Rámec zásad odesílatele

W en.wikipedia.org/wiki/Sender_Policy_Framework

> Tento článek **možná obsahuje původní výzkum** . Vylepšete jej prosím ověřením provedených tvrzení a přidáním vložených citací . Výroky obsahující pouze původní výzkum by měly být odstraněny. *(srpen 2019) (Zjistěte, jak a kdy odstranit tuto šablonu zprávy)*

Sender Policy Framework (**SPF**) je metoda ověřování e-mailu určená k detekci padělání adresy odesílatele během doručování e-mailu. [1] Samotný SPF se však omezuje na zjišťování podvrženého tvrzení odesílatele v obálce e-mailu, které se používá, když je e-mail vrácen. [1] Pouze v kombinaci s DMARC jej lze použít k detekci falšování viditelného odesílatele v e-mailech (e-mail spoofing [2]), což je technika často používaná při phishingu a e-mailovém spamu .

SPF umožňuje přijímajícímu poštovnímu serveru kontrolovat během doručování pošty, že e-mail, který tvrdí, že pochází z určité domény, je odeslán z IP adresy autorizované administrátory této domény. **[3]** Seznam autorizovaných odesílacích hostitelů a IP adres pro doménu je zveřejněn v DNS záznamech pro danou doménu.

Sender Policy Framework je definován v RFC 7208 z dubna 2014 jako „navrhovaný standard“. [4]

Historie

První veřejná zmínka o konceptu byla v roce 2000, ale zůstala většinou bez povšimnutí. [5] O tomto konceptu nebyla znovu zmínka, dokud nebyl v roce 2002 zveřejněn první pokus o specifikaci podobnou SPF na IETF „ namedroppers“ mailing listu Danou Valerie Reese, [6].[2].[5] , která o tom nevěděla. z roku 2000 zmínka o nápadu. Hned další den Paul Vixie zveřejnil svou vlastní specifikaci podobnou SPF na stejném seznamu. [7].[5] Tyto příspěvky vzbudily velký zájem, což vedlo k vytvoření IETF Anti-Spam Research Group (ASRG) a jejich mailing listu, kde se myšlenka SPF dále rozvíjela. Mezi návrhy

předloženými ASRG byly „Reverse MX“ (RMX) od Hadmuta Danische a „Designated Mailer Protocol“ (DMP) od Gordona Fecyka. [8]

V červnu 2003 Meng Weng Wong sloučil specifikace RMX a DMP [9] a vyžádal si návrhy od ostatních. Během následujících šesti měsíců bylo provedeno velké množství změn a velká komunita začala pracovat na SPF. [10] Původně SPF znamenalo *Sender Permitted From* a někdy se také nazývalo *SMTP+SPF* ; ale jeho název byl změněn na *Sender Policy Framework* v únoru 2004.

Na začátku roku 2004 IETF vytvořila pracovní skupinu MARID a pokusila se použít SPF a návrh CallerID společnosti Microsoft jako základ pro to, co je nyní známé jako Sender ID ; ale to se zhroutilo kvůli technickým a licenčním konfliktům. [11]

Komunita SPF se vrátila k původní „klasické“ verzi SPF. V červenci 2005 byla tato verze specifikace schválena IESG jako experiment IETF , který pozval komunitu, aby pozorovala SPF během dvou let po zveřejnění. 28. dubna 2006 byl SPF RFC publikován jako experimentální RFC 4408.

V dubnu 2014 IETF zveřejnila SPF v RFC 7208 jako „navrhovaný standard“.

Principy fungování

Další informace: Sender Rewriting Scheme (SRS)
Simple Mail Transfer Protocol umožňuje libovolnému počítači odesílat e-maily, které tvrdí, že jsou z libovolné zdrojové adresy. Toho využívají spameři a podvodníci, kteří často používají padělané e-mailové adresy [12] , což ztěžuje dohledání zprávy zpět k jejímu zdroji a pro spammery je snadné skrýt svou identitu, aby se vyhnuli odpovědnosti. Používá se také v technikách phishingu , kde mohou být uživatelé podvedeni k prozrazení soukromých informací v reakci na e-mail údajně zaslaný organizací, jako je banka.

