Wearable RF-shield repositories

Abe Wits
Zurich
melon.mouse.games@gmail.com

J. Mijn
Bos en Lommer
/dev/null

ABSTRACT

We propose the use of wearable RF-shield repositories as a cost effective and realistic alternative to conventional protective measures in the fight against adversarial cables with RF capabilities.

1. INTRODUCTION

Radio Frequency (RF) transceivers (e.g. WiFi) can be hidden in the connector of a fully functional (USB) cable. Such a bugged cable can then be used for a range of attacks, including keylogging, injecting keystrokes and loading payloads on boot. Once a bugged device has found its way into an organization, it can be controlled remotely, up to ranges reaching kilometers. In 2008, this type of device was available to three letter agencies at a unit cost of 20k$ [5]. Today, they are available to anyone at a unit cost of around 100$ [6]. As a result, most organisations and valuable individuals should take defensive measures against bugged cables.

One state-of-the-art defence strategy is to ban or severely limit the use of cables (e.g. by cementing ports) in an organisation. However, this requires expensive modification of equipments, and complicates the use of hardware.

Another is to build a Faraday cage to shield an entire room or building [4]. This is even more expensive, limits the use of wireless networks, and ties equipment to dedicated physical locations.

A more flexible approach is careful supply-chain management. It is difficult and expensive to fully eliminate external access to company hardware. This problem can be partially alleviated by certifying cables. Certified cables can be recognized by labels or by using hard to mimic hardware [Fig 1]. This may deter an attacker unwilling to invest in faking certification. However, this defence strategy incurs significant costs and risks. When certified cables are unavailable, an employee may not be able to perform their job. Worse, an employee may be tempted to use an uncertified cable.

Figure 1: Hardware customization can ease the identification of a Certified USB cable (left) and makes a generic malicious USB cable (right) stand out. Source [3].

We propose a novel, inexpensive and practical strategy that allows for the use of uncertified cables, while providing full RF-cable attack immunity.

2. METHOD

RF-shield material can be molded around a cable to form a Faraday cage. We found that consumer-grade RF-shield material suffices, and should be preferred for financial and logistical reasons [2]. To allow the adhoc use of uncertified cables without a trip to the warehouse, a ready supply of RF-shield material should be carried by each employee in a portable repository. There are storage constraints - RF-shield material should not be crumpled or folded, as this could limit its efficacy. And organisational constraints exist - we rely on employees to follow protocol. To promote a positive culture and awareness around RF security, the RF-shield should be carried by employees in a visible manner. The visibility and storage constraints can be simultaneously satisfied by mandating that all employees carry a wearable RF-shield repository around the cranium. Material can be conveniently taken out of this repository at times of RF-shielding needs.

3. DISCUSSION

We recommend practicing placing RF-shield material around known RF-emitting devices before relying on our technique for mission-critical processes.

A wearable RF-shield repository has some side effects. Qualitative research has revealed that it may cause third parties to keep a distance. It appears to preemptively repel cyber security attacks and social interactions. We suspect this is due to third parties attributing strong cyber security skills to the individual wearing a RF-shield repository.

However, there are downsides to the visibility of the wearable RF-shield repository. An adversarial actor could deduce that you, being a visibly competent cyber security expert, are a worthwhile target for cyber espionage. We therefore recommend always combining a wearable RF-shield repository with anonymity enhancing apparel. The balaclava is effective and readily available, but illegal in several countries, including la France [1]. A more widely acceptable solution is the use of shades. A downside to them is that they potentially create an optical-reflection side-channel [Fig 2]. As a defensive strategy, we recommend the use of anti-reflective gadgets [Fig 3].

4. REFERENCES

[1] Assemblée Nationale, Projet de loi interdisant la dissimulation du visage dans l'espace public. `assemblee-nationale.fr/13/ta/ta0524.asp`, 2010.

Figure 2: Notice the optical reflection sidechannel.

[2] EAFA. `www.alufoil.org/files/alufoil/trophies/2020/PressRelease/EAFA-Alufoil-Trophy-2020_Summary-PR_GB.pdf`.

[3] W. Ebshop. Certified Cable. `cafago.com/en/p-pa4185-1.html`.

[4] T. Liu and Y. Li. *Standard Study of Electromagnetic Information Leakage and Countermeasures*, pages 217–230. Springer Singapore, Singapore, 2019.

[5] NSA. Cottonmouth, NSA ANT. `en.wikipedia.org/wiki/NSA_ANT_catalog`, 2008.

[6] OMG. We are not including free ads for malicious tech in scientific work. Search for it yourself if you must., 2019.

Figure 3: Wearable RF-shield repository, anonymity-enhancing apparel and anti-reflective gadgets.