**مهندسی نیاز مندی ها**

چكيده دنياي نرم افزار در سال هاي اخير با چالشي به نام امنيت روبرو شده است. رويكرد جديدي كه امروزه در امنيت نرم افزار مورد توجه قرار گرفته تفكر امنيتي در فرايند توليد نرم افزار مي باشد. از آنجايي كه امنيت يک نياز غير تابعي است، اكثر مواقع در فاز نيازمندي ها از آن چشمپوشي ميشود. اما كاهش هزينه توسعهي نرمافزار و زمان مورد نياز براي شناسايي نيازهاي امنيتي كاربر در مراحل اوليه فرآيند توسعه نرمافزار امكانپذير است. امنيت IT بايد براي اطمينان از سيستم قابل اعتماد و محافظت از داراييهاي سازمان كسب و كار اعمال شود. به اين منظور، موضوع اصلي ارائه نيازمنديهاي امنيتي به كاربر در تركيب با نيازهاي عملكردي كاربر است كه در فاز نيازمندي در چرخه عمر توسعه نرمافزار (SDLC ) جمعآوري ميشود. چرخه عمر توسعه نرمافزار امن (SSDLC ) از نيازمنديهاي امنيتي شروع ميشود. اگر بتوانيم نيازهاي امنيتي كاربر را استخراج كرده و آنها را در فاز نيازمنديها ارائه كنيم، از توسعهي نرمافزار امن از همان ابتدا اطمينان حاصل ميشود. اين مقاله نشاندهنده پژوهش حاضر در مورد مقايسه روشهاي مهندسي نيازمندي هاي امنيتي فعلي، مانند ضوابط SQUARE ،امن Tropos ،مشترک SREP ، MSRA ، و فريم مشكل، و همچنين روش هاي مبتني بر UML است.

در سال هاي اخير، رشد فزاينده ي شبكه و اهميت اطالعات باعث شده است كه به نيازمندي هاي امنيتي با نگاه ويژ ه اي نگريسته شود. افزودن نيازمندي هاي امنيتي بدين معني است كه امنيت در اولين مراحل توليد نرم افزار مدنظر بوده و هدف، ساخت نرم افزاري امن، پايدار و قابل اعتماد مي باشد),2003Firesmith). از آنجايي كه امنيت يک نياز غير تابعي است، اكثر مواقع در فاز نيازمندي ها از آن چشمپوشي ميشود. اما كاهش هزينه توسعهي نرمافزار و زمان مورد نياز براي شناسايي نيازهاي امنيتي كاربر در مراحل اوليه فرآيند توسعه نرمافزار امكانپذير است. امنيت IT بايد براي اطمينان از سيستم قابل اعتماد و محافظت از داراييهاي سازمان كسب و كار اعمال شود. بدين ترتيب موضوع اصلي ارائه نيازمنديهاي امنيتي به كاربر 7 در تركيب با نيازهاي عملكردي كاربر است كه در فاز نيازمندي در چرخه عمر توسعه نرمافزار (SDLC ) جمعآوري ميشود. 8 چرخه عمر توسعه نرمافزار امن (SSDLC ) از نيازمنديهاي امنيتي شروع ميشود. اگر بتوانيم نيازهاي امنيتي كاربر را استخراج كرده و آنها را در فاز نيازمنديها ارائه كنيم، از توسعهي نرمافزار امن از همان ابتدا اطمينان حاصل ميشود. اين مقاله نشاندهنده پژوهش حاضر در مورد مقايسه روشهاي مهندسي نيازمندي هاي امنيتي فعلي، مانند ضوابط مشترک، Tropos امن، SQUARE ، SREP، MSRA و همچنين روش هاي مبتني بر UMLو فريم مشكل است. معرفي روش تحليل نيازمندي هاي امنيتي چند جانبه )MSRA ) هدف تحليل نيازمندي هاي امنيتي چند جانبه )MSRA )اعمال اصول امنيت چند جانبه طي مرحله مهندسي نيازمندي ها توسعه سيستم است(2006 ,al et S Gurses(. اين كار با تحليل نيازهاي امنيتي و حريم خصوصي همه ذينفعان يک سيستم، شناسايي تعارض ها و تحكيم ديدگاه هاي مختلف ذينفع صورت مي گيرد. اين روش از نظريه هاي امنيت چندجانبه و مهندسي نيازمنديهاي ديدگاه محور استفاده مي كند. در شكل 2 مراحل اصلي روش تحليل نيازمندي هاي امنيتي چندجانبه ارائه شده، البته وقتي تحليل نيازمندي هاي كاركردي اوليه براي كاركردهاي اصلي سيستم صورت مي گيرد:

****

در اين روش همه اهداف CIA در نظر گرفته مي شوند، اگرچه بر حريم خصوصي، محرمانگي و انسجام تمركز كرده است. MSRA بر امنيت چندجانبه تاكيد مي كند و بر ديدگاه هاي ذينفعان، نيازمندي امنيتي و تطبيق نيازمندي مغاير تمركز مي كند. اين روش به تعامالت ميان نيازمندي هاي امنيتي و نيازمندي هاي كاركردي و امنيتي اشاره مي كند.

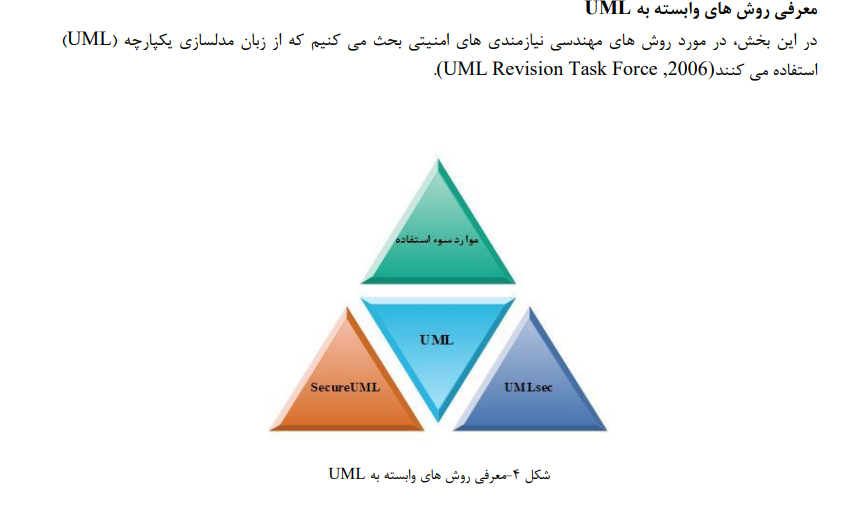
معرفي روش مهندسي نيازمندي هاي كيفيت امنيتي )SQUARE) SQUARE) 2006 ,al et S Gurses(يک روش جامع براي مهندسي نيازمندي هاي امنيتي است كه استفاده از تكنيک هاي ديگري كه در اين حوزه توسعه يافته اند را توصيه مي كند. هدف آن، ادغام مهندسي نيازمندي هاي امنيتي با فرايندهاي توسعه نرم افزار است(2008 ,al et N Mead(. SQUARE بر قابليت اجرا در پروژه هاي توسعه نرم افزار واقعي تاكيد مي كند و بنابراين يک چهارچوب سازماني براي اجراي فعاليت هاي مهندسي نيازمندي هاي امنيتي فراهم مي كند. فرض شده كه SQUARE توسط ذينفعان و مهندسين نيازمندي ها صورت مي گيرد. اين روش شامل 9 مرحله مي شود كه در شكل 1 نشان داده شده است.



معرفي روش SQUARE-

تكميل تمام 9 مرحله فرآيند SQUARE ممكن است براي پروژه هاي بزرگ دو تا سه ماه طول بكشد. متاسفانه برخي از سازمانها قادر نيستند و يا نمي خواهند زمان و منابع زيادي را فقط براي نيازمندي هاي امنيتي اختصاص دهند. آنها مي خواهند با صرف هزينه كمتر به نتيجه مشابه برسند. قابليت استفاده مجدد از نيازمندي هاي امنيتي، فرصتي براي كاهش هزينه اجراي SQUARE مي باشد. استفاده مجدد از نيازمندي هاي امنيتي چندين فايده به فرآيند مهندسي نيازها ارائه مي دهد كه در جدول 2 شرح داده شده است.





