روشي براي تحليل نقش نفوذي در پروتكلهاي رمزنگاري

بهروز ترك لاداني 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

يكي از اهداف در طراحي پروتكلهاي رمزنگاري, مقاومسازي آنها در برابر عوامل غير مجازي است كه قصد برهمزدن اهداف پروتكل را دارند. براي انجام اين كار لازم است پروتكل طراحي شده مورد تحليل قرار گيرد. روشهاي صوري[(1)] به صورت وسيعي براي انجام اين كار مورد استفاده قرار ميگيرند [۱و۲]. اين روشها را ميتوان به دو دستة روشهاي تحليل منطقي و روشهاي ساخت حمله تقسيم نمود [۱]. در رويكرد اول، هدف اين است كه با مدل كردن منطق حاكم بر اجزاء پروتكل (توابع رمزنگاري و روشهاي طراحي پروتكل) روشي براي اثبات ايجاد ويژگيهاي امنيتي در پروتكل فراهم گردد. منطقهاي BAN [۳] و GNY [۴] نمونههايي از اين روشها هستند. در رويكرد دوم، پروتكل به همراه يك عامل نفوذي در نظر گرفته ميشود و سعي ميشود با مدل كردن اين سيستم, راهي براي كشف روالهاي نقض ويژگيهاي امنيتي يافت شود.

در رويكرد ساخت حمله, از دو روش اثبات قضيه[(2)] و جستجوي فضاي حالت[(3)] استفاده ميشود [۵]. روش اول شامل تعريف بعضي نامتغيرها[(4)] و اثبات صحيح باقي ماندن آنها در طي گذرهاي وضعيت سيستم است، در حاليكه در روش دوم از Model Checker استفاده ميشود. Model Checker با ايجاد تمامي فضاي حالت ممكن, براي يافتن يك وضعيت ناامن در سيستم (يعني يك حمله) تلاش ميكند. بعضي روشهاي ساخت حمله مثل تحليلگر NRL [۶] از تركيب اين دو روش نيز استفاده مي كنند. [۶-۱۰] نمونههايي از روشهاي ساخت حمله هستند. در [۵], روشهاي مختلف در اين رويكرد، مرور و با يكديگر مقايسه شدهاند.

بيشتر روشهاي ساخت حمله مبتني بر مجموعهاي از فرضيات انتزاعي مدلسازي هستند كه تحت عنوان مدل Doleve-Yao [۱۱] مشهور هستند. در اين مدل محاسباتي از پروتكل, پيامها به عنوان مقادير مجرد غيرقابل تفكيك - و نه دنبالهاي از بيتها- در نظر گرفته ميشوند. رمزنگاري در اين مدل به صورت ايدهال در نظر گرفته ميشود و نفوذي داراي قابليتهاي ارتباطي و محاسباتي روي روند اجراي پروتكل ميباشد. در مقابل، در مورد روشهاي منطقي, مدل محاسباتي پروتكل بيشتر معطوف به بيان وضعيتهاي محلي عوامل پروتكل و توصيف نحوة تغيير آنها در اثر اجراي قدمهاي پروتكل است [۱۲].

در [۱۳] چارچوبي براي بيان روشهاي تحليل ارائه شده است. اين چارچوب داراي چهار مؤلفه است و با Analyze (L,M,PIR,EIR) نشان داده ميشود. L زباني است كه از طريق آن ويژگيهاي عوامل مجاز و نفوذي در پروتكل بيان مي شود، M يك مدل محاسباتي از پروتكل و نحوة اجراي آن است، PIR[(5)] و EIR[(6)] نيز به ترتيب مجموعه اصول براي انجام استنتاجهاي عوامل مجاز و نفوذي است. توصيف پروتكل در مدل محاسباتي M و اصول لازم در مجموعههاي PIR و EIR به زبان L بيان ميشوند. هدف از ارائة چارچوب اين است كه با تغيير مؤلفههاي L، M، PIR و EIR، بتوان روشهاي تحليل مختلفي عرضه نمود. در [۱۴] ضمن تحليل دقيقتر قابليتها و تواناييهاي چارچوب مذكور, يك تفسير اجرايي از آن براساس روشهاي بازنويسي[(7)] ارائه شده است. در [۱۵] نيز, يك روش براي تحليل منطقي پروتكلهاي رمزنگاري, براساس اين چارچوب ارائه شده است.

