قسمت پیاده سازی :

قبل از شروع پیاده سازی لازم است برخی مفاهیم در اسکایتر را تعریف نمود

یک پروتکل امنیتی از مجموعه ای از نقش ها (Role) تشکیل شده است . که این نقش ها توسط عامل ها (Agents ) اجرا می گردند . نقش ها در واقع طرح کلی ای هستند که عامل ها می توانند آنها را انجام دهند . زمانی که یک پروتکل اجرا می گردد نقش ها می توانند چندین بار اجرا گردند ( احتمالا به طور موازی و توسط عامل های مختلف ) ، به هر اجرای تنها از یک نقش یک (Run ) گفته می شود .

اسکایتر از مدل Dolev and Yao استفاده میکند که در این مدل مهاجم دسترسی کامل به شبکه دارد و می تواند از پیام ها جلوگیری کرده و به محتوای آن تا حد امکان دسترسی پیدا کند و همچنین پیام هایی را ساخته و در شبکه تزریق نماید .

اسکایتر از مدل رمز نگاری کامل استفاده می کند . به این معنی که پیام رمز شده تنها در صورتی قابل مشاهده می باشد که کلید رمزگشایی و الگوریتم موجود باشند .

هر نقش می تواند ادعا های امنیتی (Claim ) که برای مدل سازی ویژگی های امنیتی به کار میروند را داشته باشد .

ادعای **Non-injective agreement** : زمانی می گوییم که در یک پروتکل تضمینی وجود دارد که شروع کننده A یک ارتباط **Non-injective agreement** با پاسخگوی B بر روی یک مجموعه ی داده D (متغییر های که در توصیف پروتکل به کارمی روند ) اگر A به عنوان شروع کننده یک Run را ظاهرا با پاسخگوی B به پایان برساند . به طوری که B Run خود را قبلا شروع کرده باشد و پاسخگوی A در آن Run باشد . و دو Agent بر روی تمام اعضای D توافق کنند .

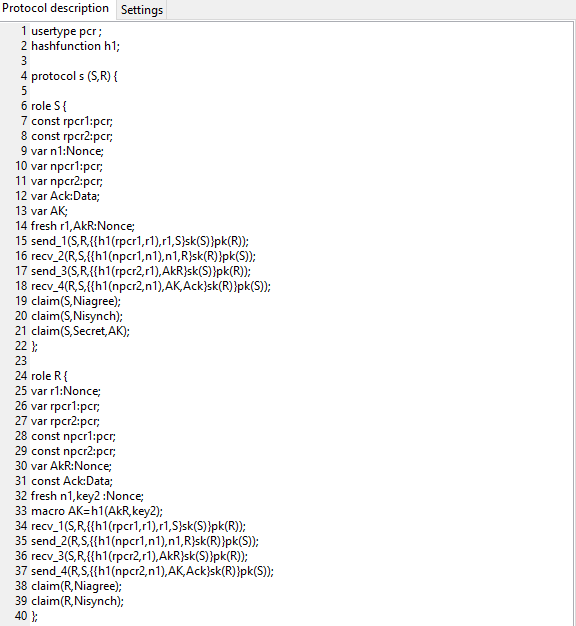
ادعای Secret :این ادعا به عدم دسترسی مهاجم به منبع مورد نظر اشاره می کند . بدین معنی که منبع مورد ادعا برای مهاجم نا مشخص باشد.

ادعای **Non-injective agreement** :بدین معناست که تمام پیام هایی که در نقش R در یافت می گردد . پیام هایی باشند که از طرف شریک ارتباطی R برای شریک ارتباطی دوم یعنی R ارسال شده باشند .

