وقتی هیچ‌کس در میان نیست

رمزگذاری آنچه از یک سرور عبور می‌کند از محتوا محافظت می‌کند. نداشتن سرور در میان، صورت مسئله را پاک می‌کند. این دو یکی نیستند.

دو نفر، یک گفتگو

وقتی دو نفر در یک اتاق رو در رو صحبت می‌کنند، هیچ‌کس مجبور نیست قول بدهد که چیزی نشنیده است. او نشنید چون آنجا نبود. وقتی دو نفر کاغذی را دست به دست می‌کنند، هیچ‌کس در این میان مجبور نیست قسم بخورد که آن را نخوانده است. هیچ‌کس در میان نیست.

بیشتر چیزها در زندگی روزمره به همین شکل عمل می‌کنند. ما نه با هوایی که صدای ما را منتقل می‌کند، و نه با کاغذی که در دست داریم، قرارداد محرمانگی امضا نمی‌کنیم. حریم خصوصی گفتگو بر قول یک واسطه استوار نیست، چون واسطه‌ای وجود ندارد. این یکی از قوی‌ترین اشکال خصوصی بودن است: نه به این دلیل که چیزی یا کسی رفتار خوبی دارد، بلکه به این دلیل که چیزی یا کسی وجود ندارد.

وقتی گفتگو به یک کانال دیجیتال منتقل می‌شود، این موضوع به طور پیش‌فرض تغییر می‌کند. مدل معمول به این صورت است: دو نفر به یک سرور متصل می‌شوند، سرور پیام را دریافت می‌کند، آن را رمزگذاری می‌کند یا به صورت رمزگذاری شده نگه می‌دارد و به گیرنده تحویل می‌دهد. سرور در میان است. سرور می‌تواند صادق باشد. می‌تواند مورد ممیزی قرار گرفته باشد. می‌تواند در یک حوزه قضایی مطلوب و تحت یک سیاست حریم خصوصی سختگیرانه فعالیت کند. همه این‌ها می‌تواند درست باشد. اما سرور در میان است.

تفاوت بین رمزگذاری و عدم جمع‌آوری (قسمت دوم)

در مقاله قبلی از همین مجموعه استدلال کردیم که رمزگذاری محتوا و عدم جمع‌آوری متاداده یکی نیستند. گام دیگری وجود دارد که شایسته است با وضوح بیان شود: رمزگذاری آنچه از یک سرور عبور می‌کند و نداشتن سرور نیز یکی نیستند.

مدل اول - سرور در میان، محتوای رمزگذاری شده - از محتوا در برابر اپراتور سرور، کارکنان تعمیر و نگهداری آن یا مهاجم خارجی که سیستم را به خطر می‌اندازد محافظت می‌کند. و این مهم است. اما سرور را حذف نمی‌کند. سرور همچنان آنجاست. همچنان متاداده‌ها را پردازش می‌کند. همچنان نقطه‌ای است که می‌تواند دستور قضایی، مداخله قانونی، فشار سیاسی یا نشت امنیتی را دریافت کند. همچنان نقطه‌ای است که نیاز به سپردن اعتماد به کسی دارد.

مدل دوم - نبود سرور بین دو انتها - از محتوای رمزگذاری شده بهتر محافظت نمی‌کند: اگر رمزنگاری قوی باشد، محتوا در هر دو مورد محافظت می‌شود. آنچه تغییر می‌کند محتوا نیست. آنچه تغییر می‌کند این است که سوال «*چه بر سر سرور می‌آید؟*» دیگر موضوعیتی ندارد، زیرا سروری وجود ندارد که درباره آن سوال شود.

اعتماد، فقدان، و تفاوت بین این دو

اعتماد می‌تواند به درستی سپرده شده باشد. شرکت‌های صادق وجود دارند. ممیزان دقیق وجود دارند. قوانین مطلوب کاربر وجود دارند. خدمات جدی که با دقت تمام موارد فوق را رعایت می‌کنند وجود دارند. اعتماد، وقتی به اپراتوری که شایسته آن است داده شود، معامله بدی نیست.

