Universidad de Oviedo

Informática Forense y Auditoría

Grado en Ingeniería Informática del Software
Escuela de Ing. Informática de Oviedo
Universidad de Oviedo

Aspectos básicos de trazabilidad en redes de comunicaciones móviles

Universidad de Oviedo (Escuela de Ingeniería Informática)

Grado en Ingeniería Informática del Software

Informática Forense y Auditoría (curso 2023/2024)

Profesor: Alberto Antonio Núñez Oliveira

(Departamento de Informática, Área de Lenguajes y Sistemas Informáticos)

Arquitectura y acceso

- Una red de comunicaciones móviles, actualmente coexisten en servicio tecnologías 2G, 3G, 4G y 5G, se instancia y manifiesta, en el segmento de acceso y con independencia del estándar xG concreto, mediante células. Una célula es una entidad radioeléctrica, voluminosa, contenida estrictamente en un paralelepípedo y abstraída en señalización y control, mediante un plano de gestión, por un set de descriptores que contiene varios cientos de parámetros. Habitualmente, una célula se representa proyectada en un plano como una superficie de su área de cobertura.

- Las redes pueden ser públicas o privadas, físicas o virtuales, e incluso pueden incluir slices de comunicaciones fijas o para ciertas aplicaciones, lo que supone distintas consideraciones en términos de características del servicio y trazabilidad. En todo caso, el soporte a la movilidad se implementa mediante una intersección efectiva en el área de cobertura de las distintas células, varios miles para una región como Asturias y un proveedor de escala, que componen la red en cuestión.

- Los distintos estándares xG se integran funcionalmente en la misma red y ofrecen el soporte necesario a los terminales compatibles. En el corto plazo, previsiblemente antes de 2024, 3G se apagará, 2G se relegará a M2M (IoT) y telefonía pública legacy y serán 4G y 5G quienes absorberán la mayor parte del tráfico.

Tecnologías y estándares xG

- Las tecnologías y estándares xG se establecen según las sucesivas generaciones que son objeto de especificación: hasta el momento, se incluyen 1G, 2G, 3G, 4G y 5G, con 1G fuera de servicio y el resto todavía desplegadas en redes comerciales y en servicio.

- En realidad, cada estándar xG es, a su vez, un conjunto de estándares relativos a distintos aspectos técnicos y tecnológicos de la correspondiente generación. La simplificación más habitual es identificar una generación con sus principales estándares y tecnologías de acceso: 2G (GSM y CDMA); 3G (UMTS y CDMA-2000); 4G (LTE); 5G (NR).

- Los estándares de acceso y la regulación en bandas de frecuencia de cada país impactan directamente en la operatividad internacional completa de un terminal móvil haciéndola inviable. Hasta la llegada de 4G, América del Norte y Europa, por ejemplo, utilizaban distintos estándares (2G/CDMA y 2G/GSM - 3G/CDMA-2000 y 3G/UMTS, respectivamente). A partir de 4G los estándares de acceso son de aplicación mundial pero persiste la fragmentación en bandas de frecuencia imposibilitando, por limitaciones de implementación electrónica, la portabilidad internacional completa de terminales.

Dispositivos terminales

- Un terminal móvil es todo aquel provisto de al menos un interfaz xG con aplicación a comunicaciones entre máquinas o personas en cualquier combinación: smartphone, featurephone –teléfonos móviles anteriores al smartphone-, modem, router, tablet, etc.

- En todos los casos, el terminal se asocia a una SIM (Suscriber Identification Module), física o virtual –implementada electrónicamente en el dispositivo y provisionada online-, que soporta y hace efectivo el correspondiente servicio en relación al proveedor del mismo.

- Un terminal incorpora, en el ámbito de la conectividad móvil, unas especificaciones concretas que determinan, entre otras cosas, los interfaces xG integrados y la categoría del servicio soportada para cada uno de ellos.