موارد سوء استفاده )2001 ,AL Opdahl and G Sindre )روش مورد استفاده سيندر و اپدال مرسوم را تعميم مي دهند و موارد سوء استفاده را نيز در آن لحاظ مي كنند، كه رفتار ناخواسته در سيستم را نشان مي دهند، سيندر و اپدال اين الگو را براي توصيف

موارد سوء استفاده مناسب مي كنند، كه از استنباط و تحليل مفصل تهديدهاي امنيتي پشتيباني مي كند. به عالوه، آنها يک

روش تكرار شونده براساس تحليل تهديد و ريسک رايج ارائه مي كنند:

.2 شناسايي دارايي هاي حساس در سيستم

.1 تعريف اهداف امنيتي براي هر دارايي

.3 شناسايي تهديدهاي هر هدف امنيتي با شناسايي ذينفعاني كه ممكن است عمدا به سيستم يا محيط آن آسيب

بزنند. شناسايي مجموعه اقداماتي كه ممكن است باعث آسيب عمدي شوند.

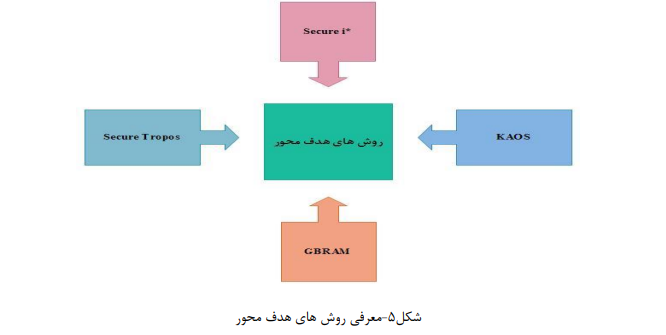
.4 شناسايي و تحليل ريسک هاي تهديدها )با استفاده از تكنيک هاي استاندارد(

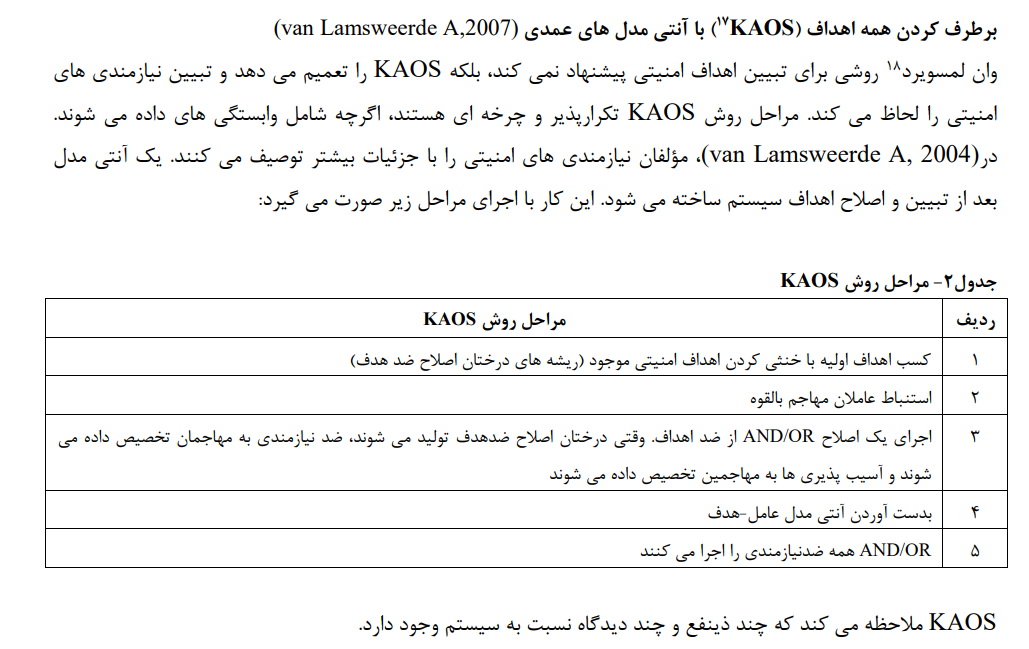
.5 تعريف نيازمندي هاي امنيتي براي تهديدها براي تطبيق با ريسک ها و هزينه هاي محافظت