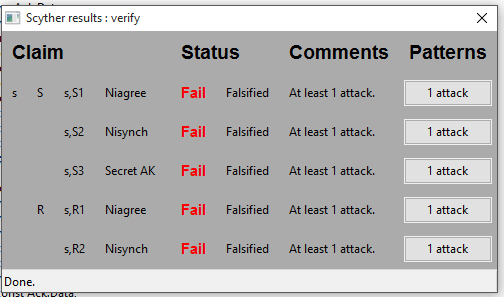
به دلیل اینکه در پروتکل مربوطه اصل چالش به تبادل کلید جلسه بر می گردد .و اگر کلید جلسه بدون هیچ مشکل و تهدید امنیتی منتقل گردد و طرفین به یک توافق بر روی کلید جلسه برسند . دیگر مراحل بعدی به سادگی صورت می گیرد .

بنابر این تنها 4 پیام اول که برای تبادل کلید جلسه و احراز هویت platform ها می باشد را مورد بررسی قرار می دهیم .

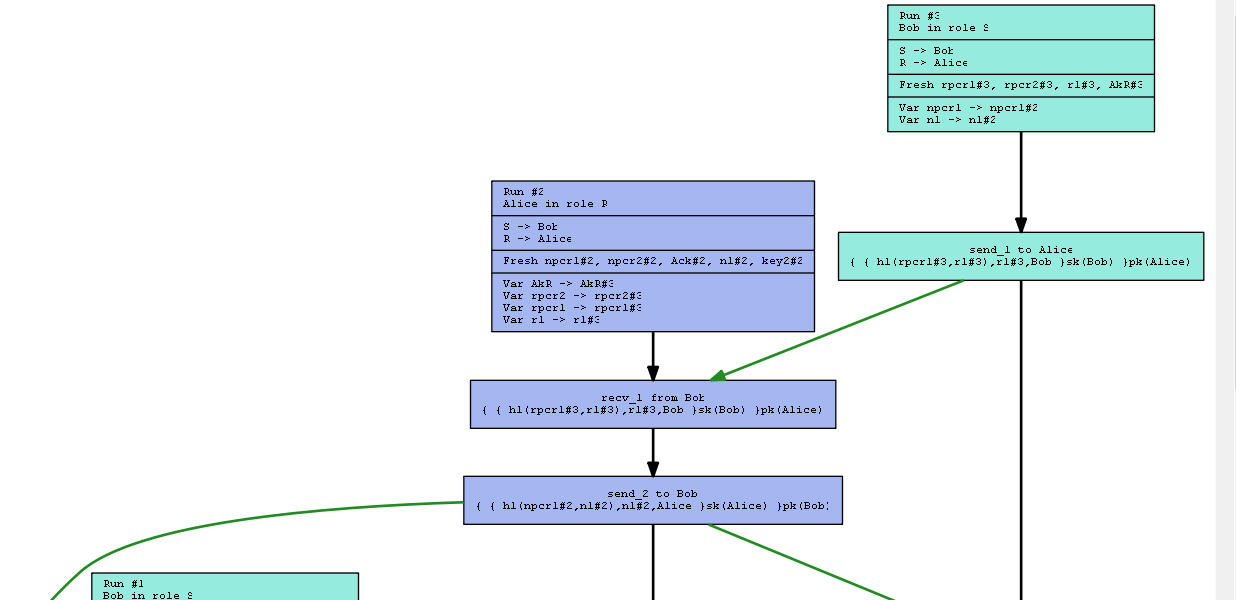
پیاده سازی در اسکایتر :