ما در اين مقاله با بهكارگيري چارچوب كلي و مدل محاسباتي ارائه شده در [۱۳], يك روش براي تحليل نقش نفوذي و ساخت حملات ممكن در روند اجراي پروتكلهاي رمزنگاري ارائه نمودهايم. در اين روش, نقش نفوذي در دو حالت غيرفعال و فعال در نظر گرفته ميشود. در تحليل پروتكل با نفوذي غيرفعال ميتوان ويژگيهاي امنيتي از پروتكل كه ممكن است از طريق يك نفوذي غيرفعال نقض شود, مثل ويژگي اختفا[(8)] را وارسي نمود. نفوذي غيرفعال روي مسير اجراي پروتكل فقط توانايي شنود دارد و داراي يك مجموعه دانش است كه با يك مقدار اوليه شروع ميشود و با شنود پيامهاي پروتكل در روند اجرا و با كمك مجموعه قوانين استنتاج نفوذي (EIR), گسترش مييابد.

اگر در چارچوب ارائه شده, نفوذي را به صورت فعال در نظر بگيريم, ميتوان حملاتي كه از طريق نفوذي فعال امكانپذير 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 تكرار[۱], انعكاس[۲]و در هم بافي[۳] را تشخيص داد. اين حملات عموماً منجر به نقض ويژگي اصالت موجوديت از طريق فريب عامل وارس اصالت ميگردد. نفوذي فعال علاوه بر دارا بودن قابليتهاي نفوذي غيرفعال يعني شنود پيامهاي پروتكل و گسترش مجموعه دانش خود با كمك قوانين استنتاجي خود(EIR) , ميتواند به صورت فعال نيز وارد پروتكل شود و براساس راهبرد[۴] از پيش تعيين شده، يك يا چند عامل مجاز پروتكل را فريب دهد. يك عامل وقتي فريب ميخورد كه تصور كند يك ويژگي امنيتي رعايت شده است ولي در عمل با فعاليتهايي كه نفوذي انجام داده است, اين ويژگي نقض شده باشد.

در ادامة مقاله, ابتدا چگونگي توصيف صوري پروتكلهاي رمزنگاري به كمك يك زبان توصيف و مدل محاسباتي ارائه شده در [۱۳] به اختصار بيان ميشود. سپس چگونگي تحليل پروتكل با فرض وجود نفوذي غيرفعال و همچنين كشف سناريوهاي حملة جعل نقش عليه پروتكلهاي احراز اصالت با وجود نفوذي فعال بيان ميگردد. در ادامه به عنوان نمونه، توصيف و تحليل پروتكل احراز اصالت Woo-Lam [۱۶] و چگونگي كشف يك سناريوي حمله عليه آن به كمك روش ارائه شده را شرح ميدهيم. در پايان نيز نتيجهگيري مطلب ارائه خواهد شد.

۲- توصيف صوري پروتكل

در اين قسمت ابتدا يك زبان توصيف نمونه براي توصيف پروتكل و قابليتهاي نفوذي ارائه ميكنيم، سپس به تشريح مختصر مدل محاسباتي مطرح شده در [۱۳] ميپردازيم. توصيف پروتكل به كمك اين مدل، بستر صوري لازم را براي تحليل نقش نفوذي فراهم ميكند كه در بخشهاي بعد به آن ميپردازيم.

۲-۱- زبان توصيف L

چون در اين مقاله هدف تحليل عملكرد نفوذي است، تنها به بيان نمادها و مسندات موردنياز براي توصيف پروتكل و بيان قابليتهاي نفوذي (EIR) بسنده ميكنيم. گرامر يك زبان ساده براي انجام اين كار به همراه برخي توضيحات راجع به مفهوم نمادهاي به كار رفته در شكل (۱) نشان داده شده است.

