Lịch sử tóm tắt về dấu sáp

Trong bốn thế kỷ, một giọt sáp đỏ đảm bảo rằng không ai đọc được một bức thư. Chúng ta đã đánh mất điều đó khi chuyển sang thời đại kỹ thuật số. Nó có thể được phục hồi.

Trước khi có giấy

Nhu cầu truyền đạt bí mật một điều gì đó cho người ở xa còn lâu đời hơn cả chữ viết. Ở Mesopotamia, những tấm đất sét chứa tin nhắn hành chính hoặc riêng tư được gửi đi bên trong các viên nang cũng làm bằng đất sét, được niêm phong trước khi nung: bất kỳ nỗ lực nào để đọc nội dung đều buộc phải đập vỡ lớp vỏ, và người nhận chỉ cần nhìn qua là biết viên nang có còn nguyên vẹn hay không. Ở thời La Mã cổ đại, các cuộn giấy da được buộc bằng dây và niêm phong bằng sáp hoặc chì. Ý tưởng luôn giống nhau: bất kỳ việc đọc trái phép nào đều phải để lại một dấu vết vật lý không thể xóa nhòa.

Kỷ nguyên của dấu sáp

Trong nhiều thế kỷ, từ cuối thời Trung Cổ cho đến thế kỷ 20, công cụ kinh điển cho thư tín bí mật ở châu Âu là giấy gấp lại và niêm phong bằng dấu sáp. Sáp nóng chảy được đổ lên chỗ nối của nếp gấp và in bằng con dấu cá nhân hoặc tổ chức. Nó không phải là vật trang trí. Các công chứng viên, nhà ngoại giao, thương gia và cá nhân đã sử dụng nó với cùng một logic: nếu dấu sáp còn nguyên vẹn và con dấu có thể nhận ra được, nội dung chưa bị đọc; nếu nó bị hỏng, thư tín đã bị xâm phạm ngay cả trước khi mở.

Sức mạnh của dấu sáp không nằm ở chi phí hay sự trang trọng của nó. Nó nằm ở một đặc tính cấu trúc rất cụ thể: bất kỳ nỗ lực nào để gỡ nó ra và dán lại đều để lại dấu vết rõ ràng. Không có cách nào im lặng để mở một bức thư đã niêm phong. Và điều đó có nghĩa là tính bảo mật không phụ thuộc vào lời hứa của bất kỳ trung gian nào — từ người đưa tin, người lái xe ngựa, đến nhân viên bưu điện — mà phụ thuộc vào chính thiết kế vật lý của lớp vỏ bọc. Đó là niềm tin dựa trên bằng chứng, không phải dựa trên lời nói của bất kỳ ai.

Sự chuyển đổi kỹ thuật số

Điện tín, điện thoại, email, tin nhắn doanh nghiệp. Truyền thông điện tử mang lại tốc độ, phạm vi toàn cầu và chi phí gần như bằng không cho mỗi tin nhắn. Nó cũng lấy đi sự đảm bảo của dấu sáp. Theo mặc định, mọi tin nhắn đều đi qua các trung gian mà tính toàn vẹn của họ chúng ta chỉ có thể xác minh thông qua những lời hứa được viết trong điều khoản dịch vụ, chứng nhận kỹ thuật và các cuộc kiểm toán không minh bạch. Không có gì tương đương với một giọt sáp bị vỡ để cảnh báo chúng ta.

Một dấu sáp kỹ thuật số

Đặc tính mang lại sức mạnh cho dấu sáp không phải là bản thân dấu sáp, mà là những gì nó đại diện: tính toàn vẹn có thể xác minh bằng thiết kế, không cần phải tin tưởng vào bên thứ ba. Đặc tính này có thể được tái tạo trên mặt phẳng kỹ thuật số, mặc dù với hai yếu tố thay vì một. Đầu tiên là con dấu mật mã — hàm băm SHA-256 xuất hiện ở cuối mỗi bài viết của ấn phẩm này, theo nghĩa đen, là một dấu sáp kỹ thuật số: bất kỳ sự sửa đổi nội dung nào đều làm thay đổi hàm băm một cách rõ ràng, giống như sáp vỡ tiết lộ việc đọc trái phép. Thứ hai là

kiến trúc của kênh: khi không có máy chủ ở giữa hai người đang giao tiếp, không có trung gian nào cần được cấp sự tin tưởng. Sự kết hợp của cả hai yếu tố — tính toàn vẹn có thể xác minh và sự vắng mặt của trung gian — tái tạo lại, trong các thuật ngữ kỹ thuật số, những gì mà sáp đỏ trên giấy gấp đã làm hàng ngày trong suốt bốn thế kỷ.

Tên gọi

Ấn phẩm này được gọi là Cuadernos Lacre vì dấu sáp không phải là một món đồ trang trí lịch sử, mà là một đặc tính kỹ thuật cụ thể: tính toàn vẹn có thể xác minh bằng cấu trúc, không có lời hứa của bất kỳ nhà điều hành nào. Mỗi bài viết trong loạt bài phân tích, trong phiên bản kỹ thuật số đương đại của nó, một phần của cùng một ý tưởng: mã hóa, siêu dữ liệu, bí mật nghề nghiệp, kiến trúc truyền thông, khuôn khổ pháp lý châu Âu. Tên gọi cũng là một cách để nhắc nhở rằng tính bảo mật không phải là một dịch vụ được thuê, mà là một đặc tính của chính kênh mà thông lưu thông.

Nguồn tham khảo và đọc thêm

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (các chương về việc niêm phong các tấm đất sét và bullae của Mesopotamia).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. Các chương về dấu sáp như một công cụ của tính toàn vẹn và quyền tác giả.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Công thức hiện đại của nguyên tắc dấu sáp: các đảm bảo ở các điểm cuối, không phải trong kênh.

Tiếp theo → Mã hóa không có nghĩa là quyền riêng tư: siêu dữ liệu nói gì về bạn

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 11817f64b5ed640393e2e755eeae3b7542d7c78924d372b92e4170bd2ce9c1d6
ES

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