اما اعتماد، هر چقدر هم که محکم باشد، همچنان اعتماد است. این یک راه حل اجتماعی است، نه یک راه حل فنی. یک شرکت می‌تواند دست به دست شود. یک حوزه قضایی می‌تواند تغییر حکومت دهد. یک حکم قضایی می‌تواند فردا برسد. یک آسیب‌پذیری جدید می‌تواند ماه آینده کشف شود. هیچ‌کدام از این‌ها از روی بدخواهی اتفاق نمی‌افتد. به این دلیل اتفاق می‌افتد که اپراتور وجود دارد و هر چیزی که وجود دارد در معرض اتفاقات دنیاست.

فقدان یک اپراتور در معرض آن اتفاقات نیست. یک حکم قضایی نمی‌تواند از سروری که وجود ندارد داده‌ای بخواهد. یک مهاجم نمی‌تواند سروری را که وجود ندارد به خطر بیندازد. تغییری در سیاست یک شرکت نمی‌تواند بر داده‌هایی که آن شرکت هرگز نداشته است تأثیر بگذارد. جمله کلیدی ساده است: داده‌هایی که وجود ندارند نمی‌توانند گم شوند.

درباره استدلال مشروع در سمت سرور

کسی که یک سرویس پیام‌رسان حرفه‌ای با سرور در میان ارائه می‌دهد، معمولاً سه استدلال کاملاً معتبر را مطرح می‌کند. اول، اینکه سرور برای تضمین تحویل در زمانی که گیرنده آفلاین است ضروری است. دوم، اینکه رمزگذاری محتوا قوی است و بنابراین اپراتور نمی‌تواند آن را بخواند. سوم، اینکه سرویس با قوانین اروپا مطابقت دارد و داده‌ها توسط قانون محافظت می‌شوند.

هر سه استدلال درست هستند. هیچ‌کدام ماهیت موضوع را تغییر نمی‌دهند. درست است که یک سرور امکان ذخیره پیام‌ها را برای تحویل با تأخیر فراهم می‌کند؛ همچنین درست است که تحویل با تأخیر می‌تواند به روش دیگری، از طریق پروتکل‌های ارتباط مستقیم بین دستگاهی که دهه‌هاست اصلاح شده و امروز عملیاتی هستند، حل شود. درست است که رمزگذاری محتوا در حال انتقال در خدمات جدی قوی است. و درست است که قوانین اروپا بیش از بسیاری از جاهای دیگر از کاربران محافظت می‌کند.

مسئله این نیست که آیا خدمات با سرور در میان قانونی هستند، یا امن هستند، یا از محتوا محافظت می‌کنند. آن‌ها می‌توانند باشند، قانونی هستند و معمولاً امن هستند. مسئله این است که داشتن سرور در میان یک انتخاب معماری است، نه یک تحمیل فنی. و هر انتخاب پیامدهایی دارد. معماری با سرور در میان لزوماً بازیگری را ایجاد می‌کند که باید به او اعتماد کرد. معماری بدون سرور در میان، خیر.

آنچه قانون می‌گوید و آنچه معماری انجام می‌دهد

RGPD مدل معماری خاصی را الزام نمی‌کند. نتایج را می‌طلبد: به حداقل رساندن داده‌ها، هدف محدود، محافظت از طریق طراحی و به طور پیش‌فرض، توانایی اثبات انطباق. یک سرویس با سرور در میان می‌تواند تمام این شرایط را برآورده کند. یک سرویس بدون سرور در میان، چندین مورد از آن‌ها را از طریق ساخت و نه از طریق اظهار، برآورده می‌کند. به حداقل رساندن مطلق - جمع‌آوری نکردن هیچ چیزی که برای تحویل پیام کاملاً ضروری نیست - زمانی که سروری وجود ندارد که بتواند چیزی جمع‌آوری کند، بدیهی است.

