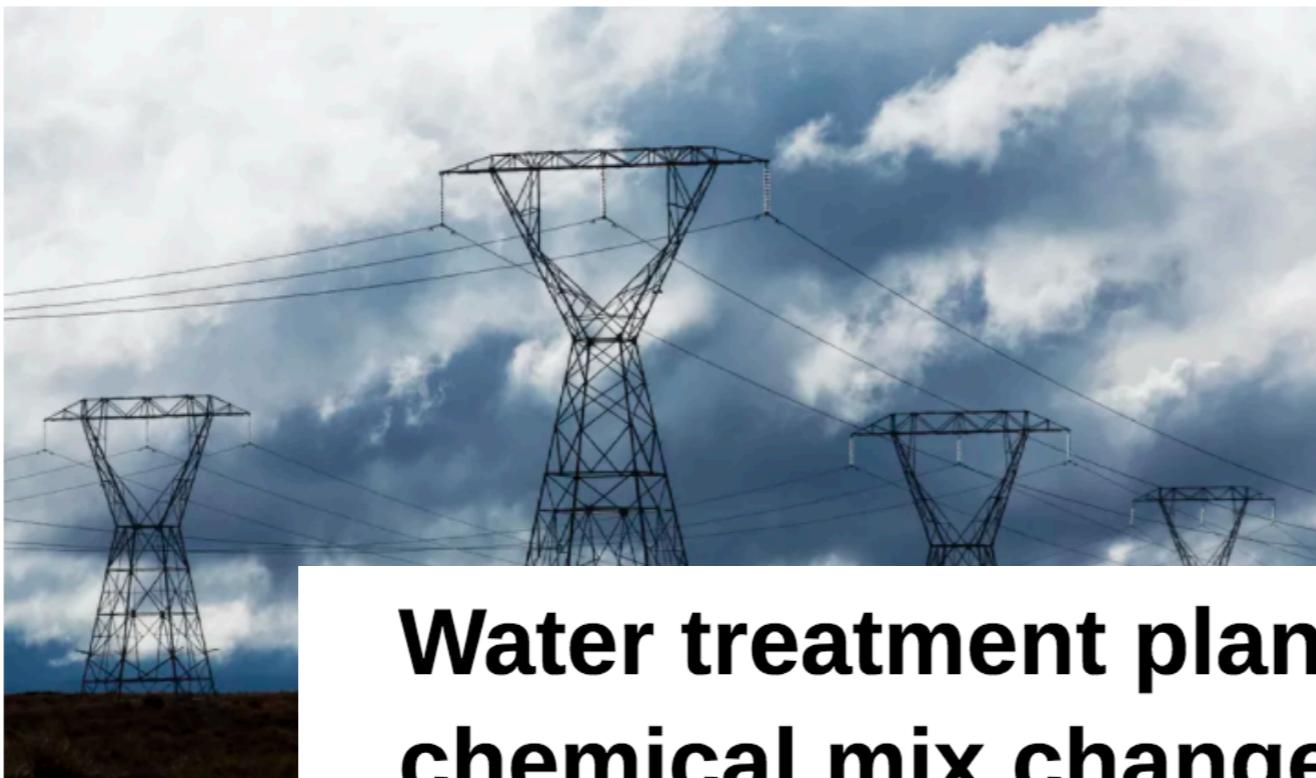
Security



by **Alfred Ng**

6 September 2017 5:56 pm BST

@alfredwng



Hundreds of po

CNET  
September 2017

The Register

March 2016

## 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 U.S. state of Florida and remotely changed a setting that drastically altered hydroxide (NaOH) in the water.

# The Hacker News

# 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.

# Pwn2Own Miami: Hackers earn \$400,000 by cracking ICS platforms

John Leyden 22 April 2022 at 15:06 UTC

Updated: 03 May 2022 at 09:19 UTC

Hacking News Bug Bounty Vulnerabilities



*Industrial control insecurity laid bare during competition*



The second edition of Pwn2Own Miami has thrown up dozens of previously undiscovered exploits to [industrial control systems](#), earning security researchers pay-outs of \$400,000 in the process.

