

Když vás vlastní hardware zrazuje

Skryté hrozby v kapse

Zboření iluze o bezpečí běžné spotřební elektroniky, kterou denně nosíme do školních tříd i kabinetů.

Laboratoř penetračních testů
Fakulta aplikované informatiky UTB ve Zlíně

Považujeme je za pomocníky. Co když “a někdy i tzv. v našem zájmu” skenují naše životy a profilují naši osobnost, náš svět?

📱 Nositelná AI elektronika (technologie pod kůží)

Neustálý odliv telemetrie, polohy a systémových dat do zahraničních cloudů bez vědomí uživatele. Mikrokamera a mikrofon v “běžných” brýlích

🔌 Obyčejně vyhlížející USB kabely

Miniaturní čip uvnitř konektoru emuluje klávesnici a odesílá příkazy přímo do operačního systému. Kapesní hackovací multitooly které umí skenovat čipy.



Image sources: <https://cybersecurityventures.com/wp-content/uploads/2026/06/WireBadgergraphic-2.pn>

Jak rychle dokáže hardware selhat či zaútočit?

3s

Převzetí kontroly

Doba zapojení BadUSB kabelu do instalace zadních vrátkek.

24/7

Odliv dat do cloudu

Nepřetržité odesílání mikrofonních záznamů a polohy z aplikací. Nepřetržitý přenos záznamů z nositelné AI elektroniky a kamer.

1s

Klonování čipu

Zkopírování karty do docházky či jídelny při míjení na chodbě.



Tradiční antivirus ani školní firewall hardwarový útok a klonování čipů nedokáže detekovat

Navazující program • 30 minut živých ukázek

Co uvidíte v praxi na workshopu PTLAB?



1. Živá ukázka jak klonovat čipy

Ukázka jak lze snadno klonovat čipy, karty a rušit bezdrátové sítě



2. Analýza cloudového toku

Sledování dat, které telefony odesílají na vzdálené servery.



3. Kuchařka zabezpečení

Návod na zabezpečení telefonů učitelů i žáků.

Přijďte se podívat, jak tenká je hranice mezi důvěrou a kompromitací.

Těšíme se na vás na praktické části penetrační laboratoře PTLAB.

Pokračujeme na workshopu