ویکی‌پدیا
دانشنامهٔ آزاد

مبادله کلید اینترنت

از ویکی‌پدیا، دانشنامهٔ آزاد

در محاسبات، **مبادله کلید اینترنت** (**Internet Key Exchange**، گاهی **IKEv1** یا **IKEv2**، بسته به نسخه) پروتکل مورد استفاده برای راه اندازی یک انجمن امنیتی (SA) در مجموعه پروتکل IPsec است که بر اساس پروتکل اوکلی و ISAKMP ساخته شده‌است.[۱] IKE از گواهینامه‌های X.509 برای تأیید اعتبار استفاده می‌کند - یا از قبل به اشتراک گذاشته شده یا با استفاده از DNS (ترجیحاً با DNSSEC) توزیع شده - و یک مبادله کلید Diffie-Hellman برای تنظیم یک جلسه مشترک مخفی که از آن کلیدهای رمزنگاری گرفته می‌شوند.[۲][۳]

کارگروه مهندسی اینترنت (IETF) در اصل IKE را در نوامبر ۱۹۹۸ در یک سری نشریات (درخواست نظر - RFC) معروف به RFC 2407 ، RFC 2408 و RFC 2409 تعریف کرد:

- RFC 2407 دامنه تفسیر امنیت اینترنت IP برای ISAKMP را تعریف کرد.[۴]
- RFC 2408 انجمن امنیت اینترنت و پروتکل مدیریت کلیدی (ISAKMP) را تعریف کرد.[۵]
- RFC 2409 پروتکل مبادله کلید اینترنت (IKE) را تعریف کرد.[۶]

RFC 4306 در دسامبر 2005 پروتکل IKE را به نسخه دوم (IKEv2) به روز کرد.[۷] RFC 4718 در اکتبر ۲۰۰۶ برخی از جزئیات را روشن کرد.[۸] RFC 5996 این دو سند و توضیحات اضافی را در IKEv2 به روز شده[۹] که در سپتامبر ۲۰۱۰ منتشر شد، ترکیب کرد. به روزرسانی بعدی، این سند را از نسخه پیشنهادی استاندارد به استاندارد اینترنت ، که در اکتبر ۲۰۱۴ به عنوان RFC 7296 منتشر شده‌است، ارتقا داد.

محتویات

معماری

اکثر پیاده‌سازی‌های IPsec شامل یک Daemon IKE است که در فضای کاربر و یک پشته IPsec در هسته اجرا می‌شود که بسته‌های IP واقعی را پردازش می‌کند.
مکانهای فضای کاربر در صورت لزوم دسترسی آسان به ذخیره انبوه شامل اطلاعات پیکربندی مانند آدرس‌های انتهایی IPsec، کلیدها و گواهینامه‌ها دارند. از طرف دیگر ماژول‌های هسته می‌توانند بسته‌ها را به صورت کارآمد و با حداقل سربار پردازش کنند - که به دلایل عملکرد بسیار مهم است.

پروتکل IKE از بسته‌های UDP، معمولاً در پورت ۵۰۰ استفاده می‌کند، و به‌طور کلی برای ایجاد یک SA (انجمن امنیتی) از هر دو طرف به ۴-۶ بسته با ۲-۳ دور سفر نیاز دارد. مواد اصلی مورد مذاکره سپس به پشته IPsec داده می‌شود. به عنوان مثال، این می‌تواند یک کلید AES باشد؛ اطلاعاتی که نقاط پایانی IP و پورت‌هایی را که باید محافظت شوند، و همچنین نوع تونل IPsec ساخته شده را شناسایی می کند. IPsec، به نوبه خود، بسته‌های IP مربوطه را در صورت لزوم رهگیری می‌کند و رمزگذاری / رمزگشایی را طبق نیاز انجام می‌دهد. پیاده‌سازی‌ها بستگی به نحوه عملکرد رهگیری بسته‌ها دارد. مثلاً برخی از دستگاه‌های مجازی استفاده می‌کنند، برخی دیگر برشی را از دیواره آتش می‌گیرند و غیره.