Pwn2Own Miami followed a similar format to more established [hacking](#) contests from Trend Micro's Zero Day Initiative but with a different focus around industrial control systems (ICS) rather than computers or mobile devices.

## The Daily Swig

# bZx crypto heist results in reported losses of more than \$55 million

Adam Bannister 09 November 2021 at 15:46 UTC

Updated: 09 November 2021 at 15:48 UTC

Cryptocurrency Cyber-attacks Phishing



BSC and Polygon funds drained – but Ethereum contracts ‘safe’ – following phishing attack



bZx, the decentralized finance (DeFi) platform, says “possible terms of compensation will be determined after investigating the theft of millions of dollars’ worth of [cryptocurrency](#) funds.

A cybercriminal pulled off the heist after compromising a bZx developer’s PC and wallet’s private keys via a [phishing](#) attack, bZx revealed on Friday (November 5).

The attacker then drained the developer’s wallet and obtained keys to the bZx platform (BSC) deployments.

# The Daily Swig

November 2021

## Hackers Steal Over \$600 Million Worth of Cryptocurrencies from Poly Network

August 11, 2021 Ravie Lakshmanan



## The Hacker News

August 2021

Hackers have siphoned \$611 million worth of cryptocurrencies from a blockchain-based financial network in what’s believed to be one of the largest heists targeting the digital asset industry, putting it ahead of breaches targeting exchanges [Coincheck](#) and Mt. Gox in recent years.

## Flash loan attack on One Ring protocol nets crypto-thief \$1.4 million

Adam Bannister 24 March 2022 at 11:53 UTC  
Updated: 24 March 2022 at 13:30 UTC

Cryptocurrency Finance Cyber-attacks



Price manipulation of LP tokens ejected OShare tokens from protocol



Attackers have stolen \$1.4 million from the One Ring protocol via a flash loan attack, blockchain platform One Ring Finance has revealed.

Losses from the attack, which unfolded on Monday (March 21), totaled \$2 million after swap and flash loan fees, said One Ring, a 'multi-chain cross-stable yield optimizer platform'.

The hacker borrowed \$80 million in USDC with Solidly flash loans to raise the price of the underlying [LP tokens](#) in the block span, according to a One Ring [post-mortem](#) published on Tuesday (March 22).

# FBI, IC3

August 2022

August 29, 2022

Alert Number  
**I-082922-PSA**

Questions regarding this PSA  
should be directed to your  
local **FBI Field Office**.

Local Field Office Locations:  
[www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices)

# The Daily Swig

March 2022

## Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



### Cyber Criminals Increasingly Exploit Vulnerabilities in Decentralized Finance Platforms to Obtain Cryptocurrency, Causing Investors to Lose Money

#### SUMMARY

The FBI is warning investors cyber criminals are increasingly exploiting vulnerabilities in decentralized finance (DeFi) platforms to steal cryptocurrency, causing investors to lose money. The FBI has observed cyber criminals exploiting vulnerabilities in the smart contracts governing DeFi platforms to steal investors' cryptocurrency. The FBI encourages investors who suspect cyber criminals have stolen their DeFi investments to contact the FBI via the Internet Crime Complaint Center or their local FBI field office.

# 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

# CAR HACKING AT DEF CON 26

by: **Mike Szczys**

f t g+



9 Comments

August 11, 2018

# Hackaday

August 2018

## Keen Security Lab

August 2017

Tencent 腾讯 KEEN security lab

black hat

## FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS

Sen Nie, Ling Liu, Yuefeng Du  
Keen Security Lab of Tencent  
{snie, dlingliu, davendu}@tencent.com

### ABSTRACT

In today's world of connected cars, security is of vital importance. The security of these cars is not only a technological issue, but also an issue of human safety. In our research, we focused on perhaps the most famous connected car model: Tesla.

In September 2016, our team (Keen Security Lab of Tencent) successfully implemented a remote attack on the Tesla Model S in both Parking and Driving mode.<sup>[1-3]</sup> This remote attack utilized a complex chain of vulnerabilities. We have proved that we can gain entrance from wireless (Wi-Fi/Cellular), compromise many in-vehicle systems like IC, CID, and Gateway, and then inject malicious CAN messages into the CAN Bus. Just 10 days after we submitted our research to Tesla, Tesla responded with an update using their OTA mechanism and introduced the code signing protection into Tesla cars.