برای مصارف روزمره غیرحساس، معماری با سرور کاملاً معقول است و اعتماد به یک اپراتور جدی معامله معتبری است. برای مصارف دیگر - مواردی که شامل رازداری حرفه‌ای قانونی، مسئولیت اخلاقی یا اطلاعات حساس خاص هستند - فقدان یک نقطه اعتماد یک تجمل نیست، بلکه یک مزیت ساختاری است.

برای خواننده حرفه‌ای

سوالاتی که باید در مقابل یک سرویس ارتباطی حرفه‌ای از خود پرسید، که از مقالات قبلی همین مجموعه آشنا هستند، با یک سوال معماری دیگر تکمیل می‌شوند:

1. آیا محتوا را در حال انتقال رمزگذاری می‌کند؟ (احتمالاً بله.)

2. آیا متاداده‌هایی درباره اینکه با چه کسی و چه زمانی صحبت می‌کنم تولید و ذخیره می‌کند؟ (احتمالاً بله.)
3. آیا سروری در مسیر بین دستگاه من و دستگاه گیرنده وجود دارد؟
4. اگر وجود دارد: چه کسی آن را اداره می‌کند، در کدام حوزه قضایی، و چه اتفاقی باید بیفتد تا داده‌هایی درباره من تحویل دهد؟
5. اگر وجود ندارد: سوالات قبلی موضوعیتی ندارند.

تفاوت بین این دو دسته از نظر درجه نیست، بلکه از نظر نوع است. وقتی زمان توضیح دادن آن به یک مشتری، یک بیمار یا یک همکار فرا می‌رسد، صادقانه‌ترین فرمول‌بندی ساده‌ترین هم هست: در یکی کسی در میان است؛ در دیگری، خیر.

این مقاله چرخه اولیه Cuadernos Lacre را می‌بندد. پس از صحبت درباره رمزگذاری، متاداده و رازداری حرفه‌ای، تابلوی معماری را کامل می‌کنیم: رمزگذاری محتوا و نداشتن سرور در میان چیزهای متفاوتی هستند. هر دو می‌توانند قانونی باشند؛ فقط یکی نقطه اعتماد را حذف می‌کند.

منابع و مطالعه بیشتر

- سالتزر، جی. اچ.؛ رید، دی. پی.؛ کلارک، دی. دی. — *End-to-end arguments in system design*، ACM TOCS، ۱۹۸۴. متن بنیادی اصلی که طبق آن تضمین‌های یک سیستم باید در دو انتها اجرا شوند، نه در کانال واسطه.
- مقررات (اتحادیه اروپا) ۲۰۱۶/۶۷۹، ماده ۲۵ — حفاظت از داده‌ها از طریق طراحی و به طور پیش‌فرض.
- مقررات (اتحادیه اروپا) ۲۰۱۶/۶۷۹، ماده ۵.۱.ج — اصل به حداقل رساندن داده‌ها.
- اشنایر، بی. — *Data and Goliath: the hidden battles to collect your data and control your world* (۲۰۱۵)، دبلیو. دبلیو. نورتون. فصل‌های مربوط به معماری‌هایی که جمع‌آوری را از طریق ساخت به حداقل می‌رسانند.

← السابقGDPR و پیام‌رسانی حرفه‌ای: چرا اکثر مردم ندانسته قوانین را نقض می‌کنندالتالي
CUADERNOS_LIST_SCHREMS_TITLE →

قراءات حديثة

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

این مقاله را هر کجا که نیاز دارید همراه خود ببرید.

↓ مارک‌داون ↓ متن ساده ↓ PDF

فایل در دستگاه شما دانلود خواهد شد. از آنجا می‌توانید آن را ذخیره کنید، به Solo2 وارد کنید یا در هر کجا که می‌خواهید به اشتراک بگذارید. Cuadernos مقصد را برای شما تعیین نمی‌کند.

ختم شمعي · SHA-256 6d8a4e2de00c8de90b1977e911680e115d20b2aeb79e3525633a0af0ed08bd4a

Cuadernos Lacre · نشريّة من Menzuri Gestión S.L. ·
كتبها R.Eugenio · حرّرها فريق Solo2.