EXFILTRATING DATA FROM AN ISOLATED COMPUTER SYSTEM

Project ID: #2722

(Any Non-Referenced Images are Creative Commons or the creator's own images

CYBERSECURITY IMPORTANCE

COLONIAL PIPELINE ATTACK

This 2021 ransomware virus led to gas shortages all over the US

NASA SYSTEMS ATTACK

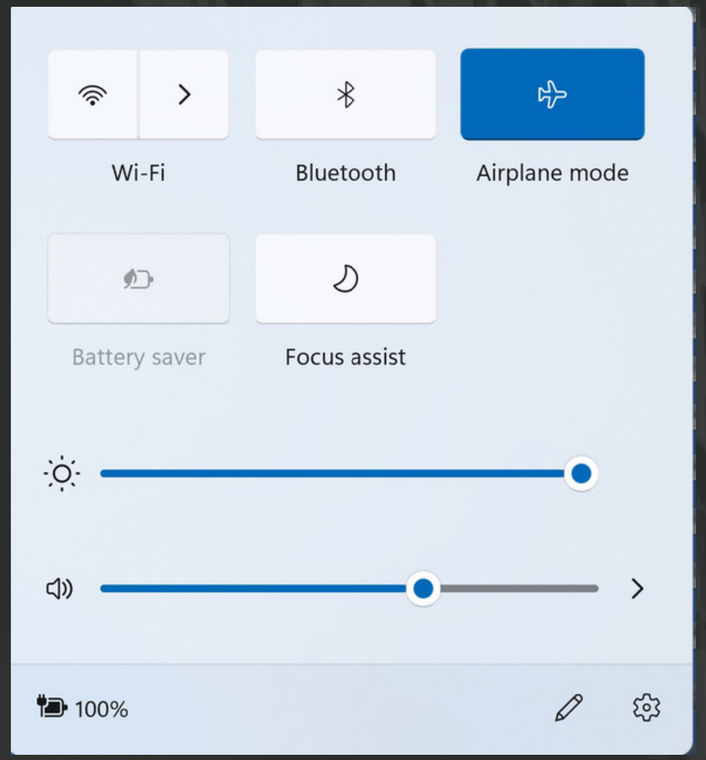
The start of the pandemic in 2020 saw a record 1,785 cyber attacks against NASA

HEALTHCARE CONFIDENTIALITY

A 41% increase in attacks on healthcare IT information was reported in 2021

TESTING THE AIR-GAP (ISOLATED SYSTEM)

PURPOSE: DEMONSTRATE HOW THE SECURITY GOLD STANDARD OF AIRGAPPING CAN BE COMPROMISED

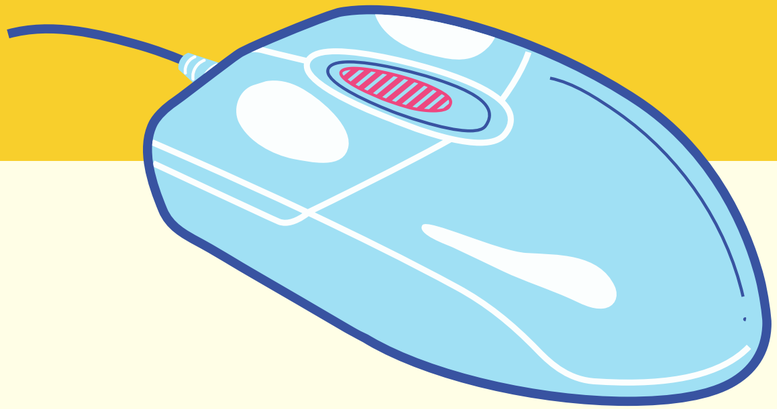


(Screenshot from my air-gapped computer)

AIR-GAP CREATED:

