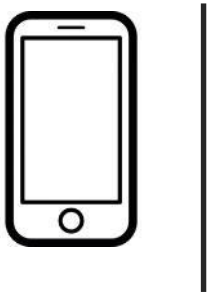
Performing aggregation attack (CVE-2020-24588) in practice

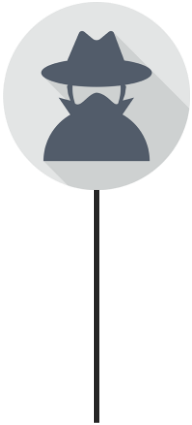
Mathy Vanhoef

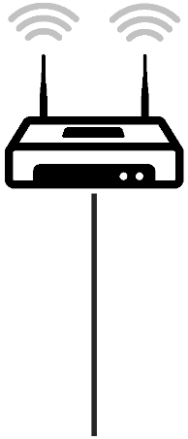
20 January 2021

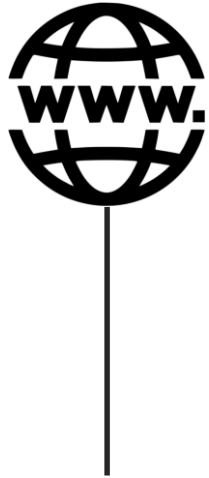
NEW YORK UNIVERSITY

Aggr. Attack

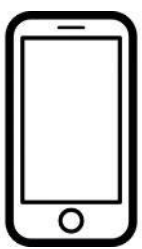


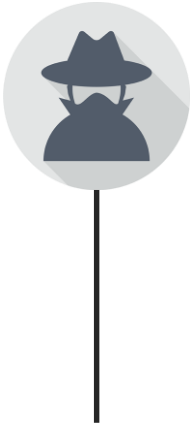


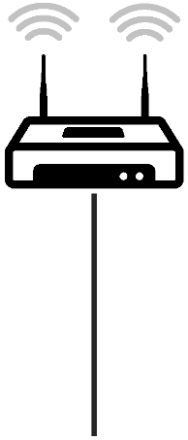


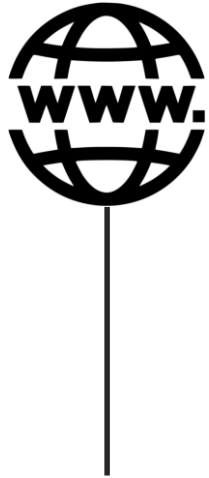


Aggr. Attack



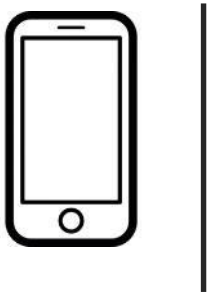


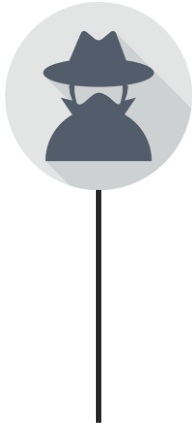


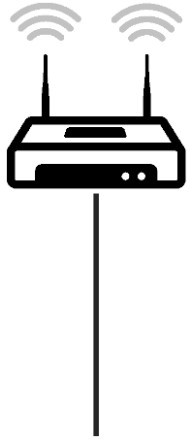


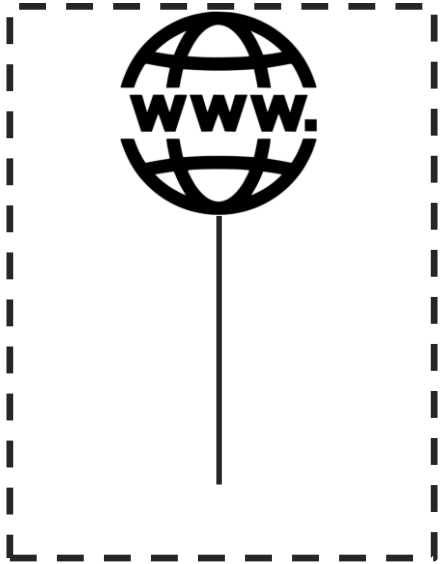
This is the Wi-Fi network we are targeting.

