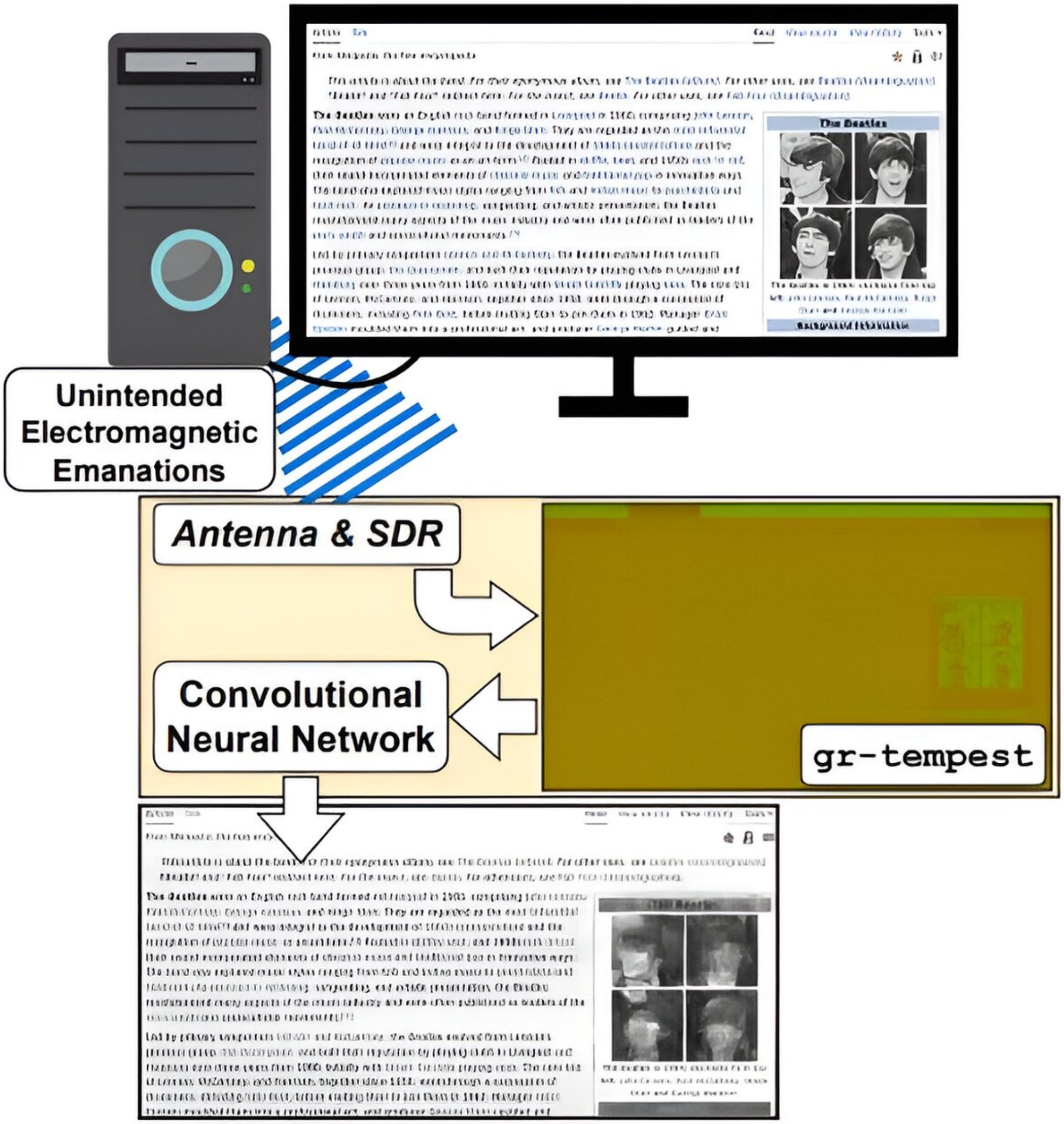
TechXplore

Security researchers reveal it is possible to eavesdrop on HDMI cables to capture computer screen data

July 30 2024, by Bob Yirka


Unintended Electromagnetic Emanations
Antenna & SDR
Convolutional Neural Network
gr-tempest

Proposed system. The HDMI cable and connectors emit unintended electromagnetic signals, which are captured by the SDR and processed by gr-tempest, obtaining a degraded complex-valued image, which in turn is fed to a convolutional neural network to infer the source image. All three images correspond to actual results. Credit: *arXiv* (2024). DOI: 10.48550/arxiv.2407.09717

A trio of computer security researchers at Universidad de la República Montevideo, in Uruguay, reports that it is possible to reproduce text on a computer screen by eavesdropping on its HDMI cable. Santiago Fernández Emilio Martínez, Gabriel Varela, and Pablo Musé Federico Larroca, have published a paper describing their discovery on the *arXiv* preprint server.

Back in the days of CRT-based computer screens, hackers learned early on that it was not difficult to translate the electromagnetic radiation emissions into imagery that revealed the contents of someone else's computer screen. When the industry moved to LED-based screens, which use HDMI cables, hacking became much more difficult due to the vastly more complex signaling. In this new study, the team in Uruguay has found that applying AI to the problem makes it possible.

The work involved capturing electromagnetic radiation emitted from a computer's HDMI cables. They then trained an AI system by giving it screen samples associated with radiation signals moving through the computer's HDMI cable. Over time, the system gradually grew better at deciphering the text displayed on a given computer screen.

Testing showed the system capable of reconstructing text from a random computer screen with 70% accuracy. Good enough, the research team suggests, for most people to get the gist of text on a given computer screen. They also note it is likely good enough to steal passwords, sensitive data, or in some cases, encrypted communications. The researchers found they could improve their results by using text recognition software on the text after it was deciphered.

The researchers suggest hackers have likely already conducted similar research, meaning such screen-grabbing is probably already targeting hapless users. All it would take, they note, is hardware capable of capturing the electromagnetic radiation emitted by HDMI cables placed near a building, such as in the back seat of a car.

The team further suggests that most people are not at risk of such an attack, however, due to the skillset the technique requires. Instead, they suggest it is much more likely a government or corporate entity would be targeted.

More information: Santiago Fernández et al, Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations, *arXiv* (2024). DOI: 10.48550/arxiv.2407.09717

Code: github.com/emidan19/deep-tempest

Citation: Security researchers reveal it is possible to eavesdrop on HDMI cables to capture computer screen data (2024, July 30) retrieved 30 July 2024 from https://techxplore.com/news/2024-07-reveal-eavesdrop-hdmi-cables-capture.html