

# Exploiting Wireless Authentication Weaknesses

---



# Demo



## Finding Hidden SSIDs



# Demo



## Beating MAC Filters



# Bypassing Shared Key Authentication

---



# Shared Key Authentication

$$p = \langle m, CRC(m) \rangle$$

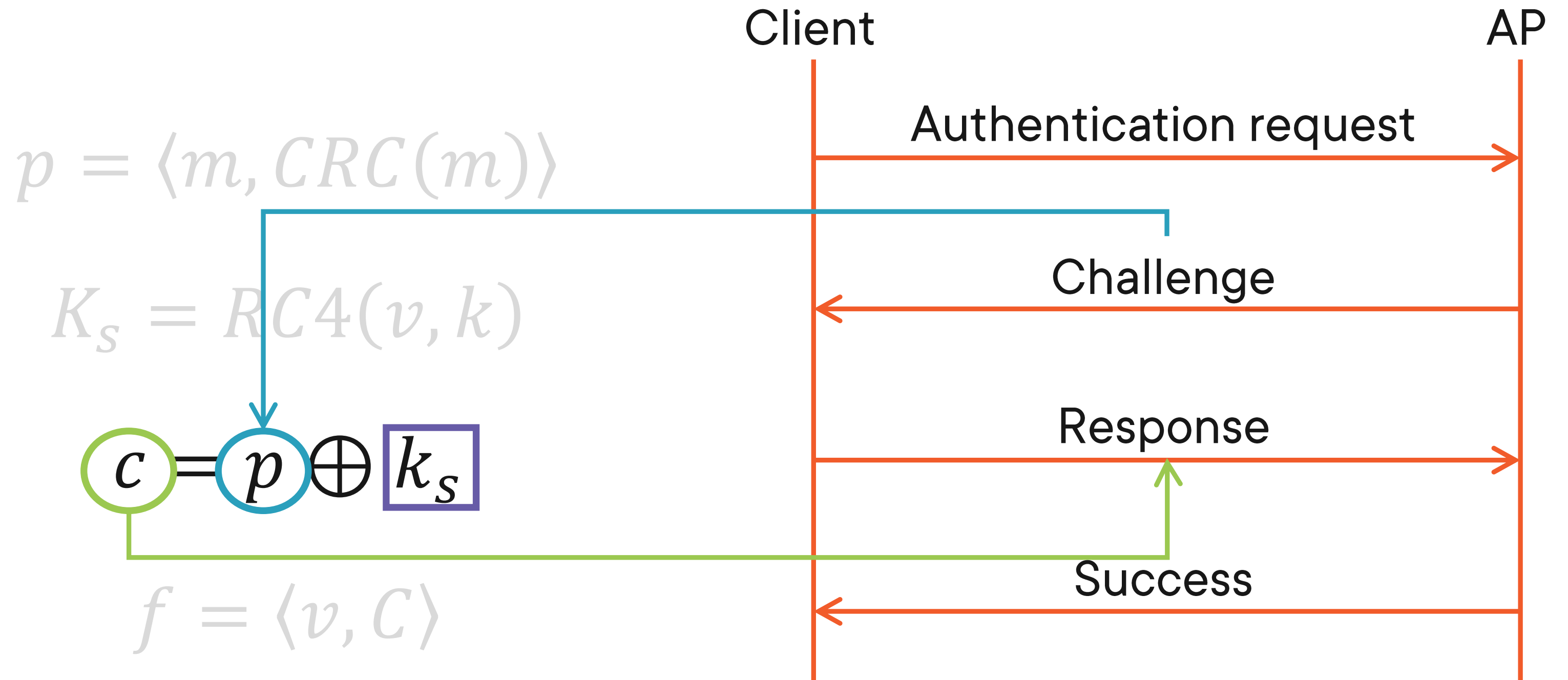
$$K_s = RC4(v, k)$$

$$c = p \oplus k_s$$

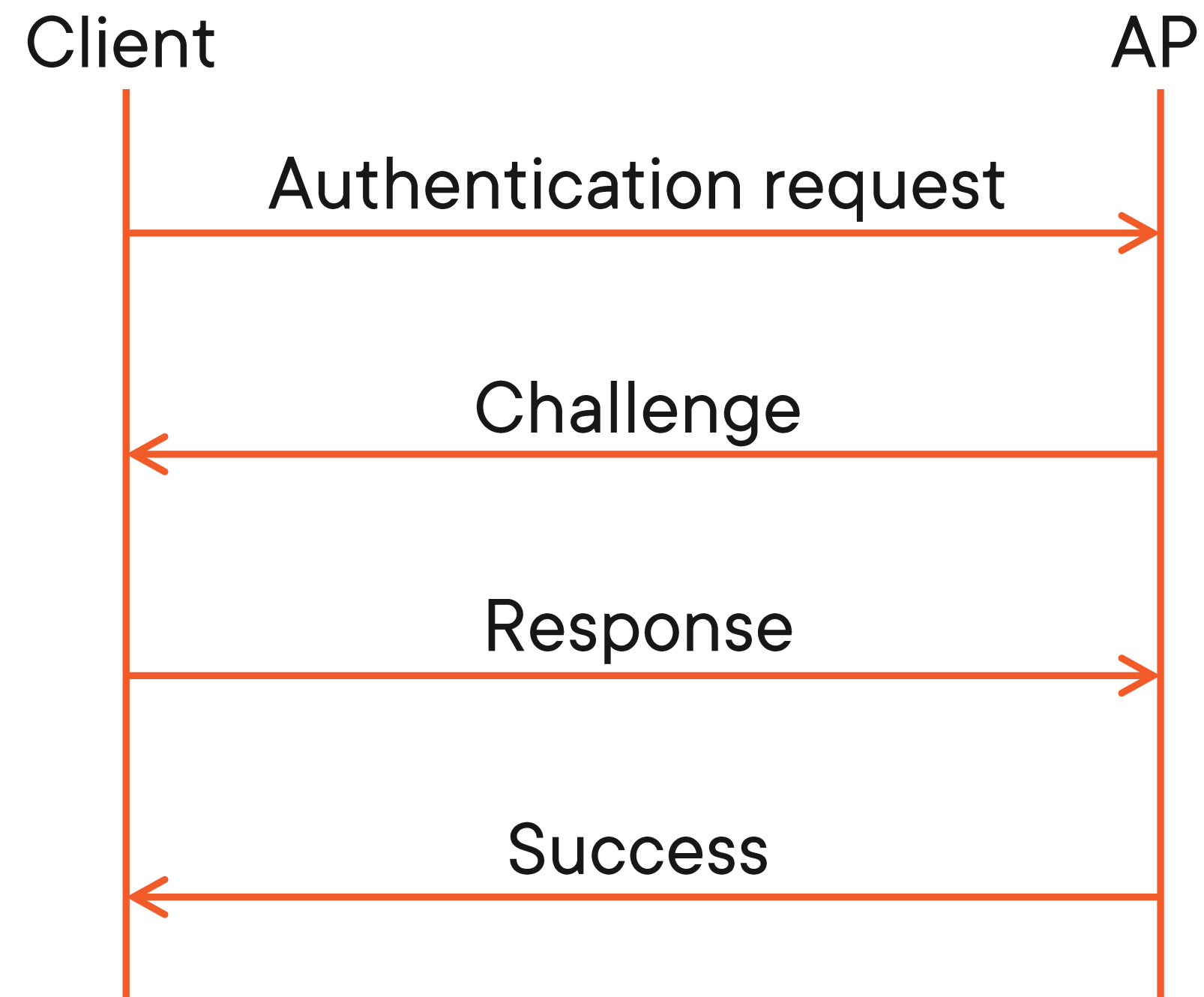