نمادهاي $\lhd$ و $\ni$ را به ترتيب جهت نشان دادن مسند پيام و مسند مالكيت به كار ميبريم. $\lhd$ (P,Q,X) به معناي ارسال پيام X از طرف عامل P به عامل Q و $\ni$ (P, X) به معناي تملك پيام X توسط عامل P است. مسندات $State_i$ نيز مسندات وضعيت هستند.

۲-۲- مدل محاسباتي پروتكل

هر عامل در پروتكل براي انجام صحيح پروتكل نياز به انجام يك سري عمليات دارد. ريزترين عمليات پايهاي[۵] كه در يك پروتكل توسط يك عامل انجام ميشود را يك توانايي[۶] مينامیم. يك توانايي داراي دو مؤلفه است: مجموعه پيششرطهاي آن توانايي و مجموعه پسشرطهاي آن توانايي. در صورت فراهم بودن پيششرطهاي يك توانايي، آن توانايي قابل اجرا است و با اجراي آن توانايي، پسشرطهاي آن نيز فراهم ميشوند. به عبارت ديگر، هر توانايي براي قابل انجام بودن نيازمند وجود بعضي شرايط در پروتكل است و در صورت انجام, ممكن است شرايط را تغيير دهد.

تعريف ۱ (توانايي): دوتايي < pre , post > كه در آن pre و post هر كدام مجموعهاي از دانشها با پارامترهاي متغير[۷] در زبان L هستند, تشكيل يك توانايي α را ميدهند.

توانايي α را به صورت ظاهري $L_\alpha : \frac{pre}{post}$ نشان ميدهيم كه L_α برچسب نام اين توانايي است.

pre و post به ترتيب مجموعه پيششرطها و پسشرطهاي توانايي هستند. اگر α يك توانايي باشد، از $pre(\alpha)$ و $post(\alpha)$ به ترتيب براي نشان دادن اين دو مجموعه استفاده ميكنيم. عناصر اين دو مجموعه، عباراتي در رابطه با دانش پروتكل (دانش محلي عوامل يا دانش سراسري پروتكل) هستند. در صورت فراهم بودن پيششرطهاي يك توانايي، آن توانايي قابل اجرا است و با اجراي آن توانايي، پسشرطهاي آن نيز فراهم ميشوند. در ساخت مجموعههاي pre و post بايستي از دانش قابل تعريف در زبان L استفاده كرد.

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) |	// لیستي شامل X و Y
$\{X{:}Formula\}_{K:Formula}$ |	// رمز شدة X با كليد K
$F(X_1 : Formula, X_2 : Formula, \ldots)$ |	// 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::= $\lhd$ (P: Principal, Q: Principal, X: Formula) |	// پيام X از طرف P به Q ارسال شده
$\ni$ (P: Principals, X: Formula) |	// عامل P فرمول X را مالك است.
$State_1 \mid State_2 \mid \ldots$	// 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 ($\lhd$) 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:

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

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

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 مفاهيم قدم و توانايي كه در بالا مطرح شد، براي تكميل مدل محاسباتي پروتكل بايستي نحوة ارتباط بين قدمهاي پروتكل را نيز تعيين نماييم. براي اينكار براي هر پروتكل يك مسير اجرا تعريف مي‌كنيم. مسير اجراي پروتكل حاصل تلفيق نحوي[1] قدمهاي نقشهاي پروتكل است. ساخت مسير اجراي يك پروتكل يك فرايند نحوي است به اين معني كه براي ايجاد مسير اجرا، قدمهاي مختلف براساس يك سري ضوابط نحوي با يكديگر مرتبط مي‌شوند و در اين مرحله معناي پيش‌شرط و پس‌شرط تواناييهاي هر قدم دخالتي ندارند. دو قدم از پروتكل با يكديگر مرتبط مي‌شوند، اگر دانش پس‌شرط آخرين توانايي يكي از قدمها با دانش پيششرط اولين توانايي قدم ديگر قابل انطباق باشد. به عبارت ديگر ضابطة نحوي مورد استفاده در ارتباط قدمهاي پروتكل با يكديگر، قابليت يكسان‌سازي[2] دانشهاي پس شرط و پيش‌شرط تواناييهاي اول و آخر آنها است.

