روشي براي تحليل نقش نفوذي در پروتكلهاي رمزنگاري

بهروز ترك لادانی استاديار گروه كامپيوتر، دانشكدة فني و مهندسي، دانشگاه اصفهان
سعيد جليلي استاديار گروه مهندسی كامپيوتر، دانشكدة فني و مهندسي، دانشگاه تربيت مدرس

چكيده

در اين مقاله روشي براي تحليل نقش نفوذي در پروتكلهاي رمزنگاري و كشف خودكار سناريوهاي حمله احتمالي عليه اين پروتكلها ارائـه شده است. در روش ارائه شده، قابليت نفوذي در شنود و بهكارگيري اطلاعات پروتكل و همچنين ايجاد روالهاي جعل نقش در پروتكلهاي احراز اصالت به كمك دانش، قدرت استنتاج و بهكارگيري راهبرد توسط نفوذي مدل شده است. وجود راهبرد در طراحي حمله توسط نفوذي هوشمند در قالب مدل‌سازي توانايي نفوذي در بهكارگيري نمونه‌هاي مختلف اجراي پروتكل به عنوان منبع توليد دانش موردنياز براي انجام حمله، در مدل ارائه شده به خوبي مورداستفاده قرارگرفته است. دو ويژگي مهم در پروتكلهاي رمزنگاري، يعني اختفاي پيامها و اصالت موجوديتها به كمك اين روش قابل تحليل است. تحليل نقش نفوذي در پروتكل احراز اصالت Woo-Lam به كمك روش ارائه شده و چگونگي كشف يك سناريوي حمله عليه آن نيز به عنوان نمونه در اين مقاله ارائه شده است.

كلمات كليدی: پروتكلهاي رمزنگاري, پروتكلهاي احـراز اصـالت, وارسـي صـوري پروتكلهـاي رمزنگـاري, جعـل نقـش در پروتكلهاي احراز اصالت.

Analyzing the Intruder Role in Cryptographic Protocols

B. Tork Ladani Department of Computer Engineering, University of Isfahan
S. Jalili Department of Computer Engineering, Tarbiat Modarres University

Abstract

In this paper a method for analyzing the role of the intruder and automatic exploration of possible attack scenarios in cryptographic protocols is presented. In the presented method, the intruder's capability for eavesdropping the protocol messages and using them to masquerade the protocol principals by means of a set of inference capabilities is modeled. Furthermore, the existence of a proper attack strategy as a general capability of an intelligent intruder for designing the attack scenario is considered in the model. The intruder strategy is based on finding proper instances of the protocol execution as a source of obtaining necessary attack information. Two important properties of the cryptographic protocols (i.e. secrecy and authentication) can be analyzed using the presented method. To show the strength of the presented method, formal specification of the Woo-Lam authentication protocol and the way of finding an attack scenario against it is described as a sample.

Key words: Cryptographic protocols, Authentication protocols, Formal verification, Masquerading.

۱- مقدمه

یکي از اهداف در طراحي پروتکلهاي رمزنگاري, مقاومسازي آنها در برابر عوامل غیر مجازي است که قصد برهمزدن اهداف پروتکل را دارند. براي انجام این کار لازم است پروتکل طراحي شده مورد تحلیل قرار گیرد. روشهاي صوري[1] به صورت وسیعي براي انجام این کار مورد استفاده قرار میگیرند [۱و۲]. این روشها را میتوان به دو دستة روشهاي تحلیل منطقي و روشهاي ساخت حمله تقسیم نمود [۱]. در رویکرد اول، هدف این است که با مدل کردن منطق حاکم بر اجزاء پروتکل (توابع رمزنگاري و روشهای طراحي پروتکل) روشي براي اثبات ایجاد ویژگیهاي امنیتي در پروتکل فراهم گردد. منطقهاي BAN [۳] و GNY [۴] نمونههایي از این روشها هستند. در رویکرد دوم، پروتکل به همراه یك عامل نفوذي در نظر گرفته ميشود و سعي ميشود با مدل کردن این سیستم, راهي براي کشف روالهاي نقض ویژگیهاي امنیتي یافت شود.

در رویکرد ساخت حمله, از دو روش اثبات قضیه[2] و جستجوي فضاي حالت[3] استفاده میشود [۵]. روش اول شامل تعریف بعضي نامتغیرها[4] و اثبات صحیح باقي ماندن آنها در طي گذرهاي وضعیت سیستم است، در حالیکه در روش دوم از Model Checker استفاده ميشود. Model Checker با ایجاد تمامي فضاي حالت ممکن, براي یافتن یك وضعیت ناامن در سیستم (یعني یك حمله) تلاش ميکند. بعضي روشهاي ساخت حمله مثل تحلیلگر NRL [۶] از ترکیب این دو روش نیز استفاده مي کنند. [۶-۱۰] نمونههایي از روشهاي ساخت حمله هستند. در [۵], روشهاي مختلف در این رویکرد، مرور و با یکدیگر مقایسه شدهاند.

بیشتر روشهاي ساخت حمله مبتني بر مجموعهاي از فرضیات انتزاعي مدلسازي هستند که تحت عنوان مدل Doleve-Yao [۱۱] مشهور هستند. در این مدل محاسباتي از پروتکل, پیامها به عنوان مقادیر مجرد غیرقابل تفکیك - و نه دنبالهاي از بیتها- در نظر گرفته میشوند. رمزنگاري در این مدل به صورت ایدهال در نظر گرفته میشود و نفوذي داراي قابلیتهاي ارتباطي و محاسباتي روي روند اجراي پروتکل میباشد. در مقابل، در مورد روشهاي منطقي, مدل محاسباتي پروتکل بیشتر معطوف به بیان وضعیتهاي محلي عوامل پروتکل و توصیف نحوة تغییر آنها در اثر اجراي قدمهاي پروتکل است [۱۲].

در [۱۳] چارچوبي براي بیان روشهاي تحلیل ارائه شده است. این چارچوب داراي چهار مؤلفه است و با Analyze (L,M,PIR,EIR) نشان داده ميشود. L زباني است که از طریق آن ویژگیهاي عوامل مجاز و نفوذي در پروتکل بیان مي شود، M یك مدل محاسباتي از پروتکل و نحوة اجراي آن است، PIR[5] و EIR[6] نیز به ترتیب مجموعه اصول براي انجام استنتاجهاي عوامل مجاز و نفوذي است. توصیف پروتکل در مدل محاسباتي M و اصول لازم در مجموعههاي PIR و EIR به زبان L بیان میشوند. هدف از ارائة چارچوب این است که با تغییر مؤلفههاي L، M، PIR و EIR، بتوان روشهاي تحلیل مختلفي عرضه نمود. در [۱۴] ضمن تحلیل دقیقتر قابلیتها و تواناییهاي چارچوب مذکور, یك تفسیر اجرایي از آن براساس روشهاي بازنویسي[7] ارائه شده است. در [۱۵] نیز, یك روش براي تحلیل منطقي پروتکلهاي رمزنگاري, براساس این چارچوب ارائه شده است. ما در این مقاله با بهکارگیري چارچوب کلي و مدل محاسباتي ارائه شده در [۱۳]، یك روش براي تحلیل نقش نفوذي و ساخت حملات ممکن در روند اجراي پروتکلهاي رمزنگاري ارائه نمودهایم. در این روش, نقش نفوذي در دو حالت غیرفعال و فعال در نظر گرفته ميشود. در تحلیل پروتکل با نفوذي غیرفعال ميتوان ویژگیهاي امنیتي از پروتکل که ممکن است از طریق یك نفوذي غیرفعال نقض شود, مثل ویژگي اختفا[8] را وارسي نمود. نفوذي غیرفعال روي مسیر اجراي پروتکل فقط توانایي شنود دارد و داراي یك مجموعه دانش است که با یك مقدار اولیه شروع مي شود و با شنود پیامهاي پروتکل در روند اجرا و با کمك مجموعه قوانین استنتاج نفوذي (EIR), گسترش مي یابد.

اگر در چارچوب ارائه شده, نفوذي را به صورت فعال در نظر بگیریم, ميتوان حملاتي که از طریق نفوذي فعال امکانپذیر است

1- Formal Methods
2- Theorem Proving
3- State Space Exploration
4- Invariants

5- Principal Inference Rules
6- Eavesdropper Inference Rules
7- Term Rewriting
8- Secrecy

[۷]، مثل حملات تکرار[۱]، انعکاس[۲]و در هم بافي[۳] را تشخیص داد. این حملات عموماً منجر به نقض ویژگي اصالت موجودیت از طریق فریب عامل وارس اصالت مي‌گردد. نفوذي فعال علاوه بر دارا بودن قابلیتهاي نفـوذي غیـرفعال یعنـي شنود پیامهاي پروتکل و گسـترش مجموعـه دانـش خـود با کمك قوانین استنتاجي خود(EIR) , مي‌تواند به صورت فعال نیز وارد پروتکل شود و براساس راهبرد[۴] از پیش تعیین شده، یك یا چند عامل مجاز پروتکل را فریب دهد. یك عامل وقتي فریب مي‌خورد که تصور کند یك ویژگي امنیتي رعایت شده است ولي در عمل با فعالیتهایـي که نفوذي انجام داده است، این ویژگي نقض شده باشد.

