분석 · 2026년 5월 16일

← 이전·다음 →

중간에 아무도 없을 때

서버를 통과하는 데이터를 암호화하는 것은 내용을 보호합니다. 중간에 서버가 없는 것은 그 질문 자체를 제거합니다. 이 둘은 같지 않습니다.

두 사람, 하나의 대화

두 사람이 방 안에서 얼굴을 마주보고 대화할 때, 아무도 아무것도 듣지 못했다고 약속할 필요가 없습니다. 거기에 없었기 때문에 듣지 못한 것입니다. 두 사람이 손에서 손으로 종이를 건넬 때, 중간에 있는 누군가가 그것을 읽지 않았다고 맹세할 필요가 없습니다. 중간에는 아무도 없습니다.

일상생활의 대부분은 이런 식으로 작동합니다. 우리는 목소리를 전달하는 공기나, 우리가 들고 있는 종이와 비밀 유지 계약을 맺지 않습니다. 대화의 프라이버시는 중개자의 약속에 의존하지 않습니다. 중개자가 없기 때문입니다. 이것은 프라이버시를 지키는 가장 강력한 방법 중 하나입니다. 무언가나 누군가가 행동을 잘해서가 아니라, 무언가나 누군가가 존재하지 않기 때문입니다.

대화가 디지털 채널로 옮겨가면 이는 기본적으로 바뀝니다. 일반적인 모델은 다음과 같습니다. 두 사람이 서버에 연결하고, 서버는 메시지를 받아 암호화하거나 암호화된 상태로 저장하여 수신자에게 전달합니다. 서버가 중간에 있습니다. 서버는 정직할 수 있습니다. 감사를 받을 수 있습니다. 유리한 관할 구역에서 엄격한 개인정보 보호 정책에 따라 운영될 수 있습니다. 이 모든 것이 사실일 수 있습니다. 하지만 서버는 중간에 있습니다.

암호화와 수집하지 않음의 차이 (2부)

같은 시리즈의 이전 기사에서 우리는 내용을 암호화하는 것과 메타데이터를 수집하지 않는 것은 같지 않다고 주장했습니다. 명확하게 공식화해야 할 한 걸음이 더 있습니다. 서버를 통과하는 데이터를 암호화하는 것과 서버를 두지 않는 것 또한 같지 않습니다.

첫 번째 모델(중간에 서버, 암호화된 콘텐츠)은 서버 운영자, 유지 보수 담당자, 시스템을 침해하는 외부 공격자로부터 콘텐츠를 보호합니다. 그리고 그것은 중요합니다. 하지만 그것이 서버를 제거하지는 않습니다. 서버는 여전히 거기에 있습니다. 메타데이터를 계속 처리합니다. 법원 명령, 법적 개입, 정치적 압력 또는 보안 침해를 받을 수 있는 지점으로 계속 남아 있습니다. 여전히 누군가를 신뢰해야 하는 지점입니다.

두 번째 모델(두 끝 사이에 서버 없음)은 암호화된 콘텐츠를 더 잘 보호하지는 않습니다. 암호화가 강력하다면, 콘텐츠는 두 경우 모두 보호됩니다. 변하는 것은 콘텐츠가 아닙니다. 변하는 것은 *«서버는 어떻게 되는가?»*라는

질문의 대상이 사라진다는 것입니다. 질문을 던질 대상인 서버가 존재하지 않기 때문입니다.

신뢰, 부재, 그리고 둘 사이의 차이

신뢰는 정당하게 부여될 수 있습니다. 정직한 기업은 존재합니다. 엄격한 감사관도 존재합니다. 사용자에게 유리한 법률도 존재합니다. 위 사항들을 철저히 준수하는 진지한 서비스도 존재합니다. 그럴 자격이 있는 운영자에게 주어지는 신뢰는 나쁜 계약이 아닙니다.

그러나 신뢰는 아무리 굳건하더라도 신뢰로 남습니다. 그것은 사회적 해결책이지 기술적 해결책이 아닙니다. 기업의 소유주가 바뀔 수 있습니다. 관할 구역의 정부가 바뀔 수 있습니다. 법원 명령이 내일 도착할 수 있습니다. 새로운 취약성이 다음 달에 발견될 수 있습니다. 이 중 어느 것도 악의로 일어나는 것은 아닙니다. 운영자가 존재하고, 존재하는 모든 것은 세상의 우발적 상황에 노출되어 있기 때문에 일어나는 일입니다.

운영자의 부재는 동일한 우발적 상황에 노출되지 않습니다. 법원 명령은 존재하지 않는 서버에 데이터를 요구할 수 없습니다. 공격자는 존재하지 않는 서버를 침해할 수 없습니다. 회사의 정책 변경은 회사가 가진 적 없는 데이터에 영향을 미칠 수 없습니다. 핵심 문구는 간단합니다. 존재하지 않는 데이터는 분실할 수 없습니다.

서버 측의 합당한 주장에 대하여

중간에 서버를 두고 전문적인 메시징 서비스를 제공하는 사람은 일반적으로 완벽하게 유효한 세 가지 주장을 합니다. 첫째, 수신자가 오프라인일 때 전달을 보장하기 위해 서버가 필요하다는 것. 둘째, 콘텐츠 암호화가 강력하므로 운영자가 이를 읽을 수 없다는 것. 셋째, 서비스가 유럽 법률을 준수하며 데이터는 법으로 보호된다는 것.