تعريف ۳ (قابليت دسترسي قدمها به يكديگر): 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 صورتيكه $out(S_i)\theta = in(S_j)\theta$، يعني $out(S_i)$ و $in(S_j)$ قابل يكسان‌سازي[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 تشكيل مي‌دهند. اگر ρ يك نقش به صورت $S_1.S_2\dots S_m$ باشد، $S_i(\rho)$ نشان دهندة قدم i ام نقش ρ است.

تعريف ۵ (پروتكل): پروتكل P يك سه تايي به صورت $<\Lambda, S, A>$ است كه در آن Λ مجموعة نقشهاي پروتكل است، S مجموعة قدمهاي تشكيل دهنده اين نقشها و A مجموعة تواناييهاي تشكيل دهندة قدمها است. اگر قدمهاي مقداردهي اوليه (S_{INIT}) و شروع (S_{START}) در مجموعه قدمهاي يك پروتكل P به كمك يك تابع جايگذاري σ، ground شوند، به ماحصل يك نمونة پروتكل P به ازاء σ گوئيم و با P_σ نشان مي‌دهيم.

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

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

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

-قدمهاي سوم تا آخر اين مسير اجرا، ساير قدمهاي نقشهاي Λ هستند، به صورتي كه هر قدم از قدم بلافاصله قبل از آن قابل دسترس است.

-هيچ دو قدم پي‌درپي در مسير اجرا متعلق به يك نقش نيستند.

-رعايت تقدم و تأخر قدمهاي هر نقش، در رشتة اجرا نيز به قوت خود باقي است.

مسير اجرايي R(P) را به صورت دقيق‌تر مي‌توان چنين توصيف نمود :

$$
\begin{aligned}
&R(P) = t_0, t_1, t_2, \ \dots, t_n \\
&t_0 = S_{INIT} \\
&t_1 = S_{START} \\
&\forall i \ge 1, \exists \rho', \rho'' \in \Lambda, \exists k', k'', \delta_i \bullet \\
&\qquad S_{k'}(\rho') = t_i, S_{k''}(\rho'') = t_{i+1}, \\
&\qquad\qquad out\,(t_i\delta_1\dots\delta_i) = in\,(t_{i+1}\delta_1\dots\delta_i), \\
&\qquad \rho' \ne \rho'' \\
&\forall i, j \exists \rho' \in \Lambda, \exists k', k'' \bullet S_{k'}(\rho') = t_i, S_{k''}(\rho') = t_j, \\
&\qquad k' < k'' \Rightarrow i < j
\end{aligned}
$$

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

تعريف ۷ (نشست پروتكل): اگر P يك پروتكل و $R(P) = t_0, t_1,\dots, t_n$ مسير اجراي پروتكل P باشد، Session(P) نشست پروتكل P، يك نمونة خاص شده از R(P) است كه به صورت زير ساخته مي‌شود:

$$
\begin{aligned}
Session(P) &= t_0.t_1.(t_2\delta_1).(t_3\delta_1\delta_2). \ \dots \ .(t_n\delta_1\dots\delta_{n-1}), \\
&\forall i \ge 1,\ out(t_i\delta_1\dots\delta_i) = in(t_{i+1}\delta_1\dots\delta_i)
\end{aligned}
$$

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

۳- تحليل پروتكل با فرض وجود نفوذي

در مدل محاسباتي مطرح شده در بخش قبل، مسير اجراي يك پروتكل را تعريف نموديم. اين مسير اجرا رشته‌اي از قدمهاي مختلف از نقشهاي پروتكل است كه از طريق يك رابطة نحوي با يكديگر مرتبط شده‌اند. نفوذي با داشتن بعضي دانشهاي اوليه و قابليتها

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.

۳-۱- 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 اولية 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 اولية 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 ۸ (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 ۲). 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.

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

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

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

- **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).

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

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

- 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.