IKEv1 از دو مرحله تشکیل شده‌است: فاز ۱ و فاز 2.[۱۰]

مراحل IKEv1

هدف IKE فاز اول ایجاد کانال ارتباطی معتبر با استفاده از الگوریتم تبادل کلید Diffie-Hellman برای تولید یک کلید مخفی مشترک برای رمزگذاری ارتباطات IKE است. این مذاکره منجر به یک انجمن امنیتی دو جانبه ای (ISAKMP (SA می‌شود.[۱۱] احراز هویت را می‌توان با استفاده از کلید پیش اشتراک شده(راز مشترک)، امضاها یا رمزگذاری کلید عمومی انجام داد.[۱۲] فاز ۱ در حالت اصلی یا حالت تهاجمی عمل می‌کند. حالت اصلی با رمزگذاری آنها، از هویت همتایان و هش کلیدهای مشترک محافظت می‌کند و حالت تهاجمی ندارد.[۱۰]

در فاز دوم IKE، همتایان IKE از کانال ایمن مستقر در فاز ۱ برای مذاکره انجمنهای امنیتی به نمایندگی از سایر خدمات مانند IPsec استفاده می‌کنند. مذاکرات منجر به حداقل دو انجمن امنیتی یک طرفه (یک درون مرزی و یک برون مرزی) می‌شود.[۱۳] فاز ۲ فقط در حالت سریع (Quick Mode) عمل می‌کند.[۱۰]

مشکلات IKE

در اصل، IKE گزینه‌های پیکربندی بی شماری را داشت اما فاقد امکانات کلی برای مذاکره خودکار برای یک مورد پیش فرض شناخته شده‌است که به‌طور جهانی اجرا می‌شود. در نتیجه، هر دو طرف IKE مجبور بودند دقیقاً در مورد نوع انجمن امنیتی که می‌خواستند ایجاد کنند، توافق کنند - گزینه به گزینه - یا امکان ایجاد ارتباط وجود نداشت. عوارض بیشتر ناشی از این واقعیت است که در بسیاری از پیاده‌سازی‌ها، در صورت وجود هرگونه امکانات برای تولید خروجی تشخیصی (diagnostic output)،تفسیر خروجی اشکال زدایی دشوار بود.

مشخصات IKE در حد قابل توجهی از تفسیر واضح بودند؛ محدود بودن به خطاهای طراحی (Dead-Peer-Detection مورد در مورد) و به وجود آوردن پیاده سازی های مختلف IKE به هیچ وجه قادر به ایجاد یک انجمن امنیتی توافق شده برای بسیاری از گزینه ها نیست ، با این حال به درستی پیکربندی شده است و ممکن است در انتهای هرکدام از آنها ظاهر شود.

پیشرفت‌هایی با IKEv2

پروتکل IKEv2 در پیوست RFC 4306 در سال ۲۰۰۵ شرح داده شده و به موضوعات زیر پرداخته شد:

- درخواست برای نظرات کمتر (Fewer RFC): مشخصات IKE حداقل در سه RFC یا بیشتر تحت پوشش قرار می‌گرفت؛ بیشتر از سه RFC اگر یکی از آن ها در حساب گذرگاه NAT و سایر برنامه های افزودنی (Extensions) که به صورت متداول استفاده می شوند، مورد استفاده قرار بگیرد) . IKEv2 اینها را در یک RFC ترکیب می‌کند و همچنین باعث می‌شود پیشرفت‌هایی در پشتیبانی از گذرگاه NAT (برگردان نشانی شبکه (NAT)) و گذرگاه فایروال

به‌طور کلی انجام شود.

