DIGITAL FORENSIC RESEARCH CONFERENCE

School Cyber Risk & Challenges for Community Oriented Policing, Crime Prevention, and Investigations

By

Nicholas Dubois

From the proceedings of

The Digital Forensic Research Conference

DFRWS 2019 USA

Portland, OR (July 15th - 19th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

https://dfrws.org

School Cyber Risk & Challenges for Community Oriented Policing, Crime Prevention, and Investigations

About Me

Junior in High School • Self Taught • Linux Essentials Certified • SANS Netwars Scholarship

STUDENT

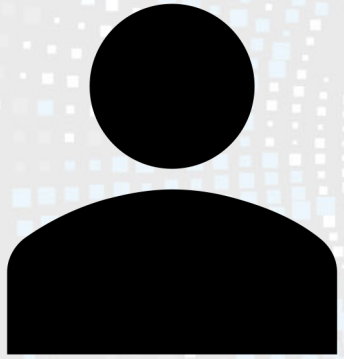
Nicholas Dubois

nick32124@gmail.com

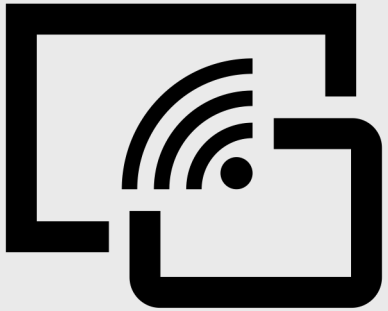
@nick32124

Why Schools?

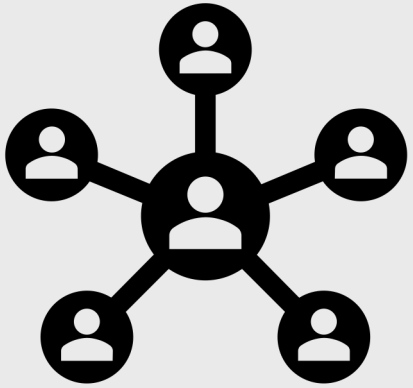
Attack Methods



Physically



Remotely



With Access To Devices

Physically

- Unauthorized people put student’s lives at risk
- Students gain access to restricted facilities
- Can steal from school and students

Physically – 3D Printing Keys

- 3D modeling software, such as Inventor, can be used to precisely copy keys with the use of pictures
- Printers are becoming cheaper and more obtainable

  (Often found in schools)

Physically – 3D Printing Keys

Physically – RFID Cards

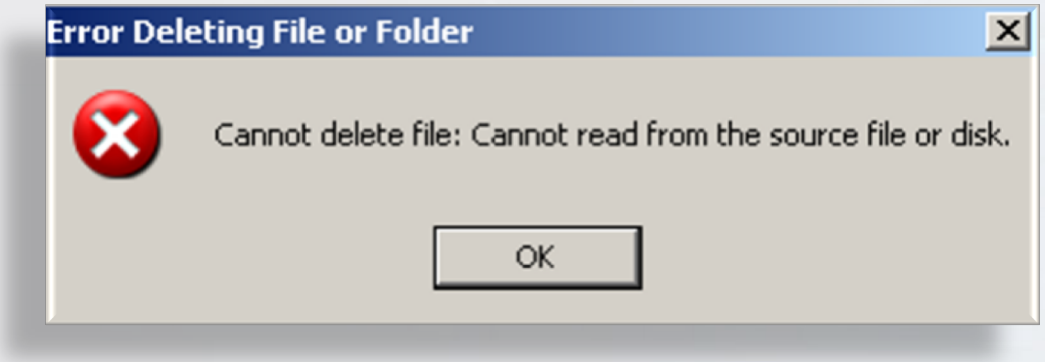
- If provided with tools such as long range RFID card readers found at places of work can **walk by and steal card data** from feet away

- Short range readers can be found/made cheaply and **used to read cards closely**

Remotely

Poor security can lead to:

