Trumpa vaško antspaudo istorija

Keturis šimtmečius raudono vaško lašas garantavo, kad laiško niekas neskaitė. Mes jį praradome pereidami į skaitmeninę erdvę. Jį galima susigrąžinti.

Prieš atsirandant popieriui

Poreikis ką nors konfidencialiai pranešti toli esančiam asmeniui yra senesnis nei raštas. Mesopotamijoje molinės lentelės su administraciniais ar asmeniniais pranešimais buvo siunčiamos taip pat molinėse kapsulėse, kurios buvo užplombuojamos prieš išdegant: bet koks bandymas perskaityti turinį vertė sulaužyti apvalkalą, ir gavėjas iš pirmo žvilgsnio suprasdavo, ar kapsulė atkeliavo nepažeista. Klasikinėje Romoje pergamento ritinėliai buvo surišami virvele ir užplombuojami vašku arba švinu. Idėja visada buvo ta pati: bet koks neteisėtas skaitymas turėjo palikti neišdildomą fizinį pėdsaką.

Vaško antspaudo epocha

Kelis šimtmečius, nuo viduramžių pabaigos iki pat XX amžiaus, Europos konfidencialios korespondencijos kanoninis įrankis buvo sulankstytas popierius, užplombuotas vaško antspaudu. Išlydytas vaškas buvo užpilamas ant popieriaus sujungimo ir įspaudžiamas asmeniniu ar instituciniu spaudu. Tai nebuvo ornamentas. Notarai, diplomatai, pirkliai ir privatūs asmenys jį naudojo ta pačia logika: jei vaško antspaudas buvo nepažeistas, o spaudas atpažįstamas, turinys nebuvo skaitytas; jei jis buvo sulaužytas, korespondencija buvo pažeista dar prieš ją atidarant.

Vaško antspaudo galia slypėjo ne jo brangume ar iškilmingume. Ji glūdėjo labai konkrečioje struktūrinėje savybėje: bet koks bandymas jį nuimti ir vėl uždėti palikdavo matomus pėdsakus. Nebuvo jokio tylaus būdo atidaryti užplombuotą laišką. O tai reiškė, kad konfidencialumas priklausė ne nuo jokio tarpininko – pasiuntinio, vežėjo, pašto pareigūno – pažado, bet nuo paties fizinio voko dizaino. Tai buvo pasitikėjimas, grįstas įrodymais, o ne kieno nors žodžiais.

Skaitmeninis perėjimas

Telegrafas, telefonas, elektroninis paštas, įmonių susirašinėjimas. Skaitmeninis ryšys atnešė greitį, pasaulinį pasiekiamumą ir beveik nulinę vieno pranešimo kainą. Kartu jis sunaikino vaško antspaudo garantiją. Pagal nutylėjimą kiekvienas pranešimas praeina per tarpininkus, kurių vientisumą galime patikrinti tik per rašytinius paslaugų teikimo sąlygų pažadus, techninius sertifikatus ir neskaidrius auditus. Nėra nieko panašaus į sulūžusio vaško lašą, kuris mus įspėtų.

Skaitmeninis vaško antspaudas

Savybė, kuri suteikė vaško antspaudui galią, buvo ne pats vaško antspaudas, o tai, ką jis atstovavo: tikrinamas vientisumas pagal dizainą, be poreikio pasitikėti trečiąja šalimi. Šią savybę galima atkurti skaitmeninėje plotmėje, nors ir su dviem elementais vietoj vieno. Pirmasis yra kriptografinis antspaudas — SHA-256 pėdsakas, kuris rodomas kiekvieno šio leidinio straipsnio apačioje, yra, tiesiogine prasme, skaitmeninis vaško antspaudas:

bet koks turinio pakeitimas matomai pakeičia pėdsaką, lygiai taip pat, kaip sulūžęs vaškas išduodavo neteisėtą skaitymą. Antrasis yra kanalo architektūra: kai tarp dviejų bendraujančių žmonių nėra viduryje esančio serverio, nėra jokio tarpininko, kuriuo reikėtų pasitikėti. Abiejų elementų kombinacija – tikrinamas vientisumas ir tarpininko nebuvimas – skaitmenine forma atkuria tai, ką keturis šimtmečius kasdien darė raudonas vaškas ant sulankstyto popieriaus.

Pavadinimas

Šis leidinys vadinamas Cuadernos Lacre, nes vaško antspaudas nėra istorinis papuošimas, o konkreti techninė savybė: konstrukcijos užtikrinamas tikrinamas vientisumas, be jokio operatoriaus pažado. Kiekvienas serijos straipsnis savo šiuolaikine skaitmenine versija analizuoja tam tikrą šios idėjos dalį: šifravimą, metaduomenis, profesinę paslaptį, ryšių architektūrą, Europos teisinę bazę. Šis pavadinimas taip pat yra būdas priminti, kad konfidencialumas nėra paslauga, kurią samdome, o paties kanalo, kuriuo cirkuliuoja informacija, savybė.

Šaltiniai ir papildomas skaitymas

- Maxwell, M. — *The Wax Tablets of the Mind: Cognitive Studies of Memory and Literacy in Classical Antiquity*, Routledge, 1992 (skyriai apie lentelių ir Mesopotamijos bulių antspaudavimą).
- Daybell, J. — *The Material Letter in Early Modern England: Manuscript Letters and the Culture and Practices of Letter-Writing, 1512-1635*, Palgrave, 2012. Skyriai apie vaško antspaudą kaip vientisumo ir autorystės instrumentą.
- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Moderni vaško antspaudo principo formuluotė: garantijos galuose, ne kanale.

Kitas → Šifruoti nereiškia būti privačiam: ką apie jus sako metaduomenys

Naujausi skaitiniai

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Pasiimkite šį straipsnį su savimi ten, kur jums reikia.

↓ Markdown ↓ Paprastas tekstas ↓ PDF

Failas bus atsisiųstas į jūsų įrenginį. Iš ten galite jį išsaugoti, importuoti į Solo2 arba bendrinti bet kur. Cuadernos nusprendžia ne jūsų naudai dėl paskirties vietos.

Vaško antspaudas · SHA-256 d6dd221f62e498202ae98df40ea45828c075d9ec9d11e1ffe7e5c0de42f56437

ES

Cuadernos Lacre · Menzuri Gestión S.L. leidinys ·
parašė R.Eugenio · redagavo Solo2 komanda.

Ši svetainė nenaudoja slapukų ir neįkelia trečiųjų šalių išteklių. Ji naudoja savarankiškai priglobtą anoniminį lankytojų skaitiklį (Umami, mūsų Europos serveryje) ir minimalų JavaScript kiekį, būtiną jūsų šviesios/tamsios temos pasirinkimui. Jokių seklių, jokio profiliavimo, jokio dalijimosi duomenimis. Jei norite mus sekti: RSS.