Wireless AKA Progression Cross-Chapter Comparison Sidebar

2,679 words · ~12 min read

---

*Cross-chapter shared reference for `vca-wir-101` Week 4 (802.11 security protocols -- WEP / WPA-PSK / WPA2 / WPA3-SAE / 802.1X) + `vca-rf-301` Ch 4 (RF security primitives -- encryption at RF layer; physical-layer authentication) + `vca-net-201` security module (intermediate-register security cross-cut) + `vca-net-301` Ch 8 (Wireless / 802.11 deep-dive -- 4-way handshake, WPA3-Enterprise) + cross-reference from `vca-sec-101` (wireless-CVE list; KRACK / Dragonblood / FragAttacks). Anchors: Kurose & Ross, *Computer Networking: A Top-Down Approach*, 9th ed., Pearson, 2021 -- §8.8.1 (WPA / WPA2 / WPA3-SAE) + §8.8.2 (5G-AKA, SUCI, IMSI-catcher attack-class). *

Purpose: explicit three-way comparison of three contemporary wireless **Authentication and Key Agreement (AKA)** protocols students encounter at intermediate-to-advanced register -- **WPA2-SAE** (802.11i, 2004), **WPA3-SAE / Dragonfly** (802.11-2020 / WPA3, 2018), and **5G-AKA** (3GPP Rel-15, 2018) -- against a common set of three architectural axes (trust-anchor model, long-term-identity privacy, forward-secrecy and replay-protection mechanism). **Pedagogical thesis:** *the AKA protocols students walk into across the wireless and cellular tracks are not three disconnected designs; they are three points on a single design-evolution arc -- each one is the answer to the attack class that broke the previous one.* When a student reads a KRACK reproduction trace, a Dragonblood timing-side-channel writeup, or a 5G-AKA SUCI capture against an IMSI-catcher, the architectural axes below are what makes each readable as a coherent response to a specific historical failure rather than a flat protocol roster.

Print and pin during `wir-101` Week 4 (802.11 security-protocol introduction), `rf-301` Ch 4 (RF security primitives -- physical-layer authentication), `net-201`'s security module (intermediate-register security cross-cut), and `net-301` Ch 8 (wireless deep-dive -- the 802.11/5G companion framing).

At a glance

Property	Value
Architectures compared	WPA2-SAE (802.11i, 2004), WPA3-SAE / Dragonfly (802.11-2020 / WPA3, 2018), 5G-AKA (3GPP Rel-15, 2018)
Comparison axes	3 (trust-anchor model / long-term-identity privacy / forward-secrecy + replay-protection mechanism)
Primary anchor	Kurose & Ross 9e -- §8.8.1 (WPA / WPA2 / WPA3-SAE) + §8.8.2 (5G-AKA / SUCI / SUPI / IMSI-catcher closure)
Track readers	wir-101 Week 4 (entry-register AP-authentication lens) + rf-301 Ch 4 (signal-side capture-and-replay lens) + net-201 security module (protocol-side AKA-design-rationale lens) + net-301 Ch 8 (control-plane wireless lens; cross-link to CT-B) + sec-101 (CVE-register cross-reference)
Voice family	Petzold-style Architecture Comparison Sidebar (parallels CT-B 5G-Core/SDN/Mobile-IP, RF-301 OFDM/CDMA/TDMA/FHSS/DSSS, NET-301 Snort/Suricata/Zeek, and the canonical CSA-101 ARM/x86/MIPS/RV32I-Lite roster pattern)
Companion sidebar	`handouts/cross-chapter-control-plane-architectures.md` (CT-B; 5G-Core ↔ SDN ↔ Mobile-IP). 5G-AKA appears in both: CT-A reads it as an AKA-progression endpoint; CT-B reads it as a control-plane decomposition expression. The two readings are complementary.