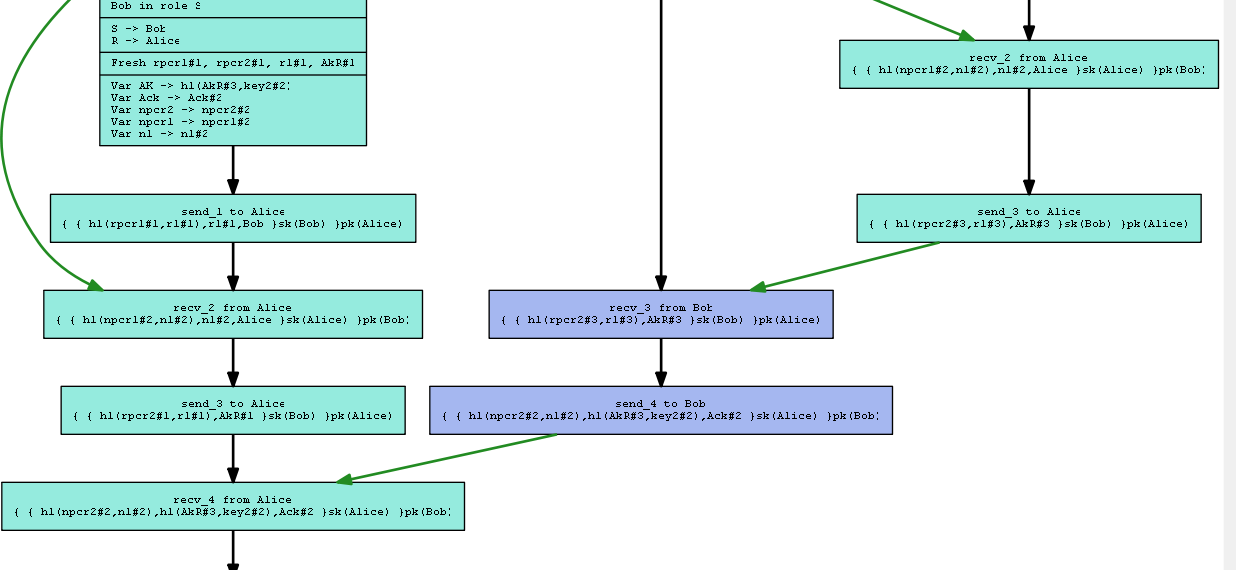


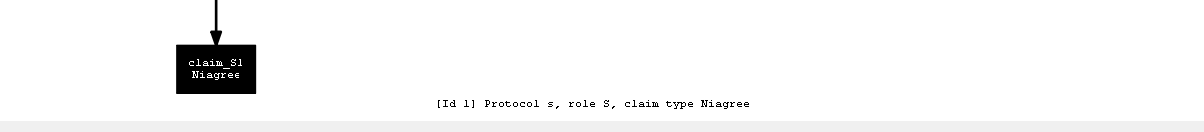
نتیجه ی اجرا :



بررسی حمله اول :