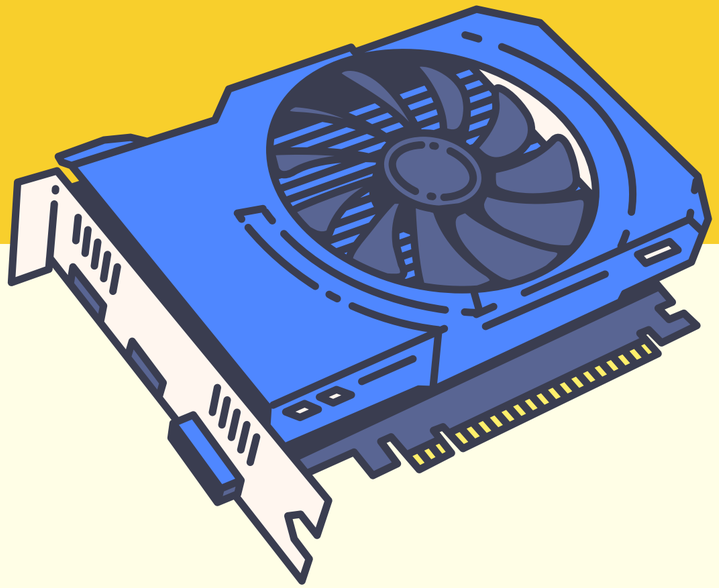
DISCONNECTING DEVICE FROM WIFI OR BLUETOOTH

Sensory Methods for Data Exfiltration



THE MOUSE

An accelerometer can analyze modulations in mouse clicks to decipher a message



GRAPHICS CARD

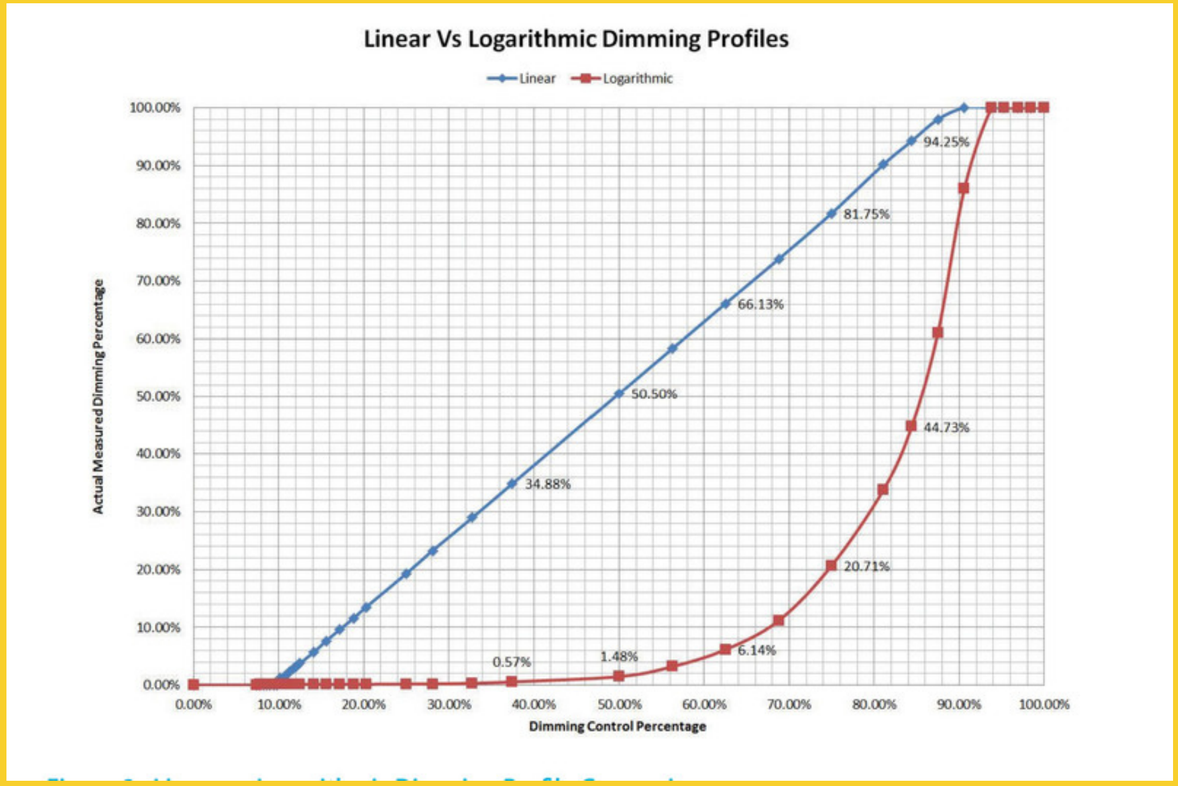
Temperature modulations in the graphics card of an air-gapped device can be used to transmit data from supposedly secured files

SCREEN BRIGHTNESS

Screen brightness fluctuations can transmit binary signals that can be used to decode the data