در ادامة مقاله، ابتدا چگونگي توصیف صوري پروتکلهاي رمزنگاري به کمك یك زبان توصیف و مدل محاسباتي ارائه شده در [۱۳] به اختصار بیان مي‌شود. سپس چگونگي تحلیل پروتکل با فرض وجود نفوذي غیرفعال و همچنین کشف سناریوهاي حملة جعل نقش علیه پروتکلهاي احراز اصالت با وجود نفوذي فعال بیان مي‌گردد. در ادامه به عنوان نمونه، توصیف و تحلیل پروتکل احراز اصالت Woo-Lam [۱۶] و چگونگي کشف یك سناریوي حمله علیه آن به کمك روش ارائه شده را شرح میدهیم. در پایان نیز نتیجهگیري مطلب ارائه خواهد شد.

۲- توصیف صوري پروتکل

در این قسمت ابتدا یك زبان توصیف نمونه براي توصیف پروتکل و قابلیتهاي نفوذي ارائه میکنیم، سپس به تشریح مختصر مدل محاسباتي مطرح شده در [۱۳] میپردازیم. توصیف پروتکل به کمك این مدل، بستر صوري لازم را براي تحلیل نقش نفوذي فراهم میکند که در بخشهاي بعد به آن میپردازیم.

۲-۱- زبان توصیف L

چون در این مقاله هدف تحلیـل عمل‌کرد نفوذي است، تنها به بیان نمادها و مسندات موردنیاز براي توصیف پروتکل و بیان قابلیتهاي نفوذي (EIR) بسنده میکنیم. گرامر یك زبان ساده براي انجام این کار به همراه برخي توضیحات راجع به مفهوم نمادهاي به کار رفته در شکل (۱) نشان داده شده است.

نمادهاي $\lhd$ و $\ni$ را به ترتیب جهت نشان دادن مسند پیام و مسند مالکیت به کار مي‌بریم. $(P,Q,X)\lhd$ به معناي ارسال پیام X از طرف عامل P به عامل Q و $(P, X)\ni$ به معناي تملك پیام X توسط عامل P است. مسندات $State_i$ نیز مسندات وضعیت هستند.

۲-۲- مدل محاسباتي پروتکل

هر عامل در پروتکل براي انجام صحیح پروتکل نیاز به انجـام یك سري عملیات دارد. ریزترین عملیات پایه‌اي[۵] کـه در یـك پروتکل توسـط یـك عامـل انجـام مـي‌شـود را یـك توانـایي[۶] مـي‌نـامیم. یـك توانـایي داراي دو مؤلفـه اسـت: مجموعـه پیش‌شرطهاي آن توانایي و مجموعه پس‌شـرطهاي آن توانـایي. در صورت فراهم بودن پیـششرطهاي یـك توانـایي، آن توانـایي قابل اجرا است و با اجـراي آن توانـایي، پـس‌شـرطهاي آن نیـز فراهم مي‌شوند. به عبارت دیگر، هر توانـایي بـراي قابـل انجـام بودن نیازمند وجود بعضي شرایط در پروتکل است و در صـورت انجام، ممکن است شرایط را تغییر دهد.

تعریف ۱ (توانایي): دوتـایـي $< pre , post >$ که در آن pre و post هر کدام مجموعه‌اي از دانشها با پارامترهاي متغیر[۷] در زبان L هستند، تشکیل یك توانایي α را مي‌دهند. توانایي α را به صورت ظاهري $L_\alpha : \frac{pre}{post}$ نشان مي‌دهیم که L_α برچسب نام این توانایي است.

pre و post به ترتیب مجموعه پیش‌شرطها و پس‌شرطهاي توانایي هستند. اگر α یك توانایي باشد، از $pre(\alpha)$ و $post(\alpha)$ به ترتیب براي نشان دادن این دو مجموعه استفاده مي‌کنیم. عناصر این دو مجموعه، عباراتي در رابطه با دانش پروتکل (دانش محلي عوامل یا دانش سراسري پروتکل) هستند. در صورت فراهم بودن پیششرطهاي یك توانایي، آن توانایي قابل اجرا است و با اجراي آن توانایي، پس‌شرطهاي آن نیز فراهم مي‌شوند. در ساخت مجموعه‌هاي pre و post بـایستي از دانش قابل تعریف در زبان L استفاده کرد.

1- Replay Attack
2- Reflection Attack
3- Interleaving Attack
4- Strategy

5- Primitive Operation
6- Ability
7- Non-ground

```
Formula ::= X | Y | K |
          (X : Formula,Y: Formula) |          // ليستي شامل X و Y //
          {X:Formula}K :Formula |             // رمز شدة X با كليد K //
          F(X1 : Formula,X2 :Formula , …) |   // يك تابع بازگشتپذير //
          ID ( P : Principals) |              // شناسة عامل P //
          Nonce(X: Formula, P: Principal) |   // نانس X كه توسط عامل P ايجاد شده //
          Shk(P: Principal,Q: Principal)      // كليد مخفي مشترك بين عوامل P و Q //
Principals ::= P |Q |…
Intruders ::= E | I
Predicates::= ◁ (P: Principal, Q: Principal, X: Formula) |   // پيام X از طرف P به Q ارسال شده //
          ∋ (P: Principals, X: Formula) |   // عامل P فرمول X را مالك است. //
          State1 | State2 | …               // مسندات وضعيت //
```

شكل ١- گرامر زبان نمونة L

Send و Receive دو توانايي پايه هستند كه دلالت بر ارسال يا دريافت يك پيام از/ به شبكه دارند. پيش‌شرط توانايي Receive و پس‌شرط توانايي Send بايستي حتماً مشتمل بر دانشهاي يكتاي وضعيت (state) و دانش پيام (◁) باشند. تواناييهاي Send و Receive را مي‌توان به صورت ظاهري زير نشان داد كه در آن مجموعه پيششرط هر توانايي در بالا و مجموعه پسشرطهاي آن در پايين خط قرار گرفته است:

$$\text{Receive}: \frac{\{\lhd (I', R', M'), state_j(\cdots)\}}{\{\cdots\}}$$

$$\text{Send}: \frac{\{\cdots\}}{\{\lhd (I, R, M), state_i(\cdots)\}}$$

پس‌شرط توانايي Send و پيش‌شرط توانايي Receive شامل دانش انتقال پيام و دانش وضعيت هستند. توانايي Send نشان مي‌دهد كه در صورت وجود پيش‌شرطهاي لازم، وضعيت جديدي به وجود خواهد آمد و پيام خاصي مثل M از فرستندة I به گيرندة R ارسال خواهد شد. در مقابل، توانايي Receive به اين معني است كه در صورت به وجود آمدن يك وضعيت مناسب و به شرط انتقال يك پيام روي شبكه، توانايي Receive فعال مي‌شود، مي‌توان آن پيام را دريافت نموده، پس شرطهاي مناسب آن را ايجاد نمود.

تعريف ٢ (قدم): رشته‌اي از تواناييها، نشان‌دهندة يك قدم اجراي پروتكل است. قدم S را به صورت $(\alpha_1. \alpha_2 \ldots \alpha_n)$ نشان مي‌دهيم كه در آن α_1 تا α_n تواناييهاي تشكيل دهندة قدم S هستند.

اگر S يك قدم باشد، از $\alpha_i(S)$ براي رجوع به توانايي i ام قدم S استفاده مي‌كنيم و |S| طول قدم S برحسب تعداد تواناييهاي آن را نشان مي‌دهد. پيش‌شرط اولين توانايي و پس‌شرط آخرين توانايي قدم S به ترتيب نشان‌دهندة ورودي و خروجي قدم S است. ورودي قدم S را با in(S) و خروجي اين قدم را با out(S) نشان مي‌دهيم:

$$in(S) = pre(\alpha_1(S)), \quad out(S) = post(\alpha_{|S|}(S))$$

تواناييهاي اول و آخر قدم S را به ترتيب با first(S) و last(S) نشان مي‌دهيم.

با توجه به ويژگيهاي دو توانايي اصلي Send و Receive، مي‌توان قدمهاي يك پروتكل را به چهار نوع متمايز تقسيم نمود:

- قدم مقداردهي اوليه قدمي است كه نه با توانايي Receive شروع و نه با توانايي Send تمام شود.
- قدم شروع قدمي است كه با توانايي Receive شروع نشود.
- قدم پايان قدمي است كه با توانايي Send تمام نشود.
- قدم واسط قدمي است كه با يك توانايي Receive شروع و با يك توانايي Send تمام شود.

با توجه به مفاهیم قدم و توانایي که در بالا مطـرح شـد، بـراي تکميـل مـدل محاسـباتي پروتکـل بايـستي نحـوة ارتبـاط بـين قدمهاي پروتکل را نيز تعيـين نمـاييم. بـراي ايـنکـار بـراي هـر پروتکل يك مسير اجرا تعريف مي‌کنـيم. مـسير اجـراي پروتکـل حاصل تلفيق نحوي[1] قدمهاي نقشهاي پروتکـل اسـت. سـاخت مسير اجراي يك پروتکل يك فرايند نحوي است بـه ايـن معنـي که براي ايجاد مسير اجرا، قدمهاي مختلف براسـاس يـك سـري ضوابط نحوي با يکديگر مرتبط مي‌شوند و در اين مرحله معنـاي پيش‌شرط و پس‌شرط تواناييهاي هر قدم دخالتي ندارند. دو قدم از پروتکل با يکديگر مرتبط مي‌شوند، اگر دانش پس‌شرط آخرين توانايي يکي از قدمها با دانش پيششرط اولين توانايي قـدم ديگـر قابل انطباق باشد. به عبارت ديگر ضابطة نحوي مورد اسـتفاده در ارتباط قـدمهاي پروتکـل بـا يکـديگر، قابليـت يکـسان‌سـازي[2] دانشهاي پس شرط و پيش‌شرط تواناييهاي اول و آخر آنها است.