- La combinación de los registros de la SIM, las especificaciones y categoría del terminal y la suscripción o servicio adquirido con el proveedor, determinarán las posibilidades reales del servicio de una línea móvil.

Dinámica del servicio

- Un terminal móvil, con el servicio activado, admitirá dos estados posibles que no resultan excluyentes sino complementarios: Idle (registrado en la red); Dedicated (registrado y utilizando la red en términos de comunicaciones efectivas). En cualquiera de los dos estados, el dispositivo tendrá conectividad con al menos una célula de la red. A partir de 3G, que incorporó efectivamente la banda ancha móvil, los smartphones, con interfaces activas 3G o superior, suelen estar permanentemente en modo Dedicated (always on).

- La conectividad se establece en dos planos distintos: Plano de Control (señalización) y Plano de Usuario (voz y datos que categorizan por agregación todos los tipos de tráfico posibles).

- El soporte a la movilidad se consigue mediante los procesos de reselección y handover (traspaso) en los que, a través de los planos de conectividad y el solapamiento de las áreas de cobertura, se hace efectivo el cambio de células de servicio en los posibles estados del dispositivo.

- El proveedor del servicio incorpora, en la infraestructura de la red, la arquitectura FrontEnd y BackEnd necesaria para hacer efectivo el servicio y registrar todos los eventos asociados a una línea móvil.

Descriptores de trazabilidad I

- **CGI** (Cell Global Identity): identificador internacional único para una célula de una red móvil. Está compuesto de un número variable (debido a los nuevos estándares xG) de dígitos decimales. Está formado por la concatenación de 4 campos (MCC y MNC cinco primeros dígitos):
  - **MCC** (Mobile Country Code): identificador internacional único para cada país que posea redes de comunicaciones móviles.
  - **MNC** (Mobile Network Code): identificador nacional único para cada proveedor que preste servicios de comunicaciones móviles en un determinado país.
  - **LAC** (Location Area Code): fijados MCC y MNC, identifica un cluster de células, compacto geográficamente, que facilita el networking en los Planos de Control y Usuario de la red.
  - **CI** (Cell Identification): fijados MCC, MNC y LAC, identifica de forma única una célula de acceso.

- Ejemplo de CGI: 214 (MCC) + 07 (MNC) + 2418 (LAC) + 14264 (CI)

Descriptores de trazabilidad II

- **IMEI** (International Mobile Equipment Identity): identificador internacional único, compuesto de 15 dígitos decimales, para un terminal móvil. Los terminales incluyen también otras numeraciones de fábrica, direcciones de interfaces de red, etc. Se podría identificar cierto paralelismo entre el IMEI y la dirección MAC de una tarjeta de red Ethernet.

- Los fabricantes y proveedores de servicio comparten IMEIs para facilitar la trazabilidad de terminales y permitir su eventual inclusión en Black Lists, sujetas a variabilidad regulatoria, que potencialmente podrían inhabilitar el servicio efectivo del terminal.

- Ejemplo de IMEI: 862551036005121

Descriptores de trazabilidad III

- **IMSI** (International Mobile Subscriber Identity): identificador internacional único para una línea móvil, guarda relación con la SIM, admite portabilidad entre distintos terminales móviles y, dependiendo del servicio suscrito o adquirido con el proveedor, puede incluir operatividad internacional.

- El IMSI se compone de tres campos: MCC y MNC con el mismo significado y asignaciones que para el CGI y el MSIN (Mobile Subscriber Identification Number) que resulta ser el número ordinario de línea con pleno significado y portabilidad en un ámbito regulatorio concreto como puede ser un país, además, si corresponde, se integrará en formato de numeración internacional para soportar la correspondiente operatividad.