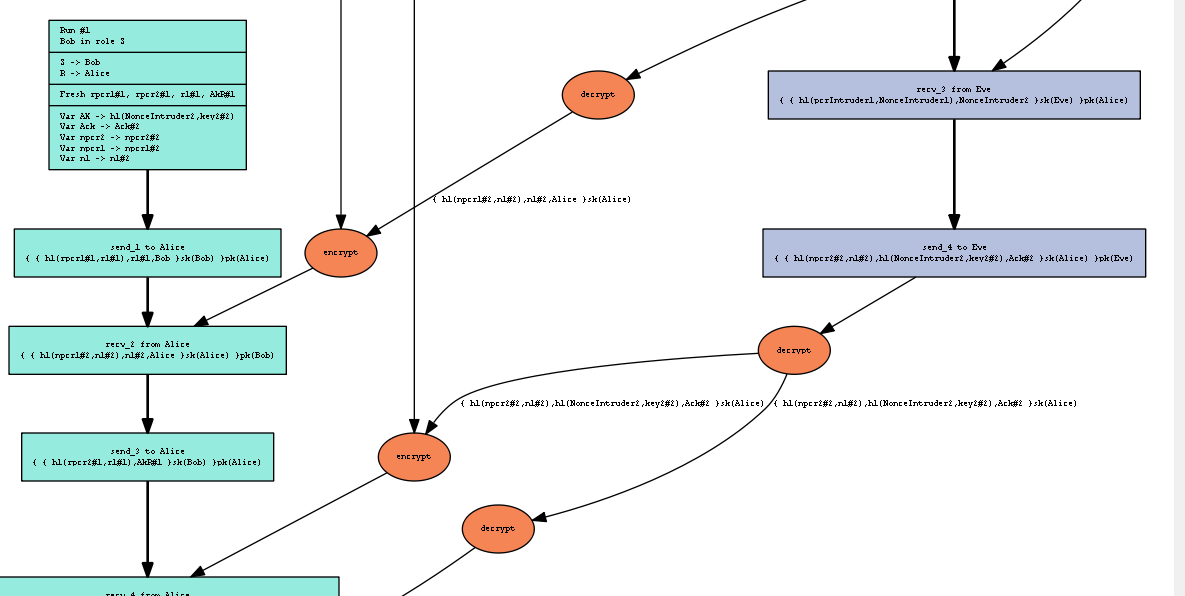
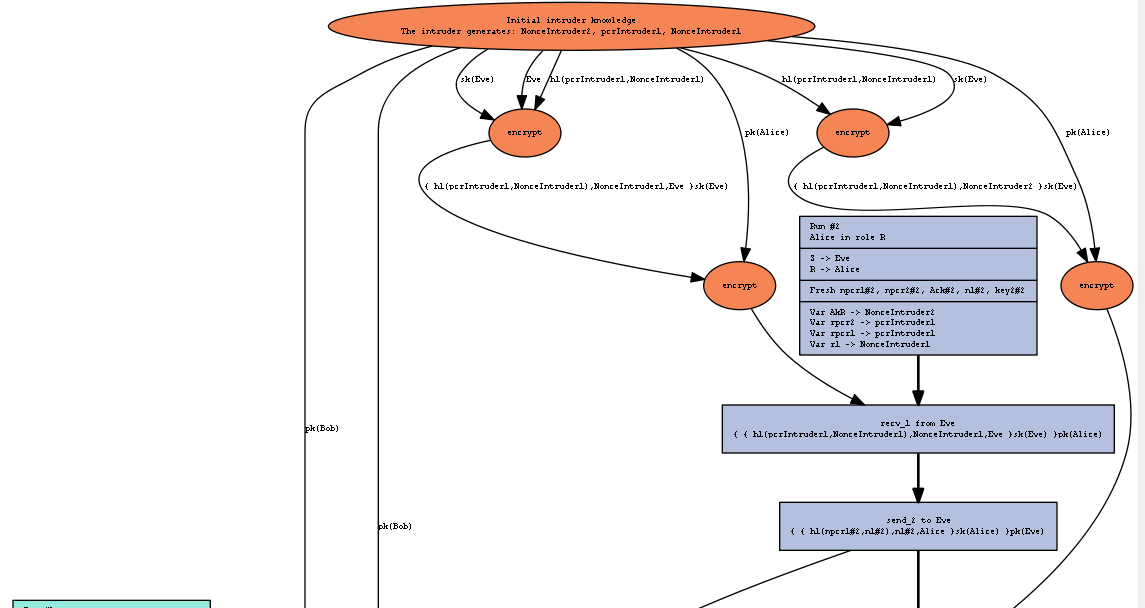


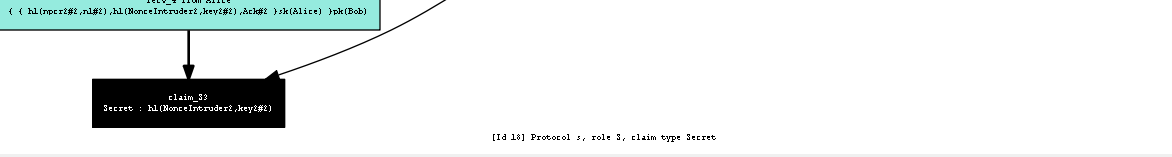
همانطور که در شکل نشان داده شده است . اگر دو Run مختلف از نقش S و یک Run از نقش R اجرا شود ممکن است پیام هایی بین این دو جابه جا گردد و ادعای Niagree و همچنین ادعای Nisych را نیز زیر سوال ببرد .

