Phân tích · 16 tháng 5, 2026

← Trước·Tiếp theo →

# Khi không có ai ở giữa

Mã hóa những gì đi qua máy chủ bảo vệ nội dung. Không có máy chủ ở giữa loại bỏ câu hỏi đó. Chúng không giống nhau.

## Hai người, một cuộc trò chuyện

Khi hai người nói chuyện mặt đối mặt trong một căn phòng, không ai phải hứa rằng họ không nghe thấy gì. Họ không nghe thấy vì họ không ở đó. Khi hai người truyền cho nhau một tờ giấy từ tay người này sang tay người kia, không ai ở giữa phải thề rằng họ chưa đọc nó. Không có ai ở giữa cả.

Hầu hết mọi thứ trong cuộc sống hàng ngày đều hoạt động theo cách đó. Chúng ta không ký thỏa thuận bảo mật với không khí truyền tải giọng nói của mình, hoặc với tờ giấy chúng ta cầm. Tính riêng tư của cuộc trò chuyện không dựa trên lời hứa của người trung gian, vì không có người trung gian. Đó là một trong những hình thức riêng tư mạnh mẽ nhất tồn tại: không phải vì ai đó hay điều gì đó cư xử tốt, mà vì không có ai đó hay điều gì đó.

Khi cuộc trò chuyện chuyển sang kênh kỹ thuật số, điều này thay đổi theo mặc định. Mô hình thông thường như sau: hai người kết nối với một máy chủ, máy chủ nhận tin nhắn, mã hóa nó hoặc lưu trữ nó dưới dạng mã hóa, và giao nó cho người nhận. Máy chủ ở giữa. Máy chủ có thể trung thực. Nó có thể được kiểm toán. Nó có thể hoạt động trong một khu vực tài phán thuận lợi và theo một chính sách bảo mật nghiêm ngặt. Tất cả những điều đó có thể là sự thật. Nhưng máy chủ vẫn ở giữa.

## Sự khác biệt giữa mã hóa và không thu thập (phần hai)

Trong một bài viết trước của cùng loạt bài này, chúng tôi đã lập luận rằng mã hóa nội dung và không thu thập siêu dữ liệu không giống nhau. Có một bước xa hơn cần được xây dựng rõ ràng: mã hóa những gì đi qua máy chủ và không có máy chủ cũng không giống nhau.

Mô hình đầu tiên — máy chủ ở giữa, nội dung được mã hóa — bảo vệ nội dung khỏi người vận hành máy chủ, nhân viên bảo trì của họ, và những kẻ tấn công bên ngoài có thể xâm phạm hệ thống. Và điều đó rất quan trọng. Nhưng nó không loại bỏ máy chủ. Máy chủ vẫn ở đó. Nó vẫn xử lý siêu dữ liệu. Nó vẫn là một điểm có thể nhận được lệnh của tòa án, sự can thiệp hợp pháp, áp lực chính trị hoặc sự vi phạm an ninh. Nó vẫn là một điểm đòi hỏi phải đặt niềm tin vào ai đó.

Mô hình thứ hai — không có máy chủ giữa hai đầu — không bảo vệ nội dung được mã hóa tốt hơn: nếu mật mã vững chắc, nội dung được bảo vệ trong cả trường hợp. Điều thay đổi không phải là nội dung. Điều thay đổi là câu hỏi *«điều gì xảy ra với máy chủ?»* không còn đối tượng nữa, vì không có máy chủ nào để hỏi.

## Niềm tin, sự vắng mặt và sự khác biệt giữa hai điều này

Niềm tin có thể được đặt đúng chỗ. Những công ty trung thực là có thật. Các kiểm toán viên nghiêm ngặt là có thật. Luật pháp thuận lợi cho người dùng là có thật. Các dịch vụ nghiêm túc tuân thủ nghiêm ngặt tất cả những điều trên là có thật. Niềm tin, khi được trao cho một nhà vận hành xứng đáng, không phải là một sự sắp xếp tồi.