۲-۳- 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 وروديهاي قدمهاي آن نقش را در آن مسير اجرا تأمين كند. اين اصل شرط لازم براي انجامپذيري 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 انجامپذيري آن استفاده مي‌كنيم.

تعريف ۹ (قدمهاي يك نقش در مسير اجرا): فرض كنيد كه $P=\langle\Lambda, S, A\rangle$ 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:

$$\text{(پيشكش)}\quad gift(\rho @ R_l(P)) = out(r_m)\ ,$$

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

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 $P=\langle\Lambda, S, A\rangle$ 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.

تعريف 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 $K(\varepsilon) \not\models_{EIR} G'$)

تعريف ۱۳ (وارسي ويژگي اصـالت موجوديتهـا): نفـوذي مي‌تواند يك نقش را به كمك راهبرد فريب در يك مسير اجـرا فريب دهد اگر بتوانـد تمـامي جاخاليهـاي وي را در آن مـسير اجرا فراهم كند، يعني با كمك دانش و قابليتهاي خود قادر بـه استنتاج آنها باشد (يعني $K(\varepsilon) \models_{EIR} \text{hole}(\rho @ R(P))$)

۴- وارسي يك پروتكل نمونه

در ايـن بخش پروتـكل احـراز اصـالت 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.

$$
\begin{array}{ll}
(1) & A \rightarrow B : A \\
(2) & B \rightarrow A : N_B \\
(3) & A \rightarrow B : \{N_b\}_{K_{AS}} \\
(4) & B \rightarrow S : \{A, \{N_b\}_{K_{AS}}\}_{K_{BS}} \\
(5) & S \rightarrow B : \{N_b\}_{K_{BS}}
\end{array}
$$