Aggr. Attack



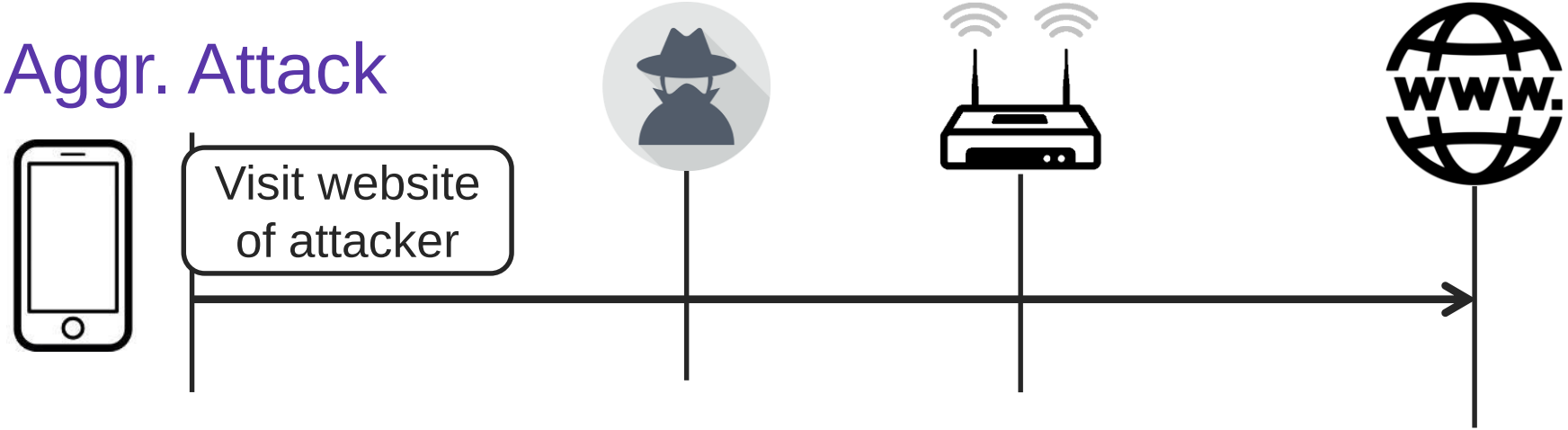






This is a server on the internet under control of the attacker. For example, a website owned by the attacker.

