

نمودن‌پذیری در شبکه‌های VOIP

مؤلفان:

سعید بختیاری

استاد ارشد دانشگاه علوم انتظامی امین

روینب رستمی

رکاب‌شناس ارشد نرم‌افزار

انتشارات فرهنگ‌شناسی

۱۳۹۷

نفوذناپذیری در شبکه‌های VOIP

مؤلفان: سعید بختیاری، زینب رستمی

صفحه‌آرا: شیرین میرزائی

ناشر: نشر فرهنگ شناسی

شمارگان: ۵۰۰ نسخه

تاریخ انتشار: ۱۳۹۷

نوبت چاپ: اول

قیمت: ۲۰۰ ۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۶۷۲۴-۳۶-۲

mail: farhangshenasi@hctmail.com
www.farhangshenasi.com

آدرس: تهران، خیابان مفتاح مالی، پلاک ۳۶۶، طبقه چهارم، واحد ۱۲.
تلفن: ۰۹۱۰۹۸۰۸۲۱ - ۸۷ ۳۵۴۵۵۱

سرشناسه	بختیاری، سعید،
عنوان و نام پدیدآور	نفوذناپذیری در شبکه‌های VOIP / مؤلفان: سعید بختیاری، زینب رستمی.
مشخصات نشر	تهران: انتشارات فرهنگ شناسی، ۱۳۹۷.
مشخصات ظاهری	۱۹۳ ص: مصور، جدول.
شابک	۹۷۸-۶۰۰-۶۷۲۴-۳۶-۲
وضعیت فهرست نویسی: فیا	شناسه افزوده: رستمی، زینب،
بازداشت	کتابنامه: ص. [۱۸۷] - ۱۹۳.
موضوع	تلفن اینترنتی / Internet telephony
موضوع	پروتکل آغازگر جلسه (پروتکل شبکه کامپیوتری)
موضوع	Session Initiation Protocol (Computer network protocol)
رده بندی کنگره	TK۵۱۰۵/۸۸۶۵/۳ ن ۱۳۹۷
رده بندی دیویی	۶۲۱/۳۸۲۱۲
شماره کتابشناسی ملی	۵۱۲۰۷۷۰

فهرست مطالب

صفحه	عنوان
۱۳	مقدمه
۱۵	فصل نخست: مرور کلی بر ساختار VOIP
۱۵	ویپ VoIP چیست و چگونه کار می کند؟
۱۷	مزایای ویپ (VOIP)
۱۸	امکانات ویپ (VOIP)
۲۰	محدودیت های ویپ (VOIP)
۲۱	اجزا تشکیل دهنده VOIP
۲۲	دروازه PSTN
۲۲	آدرس سرورهای مجزا
۲۲	سرورهای حسابداری و شناسایی و اعلان منجر
۲۵	فصل دوم: پروتکل SIP در ارتباطات VOIP
۲۵	لایه شبکه
۲۶	لایه انتقال
۲۷	لایه اتصال داده
۲۸	لایه فیزیکی
۲۸	پروتکل های VOIP
۴۵	آشنایی با ساختار پروتکل SIP
۵۱	اجزای اصلی شبکه های تلفنی اینترنتی
۵۲	۱. سرور ثبت نام و سرویس موقعیت
۵۶	۲. سرور تغییر مسیر
۵۸	۳. سرور پروکسی
۶۰	سرور پروکسی فرکنینگ

۶۲	 SIP معماری
۶۳	 برخی از معماری‌های امنیتی موجود
۶۴	 sip معماری مثال از
۶۶	 سیگنالینگ SIP
۶۷	 پیام‌های SIP
۶۷	 انواع پیام‌های SIP
۶۹	 سایر از پیام‌های SIP
۷۰	 SIP اعتبارسنجی در
۷۱	 ساروکارهای اعتبارسنجی در SIP
۷۳	 ارتباط امن نقطه به نقطه با استفاده از TLS, IPSec
۷۴	 ارتباط امن انتها به انتها: S/MIME
۷۵	 سازوکار اعتبارسنجی HTTP - Digest
۸۰	 مکانیزم‌های امنیتی پروتکل SIP
۸۰	 اعتبارسنجی خلاصه
۸۱	 اعتبارسنجی شناسه
۸۳	 الحاقات مراسلات اینترنتی ایمن / چندمنظوره (S/MIME)
۸۴	 RTP ایمن
۸۷	 فصل سوم: تهدیدات و خطرات موجود بر روی VOIP
۸۹	 انواع حملات موجود در VOIP
۸۹	 حملات جلوگیری از سرویس
۸۹	 پذیرفتن سرویس
۹۰	 حملات خرابی پهنای باند
۹۰	 حملات سیل invite
۹۰	 حملات سیل UDP
۹۱	 حملات خرابی حافظه
۹۱	 حملات سعی و خطا