SPF umožňuje vlastníkovi internetové domény určit, které počítače jsou oprávněny odesílat poštu s adresami z obálky v dané doméně, pomocí záznamů DNS (Domain Name System). Příjemci ověřující informace SPF v záznamech TXT mohou odmítnout zprávy z neautorizovaných zdrojů před tím, než obdrží tělo zprávy. Principy fungování jsou tedy podobné jako u seznamů černých děr založených na DNS (DNSBL), kromě toho, že SPF používá schéma delegování oprávnění systému doménových jmen. Současná praxe vyžaduje použití TXT záznamů, [13]stejně jako rané implementace. Na chvíli byl zaregistrován nový typ záznamu (SPF, typ 99) a zpřístupněn v běžném softwaru DNS. Použití TXT záznamů pro SPF bylo v té době zamýšleno jako přechodný mechanismus. Experimentální RFC, RFC 4408, sekce 3.1.1, navrhl „název domény vyhovující SPF BY MĚL mít SPF záznamy obou typů RR“. [14] Navrhovaný standard, RFC 7208, říká, že „použití alternativních typů DNS RR bylo podporováno v experimentální fázi SPF, ale bylo ukončeno“. [13]

Adresa odesílatele obálky je přenášena na začátku dialogu SMTP. Pokud server odmítne doménu, neautorizovaný klient by měl obdržet zprávu o odmítnutí, a pokud byl tento klient agentem přenosu zpráv (MTA), může být vygenerována zpráva o nedoručení na původní adresu obálky. Pokud server přijme doménu a následně přijme i příjemce a tělo zprávy, měl by do hlavičky zprávy vložit pole Return-Path, aby se adresa obálky uložila. Zatímco adresa v Return-Path se často shoduje s jinými adresami původce v hlavičce pošty, jako je *header-from*nemusí tomu tak být a SPF nezabrání padělání těchto dalších adres, jako je hlavička *odesílatele* .

Spameři mohou odesílat e-maily s výsledkem SPF PASS, pokud mají účet v doméně se zásadami pro odesílatele, nebo zneužívat kompromitovaný systém v této doméně. To však usnadňuje dohledání spammerů.

Hlavní výhoda SPF je pro vlastníky e-mailových adres, které jsou podvrženy v Return-Path. Dostávají velké množství nevyžádaných chybových zpráv a dalších automatických odpovědí. Pokud takoví

příjemci používají SPF ke specifikaci svých legitimních zdrojových IP adres a indikují FAIL výsledek pro všechny ostatní adresy, příjemci kontrolující SPF mohou odmítnout padělky, a tak snížit nebo eliminovat množství zpětného rozptylu .

SPF má potenciální výhody kromě pomoci s identifikací nevyžádané pošty. Konkrétně, pokud odesílatel poskytuje informace SPF, pak mohou příjemci použít výsledky SPF PASS v kombinaci se seznamem povolených k identifikaci známých spolehlivých odesílatelů. Scénáře, jako jsou kompromitované systémy a sdílené odesílání pošty, toto použití omezují.

Důvody k implementaci

Pokud doména publikuje SPF záznam, spammeři a phisheři méně pravděpodobně padělají e-maily, které předstírají, že jsou z této domény, protože padělané e-maily jsou s větší pravděpodobností zachyceny spamovými filtry, které kontrolují SPF záznam. Proto je doména chráněná SPF méně atraktivní pro spammery a phishery. Protože doména chráněná SPF je méně atraktivní jako falešná adresa, je méně pravděpodobné, že bude odmítnuta spamovými filtry, a tak je v konečném důsledku pravděpodobnější, že projde legitimní e-mail z domény. [15]

FAIL a přeposílání

SPF přeruší přeposílání obyčejných zpráv . Když doména publikuje zásady SPF FAIL, legitimní zprávy odeslané příjemcům, kteří předávají jejich poštu třetím stranám, mohou být odmítnuty a/nebo vráceny, pokud nastanou všechny následující skutečnosti:

1. Forwarder nepřepisuje Return-Path , na rozdíl od mailing listů.
2. Další skok nepovolí seznam přeposílání.
3. Tento hop kontroluje SPF.

To je nezbytná a samozřejmá vlastnost SPF – kontroly *za* „hranicí“ MTA (MX) přijímače nemohou fungovat přímo.

Vydavatelé zásad SPF FAIL musí přijmout riziko, že jejich legitimní e-maily budou odmítnuty nebo vráceny. Měli by testovat (např. pomocí zásady SOFTFAIL), dokud nebudou spokojeni s výsledky. Níže naleznete seznam alternativ k prostému přeposílání zpráv.

HELO testy

Pro prázdnou návratovou cestu, jak se používá v chybových zprávách a jiných automatických odpovědích, je kontrola SPF identity HELO povinná.