تعريف ۳ (قابليت دسترسي قدمها به يکديگر): اگر S_i و S_j دو قدم باشند، S_j از S_i قابل دسترس است اگر تابع جايگذاري[3] مثل θ وجود داشته باشد به صورتيکه $out(S_i)\theta = in(S_j)\theta$، يعني $out(S_i)$ و $in(S_j)$ قابل يکسان‌سازي[4] باشند. در اين حالت S_j قدم بعد از S_i است، يعني $S_j=succ(S_i)$.

تعريف ۴ (نقش): رشتة محدودي از يك سري قدمها يك نقش را تشکيل مي‌دهند. اگر ρ يك نقش به صورت $S_1.S_2\ldots S_m$ باشد، $S_i(\rho)$ نشان دهندة قدم i ام نقش ρ است.

تعريف ۵ (پروتـکل): پروتـکل P يك سـه تـايي بـه صـورت $<\Lambda, S, A>$ است که در آن Λ مجموعة نقشهاي پروتکل است، S مجموعـة قـدمهاي تـشکيل دهنـده ايـن نقـشها و A مجموعـة تواناييهاي تشکيل دهندة قدمها است. اگـر قـدمهاي مقـداردهي اوليه (S_{INIT}) و شروع (S_{START}) در مجموعه قدمهاي يك پروتکل P به کمك يك تابع جايگذاري σ، ground شـوند، بـه ماحـصل يك نمونة پروتکل P به ازاء σ گوئيم و با P_σ نشان مي‌دهيم.

تعريف ۶ (مسير اجراي پروتکل): اگر $P=<\Lambda, S, A>$ يك پروتکل باشد، R(P) مسير اجراي پروتکل P، رشته محدودي از قدمهاي درهم شده از نقشهاي مختلف P است که به صورت زير ساخته مي‌شود:

-قدم اول رشته، قدم مقداردهي اولية پروتکل است (S_{INIT})

-قدم دوم رشته، قدم شروع پروتکل است (S_{START})

-قدمهاي سوم تا آخر اين مسير اجرا، ساير قـدمهاي نقـشهاي Λ هستند، به صورتي که هر قدم از قدم بلافاصـله قبـل از آن قابـل دسترس است.

-هيچ دو قدم پـي‌درپـي در مـسير اجـرا متعلـق بـه يـك نقـش نيستند.

-رعايـت تقـدم و تـأخر قـدمهاي هر نقش، در رشتة اجرا نيز بـه قوت خود باقي است.

مسير اجرايي R(P) را بـه صـورت دقيـق‌تـر مـي‌تـوان چنـين توصيف نمود :

$$R(P) = t_0, t_1, t_2, \ldots, t_n$$
$$t_0 = S_{INIT}$$
$$t_1 = S_{START}$$
$$\forall i \geq 1, \exists \rho', \rho'' \in \Lambda, \exists k', k'', \delta_i \bullet$$
$$S_{k'}(\rho') = t_i, S_{k''}(\rho'') = t_{i+1},$$
$$out(t_i\delta_1\ldots\delta_i) = in(t_{i+1}\delta_1\ldots\delta_i),$$
$$\rho' \neq \rho''$$
$$\forall i, j \exists \rho' \in \Lambda, \exists k', k'' \bullet S_{k'}(\rho') = t_i, S_{k''}(\rho') = t_j,$$
$$k' < k'' \Rightarrow i < j$$

طول يك مسير اجرا را بنا به تعريف برابر تعداد قدمهاي آن در نشان مي‌دهيم. به هر زير رشتة |R(P)|نظر مي‌گيريم و با l، يك پيشوند مسير اجرا با طول 1 با طول R(P)سمت چپ از نشان مي‌دهيم.$R_l(P)$گوييم و با

تعريف ۷ (نشـست پـروتکل): اگـــر P يـــك پروتکل و $R(P) = t_0, t_1, \ldots, t_n$ مسير اجراي پروتکل P باشد، Session(P) نشست پروتـکل P، يـك نمونـة خاص شده از R(P) است که بـــه صورت زير ساخته مي‌شود:

$$Session(P) = t_0.t_1.(t_2\delta_1).(t_3\delta_1\delta_2). \ldots .(t_n\delta_1\ldots\delta_{n-1}),$$
$$\forall i \geq 1,\ out(t_i\delta_1\ldots\delta_i) = in(t_{i+1}\delta_1\ldots\delta_i)$$

اگر P_σ يك نمونة σ از پروتکل P باشد، $Session(P_\sigma)$ را نيز يك نشست نمونة σ از پروتکل P مي‌ناميم.

۳- تحليل پروتکل با فرض وجود نفوذي

در مدل محاسباتي مطرح شده در بخش قبل، مسير اجراي يـك پروتکل را تعريف نموديم. اين مسير اجرا رشته‌اي از قدمهاي مختلف از نقشهاي پروتکل است که از طريق يك رابطـة نحـوي بـا يکـديگر مرتبط شده‌اند. نفوذي با داشـتن بعـضي دانـشهاي اوليـه و قابليتهـا

1- Syntactical
2- Unification
3- Substitution Function
4- Unifiable

مي‌تواند روي مسير اجراي پروتكل دست به انجام استنتاج و گسترش مجموعه دانش خود بزند. به اين ترتيب امكان تحليل عملكرد نفوذي در پروتكل فراهم مي‌شود. به عنوان مثال مي‌توان بررسي نمود كه آيا نفوذي مي‌تواند يك پيام مخفي پروتكل (مثل كليد نشست يا كليد اصلي در يك پروتكل تبادل كليد) را مالك شود يا خير و يا اينكه آيا نفوذي مي‌تواند در يك پروتكل احراز اصالت نقش يك عامل را به گونه‌اي جعل كند كه طرف مقابل هويت نفوذي را به عنوان هويت عامل اصلي بپذيرد. انجام چنين تحليلهايي از طريق تعريف بعضي شرايط روي مسير اجرا و دانش و قابليتهاي نفوذي و بررسي درست بودن يا نبودن آن شرايط قابل انجام است.

قابليتهاي نفوذي براي هر پروتكل مي‌تواند متفاوت باشد ولي به صورت كلي يك نفوذي ميتواند در دو نقش فعال يا غيرفعال در روند پروتكل دخالت كند. نفوذي غيرفعال روي مسير اجراي پروتكل فقط توانايي شنود دارد و ميتواند مجموعه دانش خود را با كمك قوانين استنتاجي گسترش دهد. نفوذي فعال علاوه بر دارا بودن قابليتهاي نفوذي غيرفعال, مي‌تواند به صورت فعال نيز وارد پروتكل شود و براساس راهبرد از پيش تعيين شده، يك يا چند عامل مجاز پروتكل را فريب دهد. در ادامه به بيان قابليتهاي ويژه نفوذي در اين دو نقش و چگونگي بررسي اهداف امنيتي در پروتكلها با توجه به اين قابليتها مي‌پردازيم.

٣-١- قابليتهاي نفوذي غير فعال

نفوذي غيرفعال روي مسير اجراي پروتكل توانايي شنود دارد. براي توصيف قابليتهاي نفوذي در اين حالت، ما يك مجموعه دانش براي نفوذي در نظر مي‌گيريم كه مقدار اوليه آن به عنوان فرضيات اوليه راجع به پروتكل تعيين مي‌شود. به عنوان مثال در يك پروتكل خاص مي‌توان در نظر گرفت كه نفوذي خود يك عامل مجاز شبكه نيز هست و بنابراين داراي كليد مخفي اشتراكي با ديگران (يا زوج كليد عمومي/خصوصي) نيز هست. مجموعه دانش نفوذي حاوي مسندات صحيح راجع به يافته‌هاي نفوذي است. اين مسندات متعلق به زبان L هستند و مقدار اوليه اين مجموعه, دانش پيشفرض نفوذي است. مجموعه دانش نفوذي در طي مسير اجرا با به فعليت رسيدن هر توانايي, باكمك مجموعه EIR به صورت يكنوا گسترش مي‌يابد. در ادامه به تشريح دقيق‌تر اين تعبير از مداخله نفوذي در اجراي پروتكل مي‌پردازيم.