Nhưng niềm tin, dù vững chắc đến đâu, vẫn là niềm tin. Đó là một giải pháp xã hội, không phải là một giải pháp kỹ thuật. Một công ty có thể đổi chủ. Một khu vực tài phán có thể thay đổi chính phủ. Một lệnh của tòa án có thể đến vào ngày mai. Một lỗ hổng mới có thể được phát hiện vào tháng tới. Không điều nào trong số này xảy ra vì ác ý. Nó xảy ra bởi vì nhà vận hành tồn tại, và mọi thứ tồn tại đều phải chịu những bất trắc của thế giới.

Sự vắng mặt của một nhà vận hành không phải chịu những bất trắc tương tự. Một lệnh của tòa án không thể yêu cầu dữ liệu từ một máy chủ không tồn tại. Một kẻ tấn công không thể thỏa hiệp một máy chủ không tồn tại. Một sự thay đổi trong chính sách của công ty không thể ảnh hưởng đến dữ liệu mà công ty đó chưa bao giờ có. Cụm từ then chốt rất đơn giản: dữ liệu không tồn tại thì không thể bị mất.

## Về lập luận hợp pháp từ phía máy chủ

Những người cung cấp dịch vụ nhắn tin chuyên nghiệp có máy chủ ở giữa thường đưa ra ba lập luận hoàn toàn hợp lệ. Thứ nhất, máy chủ là cần thiết để đảm bảo việc phân phối khi người nhận ngoại tuyến. Thứ hai, mã hóa nội dung là mạnh mẽ và do đó nhà điều hành không thể đọc được. Thứ ba, dịch vụ tuân thủ luật pháp châu Âu và dữ liệu được luật pháp bảo vệ.

Cả ba lập luận đều đúng. Không có lập luận nào thay đổi bản chất của vấn đề. Đúng là một máy chủ cho phép lưu trữ tin nhắn để phân phối bị trì hoãn; cũng đúng là việc phân phối bị trì hoãn có thể được giải quyết theo cách khác, thông qua các giao thức liên lạc trực tiếp giữa các thiết bị đã được tinh chỉnh trong nhiều thập kỷ và đang hoạt động ngày nay. Đúng là mã hóa nội dung trong quá trình truyền tải là mạnh mẽ ở các dịch vụ nghiêm túc. Và đúng là luật pháp châu Âu bảo vệ người dùng nhiều hơn ở nhiều nơi khác.

Vấn đề không phải là liệu các dịch vụ có máy chủ ở giữa có hợp pháp hay không, chúng có an toàn hay không, hay chúng có bảo vệ nội dung hay không. Chúng có thể như vậy, chúng hợp pháp, và chúng thường an toàn. Vấn đề là việc có một máy chủ ở giữa là một sự lựa chọn về kiến trúc, không phải là một sự áp đặt về kỹ thuật. Và mọi sự lựa chọn đều có hậu quả. Một kiến trúc có máy chủ ở giữa nhất thiết phải tạo ra một tác nhân cần được tin tưởng. Một kiến trúc không có máy chủ ở giữa thì không.

## Những gì luật pháp nói và những gì kiến trúc làm

Quy định chung về bảo vệ dữ liệu (RGPD) không yêu cầu một mô hình kiến trúc cụ thể. Nó yêu cầu kết quả: giảm thiểu dữ liệu, mục đích giới hạn, bảo vệ từ khâu thiết kế và theo mặc định, khả năng chứng minh sự tuân thủ. Một dịch vụ có máy chủ ở giữa có thể đáp ứng tất cả các yêu cầu này. Một dịch vụ không có máy chủ ở giữa đáp ứng nhiều yêu cầu trong số đó theo cấu trúc, không phải bằng tuyên bố. Giảm thiểu tuyệt đối — không thu thập bất cứ thứ gì không thực sự cần thiết để gửi tin nhắn — là điều tầm thường khi không có máy chủ nào có thể thu thập bất cứ thứ gì.

