Wi-Fi Protected Access 3 (WPA3) -

Dragonblood attack

(2019)

2018
IEEE 802.1s (SAE,2016)

Types

Personal		
Enterprise		
Enterprise with 192-bit mode		

+ *Better cryptography*

+ *Forward secrecy*

+ *Management frame protection*

+ *Open Wi-Fi Networks:* unauth. data encryption

− *Attacks:* downgrade (WPA2), side-channels vs. DoS, Dragonblood, etc.
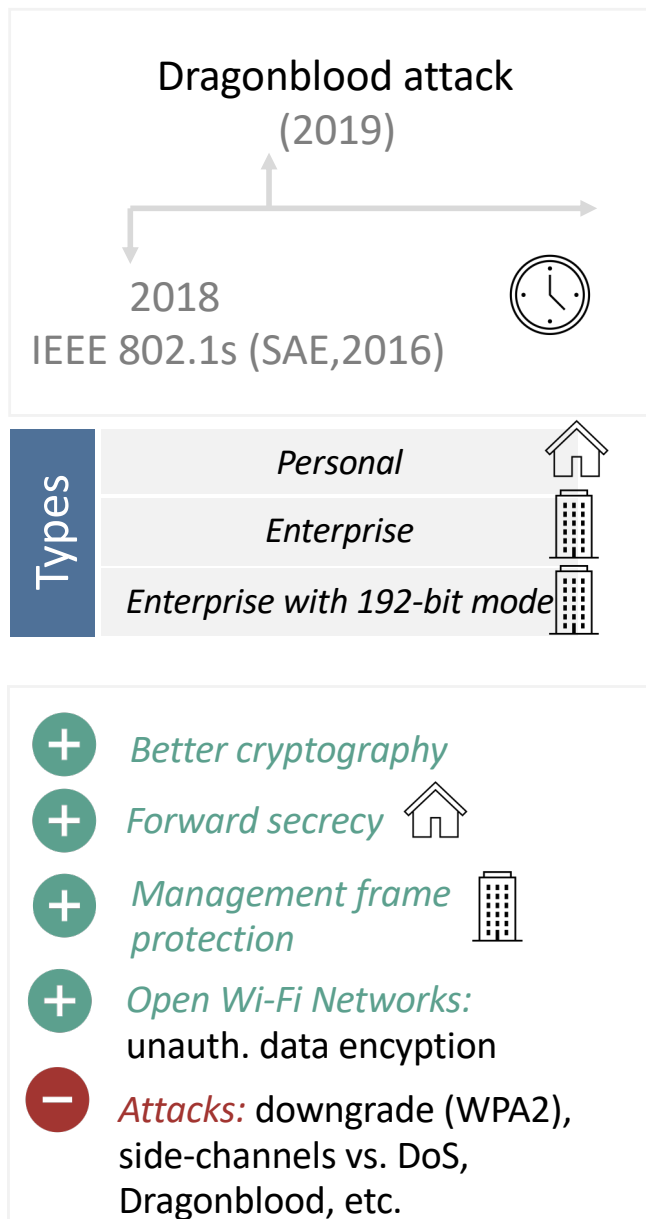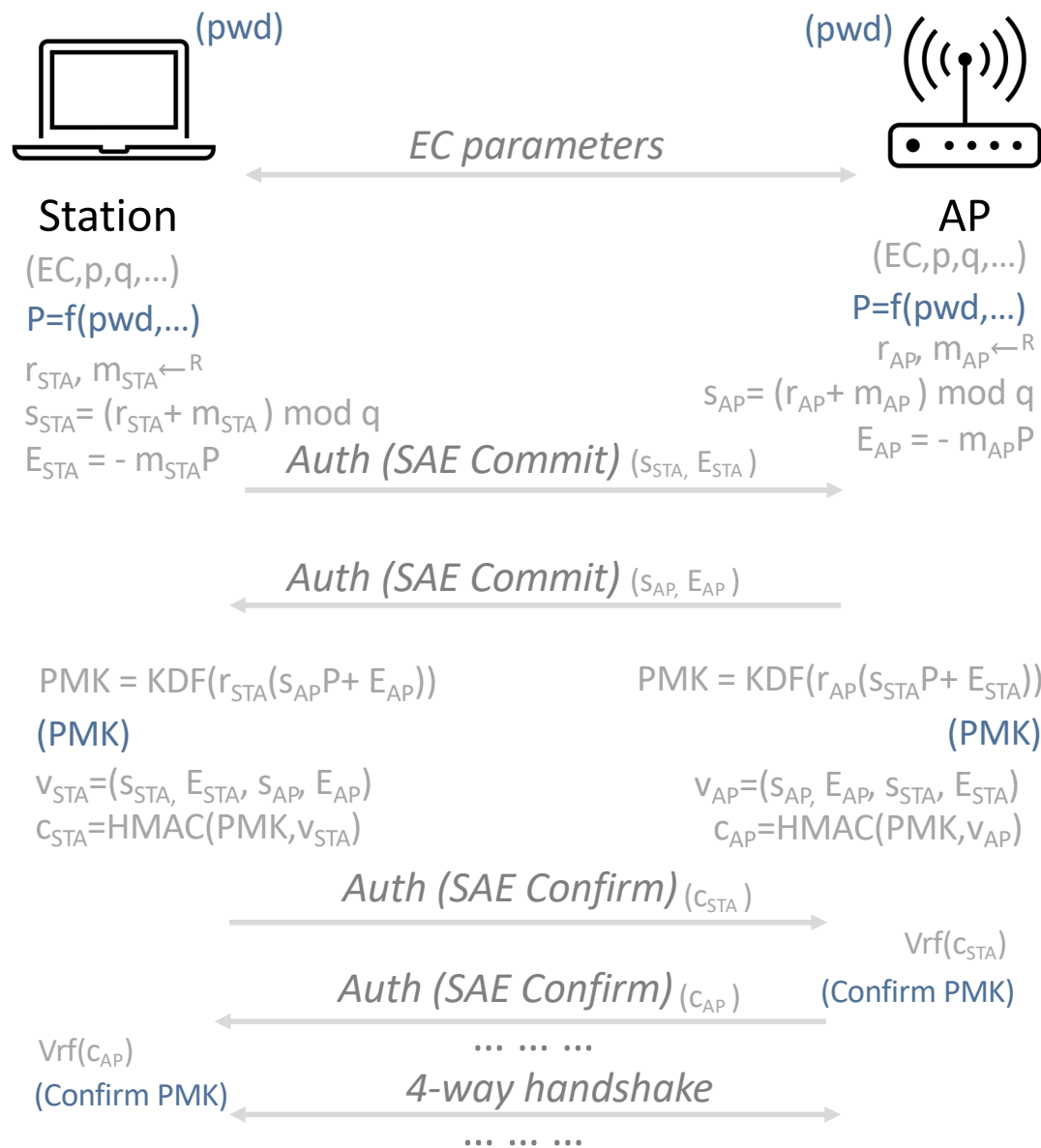
SAE: Simultaneous Authentication of Equals
DoS: Denial of Service
PAKE: Password Authentication Key Exchange
EC: Elliptic Curve
KDF: Key Derivation Function

