

CYBERSÉCURITÉ DES SYSTÈMES EMBARQUÉS : ÉTUDE DES COMPOSANTS, PROTOCOLES, Outils D'ANALYSE ET TECHNIQUES D'ATTAQUE ET DE DÉFENSE EN CYBERSÉCURITÉ PHYSIQUE ET RADIO

ABDEL-MALIK FOFANA
MAÎTRE : LUC BOUGHANIM (INRIA)
TUTEUR : PATRICE MARTIN (UNIVERSITÉ PARIS CITÉ)

INTRODUCTION

- Étude de composants : MCU, EEPROM, TPM, etc.
- Tests pratiques avec Flipper Zero, ESP32, EEPROM Reader
- Expérimentations sur Wi-Fi, Bluetooth, NFC, EEPROM

EXPLICATION DES TERMES ET COMPOSANT

MICROCONTRÔLEURS (MCU, CPU, SOC, STM32, ESP32)

- Les MCU regroupent un CPU, de la mémoire et des entrées sorties sur une seule puce.
- Les SoC intègrent aussi des fonctions comme le Wi-Fi ou le Bluetooth (ex : ESP32).
- Les STM32 sont des microcontrôleurs 32 bits modulaires, très utilisés dans l'industrie.
- Ces composants pilotent les objets connectés, les capteurs, ou les systèmes critiques.

STOCKAGE EMBARQUÉ (EEPROM, EMMC, NVME, HDD, SD)

- L'EEPROM est utilisée pour stocker des clés, des identifiants ou des configurations.
- Les cartes SD et eMMC sont courantes dans les systèmes embarqués pour le stockage de fichiers.
- Le HDD est plus rare mais présent dans certains équipements industriels.
- Ces supports peuvent être ciblés par des attaques physiques (dump, lecture, remplacement).

MODULES DE SÉCURITÉ (TPM)

- Le TPM est un coprocesseur cryptographique dédié à la sécurité des données.
- Il permet le stockage de clés non exportables, la vérification de l'intégrité, et le démarrage sécurisé.
- Utilisé notamment avec BitLocker, Windows Hello et Secure Boot.
- Il existe en version matérielle ou logicielle (simulateur pour test/développement).
- Référence utile : Arthur & Challener – A Practical Guide to TPM 2.0 (2015).

ATTAQUES PHYSIQUES CONNUES

ACCÈS AUX BUS DE COMMUNICATION (I2C, UART, SPI)

- INTERFACES SOUVENT LAISSES ACCESSIBLES DANS LES PRODUITS FINAUX.
- PERMETTENT D'EXTRAIRE LA MÉMOIRE, DE SNIFFER LES ÉCHANGES, OU D'INJECTER DES COMMANDES.
- EXEMPLE : ACCÈS UART SUR ROUTEUR POUR OBTENIR UN SHELL.

LECTURE DIRECTE D'EEPROM (ECU, BIOS, CONSOLES)

- EXTRACTION DE DONNÉES CRITIQUES (RED KEY MOTO, MOT DE PASSE BIOS).
- LECTURE POSSIBLE VIA PROGRAMMATEUR TYPE CH341A.
- UTILISÉE AUSSI POUR CONTOURNER PROTECTIONS SUR CONSOLES DE JEUX.

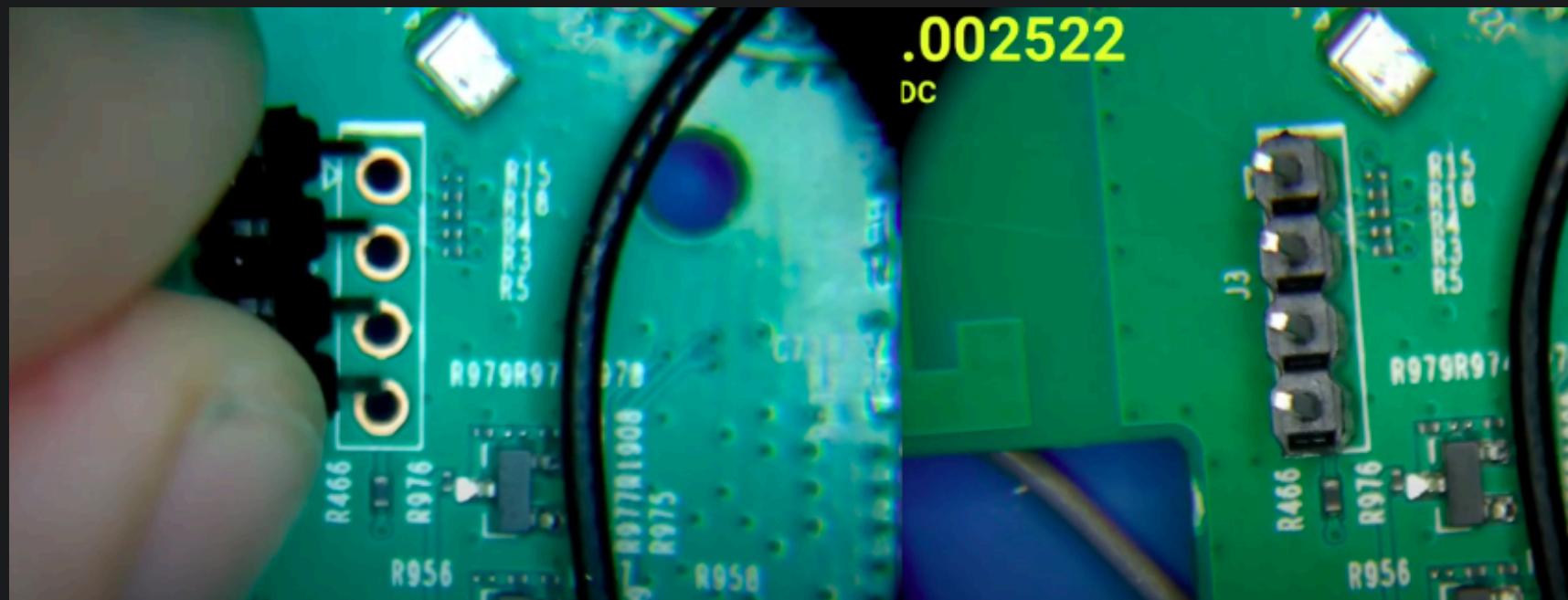
ATTAQUES PHYSIQUES SUR LE MATÉRIEL

- GLITCHING : PERTURBATION ÉLECTRIQUE (BYPASS D'AUTHENTICATION).
- COLD BOOT : RÉCUPÉRATION DE DONNÉES SENSIBLES (EX. CLÉS BITLOCKER) VIA RAM REFROIDIE.

