WE HAVE A DEAL:

WE PROVIDE THE LEGO BRICKS, YOU BUILD COOL WIRELESS ATTACKS !

Romain Cayre + Damien Cauquil / SSTIC 2025

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES TOULOUSE

LAAS CNRS

Quarkslab

/WHO

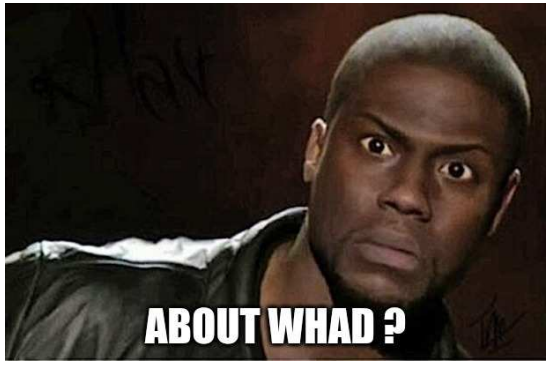
Romain Cayre

- Auteur de *Mirage*, *WazaBee* & WHAD
- Enseignant-chercheur à l'**INSA Toulouse**

Damien Cauquil

- Auteur de *Btlejack*, *BumbleBee* & WHAD
- Ingénieur sécurité à **Quarkslab**

QUELQUES MOTS SUR *WHAD*...



- **W**ireless **HA**cking for **D**ummies 🤔
  - Protocole *Host/Hardware* unifié
  - API Python + *outils sur étagère*
  - En développement depuis **2021**...
  - Première *release* en **2024**

https://whad.io

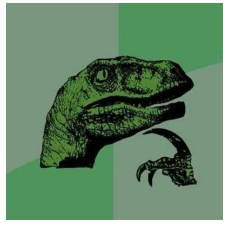
PWNING AVEC WHAD

/WHY

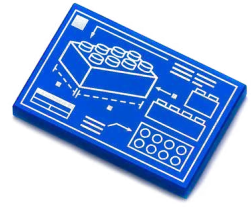
/WHY

Durant la conception, on s'est demandé quels outils étaient *vraiment* indispensables dans WHAD ...

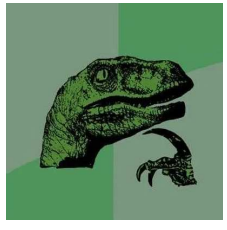
/WHY



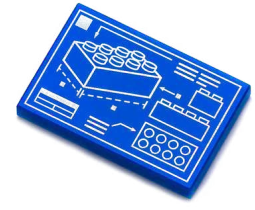
Est-ce qu'on ne pourrait pas décrire les attaques sans fil comme une combinaison de briques de base ?



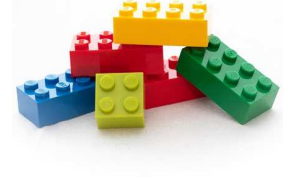
/WHY



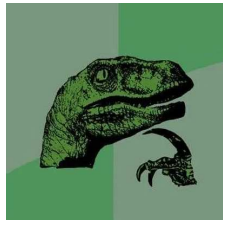
Est-ce qu'on ne pourrait pas décrire les attaques sans fil comme une combinaison de briques de base ?



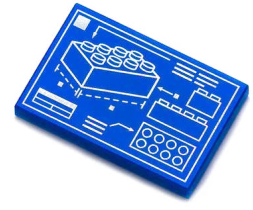
Dans ce cas, on a juste à implémenter ces briques ...



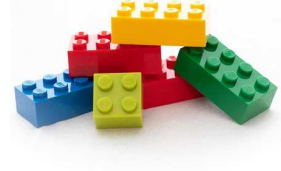
/WHY



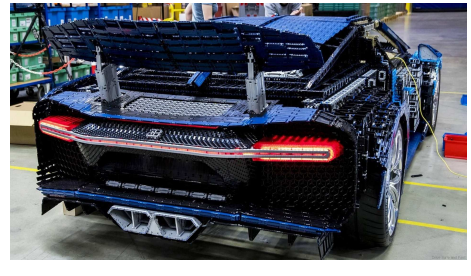
Est-ce qu'on ne pourrait pas décrire les attaques sans fil comme une combinaison de briques de base ?



Dans ce cas, on a juste à implémenter ces briques ...



... et voir comment les chercheurs les combinent pour construire des attaques !



EXEMPLE: MONITORING DE RYTHME CARDIAQUE EN TEMPS RÉEL !

Implémenté avec seulement 2 briques de base !

✋ NOTA BENE

Nous vous suggérons la lecture des actes de SSTIC pour une description détaillée des briques de base, ou *primitives*, que nous allons introduire relativement brièvement dans cette présentation.

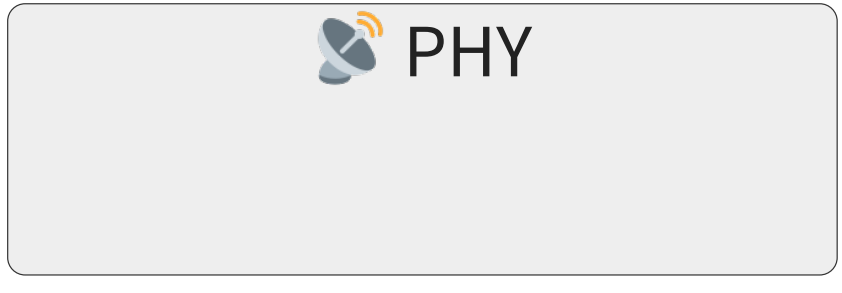
SYSTÉMATISATION D'ATTAQUES SANS FIL

MÉTHODOLOGIE

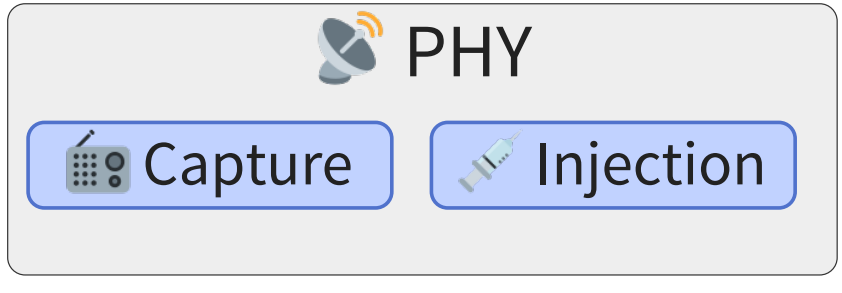
- Definition d'un **modèle de menaces**
- **Analyse & classification** d'attaques sans fil connues
- **Identification** de 11 *primitives* uniques