بررسی حمله دوم :

اگر دو Run از نقش S اجرا گردد پیام ارسال شده ی اول می تواند به همان شکل در recv یک همان نقش دریافت گردد و ادعای Nisynch و همچنین Niagree را زیر سوال ببرد .

بررسی حمله سوم :





همانطور که در این حمله مشاهده می شود intruder (مهاجم) می تواند پیامی را مطابق با recv دو که با کلید خصوصی خودش و کلید عمومی S رمز شده است تولید و برای Alice که در حال اجرای نقش S می باشد ارسال کند . و سپس پیام های ارسالی آلیس را با کلید های خود رمز گشایی و سپس آن را مجددا برای Bob که او در حال اجرای نقش R می باشد .ابتدا با کلید خصوص خود و سپس با کلید عمومی Bob رمز و برای وی ارسال نماید . در نتیجه به این شکل مهاجم می تواند به کلید جلسه دستیابی داشته باشد و محرمانگی آن را زیر سوال ببرد .

بهبود :

علت حملات مطرح شده به این دلیل می باشد که پیام های ارسالی و دریافتی از نظر ساختار مشابه هم می باشد . بنابراین با تغییر پروتکل مطرح شده به شکل زیر می توان از وقوع این حملات جلوگیری نمود .

R -> N:{{Hash(R\_PCR1,NonceR)||NonceR||Plat\_IDR}R-1}NPUB

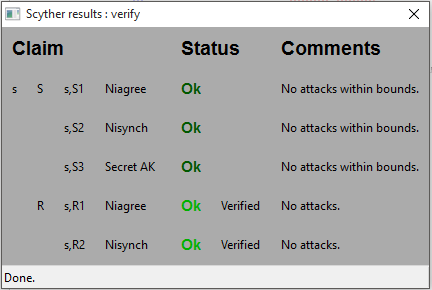
N -> R:{{Hash(N\_PCR1,NonceN)||NonceN|| NonceR||Plat\_IDN}N- 1} RPUB

R -> N:{{Hash(R\_PCR2,NonceR)|| ||NonceN|| NonceR||AKR}R-1}NPUB

N -> R:{{Hash(N\_PCR2,NonceN)||ACK||AK}N-1}RPUB

حال با تغییرات اعمال شده . مجددا پروتکل را در اسکایتر پیاده سازی و اجرا می کنیم .

نتیجه ی اجرا :



نتیجه گیری :

در این مقاله پروتکل مطرح شده برای احراز هویت کنترلر ها در شبکه SDN ، را با ابزار اسکایتر مورد بررسی و حملات موجود در این پروتکل را شرح دادیم و همچنین بهبودی را برای این پروتکل پیشنهاد کرده ایم . که می تواند به عنوان پروتکل احراز هویت در این شبکه ها و برای احراز هویت کنترلر ها مورد استفاده قرار گیرد .

منابعی که من استفاده کردم (به جز منابع خانم رضایی ) و باید به قسمت منابع اضافه شود :

[1] Cas Cremers and Sjouke Mauw. Operational Semantics and Veri\_cation of Security Protocols.

Information Security and Cryptography. Springer, 2012.

[4] G. Lowe. A hierarchy of authentication speci\_cations. In Proc. 10th IEEE Computer Security

Foundations Workshop (CSFW), pages 31{44. IEEE, 1997.

H Yang, [V Oleshchuk](https://scholar.google.com/citations?user=NPnhyvoAAAAJ&hl=en&oi=sra), [A Prinz](https://scholar.google.com/citations?user=IwpfSKUAAAAJ&hl=en&oi=sra) . Verifying Group Authentication Protocols by Scyther Journal of Wireless Mobile Networks, …, 2016 - isyou.info

Scyther Manual