تعريف ٨ (دانش نفوذي غير فعال): اگر P يك پروتكل باشد و r_i قدم i نشست Session(P) از اين پروتكل باشد, دانش نفوذي غير فعال در اين نشست مجموعه‌اي از دانشها در زبان L است كه به صورت زير روي Session(P) گسترش مي‌يابد:

- $K_0(\varepsilon)$ دانش اولية نفوذي است.
- اگر $K_{i-1}(\varepsilon)$ دانش نفوذي غيرفعال بعد از قدم i-1 از نشست پروتكل توسط عوامل مجاز باشد, دانش نفوذي غيرفعال بعد از انجام قدم i برابر خواهد بود با: $K_i(\varepsilon) = K_{i-1}(\varepsilon) \cup out(r_i)$

فرض كنيد دانش نفوذي در قدم n يعني $K_n(\varepsilon)$ را كه در آن n طول مسير اجراي پروتكل است را به صورت ساده با $K(\varepsilon)$ نشان دهيم. مجموعه قابليتهاي پاية نفوذي كه آن را با EIR_B مي‌ناميم را مي‌توان در قالب مجموعه‌اي از اصول منطقي به شكل زير توصيف نمود. از ε براي نشان دادن عامل نفوذي استفاده كرده‌ايم، بقية نمادها نيز نمادهاي تعريف شده در زبان توصيف L هستند (بخش ٢). هر اصل به صورت $\frac{P}{C}$ (L) نشان داده مي‌شود كه در آن P شرط، C نتيجه و L برچسب نام اصل مي‌باشد:

- تجزية پيامها (Message Analysis): اگر نفوذي يك پيام تركيبي داشته باشد مي‌تواند آن را به اجزائش تجزيه كند و اجزاء آن را نيز دارد.

$$\frac{\varepsilon \ni (X,Y) \in K(\varepsilon)}{\varepsilon \ni X \in K(\varepsilon),\ \varepsilon \ni Y \in K(\varepsilon)} \quad (MA)$$

- تركيب پيامها (Message Synthesis): نفوذي مي‌تواند پيامهايي كه دارد را تركيب نموده، مالك پيامهاي تركيبي شود.

$$\frac{\varepsilon \ni X \in K(\varepsilon),\ \varepsilon \ni Y \in K(\varepsilon)}{\varepsilon \ni (X,Y) \in K(\varepsilon)} \quad (MS)$$

- شنود و تملك پيامها (Message Possession): هر پيامي كه روي شبكه قرار گيرد به تملك نفوذي در خواهد آمد.

$$\frac{\triangleleft(X)\in K(\varepsilon)}{\varepsilon \ni X\in K(\varepsilon)}\ (MP)$$

-رمز کردن پیامها (Message Encryption): اگر نفوذي يك پيام و يك كليد داشته باشد، مي‌تواند رمز شدة آن پيام با كليد را نيز مالك شود (براي هر دو سيستم رمز متقارن و غير متقارن).

$$\frac{\varepsilon \ni shk(P,Q)\in K(\varepsilon),\ \ \varepsilon \ni X\in K(\varepsilon)}{\varepsilon \ni \{X\}_{shk(P,Q)}\in K(\varepsilon)}\ (ME_S)$$

$$\frac{\varepsilon \ni Pubk(P)\in K(\varepsilon),\ \ \varepsilon \ni X\in K(\varepsilon)}{\varepsilon \ni \{X\}_{Pubk(P)}\in K(\varepsilon)}\ (ME_P)$$

- رمزگشايي پيامها (Message Decryption): اگر نفوذي يك پيام رمز شده در اختيار داشته باشد و كليد رمزگشايي مربوط به آن پيام را نيز مالك باشد، مي‌تواند آن پيام را رمزگشايي نموده، و مالك آن شود (براي هر دو سيستم رمز متقارن و غيرمتقارن).

$$\frac{\varepsilon \ni shk(P,Q)\in K(\varepsilon),\ \varepsilon \ni \{X\}_{shk(P,Q)}\in K(\varepsilon)}{\varepsilon \ni X\in K(\varepsilon)}\ (MD_S)$$

$$\frac{\varepsilon \ni Prvk(P)\in K(\varepsilon),\ \varepsilon \ni \{X\}_{Pubk(P)}\in K(\varepsilon)}{\varepsilon \ni X\in K(\varepsilon)}\ (MD_P)$$

توضيح اينكه قابليتهاي فوق به عنوان نمونه ذكر شده‌اند و قوانين فوق ليست كاملي از قابليتهاي نفوذي نيست. قابليتهاي ديگر نفوذي را نيز (مثل توليد و بررسي مقادير درهم[1]) ميتوان به صورت فوق توصيف نمود.

۳-۲- قابليتهاي نفوذي فعال

نفوذي فعال علاوه بر داشتن مجموعه‌اي از دانشها، قدرت استنتاج روي دانشهاي قبلي و قابليت شنود روي پيامهاي نشستهاي مختلف پروتكل، ميتواند عملاً نيز به عنوان يك عامل فعال در شبكه مبادرت به ارسال پيام نمايد. براي اين منظور قابليت زير را براي نفوذي فعال در نظر ميگيريم:

1- Hash value

- ارسال پيام روي شبكه (Sending messages to Network): نفوذي مي‌تواند پيامهاي تحت تملك خود را از طرف هر عامل دلخواه به هر عامل دلخواه بفرستد.

$$\frac{\varepsilon \ni X\in K(\varepsilon)}{\triangleleft(P,Q,X)\in K(\varepsilon)}\ (NET)$$

علاوه براين، نفوذي فعال مي‌تواند براي ارسال پيامها روي شبكه تابع يك راهبرد حمله نيز باشد. داشتن راهبرد به نفوذي كمك مي‌كند كه فعاليتهايش در جهت رسيدن به هدف حمله جهت‌دار شود. فرض كنيد كه هدف حملة نفوذي فريب دادن يك يا چند عامل پروتكل باشد. يك عامل مجاز در پروتكل توسط نفوذي فريب خورده است، اگر تصور كند كه پروتكل به صورت معمول اجرا شده است در حاليكه در واقع برخي ويژگيهاي امنيتي پروتكل توسط نفوذي نقض شده باشد. به عنوان يك راهبرد براي رسيدن به اين هدف حمله، نفوذي تلاش مي‌كند كه اجراي پروتكل را براي عامل موردنظر عادي جلوه دهد در حاليكه همچنان به دنبال نقض ويژگي امنيتي موردنظر است.

براي رسيدن به راهبرد مناسب انجام حمله توسط نفوذي، پروتكل احراز اصالت زير را در نظرگرفته، راهبرد نفوذي براي حمله به اين پروتكل را تحليل نموده، سپس نتايج به دست آمده را تعميم مي‌دهيم:

1. $P \to Q : N_P$
2. $Q \to P : \{N_P\}_{K_{PQ}}$

عامل P به عنوان اثبات كنندة هويت, نانس N_P را به عنوان تحدي[2] براي Q مي‌فرستد و عامل Q, در جواب به عنوان مقابله[3] با اين تحدي, آن را با كليد مشترك P و Q رمز نموده, براي وي ارسال مي‌كند. P با دريافت اين پيام, چون به انحصاري بودن K_{PQ} اعتقاد دارد, اصالت Q را احراز مي‌كند. حال روال حملة زير را در نظر بگيريد:

1. $P \to E_Q : N_P$
   1′. $E_Q \to P : N_P$
   2′. $P \to E_Q : \{N_P\}_{K_{PQ}}$
2. $E_Q \to P : \{N_P\}_{K_{PQ}}$

2- Challenge
3- Response

نفوذي قصد فريب P و جعل نقش Q را براي وي دارد. نفوذي در نقش Q را با E_Q نشان داده‌ايم. عامل P براساس پروتـــكل، پيام تحدي N_P را بـراي Q مي‌فرستد ولي نفوذي بـه جاي Q آن را دريافت ميكند. حال براي جعل نقش Q در مقابل P، لازم است نفوذي با اين تحدي مقابله كند، ولي چون K_{PQ} را در اختيار ندارد نميتواند مستقيماً اين كار را انجام دهد. با اين‌حال نفوذي با هوش مي‌داند كه اگر همين پروتكل را يكبار در نقش Q در مقابل P اجرا كند, مي‌تواند پيام تقابل موردنياز خود را به آساني به دست آورد. به همين دليل نشست دوم پروتكل را در نقش Q با P آغازكرده, از N_P به عنوان پيام تحدي استفاده مي‌كند. عامل P نيز براساس پروتكل براي اثبات هويت خود, $\{N_P\}_{KPQ}$ را براي E_Q ارسال مي‌كند. به اين ترتيب نفوذي قادر خواهد بود نشست اول خود با P را به اتمام رسانده, روال فريب خود را كامل كند.

اگر وضعيت عوامل مجاز و فعاليتهاي نفوذي را در حملة فوق تحليل كنيم، درمي‌يابيم كه عامل P در نشست دوم اصالت Q را احراز مي‌كند و البته اين يك باور اشتباه است كه از طرف نفوذي به وي تحميل شده است. راهبرد نفوذي براي تحميل اين باور اشتباه اين است كه تمامي درخواستهاي عامل P در طي پروتكل را به نحو مناسبي پاسخ دهد. نفوذي براي انجام اين كار مي‌تواند از دانشي كه از طريق شنود پيامهاي پروتكل به دست مي‌آورد, استنتاج دانشهاي جديد و استفاده از خود پروتكل به عنوان منبع توليد پيامها استفاده كند. در حالت اخير نفوذي فقط بايستي بداند پيام موردنظر خود را با كمك اجراي كداميك از نمونه‌هاي اجرايي پروتكل (تركيبات مختلف نقشها به عنوان آغازگر, مخاطب و ...) و در چه مقطعي از اجراي آن مي‌تواند به دست آورد.

