امنیت سامانه اسپیکرهای تحت شبکه

PERSAVA
IP Based Systems

IP SPEAKER به نسل جدیدی از SPEAKER ها اطلاق می شود که قابلیت کنترل پذیری از طریق شبکه های ذیل را دارا می باشند.

Wi-Fi.۱ LAN .۲ (POE) 3G .۳ 4G .۴

امنیت سامانه :

با توجه به اینکه امنیت یکی از اصلی ترین دغدقه ای فعلی در تمامی سامانه های تحت شبکه می باشد، از سوی کارشناسان شبکه این شرکت تمهیدات گسترده ای برای بستن راه های نفوذ به اسپیکرهای تحت شبکه در نظر گرفته شده است که در ادامه به تشریح آن می پردازیم.

پیاده سازی فایروال (IPV4 & IPV6) بروی هر یک از اسپیکر ها:

در این حالت با تعریف IP Table بروی هر یک از اسپیکرها دسترسی به اسپیکرها برای کلاینت ها و یا PC های غیر مجاز بسته می شود، فقط سرور قابلیت ارتباط مستقیم با هر یک از اسپیکرها را دارا می باشد و حتی ادمین پشتیبانی سامانه هم بعد از ارتباط با سرور و چک شدن دسترسی و مجوزها قابلبت چک کردن اسپیکرها را دارا می باشد.

امنیت VoIP:

رمزنگاری بسته های VoIP :

یکی از روش های امن سازی ارتباطات تلفنی بر روی بسترهای عمومی ، بکارگیری پروتکل های امن همچون پروتکل TLS به منظور امن سازی سیگنالینگ و پروتکل SRTP به منظور محافظت از کانال های صوتی می باشد.

محدود سازی IP های قابلیت ارتباط با سامانه :

فایروال با فیلتر کردن ترافیک های ورودی / خروجی، آدرس های IP و پورت ها، و به صورت کلی با ایجاد یک مانع بر سر راه ترافیک های ورودی، مانع از بروز بسیاری از حملات می گردد.

محدود سازی افرادی که قابلیت تماس با اسپیکر ها را دارند :

در این حالت تنها اشخاصی قابلیت تماس با اسپیکر ها و پخش صوت را دارا می باشند که برای آنها دسترسی ها تعریف شده باشد.

می توان انواع دسترسی برای افراد تعریف کرد به طور مثال مدیر یک منطقه و یا ناحیه از شهر فقط قابلیت تماس با اسپیکرهای منطقه خود را دار باشد و به اسپیکرهای ناحیه و مناطق دیگر دسترسی نداشته باشد.

رمز نگاری (Encrypt) کردن فایل ها و کدها ی اصلی بروی SD Card :

تمامی فایل ها، کدها و تنظیمات اصلی ذخیره شده در SD کارت داخلی Encrypt شده اند و در صورتی که یکی از اسپیکرها به سرقت رود و به صورت غیر مجاز SD کارت بروی کامپیوتر دیگری قرار گیرد قابلیت مشاهده و یا تغییر در کدها موجود نمی باشد.

بررسی عدم تغییر در مدیا ذخیره شده :

یکی از راهای خرابکاری در سامانه، دسترسی غیر مجاز به مدیا های ذخیره شده در SD کارت و تغییر فایل های صوتی ذخیره شده در اسپیکرها می باشد. بدین منظور هر بار که فایلی پخش می گردد ابتدا SHA Checksum فایل صوتی چک می شود که در صورت تغییر در فایل، پخش نخواهد شد.

anti-tamper sensor:

بروی هر یک از اسپیکرها سنسور های شتاب سنج سه محوره قرار گرفته در صورتی هر یک از اسپیکرها جداشده و یا اینکه مورد نفوذ مکانیکی قرار گیرد به سرور اطلاع داده می شود و اسپیکر فوق وارد Blacklist می گردد، تا موضوع بررسی و چک گردد.

استفاده از پروتکل HTTPS برای ارتباطات تحت وب :

تمامی ارتباطات بین کاربرها و سرور امن و تحت پرتکل HTTPS قرار دارد.

اسکن شبکه برای بررسی اضافه شدن دستگاه غیر مجاز :

تمامی اسپیکرها داخل سامانه به طور متداوم اسکن شده و هرگونه قطعی و یا خروج و ورود اسپیکرها چک می شوند و در صورتی که مورد مشکوکی موجود باشد، به مسئول مانیتورینگ سامانه بروی نقشه شهر نشان داده می شود.

به طور مثال با خارج شدن هر یک از اسپیکرها از سامانه، مارکر مربوط به اسپیکر شروع به جهش بروی بروی نقشه می کند.

بکارگیری از روش رمزنگاری WPA2-Enterprise در صورت استفاده از Wi-Fi :

در این روش کلاینت شبکه از طریق یک سرور تائید هویت میشود. برای این کار از EAP و یا RADIUS برای احراز هویت مرکزی کلاینت استفاده شده و از شیوه های مختلف مثل Token card، Kerberos، Certificate و ... برای این کار استفاده میشود. اعتبار ورود به شبکه وایرلس از طرف سرور به کلاینت اختصاص میابد که بواسطه آن مجوز لازم برای اتصال به شبکه وایرلس را پیدا میکند.