Đối với các mục đích sử dụng hàng ngày không nhạy cảm, kiến trúc máy chủ là hoàn toàn hợp lý, và sự tin tưởng vào một nhà điều hành nghiêm túc là một sự sắp xếp hợp lệ. Đối với các mục đích sử dụng khác — những mục đích liên quan đến bí mật nghề nghiệp được quản lý, những mục đích đòi hỏi trách nhiệm đạo đức, những mục đích chạm đến thông tin đặc biệt nhạy cảm — việc không có điểm đáng tin cậy không phải là một điều xa xỉ, mà là một lợi thế cấu trúc.

## Dành cho độc giả chuyên nghiệp

Các câu hỏi nên được đặt ra đối với một dịch vụ truyền thông chuyên nghiệp, đã quen thuộc từ các bài viết trước trong loạt bài này, được hoàn thiện với chỉ một câu hỏi về kiến trúc nữa:

1. Nó có mã hóa nội dung khi truyền tải không? (Có thể có.)
2. Nó có tạo và lưu trữ siêu dữ liệu về việc tôi nói chuyện với ai và khi nào không? (Có thể có.)
3. Có máy chủ trên đường đi giữa thiết bị của tôi và thiết bị của người nhận không?

4. Nếu có: ai vận hành nó, ở khu vực tài phán nào, và điều gì sẽ phải xảy ra để họ giao nộp dữ liệu về tôi?
5. Nếu không có: các câu hỏi trước đó không còn đối tượng nữa.

Sự khác biệt giữa hai danh mục không phải ở mức độ, mà là ở loại hình. Khi đến lúc giải thích điều đó với khách hàng, bệnh nhân hoặc đồng nghiệp, công thức trung thực nhất cũng là công thức đơn giản nhất: trong cái này, có ai đó ở giữa; trong cái kia thì không.

---

*Bài viết này kết thúc chu kỳ đầu tiên của Cuadernos Lacre. Sau khi nói về mã hóa, siêu dữ liệu và bí mật nghề nghiệp, chúng ta hoàn thành bức tranh kiến trúc: mã hóa nội dung và không có máy chủ ở giữa là những điều khác nhau. Cả hai đều có thể hợp pháp; chỉ một cái loại bỏ điểm đáng tin cậy.*

## Nguồn tham khảo và đọc thêm


- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Văn bản nền tảng của nguyên tắc trong đó các đảm bảo của một hệ thống phải được thực hiện ở các điểm cuối, không phải ở kênh trung gian.
- Quy định (EU) 2016/679, Điều 25 — bảo vệ dữ liệu từ khâu thiết kế và theo mặc định.
- Quy định (EU) 2016/679, Điều 5.1.c — nguyên tắc giảm thiểu dữ liệu.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Các chương về kiến trúc giảm thiểu việc thu thập thông qua thiết kế.



← TrướcGDPR và tin nhắn chuyên nghiệp: tại sao hầu hết đang vi phạm mà không hề hay biếtTiếp theo →CUADERNOS_LIST_SCHREMS_TITLE


## Các bài đọc gần đây


- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE


Tải bài viết này để sử dụng ở bất cứ đâu bạn cần.

↓ Markdown ↓ Văn bản thuần túy ↓ PDF

Tệp sẽ được tải xuống thiết bị của bạn. Từ đó, bạn có thể lưu trữ, nhập vào Solo2 hoặc chia sẻ ở bất cứ đâu. Cuadernos không quyết định điểm đến thay cho bạn.


Dấu sáp · SHA-256 2dd8b439982009868387064dce818d2b4291c07585c7a4e425750d561ba87876

Cuadernos Lacre · Một ấn phẩm của Menzuri Gestión S.L. ·
viết bởi R.Eugenio · được biên tập bởi đội ngũ Solo2.