분석 · 2026년 5월 16일

← 이전·다음 →

암호화가 곧 프라이버시는 아니다: 메타데이터가 말해 주는 진실

암호화된 내용과 가시적인 메타데이터는 서로 다른 개념입니다. 서비스가 '종단간 암호화'를 말할 때, 그것은 이야기의 절반에 불과합니다.

모든 것을 보호하지는 못하는 자물쇠

오늘날 대부분의 메시징 서비스는 종단간 암호화를 광고합니다. 이는 사실입니다. 메시지 내용은 암호화되어 전송되므로 통신 경로상의 누구도, 심지어 서비스 제공자조차도 전송 중인 텍스트를 읽을 수 없습니다. 여기까지는 정확한 설명입니다.

문제는 내용이 이야기의 일부분일 뿐이라는 점입니다. 당신이 무엇을 말했는지 아무도 읽을 수 없더라도, 서비스 측은 다른 정보를 매우 높은 정밀도로 파악하고 있습니다. 누구와 언제 얼마나 자주, 대략 어느 위치에서 어떤 기기로 대화하는지. 전송 및 수신된 메시지의 수와 공유된 파일의 수. 이 모든 것을 '메타데이터'라고 부릅니다. 그리고 많은 경우 메타데이터는 메시지 자체만큼이나 많은 정보를 알려줍니다.

메타데이터가 노출하는 것

많은 것을 알기 위해 메시지를 읽을 필요는 없습니다. 어떤 인물이 6개월 동안 매주 화요일 오전 9시에 종양학 전문의에게 전화를 걸거나 메시지를 보낸다면, 대화 내용을 듣지 않아도 무슨 일이 일어나고 있는지 짐작할 수 있습니다. 두 인물이 하루에 100통의 메시지를 주고받다가 갑자기 멈춘다면, 이유를 이해하기 위해 단 한 통의 메시지도 읽을 필요가 없습니다. 세무사가 분기 결산 전날 밤에 동일한 고객으로부터 20통의 메시지를 연속으로 받는다면, 그 패턴이 모든 것을 말해줍니다.

메타데이터는 행동 패턴을 노출시킵니다. 누가 누구와 관계를 맺고 있는지, 각각의 일정, 깨어 있는 시간, 자는 시간, 이동 여부. 가장 활동적인 고객은 누구인지, 가장 밀접한 비즈니스 관계는 무엇인지. 메타데이터를 수집하는 서버는 사용자가 쓰는 단어를 단 한 글자도 읽지 않고도 그 인물의 사생활 및 업무 생활에 대한 상세한 프로필을 작성할 수 있습니다.

이를 여실히 보여주는 역사적인 사례가 있습니다. 전 NSA 국장 마이클 헤이든은 2014년에 다음과 같이 명언했습니다. *「We kill people based on metadata(우리는 메타데이터를 근거로 사람을 죽인다)」*. 이 발언은 통신 패

턴만을 근거로 특정된 표적에 대한 미군의 군사 작전을 지칭한 것이었습니다. 읽힌 메시지는 단 한 통도 없습니다. 오직 연락처 그래프와 일정만이 근거가 된 것입니다.

서비스가 메타데이터를 수집한다고 해서 반드시 그것을 사용자에게 악용한다는 뜻은 아닙니다. 하지만 그것을 수행할 '능력'을 보유하고 있으며, 법원의 명령, 보안 침해 또는 약관에 의해 허용된다면 제3자에게 판매함으로써 그 데이터에 접근한 제3자 또한 그 능력을 손에 넣게 됩니다.

연락처에 대한 접근

거의 인지되지 못하는 또 다른 경로는 연락처 목록입니다. 메시징 서비스의 대부분은 가입 시 스마트폰 연락처에 대한 접근 권한을 요구합니다. 그들은 모든 번호를 서버에 업로드하고 다른 누가 서비스를 이용 중인지 표시합니다. 그 순간부터 사용자가 누구에게도 메시지를 보내지 않았더라도 운영 회사는 사용자의 인간관계에 대한 완전한 맵을 보유하게 됩니다.