ATTAQUES VIA PÉRIPHÉRIQUES USB

- RUBBER DUCKY : INJECTION DE COMMANDES COMME UN CLAVIER.
- OMG CABLE : CÂBLE USB MODIFIÉ POUR ESPIONNAGE OU CONTRÔLE.
- USB KILLER : ENVOI D'IMPULSIONS ÉLECTRIQUES DESTRUCTRICES.
- EXEMPLE CÉLÈBRE : STUXNET A COMPROMIS DES AUTOMATES VIA USB DANS UN RÉSEAU ISOLÉ.

CYBERSÉCURITÉ DES SYSTÈMES EMBARQUÉS :



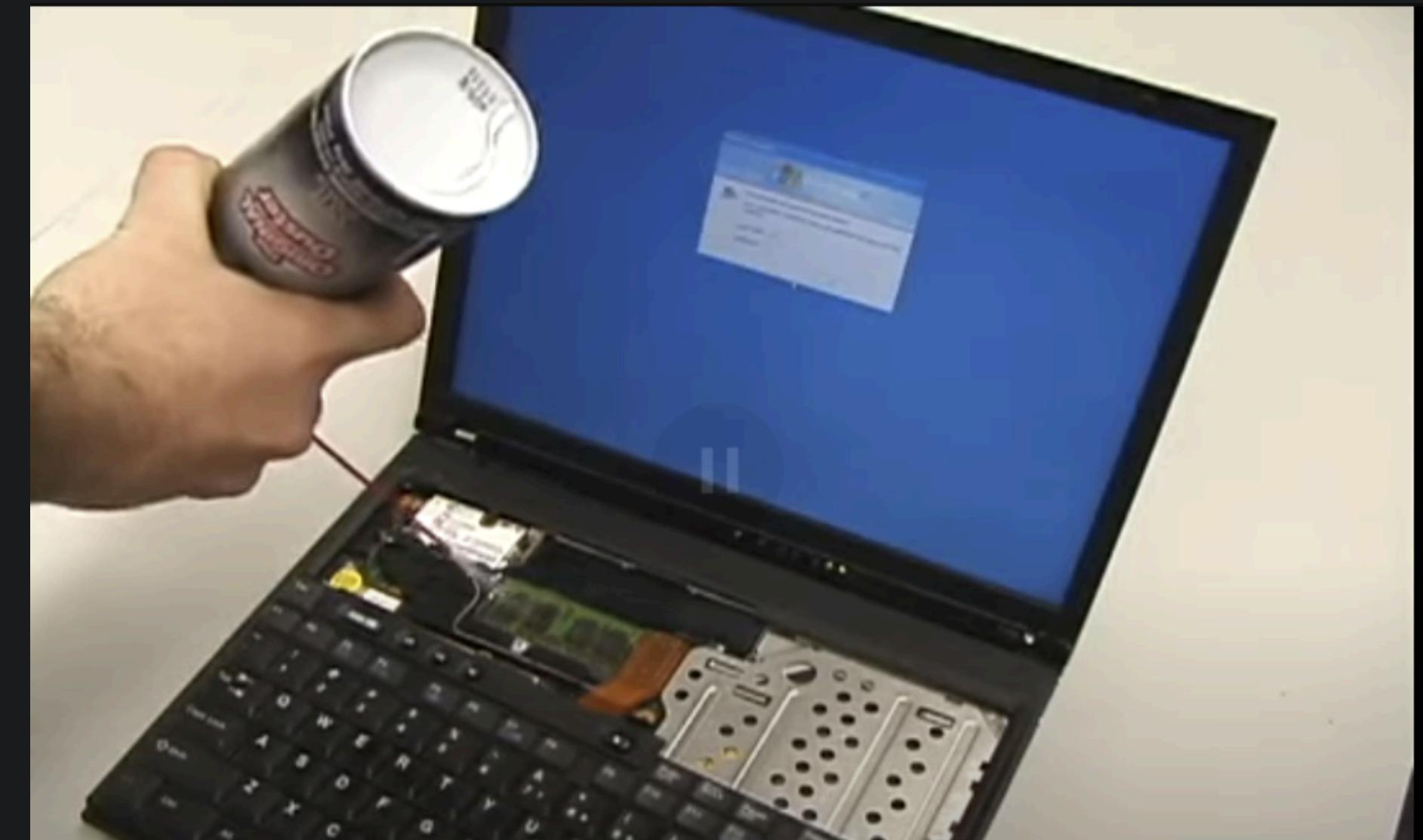
6,79€ -1% 6,82€ ⓘ
6,39€ chaque, ≥ 10 pièces

Adaptateur de programmeur CH341A + adaptateur SOIC8 + clip SOP8 avec câble + adaptateur 1.8 V CH341A EEPROM Flash BIOS programmeur USB adaptateur ZIF