S falešnou identitou HELO by výsledek NONE nepomohl, ale pro platná jména hostitelů SPF také chrání identitu HELO. Tato funkce SPF byla vždy podporována jako možnost pro přijímače a pozdější návrhy SPF včetně konečné specifikace doporučují vždy zkontrolovat HELO.

To umožňuje příjemcům zařadit do seznamu odesílající mailery na základě HELO PASS nebo odmítnout všechny maily po HELO FAIL. Může být také použit v systémech reputace (jakýkoli seznam povolení nebo zakázání je jednoduchý případ systému reputace).

Implementace

Soulad s SPF se skládá ze tří volně souvisejících úkolů:

- **Publikování zásad** : Domény a hostitelé identifikují počítače oprávněné odesílat e-maily jejich jménem. Dělají to přidáním dalších záznamů ke svým stávajícím informacím DNS: každý název domény nebo hostitel, který má záznam A nebo MX , by měl mít záznam SPF určující zásady, pokud je použit buď v e-mailové adrese nebo jako argument HELO/EHLO. Hostitelé, kteří neodesílají poštu, by měli mít zveřejněný záznam SPF, který to označuje ("v=spf1 -all").
- **Kontrola a používání informací SPF** : Přijímače používají běžné dotazy DNS, které jsou obvykle ukládány do mezipaměti pro zvýšení výkonu. Přijímače pak interpretují informace SPF tak, jak jsou specifikovány, a jednají podle výsledku.

- **Revize přeposílání pošty** : Přeposílání prosté pošty není SPF povoleno. Alternativy jsou:
  - Remailing (tj. nahrazení původního odesílatele odesílatelem patřícím do místní domény)
  - Odmítnout (např. odpovědět `551 User not local; please try <user@example.com>`)
  - Seznam povolených na cílovém serveru, aby neodmítl přeposílanou zprávu
  - Sender Rewriting Scheme , složitější mechanismus, který řeší směrování oznámení o nedoručení původnímu odesílateli

Klíčovým problémem v SPF je tedy specifikace nových informací DNS, které nastavují domény a používají příjemci. Níže uvedené záznamy jsou v typické syntaxi DNS, například:

```
"v=spf1 ip4:192.0.2.0/24 ip4:198.51.100.123 a -all"
```

"v=" definuje použitou verzi SPF. Následující slova poskytují *mechanismy* , které lze použít k určení, zda je doména způsobilá k odesílání pošty. "ip4" a "a" určují systémy, které mohou odesílat zprávy pro danou doménu. "-all" na konci určuje, že pokud se předchozí *mechanismy* neshodují, zpráva by měla být odmítnuta.

Mechanismy

Je definováno osm *mechanismů :*

VŠECHNO	Vždy odpovídá; používá se pro výchozí výsledek, jako `-all` pro všechny adresy IP, které se neshodují s předchozími mechanismy.
A	Pokud má název domény záznam adresy (A nebo AAAA), který lze přeložit na adresu odesílatele, bude se shodovat.
IP4	Pokud je odesílatel v daném rozsahu adres IPv4 , shodujte se.
IP6	Pokud je odesílatel v daném rozsahu adres IPv6 , shodujte se.
MX	Pokud má doménové jméno MX záznam překládaný na adresu odesílatele, bude se shodovat (tj. pošta přichází z některého ze serverů příchozí pošty domény).

PTR	Pokud je doménové jméno (PTR záznam) pro adresu klienta v dané doméně a toto doménové jméno se překládá na adresu klienta (forward-confired reverzní DNS), shodujte se. Tento mechanismus se nedoporučuje a je třeba se mu pokud možno vyhnout. [13]
EXISTUJE	Pokud se daný název domény překládá na jakoukoli adresu, shodujte se (bez ohledu na adresu, na kterou se překládá). To se používá zřídka. Spolu s jazykem maker SPF nabízí složitější shody, jako jsou dotazy DNSBL .
ZAHRNOUT	Odkazuje na politiku jiné domény. Pokud zásady dané domény projdou, tento mechanismus projde. Pokud však zahrnutá zásada selže, zpracování pokračuje. Chcete-li plně delegovat zásady jiné domény, je nutné použít rozšíření *přesměrování* .