- Corruption of files
- Stealing test/answers
- Accessing teacher and student files (including social security numbers, medical records)



Remotely- WiFi attacks

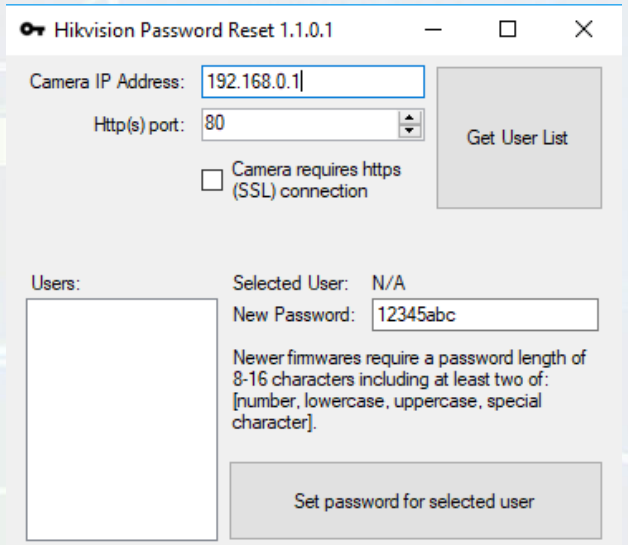
- Ability to shut down and DOS Wireless systems with linux and pineapple
- Google Drive

Remotely – Website Vulnerabilities & Captive Portal Clones

- Many school websites run old unpatched Apache systems which **may be changed easily**
- Attackers can use Wireshark or a packet analyzing tool to **find http usernames and passwords**
- Laptops and Wi-Fi Pineapples can be used to **copy and clone** guest Wi-Fi logins and websites

Remotely – Cameras

- IOT and CCTV cameras **need to be updated** frequently to avoid security breeches
- Hikvision Cameras



Remotely – Old Systems 

- Largest current threat for schools is **old systems** (especially public schools)
- **54%** of businesses and organizations still use Windows XP*
- Unpatched, old Windows XP can be **remotely exploited** using the MS08-67 exploit, then keyloggers can be planted to store usernames and passwords

*Spiceworks survey (2017)

Remotely – Printers

Everything printed on a wireless printer is stored, including:

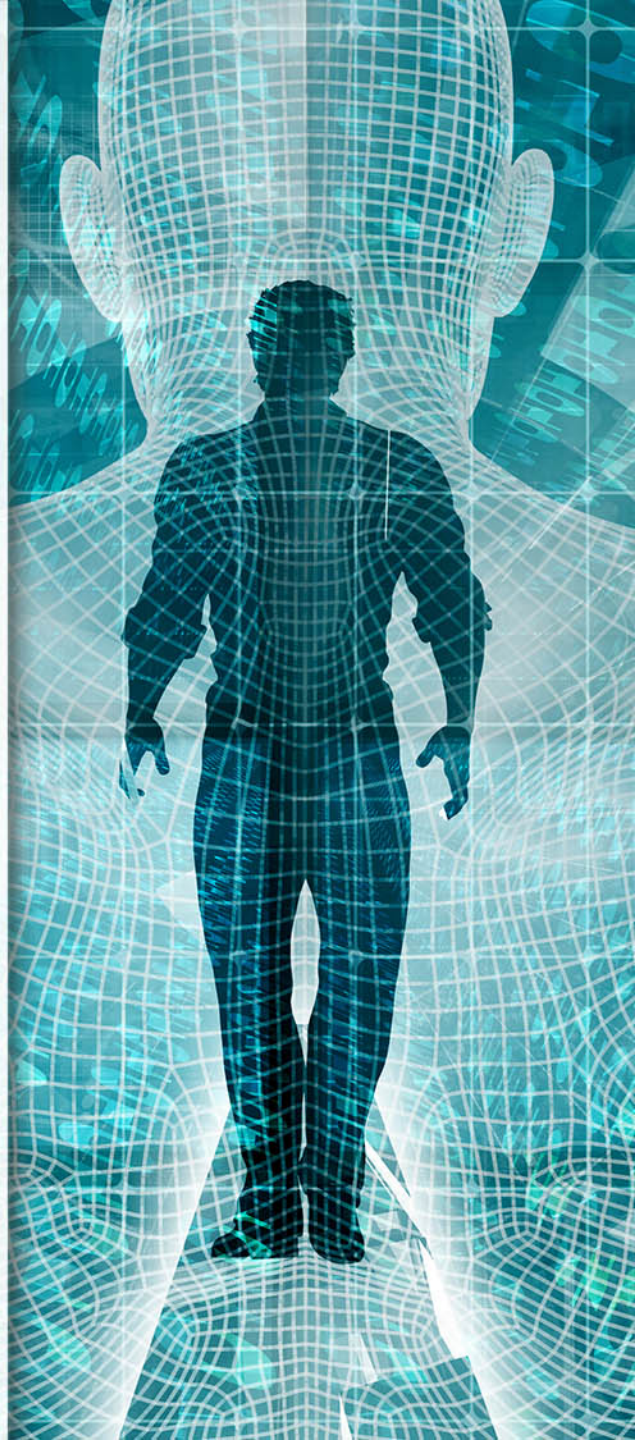
- Answer keys
- Teacher information
- Student transcripts