۹۱	حمله‌های سیل SYN
۹۱	حمله‌های تراکنش ناقص
۹۲	حمله مرد میانی
۹۲	حمله اختلال در سرویس دهی و اختلال توزیع شده در سرویس دهی
۹۲	پیام‌های بی‌معنی در ویپ
۹۳	حمله کد مخرب
۹۳	حمله دسته‌های ولگرد
۹۳	حمله ازدحام ناگهانی
۹۳	حمله فارمینگ
۹۴	حمله بات نت
۹۴	حمله تلفن ناشناس
۹۵	نفوذ به سیستم کنترل ترافیک Toll Fraud
۹۵	جعل هویت
۹۵	استراق سمع
۹۵	جاسوسی در DHCP
۹۶	ارسال صحیح اطلاعات
۹۶	حالت ناامن
۹۷	روش‌های نفوذ هکرها به شبکه VOIP
۹۷	دسترسی به واسطه‌های سرور وب
۹۷	آسیب‌پذیری به نت ماسک تلفن IP
۹۸	گسترش به آسیب‌پذیری نگاشت آدرس‌های IP
۹۸	حمله تعبیه‌شده سرور TFTP
۹۹	حمله به منبع تغذیه CPU بدون داشتن هیچ اطلاعات اکانت
۹۹	آسیب‌پذیری کلمه عبور پیش فرض
۱۰۰	حمله فریبکاری ARP
۱۰۱	حمله بر روی لایه کاربردی

- ۱۰۱..... بعضی تنظیمات موجود در asterisk
- ۱۰۳..... رمزگذاری در رسانه
- ۱۰۴..... تزریق در Dialplan سیستم‌های ستاره‌ای
- ۱۰۵..... تهدیدهای موجود در SIP برای ایجاد هرز تماس‌ها
- ۱۰۵..... تهدیدهای ناشی از آسیب‌پذیری‌های پروتکل SIP
- ۱۰۶..... ارسال درخواست‌های مبهم به سرور پروکسی
- ۱۰۶..... گوش دادن به آدرس چندبخشی
- ۱۰۷..... سوءاستفاده از آدرس‌های فعال
- ۱۰۷..... ارسال درخواست‌های مبهم به سرور تغییر مسیر
- ۱۰۸..... سوءاستفاده از سرورهای بدون حالت
- ۱۰۸..... سرورهای بدون حالت B2BUA SIP ها
- ۱۰۹..... ارسال پیام به آدرس‌های چندبخشی
- ۱۰۹..... سوءاستفاده از سرورهای پروکسی رکنگ
- ۱۱۰..... سوءاستفاده از فیلدها و بدنه پیام
- ۱۱۲..... سوءاستفاده از امکان ایجاد چندین حساب کاربری
- ۱۱۳..... تهدیدهای ناشی از پیشنهادهای اختیاری پروتکل
- ۱۱۳..... سوءاستفاده از سرورهای ثبت نام
- ۱۱۳..... تهدیدهای ناشی از ارتباط با دیگر پروتکل‌ها
- ۱۱۳..... بهره‌گیری از فرآیندهای خاص تخصیص دامنه
- ۱۱۴..... تهدیدهای ناشی از دیگر ریسک‌های امنیتی
- ۱۱۴..... پایش ترافیک اطراف سرورهای SIP
- ۱۱۴..... پوش پورت‌های شناخته‌شده SIP
- ۱۱۵..... پروکسی میانی
- ۱۱۵..... سوءاستفاده از پیام درخواست re-INVITE
- ۱۱۶..... سوءاستفاده از فیلد record - route
- ۱۱۶..... روش‌های مقابله با هرز تماس‌ها

۱۱۶	۱. روش مبتنی بر شبکه شهرت
۱۱۹	۲. روش مبتنی بر پرداخت هزینه
۱۲۱	۳. جلوگیری از هرز تماس‌ها با استفاده از موجودیت‌های تأییدکننده ناشناس
۱۲۴	۴. اسپایدر
۱۲۸	۵. الگوریتم چند سطحی خاکستری پیوسته (PMG)
۱۲۹	۶. روش بهبودیافته چند سطحی خاکستری پیوسته (E-PMG)
۱۲۹	۷. کاهش هرز تماس‌ها به کمک یک موجودیت لایه شبکه
۱۳۱	۸. روش مبتنی بر تشخیص صدا (VSD)
۱۳۳	۹. روش Decoy
۱۳۴	ارزیابی روش‌های مقابله با هرز تماس‌ها
۱۳۵	انواع حملات بر روی SIP و برخی از راهکارهای موجود
۱۳۵	حملات جلوگیری از سرویس طبقه‌بندی آنها در پروتکل SIP
۱۳۸	حملات پردازنده‌ای در SIP
۱۳۸	حملات تهی‌سازی پردازنده
۱۳۹	حملات مربوط به پیام‌های ناهنجار
۱۳۹	حملات سیل آسا در SIP
۱۴۰	حملات سیل آسا سوءاستفاده از مکانیسم اعتبارسنجی در SIP
۱۴۳	تشخیص حملات اعتبارسنجی
۱۴۳	روش‌های مقابله با حملات سوءاستفاده از اعتبارسنجی در SIP
۱۴۳	روش‌های پیشگیری و مقاوم‌سازی
۱۴۶	روش‌های تشخیص و مقابله‌ای
۱۴۷	تشخیص حملات سیل آسای SIP
۱۴۷	روش‌های مبتنی بر ویژگی
۱۵۰	روش‌های مبتنی بر ماشین حالت
۱۵۱	حملات اختلال در جریان پیام‌های SIP
۱۵۱	تغییر محتوای پیام‌های SIP