★★★★★ 4.9 1269 Avis | + 5 000 vendus

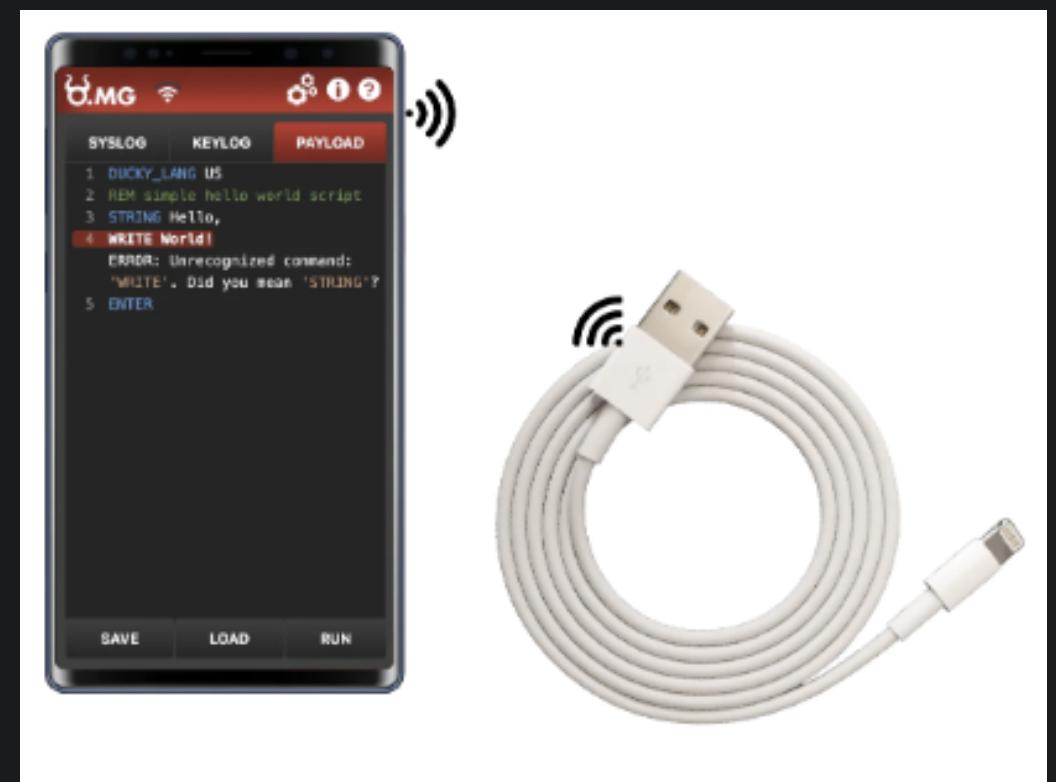
Couleur: 1 Set

CH341A+SOP8 Test Clip+150mil Socket



- 1) <https://www.youtube.com/watch?v=AtSyGnATm-s>
- 2) <https://www.youtube.com/watch?v=Ej-Nr79bVjg>
- 3) Lien du lecteur d'eeprom

CYBERSÉCURITÉ DES SYSTÈMES EMBARQUÉS :



<https://lab401.com/fr/products/o-mg-cable-programmer-usb>

<https://www.amazon.fr/HAK5-Canard-caoutchouc-Nouvelle-version/dp/B0C1HBSQS2>

<https://news.sophos.com/fr-fr/2017/03/27/le-usb-killer-dans-mauvaises-mains/>

DEFENSE PHYSIQUES CONNUES

PROTECTION DES INTERFACES

- Désactiver les ports inutilisés (UART, SPI, JTAG...)
- Authentification forte pour les interfaces critiques
- Résine epoxy ou couches internes PCB pour cacher les broches
- Détection d'ouverture de boîtier → effacement de données sensibles

SÉCURISATION DES DONNÉES

- Chiffrement matériel (TPM, HSM, Secure Element).
- Cloisonnement mémoire (MPU, TrustZone).
- Contre-mesures physiques (blindage, bruit, masquage).
- Firmware chiffré + Secure Boot.

LIMITATION DES ACCÈS

- Boîtiers verrouillés et vis inviolables.
- Capteurs de sabotage (température, lumière).
- Mise à jour signée/chiffrée uniquement.
- Réduction de la surface d'attaque.

DÉFENSE DANS LES ENVIRONNEMENTS INDUSTRIELS

- SCADA/ICS souvent isolés, sans surveillance directe.
- Coffrets renforcés, accès restreint (badge, clé, vidéo).
- Désactivation des ports de maintenance inutiles.
- Disques chiffrés, Secure Boot, journalisation.

DEFENSE PHYSIQUES CONNUES

WEP (WIRED EQUIVALENT PRIVACY)

- ANCIEN PROTOCOLE DE CHIFFREMENT WI-FI BASÉ SUR RC4
 - + IV 24 BITS.
- IV TROP COURT, ENVOYÉ EN CLAIR → COLLISIONS ET ATTAQUES STATISTIQUES.
- FACILEMENT CASSABLE VIA AIRCRACK-NC APRÈS CAPTURE DE PAQUETS.

WPA2

- CHIFFREMENT AES, HANDSHAKE EN 4 ÉTAPES (EAPOL).
- CAPTURE POSSIBLE DU 4-WAY HANDSHAKE APRÈS UNE ATTAQUE DE DÉSAUTHENTIFICATION.
- VERSION ENTREPRISE + SÉCURISÉE VIA SERVEUR RADIUS (AUTHENTIFICATION INDIVIDUELLE).

RFC 3748 (EAP) ET RFC 2865 (RADIUS) DÉTAILLENT CES MÉCANISMES D'AUTHENTIFICATION.

WPA3

- INTRODUIT SAE : ÉCHANGE SÉCURISÉ PAR PREUVE (REPLACE PSK).
- CHIFFREMENT RENFORCÉ (AES-GALLOIE COUNTER MODE), CLÉS JUSQU'À 256 BITS.
- CHIFFRE AUSSI LES RÉSEAUX PUBLICS OWE) MEME SANS MOT DE PASSE (
- GESTION SÉCURISÉE DES TRAMES DE DÉSAUTHENTIFICATION VIA PMF (802.11W).

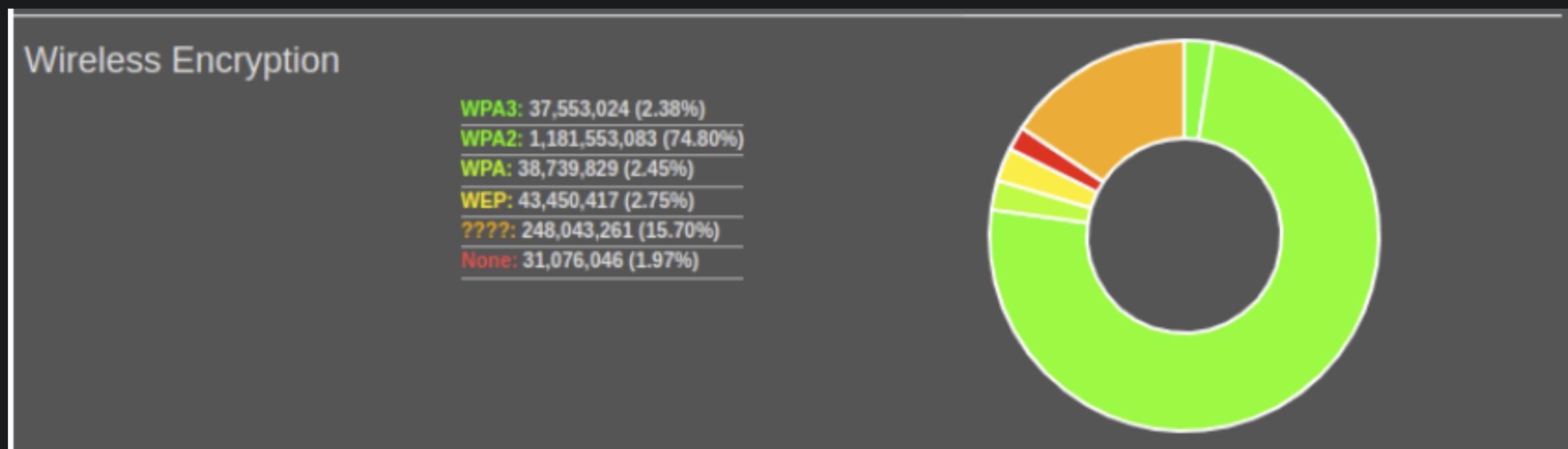
CYBERSÉCURITÉ DES SYSTÈMES EMBARQUÉS :