DETERMINING THE BEST METHOD

PERCEPTIVE VS ACTUAL SCREEN BRIGHTNESS

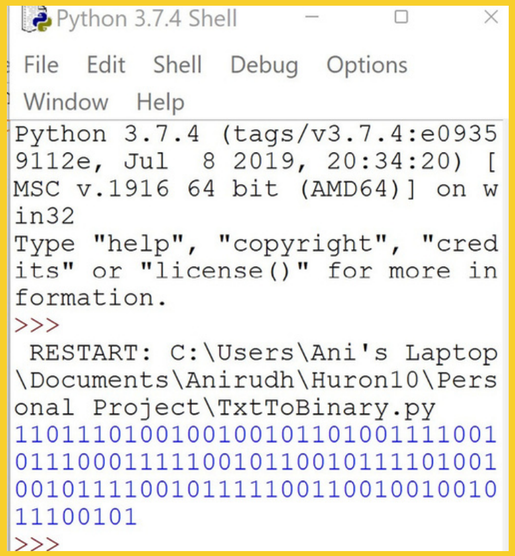


(From Reference #10)

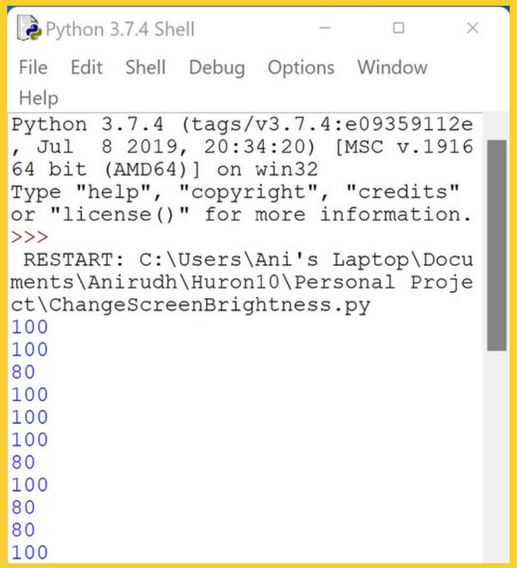
Until 40% actual dimming has occurred, there is barely any change in perceptive dimming

=> SCREEN BRIGHTNESS IS THE MOST EFFECTIVE TO SUCCESSFULLY BREACH THE AIRGAP WITH THE LEAST NOTICE

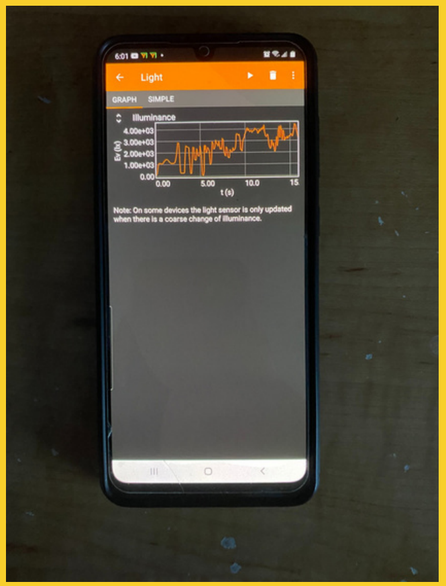
Process



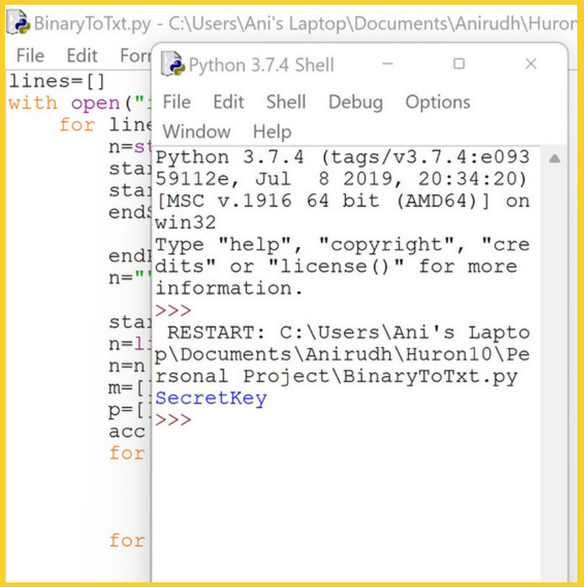
The secured file in the air gapped computer contains "SecretKey", which is promptly converted to binary



Screen Brightness of the air-gapped system is adjusted every second based on the binary