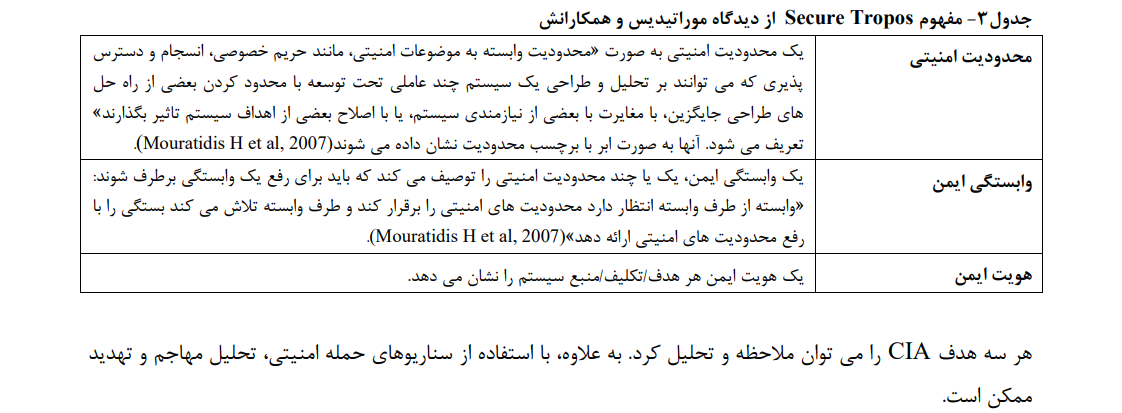
موارد سوء مصرف را مي توان براي يک سيستم طراحي اعمال كرد كه نيازهاي امنيتي مختلف را در برمي گيرد. مي توان هر

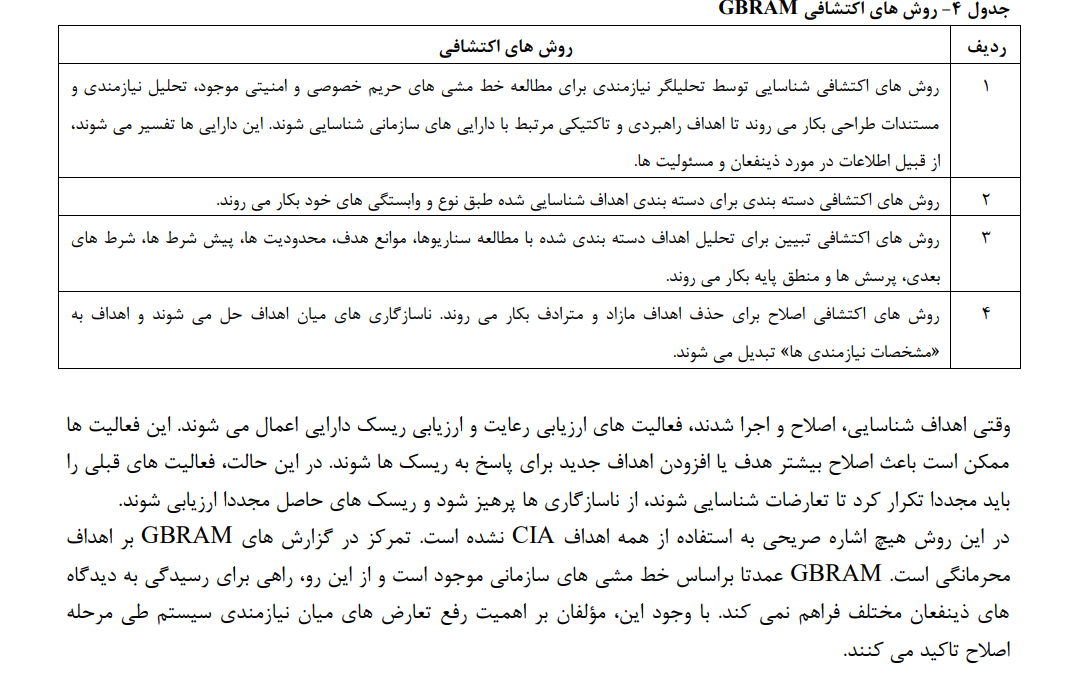
سه هدف CIA را در نظر گرفت. اين شامل تكنيک هاي تحليل تهديد و ريسک رايج مي شود.

