Analýza · 16. května 2026

← Předchozí·Další →

Když není nikdo uprostřed

Šifrování toho, co prochází serverem, chrání obsah. Absence serveru uprostřed eliminuje otázku. Není to totéž.

Dva lidé, jeden rozhovor

Když spolu dva lidé mluví tváří v tvář v místnosti, nikdo nemusí slibovat, že nic neslyšel. Neslyšel to, protože tam nebyl. Když si dva lidé podávají papír z ruky do ruky, nikdo uprostřed nemusí přísahat, že ho nečetl. Uprostřed nikdo není.

Většina věcí v každodenním životě funguje právě takto. Nepodepisujeme dohody o mlčenlivosti se vzduchem, který přenáší náš hlas, ani s papírem, který držíme. Soukromí rozhovoru nespočívá na slibu zprostředkovatele, protože žádný zprostředkovatel neexistuje. To je jeden z nejsilnějších způsobů, jak zajistit soukromí: ne proto, že se něco nebo někdo chová dobře, ale proto, že tam nic nebo nikdo není.

Když se rozhovor přesune do digitálního kanálu, situace se standardně mění. Obvyklý model je následující: dva lidé se připojí k serveru, server přijme zprávu, zašifruje ji nebo ji uloží zašifrovanou a doručí ji příjemci. Server je uprostřed. Server může být čestný. Může být auditován. Může fungovat v příznivé jurisdikci a podle přísných zásad ochrany osobních údajů. To vše může být pravda. Ale server je uprostřed.

Rozdíl mezi šifrováním a nesbíráním (druhá část)

V předchozím článku této série tvrdíme, že šifrování obsahu a nesbírání metadat není totéž. Je zde ještě jeden krok dál, který je vhodné jasně formulovat: šifrování toho, co prochází serverem, a absence serveru také není totéž.

První model — server uprostřed, zašifrovaný obsah — chrání obsah před operátorem serveru, jeho pracovníky údržby a externím útočníkem, který by systém kompromitoval. A to je důležité. Ale neodstraňuje to server. Server tam stále je. Stále zpracovává metadata. Stále je to bod, který může obdržet soudní příkaz, legální odposlech, politický tlak nebo bezpečnostní trhlinu. Stále je to bod, který vyžaduje vložení důvěry v někoho.

Druhý model — absence serveru mezi oběma konci — nechrání zašifrovaný obsah lépe: pokud je kryptografie solidní, obsah je chráněn v obou případech. To, co se mění, není obsah. Mění se to, že otázka *„co se děje se serverem?“* přestává mít smysl, protože neexistuje žádný server, na který by se bylo možné ptát.

Důvěra, absence a rozdíl mezi nimi

Důvěra může být zasloužená. Čestné firmy existují. Přísní auditoři existují. Legislativa nakloněná uživateli existuje. Seriózní služby, které svědomitě splňují vše výše uvedené, existují. Důvěra, pokud je udělena operátorovi, který si ji zaslouží, není špatné uspořádání.

But důvěra, i když je pevná, stále zůstává důvěrou. Je to sociální řešení, nikoli technické. Firma může změnit majitele. Jurisdikce může změnit vládu. Zítra může přijít soudní příkaz. Příští měsíc může být objevena nová

zranitelnost. Nic z toho se neděje ze zlé vůle. Děje se to proto, že operátor existuje a vše, co existuje, podléhá nahodilostem světa.

Absence operátora těmto nahodilostem nepodléhá. Soudní příkaz nemůže žádat data od serveru, který neexistuje. Útočník nemůže kompromitovat server, který neexistuje. Změna v politice firmy nemůže ovlivnit data, která tato firma nikdy neměla. Klíčová věta je jednoduchá: data, která neexistují, nelze ztratit.

O legitimním argumentu na straně serveru

Kdo nabízí profesionální messaging se serverem uprostřed, obvykle uvádí tři naprosto platné argumenty. Za prvé, že server je nezbytný k zajištění doručení, když je příjemce odpojen. Za druhé, že šifrování obsahu je robustní a operátor jej tedy nemůže číst. Za třetí, že služba splňuje evropskou legislativu a data jsou chráněna zákonem.