شكل ۲- پروتكل احراز اصالت Woo-Lam

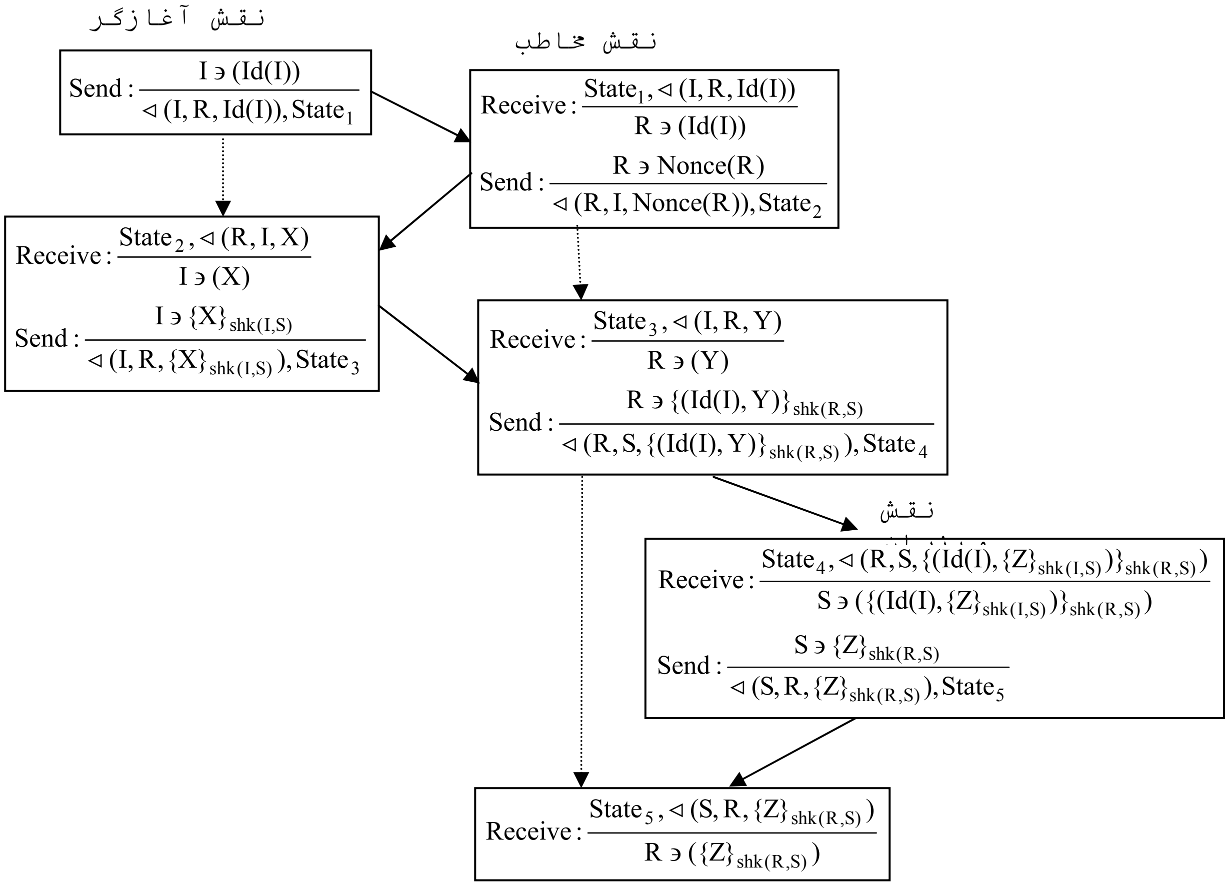
پروتكل به صورت زير عمل ميكند: (۱) نقش آغازگر در قدم اول پروتكل با ادعاي هويت A و ارسال آن به مخاطب، از وي تقاضاي احراز اصالت مي‌كند. (۲) مخاطب با ارسال نانس N_B، آغازگر را براي اثبات ادعاي خود به تحدي فرا مي‌خواند. (۳) در قدم سوم، آغازگر براي مقابله با اين تحدي، پيام N_B را با كليد مشترك بين خود و ميزبان 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 مشتـرك بين خود و ميزبان رمزكرده، براي ميزان ارسال ميكنـد. (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 آغازگـر پروتـكل 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 تـوانايي Receive و Send است. به شرط قرار گرفتن در وضعيت $State_2$ و ارسال پيامي‌مثل X روي شبكه، آغازگر مالك پيام X خواهد شد و در صورتيكه او بتواند پيام X را با كليد مشترك بين خود و ميزبان رمز كند (و آن را مالك شود)، آن را روي شبكه خواهد گذاشت و وضعيت $State_3$ خواهد شد. قدمهاي ساير نقشها نيز به همين ترتيب توصيف شده‌اند.

فرضيات اوليه پروتكل Woo-Lam بايستي در قالب قدم مقداردهي اولية پروتكل تعيين شود. اين فرضيات، دانش اولية همة نقشها را تعيين مي‌كند. نقشهاي آغازگر و مخاطب پروتكل Woo-Lam داراي كليدهاي اشتراكي با ميزبان هستند. نقش مخاطب در پروتكل داراي يك نانس است و ميزبان نيز هر دو كليد مشترك را دارا است. به علاوه براي شروع پروتكل لازم است آغازگر شناسة خود را نيز بداند. قدم مقداردهي اولية پروتكل 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 پروتكل (تعريف ۷)، با در نظر گرفتن يك تابع جايگزيني براي نمونة موردنظر پروتكل، شروع از قدم اول آغازگر (قدم شروع پروتكل) و يكسانسازي ورودي/خروجي قدمهاي دسترسي‌پذير، مي‌توان نشست موردنظر پروتكل را ايجاد نمود.

۴-۳- وارسي صوري پروتكل Woo-Lam

فرض كنيد براي تحليل آسيب‌پذيري پروتكل، نشستي از پروتكل را كه با تابع جايگذاري $\sigma_1 = \{I/a, R/b, S/s\}$ مشخص مي‌شود را در نظر بگيريم. هدف پروتكل، 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:

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

(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:

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

(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 $\sigma_2 = \{I/a, R/b, S/s\}$ است را شروع مي‌كند. در اين حالت داريم:

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

(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:

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

(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)

$$\begin{array}{l} \lhd (b,a,Nonce(b)) \in K(\varepsilon) \overset{NET}{\Rightarrow} \\ \lhd (b,a,Nonce(b)) \in K(\varepsilon) \Rightarrow \\ K(\varepsilon) \models \lhd (b,a,Nonce(b)) \end{array}$$