Three AKA protocols -- one-paragraph each

WPA2-SAE (802.11i, 2004). WPA2's authentication-and-key-agreement is the **4-way handshake**, confirmed in IEEE 802.11i in 2004 and the deployed mainstream of enterprise and consumer WiFi for a decade and a half. The pre-shared key (PSK; the network passphrase the user types into the device) is the **trust anchor at both ends** -- AP and station each derive the Pairwise Master Key (PMK) from the PSK independently. Inside the 4-way handshake the AP and station exchange nonces (ANonce + SNonce), derive the Pairwise Transient Key (PTK), confirm the PTK with a MIC-checked message-pair, and install the PTK as the per-session encryption key. Variant **WPA2-Enterprise** replaces the PSK trust anchor with an EAP-driven RADIUS exchange (EAP-TLS most prominently), but the handshake-and-key-derivation skeleton is unchanged. 9e §8.8.1 anchor.

WPA3-SAE (Dragonfly handshake; 802.11-2020 / WPA3, 2018). WPA3's authentication-and-key-agreement is **Simultaneous Authentication of Equals (SAE)** built on the **Dragonfly password-authenticated key exchange (PAKE)** primitive (RFC 7664; IETF 2015). The trust anchor is still the network passphrase -- but Dragonfly's PAKE construction means *the passphrase is never transmitted, never derivable from the captured handshake, and never susceptible to the offline-dictionary attack class that broke WPA2's PSK story.* Each side commits to its passphrase-derived element first; only after the commit-pair does the key-derivation proceed; and a captured Dragonfly handshake is provably useless to an offline attacker who does not already know the passphrase. WPA3 also bakes in **forward secrecy by design** -- a captured-and-cracked handshake from session N does not compromise sessions N−1 or N+1 even if the passphrase is later disclosed. 9e §8.8.1 anchor (WPA3 extensions section).

5G-AKA (3GPP Rel-15, 2018; cellular-AKA endpoint). 5G-AKA is the cellular-track endpoint of this design-evolution arc. The trust anchor is **not at the device's edge** -- it lives **inside the operator's home network**, in the **Unified Data Management (UDM)** function and the **Authentication Server Function (AUSF)**. The long-term subscriber key (the "K" in the 3GPP AKA family -- historically the Ki of GSM, the K of UMTS-AKA, the K of EPS-AKA in 4G, and now the K of 5G-AKA) is provisioned into the SIM/USIM/eSIM at manufacture and into the home-network UDM at subscriber activation; **the network and the subscriber share a long-term secret that the UE itself never has to send over the air.** 5G-AKA's challenge-response runs on top of this shared secret with home-network sequence-number tracking (SQN) to defeat replay. The architectural break with 4G/3G/2G AKA is **SUCI / SUPI separation:** the 5G UE never transmits its long-term identity (SUPI ≈ IMSI in legacy AKA) in the clear -- it transmits the **SUCI**, an ECIES-encrypted form of the SUPI that only the home network can decrypt -- closing the IMSI-catcher attack class that defined cellular AKA's vulnerability surface for thirty years. 9e §8.8.2 anchor.

Three comparison axes

Axis 1 -- Trust anchor / authentication root

Architecture	Trust anchor	Where it lives
WPA2-SAE	**Pre-shared key (PSK)** derived from the network passphrase	At AP and at station -- both endpoints hold the PSK directly
WPA3-SAE	**Same PSK** -- but the Dragonfly PAKE means the PSK is never transmitted, never derivable from a captured handshake, and never offline-dictionary-attackable	At AP and at station -- same physical locus as WPA2; the cryptographic construction is what changes
5G-AKA	**Long-term subscriber key (K)** provisioned into SIM/USIM/eSIM at manufacture	At the **home network's UDM/AUSF** + at the SIM -- *not at the visited network*; the visited network never sees K

Reading the axis. All three protocols share the same architectural shape -- a long-term secret known to two parties drives a per-session key derivation -- but the *locus* of the long-term secret tells a story. WPA2 and WPA3 keep the secret at the network's physical edge (the AP or the EAP server); the visited-vs-home distinction does not exist for residential or enterprise WiFi. 5G inherits that distinction from cellular roaming: because a 5G UE may attach to a visited network thousands of kilometres from home, the trust anchor must live with the home network and the per-session derivation must work *via* the visited network without disclosing K to it. The WiFi-to-cellular AKA-design jump is structurally driven by this roaming requirement; everything else in 5G-AKA's complexity follows from it.