در این حالت برخلاف شبکه Wi-Fi خانگی کلید دسترسی برای هریک از اسپیکرها متفاوت می باشد و در صورتی که یکی از اسپیکرها مورد سرقت قرار گیرد فقط همان اسپکر وارد Blacklist می شود، وکلید اتصال به Wi-Fi باقی اسپیکرها در امان می ماند.

بکارگیری از SBC ها برای کنترل و آنالیز کلیه ارتباطات VoIP :

مهم ترین وظیفه ی یک SBC در شبکه VoIP، ایجاد یک لایه امنیتی و حفظ سیستم تلفنی از سوء استفاده توسط هکرها و کلاه برداران تلفنی می باشد. این المان کنترل سیگنالینگ و مدیا را که جهت برقراری یک مکالمه الزامیست، بر عهده دارد. به عبارت دیگر SBC یک B2BUA یا Back to Back User Agents می باشد. درخواست های رسیده درلبه ی بیرونی را دریافت کرده و برای آن ها، یک درخواست جدید در طرف مقابل ایجاد می کند. این قابلیت، به SBC اجازه می دهد تا کلیه ارتباطات VoIP را کنترل و آنالیز کرده و سیاست های امنیتی را به صورت پویا اعمال کند.

تشخیص و جلوگیری از نفوذ :

SBC این قابلیت را دارد که الگوی درخواست های ارسالی را شناسایی کند و مانع از انتقال ترافیک غیر عادی به داخل و یا خارج شبکه گردد. با استفاده از این مکانیزم تشخیص، SBC این قابلیت را دارد تا حملات DoS/DDoS، اسکن SIP Registration و حتی حملات Fuzzing همچون SIP Malformed Packet (ارسال پیام هایی که ساختار درستی ندارند)، را نیز تشخیص دهد و منبع ارسال کننده را مسدود کند.

پنهان سازی توپولوژی(Topology Hiding) :

عبور هر پیام مربوط به پروتکل سیگنالینگ SIP، از المان های مختلف شبکه VoIP، باعث می شود تا فیلدی با عنوان "Via" به آن پیام اضافه گردد. در این صورت، هر پیام در هنگام خروج از شبکه، دارای مجموعه ای از این فیلدهاست

که مسیر طی شده توسط آن پیام را نشان می دهد. این اطلاعات می تواند توپولوژی و ساختار شبکه VoIP را در اختیار نفوذگران قرار دهد. SBC با استفاده از قابلیت B2BUA، این فیلد ها را حذف کرده و فقط یک فیلد "Via" که آدرس خودش را در آن قرار می دهد، درخواست های رسیده را به طرف دیگر منتقل می کند؛ و در نتیجه توپولوژی شبکه VoIP داخلی برای محیط بیرونی، مخفی می ماند.

SBC برای مانیتورینگ:

کنترل ترافیک های ورودی و یا خروجی شبکه VoIP و مانیتورینگ لحظه ای و آنلاین آن ها، از جمله روش هایی است که به منظور برقراری امنیت در شبکه VoIP، بر آن تاکید می شود. متاسفانه بسیاری از سیستم های تلفنی این قابلیت را ندارند و برای مدیران سیستم دشوار است که Log های سیستم را به صورت مداوم چک کنند.

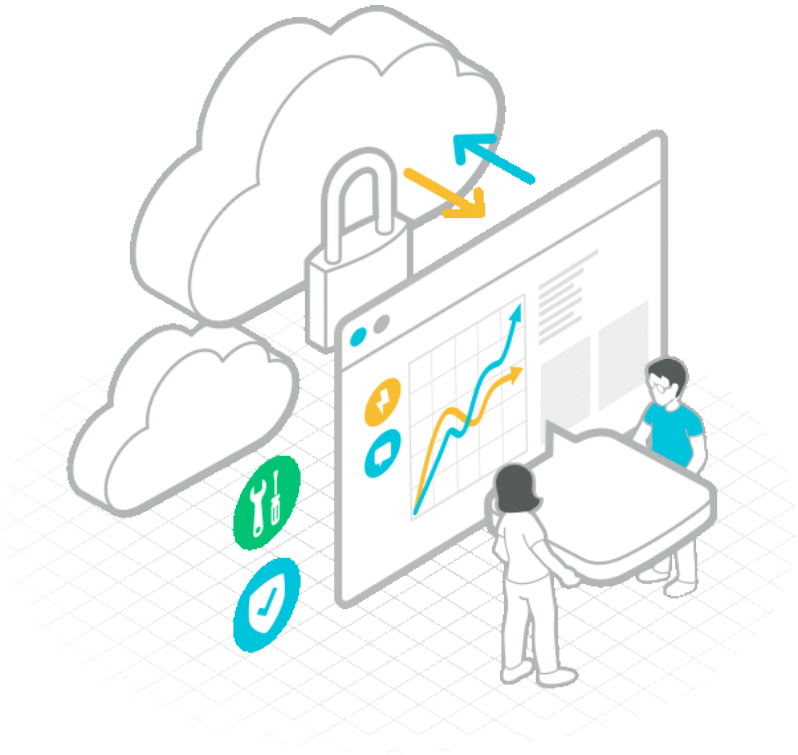
SBC به دلیل عملکرد در لایه های مختلف، این امکان را فراهم می کند تا به صورت آنلاین و در لحظه، بتوان ترافیک صوتی جاری را مانیتور کرد. همچنین با فراهم کردن جزییات تماس (CDR) که قابلیت یکپارچه شدن با سرور Radius را نیز دارد، می توان تماس ها را به صورت دقیق‌تر مورد بررسی قرار داد.