- Ejemplo de IMSI: 214 (MCC) + 07 (MNC) + 999999999 (MSIN)

Descriptores de trazabilidad IV

- **ICC** (International Circuit Card): identificador internacional único para una SIM física o virtual, se compone de 19 dígitos decimales: los dos primeros siempre se registran como 89; los dos siguientes identifican el país del proveedor de servicio según el código internacional de telefonía pública (por ejemplo, 34 para el caso de España); los dos siguientes el código del proveedor de servicio en el país en cuestión –el MNC del CGI con idéntico significado y asignación-; el resto identificarán, de forma única, una determinada SIM dentro de un proveedor de servicio concreto.

- La mayor parte de los proveedores de servicio ofrecen paquetes comerciales multi SIM. En ese caso, una misma línea móvil (IMSI) puede incluir varios ICCs –uno sería el principal y el resto secundarios-: potencialmente, varios terminales móviles (IMEIs) pueden cursar en tráfico, y en general actuar en movilidad, en distintas localizaciones, de ámbito nacional o internacional, al mismo tiempo.

- Ejemplo de ICC: 89 + 34 (código telefónico internacional del país) + 07 (MNC) + 9999999999999 (ICCID)

Características de trazabilidad I

- Un IMSI y el ICC o ICCs que se hayan provisionado para el mismo, está asociado, de forma exclusiva, con un proveedor/país home (de origen): proveedor/país donde se suscribe o adquiere el servicio (prepago o pospago).

- El servicio suscrito o adquirido puede incluir roaming (itinerancia): posibilidad de que un IMSI se utilice, al margen del proveedor/país home, con distinto proveedor en el país home (roaming nacional) e incluso con otros proveedores en distintos países (roaming internacional), todo ello sujeto a los acuerdos comerciales y obligaciones regulatorias del proveedor home.

- A efectos forenses, el servicio, según las correspondientes aplicaciones, admite dos categorías: Carrier Class (CC), por ejemplo la telefonía pública convencional, SMS/MMS etc., que está regulada en el país home; Over The Top (OTT), por ejemplo mensajería de terceras partes, navegación web, etc., que tendrá variabilidad regulatoria, implicando, en ciertos casos, ámbitos o escenarios internacionales.

Características de trazabilidad II

- Es habitual que los proveedores de servicio deban entregar a instancias judiciales los registros de comunicaciones y posicionales de un IMSI/IMEI/ICC relacionado con alguna investigación.
- En general, se tratará de archivos con datos en crudo que incluirán, entre otras cosas, los CGIs e IMEIs, quizá los ICCs, implicados junto con referencias posicionales, más o menos precisas, y también fechas y horas locales.
- Las referencias posicionales se derivarán de la siguiente combinación: ubicación registrada por el proveedor para la infraestructura de acceso o estación base a la que pertenece la célula en cuestión; distancia estimada, en función del networking del Plano de Control, entre la célula y el terminal móvil.

Características de trazabilidad III

- Cualquier red móvil, al igual que la mayor parte de las redes de comunicaciones actuales, se ajusta al estándar IP-CAN (Internet Protocol-Capable Access Network); una investigación forense admite, al margen de procesos o herramientas específicas de comunicaciones móviles, técnicas y tecnologías tradicionales para Network Forensics.

- El servicio con categoría OTT es, según lo anterior, potencialmente inspeccionable extremo a extremo (IP-Bearer) pues estaría integrado en Internet como red pública y expuesto a la correspondiente variabilidad regulatoria.

- El servicio con categoría CC está implantando sobre redes IP aisladas de Internet y sujeto a la correspondiente regulación de cada país (alternativamente de organizaciones supranacionales como la Unión Europea), incluyendo la obligación de que el proveedor de servicio almacene registros durante cierto tiempo; admitirá una aplicación singular de técnicas y tecnologías tradicionales en Network Forensics.

Enlaces de interés

- 3GPP (organismo internacional de especificación para redes móviles): https://www.3gpp.org/
- IANA (autoridad de asignación de numeraciones en interredes): https://www.iana.org/
- Especificaciones de terminales móviles: https://www.movilcelular.es/especificaciones/
- Verificación de IMEIs: https://www.movical.net/
- Listado de MCCs y MNCs: https://www.mcc-mnc.com/