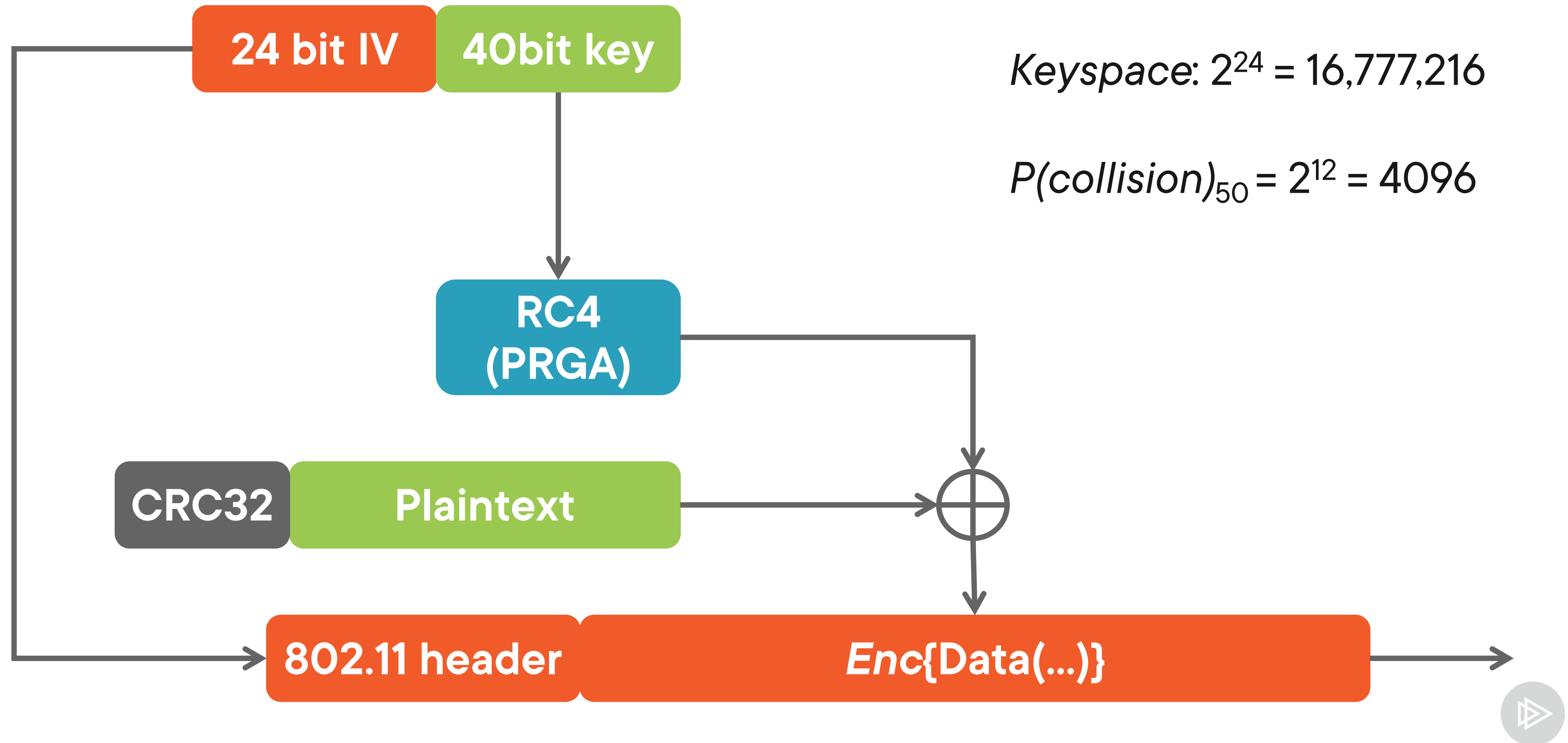


Cracking Wireless Authentication Keys



WEP Encryption



Demo



Cracking WEP



Cracking WPA Encryption with Dictionary Attacks



WPA

Pros

Addresses security vulnerabilities of its predecessor WEP

Uses a 256-bit key for encryption

TKIP encryption method is better than fixed-key encryption

Uses MIC instead of CRC for data integrity check

Cons

TKIP is RC4 cipher stream based

When rolled out onto WEP devices, TKIP has similar security vulnerabilities to WEP



WPA2

Pros

- Uses the AES encryption method
- CCMP replaces TKIP as the encryption protocol
- Uses CCMP instead of MIC for data integrity check