- پشتیبانی پویای استاندارد (Standard Mobility support): یک برنامه افزودنی استاندارد برای IKEv2 وجود دارد به نام MOBIKE [rfc:4555 Mobility and Multihoming Protocol] (به IPsec نیز مراجعه کنید) که برای پشتیبانی از پویایی و برای multihoming (برگردان مناسبی برای این کلمه در زبان فارسی نیافتم) آن و کپسوله کردن بار امنیتی(ESP) از آن استفاده می‌شود. با استفاده از این پسوند IKEv2 و IPsec می‌توانند توسط موبایل و کاربران multihomed مورد استفاده قرار گیرند.
- گذرگاه NAT: کپسوله کردن IKE و ESP در پروتکل Datagram User (پورت UDP 4500) این پروتکل‌ها را قادر می‌سازد که از طریق دستگاه یا فایروالی که از برگردانی نشانی شبکه استفاده می کند، عبور کنند.[۱۴]
- پشتیبانی از پروتکل انتقال کنترل جریان: IKEv2 به پروتکل انتقال کنترل جریان نیز مانند پروتکل تلفن اینترنتی (VoIP) اجازه استفاده می دهد.
- تبادل پیام ساده: IKEv2 دارای یک مکانیسم تبادل اولیه چهار-پیام است که IKE هشت مکانیسم مجزای تبادل اولیه متفاوت را ارائه می‌دهد، که هر یک مزایا و معایب اندکی دارند.
- مکانیسم‌های رمزنگاری کمتر: IKEv2 از مکانیزم‌های رمزنگاری برای محافظت از بسته‌های خود که بسیار شبیه به آنچه IPsec ESP برای محافظت از بسته‌های IPsec استفاده می‌کند، استفاده می‌کند. این امر منجر به پیاده‌سازی‌ها و گواهینامه‌های ساده‌تر برای معیارهای مشترک و FIPS 140-2 (استاندارد پردازش اطلاعات فدرال (FIPS)) می‌باشد؛ که هرکدام نیاز به اجرای رمزنگاری به‌طور جداگانه دارد،
- قابلیت اطمینان و مدیریت دولتی: IKEv2 از اعداد توالی و تأییدیه‌هایی برای تأمین اعتبار استفاده می‌کند و برخی از لجستیک‌های پردازش خطا و مدیریت دولت مشترک را موظف می‌کند. IKE به دلیل عدم وجود چنین اقدامات قابل اطمینانی، در جایی که هردو طرف انتظار دیگری را برای شروع عملی داشتند - که هرگز چنین اتفاقی نیفتاده است - می‌تواند در حالت مرده(dead state) به پایان برسد. کار در محیط اطراف (مانند Dead-Peer-Detection) توسعه یافته اما استاندارد نشده‌است. این بدان معنی است که پیاده‌سازی‌های مختلف از محیط کار همیشه سازگار نیست.
- اانعطاف‌پذیری حمله منع سرویس: IKEv2 پردازش زیادی انجام نمی‌دهد تا زمانی که مشخص کند درخواست کننده در واقع وجود دارد یا خیر. این مسئله به برخی از مشکلات DoS رنج می‌برد که IKE باعث پردازش رمزنگاری گران‌قیمت زیادی از مناطق مضراب شده‌است.

با فرض **اینکه HostA** دارای یک شاخص پارامتر امنیتی (SPI) از A و **HostB** دارای SPI B ، سناریو به این شکل است:

```
HostA ---------------------------------------- HostB
|HDR(A,0),sai1,kei,Ni----------------------> |
| <------------------------HDR(A,0),N(cookie)|
|HDR(A,0),N(cookie),sai1,kei,Ni------------> |
| <----------------------HDR(A,B),SAr1,ker,Nr|
```

اگر **HostB** (پاسخ دهنده) در حال تجربه مقادیر زیادی از اتصالات IKE نیمه باز، ان را به پیام پاسخ تکه‌تکه کردن از ارسال IKE_SA_INIT به **HostA** (آغازگر) با یک پیام اطلاع از نوع COOKIE ، و از **HostA** انتظار می رود که یک درخواست IKE_SA_INIT با آن مقدار کوکی را در یک بار اطلاع‌رسانی به **HostB** ارسال کند. این امر برای اطمینان از این است که آیا ابتکار عمل واقعاً قادر به پاسخگویی IKE از پاسخ دهنده است یا خیر.