Axis 2 -- Long-term-identity privacy

Architecture	Long-term identity exposure	Attack class addressed
WPA2-SAE	**AP MAC + station MAC visible in every frame** (no privacy of long-term identity at the AKA layer)	None -- privacy not a design goal at the 802.11i layer; randomised-MAC arrived later as an OS-side feature
WPA3-SAE	**Same** -- AP MAC + station MAC visible (the WPA3 privacy improvements live in **OWE / Opportunistic Wireless Encryption** for open networks, not in the SAE handshake itself)	None directly; the privacy story for open-network WiFi is parallel to the WPA3-SAE story
5G-AKA	**SUCI = ECIES(SUPI)** -- the long-term identity (SUPI ≈ IMSI) is never transmitted in the clear; only the home-network UDM holds the private key to decrypt SUCI back to SUPI	**IMSI-catcher attack class** -- the thirty-year cellular vulnerability where any party with a fake-base-station could harvest IMSIs by triggering Identity-Request frames

Reading the axis. This is the axis where the WiFi family and the cellular family diverge most sharply. WPA2 and WPA3 do not address long-term-identity privacy at the AKA layer at all -- and arguably do not need to, because a residential or enterprise WiFi AP is a known fixed party in a small-scale deployment context where MAC visibility is not the dominant attack surface. Cellular's threat model is the inverse: the UE attaches to whatever base station the radio finds, the operator cannot know in advance which base stations are real and which are fake-base-station IMSI-catchers, and the long-term identity (IMSI / SUPI) is the durable subscriber-identifying key whose disclosure enables long-term tracking. 5G-AKA's SUCI-over-the-air design directly closes this attack class -- the *exact* IMSI-catcher attack class that defined the cellular-AKA threat model from GSM forward. Pedagogical lesson: the design choices are not architectural taste; they are responses to specific named attack classes against specific deployment-context threat models.

Axis 3 -- Forward secrecy + replay-protection mechanism

Architecture	Forward-secrecy story	Replay-protection mechanism
WPA2-SAE	**None by default** -- the PMK is derived from the static PSK; once an attacker recovers the PSK (offline-dictionary attack against captured handshakes is the dominant pathway), all past and future sessions are compromised	**Per-message nonces (ANonce + SNonce)** -- but the **KRACK** attack class (Vanhoef + Piessens, 2017) showed that nonce-reuse in the 4-way handshake's message-3 retransmission path was the door to full key-stream recovery; widely-deployed implementations were vulnerable until coordinated patching
WPA3-SAE	**Forward secrecy by design** -- Dragonfly's PAKE construction means each session's key is independent of the long-term passphrase; passphrase recovery does not retroactively compromise past or future sessions	**Per-handshake commit nonces** -- the Dragonblood attack class (Vanhoef + Ronen, 2019) demonstrated timing and side-channel weaknesses in early WPA3-SAE implementations, all of which were addressable in implementation rather than requiring protocol redesign
5G-AKA	**Forward secrecy depends on operator implementation** -- the long-term key K does not directly derive per-session keys (per-session keys come from K + RAND + SQN through the AKA challenge-response), so K-disclosure does not retroactively decrypt past sessions, *but* a compromised K compromises future session-establishment	**Sequence numbers (SQN) tracked at home-network UDM** -- replay-protection follows from SQN monotonicity; the residual concern is **downgrade attacks** (forced fallback to legacy AKA generations with weaker properties), and 3GPP working-group countermeasures against downgrade are an active area

Reading the axis. This is the axis where the AKA-progression story is most visible as a *story.* WPA2's no-forward-secrecy story is what made KRACK so consequential -- the protocol design and the implementation bug compounded. WPA3's forward-secrecy-by-design story is the protocol-design response to that compound failure. 5G-AKA's SQN-based replay-protection inherits a thirty-year cellular tradition (SQN tracking goes back to UMTS-AKA in the early 2000s) and applies it to a home-network-anchored trust model rather than a device-anchored one. Three protocols, three different forward-secrecy and replay stories -- each one a response to the threats the previous design left unaddressed.