# REGULAR EXPLOITATION OF A TESLA MODEL 3 THROUGH CHROMIUM REGEXP

December 19, 2019 | Jasiel Spelman

[TO THE BLOG](#)



*This is the fourth in our series of Top 5 interesting cases from bugs has some element that sets them apart from the more released by the program this year. Today, we look at the exploit Model 3 in Vancouver at Pwn2Own this year.*

## Zero Day Initiative

December 2019

### Keen Security Lab

August 2018

## New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars

by Tencent Keen Security Lab



After conducting the intensive security analysis of multiple BMW cars' electronic control units, Keen Security Lab has found 14 vulnerabilities with local and remote access vectors in BMW connected cars. And 7 of these vulnerabilities were assigned CVE (Common Vulnerabilities and Exposures) numbers.

### Introduction

The research of BMW cars is an ethical hacking research project. In the research, Keen Security Lab performed an in-depth and comprehensive analysis of both hardware and software on in-vehicle infotainment Head Unit, Telematics Control Unit and Central Gateway Module of multiple BMW vehicles. Through mainly focusing on various external attack surfaces, (including GSM network, BMW Remote Service, BMW ConnectedDrive System, Remote Diagnosis, NGTP protocol, Bluetooth protocol, USB and OBD-II interfaces), Keen Security Lab has gained local and remote access to infotainment components, T-Box components and UDS communication above certain speed of selected multiple BMW vehicle modules and been able to gain control of the CAN buses with the execution of arbitrary, unauthorized diagnostic requests of BMW in-car systems remotely.

# Why do we have security issues?

- **Vulnerabilities**  
Memory access violations, Improper input validation ...
- **Insecure configuration**  
Improper authorization, Incomplete mediation ...
- **Design Weakness**  
Insufficient regard for security in system/protocol design
- **Human error**  
Careless, malicious or uninformed use of digital assets

# Why security should matter to you?

- Because **you** are going to build the next computer systems, networks and software
- Because services and systems **you** trust can become compromised

# Why security should matter to you?

- Because **you** and **your** loved ones and their loved ones use connected digital assets
- Because **you** could be inspired to join the defence ;)