برنامه‌های افزودنی پروتکل

کارگروه IETF ipsecme تعدادی از برنامه‌های استاندارد را با هدف مدرن سازی پروتکل IKEv2 و تطبیق بهتر آن با محیط‌های با حجم بالا، بطور استاندارد تنظیم کرده‌است. این پسوندها شامل موارد زیر است:

- **از سرگیری جلسه IKE**: امکان از سرگیری یک "جلسه" IKE / IPsec شکست خورده پس از یک شکست، بدون نیاز به طی کل مراحل تنظیم IKE (ارجاع به RFC 5723).
- **تغییر مسیر IKE**: تغییر مسیر درخواستهای IKE ورودی، امکان ایجاد توازن ساده بین چندین نقطه انتهایی IKE(ارجاع به RFC 5685).
- **قابلیت مشاهده ترافیک IPsec**: برچسب زدن ویژه بسته‌های ESP که احراز هویت شده اما رمزگذاری نشده‌اند، با هدف آسان‌تر کردن جعبه‌های میانی (مانند سیستم‌های تشخیص نفوذ) برای تحلیل جریان (RFC 5840).
- **احراز هویت EAP متقابل**: پشتیبانی از **احراز هویت** EAP - تنها (یعنی گواهی کمتر) از هر دو همکار IKE. هدف این است که امکان استفاده از روشهای تأیید هویت مدرن مبتنی بر رمز عبور (RFC 5998) فراهم شود.
- **تشخیص سریع تصادف**: به حداقل رساندن زمان تا زمانی که یک همکار IKE تشخیص دهد که همتای مخالف خود سقوط کرده‌است (RFC 6290).
- **پسوندهای در دسترس بالا**: بهبود هماهنگ سازی پروتکل سطح IKE / IPsec بین خوشه نقاط پایانی IPsec و یک همتای، برای کاهش احتمال اتصالات افت شده پس از یک رویداد عدم موفقیت (RFC 6311).

پیاده‌سازی‌ها

IKE به عنوان بخشی از پیاده‌سازی IPsec در Windows 2000، Windows XP، Windows Server 2003، Windows Vista و Windows Server 2008 پشتیبانی می‌شود.[۱۵] اجرای ISAKMP / IKE به‌طور مشترک توسط سیسکو و مایکروسافت تهیه شده‌است.[۱۶]

چندین پیاده‌سازی منبع باز از IPsec با قابلیت IKE همراه وجود دارد. در لینوکس، پیاده‌سازی Libreswan , Openswan و strongSwan یک Daemon IKE را ارائه می‌دهد که می‌تواند پیکربندی‌های IPSec را با هسته KLIPS یا XFRM / NETKEY پیکربندی کند. XFRM / NETKEY اجرای IPsec بومی لینوکس است که از نسخه ۲٫۶ موجود است.

توزیع نرم‌افزار Berkeley همچنین دارای پیاده‌سازی IPsec و Daemon IKE و از همه مهمتر یک چارچوب رمزنگاری (OpenBSD Cryptographic Framework , OCF) است که پشتیبانی از شتاب‌دهنده‌های رمزنگاری را بسیار ساده‌تر می‌کند. OCF اخیراً به لینوکس منتقل شده‌است.

تعداد قابل توجهی از فروشندگان تجهیزات شبکه، Daemons IKE (و پیاده‌سازی IPsec) خود را ایجاد کرده‌اند، یا یک پشته را از یکدیگر مجوز داده‌اند.

تعدادی از پیاده‌سازی‌های IKEv2 وجود دارد و برخی از شرکت‌هایی که در صدور گواهینامه IPsec و آزمایش قابلیت کارکردن مشغول به کار هستند، شروع به برگزاری کارگاه‌های آزمایش برای آزمایش و همچنین الزامات اخذ گواهینامه به روز شده برای مقابله با آزمایش IKEv2 می‌کنند. آزمایشگاه‌های ICSA (http://www.icsalabs.com/) آخرین مارس کارگاه

قابلیت همکاری IKEv2 خود را در اورلاندو، فلوریدا در مارس ۲۰۰۷ با ۱۳ فروشنده از سراسر جهان برگزار کرد.

