نگاهی به نسخه سوم پروتکل SNMP

هومن فروزان

نسخه سوم پروتکل SNMP، با حفظ ماهیت پروتکل قبلی، ویژگی‌های امنیتی و مدیریت از راه دور را به آن افزوده است. از زمان پیدایش پروتکل SNMP نقطه ضعف اصلی آن امنیت پایین این پروتکل بوده است. در نسخه‌های ۱ و ۲ این پروتکل، رمزعبور (Community String) با امنیت بسیار پایین به‌صورت متنی یا به‌صورت Clean Text ارسال می‌شود. ویژگی‌های امنیتی در نسخه سوم پروتکل SNMP به طور کلی تغییر کرده است، هر پیغامSNMP V3 پارامترهای امنیتی خاص خود را داشته که بر اساس مدل امنیتی استفاده شده، از سطوح امنیتی متفاوتی برخوردار می‌باشد.

به طور خلاصه ویژگی‌های جدید اضافه شده به SNMP V3 شامل شناسایی(Authentication)، حفظ تمامیت پیغام (Message Integrity) و کدگذاری (Encryption) است. در SNMP می‌توان مدل‌های امنیتی و سطوح امنیتی تعریف کرد. به یک استراتژی شناسایی که بر ای یک کاربر یا گروهی از کاربران تعریف می‌شود، مدل امنیتی می‌گویند. سطوح امنیتی به معنی سطح امنیت مجاز در یک مدل امنیتی تعریف شده است. ترکیبی از مدل امنیت و سطح امنیت مکانیسم امنیتی را درمورد پیغام‌های SNMP تعیین می‌کند. در SNMP V3 قابلیت اعمال سه مدل امنیتی وجود دارد.

انواع سطوح امنیتی

۱ – سطح امنیتی NoauthNoPriv:

در این سطح امنیتی که پایین‌ترین سطح امنیتی SNMP V3 می‌باشد، شناسایی توسط ایجاد نام کاربری انجام می‌شود. در این سطح امنیتی پیغام‌های SNMP کدگذاری نمی‌شوند.

۲ – سطح امنیتی AuthNoPriv:

در این سطح امنیتی، شناسایی توسط ایجاد نام کاربری و رمزعبور با استفاده از الگوریتم Message Digest 5 یا الگوریتم (Secure Hash SHA) انجام می‌شود. در این سطح امنیتی پیغام‌های SNMP کدگذاری نمی‌شوند.

۳ – سطح امنیتی AuthPriv:

این سطح بالاترین سطح امنیتی SNMP V3 می‌باشد که در آن شناسایی توسط الگوریتم MD5 یا SHA صورت گرفته و کدگذاری پیغام‌های SNMP براساس استاندارد Cipher Block Chaining DES توسط الگوریتم DES 56-bit انجام می‌شود. در این روش کدگذاری، Payload پیغام‌هایSNMP کدگذاری می‌شود. لازم به ذکر است که در نسخه‌های قبلی SNMP تنها سطح امنیتی NoauthNoPriv پشتیبانی می‌شد که شناسایی با استفاده از Community String انجام می‌شد (شکل ۱).

SNMP SECURITY MODEL PER LEVEL

Version	Level	Authentication	Encryption	Process
V1	noAuthNoPriv	Community String	No	Uses a community string match for authentication
V2c	noAuthNoPriv	Community String	No	Uses a community string match for authentication
V3	noAuthNoPriv	Username	No	Uses a username match for authentication
V3	authNoPriv	MD5 or SHA	No	Authenticates based on HMAC-MD5 or HMAC-SHA
V3	authPriv	MD5 or SHA	DES	Same as previous plus 56-bit DES encryption

Based on Chart from http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/snmp3.

شکل ۱

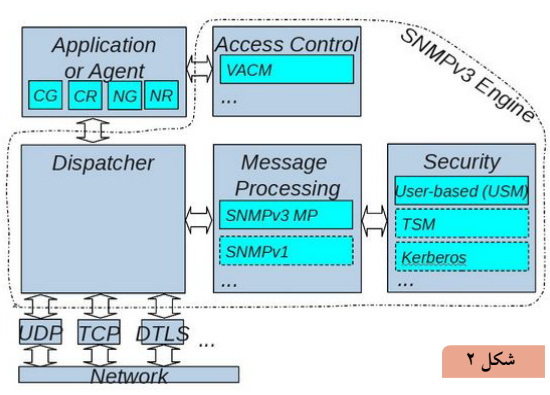
گروه‌های کاربری

- در SNMP V3 هر کاربر (USER) می‌تواند عضو یک گروه باشد.
- در هر گروه می‌توان سیاست‌های دسترسی (Access Policy) جداگانه‌ای درمورد کاربران آن گروه تعریف کرد.
- سیاست دسترسی، اجازه دسترسی خواندن، ایجاد تغییرات و ساختن آبجکت‌های SNMP را تعیین می‌کند
- هر گروه، نحوه دریافت اخطارهای کاربران را مشخص می‌کند
- هر گروه همچنین مدل امنیتی و سطح امنیتی را برای کاربران آن گروه مشخص می‌کند

عملکرد

در SNMP V3، دستگاه‌های SNMP شناسایی می‌شوند تا تبادلات SNMP تنها بین دستگاه‌های مجاز صورت پذیرد. هر دستگاه SNMP یک شناسه منحصر به‌فرد دارد که به آن SNMPEngine ID می‌گویند. تبادلات SNMP تنها در صورتی انجام می‌شود که دستگاه فرستنده SNMP از هویت یا SNMPEngine ID سمت مقابل مطلع باشد. در SNMP V3 طی فرآیند شناسایی، SNMPengine IDهای دستگاه‌های SNMP شناسایی می‌شوند و طی فرآیند همگام‌سازی (Synchronization) شناسایی بین دستگاه‌ها انجام می‌شود.