Cross-track pedagogy notes

wir-101 Week 4 -- entry-register AP-authentication lens. The wireless-pentesting register reads this AKA-progression as a *story of increasingly-sophisticated attack surfaces driving protocol redesign.* WIR-101 students arrive having just completed Week 3's site survey; Week 4 is where they learn that "what security mode is this network in?" is a question with a deep technical lineage. The pedagogical move at this level is to walk WPA2 → WPA3 → 5G-AKA as a *historical* progression, surfacing the named attacks (KRACK, Dragonblood, IMSI-catcher) as the *driving force* behind each protocol redesign. By the end of Week 5's hashcat-against-WPA2 lab, students should be able to articulate why the same lab is structurally impossible against a properly-implemented WPA3-SAE network and structurally inapplicable to a 5G-AKA exchange -- and *why* each next-generation protocol's attack surface is qualitatively different from the previous one's.

rf-301 Ch 4 -- signal-side / capture-and-replay lens. The advanced-RF register reads this AKA-progression *from the radio outward.* Each protocol presents a different capture-side opportunity: WPA2's 4-way handshake is the canonical capture target (KRACK demos, hashcat-against-PMK pipeline); WPA3-SAE's Dragonfly commit-pair is the timing-and-side-channel target (Dragonblood demos); 5G-AKA's NAS Identity-Response and SUCI computation are the cellular-baseband side-channel targets (recall that 9e §8.8.2 names this class explicitly). The RF-track-register move is to read each protocol as a *signal artifact first* -- what does the capture look like, what fingerprints distinguish each handshake on the air, and where are the implementation side-channels that real-world attacks exploit?

net-201 security module -- protocol-side AKA-design-rationale lens. The intermediate-NET register reads this AKA-progression *from the protocol design outward.* NET-201's security-module register is where students first see AKA as *a class of protocols* rather than *one protocol*; the cross-track sidebar makes the protocol-design rationale explicit (why PAKE? why home-network anchoring? why SUCI?). This is also the right register to surface the cryptographic-primitive choices: HMAC-SHA1 in WPA2, ECC + Dragonfly PAKE in WPA3-SAE, ECIES + per-operator EC parameters in 5G-AKA's SUCI computation. Students who internalise the primitive-choice rationale here transfer the reading skill directly to TLS 1.2/1.3/QUIC-TLS, which lives in Ch 4 of net-201's primary curriculum.

net-301 Ch 8 -- control-plane wireless lens; cross-link to CT-B. The advanced-NET register reads this AKA-progression *together with* the control-plane-architecture comparison from CT-B. The 5G-AKA endpoint is where CT-A and CT-B meet: 5G-AKA is the AKA-progression endpoint *and* the 5G-Core control-plane authentication function.

The pedagogy at NET-301 register is to read the two sidebars in concert -- students who hold both side-by-side see that 5G-AKA's home-network anchoring (CT-A Axis 1) is what *enables* the 5G-Core's UDM/AUSF decomposition (CT-B Axis 1); the two architectural decisions are joint, not independent.

sec-101 -- CVE-register cross-reference. SEC-101 already names KRACK / Dragonblood / FragAttacks as canonical 802.11 CVE records (line 302 of `vca-sec-101.html`); CT-A is the cross-track sidebar that contextualises those CVEs *as protocol-design responses* rather than *as flat vulnerability records.* SEC-101's CVE-walk catalog pairs naturally with CT-A's protocol-progression register; students who hold both see that "read the CVE record" and "read the protocol-design rationale" are the two halves of the same skill.