Všechny tři argumenty jsou pravdivé. Žádný z nich nemění podstatu věci. Je pravda, že server umožňuje ukládání zpráv pro odložené doručení; je také pravda, že odložené doručení lze vyřešit jiným způsobem, prostřednictvím protokolů přímé komunikace mezi zařízeními, které jsou zdokonalovány po desetiletí a fungují i dnes. Je pravda, že šifrování obsahu při přenosu je u seriózních služeb robustní. A je pravda, že evropská legislativa chrání uživatele více než v mnoha jiných částech světa.

Otázkou není, zda jsou služby se serverem uprostřed legální, bezpečné nebo zda chrání obsah. Mohou být, jsou legální a obvykle bezpečné. Otázkou je, že mít server uprostřed je architektonická volba, nikoli technická nutnost. A každá volba má své následky. Architektura se serverem uprostřed nutně generuje aktéra, kterému je třeba důvěřovat. Architektura bez serveru uprostřed nikoli.

Co říká zákon a co dělá architektura

GDPR nevyžaduje konkrétní architektonický model. Vyžaduje výsledky: minimalizaci údajů, omezený účel, ochranu od návrhu a standardně, schopnost prokázat soulad. Služba se serverem uprostřed může splnit všechny tyto požadavky. Služba bez serveru uprostřed splňuje několik z nich ze své podstaty, nikoli jen prohlášením. Absolutní minimalizace — nesbírat nic, co není nezbytně nutné k doručení zprávy — je triviální, když neexistuje žádný server, který by mohl něco sbírat.

Pro běžné nesenzitivní použití je architektura se serverem naprosto rozumná a důvěra v seriózního operátora je platným uspořádáním. Pro ostatní případy — ty, které podléhají profesnímu tajemství, ty, které nesou deontologickou odpovědnost, ty, které se týkají zvláště citlivých informací — není absence bodu důvěry luxusem, ale strukturální výhodou.

Pro profesionálního čtenáře

Otázky, které je vhodné si klást u profesionální komunikační služby, již známé z předchozích článků této série, se doplňují o jednu další architektonickou otázku:

1. Šifruje obsah při přenosu? (Pravděpodobně ano.)
2. Generuje a ukládá metadata o tom, s kým mluvím a kdy? (Pravděpodobně ano.)
3. Existuje na cestě mezi mým zařízením a zařízením příjemce server?
4. Pokud existuje: kdo jej provozuje, v jaké jurisdikci a co by se muselo stát, aby vydal údaje o mně?
5. Pokud neexistuje: předchozí otázky nemají předmět.

Rozdíl mezi těmito dvěma kategoriemi není v míře, ale v typu. Když přijde čas to vysvětlit klientovi, pacientovi nebo kolegovi, nejčestnější formulace je zároveň ta nejjednodušší: v jednom případě je někdo uprostřed, ve druhém nikoli.

Tento článek uzavírá úvodní cyklus Cuadernos Lacre. Po probrání šifrování, metadat a profesního tajemství doplňujeme architektonický obraz: šifrování obsahu a absence serveru uprostřed jsou různé věci. Obě mohou být legální; pouze jedna však eliminuje bod důvěry.

Zdroje a další čtení

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Zakládající text principu, podle něhož mají být záruky systému implementovány na koncích, nikoli v prostředním kanálu.
- Nařízení (EU) 2016/679, čl. 25 — záměrná a ve výchozím nastavení provedená ochrana osobních údajů.
- Nařízení (EU) 2016/679, čl. 5.1.c — zásada minimalizace údajů.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Kapitoly o architekturách, které minimalizují sběr dat již svou konstrukcí.

← PředchozíGDPR a profesionální messaging: proč většina porušuje předpisy, aniž by o tom věděla
Další →CUADERNOS_LIST_SCHREMS_TITLE

Nedávné čtení

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Vezměte si tento článek tam, kam potřebujete.

↓ Markdown ↓ Prostý text ↓ PDF

Soubor se stáhne do vašeho zařízení. Odtud si jej můžete uložit, importovat do Solo2 nebo sdílet, kdekoli chcete. Cuadernos za vás o cíli nerozhoduje.

Pečeť · SHA-256 58ee6b216143a4cfa921ce1dbe4933a5924f2b11f4975197fceee2ca10207fc5

Cuadernos Lacre · Publikace Menzuri Gestión S.L. ·
napsal R.Eugenio · rediguje tým Solo2.