در SNMP V3 از USM MIBs جهت اعمال فرآیندهای شناسایی و کدگذاری و از VACM MIBs جهت کنترل دسترسی به Objectهای MIB به‌منظور انجام عمکردهای مختلف پس از فرآیند شناسایی استفاده می‌شود (شکل۲).



شکل ۲

اجزای مهم پیغام‌ها

۱ – MsgVersion: در این قسمت ورژن SNMP مشخص است، شماره ۳ مشخص‌کننده SNMP V3 است

۲ – MsgMaxSize: حداکثر حجم پیغام SNMP که یک دستگاه SNMP می‌تواند دریافت کند را مشخص می‌کند.

۳ – MsgFlags: این قسمت سطح امنیتی پیغام را مشخص می‌کند، بیت ۰ نشان‌دهنده شناسایی پیغام است. بیت ۱ مشخص کننده استفاده از کدگذاری است. بیت ۳ مربوط به PDU گزارش‌گیری است.

۴ – MsgSecurityModel: مشخص‌کننده مدل امنیتی است. مقدار ۳ نشان‌دهنده استفاده از USM و کدگذاری است.

۵ – MsgEngineID: در این قسمت شناسه دستگاه SNMP مشخص شده است که در تبادلات SNMP استفاده می‌شود.

۶ – MsgUserName: در این بخش، کاربری که درخواست را ایجادکرده مشخص شده است. قسمت‌های Msgusername و MsgEngine ID جهت شناسایی اطلاعات امنیتی مربوط به پیغام مربوطه از دیتابیس USM استفاده می‌شود.

۷ – msgSecurityParams: در این قسمت، پارامترهای امنیتی مرتبط به مدل‌های امنیتی مشخص است که پارامترهای شناسایی و کدگذاری USM را شامل می‌شود.

۸ – PDU: در SNMP جهت تبادلات بین دستگاه‌های SNMP از PDU (Protocol Data Unit) استفاده می‌شود. PDU انواع مختلفی دارد که شامل تمامی تبادلات SNMP می‌شود، به‌عنوان مثال، از انواع PDU می‌توان ازResponse-PDU، Request-PDU، Trap-PDU و... نام برد.

مثال‌ها

```
snmp-server engineid remote 16.20.11.14 00000063000100a1ac151003
snmp-server enable traps config
snmp-server manager
```

در مثال زیر، کاربر Remoteuser را در گروه Remotegroup می‌سازیم و تنظیم می‌کنیم که trap ها را در مدل امنیتی Noauth بگیرد و گروه Remotegroup را طوری تنظیم می‌کنیم که دسترسی Read و Write داشته باشد:

```
snmp-server group remotegroup v3 noauth read write
snmp-server user remoteuser remotegroup remote 16.20.11.14 v3
snmp-server host 16.20.11.14 informs version 3 noauth remoteuser config
```

در مثال زیر، کاربر Remoteuser را در گروه Remotegroup می‌سازیم و طوری تنظیم می‌کنیم که trap ها را در مدل امنیتی authnopriv بگیرد:

```
snmp-server group remotegroup v3 auth
snmp-server user remoteAuthUser remoteAuthGroup remote 16.20.11.14 v3 auth md5 password1
```

در مثال زیر، کاربر Remoteuser را در گروه Remotegroup می‌سازیم و طوری تنظیم می‌کنیم که trapها را در مدل امنیتی authpriv بگیرد:

```
snmp-server group remotegroup v3 priv
snmp-server user remote PrivUser remotePrivGroup remote 16.20.11.14 v3 auth md5
password1 priv des56 password2
```

مزایا

- در SNMP V3، می‌توان دیتا را از دستگاه‌های SNMP با امنیت بالا و بدون نگرانی از مخدوش شدن و دزدیده شدن محتوای آن جمع آوری کرد
- محتویات در SNMP محرمانه باقی می‌مانند. به‌عنوان مثال، می‌توان پیغام‌های دستوری SNMP که پیکربندی (Config) روتر را تغییر می‌دهند را کدگذاری کرد تا از افشا شدن آن در شبکه جلوگیری کند.
- SNMP V3 در مقابل استراق سمع در تبادلات بین SNMP Engineها محافظت می‌شود.
- در SNMP V3، هویت کاربری که پیغام‌های SNMP را دریافت می‌کند و پیغام‌های دریافتی از جانب او ایجاد می‌شود مشخص است.

معایب

- افزایش بار پردازشی روی روتر به دلیل کد گذاری روش شناسایی و کدگذاری Payload پیغام‌های SNMP و همچنین Header طولانی‌تر و پیچیده‌تر پیغام‌های SNMP V3 نسبت به نسخه‌های قبلی. محاسبات رمزنگاری می‌تواند تا ۲۰ درصد بار CPU را بالا ببرد.
- کند شدن SNMP در صورت استفاده از روش کدگذاری DES
- نیاز به تغییر کل تنظیمات SNMP در تمامی دستگاه‌ها و در نتیجه لزوم صرف زمان زیاد برای پیکربندی دوباره SNMP که شامل دستورات بیشتر نسبت به ورژن‌های قبلی SNMP است.
- با توجه به این‌که تنظیمات جدیدی اعمال می‌شود فرآیند مدیریت، نگه‌داری و عیب‌یابی نسبت به نسخه‌های قبلی SNMP پیچیده‌تر است. در صورتی که مدیریت Community string در نسخه‌های قبلی به مراتب ساده‌تر بود
- لزوم پشتیبانی IOS روتر از قابلیت SNMP V3