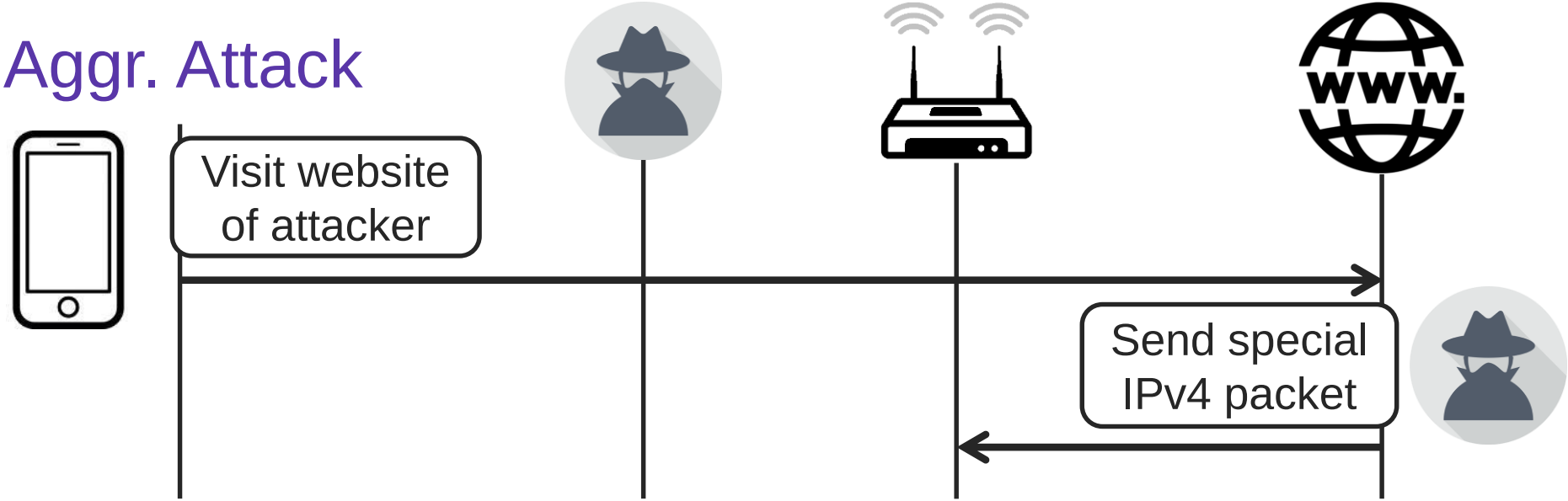
Aggr. Attack



Step 1: victim is tricked into connect to the attacker's server, for instance by visiting their website. This causes the victim to create a TCP connection with the attacker's server.

Note: this doesn't require code execution on the victim.

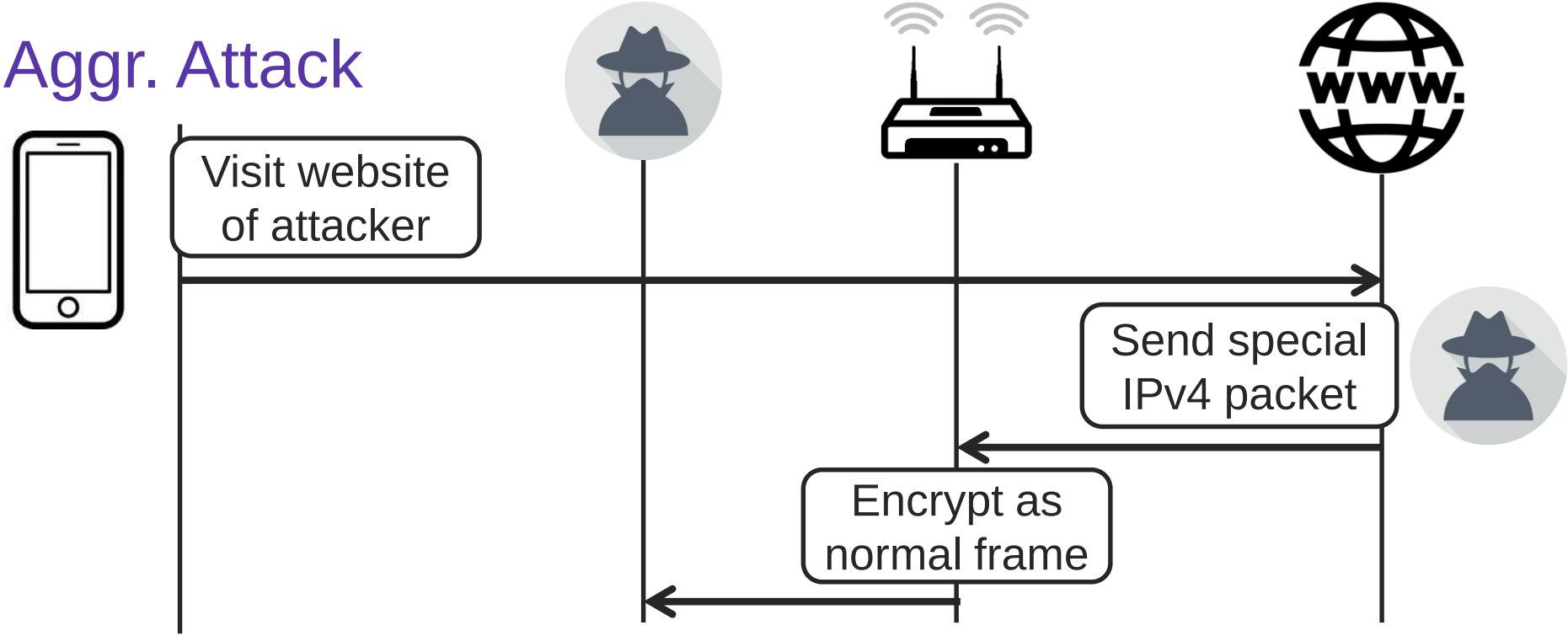
Aggr. Attack



Step 2: the attacker's server sends a special IPv4 packet to the client over this TCP connection.