Kvalifikace

Každý *mechanismus* lze kombinovat s jedním ze čtyř *kvalifikátorů* :

- `+` pro výsledek PASS. To lze vynechat; např. `+mx` je stejný jako `mx` .
- `?` pro NEUTRÁLNÍ výsledek interpretovaný jako ŽÁDNÝ (žádná politika).
- `~` (tilda) pro SOFTFAIL, pomoc při ladění mezi NEUTRAL a FAIL. Zprávy, které vracejí SOFTFAIL, jsou obvykle přijaty, ale označeny.
- `-` (mínus) pro FAIL by měla být pošta odmítnuta (viz níže).

Modifikátory

Modifikátory umožňují *budoucí* rozšíření rámce. K dnešnímu dni byly široce nasazeny pouze dva *modifikátory* definované v RFC 4408:

- `exp=some.example.com` udává název domény s DNS TXT záznamem (interpretovaným pomocí makrojazyka SPF), aby získal vysvětlení pro výsledky FAIL – obvykle adresu URL, která je přidána do kódu chyby SMTP. Tato funkce se používá zřídka.
- `redirect=some.example.com` lze použít místo *mechanismu* ALL k propojení se záznamem zásad jiné domény. Tento *modifikátor* je srozumitelnější než poněkud podobný *mechanismus* INCLUDE- .

Zpracování chyb

Jakmile implementace SPF zjistí chyby syntaxe v zásadě odesílatele, **musí** přerušit vyhodnocení s výsledkem PERMERROR. Přeskakování chybných *mechanismů* nemůže fungovat podle očekávání, `include:bad.example` a `redirect=bad.example` také způsobit PERMERROR.

Další pojistkou je maximálně deset mechanismů dotazujících se na DNS, tedy jakýkoli mechanismus kromě IP4, IP6 a ALL. Implementace mohou vyhodnocení přerušit s výsledkem TEMPERROR, když to trvá příliš dlouho nebo vyprší časový limit DNS dotazu, nebo mohou pokračovat v předstírání, že dotaz nevrátil žádná data – čemuž se říká „vyhledání neplatnosti“. **Musí** však vrátit PERMERROR, pokud politika přímo nebo nepřímo potřebuje více než deset dotazů na *mechanismy* . Kromě toho **by měli** vrátit PERMERROR, jakmile dojde k více než dvěma "vyhledávání neplatnosti". `redirect=` Do těchto *limitů zpracování* se započítávají i jakékoli . [16]

Typická zásada SPF HELO `v=spf1 a mx ip4:192.0.2.0 -all` může provádět čtyři nebo více DNS dotazů: (1) záznam TXT (typ SPF byl zastaralý podle RFC 7208), (2) A nebo AAAA pro mechanismus `a` , (3) záznam MX a (4+) A nebo AAAA pro každý název MX, pro mechanismus `mx` . Kromě prvního se všechny tyto dotazy započítávají do limitu 10. Pokud má navíc odesílatel např. IPv6 adresu, zatímco jeho jméno a jeho dva MX názvy mají pouze IPv4 adresy, pak vyhodnocení prvních dvou mechanismů již vede k více než dvěma vyhledáváním prázdných míst, a proto PERMERROR. Všimněte si , že mechanismy `ip4` a nepotřebují žádné vyhledávání DNS. `ip6` `all`

Problémy

DNS SPF záznamy

Aby bylo umožněno rychlé testování a nasazení, počáteční verze SPF zkontrolovaly své nastavení v DNS TXT záznamu odesílající domény – i když tento záznam měl být tradičně volně formátovaný text bez připojené sémantiky. [17] Ačkoli v červenci 2005 IANA přidělila SPF specifický Resource Record typ 99, jeho využití nebylo nikdy vysoké a mít dva mechanismy bylo pro uživatele matoucí. V roce 2014 bylo používání tohoto záznamu ukončeno poté, co pracovní skupina SPFbis dospěla k závěru, že *„...významná migrace na typ SPF RR v dohledné době je velmi nepravděpodobná a že nejlepším řešením pro vyřešení tohoto problému interoperability je ukončení podpory Typ SPF RR."* [13]

Omezení záhlaví

Vzhledem k tomu, že SPF stále více brání spammerům ve zfalšování adresy odesílatele obálky, mnozí se přesunuli pouze na zfalšování adresy v poli From v hlavičce e-mailu, které se ve skutečnosti zobrazí příjemci, nikoli pouze zpracováno agentem přenosu zpráv příjemce (MTA) . . SPF (nebo DKIM) však lze použít společně s DMARC , aby bylo možné zkontrolovat také pole From v hlavičce pošty. Toto se nazývá „zarovnání identifikátorů“.