Cons

- Still contains some security vulnerabilities
- Requires the most processing power



WPA3

Pros

Makes a number of security improvements

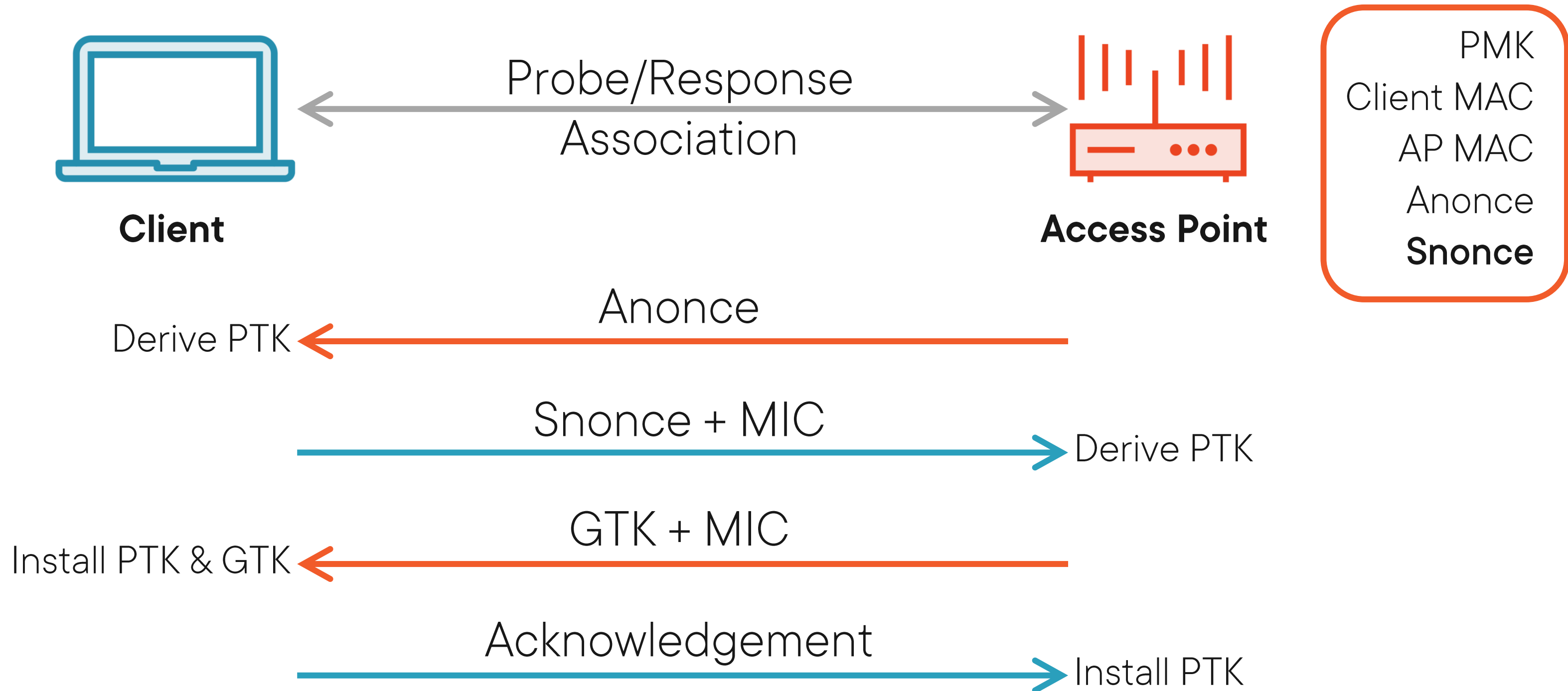
Replaces AES with simultaneous authentication of equals (SAE) encryption

Cons

Not yet widely adopted



The WPA 4-way Handshake



Authenticated!