پیاده‌سازی‌های منبع باز زیر IKEv2 در حال حاضر در دسترس هستند:

- OpenIKEv2 (http://sourceforge.net/projects/openikev2)،
- strongSwan،
- لیبرسوان،
- Openswan،
- IKEv2 (http://sourceforge.net/projects/ikev2)،
- Racoon و Racoon2 (http://www.racoon2.wide.ad.jp/w/) بایگانی‌شده (https://web.archive.org/web/20081015044410/http://www.racoon2.wide.ad.jp/w/) در ۱۵-۱۰-۲۰۰۸ توسط Wayback Machine از پروژه KAME،
- iked (http://man.openbsd.org/OpenBSD-current/man8/iked.8) از عاملها پروژه می‌باشد.
- نرم‌افزار Rockhopper VPN (http://rockhoppervpn.sourceforge.net/)

ارائه NSA منتشر شده توسط *Der Spiegel* نشان می‌دهد که IKE به شیوه ای ناشناخته برای رمزگشایی ترافیک IPSec، مانند ISAKMP مورد سوء استفاده قرار می‌گیرد.[۱۷] محققانی که حمله Logjam را کشف کرده‌اند اظهار داشتند که شکستن یک گروه ۱۰۲۴ بیتی Diffie-Hellman باعث شکستن ۶۶٪ سرورهای VPN، ۱۸٪ از میلیون‌ها دامنه HTTPS برتر و ۲۶٪ از سرورهای SSH می‌شود که محققان ادعا می‌کنند مطابق با نشت. این ادعا توسط Eyal Ronen و Adi Shamir در مقاله خود «نقد انتقادی از رازهای بی نقص به جلو»[۱۸] و توسط Paul Wouters از لیبرسوان در مقاله ای «66% VPN در حقیقت شکسته نیستند» رد شد[۱۹]

تنظیمات IPSec VPN که امکان مذاکره در مورد پیکربندی‌های متعدد را فراهم می‌کند، در معرض حملات تخریب مبتنی بر MITM بین تنظیمات ارائه شده، با IKEv1 و IKEv2 قرار می‌گیرند.[۲۰] با تفکیک دقیق سیستم‌های مشتری در نقاط دسترسی به خدمات متعدد با تنظیمات دقیق تر می‌توان از این امر جلوگیری کرد.

هر دو نسخه از استاندارد IKE در هنگام استفاده از رمز ورود آنتروپی پایین مستعد حمله دیکشنری آفلاین هستند. برای IKEv1 این مسئله در مورد حالت اصلی و حالت تهاجمی صادق است.[۲۱][۲۲][۲۳]

جستارهای وابسته

- IPsec
- پروتکل توافق‌نامه کلیدی
- دامنه تفسیر گروهی(GDOI)
- پروتکل KINK
- شبکه کامپیوتری

منابع

۱. The Internet Key Exchange (IKE), RFC 2409, §1 Abstract

۳. *RFC 4322: Opportunistic Encryption* s.ietf.org/html/rfc3129), Internet Engineering Task Force, June 2001, p. 1

۲. *RFC 3129: Requirements for Kerberized Internet Negotiation of Keys* (http://tool

Internet Engineering Task Force, June 2001, p. 5

۴. RFC 2407 The Internet IP Security" Domain of Interpretation for ISAKMP" (http://www.ietf.org/rfc/rfc2407.txt). .(Internet Engineering Task Force (IETF

۵. RFC 2408 Internet Security Association" and Key Management Protocol (ISAKMP)" (http://www.ietf.org/rfc/rfc2408.txt). Internet Engineering Task Force ((IETF.

۶. D. Harkins. "RFC 2409 The Internet Key Exchange (IKE)" (http://www.ietf.org/rfc/rfc2409.txt). Internet Engineering Task Force (IETF).

۷. C. Kaufman (Microsoft) (December 2005). "RFC 4306 Internet Key Exchange (IKEv2) Protocol" (http://www.ietf.org/rfc/rfc4306.txt). Internet Engineering Task Force (IETF).

۸. Eronen, P.; Hoffman, P. (October 2006). "RFC 4718 IKEv2 Clarifications and Implementation Guidelines" (http://www.ietf.org/rfc/rfc4718.txt). Internet Engineering Task Force (IETF).