با توجه به مثال فوق و تعاريف مربوط به مسير اجراي پروتكل و ورودي/خروجي هر قدم, دو راهبرد زير را مي‌توان در مورد فعاليتهاي نفوذي بيان نمود:

- نفوذي مي‌تواند يك نقش را در يك مسير اجرا فريب دهد، اگر بتواند تمام ورودیهاي قدمهاي آن نقش را در آن مسير اجرا تأمين كند. اين اصل شرط لازم براي انجاميذيري جعل اصالت يك عامل توسط نفوذي است.
- نفوذي مي‌تواند خروجي يكي از قدمهاي يك نقش در يك مسير اجرا را به دست آورد، اگر بتواند ورودي قدمهاي ماقبل وي را تأمين كند.

ما از اين دو راهبرد براي توصيف چگونگي انجام فريب توسط نفوذي روي يك مسير اجرا و وارسي انجاميذيري آن استفاده مي‌كنيم.

تعريف ۹ (قدمهاي يك نقش در مسير اجرا): فرض كنيد كه $P=<\Lambda, S, A>$ يك پروتكل، $R(P)$ مسير اجراي پروتكل P و $\rho\in\Lambda$ يكي از نقشهاي آن باشد، رشتة قدمهاي ρ در مسير اجراي $R(P)$ را با $\rho@R(P)$ نشان مي‌دهيم. به صورت متناظر $\rho@R_l(P)$، نقش ρ در پيشوند مسير اجراي $R_l(P)$ را نشان مي‌دهد.

تعريف ۱۰ (پيشكش و جاخالي): اگر P يك پروتكل و $R_l(P)$ يك پيشوند مسير اجراي آن باشد و $\rho@R_l(P)$ يعني قدمهاي نقش ρ در $R_l(P)$ را به صورت رشتهاي از m قدم $r_1, r_2, \dots, r_m$ نشان دهيم، مقادير پيشكش و جاخالي نقش ρ در پيشوند مسير اجراي $R_l(P)$ به صورت زير تعريف مي‌شوند:

(پيشكش) $gift(\rho@R_l(P)) = out(r_m)$,

(جاخالي) $hole(\rho@R_l(P)) = \bigcup_{i=1}^{m} in(r_i)$

پيشكش يك نقش در يك مسير اجرا، پيامهايي است كه آن نقش در اثر اجراي قدمهاي قبلي خود به نفوذي هديه مي‌كند. جا خالي يك نقش نيز پيامهايي است كه آن نقش براي اجراي قدمهاي خود به آنها نياز دارد.

به اين ترتيب ما مي‌توانيم قابليت راهبردي فريب عوامل توسط نفوذي را با تعريف زير به مجموعه قابليتهاي نفوذي اضافه كنيم.

تعريف ۱۱ (راهبرد فريب): فرض كنيد كه $P=<\Lambda, S, A>$ يك پروتكل باشد، اگر نفوذي بتواند جاخاليهاي يك نقش در يك پيشوند مسير اجرا از يك نمونة اجراي پروتكل را فراهم كند، مي‌تواند پيشكش آن را به مجموعه دانش خود اضافه كند. اين قابليت را مي‌توان به شكل صوري زير بيان نمود:

$$\frac{\exists\sigma,\exists\rho\in\Lambda,\exists l<|R(P)|\bullet K(\varepsilon)\models_{EIR} hole(\rho@R_l(P_\sigma))}{K(\varepsilon)=K(\varepsilon)\cup gift(\rho@R_l(P_\sigma))} \quad (PM)$$

اكنون ما مي‌توانيم نحوة وارسي آسيبپذيري پروتكل با توجه به دو ويژگي مهم اختفا و اصالت موجوديتها را به صورت صوري بيان نمائيم.

تعریف ۱۲ (وارسي ويژگي اختفا) : فرض كنيم 'G عبارتي در زبان L باشد كه توصيف كنندة نقض ويژگي اختفا در پروتكل است (مثلاً افشاء بعضي پيامهاي مخفي). پروتكل P با توجه به 'G امن است اگر 'G با كمك قابليتهاي نفوذي (EIR) از دانش نفوذي قابل حصول نباشد (يعني $K(\varepsilon) \neq_{EIR} G'$)

تعریف ۱۳ (وارسي ويژگي اصالت موجوديتها): نفوذي مي‌تواند يك نقش را به كمك راهبرد فريب در يك مسير اجرا فريب دهد اگر بتواند تمامي جاخاليهاي وي را در آن مسير اجرا فراهم كند، يعني با كمك دانش و قابليتهاي خود قادر به استنتاج آنها باشد (يعني $K(\varepsilon) |=_{EIR} hole(\rho @ R(P))$)

۴- وارسي يك پروتكل نمونه

در اين بخش پروتكل احراز اصالت يكطرفة Woo-Lam [۱۶] را به عنوان نمونه توصيف و وارسي مي‌كنيم. پس از معرفي پروتكل Woo-Lam، مسير اجراي آن را توصيف نموده، سپس سعي ميكنيم آسيبپذيري آن را در مقابل نفوذي بررسي كنيم. براي توصيف اين پروتكل از زبان توصيف معرفي شده در بخش ۲ استفاده ميكنيم.

۴-۱- پروتكل Woo-Lam

پروتكل احراز اصالت يكطرفة Woo-Lam در شكل (۲) نشان داده شده است. سه نقش آغازگر (A)، مخاطب (B) و ميزبان (S) در اين پروتكل عمل مي‌كنند. هدف پروتكل احراز اصالت عامل A براي عامل B است. اين پروتكل مبتني بر سيستم رمز متقارن است و در آن N_B نانسي است كه توسط عامل B ايجاد مي‌شود، K_{AS} و K_{BS} نيز به ترتيب كليدهاي اشتراكي عوامل A و B با ميزبان S است.

$$(1) \quad A \rightarrow B : A$$
$$(2) \quad B \rightarrow A : N_B$$
$$(3) \quad A \rightarrow B : \{N_b\}_{K_{AS}}$$
$$(4) \quad B \rightarrow S : \{A, \{N_b\}_{K_{AS}}\}_{K_{BS}}$$
$$(5) \quad S \rightarrow B : \{N_b\}_{K_{BS}}$$

شكل ۲- پروتكل احراز اصالت Woo-Lam

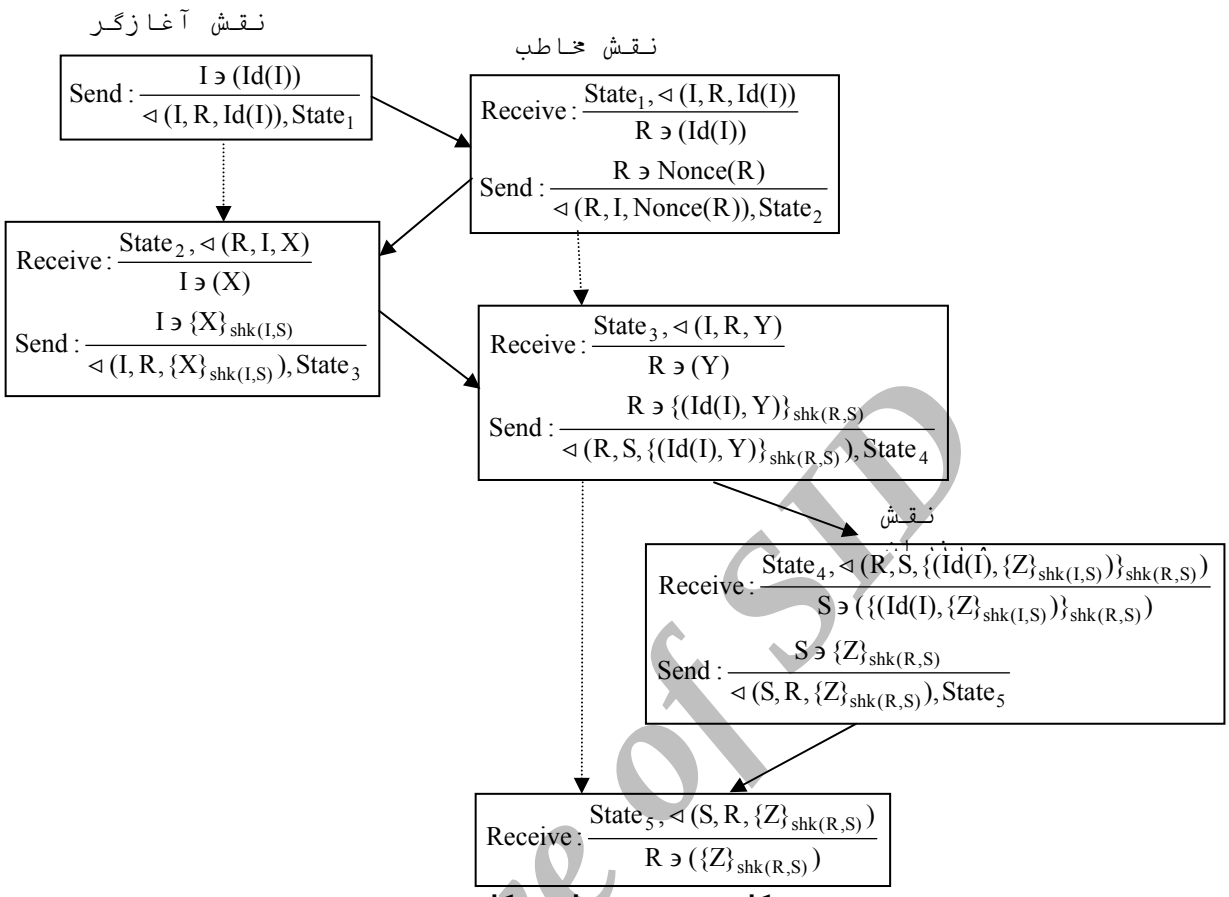
پروتكل به صورت زير عمل ميكند: (۱) نقش آغازگر در قدم اول پروتكل با ادعاي هويت A و ارسال آن به مخاطب، از وي تقاضاي احراز اصالت مي‌كند. (۲) مخاطب با ارسال نانس N_B، آغازگر را براي اثبات ادعاي خود به تحدي فرا مي‌خواند. (۳) در قدم سوم، آغازگر براي مقابله با اين تحدي، پيام N_B را با كليد مشترك بين خود و ميزبان رمز كرده براي مخاطب ارسال مي‌كند. (۴) چون اين پيام با كليد K_{AS} رمز شده است، لذا عامل B كل اين پيام را به همراه شناسة عامل مدعي هويت (يعني A) با كليد مشترك بين خود و ميزبان رمزكرده، براي ميزان ارسال مي‌كند. (۵) ميزبان قادر به رمزگشايي هر دو بستة تودرتو است، لذا داخليترين پيام يعني N_b را به دست آورده، اينبار با كليد مشترك بين خود و مخاطب رمزكرده، براي وي ارسال مي‌كند. در اين هنگام مخاطب توانايي بازيابي پيام تحدي خود كه در قدم دوم براي آغازگر فرستاده بود را پيدا مي‌كند و بدين ترتيب آغازگر براي مخاطب احراز اصالت مي‌شود.