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

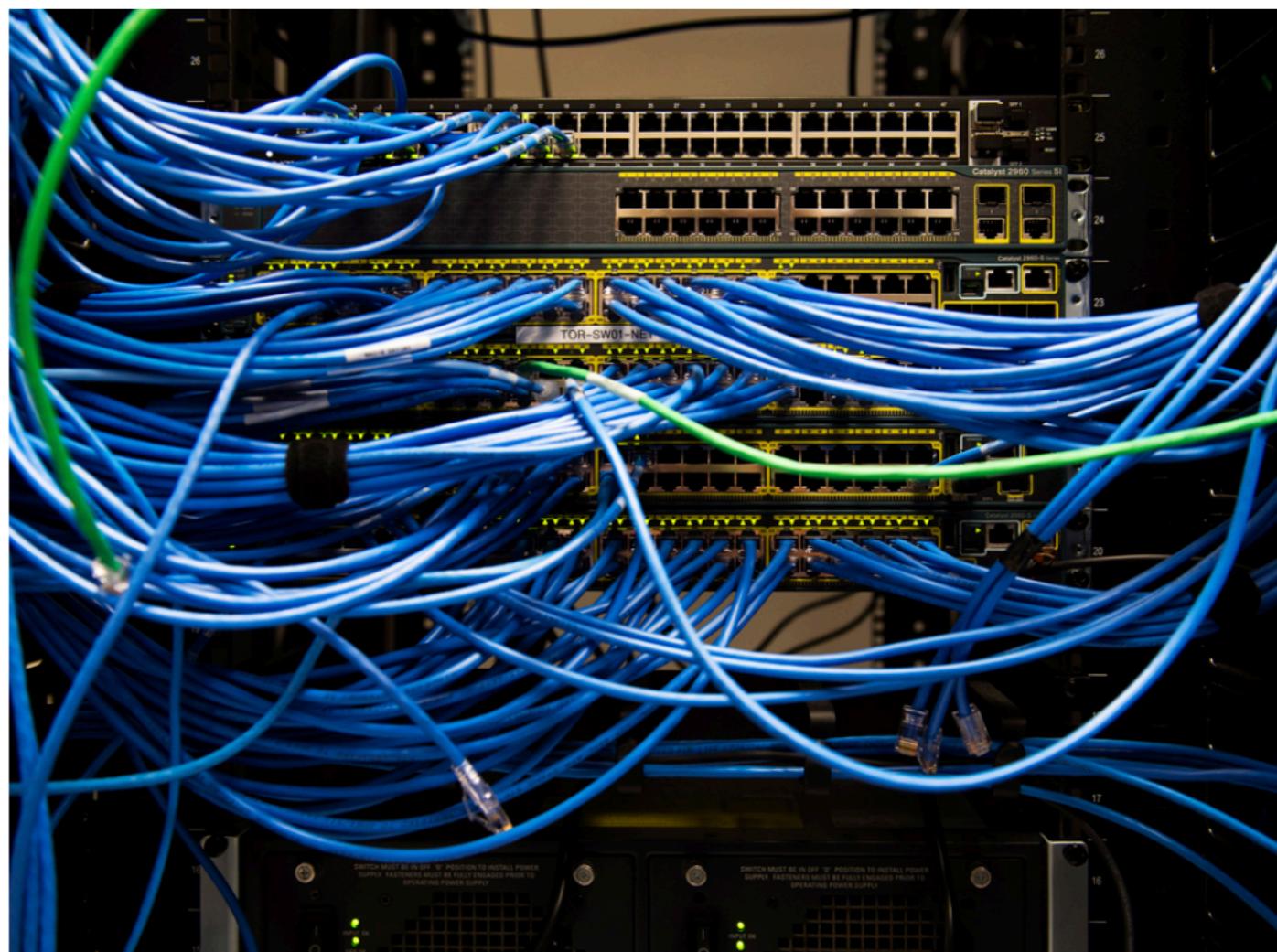
July 2018

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*

Welcome to CSCD27

# Legacy

- **CSCD27 Computer and Network Security**

Alan Rosselet

University of Toronto Scarborough

- **I5-349 Introduction to Computer and Network Security**

Iliano Cervesato, Khaled Harras and Thierry Sans

Carnegie Mellon University Qatar

- **CSCD27 Computer and Network Security**

Thierry Sans

University of Toronto Scarborough

# Who Am I ?

- Not a “Professor”: that’s a **very big** shoe to fill.
- But ...
- Ex-undergrad TA for CSCB09, CSCC69, CSCC01, CSCC37, CSCD27, CSCD58
- Ex-Division Lead, CSEC; Computer and Network Security
- Certified Information Systems Security Professional
- Security Researcher, Engineer and Trainer incl. DFIR
- Disclosed vulnerabilities to Adobe, Microsoft, Apache ...

# 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
  - Network security
  - Software security
  - Human 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. Risk Management
2. Applied Cryptography
3. Network Security
4. System Security
5. Human Security

# I. Risk Management

- Threats and Vulnerabilities
- Risk Analysis
- Total Cost of Ownership
- Risk Choices