세 가지 주장은 모두 사실입니다. 어느 것도 사안의 본질을 바꾸지 않습니다. 지연된 전달을 위해 서버에 메시지를 저장할 수 있는 것은 사실입니다. 또한 지연된 전달은 수십 년 동안 개선되어 오늘날 운영되고 있는 기기 간 직접 통신 프로토콜을 통해 다른 방식으로 해결할 수 있다는 것도 사실입니다. 진지한 서비스에서 전송 중인 콘텐츠의 암호화가 강력하다는 것은 사실입니다. 그리고 유럽 법률이 다른 많은 곳보다 사용자를 더 보호한다는 것도 사실입니다.

문제는 중간에 서버가 있는 서비스가 합법적인지, 안전한지, 콘텐츠를 보호하는지가 아닙니다. 합법적이고, 안전할 수 있으며, 콘텐츠를 보호합니다. 핵심은 중간에 서버를 두는 것이 아키텍처 상의 선택이지, 기술적 강제가 아니라는 점입니다. 그리고 모든 선택에는 결과가 따릅니다. 중간에 서버가 있는 아키텍처는 신뢰해야 할 행위자를 필연적으로 만들어냅니다. 중간에 서버가 없는 아키텍처는 그렇지 않습니다.

법이 말하는 것, 그리고 아키텍처가 하는 일

GDPR은 특정한 아키텍처 모델을 요구하지 않습니다. 데이터 최소화, 목적 제한, 설계 및 기본값에 의한 데이터 보호, 규정 준수 입증 능력과 같은 결과를 요구합니다. 중간에 서버가 있는 서비스는 이 모든 요구 사항을 충족할 수 있습니다. 중간에 서버가 없는 서비스는 선언이 아니라 구조 자체를 통해 그 중 몇 가지를 충족합니다. 절대적인 최소화, 즉 메시지를 전달하는 데 엄격하게 필요한 것 외에는 아무것도 수집하지 않는 것은, 무언가를 수집할 수 있는 서버가 존재하지 않을 때 아주 쉬운 일이 됩니다.

일상적인 비민감성 용도에서는 서버 아키텍처가 완전히 합리적이며 진지한 운영자에 대한 신뢰는 유효한 합의입니다. 규제되는 직업상 비밀이 관련되거나, 윤리적 책임이 따르거나, 특히 민감한 정보를 다루는 기타 용도에서는 신뢰 지점의 부재는 사치가 아니라 구조적 이점입니다.

전문적인 독자를 위하여

전문적인 통신 서비스를 접할 때 던져야 할 질문(동일한 시리즈의 이전 기사에서 이미 익숙한)에 아키텍처에 관한 질문 하나가 더 추가됩니다.

1. 전송 중에 콘텐츠를 암호화합니까? (아마도 '예'일 것입니다.)
2. 내가 누구와 언제 대화하는지에 대한 메타데이터를 생성하고 저장합니까? (아마도 '예'일 것입니다.)
3. 나의 기기와 수신자의 기기 사이의 경로에 서버가 존재합니까?
4. 존재한다면: 누가 그것을 운영하며, 어떤 관할 구역에 있고, 내 데이터를 넘겨주려면 어떤 일이 일어나야 합니까?
5. 존재하지 않는다면: 이전 질문들은 무의미합니다.

두 범주 사이의 차이는 정도의 차이가 아니라 종류의 차이입니다. 고객, 환자, 또는 동료에게 설명해야 할 때, 가장 정직한 공식은 가장 단순하기도 합니다. 하나는 중간에 누군가가 있고, 다른 하나는 그렇지 않다는 것입니다.

이 기사로 Cuadernos Lacre의 초기 사이클이 마무리됩니다. 암호화, 메타데이터, 직업상 비밀에 대해 이야기한 후 아키텍처의 전체 그림을 완성했습니다. 콘텐츠를 암호화하는 것과 중간에 서버가 없는 것은 다른 것입니다. 둘 다 합법적일 수 있지만, 신뢰 지점을 없애는 것은 후자뿐입니다.

참고 문헌 및 관련 자료

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. 시스템의 보증은 중간 채널이 아닌 말단에 구현되어야 한다는 원칙의 기초 텍스트.
- 규정 (EU) 2016/679, 제25조 — 설계 및 기본값에 의한 데이터 보호.
- 규정 (EU) 2016/679, 제5.1.c조 — 데이터 최소화 원칙.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. 설계에 의해 데이터 수집을 최소화하는 아키텍처에 관한 장.

← 이전GDPR과 비즈니스 메시징: 왜 대부분의 조직이 모르는 사이에 규정을 위반하는가다음 →CUADERNOS_LIST_SCHREMS_TITLE

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 33f5f202a5ce371897b2dffe7622d1e0e7c29be1111c78dc19dcc817a0458eb5

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

본 사이트는 쿠키를 사용하지 않으며 제3자 리소스를 로드하지 않습니다. 자체 호스팅 익명 방문자 카운터(유럽 서버의 Umami)를 사용하며, 라이트/다크 테마 설정을 위한 최소한의 JavaScript로만 작동합니다. 추적기, 프로파일링, 데이터 공유가 전혀 없습니다. 업데이트를 받으려면: RSS.