sniffpmkid_2.pcap

Fichier Editer Vue Aller Capture Analyser Statistiques Telephone Wireless Outils Aide

eapol

No.	Time	Source	Destination	Protocol	Length	Info
629	15.210081	FreeboxS_32:78:1e	a8:31:62:2d:48:22	EAPOL	137	Key (Message 1 of 4)
630	15.210995	FreeboxS_32:78:1e	a8:31:62:2d:48:22	EAPOL	137	Key (Message 1 of 4)
632	15.213035	a8:31:62:2d:48:22	FreeboxS_32:78:1e	EAPOL	157	Key (Message 2 of 4)
633	15.214678	FreeboxS_32:78:1e	a8:31:62:2d:48:22	EAPOL	193	Key (Message 3 of 4)
634	15.219370	a8:31:62:2d:48:22	FreeboxS_32:78:1e	EAPOL	135	Key (Message 4 of 4)
638	15.582494	FreeboxS_32:78:1e	SeikoEps_56:9e:cc	EAPOL	137	Key (Message 1 of 4)
643	15.596922	SeikoEps_56:9e:cc	FreeboxS_32:78:1e	EAPOL	159	Key (Message 2 of 4)
673	16.351544	FreeboxS_32:78:1e	SeikoEps_56:9e:cc	EAPOL	137	Key (Message 1 of 4)



<https://wigle.net/stats>

BLUETOOTH , NFC , RFID ET FIXED ET ROLLING CODE

BLUETOOTH CLASSIQUE ET BLE

LE BLUETOOTH PERMET UNE COMMUNICATION SANS FIL À COURTE PORTÉE.
DEUX VARIANTES PRINCIPALES EXISTENT :

- BLUETOOTH CLASSIQUE (BR/EDR) : CONÇU POUR LES ÉCHANGES CONTINUS ET STABLES (AUDIO, FICHIERS), MAIS CONSOMME PLUS D'ÉNERGIE.
- BLUETOOTH LOW ENERGY (BLE) : DESTINÉ AUX OBJETS CONNECTÉS À FAIBLE CONSOMMATION (CAPTEURS, DOMOTIQUE). FONCTIONNE VIA UN SYSTÈME DE DIFFUSION (ADVERTISING), SANS CONNEXION PERMANENTE.

LES DEUX PROTOCOLES COEXISTENT DANS CERTAINS APPAREILS, MAIS SONT INCOMPATIBLES ENTRE EUX. BLE PRIVILÉGIE L'AUTONOMIE, LE CLASSIQUE LA STABILITÉ.

PROTOCOLES RF PROPRIÉTAIRES : FIXED CODE VS ROLLING CODE

FIXED CODE : LA TÉLÉCOMMANDE ENVOIE TOUJOURS LE MÊME SIGNAL → VULNÉRABLE AU REPLAY ATTACK.

ROLLING CODE : LE CODE CHANGE À CHAQUE APPUI → PLUS SÉCURISÉ.
EXEMPLE D'ATTAQUE : ROLLJAM

UN BROUILLEUR EMPÈCHE LA RÉCEPTION D'UN CODE PAR LE RÉCEPTEUR TOUT EN L'ENREGISTRANT. L'UTILISATEUR ENVOIE UN NOUVEAU CODE, ÉGALEMENT INTERCEPTÉ. L'ATTACQUANT REJOUE ENSUITE L'ANCIEN CODE RESTÉ VALIDE.

NFC ET RFID

CES TECHNOLOGIES PERMETTENT UNE IDENTIFICATION OU UN ÉCHANGE DE DONNÉES À TRÈS COURTE PORTÉE :

- RFID : UNIDIRECTIONNELLE (LECTEUR → BADGE), FRÉQUENCES LF, HF OU UHF SELON L'USAGE.
- NFC : DÉRIVÉ DU RFID HF, BIDIRECTIONNEL, UTILISÉ DANS LES PAIEMENTS, SMARTPHONES ET BADGES DE TRANSPORT.

CARTES MIFARE :

- MIFARE CLASSIC : ANCIEN MODÈLE, FACILEMENT CLONABLE.
- MIFARE PLUS / DESFIRE : MODÈLES RÉCENTS PLUS SÉCURISÉS, UTILISANT AES ET PROTECTIONS AVANCÉES CONTRE LE CLONAGE.

AUTRES TECHNOLOGIES : HID PROX (TRÈS VULNÉRABLES), ICCLASS, CALYPSO, FELICA (PLUS SÛRES MAIS PARFOIS ATTAQUÉES).

ATTAQUES RADIO COURANTES (WI-FI, BLUETOOTH, NFC, RF)

EXPLOITATION WI-FI (WEP, WPA2)

- AIRCRACK-NG + CLÉ WI-FI EN MODE MONITOR
- CAPTURE D'IV (WEP) OU DU 4-WAY HANDSHAKE (WPA2)
- BRUTE-FORCE DU MOT DE PASSE (DICTIONNAIRE OU HASHCAT)
- FLIPPER ZERO & ESP32 FACILITENT LES ATTAQUES DEAUTH

ATTAQUE BLUETOOTH BLE (IPHONE DOS)

- BLE SPAM : ENVOI MASSIF DE CONNEXIONS FACTICES
- CRASH OU BLOCAGE D'IPHONE < IOS 17.2
- CORRIGÉ VIA LIMITATION APPLE + DÉSACTIVATION BLUETOOTH RECOMMANDÉ

CLONAGE NFC / RFID (FIXED CODE)

- LECTURE D'UN BADGE VIGIK AVEC FLIPPER ZERO
- COPIE VERS BADGE VIERGE (MAGIC TAG) OU ÉMULATION
- FAIBLE SÉCURITÉ → CODE FIXE NON CHIFFRÉ NI TOURNANT