Phyphox Sensor Captures the modulations

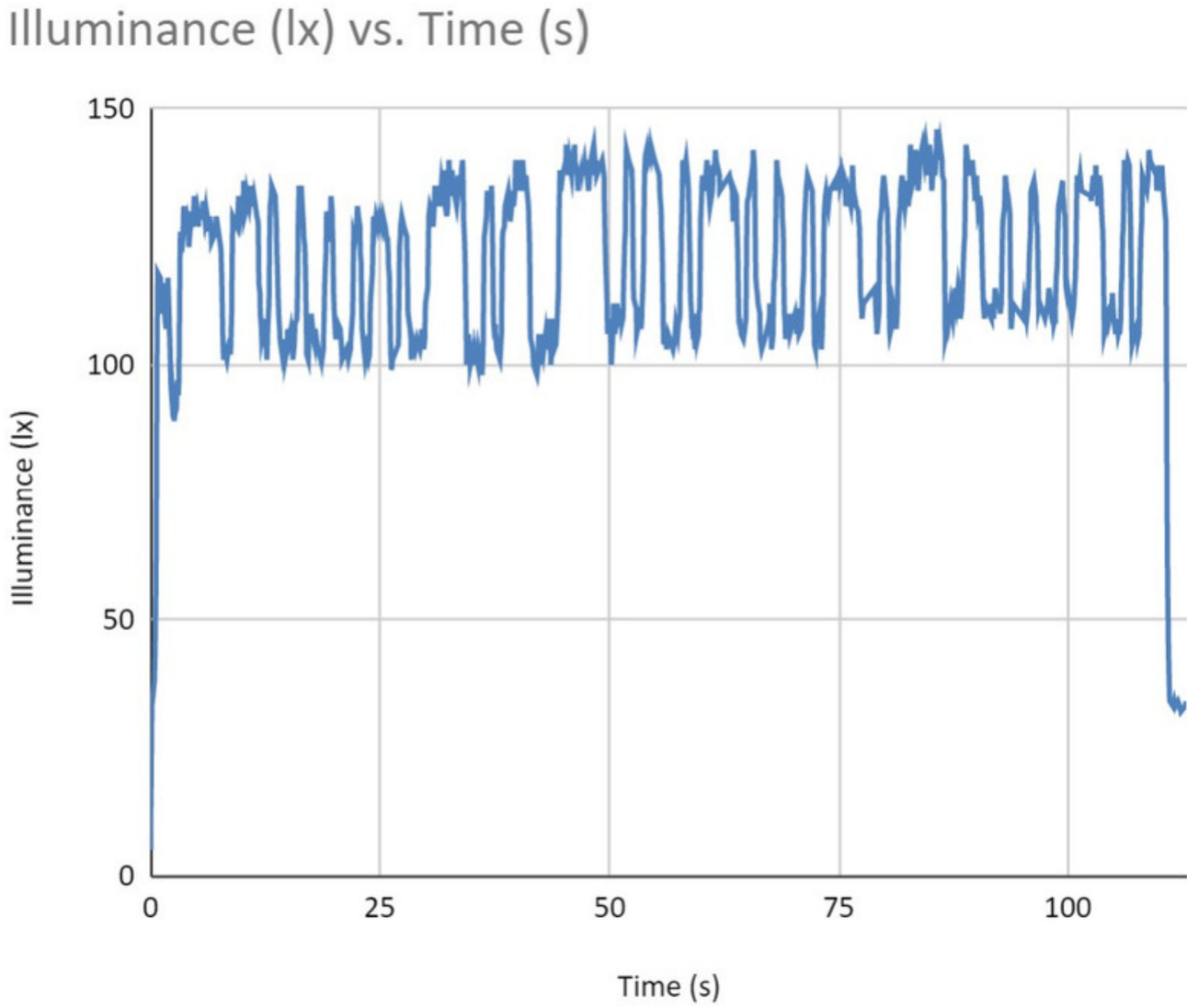


The data is intepreted back as binary and converted to "SecretKey" on the hacker's own computer

DATA ANALYSIS

MEAN LUMINESENCE = 118.266 LX

This shows my readings of the luminescence at every second. The mean of my data was used as a benchmark to categorize the data intepretation in binary to recapture the message



(Data collected from my experiment)

PREVENTION

GIVEN THAT THE GOLD STANDARD OF CYBERSECURITY CAN BE HACKED WITH SUCH ACCURACY, WE MUST IMPLEMENT THE FOLLOWING SECURITY FEATURES IN ALL OF DEVICES TO ENSURE DATA PROTECTION OF OUR MEDICAL RECORDS, NUCLEAR SECRETS, SPACE RESEARCH, ETC