Anchor citations

- **Primary.** Kurose & Ross, *Computer Networking: A Top-Down Approach*, 9th ed., Pearson, 2021. §8.8.1 (WPA / WPA2 / WPA3-SAE -- the 9e expansion of the wireless-AKA story); §8.8.2 (5G-AKA, SUCI / SUPI, IMSI-catcher attack-class closure -- new in 9e).
- **Secondary -- wireless side.** IEEE 802.11i-2004 (WPA2 4-way handshake; normative). IEEE 802.11-2020 (WPA3 / Dragonfly SAE; normative). RFC 7664 (Dragonfly PAKE; IETF reference for the SAE primitive). Vanhoef & Piessens, *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*, ACM CCS 2017 (KRACK canonical). Vanhoef & Ronen, *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd*, IEEE S&P 2020.
- **Secondary -- cellular side.** 3GPP TS 33.501 (5G security architecture; SUCI / SUPI / 5G-AKA normative). 3GPP TS 33.402 (non-3GPP access; 5G-AKA-prime variant for WiFi-to-5G-Core integration; mentioned as cross-link only). 3GPP TS 23.501 (5G system architecture; UDM / AUSF roster -- see CT-B for the control-plane decomposition reading).
- **Cross-references.** OpenAirInterface community docs for 5G-AKA hands-on (rf-301 Ch 5 lab substrate; net-301 Ch 8 cross-cut). aircrack-ng + hashcat documentation for WPA2-SAE attack reproduction (wir-101 Lab 5 substrate). Wireshark 802.11 dissector documentation for handshake-byte annotation (wir-101 Lab 4 + net-301 Lab 10 substrate).

Cross-references

Picks up at	Chapter / module	Purpose
`vca-wir-101.html`	Week 4 (802.11 security protocols -- WEP / WPA-PSK / WPA2 / WPA3-SAE / 802.1X)	Entry-register AP-authentication weave; sidebar slot anchor in the Foundational Anchor Weaves section
`vca-rf-301.html`	Ch 4 (RF security primitives -- encryption at RF layer; physical-layer authentication)	Signal-side capture-and-replay lens; sidebar slot anchor in the Architecture Comparison Sidebars section
`vca-net-201.html`	Security module (intermediate-register security cross-cut)	Protocol-side AKA-design-rationale lens; sidebar slot anchor in the Architecture Comparison Sidebars section
`vca-net-301.html`	Ch 8 (Wireless / 802.11 deep-dive -- 4-way handshake, WPA3-Enterprise)	Advanced control-plane wireless lens; sidebar slot anchor in the Architecture Comparison Sidebars section; cross-link to CT-B for the joint AKA-and-control-plane reading
`vca-sec-101.html`	Per-course skill-transfer roster (wireless-CVE list; KRACK / Dragonblood / FragAttacks)	"▶ See also" cross-reference pointer; CT-A contextualises the wireless CVEs SEC-101 names as protocol-design responses
`handouts/cross-chapter-control-plane-architectures.md` (CT-B)	Companion sidebar	Joint reading: 5G-AKA appears in both -- CT-A reads it as AKA-progression endpoint; CT-B reads it as control-plane decomposition expression

---

Pedagogical note -- the AKA-progression arc as a Petzold-style design-evolution case study

The three protocols compared above form a textbook case of *protocol-evolution-driven-by-attack-surface-discovery* -- the same compare-N-implementations-of-one-architectural-pattern shape that the canonical Petzold ARM/x86/MIPS/RV32I-Lite sidebar uses to teach instruction-set-architecture design choices. WPA2-SAE was the protocol that worked for fifteen years; KRACK was the attack class that broke it; WPA3-SAE was the design response. Cellular AKA evolved on a parallel track from GSM through UMTS

through EPS-AKA (4G) to 5G-AKA, with IMSI-catcher attacks as the analogous driving attack class and SUCI as the analogous design response. By teaching the three protocols *together* -- across the wireless-track, RF-track, NET-track, and cross-referenced from the security-fundamentals track -- students see *protocol evolution as a discipline*, not as a flat history. That is the load-bearing pedagogical move CT-A enables; the per-track readings above are the registers in which the move takes place.

Companion: `cross-chapter-control-plane-architectures.md` (CT-B; 5G-Core, SDN, Mobile-IP). Both handouts implement the same Architecture Comparison Sidebar pattern.