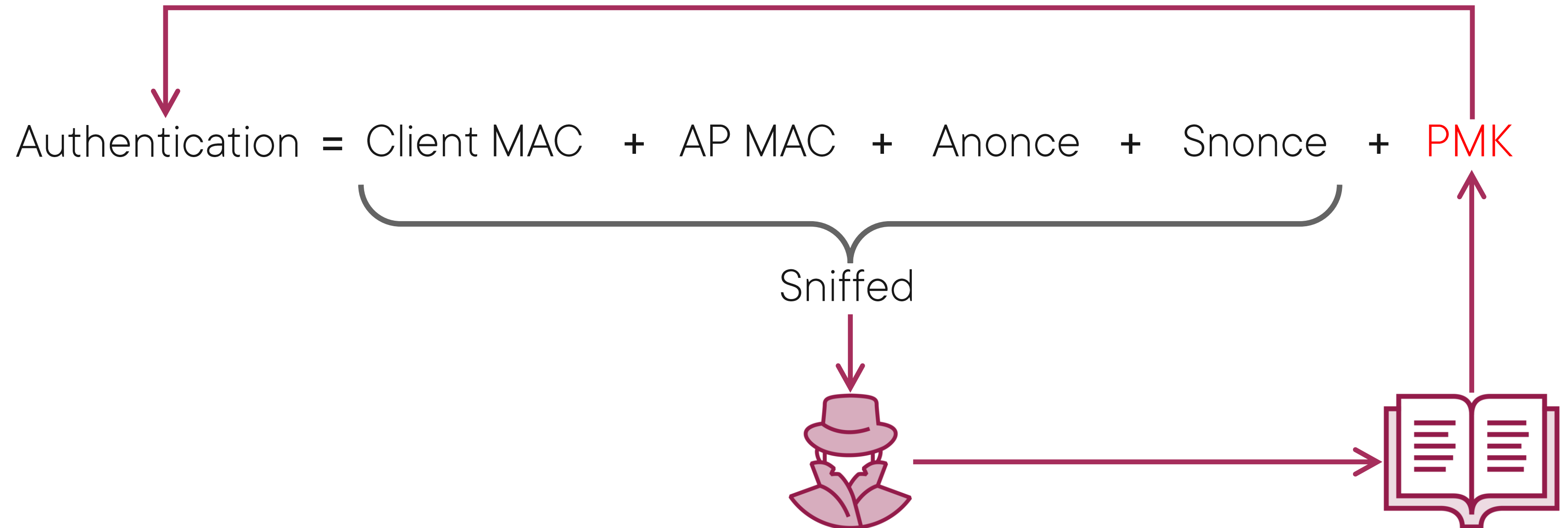


Cracking WPA

Authentication = Client MAC + AP MAC + Anonce + Snonce + PMK



Cracking WPA



Demo



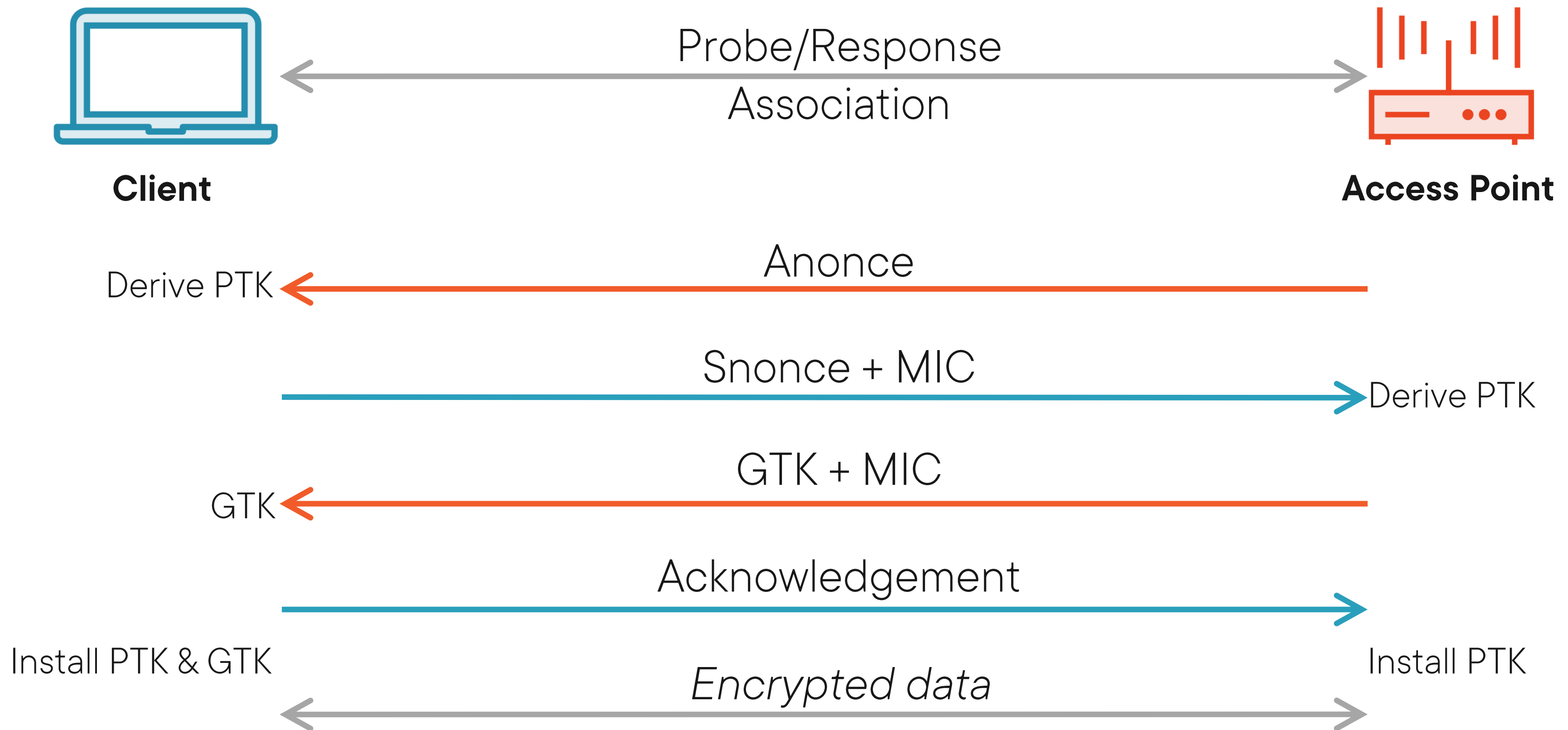
Cracking WPA/WPA2



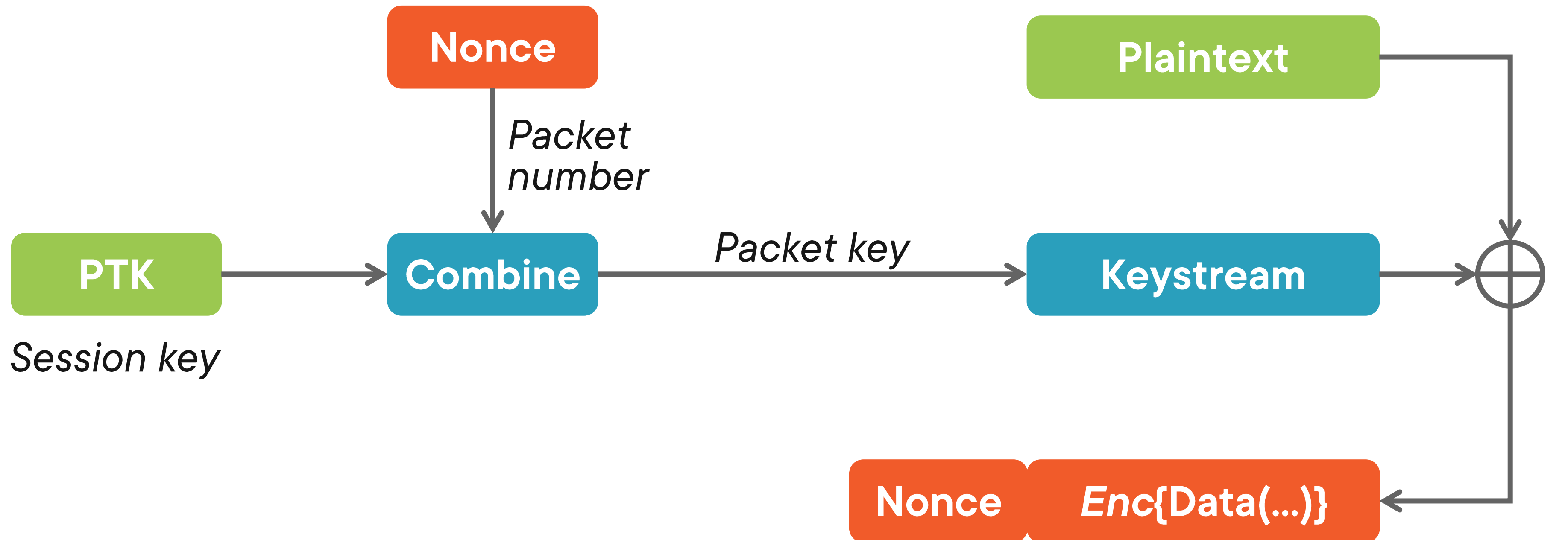