$$f = \langle v, C \rangle$$



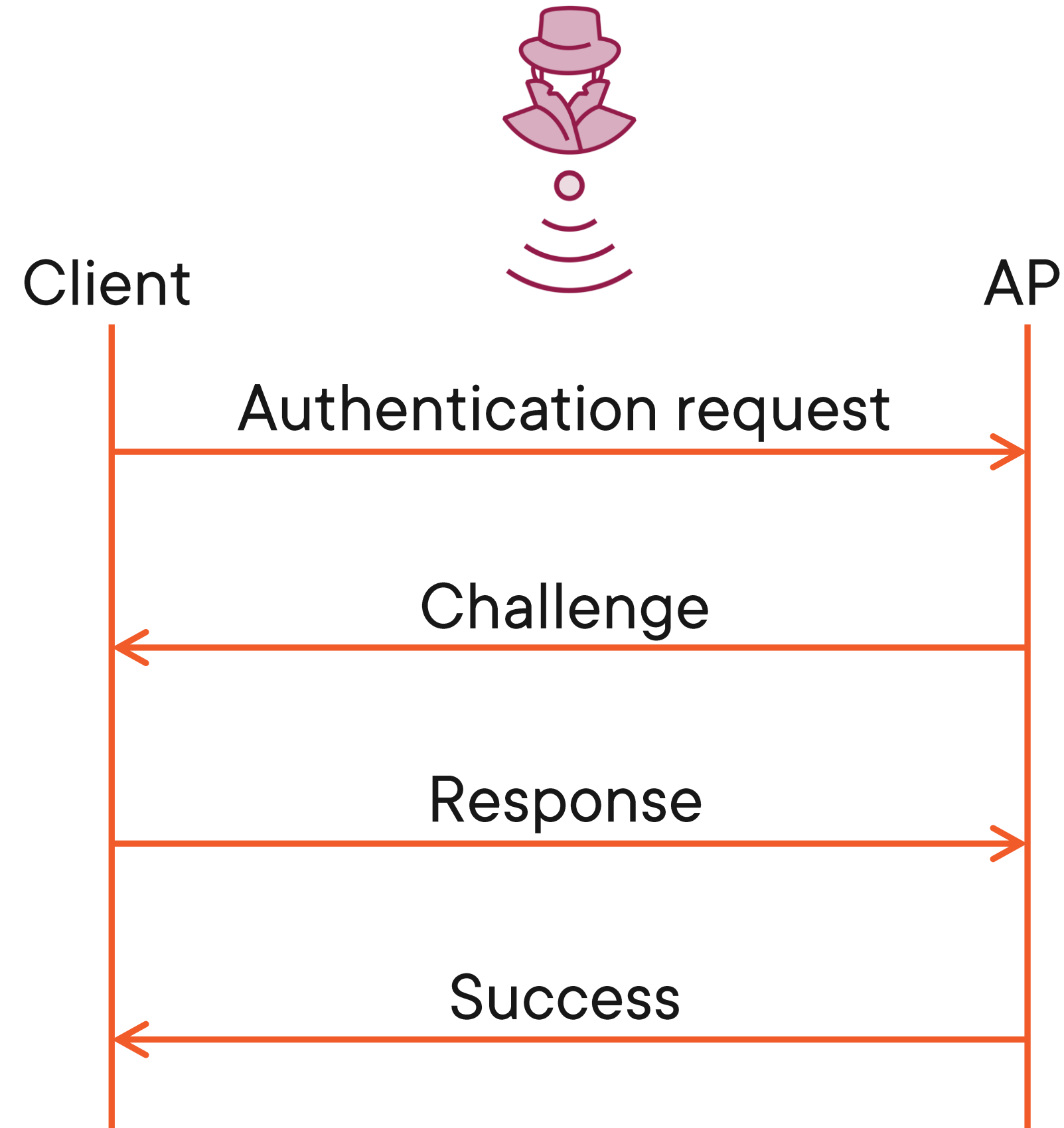
# Shared Key Authentication



# Shared Key Authentication

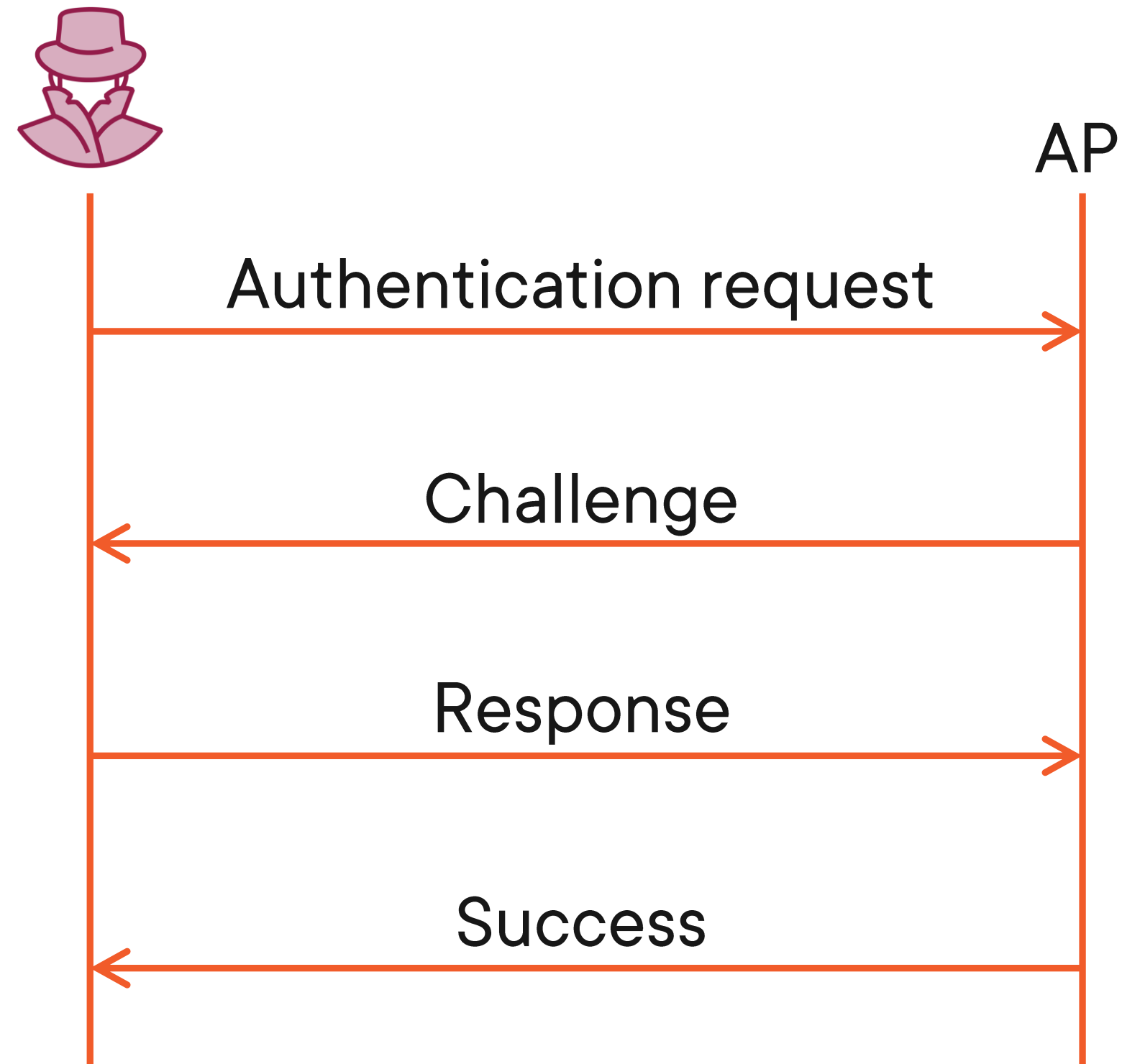


# Shared Key Authentication





# Shared Key Authentication



# Demo



## Bypassing Shared Key Authentication



# Up Next: Cracking Wireless Authentication Keys

---