변호사, 의사, 심리치료사, 컨설턴트 등 비밀 유지 의무를 지는 전문가에게 그 연락처에는 '고객'이 포함되어 있습니다. 연락처가 제3자의 서버에 업로드된 경우, 고객의 이름은 전문가가 법적 관할권이나 정책을 관리할 수 없는 인프라 내에 놓이게 됩니다. 비밀 유지 의무는 대화가 유출된 날에 깨지는 것이 아니라, 업로드에 동의한 그 순간에 이미 깨진 것입니다.

‘암호화하는 것’과 ‘수집하지 않는 것’의 차이

암호화는 내용을 보호하는 것입니다. 프라이버시란 불필요한 것을 수집하지 않는 것입니다. 이들은 별개의 것이며 그 차이는 운영상 결정적인 의미를 갖습니다. 서비스는 모든 메시지를 완벽하게 암호화하면서 동시에 메타데이터를 통해 사용자의 거의 모든 것을 파악할 수 있습니다. 이 두 가지는 완벽하게 양립합니다. 실제로 이것이 이 업계의 지배적인 비즈니스 모델입니다.

서비스의 진정한 프라이버시를 평가하기 위한 올바른 질문은 *“내용을 암호화하는가?”*가 아닙니다. 그 질문에 대한 답은 수년 전부터 알려져 있습니다. 올바른 질문은 *“어떤 메타데이터를 생성하며 그것은 어디에 저장되는가?”*, 그리고 무엇보다도 *“어떤 메타데이터를 생성할 필요가 없는가?”*입니다.

약속이나 내부 정책이 아니라 설계(privacy by design)에 의해 메타데이터를 최소화하는 아키텍처는 데이터를 수집하고 암호화하는 아키텍처보다 구조적으로 더 프라이빗합니다. 존재하지 않는 데이터는 유출될 수도, 판매될 수도, 법원의 명령에 제출될 수도, 해킹으로 소실될 수도 없기 때문입니다.

프로페셔널 독자 여러분께

만약 당신의 업무에 비밀 유지, 기밀 유지 또는 단순히 제3자의 정보에 대한 존중이 포함된다면 다음과 같은 순서로 자문해 볼 가치가 있습니다.

1. 내가 통신에 사용하는 앱은 내용을 암호화하는가? (아마도 예)
2. 그것은 메타데이터를 암호화하는가? (아마도 아니오)
3. 작동에 *불필요한* 메타데이터를 생성하고 있는가? (거의 확실히 예)

4. 그 메타데이터는 어디에, 어떤 법적 관할권 아래에 저장되는가? (아마도 유럽 경제 지역 외부)
5. 내 고객이나 환자는 자신의 데이터가 거기 있다는 사실을 알고 있는가?

마지막 질문은 불편한 것입니다. 왜냐하면 대부분의 경우 성실한 대답은 '아니오'이기 때문입니다.

이 기사는 프로페셔널 통신 도구의 실태에 관한 연재의 제1회입니다. 다음 회부터는 메시징에서의 GDPR 준수 및 디지털 시대의 비밀 유지 의무 개념에 대해 다룹니다.

참고 문헌 및 관련 자료

- 헤이든, M. – 존스 홉킨스 대학교에서의 성명, 2014년("We kill people based on metadata"). 공개 기록 있음.
- GDPR(EU 규정 2016/679), 제4조 및 제5조 – 개인 데이터의 정의와 처리 원칙(메타데이터는 개인 데이터이다).
- 유럽 데이터 보호 감독관 및 EDPB – 전자 통신에서의 트래픽 데이터 및 메타데이터 처리 관련 의견(ePrivacy 지침).

← 이전봉인의 짧은 역사다음 → 디지털 시대의 비밀 유지 의무

최근 읽은 글

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

이 기사를 다운로드하여 필요한 곳에서 활용하십시오.

↓ 마크다운 ↓ 텍스트 형식 ↓ PDF

파일이 기기에 다운로드됩니다. 해당 위치에서 저장하거나 Solo2로 가져오거나 원하는 곳에 공유할 수 있습니다. Cuadernos는 전송 대상을 결정하지 않습니다.

봉인 · SHA-256 ff8ca65e13143ecbbdaa445dfca32310e986b49fd8ff695bd34c0e5e1915abd5

Cuadernos Lacre · Menzuri Gestión S.L.의 간행물 ·
저자: R.Eugenio · Solo2 팀 편집