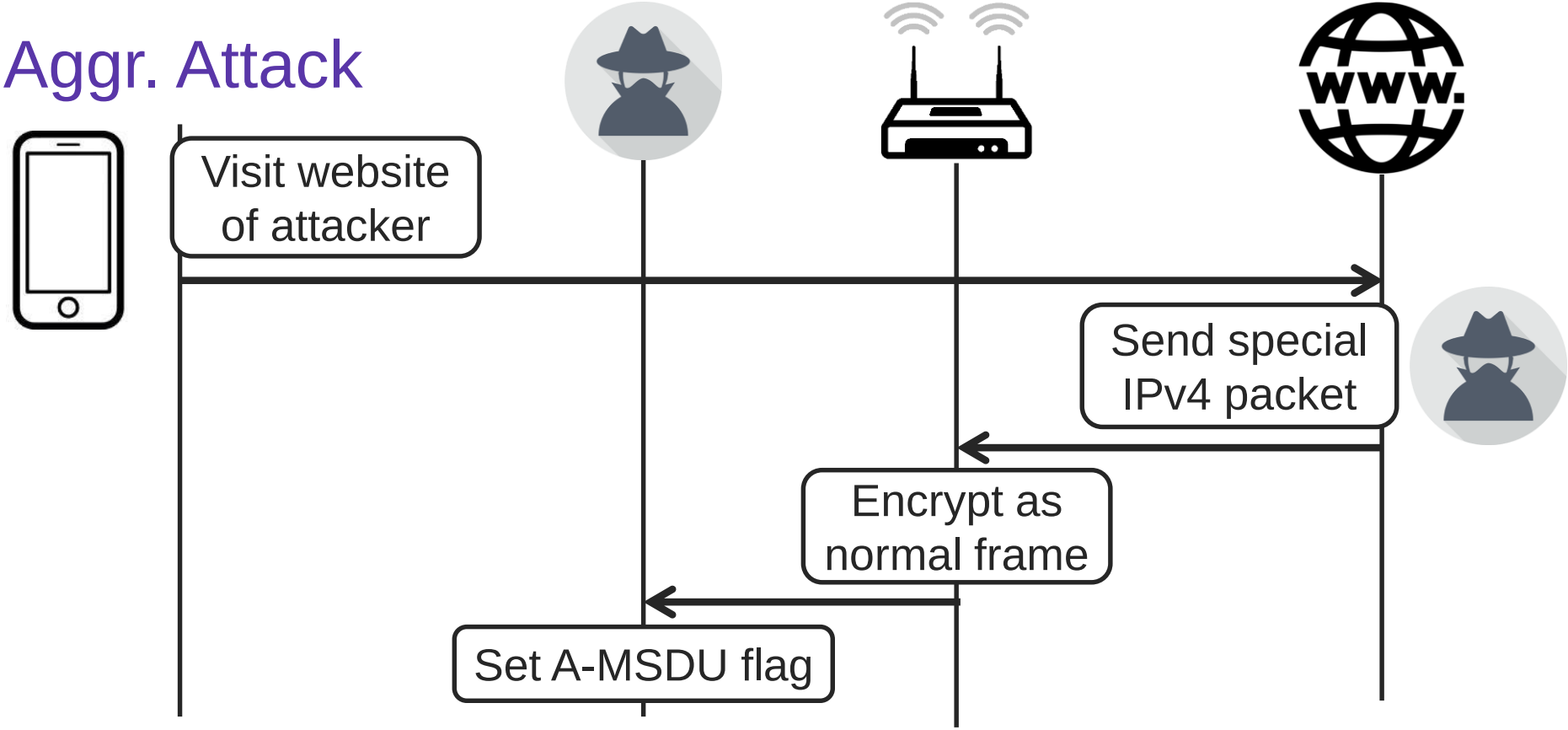
This special IPv4 packet contains the "`create_msdu_subframe(…, last=True)`" payload that is also sent in the "`amsdu-inject[-bad]`" test.