(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:

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

(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، بنـابراين در نمونـة جديـد اجـراي پروتكـل $\sigma_3=\{I/c,R/b,S/s\}$ است. حال نفوذي تحليل خود را بـه كمـك اين نشست جديد پي مي‌گيرد. وي مي‌داند كه:

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

بنابراين كافي است كه نفوذي بتواند جاخاليهاي نقش ميزبان را در مسير اجراي اين نشست به ازاء Z=Nonce(b) فراهم كند، يعني بايستي بتوانيم قضية زير را اثبات كنيم:

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

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

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

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

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

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

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

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 كمك پيام Nonce(b) كه قبلاً شنود كرده است و shk(c,s) كه به صورت پيش‌فرض جزئي از دانش نفوذي است بسازد. (دقت كنيد كه عامل c همان نفوذي است):

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

(۱۲)

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

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

حال به كمك (۲)، (۶)، و (۱۳)، قضية (۱) اثبات مي‌شود. اين بدان معنا است كه نفوذي به كمك راهبرد فريب و با استفاده از دو نشست جديد پروتكل قادر به فريب مخاطب خواهد بود. سناريوي اين فريب در شكل (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 كرد كه سناريوي حاصل منطبق بر روند تحليل فوق مي‌باشد.

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

شكل ٤- سناريوي حملة كشف شده عليه پروتكل احراز اصالت Woo-Lam

۵- نتیجه گیری

در این مقاله با بهکارگيري چارچوب و مدل محاسباتي مطـرح شده در [۱۳]، روشي براي در نظرگرفتن نقـش نفـوذي در مـدل صوري پروتكل و تحليل نقش وي در كسب دانش از پروتكـل يـا فريب دادن عوامل مجاز ارائـه شـده اسـت. در مـدل محاسـباتي مورداستفاده، عوامل پروتكل به عنوان نقشهايي داراي تواناييهـاي مشخص در نظر گرفته شده‌اند. تواناييهاي بالقوه هر نقـش دقيقـاً براساس تعريف پروتكل به فعليـت مـي‌رسـد و قـدمهاي متـوالي اجراي پروتـكل را تشـكيل مي‌دهند. رشتة خاصـي از تواناييهـاي نقشهاي مختـلف پروتـكل كـه طبـق تعريـف پروتكـل بايـستي بـه فعليت برسند، مسير اجراي پروتكل را تشكيل مي‌دهـد. روي اين مسير اجرا مي‌توان در مورد دانش نفوذي (مجموعه مسندات راجع به يافته‌هاي نفوذي از پروتكل) و همچنين قابليـت نفـوذي در سـوء اسـتفاده از ايـن مسير اجرا براي فريـب نقـشهاي مجـاز بـه استنتاج پرداخت.

در روش ارائه شده، نقش نفوذي در دو حالت غيرفعال و فعال در نظر گرفته شده است. تحليل اين دو حالت به ترتيب، امكان وارسي نقض ويژگيهاي اختفاء پيامها و اصالت موجوديتها را فراهم ميآورد. نفوذي در نقش فعال و غيرفعال ميتواند پيامهاي پروتكل را شنود كرده، با كمك اصول استنتاجي خود، دانش خود را گسترش دهد. نفوذي در حالت فعال سعي دارد عوامل مجاز پروتكل را فريب دهد كه براي انجام اينكار از دو اصل راهبردي بهره مي‌گيرد. نخست اينكه براي فريب يك عامل بايستي تمام درخواستهاي وي را پاسخ دهد، و ديگر اينكه، به شرط فراهم كردن زمينه‌هاي لازم براي اجـراي پروتـكل تـا يك مرحلة موردنظر، مي‌تواند از پروتكل بـه عنوان يك منبع توليد دانش استفاده كند.