VUE D'ENSEMBLE DES PRIMITIVES

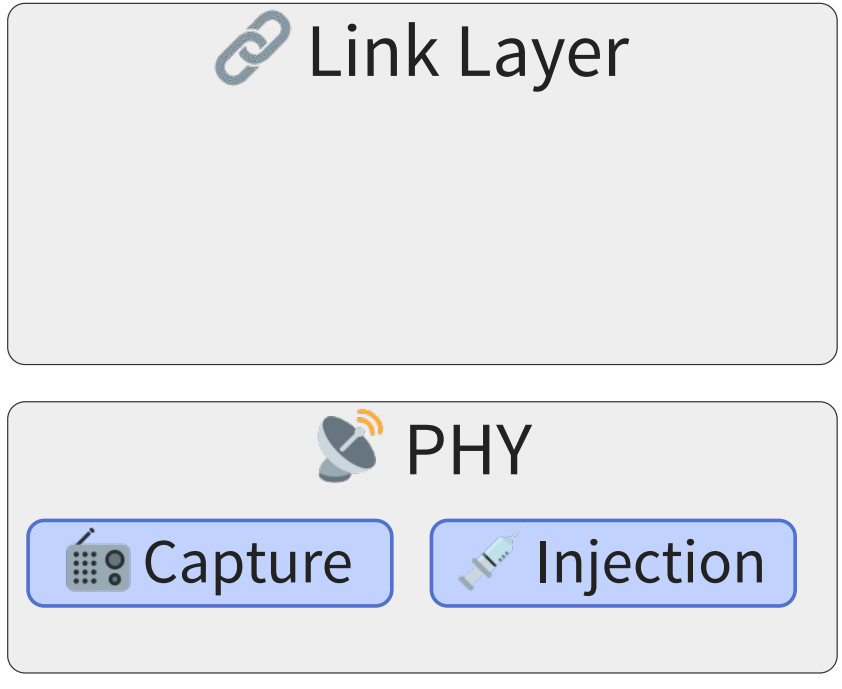
VUE D'ENSEMBLE DES PRIMITIVES



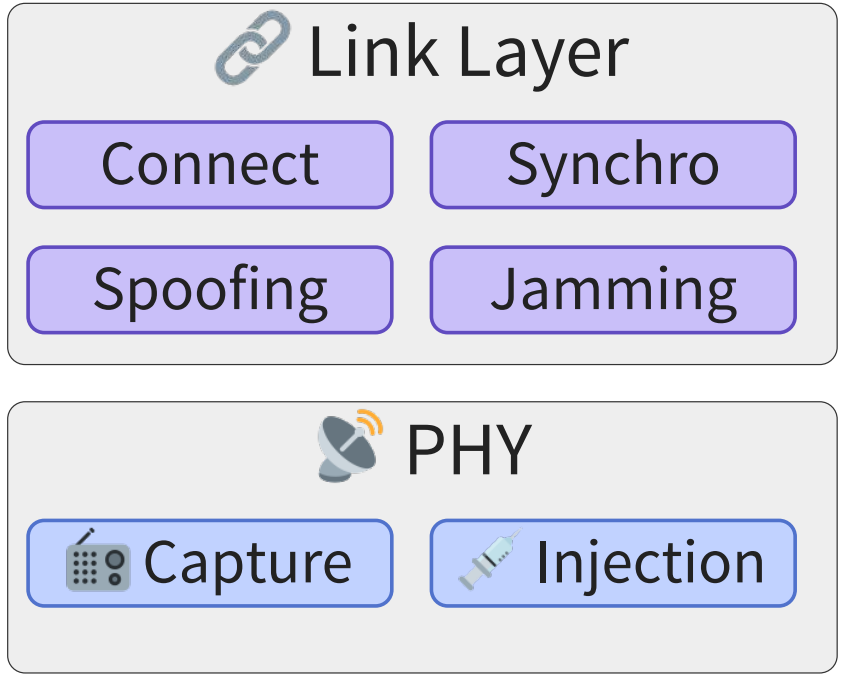
VUE D'ENSEMBLE DES PRIMITIVES



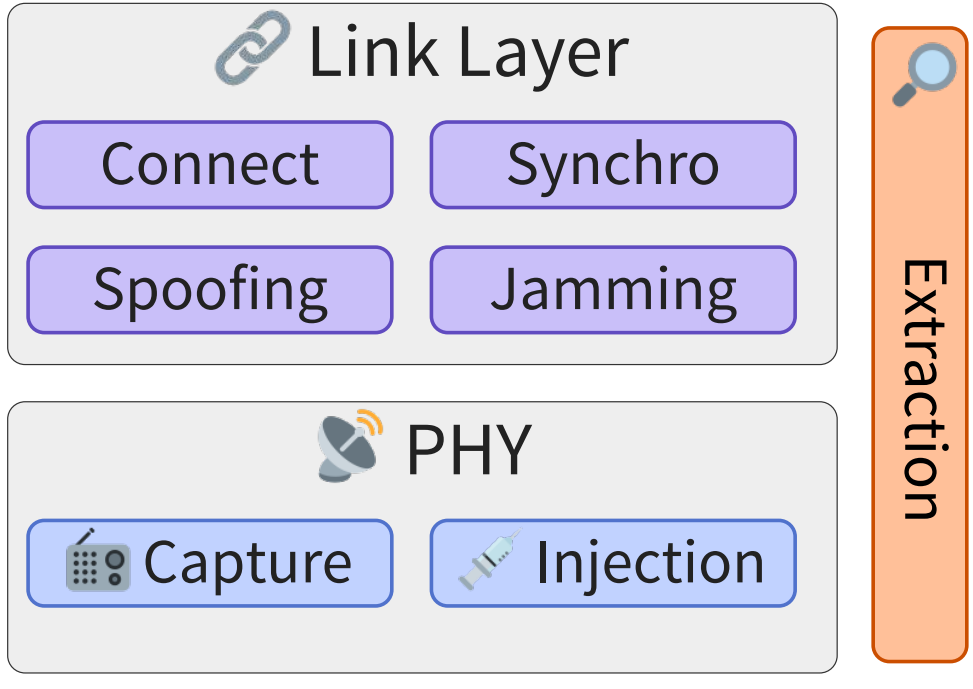
VUE D'ENSEMBLE DES PRIMITIVES



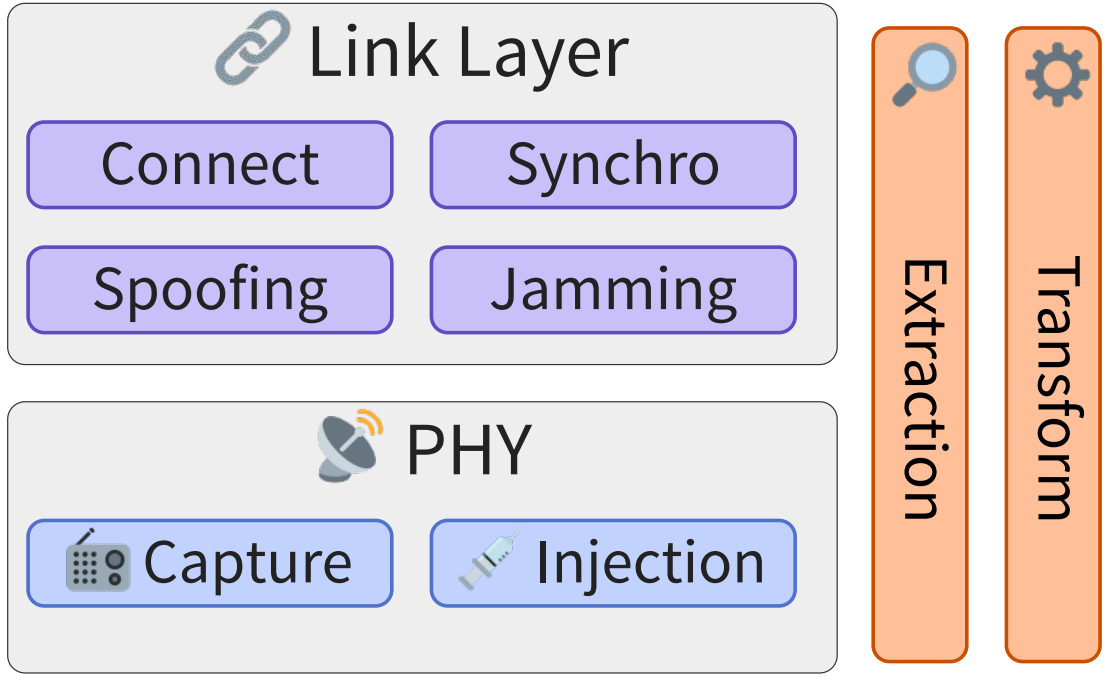
VUE D'ENSEMBLE DES PRIMITIVES



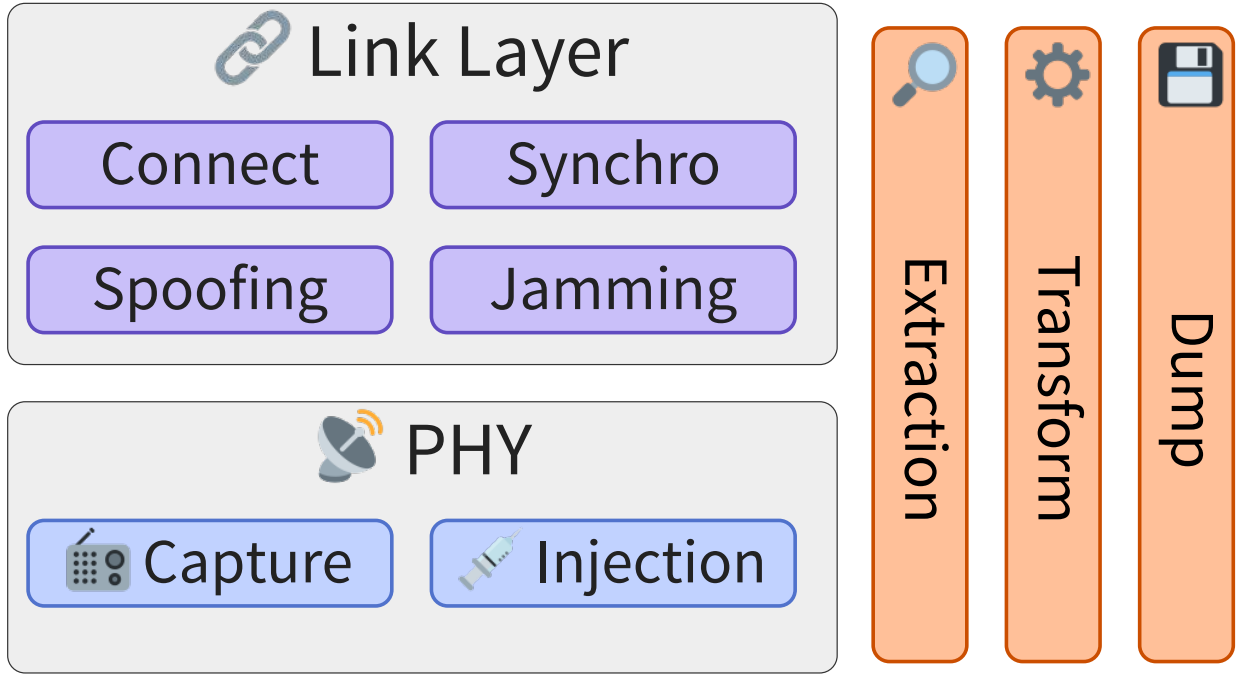
VUE D'ENSEMBLE DES PRIMITIVES



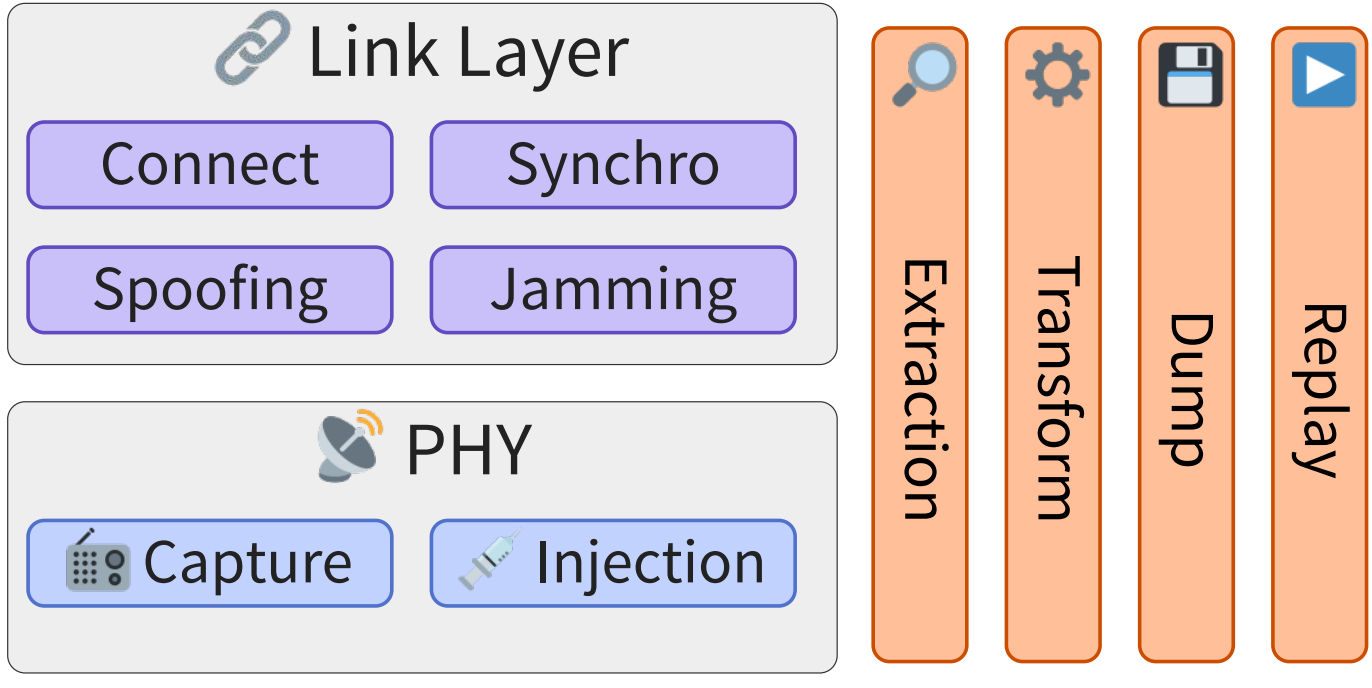
VUE D'ENSEMBLE DES PRIMITIVES



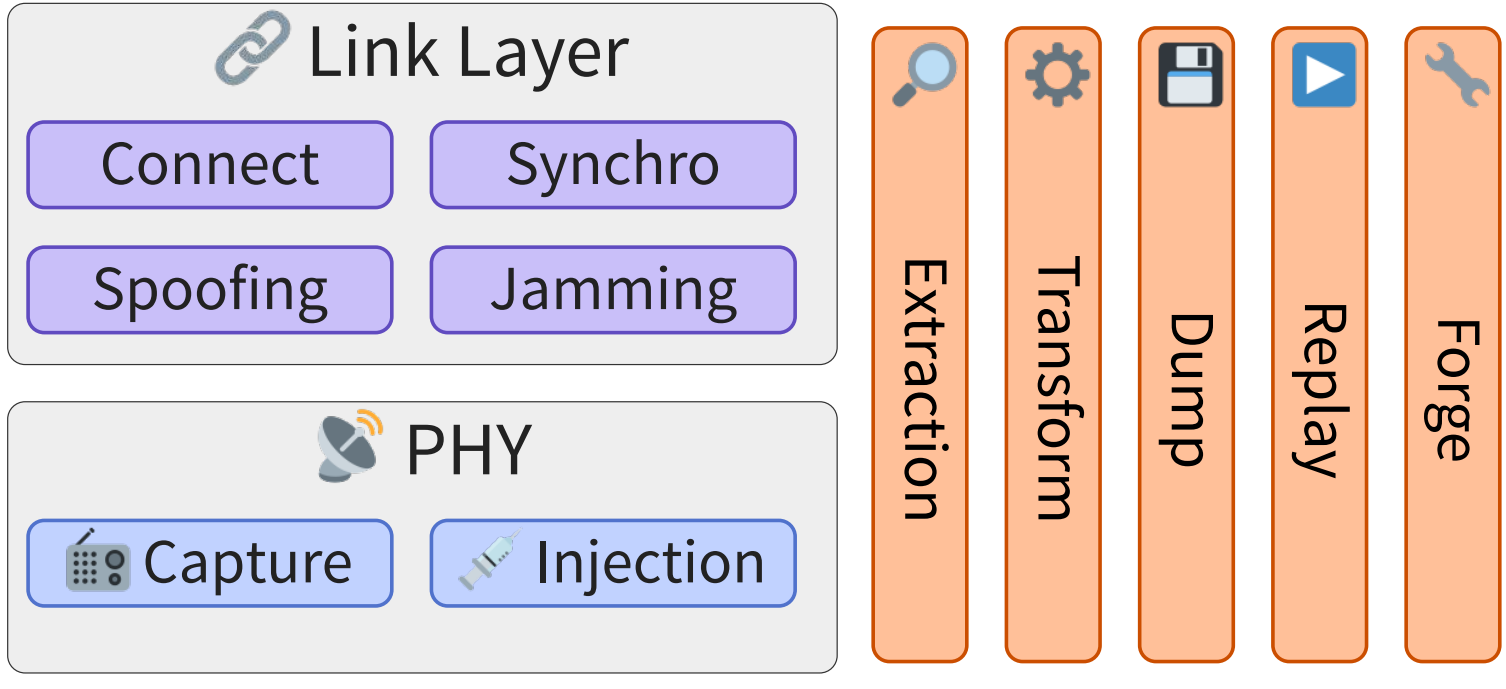
VUE D'ENSEMBLE DES PRIMITIVES