Aggr. Attack



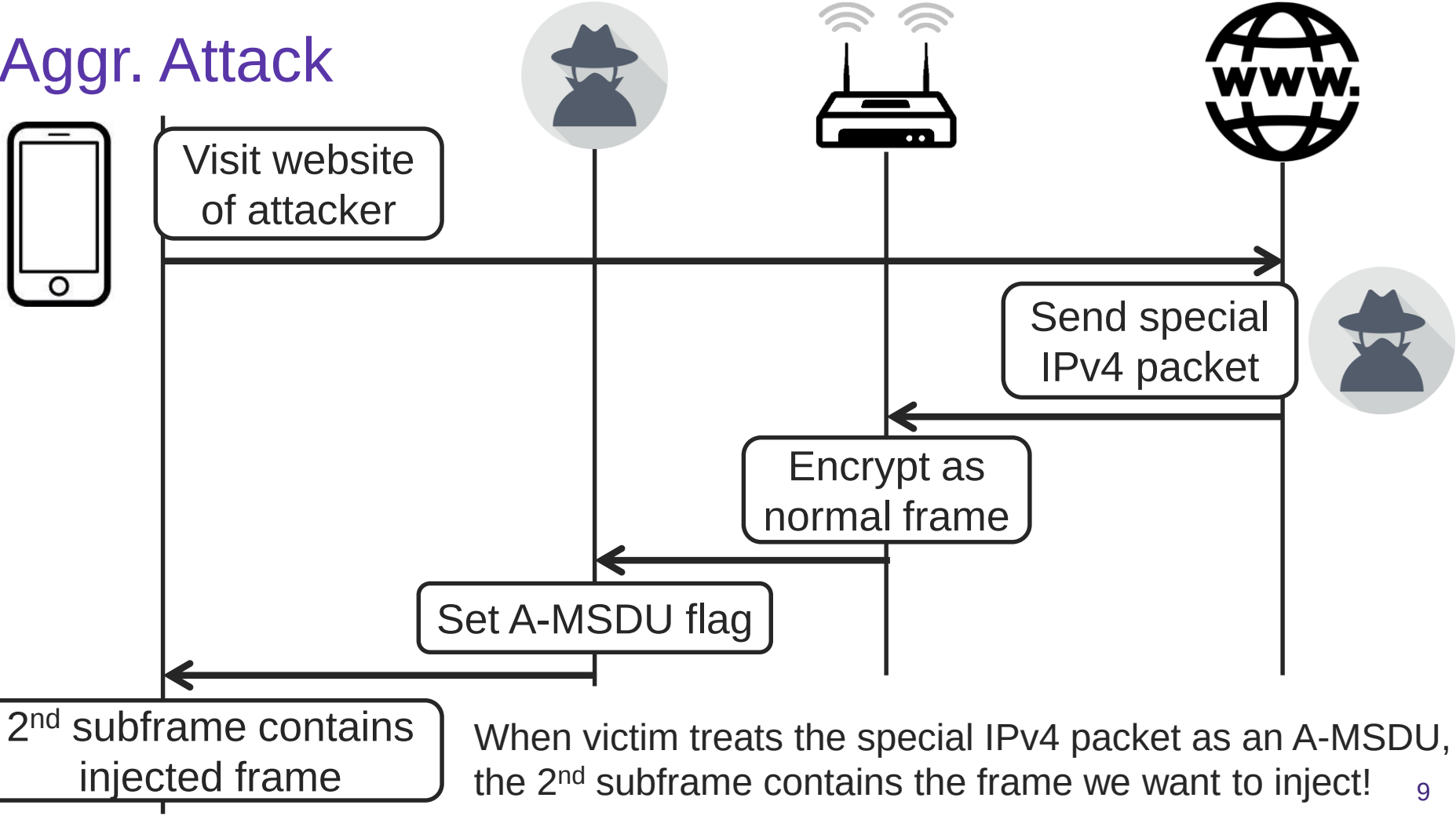
The AP will encrypt the special IPv4 packet and sent it to the client… but the attacker will intercept it first!

Aggr. Attack



Step 3: attacker sets the A-MSDU flag and then forwards the encrypted Wi-Fi frame.

Aggr. Attack



When victim treats the special IPv4 packet as an A-MSDU, the 2nd subframe contains the frame we want to inject!

Conclusion

We **can inject arbitrary network packets**, such as DHCP and ICMPv6 RA packets!

Not a trivial threat model:

- Need to trick victim into connecting to attacker's server
- Simultaneously need to be within radio range of the victim

But most devices are affected: even if non-trivial, **somewhere this attack is feasible**... Patch now before attacks get better.