۴-۲- توصيف صوري پروتكل Woo-Lam

مجموعه نقشهاي پروتكل (يعني Λ) شامل سه نقش آغازگر، مخاطب و ميزبان است كه به ترتيب با I، R و S نشان مي‌دهيم. نقش آغازگر پروتكل از دو قدم تشكيل شده است. قدمهاي مختلف نقشهاي پروتكل به همراه تواناييهاي آنها در شكل (۳) نشان داده شده است.

مسندات پيش‌شرط و پس‌شرط تواناييها داراي پارامترهاي متغير هستند كه ما آنها را با حروف بزرگ شروع كرده‌ايم. اگر قدم S_j از قدم S_i قابل دسترس باشد، ما آن را با يك فلش توپر از S_i به S_j نشان داده‌ايم. فلشهاي نقطه‌چين نيز ارتباط بين قدمهاي هر نقش را نشان مي‌دهد (رابطة succ).

آغازگر پروتكل در قدم اول خود (معادل قدم اول پروتكل) شناسة خود را براي مخاطب ارسال مي‌كند و سپس در قدم دوم (معادل قدم سوم پروتكل) پيامي را از شبكه دريافت نموده، آن را با كليد مشترك بين خود و ميزبان رمز كرده و مجدداً به شبكه ارسال مي‌كند. قدم اول نقش آغازگر تنها داراي يك توانايي Send است. اين توانايي را براساس دانش پيش‌شرط و پس‌شرط آن مي‌توان اينگونه تعبير كرد: اگر آغازگر پروتكل شناسة خود را داشته باشد (يعني $I \ni Id(I)$)، اين توانايي قابل انجام است و با انجام آن اين شناسه از طرف عامل I به عامل B ارسال مي‌شود (يعني $\lhd (I, R, Id(I))$) و وضعيت $State_1$ خواهد بود.



شکل ۳- مجموعه‌قدمهاي پروتکل Woo-Lam

قـدم دوم آغازگر داراي دو تـواناييReceive و Send است. به شرط قرار گرفتن در وضعيت $State_2$ و ارسال پيامي‌مثل X روي شبکه، آغازگر مالك پيام X خواهد شد و در صورتيکه او بتواند پيام X را با کليد مشترك بين خود و ميزبان رمز کند (و آن را مالك شود)، آن را روي شبکه خواهد گذاشت و وضعيت $State_3$ خواهد شد. قدمهاي ساير نقشها نيز به همين ترتيب توصيف شده‌اند.

فرضيات اوليه پروتکل Woo-Lam بايستي در قالب قدم مقداردهي اولية پروتکل تعيين شود. اين فرضيات، دانش اولية همة نقشها را تعيين مي‌کند. نقشهاي آغازگر و مخاطب پروتکل Woo-Lam داراي کليدهاي اشتراکي با ميزبان هستند. نقش مخاطب در پروتکل داراي يك نانس است و ميزبان نيز هر دو کليد مشترك را دارا است. به علاوه براي شروع پروتکل لازم است آغازگر شناسة خود را نيز بداند. قدم مقداردهي اولية پروتکل را مي‌توان چنين در نظر گرفت :

$$S_{INIT} = INITI: \frac{}{I \ni Id(I), I \ni shk(I,S)},$$

$$INITR: \frac{}{R \ni skk(R,S),\ R \ni Nonce(R)},$$

$$INITS: \frac{}{S \ni shk(I,S),\ S \ni shk(R,S)}$$

براساس تعريف نشست پروتکل (تعريف ۷)، با در نظر گرفتن يك تابع جايگزيني براي نمونة موردنظر پروتکل، شروع از قدم اول آغازگر (قدم شروع پروتکل) و يکسانسازي ورودي/خروجي قدمهاي دسترسي‌پذير، مي‌توان نشست موردنظر پروتکل را ايجاد نمود.

۳-۴- وارسي صوري پروتکل Woo-Lam

فرض کنيد براي تحليل آسيب‌پذيري پروتکل، نشستي از پروتکل را که با تابع جايگذاري σ_1 = {I/a, R/b,S/s} مشخص مي‌شود را در نظر بگيريم. هدف پروتکل، احراز اصالت آغازگر

براي مخاطب است و لذا نفوذي در صدد جعل نقش آغازگر براي مخاطب خواهد بود. براي اين منظور، نفوذي بايستي مخاطب را به گونه‌اي فريب دهد كه وي به اشتباه فكر كند با آغازگر واقعي در ارتباط است. براي انجام اينكار، نفوذي از راهبرد فريب (تعريف ۱۱) استفاده مي‌كند و سعي مي‌كند جاخاليهاي مخاطب را در اين نشست پروتكل پر كند. بنابراين ما بايستي قضية زير را اثبات كنيم:

$$K(\varepsilon)\overset{?}{\models} hole(\rho_b \,@\, Session(P_{\sigma 1})) = \left\{ \begin{array}{l} \lhd (a,b,Id(a)), \lhd (a,b,\{Nonce(b)\}_{shk(a,s)}), \\ \lhd (s,b,\{Nonce(b)\}_{shk(b,s)} \end{array} \right\} \quad (۱)$$

براي اثبات هدف فوق، مي‌توانيم از قابليتهاي نفوذي استفاده كنيم. شناسة عامل a دادة مهمي نيست، مي‌توانيم فرض كنيم كه نفوذي از قبل آن را مي‌داند يعني جزء مجموعه دانش اولية نفوذي است و لذا تملك بر اين شناسه توسط نفوذي از دانش نفوذي قابل حصول است. بنابراين براساس قابليت NET، نفوذي مي‌تواند آن را از طرف هر عامل دلخواه (مثل a) به هر عامل دلخواه (مثل b) ارسال كند:

$$(assumption)\ \exists\, \lhd (Id(a)) \in K(\varepsilon) \overset{NET}{\Rightarrow} \lhd (P,Q,\ Id(a)) \in K(\varepsilon) \Rightarrow K(\varepsilon)\models \lhd (a,b,Id(a)) \quad (۲)$$

دومين دانش مورد نياز نفوذي يعني $\lhd (a,b,\{Nonce(b)\}_{shk(a,s)})$ به صورت مستقيم از دانش نفوذي قابل حصول نيست، ولي با اين‌حال نفوذي باهوش مي‌داند كه اين دانش با دانش پيشكش نقش a در قدم سوم مسير اجراي پروتكل قابل انطباق است. براي استفاده از اين پيشكش، نفوذي نمونة جديدي از اجراي پروتكل كه در آن σ_2 = {I/a, R/b,S/s } است را شروع مي‌كند. در اين حالت داريم:

$$\lhd (a,b,\{X\}_{shk(a,s)}) \in gift(\rho_a \,@\, R_3(P_{\sigma 2})) \quad (۳)$$

بنابراين با توجه به راهبرد فريب، كافي است كه نفوذي بتواند جاخاليهاي نقش a در مسير اجراي پروتكل را به ازاء X=Nonce(b) فراهم كند، يعني بايستي قضية زير را اثبات نمائيم:

$$K(\varepsilon)\overset{?}{\models} hole(\rho_a \,@\, R_3(P_{\sigma 2})) = \{\lhd (b,a,Nonce(b))\} \quad (۴)$$

ولي ما مي‌دانيم كه نفوذي در نقش غيرفعال خود قبلاً دانش $\lhd (b,a,Nonce(b))$ را از طريق شنود روي نشست اول پروتكل كسب كرده است، بنابراين، اين دانش از دانش نفوذي قابل حصول است:

(Passive intruder knowledge)

$$\lhd (b,a,Nonce(b)) \in K(\varepsilon) \overset{NET}{\Rightarrow} \lhd (b,a,Nonce(b)) \in K(\varepsilon) \Rightarrow K(\varepsilon)\models \lhd (b,a,Nonce(b)) \quad (۵)$$