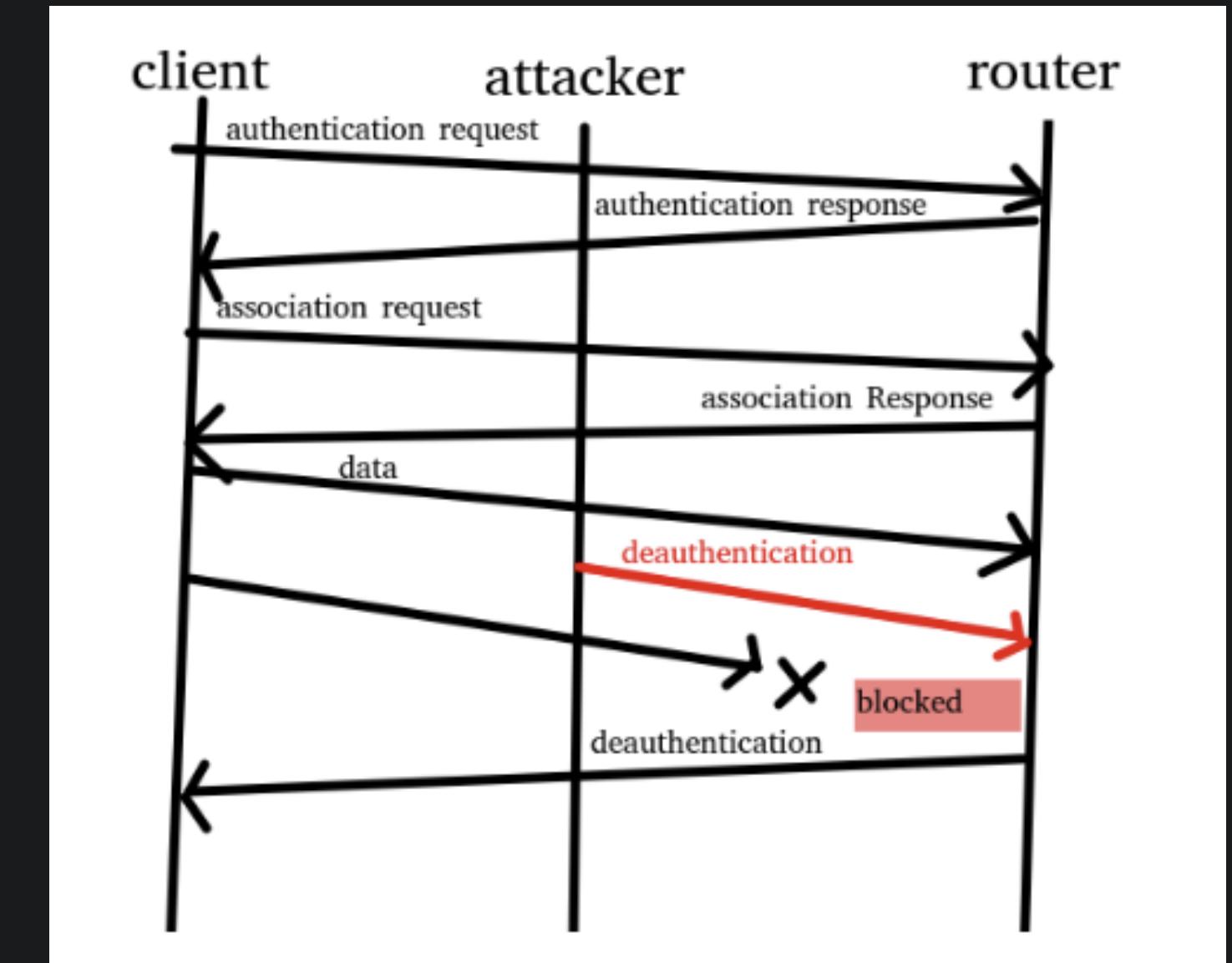
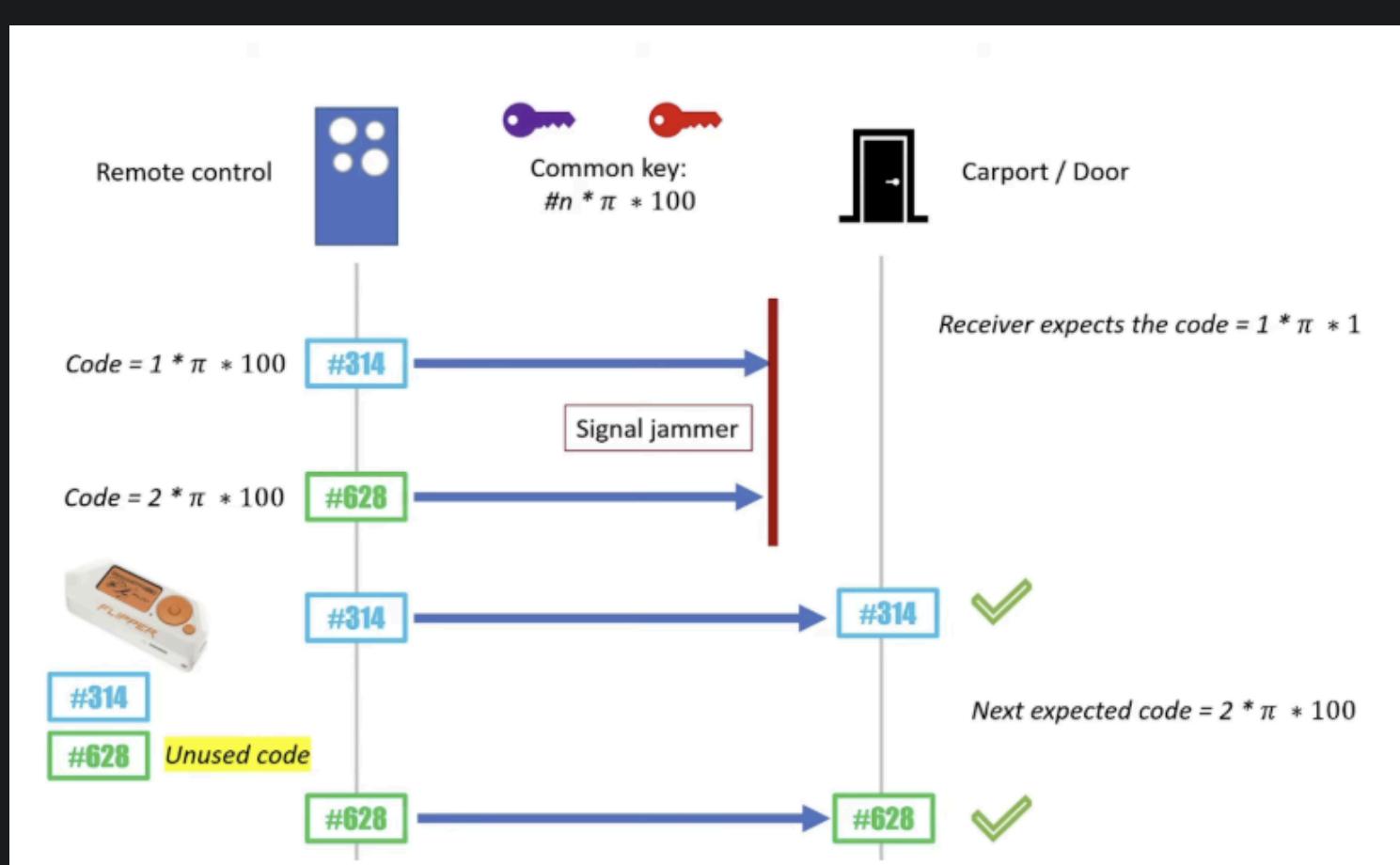
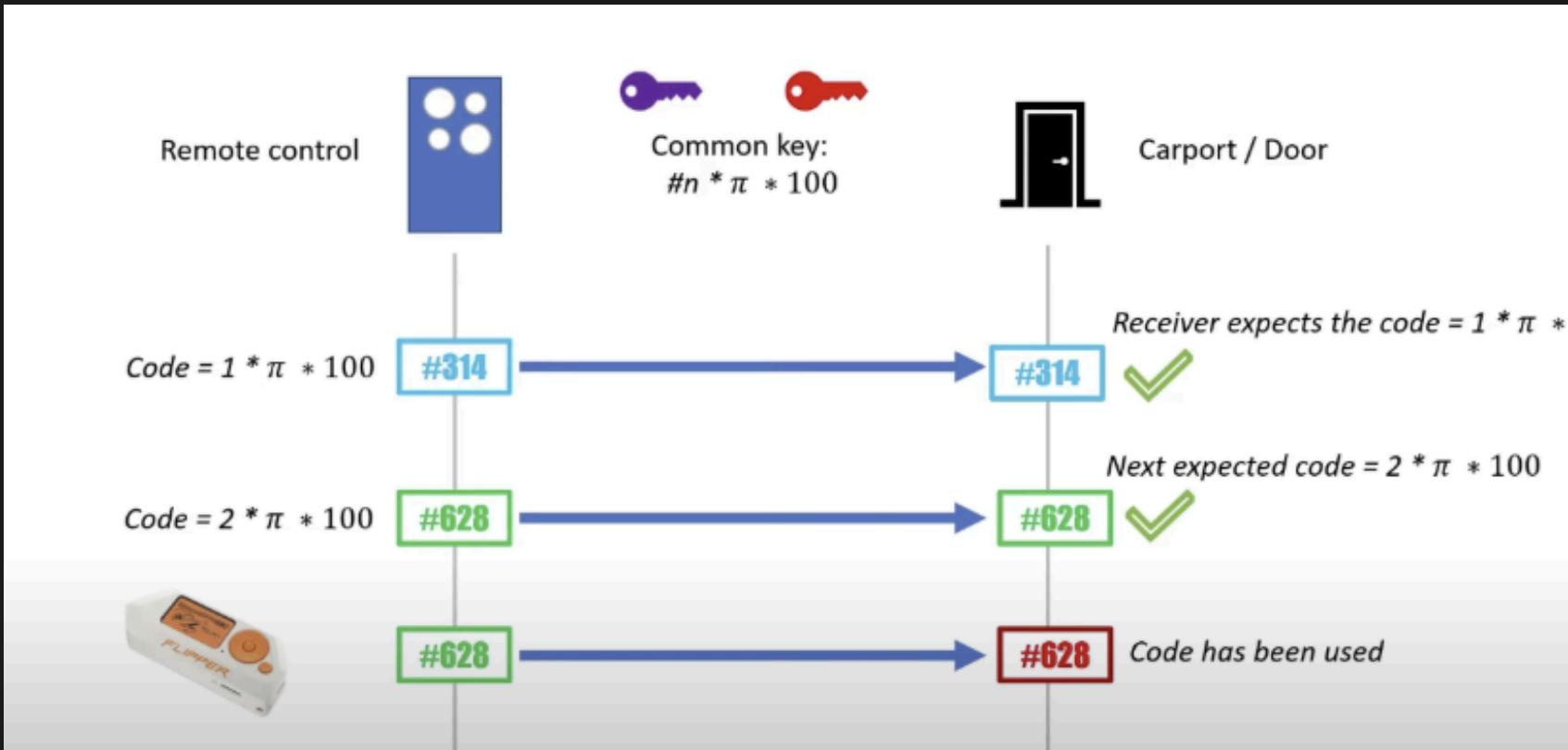
MOUSEJACKING (PÉRIPHÉRIQUES HID 2.4 GHZ NON BLUETOOTH)