K ochraně proti takovému falšování zobrazovaných jmen jsou vyžadovány vlastní proprietární implementace a nemohou používat SPF. [18] [19] [20]

Nasazení

Antispamový software jako SpamAssassin verze 3.0.0 a ASSP implementují SPF. Mnoho agentů pro přenos pošty (MTA) podporuje SPF přímo, jako je Courier , CommuniGate Pro, Wildcat , MDaemon a Microsoft Exchange , nebo mají k dispozici záplaty nebo zásuvné moduly, které podporují SPF, včetně Postfixu , Sendmailu , Exim , qmail a Qpsmtpd . [21] Od roku 2017 publikuje `-all` zásady SPF FAIL více než osm milionů domén. [22] V průzkumu zveřejněném v roce 2007 5 % `.com` a `.net` domény měly nějakou politiku SPF. Průběžný průzkum v roce 2009 ve společnosti Nokia

Research uvádí, že 51 % testovaných domén specifikuje politiku SPF. [23] Tyto výsledky mohou zahrnovat triviální zásady jako `v=spf1 ? all` . [24] [25]

V dubnu 2007 zveřejnila BITS, divize kulatého stolu finančních služeb, doporučení pro zabezpečení e-mailů pro své členy, včetně nasazení SPF. [26] V roce 2008 zveřejnila pracovní skupina pro ochranu proti zneužívání zpráv (MAAWG) článek o ověřování e-mailů zahrnující SPF, Sender ID a DomainKeys Identified Mail (DKIM). [27] MAAWG ve svých „Sender Best Communication Practices“ uvedl: „Přinejmenším by odesílatelé měli začlenit SPF záznamy pro své poštovní domény“. [28] V roce 2015 pracovní skupina pro ochranu před zneužitím zpráv (MAAWG) revidovala dokument o ověřování e-mailů pokrývající SPF, DomainKeys Identified Mail (DKIM) aDMARC (DMARC). Ve svých revidovaných „Osvědčených postupech pro komunikaci odesílatelů“ MAAWG uvedl: „Ověřování podporuje transparentnost tím, že dále identifikuje odesílatele (odesilatele) zprávy a zároveň přispívá ke snížení nebo odstranění falešných a falešných adres“. [29]

Viz také

Reference

1. ^ Přejít nahoru na: **a b** *Carranza, Pablo (16. července 2013). „Jak používat záznam SPF k zabránění falšování a zlepšení spolehlivosti e-mailu“. DigitalOcean . Archivováno zorigináludne 20. dubna 2015. Staženo 23. září 2019. “Pečlivě přizpůsobený záznam SPF sníží pravděpodobnost podvodného podvržení názvu vaší domény a zabrání tomu, aby byly vaše zprávy označeny jako spam dříve, než se dostanou k vašim příjemcům. E-mail spoofing je vytváření e-mailových zpráv s falešnou adresou odesílatele; něco, co je snadné udělat, protože mnoho poštovních serverů neprovádí ověřování. Spamové a phishingové e-maily obvykle používají takový spoofing, aby uvedly příjemce v omyl ohledně původu zprávy.”*

2. ^ Stav RFC7208
3. ^ psaní jako David Green
4. ^ *Paul, Vixie. "Re: Mail-Transmitter RR" . marc.info . Staženo 15. května 2019 .*
5. ^ *"SPF: Historie/Pre-SPF" . Získáno 16. května 2009 .*
6. ^ Pro srovnání mezi RMX, DMP a SPF viz RMX a DMP srovnání Archived 2008-04-25 na Wayback Machine na historickém openspf webu.
7. ^ *"SPF: Historie/SPF-2003" . Získáno 16. května 2009 .*
8. ^ Wong, M. a W. Schlitt. RFC 4408. Duben 2006 <rfc:4408>
9. ^ *Atkins, Steve (14 března 2016). "SPF: Pravidlo deseti" . wordtothewise.com . Staženo 23. září 2019 .*
10. ^ Steve Bellovin vyjadřuje pochybnosti Archived 2004-04-13 at Wayback Machine (leden 2004)
11. ^ *"SPF-all Domain Survey" . 2017 . Staženo 2017-11-07 .*
12. ^ *Crocker, Dave (březen 2008). "Důvěra v e-mail začíná ověřením" (PDF) . MAAWG. Archivováno z originálu (PDF) dne 29.01.2013 . Získáno 28. 7. 2011 .*

Externí odkazy