به اين ترتيب قضية (٤) اثبات مي‌شود و لذا دانش $\lhd (a,b,\{Nonce(b)\}_{shk(a,s)})$ از دانش نفوذي قابل حصول است:

$$(3),\ (5) \overset{PM}{\Rightarrow} K(\varepsilon)\models \lhd (a,b,\{Nonce(b)\}_{shk(a,s)}) \quad (۶)$$

سومين دانش موردنياز در (۱) يعني $\lhd (s,b,\{Nonce(b)\}_{shk(b,s)})$ مستقيماً در دانش نفوذي وجود ندارد، ولي نفوذي مي‌تواند با سوء استفاده از نقش ميزبان آن را كسب نمايد. اين دانش در واقع با پيشكش نقش ميزبان در قدم آخر مسير اجراي پروتكل قابل انطباق است. بنابراين، نفوذي مي‌تواند با تأمين جاخاليهاي نقش ميزبان در يك نشست از پروتكل، به اين پيشكش دستيابي پيدا كند. نفوذي انتخابهاي مختلفي براي پارامترهاي نشست جديد دارد. مثلاً مي‌تواند از همان نشست دوم (كه به صورت موازي با نشست اول ايجاد نموده است) استفاده كند يا نشست جديدي بين عوامل b و a به ترتيب به عنوان آغازگر و مخاطب ايجاد كند. ولي در هر دو اين نشستها نفوذي در فراهم كردن جاخاليهاي ميزبان به بن‌بست مي‌رسد.

در هر حال هنوز يك راه براي نفوذي باقي‌مانده است. نفوذي خود مي‌تواند يك عامل مجاز شبكه نيز باشد و مي‌تواند نشستهاي جديدي در نقش آغازگر يا مخاطب با هر كدام از عوامل a يا b به عنوان طرف ديگر انجام دهد. فرض كنيد نفوذي تحليل خود را روي يك نشست جديد از پروتكل بين خود (به عنوان آغازگر) و عامل b به عنوان مخاطب شروع مي‌كند. فرض كنيد كه شناسة نفوذي به عنوان يك عامل

مجـاز، c باشـد، بنـابراین در نمونـة جدیـد اجـراي پروتکـل σ_3={I/c,R/b,S/s} است. حال نفوذي تحليل خود را بـه کمـك اين نشست جديد پي مي‌گيرد. وي مي‌داند که:

$$\lhd (s,b,\{Z\}_{shk(b,s)} \in gift(\rho_s @ R_6(P_{\sigma 3})) \quad (۷)$$

بنابراين کافي است که نفوذي بتواند جاخاليهاي نقش ميزبان را در مسير اجراي اين نشست به ازاء Z=Nonce(b) فراهم کند، يعني بايستي بتوانيم قضية زير را اثبات کنيم:

$$K(\varepsilon)\Big|\overset{?}{=} hole(\rho_s @ R_6(P_{\sigma 3})) = \left\{\lhd (b,s,\{Id(c),\{Nonce(b)\}_{shk(c,s)}\}_{shk(b,s)})\right\} \quad (۸)$$

نفوذي در اينجا نيز از همان راهبرد سابق خود بهره مي‌گيرد. او مي‌داند که:

$$\lhd (b,s,\{Id(c),Y\}_{shk(b,s)}) \in gift(\rho_b @ R_5(P_{\sigma 3})) \quad (۹)$$

بنابراين او سعي مي‌کند جاخاليهاي نقش b در اين نشست جديد پروتکل را به ازاء Y=$\{Nonce(b)\}_{shk(c,s)}$ فراهم کند. بنابراين بايستي براي اثبات قضية زير را تلاش کنيم:

$$K(\varepsilon)\Big|\overset{?}{=} hole(\rho_b @ R_5(P_{\sigma 3})) = \left\{\lhd (c,b,Id(c)),\ \lhd (c,b,\{Nonce(b)\}_{shk(c,s)})\right\} \quad (۱۰)$$

شناسة عامل c که طبيعتاً جزئي از دانش اولية نفوذي هست، بنابراين، اولين دانش از مجموعة فوق براي نفوذي قابل حصول است:

$$(assumption)\ \varepsilon \ni (Id(c)) \in K(\varepsilon) \overset{NET}{\Rightarrow} \lhd (c,b,Id(c)) \in K(\varepsilon) \Rightarrow K(\varepsilon)\Big|=\lhd (c,b,Id(c)) \quad (۱۱)$$

دومين دانش يعني $\lhd$(c,b,{Nonce(b)}shk(c,s)) را نميتوان مستقيماً در مجموعه دانش نفوذي يافت، ولي نفوذي مي‌تواند آن را به کمك پيام Nonce(b) که قبلاً شنود کرده است و shk(c,s) که به صورت پيش‌فرض جزئي از دانش نفوذي است بسازد. (دقت کنيد که عامل c همان نفوذي است):

$$\left.\begin{array}{l}(\text{Passive intruder knowledge}) \\ \lhd (b,a,Nonce(b)) \in K(\varepsilon) \overset{MP}{\Rightarrow} \varepsilon \ni Nonce(b) \in K(\varepsilon) \\ (assumption)\ \ \varepsilon \ni shk(c,s) \in K(\varepsilon)\end{array}\right\} \overset{ME_S}{\Rightarrow}$$
$$\varepsilon \ni (\{Nonce(b)\}_{shk(c,s)}) \in K(\varepsilon) \overset{NET}{\Rightarrow}$$
$$\lhd (P,Q,\{Nonce(b)\}_{shk(c,s)}) \in K(\varepsilon) \Rightarrow$$
$$K(\varepsilon)\Big|=\lhd (c,b,\{Nonce(b)\}_{shk(c,s)}) \quad (12)$$

(۱۲)

بـه ايـن ترتيب، به کمك نتيجه‌گيريهاي (۱۱) و (۱۲)، قضية (۱۰) و به تبع قضية (۸) اثبات مي‌شوند يعني داريم:

$$(11),\ (12) \Rightarrow (10) \overset{PM}{\Rightarrow} K(\varepsilon)\Big|=\lhd (c,b,\{Nonce(b)\}shk(c,s)) \quad (۱۳)$$

حال به کمك (۲)، (۶)، و (۱۳)، قضية (۱) اثبات مي‌شود. اين بدان معنا است که نفوذي به کمك راهبرد فريب و با استفاده از دو نشست جديد پروتکل قادر به فريب مخاطب خواهد بود. سناريوي اين فريب در شکل (۴) نشان داده شده است. نفوذي در نقش a ، b و s به ترتيب با E_A ، E_B و E_S نشان داده شده است. به سادگي مي‌توان مشاهده کرد که سناريوي حاصل منطبق بر روند تحليل فوق مي‌باشد.

(1) $E_A \rightarrow B : A$
(2) $B \rightarrow E_A : N_B$
  (1′) $A \rightarrow E_B : A$
  (2′) $E_B \rightarrow A : N_B$
  (3′) $A \rightarrow E_B : \{N_B\}_{Kas}$
(3) $E_A \rightarrow B : \{N_B\}_{Kas}$
(4) $B \rightarrow E_S : \{A, \{N_B\}_{Kas}\}_{Kbs}$
  (1″) $C \rightarrow B : A$
  (2″) $B \rightarrow C : N'_B$
  (3″) $C \rightarrow B : \{N_B\}_{Kcs}$
  (4″) $B \rightarrow S : \{C, \{N_B\}_{Kcs}\}_{Kbs}$
  (5″) $S \rightarrow B : \{N_B\}_{Kbs}$
(5) $E_S \rightarrow B : \{N_B\}_{Kbs}$

شکل ٤- سناريوي حملة کشف شده عليه پروتکل احراز اصالت Woo-Lam

۵- نتیجه گیری

در این مقاله با بهکارگیری چارچوب و مدل محاسباتی مطرح شده در [۱۳]، روشی برای در نظرگرفتن نقش نفوذی در مدل صوری پروتکل و تحلیل نقش وی در کسب دانش از پروتکل یا فریب دادن عوامل مجاز ارائه شده است. در مدل محاسباتی مورداستفاده، عوامل پروتکل به عنوان نقشهایی دارای تواناییهای مشخص در نظر گرفته شده‌اند. تواناییهای بالقوه هر نقش دقیقاً براساس تعریف پروتکل به فعلیت می‌رسد و قدمهای متوالی اجرای پروتکل را تشکیل می‌دهند. رشتهٔ خاصی از تواناییهای نقشهای مختلف پروتکل که طبق تعریف پروتکل بایستی به فعلیت برسند، مسیر اجرای پروتکل را تشکیل می‌دهد. روی این مسیر اجرا می‌توان در مورد دانش نفوذی (مجموعه مسندات راجع به یافته‌های نفوذی از پروتکل) و همچنین قابلیت نفوذی در سوء استفاده از این مسیر اجرا برای فریب نقشهای مجاز به استنتاج پرداخت.

در روش ارائه شده، نقش نفوذی در دو حالت غیرفعال و فعال در نظر گرفته شده است. تحلیل این دو حالت به ترتیب، امکان وارسی نقض ویژگیهای اختفاء پیامها و اصالت موجودیتها را فراهم میآورد. نفوذی در نقش فعال و غیرفعال میتواند پیامهای پروتکل را شنود کرده، با کمک اصول استنتاجی خود، دانش خود را گسترش دهد. نفوذی در حالت فعال سعی دارد عوامل مجاز پروتکل را فریب دهد که برای انجام اینکار از دو اصل راهبردی بهره میگیرد. نخست اینکه برای فریب یک عامل بایستی تمام درخواستهای وی را پاسخ دهد، و دیگر اینکه، به شرط فراهم کردن زمینه‌های لازم برای اجرای پروتکل تا یک مرحلهٔ موردنظر، می‌تواند از پروتکل به عنوان یک منبع تولید دانش استفاده کند.