- EXPLOITATION DU MANQUE DE CHIFFREMENT SOURIS / DONGLE
- INJECTION DE FRAPPES COMME UN CLAVIER HID
- IMPACT ÉQUIVALENT À UNE CLÉ USB MALVEILLANTE

TÉLÉCOMMANDES ROLLING CODE (VOITURES, PORTAILS)

- BLOCAGE + ENREGISTREMENT DES CODES VALIDES
- REJEU DIFFÉRÉ → ACCÈS NON AUTORISÉ
- DÉTOURNEMENT DU MÉCANISME DE DÉSYNCHRONISATION (ROLLJAM)

CYBERSÉCURITÉ DES SYSTÈMES EMBARQUÉS :



https://www.youtube.com/watch?v=aTcziqO_2IM&t=127s

ATTAQUES RADIO COURANTES (MILITAIRES)

LE BROUILLAGE RADIO CONSISTE À SATURER UNE BANDE DE FRÉQUENCE AVEC DES SIGNAUX PARASITES POUR PERTURBER LES COMMUNICATIONS SANS FIL (WI-FI, RF, BLUETOOTH...).

IL PEUT ÊTRE :

MALVEILLANT, COMME DANS LES ATTAQUES DE TYPE ROLLJAM, POUR BLOQUER UN CODE ROLLING ET LE REJOUER PLUS TARD.

DÉFENSIF, COMME LES BROUILLEURS MILITAIRES EMBARQUÉS DANS LES VÉHICULES SCORPION, CAPABLES DE DÉTECTOR UN SIGNAL DE DÉCLENCHEMENT (EX. IED) ET D'ENVOYER UNE CONTRE-ÉMISSION IMMÉDIATE (TECHNO DÉVELOPPÉE PAR EVIDEN).

