1.4

Tuesday, September 19, 2023 5:59 PM

turning power of AP down exposes to evil twin attacks because users may expect to see legit AP at certain spot it no longer reaches

Fully qualified domain name FQDN

Application attack - targets vulns in headers and payloads of specific app protocols

Operational technology attack - network attack that involves connections between embedded system devices man in the browser MitB - compromise browser by installing malicious plug-ins, scripts, or intercepting API calls

HTTP response splitting - attacker crafts malicious URL and convince user to submit to web served

Locally shared objects LSO

flash cookies

data stored on user's pc by site using adobe flash player

may be able to use to track browsing behavior

IV attack - modifies IV of encrypted wireless packet during trans to compute RC4 keystream to

to compute

to compute RC4 keystream
decrypt all other traffic

WPA and WPA2 protect against
this

can combat jam attacks by
boosting signal

DNS server cache poisoning - corrupt
records of DNS server to redirect
traffic

DNS spoofing - compromises name
resolution process; can be used
to facilitate pharming or DoS

ARP poisoning - redirects IP to
with Mac address

ARP (false)

diff Mac address

IP spoofing - attacker sends IP packets from false or spoofed source address

NFC has no encryption

RFID is a means of encoding info into passive tags

Switched port analyzer SPAN/ mirror port

attaches to specificaly configured port on switch that receives copies of frames addressed to other ports

WiPhishing = evil twin