ویژگی اصلی روش ارائه شده که در واقع تعمیم مدل کلی Doleve-Yao [۱۱] به شمار میآید، مورد توجه قرار دادن راهبرد انجام حمله به عنوان یکی از قابلیتهای کلیدی نفوذی در انجام حمله است. در روشهای موجود تحلیل آسیب‌پذیری پروتکل از جمله [۶-۱۰] که همگی مبتنی بر روش Doleve-Yao هستند، مجموعه‌ای از قابلیتهای محاسباتی و ارتباطی برای نفوذی در نظر گرفته می‌شود ولی چون مدل Doleve-Yao نحوهٔ بهکارگیری این قابلیتها توسط نفوذی را تعیین نمی‌کند، این قابلیتها به عنوان ابزاری برای گسترش فضای حالت اجرای پروتکل (به همراه نفوذی) مورداستفاده قرار گرفته و نهایتاً برای یافتن وضعیتهای ناامن در این فضای ایجاد شده جستجو می‌شود. از آنجاکه فضای حالت ایجاد شده حتی با در نظر گرفتن حداقل قابلیتهای یک نفوذی نیز یک فضای نامتناهی است [۱۶]، بنابراین مشکلاتی برای روشهای تحلیل آسیب‌پذیری به وجود میآید. روشهایی که برای پیاده‌سازی تحلیل از بررسی مدل استفاده می‌کنند مجبورند با تنظیم پارامترهای تحلیل مرزهای فضای حالت را تعیین کنند که البته این کار تمامیت[1] تحلیل را از بین میبرد. در روشهای اثبات قضیه نیز به دلیل اینکه بایستی هوشمندی نفوذی خارج از حوزهٔ قابلیتهای وی و به عنوان یک ویژگی اقتضائی[2] در فرایند اثبات در نظر گرفته شود، توصیف فرایند تحلیل پیچیده میشود.

در روش ارائه شده، استفاده از راهبرد مشخص در انجام حمله به عنوان بخشی از قابلیتهای ذاتی یک نفوذی هوشمند در نظر گرفته شده و بنابراین، این قابلیت نیز به صورت یکنواخت با سایر قابلیتهای نفوذی در خدمت کسب و گسترش دانش از پروتکل و استفاده از این دانش در جهت هدف حمله قرار می‌گیرد. به این ترتیب تحلیل آسیب‌پذیری پروتکلهای رمزنگاری نسبت به حملات نفوذی در روش مطرح شده، به صورت اثبات قضایایی راجع به عملی شدن راهبرد حملهٔ نفوذی انجام می‌شود. چون تمامی قابلیتهای نفوذی در تحلیل به کمک قابلیت راهبردی وی در انجام حمله جهتدهی می‌شود، بنابراین در صورت اثبات قضایای موردنظر در تحلیل، قدمهای اثبات دقیقاً معادل سناریوی انجام حمله خواهد بود. بر این اساس می‌توان گفت که مزیت اصلی روش ارائه شده نسبت به روشهای دیگر، تأکید روی مدل‌سازی هوشمندی نفوذی به عنوان یک قابلیت اصلی وی به جای حذف این هوشمندی و انجام جستجوی فراگیر فضای حالت (کاری که روشهای بررسی مدل انجام می‌دهند) و یا مدلسازی این هوشمندی به صورت اقتضائی در توصیف فرایند تحلیل (کاری که روشهای اثبات قضیه انجام می‌دهند) میباشد.

ایدهٔ ارائه شده در این مقاله برای توصیف نقشها و قدمهای پروتکل، با مفهوم parametric strand space ارائه شده توسط Millen [۱۷] قابل مقایسه است. یک نقش را میتوان معادل یک Parametric Strand و مسیر اجرای پروتکل را معادل یک Strand bundle دانست، با این تفاوت که در روش ما، با توجه به استفاده از روش اثبات قضیه، از مزایای گذر- وضعیت

1- Completeness
2- Ad hoc

نمادين[1] در مقابل جستجوي صريح وضعيتها[2] بهره‌برداري شده است. ما براي تحليل آسيب‌پذيري از رويكرد ساخت اثبات استفاده كرده‌ايم و بنابراين بر خلاف روشهاي ساخت حمله به كمك بررسي مدل، ميتواند براي مسائل با فضاي مدل نامتناهي نيز عمل كند. علاوه براين، استفاده از روش جستجوي روبه‌عقب به انضمام مدل‌سازي و دخالت دادن راهبرد نفوذي در انجام حمله، فرايند جستجو براي كشف سناريوهاي حمله را سرعت مي‌بخشد.

در اين مقاله چگونگي كشف يك سناريوي حمله توسط نفوذي به پروتكل احراز اصالت يكطرفه Woo-Lam به كمك روش ارائه شده نيز تشريح شده است. اين حمله يك حملة جديد به اين پروتكل است و با حمله قبلي كشف شده عليه آن [۱۸] تفاوت دارد. ادعاي اصلي اين مقاله ارائه روشي سيستماتيك براي كشف اين نوع حملات است.

مراجع

[1] S. Gritzalis, D. Spinellis and P. Georgiadis, "Security protocols over open networks and distributed systems: formal methods for their analysis, design, and verification," Computer Communications 22 (1999) pp697– 709

[2] C. Meadows, "Formal Methods for Cryptographic Protocol Analysis: Emerging Issues and Trends," IEEE Journal on Selected Areas in Communication, Vol. 21, No. 1, pp. 44-54, January 2003

[3] M. Burrows, M. Abadi and R. Needham, "A Logic of Authentication," Proc. Royal Society, Series A, Vol. 246, No. 1871, pp. 233-271, 1989.

[4] L. Gong, R. Needham and R. Yahalom, "Reasoning About Belief in Cryptographic Protocols," Proc. IEEE 1990 symposium on Security and Privacy, Oakland, California, pp. 234-248, May 1990.

[5] C.Meadows, "Invariant Generation Techniques in Cryptographic Protocol Analysis," Proceedings of the 13th Computer Security Foundations Workshop, IEEE Computer Society Press, July 2000.

[6] C. Meadows, "The NRL Protocol Analyzer: An Overview," Journal of Logic Programming, 26(2): 113-131, 1996.

[7] P. Ryan and S. Shneider, Modeling and Analysis of Security Protocols, Pearson Education, 2001.

[8] F. Butler, I. Cervesato and A. Jaggard, and Andre Scedrov. "A formal analysis of some properties of kerberos 5 using MSR," In S. Schneider, editor, proceedings of 15th IEEE Computer Security Foundations Workshop (CSFW'15), pages 175– 190, Cape Breton, Nova Scotia, Canada, June 2002. IEEE Computer Society Press.

[9] C. Meadows, "A Procedure for Verifying Security Against Type Confusion Attacks," Proceedings of the 16th IEEE Computer Security Foundations Workshop, IEEE Computer Society Press, June 2003

[10] L. C. Paulson, The Inductive Approach to verifying Cryptographic Protocols, Journal of computer security, 6:85-128,1998.

[11] D. Dolev and A. C. Yao, On the Security of Public key Protocols, IEEE Transactions on Information Theory, 22, 1976.

[۱۲] ترك لاداني, بهروز و ميريان حسين آبادي, سيدحسن, توصيف معناي پروتكلهاي رمزنگاري با استفاده از زبان توصيف Z, مجموعه مقالات ششمين كنفرانس انجمن كامپيوتر ايران, دانشگاه اصفهان, اسفند ۱۳۷۹.

[۱۳] ترك لاداني، بهروز و جليلي، سعيد، چارچوبي براي وارسي پروتكلهاي رمزنگاري، مجموعه مقالات اولين كنفرانس رمز ايران، دانشگاه امام حسين(ع)، آبان ۱۳۸۰.

[۱۴] جليلي سعيد و ترك لاداني بهروز، مدلي براي توصيف پروتكلهاي رمزنگاري و تفسير اجرايي مدل با رويكرد جبري، مجلة فني و مهندسي مدرس, ص ۲۹-۱۱, شماره سيزدهم پاييز ۱۳۸۲.

[۱۵] ترك لاداني، بهروز و جليلي، سعيد، وارسي پروتكلهاي رمزنگاري بدون فرض وجود صريح نفوذي، هفتمين كنفرانس انجمن كامپيوتر ايران، مركز تحقيقات مخابرات، اسفند ۱۳۸۰.

[16] T. Woo and S. Lam, "Authentication for Distributed Systems," Computer, 25:10-10, March 1992.

[17] J. K. Millen and V. Shmatikov, "Constraint solving for bounded-process cryptographic protocol analysis," In ACM Conference on Computer and Communications Security, pages 166--175, 2001.

[18] M Abadi adn R Needham, "Prudent Engineering Practice for Cryptographic Protocols," IEEE Transactions on Software Engineering v 22 no 1 (Jan 96) pp 6-15.

1- Symbolic State-Transition
2- Explicit State Exploration