ويژگي اصلي روش ارائه شده كه در واقع تعميم مدل كلي Doleve-Yao [۱۱] به شمار مي‌آيد، مورد توجه قرار دادن راهبرد انجام حمله به عنوان يكي از قابليتهاي كليدي نفوذي در انجام حمله است. در روشهاي موجود تحليل آسيب‌پذيري پروتكل از جمله [۶-۱۰] كه همگي مبتني بر روش Doleve-Yao هستند، مجموعه‌اي از قابليتهاي محاسباتي و ارتباطي براي نفوذي در نظر گرفته مي‌شود ولي چون مدل Doleve-Yao نحوة بهكارگيري اين قابليتها توسط نفوذي را تعيين نمي‌كند، اين قابليتها به عنوان ابزاري براي گسترش فضاي حالت اجراي پروتكل (به همراه نفوذي) مورداستفاده قرار گرفته و نهايتاً براي يافتن وضعيتهاي ناامن در اين فضاي ايجاد شده جستجو مي‌شود. از آنجاكه فضاي حالت ايجاد شده حتي با در نظر گرفتن حداقل قابليتهاي يك نفوذي نيز يك فضاي نامتناهي است [۱۶]، بنابراين مشكلاتي براي روشهاي تحليل آسيب‌پذيري به وجود مي‌آيد. روشهايي كه براي پياده‌سازي تحليل از بررسي مدل استفاده مي‌كنند مجبورند با تنظيم پارامترهاي تحليل مرزهاي فضاي حالت را تعيين كنند كه البته اين كار تماميت[1] تحليل را از بين ميبرد. در روشهاي اثبات قضيه نيز به دليل اينكه بايستي هوشمندي نفوذي خارج از حوزة قابليتهاي وي و به عنوان يك ويژگي اقتضائي[2] در فرايند اثبات در نظر گرفته شود، توصيف فرايند تحليل پيچيده ميشود.

در روش ارائه شـده، اسـتفاده از راهبـرد مـشخص در انجـام حمله به عنوان بخشي از قابليتهاي ذاتي يك نفـوذي هوشـمند در نظر گرفتـه شـده و بنـابراين، ايـن قابليـت نيـز بـه صـورت يكنواخت با ساير قابليتهاي نفوذي در خدمت كسب و گسترش دانش از پـروتكل و اسـتفاده از ايـن دانـش در جهـت هـدف حملـه قـرار مـي‌گيـرد. بـه ايـن ترتيـب تحليـل آسـيبپـذيري پروتكلهاي رمزنگاري نسبت به حملات نفوذي در روش مطـرح شده، به صورت اثبات قضايايي راجع بـه عملـي شـدن راهبـرد حملة نفوذي انجام مي‌شود. چون تمامي قابليتهـاي نفـوذي در تحليل به كمك قابليت راهبردي وي در انجام حمله جهـتدهي مي‌شود، بنابراين در صورت اثبات قضاياي موردنظر در تحليـل، قدمهاي اثبات دقيقاً معادل سناريـوي انجام حمله خواهد بـود. بر اين اساس مي‌توان گفت كـه مزيـت اصـلي روش ارائـه شـده نسبت بـه روشـهاي ديـگر، تأكيـد روي مـدل‌سـازي هوشـمندي نفوذي بـه عنوان يـك قابليـت اصـلي وي بـه جـاي حـذف ايـن هوشمندي و انجام جستجوي فراگيـر فـضاي حالـت (كـاري كـه روشـهاي بررسـي مـدل انجـام مـي‌دهنـد) و يـا مـدلسازي ايـن هوشمندي به صورت اقتضائي در توصيف فرايند تحليل (كاري كه روشهاي اثبات قضيه انجام مي‌دهند) ميباشد.

ايدة ارائه شده در اين مقاله براي توصيف نقـشها و قـدمهاي پروتكل، با مفهوم parametric strand space ارائه شـده توسـط Millen [۱۷] قابل مقايسه است. يك نقش را مـيتـوان معـادل يك Parametric Strand و مسير اجراي پروتكل را معادل يـك Strand bundle دانست، با اين تفاوت كه در روش ما، بـا توجـه بـه اسـتفاده از روش اثبـات قـضيه، از مزايـاي گـذر- وضـعيت

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