PRET, a printer exploitation toolkit, can **copy, delete,** and **modify files** stored on printers

With Access to Devices

- These are the **most common** attacks on schools

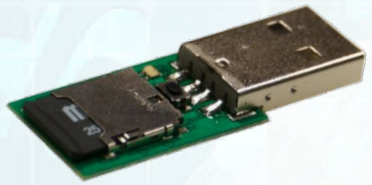
- Bash Bunny and USB Ducky tools can be used to play keyboard inputs and create backdoors or keyloggers



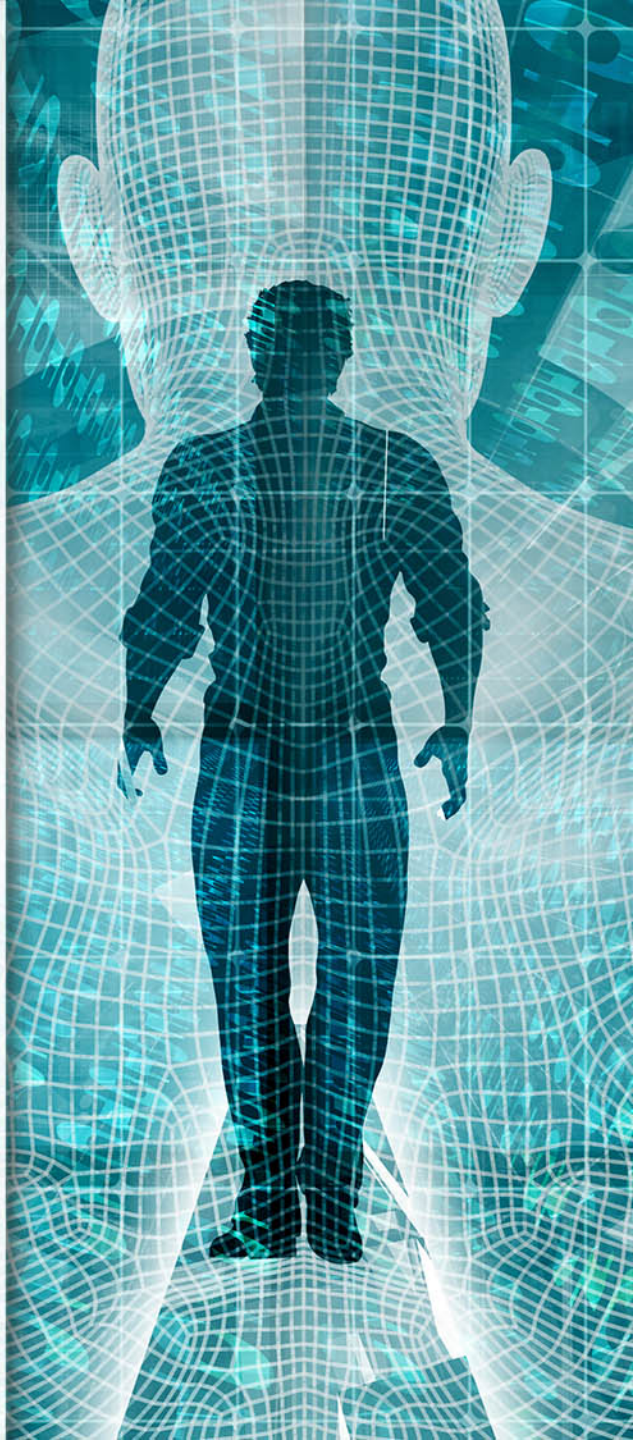
With Access to Devices- Tools

- Wi-Fi Pineapple

- USB Rubber Ducky



- Bash Bunny



Standardized Testing

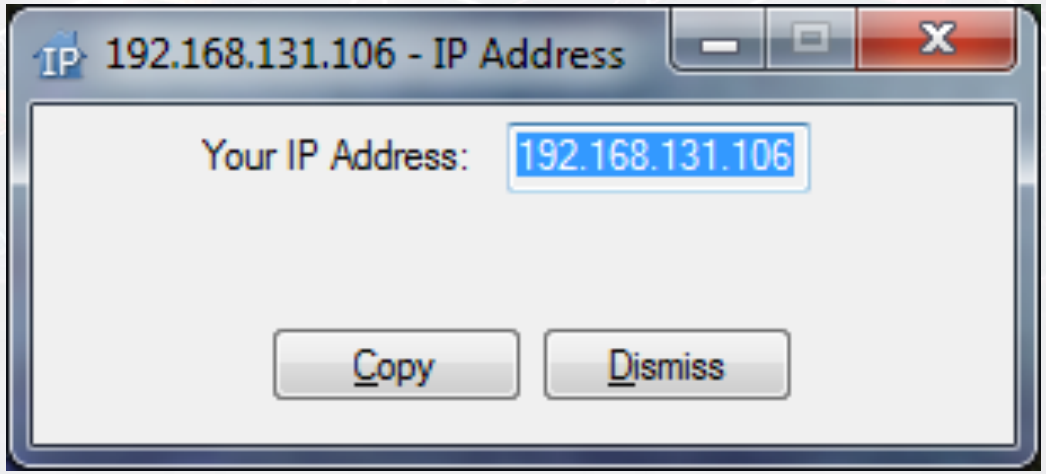
MCAS - Massachusetts Comprehensive Assessment System

- Mandatory for every student in an MA public high school
- Currently transitioning to a new computerized system
- Scores used to offer scholarship money to students
- Schools are rated based on how students rank on MCAS

Program prevents the user from exiting the program and accessing others, but with the use of remote exploitation or keyboard enumeration, this can be bypassed

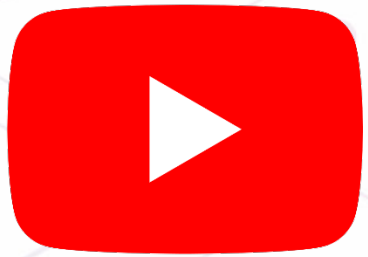
Detection ⚠

- Monitor MAC Addresses and IPs of those who connect to networks with sensitive information (dedicated Linux systems optimal or just monitoring gateway)



Prevention- Know The Attacker

Students Can Hack You!



Prevention 

- Give administrators a separate Wi-Fi to access which **only they have access to**
- Update systems as **frequently as possible,** try not to run unpatched OSs’
- **DO NOT store passwords** on computers accessible by students
- Educate teachers and teach them caution - many students are capable of hacking school systems

Thank You! Questions?

STUDENT

Nicholas Dubois

nick32124@gmail.com

@nick32124