## 2. Applied Cryptography

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

# 3. 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

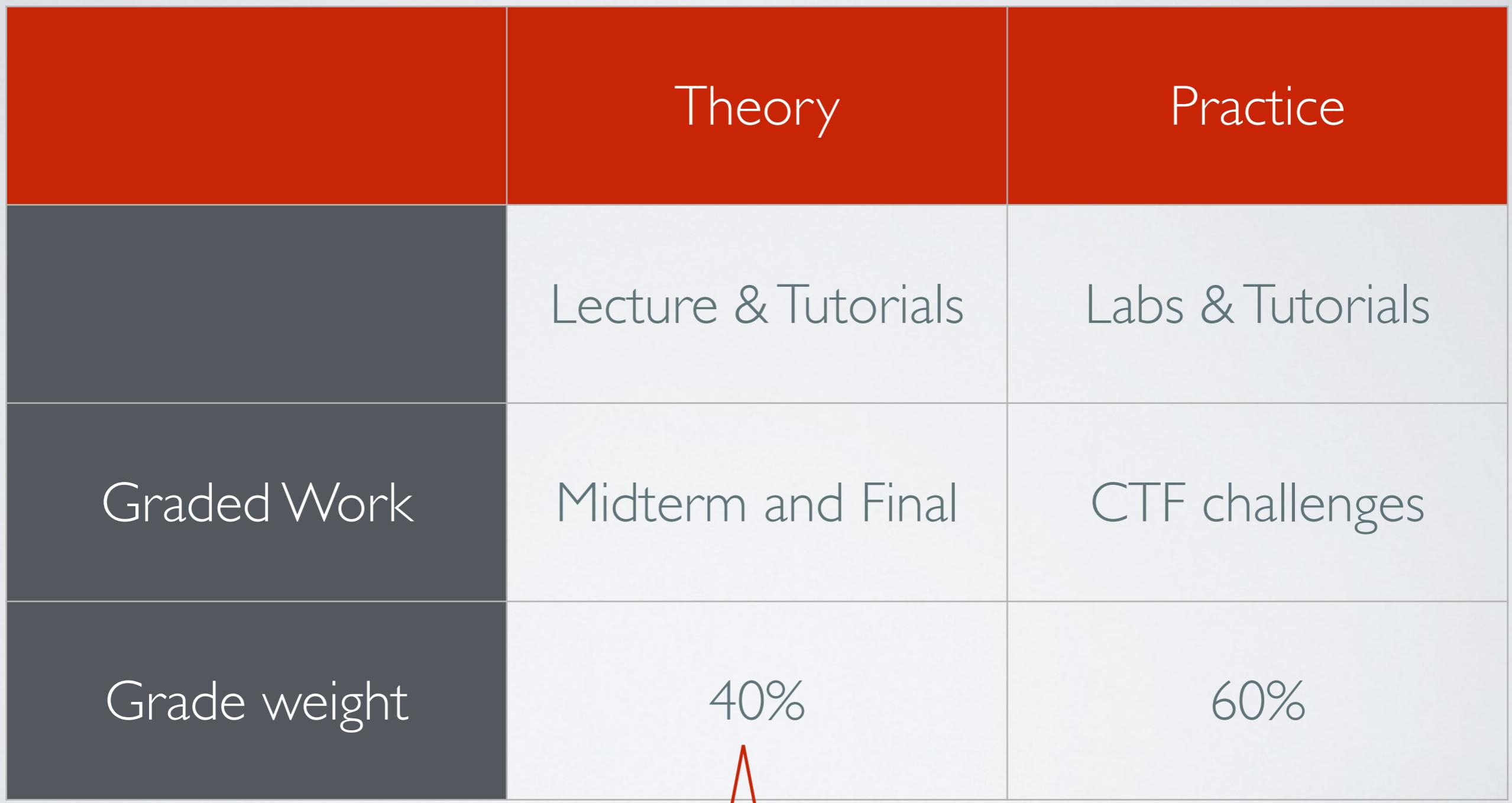
# 4. Software Security

- Operating Systems
- Programs
- Malicious code
- Web Security

## 5. Human Security

- Social Engineering
- Insider threat
- Access control
- Security awareness

# Course work, evaluation and grading



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

# A fully in-person course

- All lectures, labs and tutorials will be held in-person. Lectures are recorded and may be made selectively accessible
  - Some flexibility and failover to account for unforeseen contingency
  - Complete course work in the Linux lab. The course resources will be verified to work in this environment
- ✓ Optionally use your own computer (\*NIX distro). Limited course staff assistance

# 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 strictly enforced
- **Canadian Criminal Code** is strictly enforced

# Course website

[https://glitchnsec.github.io/  
CSCD27H3F22/](https://glitchnsec.github.io/CSCD27H3F22/)

# How to succeed in this course

[https://glitchnsec.github.io/CSCD27H3F22/doc/  
howtosucceed/](https://glitchnsec.github.io/CSCD27H3F22/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