VUE D'ENSEMBLE DES PRIMITIVES

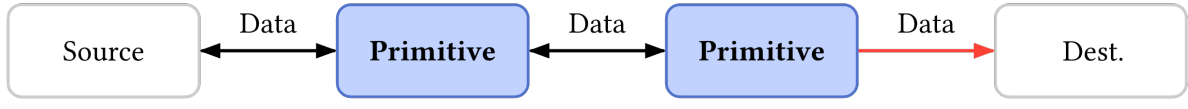


VUE D'ENSEMBLE DES PRIMITIVES

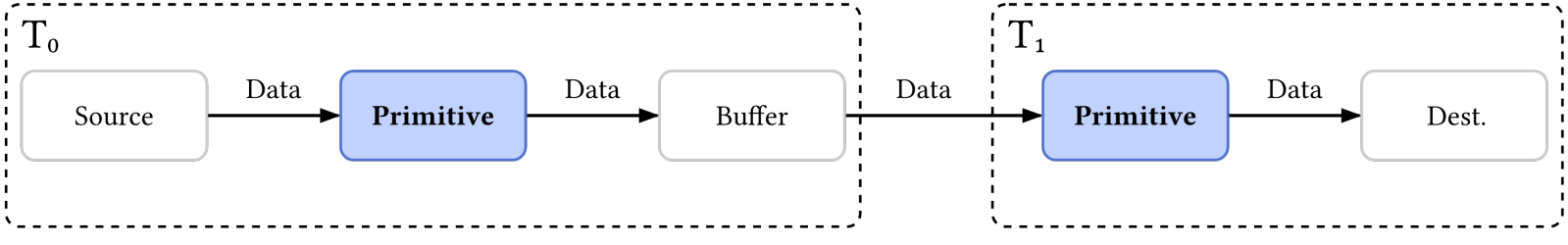


COMBINAISON DE PRIMITIVES

Le sens de circulation des données est important ...



... mais aussi le timing !

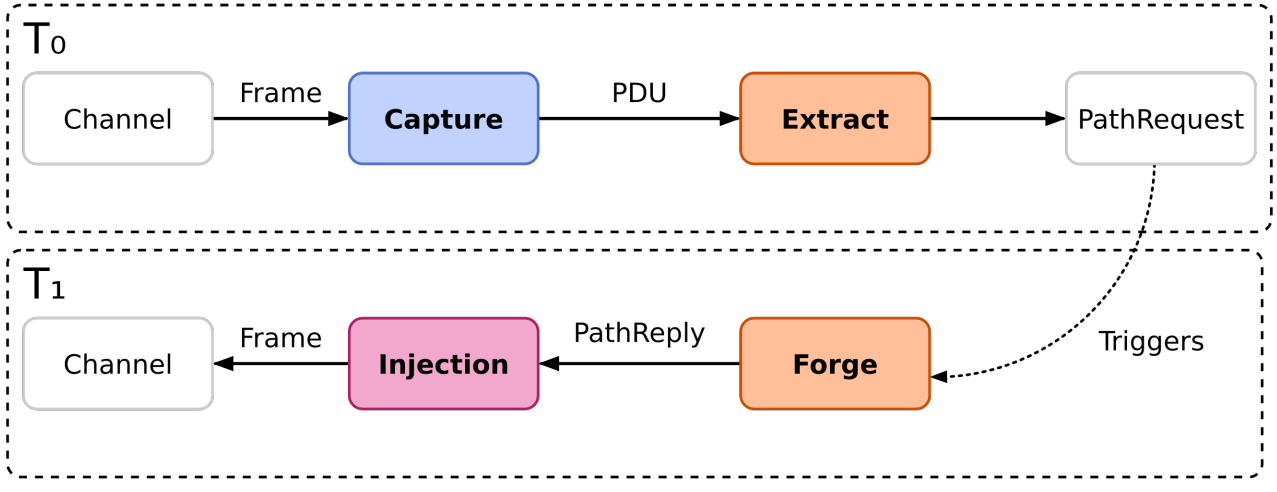


MODÉLISATION D'ATTAQUES: QUELQUES EXEMPLES

BT MESH: INJECTION DE CHEMINS ARBITRAIRES

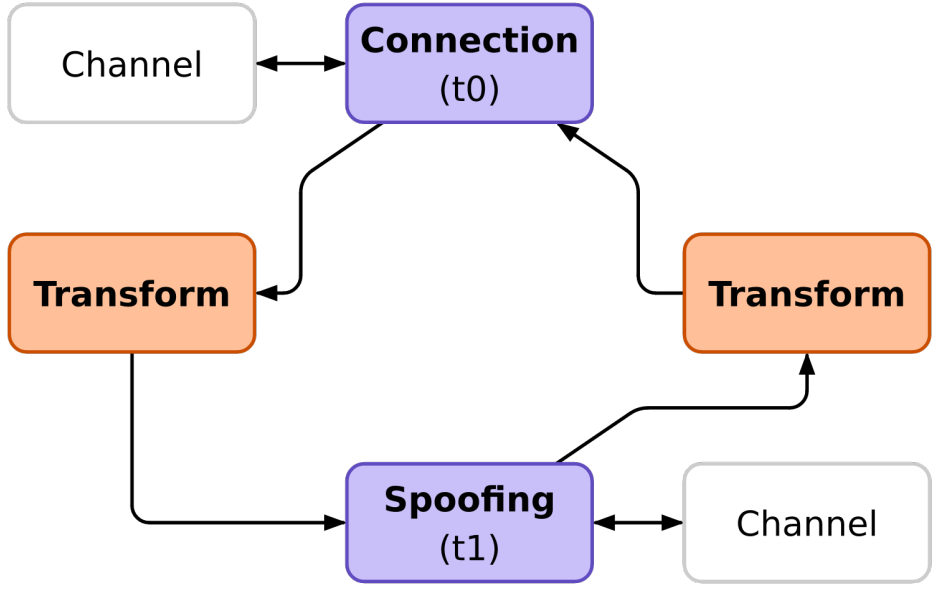
«Un attaquant peut créer un chemin depuis n'importe quel nœud du réseau vers n'importe quel autre en forgeant et transmettant une PathRequest»

BT MESH: EMPOISONNEMENT DES TABLES DE ROUTAGE



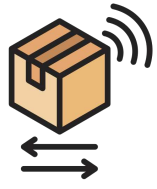
«Un attaquant peut empoisonner la table de routage du nœud à l'origine d'un chemin en répondant immédiatement à une PathRequest par l'usurpation d'un PathReply avant le nœud légitime.»

BT LE: MAN-IN-THE-MIDDLE

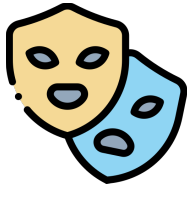


«Un attaquant peut se connecter à un équipement BLE, transmettre des données d'annonces clonées, attendre une connexion entrante et altérer les données échangées.»