Cracking WPA



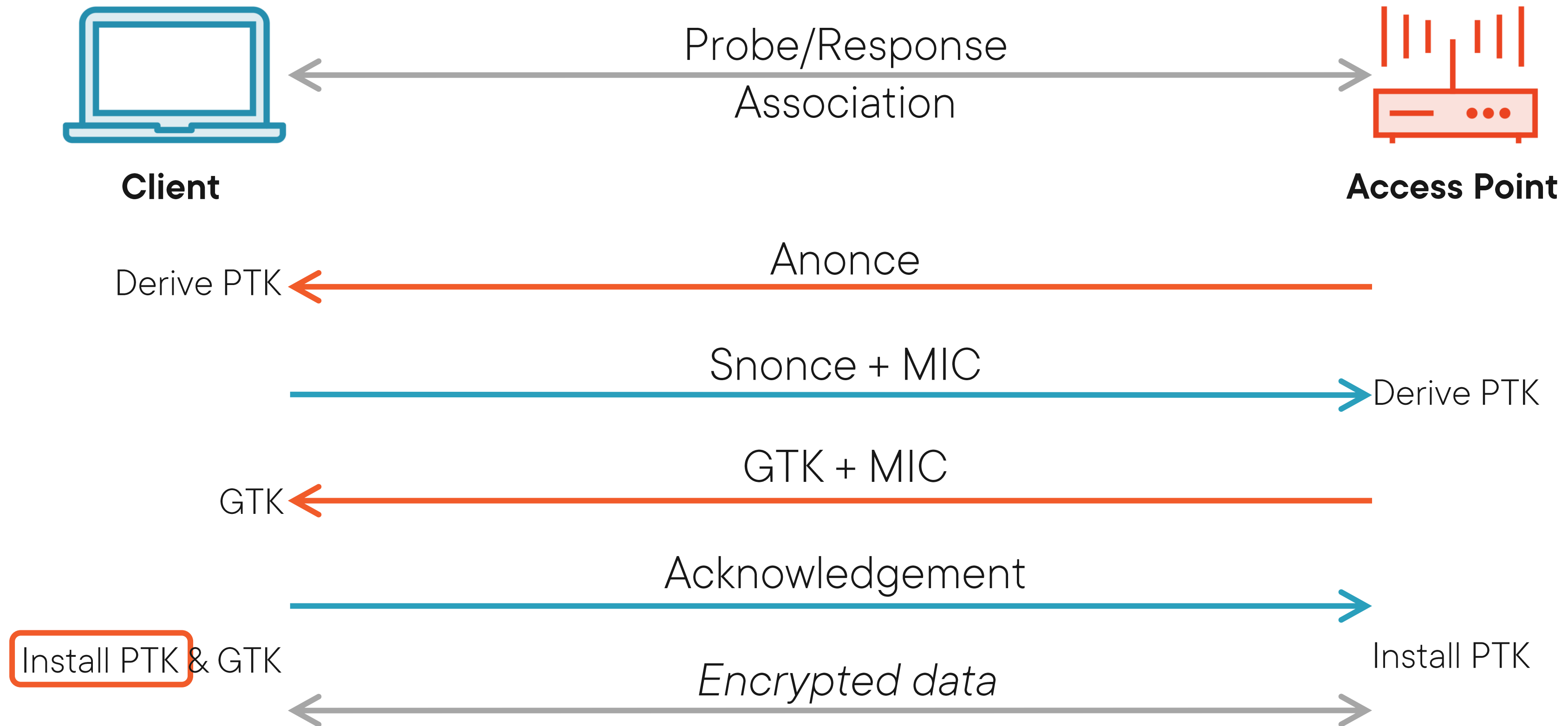
The WPA 4-way Handshake



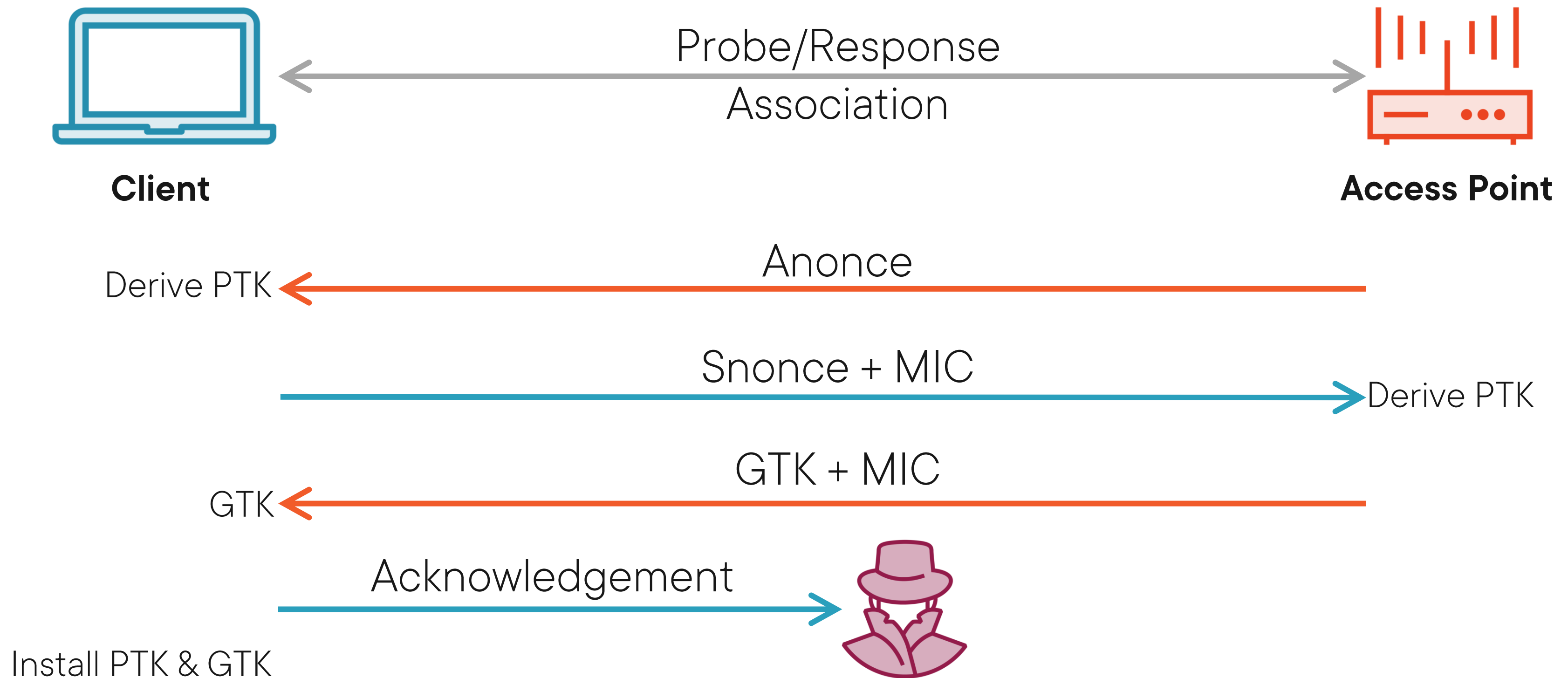
WPA Encryption



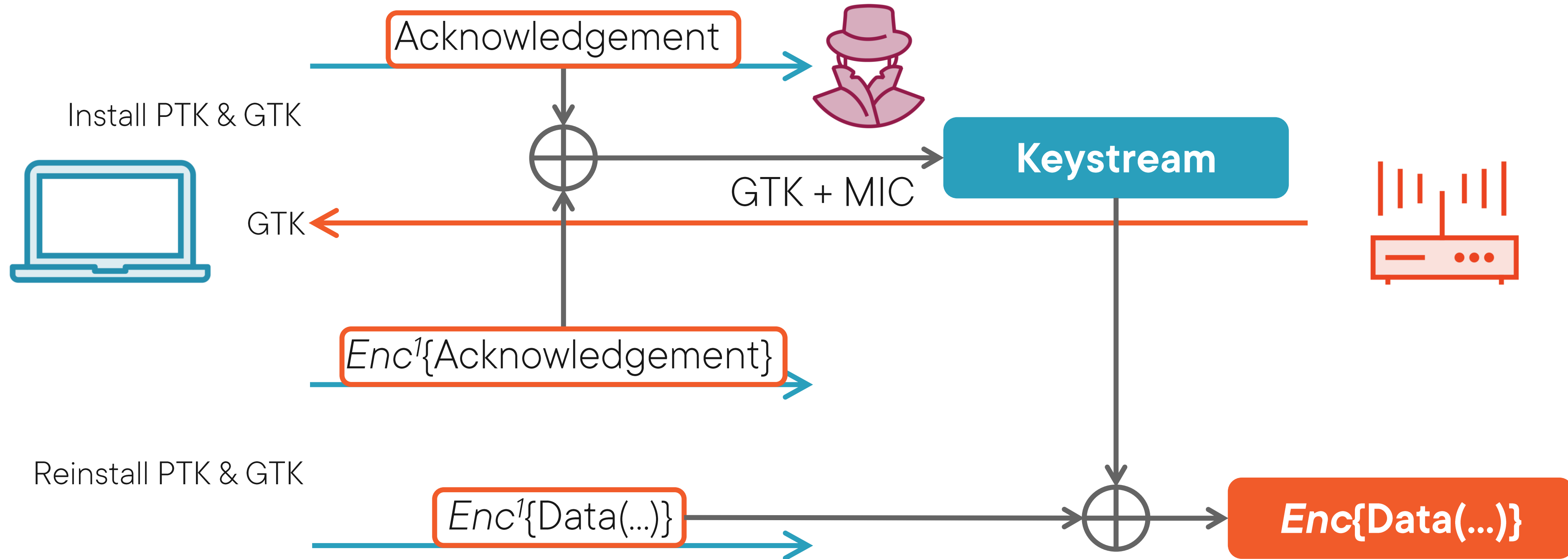
Cracking WPA



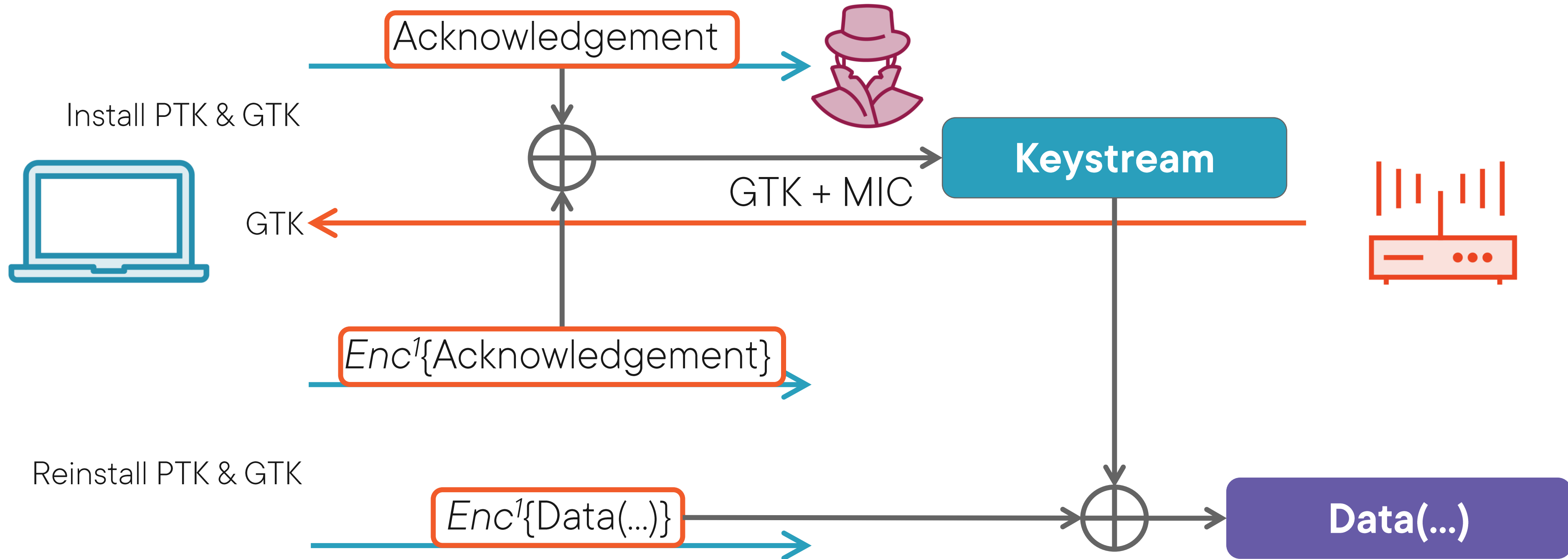
Cracking WPA



Cracking WPA



Cracking WPA



Demo



The KRACK Attack



```
# apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git  
sysfsutils python3-scapy
```

KRACK Attack Proof-of-concept

Obtaining code

Initial configuration

Prepare python virtual environment

```
# apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git  
sysfsutils python3-scapy
```

```
# git clone https://github.com/vanhoefm/krackattacks-scripts.git
```

KRACK Attack Proof-of-concept

Obtaining code

Initial configuration

Prepare python virtual environment

```
# apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git  
sysfsutils python3-scapy  
  
# git clone https://github.com/vanhoefm/krackattacks-scripts.git  
  
# cd krackattacks-scripts/krackattack
```