از دیگر امکانات کنترلی که SBC فراهم می کند، گزارشات مربوط به RTCP می باشد. به عبارت دیگر، خروجی این پروتکل کنترلی توسط SBC ثبت شده و آمار مربوطه در اختیار مدیر سیستم قرار داده می شود که با استفاده از آن می توان کیفیت ترافیک را سنجید.

سامانه کنترلی :

سامانه کنترلی یک IoT Cloud Platform است که وظیفه ارسال پکت(Packet) های کنترلی، جمع آوری اطلاعات دریافتی از کلاینت ها (IP Speakers) و بروزرسانی پارمترهای اتصال و امنیتی را برعهده دارد .

Platform فوق از سه سرویس اصلی Control ، Operationو Bootstrapتشکیل شده است.



IoT Cloud Cluster:

درCluster ها مجموعه ای ازسرورها به صورت موازی با یکدیگر کار می کنند تا مجموعه واحد با توان پردازشی و ذخیره اطلاعات بالا را به صورت پایدار تشکیل دهند و قابلیت توسعه با افرایش حجم کلاینت ها (IP Speakers) را فراهم می‌سازند.

Load Balancing:

بار پردازشی ایجاد شده‌ی اسپیکر ها توسط Cluster مدیریت شده و به صورت مساوی بین سرورها تقسیم می گردد، در صورت از کار افتادن یکی از سرورها بار بین باقی سرورها تقسیم می‌شود تا میزان Uptime سامانه افزایش یابد.

سرویس Control :

سرویس Control وظیفه مدیریت اطلاعات کلی را برعهده دارد ، این سرویس فرمان های API توسط رابط کاربری وب و دستگاههای خارجی را پردازش می کند و وظیفه ارسال Notification به سرویس Operations را دارد، این سرویس لیست بروزی از سرویس Operations قابل دسترس را توسط Zookeeper دریافت می‌کند. برای استفاده در حالت Highly Available (در صورتی خرابی یکی از کامپیوترهای سرور کامپیوتر دیگری به صورت موازی سرویس را قابل دسترس نگه می‌دارد) می توان برای کامپیوتر دیگر در Cluster را فعال نمود.

سرویس Operation :

تبادل اطلاعات و همگامی (Synchronization) با اسپیکرها وظیفه این سرویس می باشد، این سرویس توانایی ارتباط با چندین دستگاه به صورت همزمان را دارد پروسس درخواست کلاینت ها (IP Speakers) و ارسال اطلاعات به آنها بین Cluster Node ها را تقسیم می‌کند.

سرویس Bootstrap :

ارسال اطلاعات پارمترهای ارتباطی به اسپیکرها برعهده این سرویس می‌باشد، این پارامترها بر اساس Protocol Stack تعریف شده، می‌تواند شامل IP، TCP Port، Security Credentials و ... می‌باشد.

امنیت Cloud Platform :

در حال شروع ارتباط بین Cloud و کلاینت ها ابتدا توسط پرتکل RSA با کلید ۲۰۴۸ بیتی، کانال امن نامتقارن تشکیل می شود و دسترسی کلاینت به شبکه بررسی می شود در ادامه توسط پرتکل AES کلید ۱۲۸ بیتی تولید و بین طرفین به اشتراک گزارده، Session ایجاد می‌گردد وارتباط با رمزنگاری متقارن برقرار می‌شود.

VPN(Virtual Private Network):

علاوه بر تمامی پروتکل های رمزنگاری فوق، تمامی ارتباطات بین سرورها و کلاینت ها (IP Speakers) داخل یک تونل امن که توسط OPENVPN فراهم می شود قرار دارد که کل سامانه اسپیکرهای تحت شبکه را از باقی کلاینت ها داخل شبکه ایزوله می سازد و تمامی ارتباط را رمزنگاری می کند.

OpenVPN از کتابخانه های رمزنگاری شده ی OpenSSL و پروتکل SSL v3/TLS v1 استفاده می کندو از الگوریتم قدرتمند AES با طول کلید ۲۵۶ بیت برای رمزنگاری استفاده می شود.