Dragonfly Key Exchange

(pwd)   (pwd)

$\longleftrightarrow$ *EC parameters* $\longleftrightarrow$

Station   **AP**

$(EC,p,q,...)$ $(EC,p,q,...)$

$P=f(pwd,...)$ $P=f(pwd,...)$

$r_{STA}, m_{STA} \leftarrow^R$ $r_{AP}, m_{AP} \leftarrow^R$

$s_{STA} = (r_{STA} + m_{STA}) \bmod q$ $s_{AP} = (r_{AP} + m_{AP}) \bmod q$

$E_{STA} = - m_{STA}P$ $E_{AP} = - m_{AP}P$

Auth (SAE Commit) (s_{STA}, E_{STA}) $\longrightarrow$

$\longleftarrow$ *Auth (SAE Commit)* (s_{AP}, E_{AP})

$PMK = KDF(r_{STA}(s_{AP}P + E_{AP}))$ $PMK = KDF(r_{AP}(s_{STA}P + E_{STA}))$

(PMK)   (PMK)

$v_{STA} = (s_{STA}, E_{STA}, s_{AP}, E_{AP})$ $v_{AP} = (s_{AP}, E_{AP}, s_{STA}, E_{STA})$

$c_{STA} = HMAC(PMK, v_{STA})$ $c_{AP} = HMAC(PMK, v_{AP})$

Auth (SAE Confirm) (c_{STA}) $\longrightarrow$

$Vrf(c_{STA})$

(Confirm PMK)

$\longleftarrow$ *Auth (SAE Confirm)* (c_{AP})

$Vrf(c_{AP})$

... ...

(Confirm PMK)   *4-way handshake*

... ...

+ *Negotiation of keys:* Prevent offline dictionary attacks

+ *Mutual authentication*