MULTI-FACTOR AUTHENTICATION (MFA)

- The Gas Line attack could have been prevented if the proper MFA had been implemented
- Prevents the initial social-engineering breach in the air-gapped system that was assumed in my experiment

CORE FILE ENCRYPTION

- Provides a last line of defense to ensuring the privacy of data
- My python algorithm contained a start and end key to be able to time the capture in modulation
  - Encryption of the file itself will make it much harder for hackers to create reliable keys and will discourage them from trying to steal information

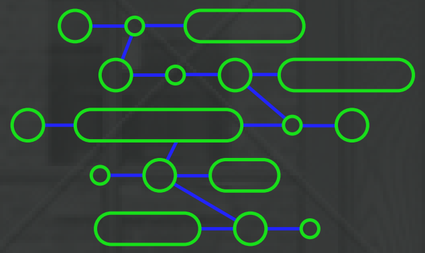
APPLICATIONS IN HEALTHCARE

- Air-Gapping is used to store records for correct medical dosages
  - Air-gap breaching and a loss of data integrity could result in doctors overdosing their patients by accident
  - File encyption is necessary (Nowadays especially) to go along with Air-Gapping as the final layer of security

APPLICATIONS IN SPACE

- Air-Gapping technology has been recently implemented into satellite communications and data services
  - Air-gap breaching and a loss of data integrity could result in multi-million dollar damages
  - Multifactor Authentication across the different space communication platforms will be the best complements for these new-gen air-gaps being implemented

Future Opportunities



NEWER TECHNOLOGIES

Quantum Computing and Magnetic Spintronic Devices provide more opportunities for magnetic transmission

INCREASED TRANSMISSION RANGE

Magnetic waves from disk drives and RAM’s of the computers can be used to transmit data.

COMPETITIVE ADVANTAGE

These magnetic transmissions can be used to gain competitive advantages international digital defense

CONCLUSION

"The perception that 'Next Gen' Air-gapping technologies result in 100% security is incorrect. They must be supplemented with other prevention measures like MFA and File Encryption in order to better protect our digital assets"

- #2722

References

1. “Beating the Air-Gap: How Attackers Can Gain Access to Supposedly Isolated Systems.” Energy Central, 24 Aug. 2018, https://energycentral.com/c/iu/beating-air-gap-how-attackers-can-gain-access-supposedly-isolated-systems.
2. Bloomberg - Are You a Robot? https://www.bloomberg.com/tosv2.html?vid=&uuid=f7192cdb-9117-11ec-bb56-5a4765464356&url=L25ld3MvYXJ0aWNsZXMvMjAyMS0wNi0wNC9oYWNrZXJzLWJyZWFjaGVkLWNvbG9uaWFsLXBpcGVsaW5lLXVzaW5nLWNvbXByb21pc2VkLXBhc3N3b3Jk. Accessed 19 Feb. 2022.
3. COVID-19 Cyberthreats. https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats. Accessed 19 Feb. 2022.
4. Cyber Defense of Space Assets - Cs.tufts.edu. https://www.cs.tufts.edu/comp/116/archive/fall2016/rhutchins.pdf.
5. Cybersecurity Threats in Space: A Roadmap for Future Policy | Wilson Center. https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy. Accessed 19 Feb. 2022.
6. “How Can Hospitals Protect Their Medical Equipment from Malware?” Healthcare IT News, 26 June 2015, https://www.healthcareitnews.com/blog/how-can-hospitals-protect-their-medical-equipment-malware.
7. How to Install Packages Using PIP & IDLE. www.youtube.com, https://www.youtube.com/watch?v=vez6UAtixHU. Accessed 19 Feb. 2022.
8. “Kubos Leverages Replicated To Provide Air Gap Installs to Their Most Security-Conscious Customers.” Replicated, https://www.replicated.com/case_study/kubos/. Accessed 19 Feb. 2022.
9. Landi, Heather. “Healthcare Data Breaches Hit All-Time High in 2021, Impacting 45M People.” Fierce Healthcare, 1 Feb. 2022, https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people.
10. Linear vs. Logarithmic Dimming — a White Paper. https://www.pathwaylighting.com/products/downloads/brochure/technical_materials_1466797044_Linear+vs+Logarithmic+Dimming+White+Paper.pdf.
11. NASA. NASA, https://oig.nasa.gov/docs/IG-21-019.pdf.