LIMITES / CONTRAINTES



Représentation simplifiée de la couche physic



***Spécialisation des nœuds* non considérée** par souci de simplicité

Modèle abstrait (& simplifié) des *réseaux*

DE LA THÉORIE À LA PRATIQUE

car l'échec est toujours une option

DU MODÈLE AUX OUTILS

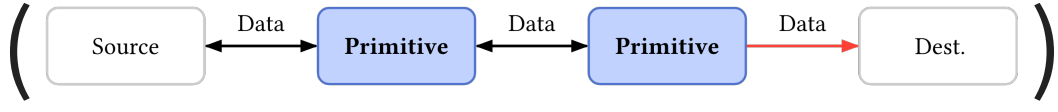
Chaque **primitive** définit un **outil de base**

Les outils peuvent être combinés pour **réaliser des tâches complexes**

KISS: **K**eep **I**t **S**imple **S**tupid !

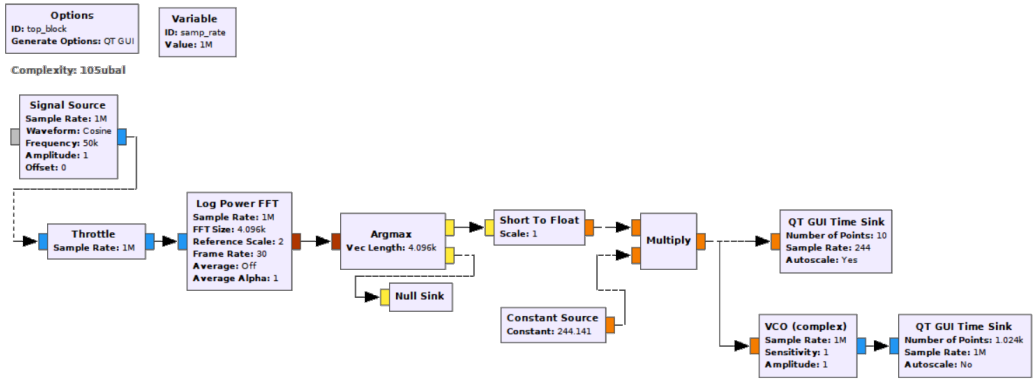
COMBINER LES OUTILS EST COMPLEXE

- **Les flux de données sont** montants et descendants

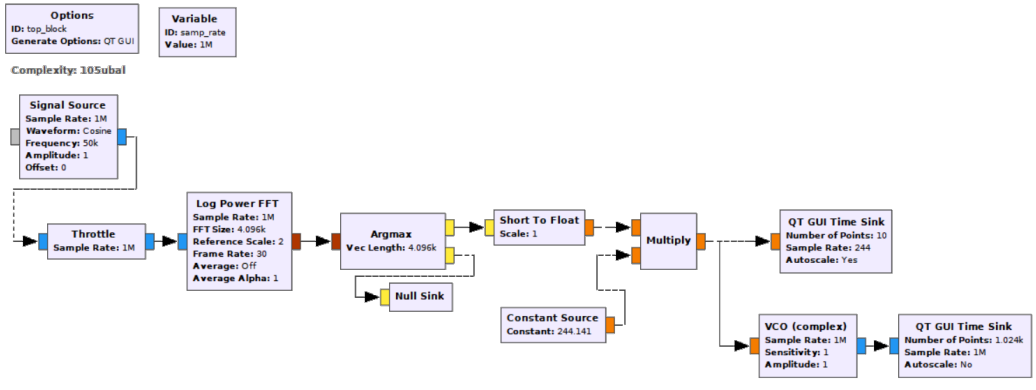


- Les outils peuvent représenter une **séquence d'actions**
  ➔ l'ordre et le timing comptent !

GNURADIO STYLE ?

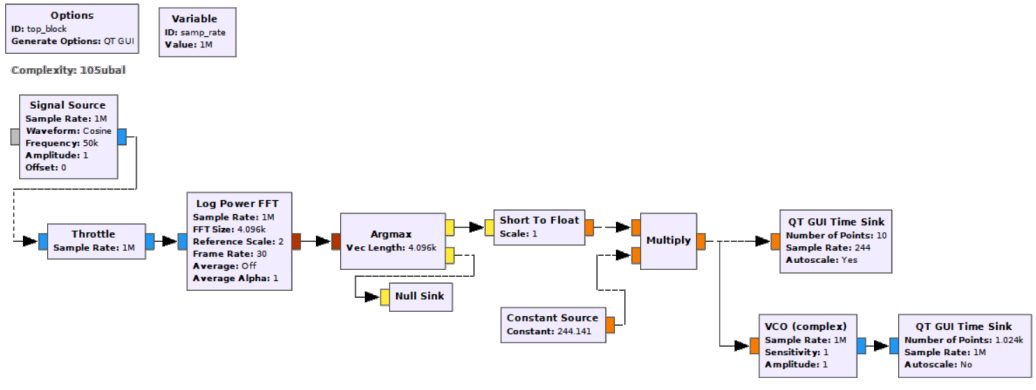


GNURADIO STYLE ?



❌ Pas vraiment KISS-compliant

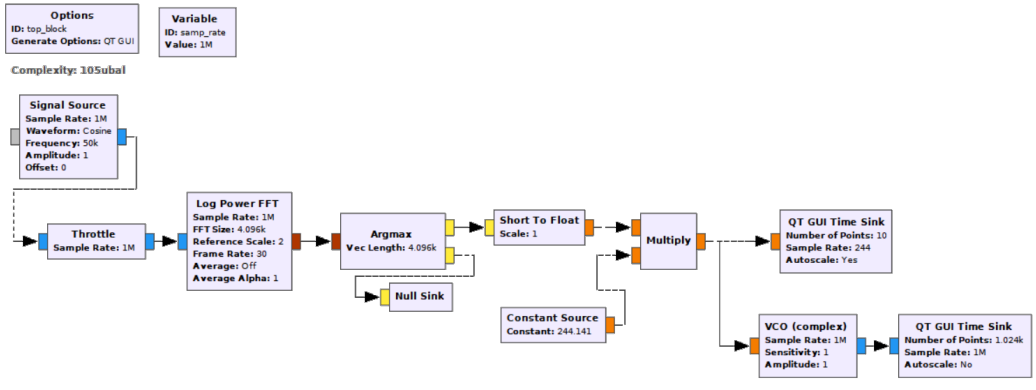
GNURADIO STYLE ?



❌ Pas vraiment KISS-compliant

✅ Supporte une séquence d'actions

GNURADIO STYLE ?