۹. Kaufman, C.; Hoffman, P.; Nir, Y.; Eronen, P. (September 2010). "RFC 5996 Internet Key Exchange (IKEv2) Protocol" (http://www.ietf.org/rfc/rfc5996.txt). Internet Engineering Task Force ((IETF.

۱۰. RFC 2409 The Internet Key Exchange" (IKE)", Internet Engineering Task Force (IETF), p. 5

۱۱. RFC 2409 The Internet Key Exchange" (IKE)", Internet Engineering Task Force (IETF), p. 6

۱۲. RFC 2409 The Internet Key Exchange" (IKE)", Internet Engineering Task Force (IETF), p. 10-16

۱۳. RFC 4306 Internet Key Exchange" (IKEv2) Protocol", Internet Engineering Task Force (IETF), p. 11,33

۱۴. RFC 4306: Internet Key Exchange" (IKEv2) Protocol", Internet Engineering Task Force (IETF), p 38-40

۱۵. Internet Key Exchange: Internet Protocol Security (IPsec): Technet (https://technet.microsoft.com/en-us/library/(cc784994(WS.10).aspx

۱۶. Using IPSec in Windows 2000 and XP, Part 1 (http://www.securityfocus.com/infocus/1519)

۱۷. *Fielded Capability: End-to-end VPN SPIN9 Design Review* (http://www.spiegel.de/media/media-35529.pdf) (PDF), NSA via 'Der Spiegel', p. 5

۱۸. Ronen, Eyal; Shamir, Adi (October 2015). "Critical Review of Imperfect Forward Secrecy" (http://www.wisdom.weizmann.ac.il/~eyalro/RonenShamirDhReview.pdf) (PDF).

۱۹. Wouters, Paul (October 2015). "66% of VPN's are not in fact broken" (https://nohats.ca/wordpress/blog/2015/10/17/66-of-vpns-are-not-in-fact-broken/).

۲۰. Bhargavan, Karthikeyan; Brzuska, Christina; Fournet, Cédric; Kohlweiss, Markulf; Zanella-Béguelin, Santiago; Green, Matthew (January 2016). "Downgrade Resilience in Key-Exchange Protocols" (https://eprint.iacr.org/2016/072.pdf) (PDF).

۲۱. Pliam, John (2 October 1999). "Authentication Vulnerabilities in IKE and Xauth with Weak Pre-Shared Secrets" (https://web.archive.org/web/20020610050311/http://www.ima.umn.edu/~pliam/xauth/). *Johns Hopkins University*. Archived from the original (http://skysrv.pha.jhu.edu/~jpliam/ima/xauth/) on 14 April 2002. Retrieved 5 February 2020.

۲۲. McGrew, David (5 July 2011). "Great Cipher, But Where Did You Get That Key" (https://web.archive.org/web/20110709020412/http://blogs.cisco.com/security/great-cipher-but-where-did-you-get-that-key/). *Cisco Blog*. Archived from the original (http://blogs.cisco.com/security/great-cipher-but-where-did-you-get-that-key/) on 9 July 2011. Retrieved 11 February 2020.

۲۳. Felsch, Dennis (August 2018). "The Dangers of Key Reuse: Practical Attacks on IPsec IKE" (https://www.usenix.org/conference/usenixsecurity18/presentation/felsch). *27th USENIX Security Symposium*. Retrieved 11 February 2020.

پیوند به بیرون

- RFC 2407 انجمن امنیت اینترنت و پروتکل مدیریت کلیدی (ISAKMP) (http://www.ietf.org/rfc/rfc2408.txt)، کارگروه مهندسی اینترنت (IETF)
- RFC 2409 تبادل کلید اینترنتی (IKE) (http://www.ietf.org/rfc/rfc2409.txt)، کارگروه مهندسی اینترنت (IETF)
- RFC 7296: پروتکل تبادل کلید اینترنتی نسخه 2 (IKEv2) (http://www.ietf.org/rfc/rfc7296.txt)، کارگروه مهندسی اینترنت (IETF)
- نمای کلی IKE (از سیسکو) (http://www.ciscopress.com/articles/article.asp?p=25474&seqNum=1)
