English

Connecting the Dots: Technical Analysis of the KT Femtocell Incident

Introduction

In September 2025, a micropayment fraud incident targeting KT subscribers revealed what appears to be large-scale eavesdropping infrastructure. This analysis synthesizes publicly available information from Korean government investigations, security research, and media reports.

***Key facts**: 368 victims, ~$180K USD in micropayment fraud, 22,227 devices connected to illegal femtocells, 20 femtocell IDs identified. One femtocell operated 305 days across multiple provinces with zero micropayment activity.*

1. Attack Vector: Femtocell Exploitation

2014 KAIST Research

KAIST researchers demonstrated femtocell compromise feasibility in 2014. They gained root access to commercial femtocells and converted them to mobile eavesdropping devices. At that time, SMS and voice lacked end-to-end encryption-all traffic was plaintext at the femtocell layer.

September 2025 Incident

Arrested suspects (Chinese nationals working as day laborers in Korea) used Chinese femtocells with portable routers, driving around Seoul and Gyeonggi. Victim devices auto-connected, enabling real-time SMS authentication code interception.

***Anomaly**: Femtocell #6 operated 305 days (October 2024 - August 2025) across four provinces, sometimes visiting 11 locations daily, with zero micropayment fraud.*

2. Security Architecture Post-2014

Carriers implemented end-to-end encryption after 2014:

***SMS**: Two methods in use*

- *SMS over IMS (KT, LG U+): PDCP/RRC encryption (radio) → IPsec (backhaul) → IMS E2E encryption (core)*

- *SMS over NAS (SKT): NAS encryption → IPsec → NAS E2E encryption*

  ** Note: E2E encryption refers to encryption 1) between IMS and UE for SMS over IMS or 2) between Core and UE for SMS over NAS.*

***VoLTE**:*

- *Signaling: End-to-end encrypted*
- *RTP voice stream: **Not encrypted** (PDCP encryption only in radio section, plaintext inside femtocell)*

With proper implementation, compromised femtocells should only see encrypted SMS. VoLTE calls remain vulnerable to eavesdropping.

3. How the Attack Succeeded

MSIT Finding: Active Attack

IMS registration security negotiation lacks authentication. Compromised femtocells can manipulate sec-agree fields to downgrade encryption:

- *Device sends: "encryption supported"*
- *Femtocell modifies to: "encryption not supported"*
- *IMS server accepts, all subsequent SMS transmit in plaintext*

NIS Finding: Encryption Disabled by Carrier

More critically, NIS reported KT disabled encryption on certain smartphone models. Security researcher perillamint confirmed this with screenshots comparing Xiaomi Redmi S2 settings: encryption active on Vodafone Portugal, disabled on KT.

***Conclusion**: Victim devices either had KT-disabled encryption or suffered active downgrade attacks. Both scenarios result in plaintext SMS visible at femtocell layer.*

4. Incident Reconstruction

Suspect Profile Inconsistency

Arrested suspects: Chinese day laborers, no technical knowledge, one couldn't speak Korean. Yet micropayment fraud requires real-time coordination of victim data entry and authentication code capture. Profile doesn't match capability requirements.

Inferred Infrastructure

If routers were included with femtocells (police mentioned portable internet routers/"eggs"), the attack architecture becomes clear:

Device → Femtocell → Router → Egg → Foreign Server → VPN → Domestic IP → KT Gateway

Router manipulation enables all traffic redirection to foreign servers. VPN exit via Korean domestic IPs bypasses foreign IP detection. Foreign server capabilities:

1. ***Passive sniffing**: Copy all passing packets (SMS, VoLTE RTP streams, data traffic)*
2. ***Active injection**: Manipulate IMS registration messages to disable encryption*

Arrested individuals were carriers-transport equipment, keep powered on. Backend automation handles everything else.

Single Authentication Key Vulnerability

MSIT investigation revealed KT used one authentication key for 157,000 femtocells. Theori's analysis showed pre-patch femtocells had:

- *No root password*
- *SSH enabled by default*
- *Certificates and keys stored in plaintext*

Anyone obtaining one KT femtocell could extract authentication keys and create unlimited virtual femtocells (cellID is software-configurable).

Scale Hypothesis

The 20 identified femtocell IDs represent software identifiers, not necessarily physical device count. With one authentication key, hundreds of physical devices could create thousands of virtual femtocells distributed nationwide, all feeding data to a central foreign server.

The 305-Day Question

Femtocell #6 operated 305 days without micropayment fraud. More critically, KT logs only exist from August 1, 2024. The prior period (2016-July 2024, ~8 years) is a complete blank. Unknown how many illegal femtocells operated during this time.

***Rational inference**: Micropayment fraud was not the primary objective. Large-scale data collection was. Someone's greed exposed the operation. Without micropayment fraud, the infrastructure likely would remain undetected.*

5. KT's Emergency Patch Analysis

Post-incident patches (per Theori analysis):

- *Certificate validity: 10 years → 1 month*
- *Private keys: Now encrypted in storage*
- *Serial console: Blocked*
- *SSH: Access restricted*
- *Disabled encryption on certain models: Corrected*

Fundamental Limitations

Critical issue: Private keys encrypted in firmware, but decryption program included in same firmware. Reverse engineering remains feasible.

Effective protection requires hardware security modules (HSM/TPM). Current software-only approach cannot prevent determined attackers with physical access from gaining root privileges.

Attacks Still Feasible with Rooted Femtocells

Femtocell architecture necessitates plaintext processing internally:

1. *PDCP decryption of radio traffic*
2. *Plaintext processing*
3. *GTP-U encapsulation for core network*

Rooted femtocells enable:

- *VoLTE eavesdropping (RTP streams unencrypted)*
- *IMS message manipulation (protocol design flaw, unfixable via femtocell patches)*
- *Device information collection (IMSI, IMEI, phone numbers, connection logs)*

The Section 4 infrastructure scenario remains technically feasible post-patch.

6. Implications for Global Telecommunications

Femtocell-based eavesdropping infrastructure is operational, not theoretical. Vulnerabilities are structural.

Carriers should assess:

- ***Rooting vulnerability**: Verify femtocells resist root access exploitation (HSM/TPM implementation, not software-only key protection)*
- ***Passive sniffing**: VoLTE RTP plaintext accessibility, SMS E2E enforcement, metadata leakage*
- ***Active attacks**: IMS registration downgrade, control plane message authentication*

- ***Detection gap****: Real-time unauthorized femtocell detection capability required to counter potential rooting exploits.*

Critical*: Without micropayment fraud, this infrastructure would remain undetected. Assess whether similar operations currently exist undetected on your network.*

Analysis based on publicly available information from Korean government investigations (MSIT, NIS, National Assembly), security research (Theori, KAIST 2014), and media reports. Technical vulnerabilities discussed apply to femtocell deployments globally.