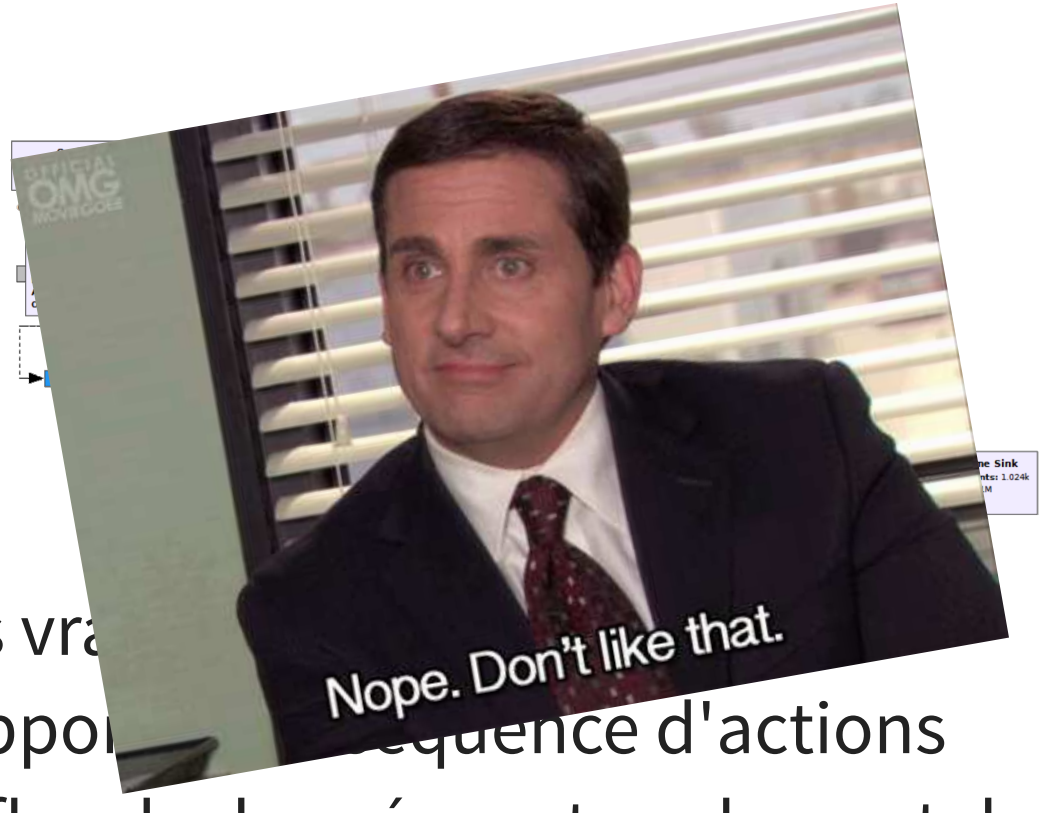


❌ Pas vraiment KISS-compliant

✅ Supporte une séquence d'actions

❌ Le flux de données est seulement descendant

GNURADIO STYLE ?



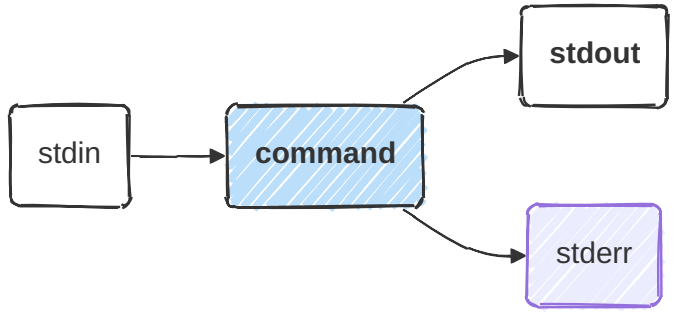
❌ Pas vra

✅ Suppo équence d'actions

❌ Le flux de données est seulement descendant

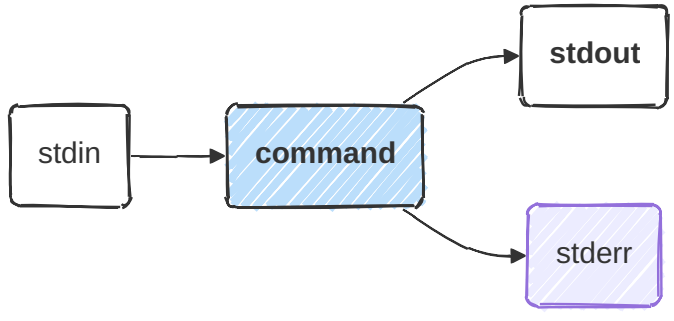
PIPES UNIX

```
cat /etc/passwd | grep root
```



PIPES UNIX

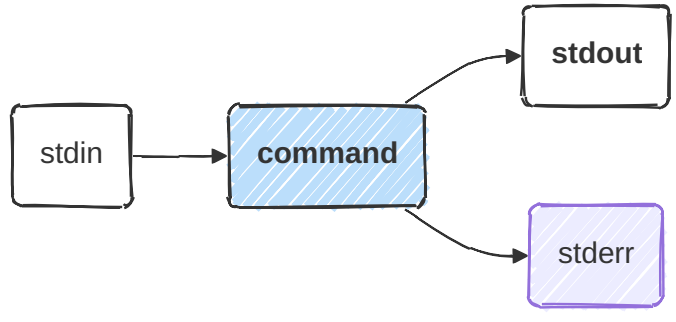
```
cat /etc/passwd | grep root
```



✅ Carrément **KISS** !

PIPES UNIX

```
cat /etc/passwd | grep root
```

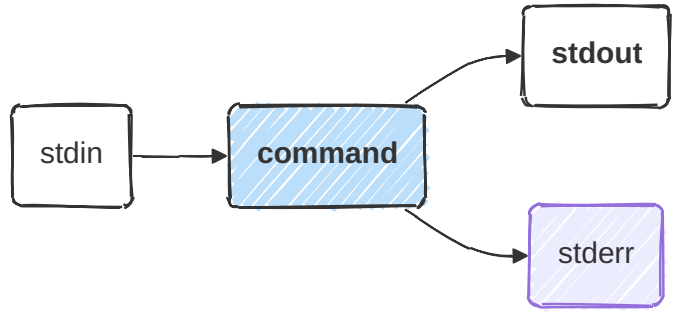


✅ Carrément **KISS** !

✅ Supporte une séquence d'actions

PIPES UNIX

```
cat /etc/passwd | grep root
```

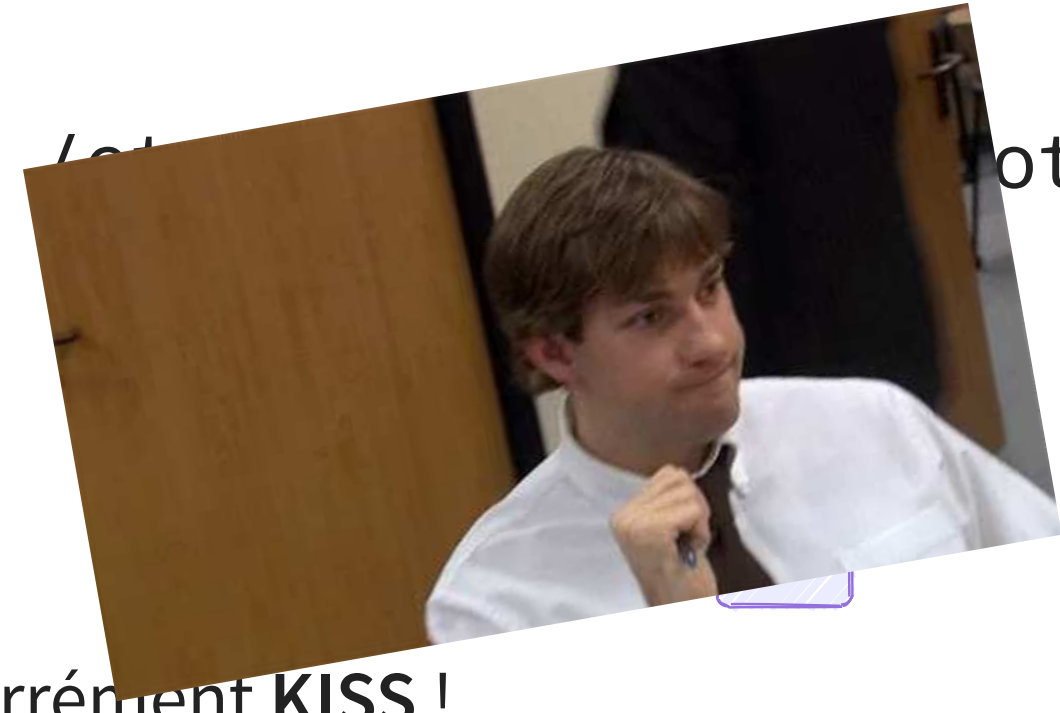


✅ Carrément **KISS** !