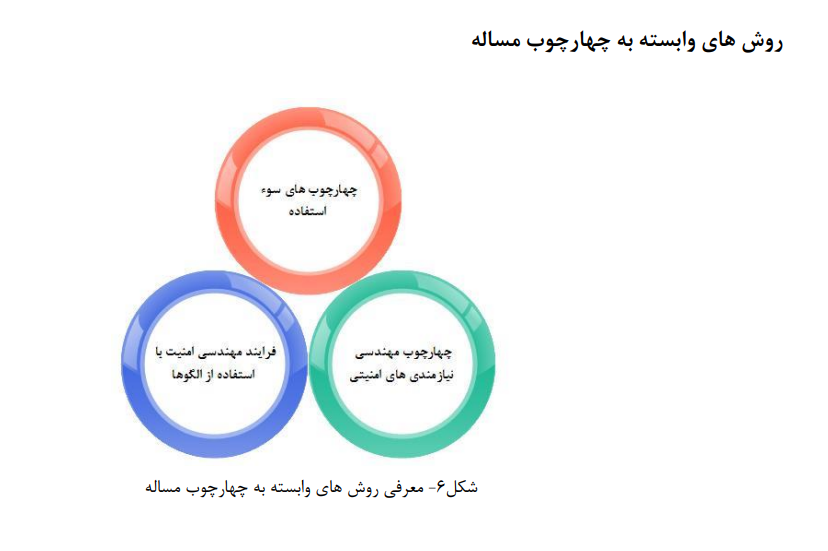
**معرفي روش هاي هدف محور**

****









چهارچوب هاي سوء استفاده

لين و همكارانش(2004 ,al et L Lin(پاد نيازمندي ها و چهارچوب هاي سوء استفاده نظير را تعريف مي كنند. يک پادنيازمندي ها، نيت هاي يک كاربر دشمن را بيان مي كند و يک چهارچوب سوء استفاده يک تهديد امنيتي را نشان مي دهد. مؤلفان بيان مي كنند كه هدف چهارچوب هاي سوء استفاده و پادنيازمندي ها، تحليل تهديدهاي امنيتي و كسب نيازمندي هاي امنيتي است. گفته مي شود كه اهداف امنيتي در ابتدا بايد با شناسايي دارايي هاي حساسي كه بايد محافظت شوند بدست آيند. مؤلفان براساس مجموعه اي از نيازمندي هاي كاركردي و اهداف امنيتي، يک روش تحليل تهديد تكراري شامل چهار مرحله پيشنهاد مي كنند: .2 شناسايي مسائل و مسائل فرعي با استفاده از چهارچوب هاي مساله رايج. توصيف نيازهاي امنيتي به عنوان محدوديت ها در كاركرد شناسايي شده. .1 شناسايي تهديدها و ايجاد نمودارهاي چهارچوب سوء استفاده. پادنيازمندي با خنثي كردن نيازهاي امنيتي و نمايش آنها در يک نمودار چهارچوب سوء استفاده بدست مي آيند. .3 شناسايي آسيب پذيري هاي امنيتي .4 اشاره به آسيب پذيري هاي امنيتي. گفته مي شود كه نيازمندي هاي امنيتي بدست مي آيند، براي مثال »محدود كردن تعداد امتحان ها براي وارد كردن رمز عبور«. هيچ مبناي رسمي يا مدل مهاجمي در اين روش در نظر گرفته نشده است. از آنجايي كه مؤلفان فقط مجموعه كوچكي از چهارچوب هاي سوء استفاده را نشان مي دهند، روشن نيست آيا سه هدف CIA در نظر گرفته شده است.