KRACK Attack Proof-of-concept

Obtaining code

Initial configuration

Prepare python virtual environment

```
# apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git  
sysfsutils python3-scapy  
  
# git clone https://github.com/vanhoefm/krackattacks-scripts.git  
  
# cd krackattacks-scripts/krackattack  
  
# ./disable-hwcrypto.sh
```

KRACK Attack Proof-of-concept

Obtaining code

Initial configuration

Prepare python virtual environment

```
# apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git  
sysfsutils python3-scapy  
  
# git clone https://github.com/vanhoefm/krackattacks-scripts.git  
  
# cd krackattacks-scripts/krackattack  
  
# ./disable-hwcrypto.sh  
  
# nano hostapd.conf
```

KRACK Attack Proof-of-concept

Obtaining code

Initial configuration

Prepare python virtual environment


```
# apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git  
sysfsutils python3-scapy  
  
# git clone https://github.com/vanhoefm/krackattacks-scripts.git  
  
# cd krackattacks-scripts/krackattack  
  
# ./disable-hwcrypto.sh  
  
# nano hostapd.conf  
  
# ./build.sh
```

KRACK Attack Proof-of-concept

Obtaining code

Initial configuration

Prepare python virtual environment

```
# apt-get install libnl-3-dev libnl-genl-3-dev pkg-config libssl-dev net-tools git  
sysfsutils python3-scapy  
  
# git clone https://github.com/vanhoefm/krackattacks-scripts.git  
  
# cd krackattacks-scripts/krackattack  
  
# ./disable-hwcrypto.sh  
  
# nano hostapd.conf  
  
# ./build.sh  
  
# ./pysetup.sh
```

KRACK Attack Proof-of-concept

Obtaining code

Initial configuration

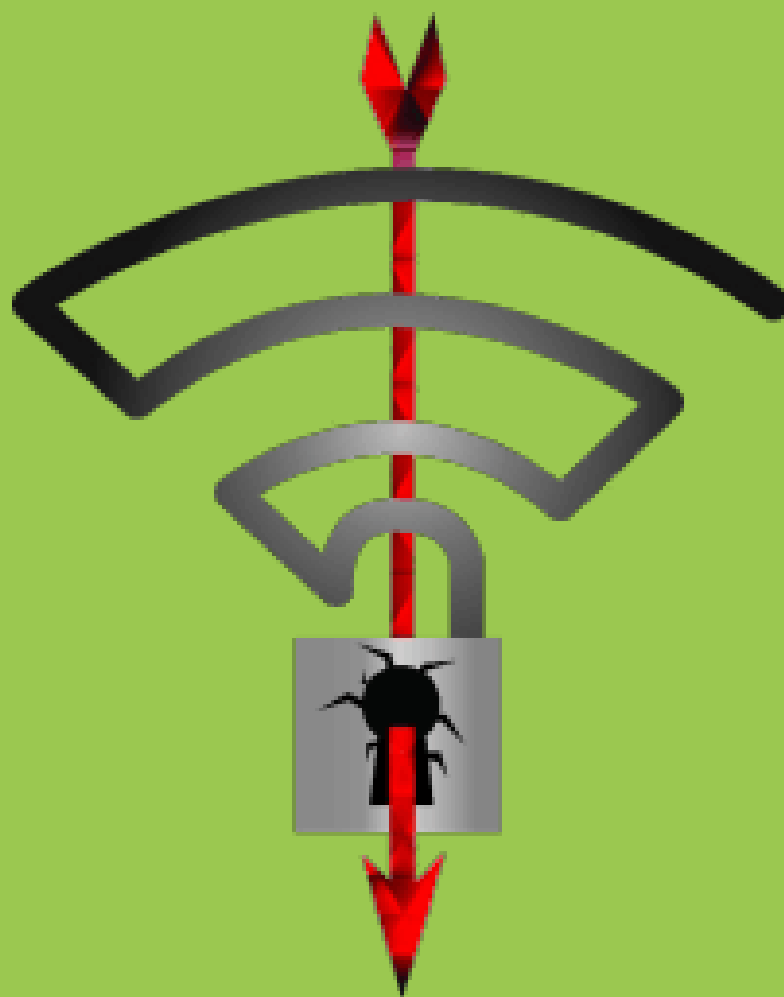
Prepare python virtual environment



Broadcast Replay

Test whether the client accepts replayed
broadcast frames





KRACK Test Client

Test for key reinstallations in the 4-way
handshake





Group Temporal Key Installation

Test whether the client installs the group key in
the 4-way handshake



Up Next: Bringing it all Together