✅ Supporte une séquence d'actions

❌ Flux de données descendant (stdin à stdout)

PIPES UNIX

`cat /e`  `ot` 😱

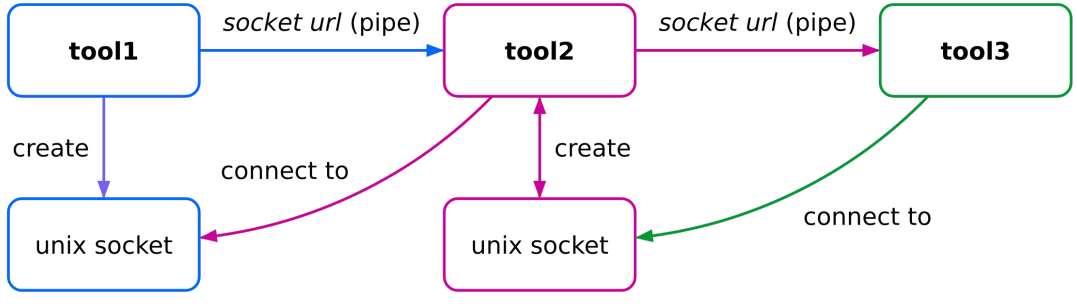
✅ Carrément **KISS** !

✅ Supporte une séquence d'actions

❌ Flux de données descendant (stdin à stdout)

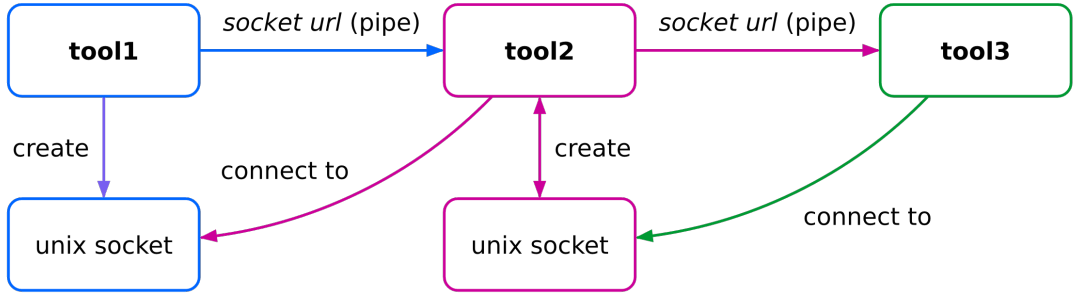
PIPES + SOCKETS

```
$ tool1 | tool2 | tool3
```



PIPES + SOCKETS

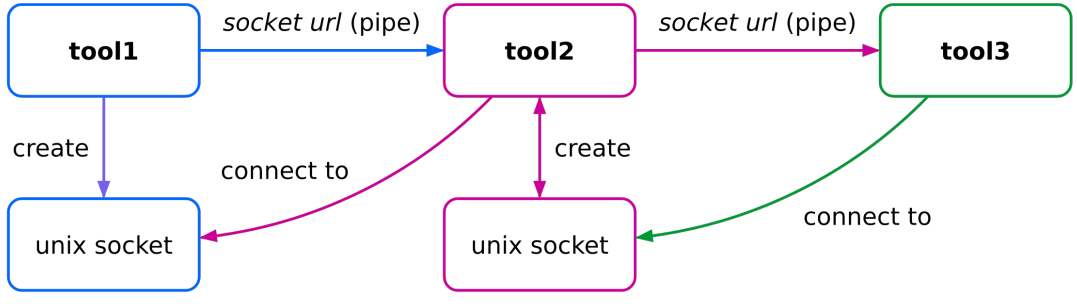
```
$ tool1 | tool2 | tool3
```



✅ Très **KISS** aussi

PIPES + SOCKETS

```
$ tool1 | tool2 | tool3
```

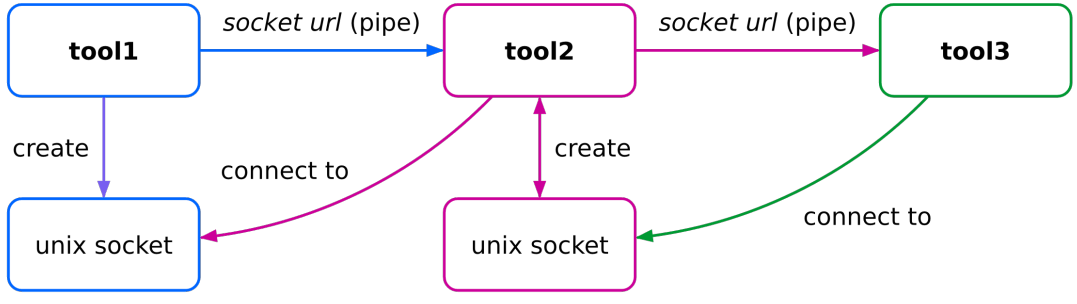


✅ Très **KISS** aussi

✅ Supporte une séquence d'actions

PIPES + SOCKETS

```
$ tool1 | tool2 | tool3
```



✅ Très **KISS** aussi

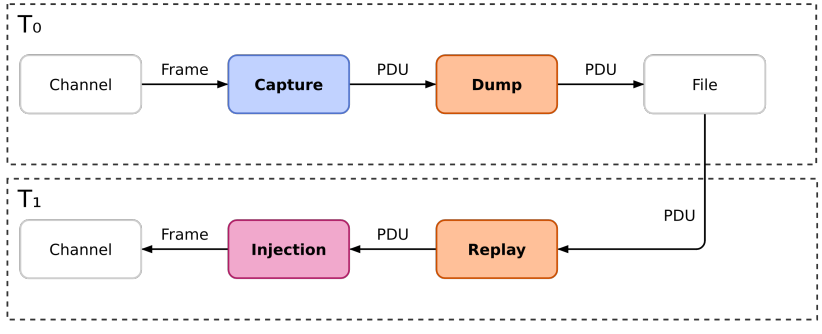
✅ Supporte une séquence d'actions

✅ Flux de données **bi-directionnel**

A L'ÉPREUVE DU RÉEL

qui a dit que tester c'est douter ?

ATTAQUE PAR REJEU SUR UNE SONNETTE 433MHZ

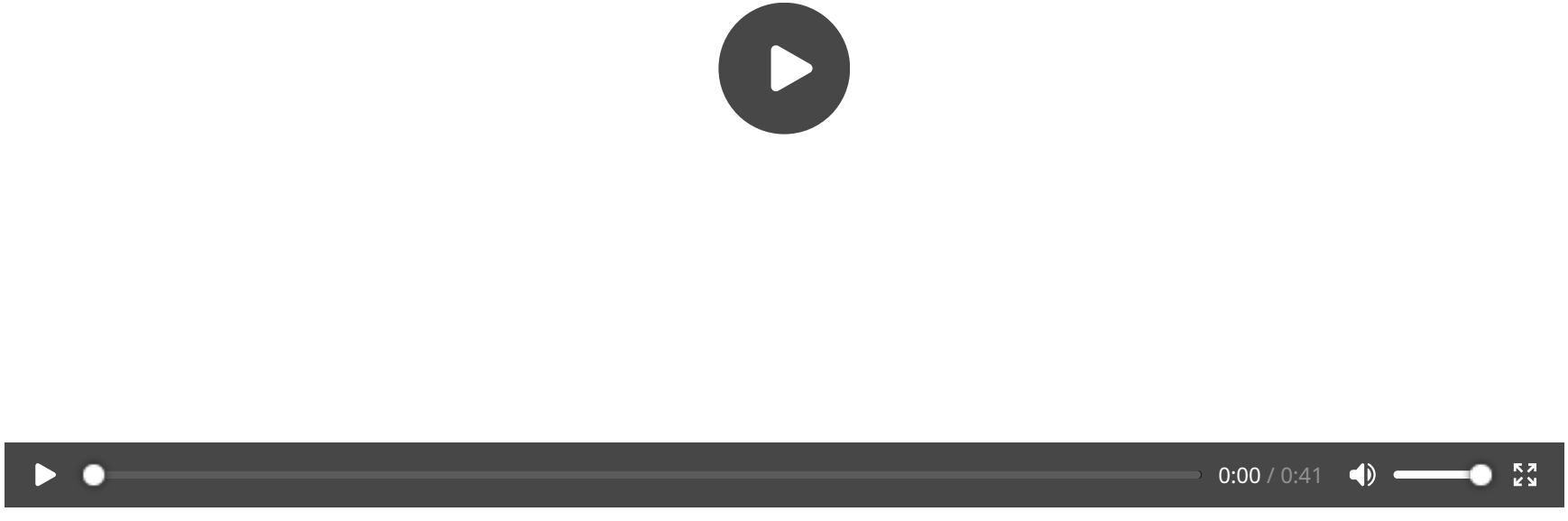


T_0:

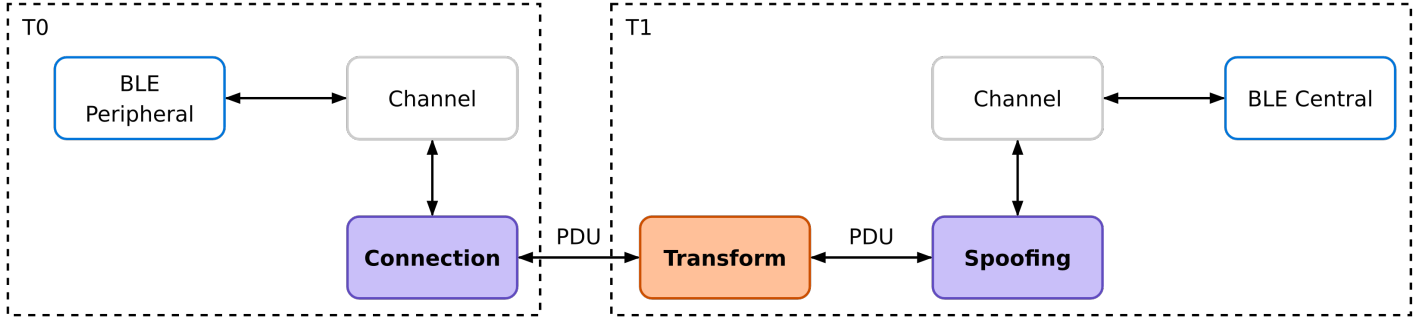
```
$ wsniff -i yardstickone0 phy -f 433920000 --ask -d 10000 |
↳ wdump doorbell-capture.pcap
```

T_1:

```
$ wplay doorbell-capture.pcap | winject -i yardstickone0
```


0:00 / 0:41

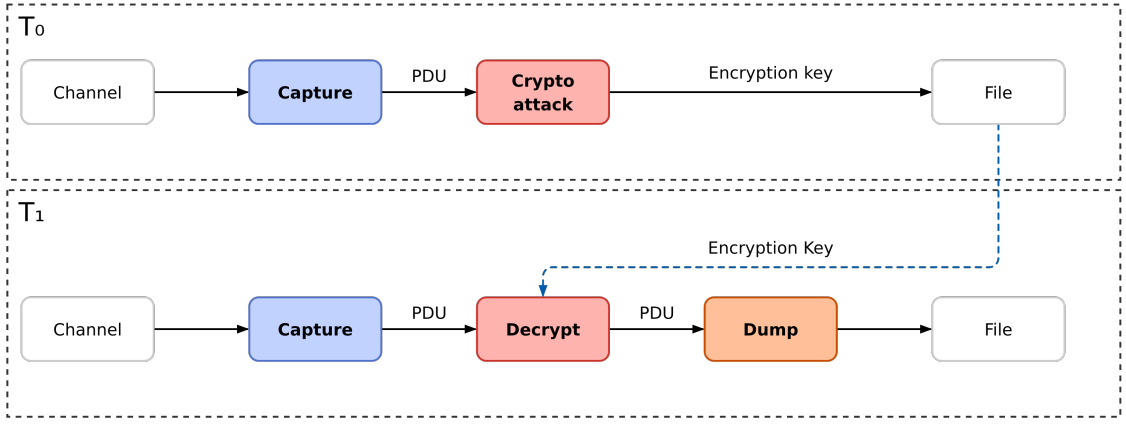
MITM BLE + ALTÉRATION À LA VOLÉE




```
$ wble-connect -i hci0 f2:c5:37:8b:cd:a2 -r |
↳ wfilter -f -t "p.data=bytes.fromhex('6f7171060001486163636b218f')"
↳ "b'Hello' in p[ATT_Write_Request].data" |
↳ wble-spawn -i hci1 -p watch.json
```

Altération à la volée d'une ATT Write Request

ATTAQUE SUR L'APPAIRAGE



T_0:

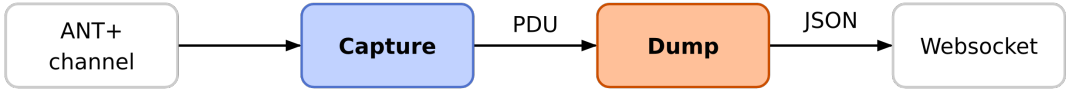
```
$ wsniff -i uart0 rf4ce -c 15 | wanalyze
```

T_1:

```
$ wsniff -i uart0 rf4ce -c 15 -d -k ENC_KEY |
↳ wdump rf4ce-cleartext.pcap
```


0:00 / 1:04

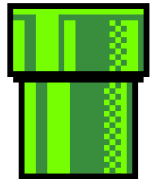
MONITORING CARDIAQUE *LIVE*




```
$ wsniff -i rfstorm0 phy --gfsk --datarate 1000000 -w a6c5e81e
↳ -f 2457000000 -s 16 | wserver --json
```

```
function initHealthBar() {
    const socket = new WebSocket('ws://localhost:12345');
    socket.addEventListener('message', function (event) {
        /* Extract HR value from packet. */
        let packet = JSON.parse(event.data)["Phy_Packet"]
        let value = parseInt(packet["data"].substr(28,2), 16);
        /* Update HTML health bar using HR value. */
        setNumber(value);
    });
}
```

LE PRIX DE LA MODULARITÉ



La complexification des *pipes* **ralentit le débogage**

L'approche KISS **augmente la fragmentation**

Certains outils de WHAD sont **multi-protocoles** (~~KISS~~)

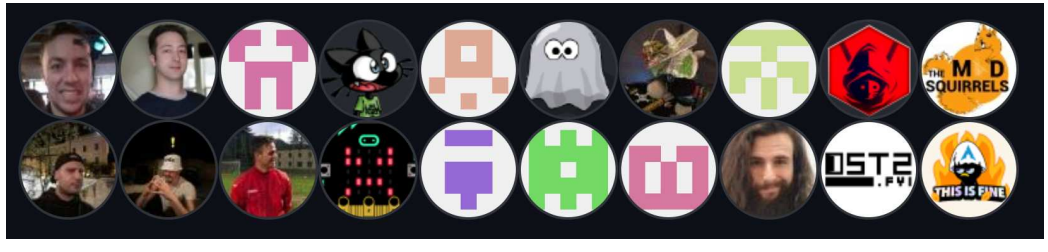
CONCLUSION

SYSTÉMATISATION DES ATTAQUES SANS FIL

- **Loin d'être parfaite** en raison des limites et contraintes
- Permet d'avoir **une meilleure compréhension des attaques**
- *Les primitives* nous ont facilité la conception d'**outils pertinents**
- Possiblités d'améliorations significatives, *n'hésitez pas à contribuer* 🙏

WHAD fournit **bien plus d'outils**, jetez y un oeil 😉

UN GRAND MERCI AUX CONTRIBUTEURS !



POUR RAPPEL ...

Les Actes du SSTIC contiennent une description détaillée de notre systématisation, de ses *primitives* et des modèles d'attaques considérés.

MERCI, DES QUESTIONS ?

https://whad.io

Romain Cayre

rcayre@laas.fr

@rcayre@infosec.exchange

Damien Cauquil

dcauquil@quarkslab.com

@virtualabs@mamot.fr