INVOLONTAIRE, CAUSÉ PAR DES APPAREILS COMME DES FOURS À MICRO-ONDES INDUSTRIELS OU ÉQUIPEMENTS MÉDICAUX, BROUILLANT LA BANDE 2,4 GHZ.

EN FRANCE :

L'ACHAT D'UN BROUILLEUR EST AUTORISÉ (EX. RECHERCHE, PÉDAGOGIE).

SON USAGE EST INTERDIT (ARTICLE L.39-1 CPCE), CAR IL PERTURBE LES SERVICES ESSENTIELS (GPS, TÉLÉPHONIE...).



<https://www.defense.gouv.fr/dga/programme-scorpion>

<https://www.skyliffr.com/brouilleur-militaire.html>

DÉFENSES CONTRE LES ATTAQUES RADIO

PROTOCOLES WI-FI – BONNES PRATIQUES

- ACTIVER 802.11W (TRAMES DE GESTION PROTÉGÉES) POUR EMPÊCHER LES ATTAQUES DE DÉSAUTHENTIFICATION.
- UTILISER DES MOTS DE PASSE ROBUSTES (16+ CARACTÈRES, LETTRES/CHIFFRES/SYMOLES).
- METTRE EN PLACE UN FILTRAGE D'ADRESSES MAC POUR LIMITER L'ACCÈS AUX APPAREILS AUTORISÉS.
- PASSER À WPA3 SI POSSIBLE, POUR BÉNÉFICIER D'UNE MEILLEURE SÉCURITÉ HANDSHAKE (SAE).
- UTILISER UN VPN, MÊME SUR WI-FI SÉCURISÉ, POUR PROTÉGER CONTRE LES INTERCEPTIONS.
- EN ENTREPRISE, PRÉFÉRER L'AUTHENTIFICATION PAR SERVEUR RADIUS PLUTÔT QUE PSK PARTAGÉ.

DÉTECTION D'ANOMALIES RADIO

- SURVEILLER L'ENVIRONNEMENT RADIO AVEC DES ANALYSEURS DE SPECTRE POUR DÉTECTER :
 - SIGNAUX SUSPECTS OU RÉPÉTITIFS (JAMMING, SPOOFING),
 - ACTIVITÉ INHABITUELLE (EX. : SPAM BLUETOOTH, REQUÊTES WI-FI ANORMALES).
- UTILISATION DE SYSTÈMES DE MONITORING DANS LES ENVIRONNEMENTS SENSIBLES (IOT, MILITAIRE, INDUSTRIEL).
- LES OPÉRATEURS (FREE, ORANGE, ETC.) PEUVENT ÉGALEMENT DÉTECTER DU BROUILLAGE SUR LEURS RÉSEAUX ET EN INFORMER L'ANFR.
- EXEMPLE : ANFR CARTORADIO POUR VISUALISER LES ZONES À RISQUE.

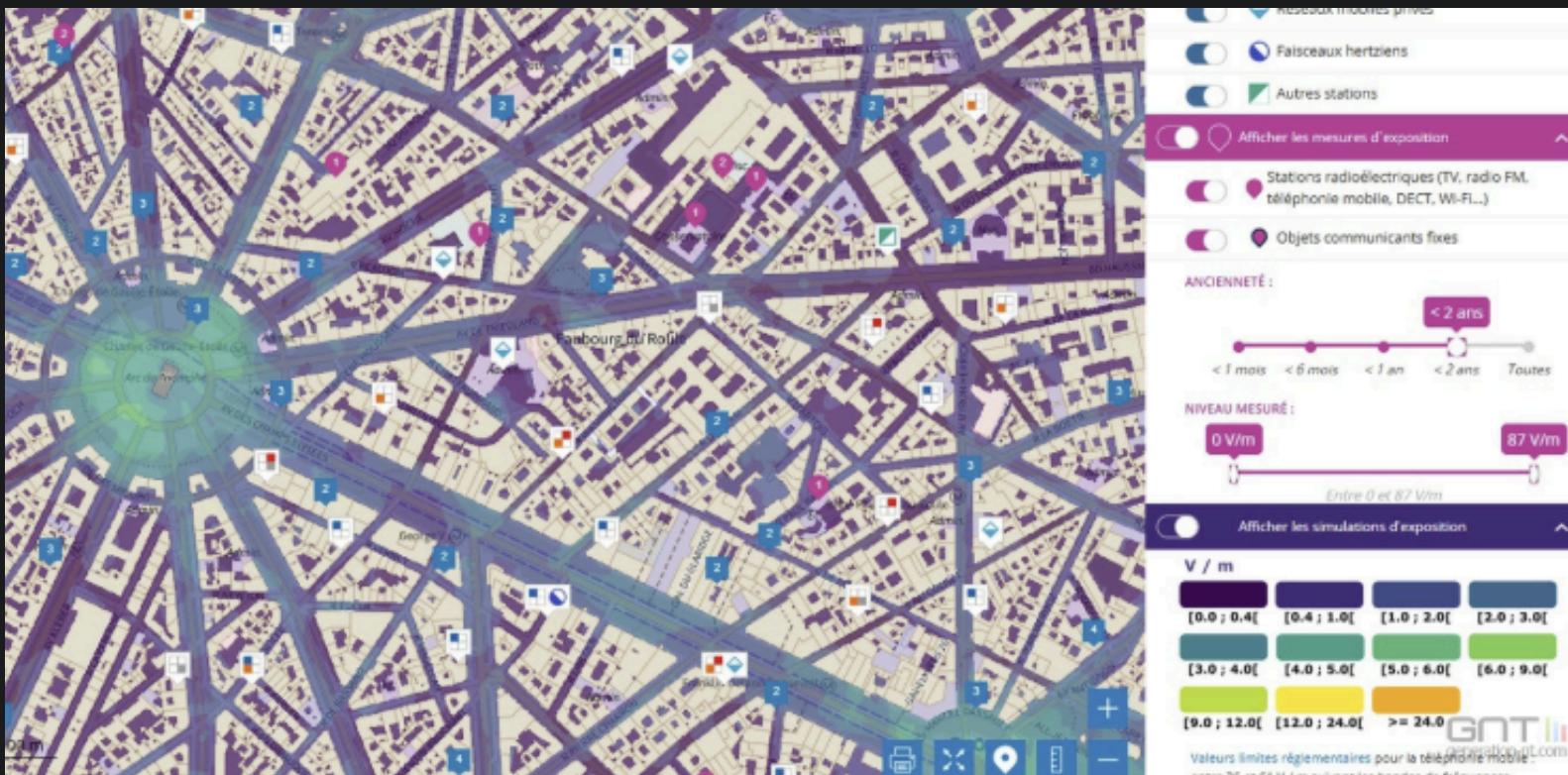
BLINDAGE PHYSIQUE ET SÉPARATION

- PORTEFEUILLES ANTI-RFID : FINE COUCHE MÉTALLIQUE POUR BLOQUER LES LECTURES NFC/RFID.
- PEINTURES, REVÊTEMENTS MÉTALLIQUES OU BÉTON : ISOLENT LES SALLES CRITIQUES DES INTERFÉRENCES.