۱۵۲	حملات توزیع شده
۱۵۵	فصل چهارم: ملاک‌های ارزیابی روش‌های تشخیص نفوذ در VOIP
۱۵۶	روش‌های کشف نفوذ مبتنی بر کشف ناهنجاری
۱۵۶	روش‌های مبتنی بر تحلیل پروتکل و ماشین حالت
۱۵۹	فصل پنجم: کاهش هرز تماس‌ها در شبکه‌های VOIP
۱۵۹	مقدمه
۱۵۹	اجزای سیستم ضد هرز تماس پیشنهادی
۱۵۹	اعتبارسنجی
۱۶۰	کاهش هرز تماس با به کمک ویژگی‌های موجودیت لایه شبکه
۱۶۱	کاهش هرز تماس‌ها به کمک CAPTCHA
۱۶۳	نحوه رفتار سیستم ضد هرز تماس پیشنهادی
۱۶۵	پیاده‌سازی روش پیشنهادی
۱۶۶	عناصر لازم جهت تولید یک تماس نفوذی
۱۶۷	تولید ترافیک عادی
۱۶۷	مؤلفه‌های ترافیک عادی
۱۶۹	تولید ترافیک هرز تماس
۱۷۰	جمع‌آوری ترافیک عادی و حمله و به دست آوردن ویژگی‌ها
۱۷۱	اندازه‌گیری دقت تشخیص حملات
۱۷۶	تحلیل ROC
۱۷۷	ارزیابی طبقه‌بندی‌های دودویی
۱۷۸	نرم‌افزار متن‌باز SIP
۱۸۰	نرم‌افزار متن‌باز چیست؟
۱۸۰	نرم‌افزار منبع باز چیست؟
۱۸۱	ویژگی‌های نرم‌افزار منبع باز
۱۸۲	مزایای استفاده از نرم‌افزار منبع باز

۱۸۲.....	معایب نرم افزار منبع باز
۱۸۴.....	رابط کاربری پیاده سازی شده سیستم امنیتی SIP
۱۸۶.....	ارزیابی مکانیزم پیشنهادی
۱۸۹.....	منابع و مآخذ

www.ketab.ir

فناوری صوت بر روی پهنای باند اینترنت یا همان VoIP¹ امکان استفاده از اینترنت به منظور مکالمات تلفنی را فراهم می‌کند. در مقابل استفاده از خطوط تلفن سنتی، ویپ از فناوری دیجیتال استفاده می‌کند و نیازمند یک اتصال broadband نظیر DSL است. ویپ از دو جزء اصلی تشکیل شده است: (۱) یک محل صوتی که بر روی شبکه منتقل می‌شود و (۲) سیگنالینگ که جهت برپایی جلسات صوت و مخابراتی بر روی IP به آن نیاز است. این جلسات شامل تماس‌های تلفن اینترنتی، توزیع مولتی‌مدیا و اجلاس‌های مولتی‌مدیا است. به عبارت دیگر پروتکل سیگنالینگ وظیفه ایجاد مدیریت و خاتمه تماس بین دو یا چند رایانه نقطه پایانی طی یک شبکه تلفنی بسته‌ای را برعهده دارد. پروتکل H.232 و پروتکل آغاز نشست SIP دو استاندارد اصلی سیگنالینگ در ویپ هستند. ساختار اصلی یک مکالمه VIOP همانند دیگر برنامه‌های کاربردی مبتنی بر IP، دارای ساختار لایه‌ای OSI است: لایه‌های فیزیکی و داده بر اساس فناوری‌هایی مانند اترنت، ATM، لایه شبکه مبتنی بر IP، لایه انتقال TCP/UDP چون از دست رفتن داده یا خطای کم‌تر چندانی بر روی کیفیت یا کارایی صوت نمی‌گذارد و در عوض انتقال سریع داده از یک نقطه به نقطه انتهایی دارای اهمیت است. پروتکل لایه انتقال در ویپ، UDP است که ترتیب بسته‌های ورودی را کنترل نمی‌کند و کنترل ترتیب صحیح بسته‌ها را برعهده برنامه کاربردی می‌گذارد؛ بنابراین این پروتکل دارای سرعت بالایی است. پروتکل کنترل انتقال TCP را

برای ارتباط سیگنالینگ استفاده می‌کند. همچنین سیستم‌های در لایه ارتباط از پروتکل انتقال بی‌درنگ RTP^۱ بهره می‌برند. لایه‌های ارتباط، نمایش و کاربرد نیز سیگنالینگ مورد نیاز برای یک سیستم ارتباط تلفنی را برقرار می‌سازند. پروتکل SIP که یکی از پرکاربردترین پروتکل‌های وب است در لایه کاربرد است که برای آغاز و پایان یک نشست به صورت انتها به انتها کاربرد دارد.

www.ketab.ir