EXEMPLE : FREE HÉBERGE CERTAINS SERVEURS DANS DES BUNKERS OU ANCIENS FORTS POUR GARANTIR :

- ISOLATION THERMIQUE ET ÉLECTROMAGNÉTIQUE,
- RÉSISTANCE PHYSIQUE,
- SÉCURITÉ RENFORCÉE CONTRE LES ATTAQUES RF OU CATASTROPHES.

CYBERSÉCURITÉ DES SYSTÈMES EMBARQUÉS :



<https://www.generation-nt.com/actualites/anfr-cartoradio-exposition-onde-telephonie-mobile-2057037>

PORTE FEUILLE ANTI RFID LIEN ICI

Mode > Bagages, sacs de voyage et accessoires > Portefeuille et porte-cartes > Homme > Portefeuilles

Portefeuille Homme en Cuir véritable avec Blocage RFID, Porte Monnaie, Porte Cartes et Compartiment sans Contact, Noir.

27⁹⁹ €

Retours GRATUITS

Livraison GRATUITE mercredi 14 mai à 93260 lors de votre première commande. [Détails](#)

Ou livraison accélérée demain 12 mai. Commandez dans les 2 h 4 min. [Détails](#)

En stock

Quantité : 1

Ajouter au panier

Acheter cet article

Some reviews may be missing. Please make sure you're logged in to all relevant marketplaces to gather complete reviews.

Visiter la boutique MR.MORGAN

4,4 ★★★★★ 31 évaluations | Rechercher sur cette page

Plus de 100 achetés au cours du mois dernier

27⁹⁹ €

Pris le plus bas des 30 derniers jours : 26,99€

Retours GRATUITS

Les prix des articles vendus sur Amazon incluent la TVA. En fonction de votre adresse de livraison, la TVA peut varier au moment du paiement. Pour plus d'informations, consultez votre résultat.

ÉTUDES DE CAS : ATTAQUES CONCRÈTES SUR SYSTÈMES EMBARQUÉS

- BLUATTACK (IOS 17.0.3) : ENVOI MASSIF DE REQUÊTES BLE VIA FLIPPER ZERO → SATURATION DE LA PILE BLUETOOTH DES IPHONES → CRASH TOTAL DE L'INTERFACE → CONTOURNÉ À PARTIR D'IOS 17.2.
- CLONAGE NFC : LECTURE D'UN BADGE NFC AVEC FLIPPER ZERO, CLONAGE SUR UN MAGIC TAG VIERGE → ACCÈS FRAUDULEUX AUX SYSTÈMES NON CHIFFRÉS (VIGIK, RÉSIDENCES, PARKINGS...).
- ROLLING CODE & RELECTURE RADIO : NORMALEMENT INVIOABLE CAR LES CODES CHANGENT À CHAQUE ÉMISSION. MAIS ATTAQUE POSSIBLE VIA BROUILLAGE + ENREGISTREMENT → INJECTION DIFFÉRÉE D'UN ANCIEN CODE VALIDE → DÉVERROUILLAGE SANS ALERTE.
- DEAUTH ATTACK SUR CAMÉRAS WI-FI : FLIPPER OU ESP32 PROVOQUE LA DÉCONNEXION WI-FI D'UNE CAMÉRA → RÉCUPÉRATION DU HANDSHAKE WPA2 → BRUTE-FORCE AVEC HASHCAT.
- EXTRACTION RED KEY (MOTO) : LECTURE DIRECTE D'UNE EEPROM (TYPE 24CO2) DANS L'ECU D'UNE MOTO → RÉCUPÉRATION DE LA RED KEY → REPROGRAMMATION DE CLÉS.

CYBERSÉCURITÉ DES SYSTÈMES EMBARQUÉS :

1) Imou Protect interface showing a live feed of a smartphone and a box.

2) Imou Protect interface showing a menu with "Targeted Deauth station >" and "Sniff < pmkid >" selected.

3) Imou Protect interface showing a message: "#attack -t deauth Sending to broadcast... Starting Deauthentication attack. Stop with stopscan >"

4) Imou Protect interface showing a message: "Press BACK to send stopscan #sniffpmkid -serial Starting PMKID sniff on channel 11. Stop with stopscan >"

5) Imou Protect interface showing a message: "Erreur de lecture. Appuyez pour actualiser." (Reading error. Press to update.)

6) Circuit board diagram of a receiver module. It shows various components like resistors (R20, R49, RAD7, C40, C26, C42, C43), capacitors, and an IC labeled IC6. A green arrow points from the text "Receiver expects the code = 1 * π * 100" to a connection point on the board.

7) A photograph of a green circuit board being programmed. A red UUUSB (UPA-USB Serial Programmer) device is connected via a cable. A green LED on the programmer is illuminated.

8) Block diagram illustrating a signal flow from a "Remote control" to a "Carport / Door". The remote sends codes #314 and #628. A "Signal jammer" is shown intercepting the signal between the remote and the receiver. The receiver expects code #314. The jammer sends code #314, which is accepted by the receiver. The receiver then expects code #628, which is also accepted. A note states: "Next expected code = 2 * π * 100".

9) Pinout diagrams for EEPROMs, I2C, and SPI connections. The EEPROM section shows pins o1-o9. The I2C section shows P2, P3, P4, P5, P6, P7, P8, P9, A0, A1, A2, Vss, WP, SCL, SDA. The SPI section shows P2, P3, P4, P5, P6, CS, Vcc, SO, HOLD, WP, SCK, SI, Vss.

CONCLUSION

- LA SÉCURITÉ DES SYSTÈMES EMBARQUÉS EST UN ENJEU CRITIQUE ET MULTIDIMENSIONNEL
- LES ATTAQUES PHYSIQUES ET RADIO METTENT EN LUMIÈRE LES FAILLES CONCRÈTES DU MATÉRIEL
- LES PROTECTIONS EXISTENT, MAIS DÉPENDENT SOUVENT D'UN ÉQUILIBRE DIFFICILE : PERFORMANCE VS SÉCURITÉ, SIMPLICITÉ VS RÉSILIENCE

MERCI !