L'architecture de sécurité OSI

Le marché de la sécurité informatique a connu une croissance significative. L'entreprise Gartner1 s'attend à ce que le marché de la cybersécurité dépasse les 100 milliards de dollars en 2019 contre 76 milliards de dollars en 2015.

Pour évaluer efficacement les besoins de sécurité d'une organisation et choisir divers produits et politiques de sécurité, le responsable de la sécurité a besoin d'un moyen systématique lui permettant de définir les exigences en matière de sécurité. L'architecture de sécurité OSI est utile aux gestionnaires pour organiser la tâche de sécurité. Elle a été développée en tant que norme internationale. Les fournisseurs d'ordinateurs et de communications ont développé des fonctionnalités de sécurité pour leurs produits et services qui se rapportent à cette définition structurée de services et de mécanismes.

L'architecture de sécurité OSI X.800 se concentre sur les attaques de sécurité, les mécanismes et les services. Ceux-ci peuvent être définis brièvement comme suit :

Attaque de sécurité : toute action qui compromet la sécurité des informations appartenant à une organisation.

Mécanisme de sécurité : un processus (ou un périphérique incorporant un tel processus) conçu pour détecter, prévenir ou récupérer une attaque de sécurité.

Service de sécurité : un service de traitement ou de communication qui améliore la sécurité des systèmes de traitement de données et les transferts d'informations d’une organisation. Les services sont destinés à contrer les attaques de sécurité, et ils utilisent un ou plusieurs mécanismes de sécurité pour fournir le service.

Les services de sécurité

- X.800 définit un service de sécurité comme un service fourni par une couche de protocoles de systèmes ouverts communicants, qui assure une sécurité adéquate des systèmes ou des transferts de données. X.800 divise ces services en cinq catégories et quatorze services spécifiques, comme présenté dans le Tableau.

Service de Sécurité	Description	Service spécifique de sécurité	Description
Authentification	L'assurance que l'entité communicante est celle qu'elle prétend être.	Authentification par entité intermédiaire	Utilisé en association avec une connexion logique pour donner confiance à l'identité des entités connectées.
		Authentification d'origine de données	Dans un transfert sans connexion, il fournit l'assurance que la source des données reçues est tel que revendiqué.
Contrôle d'accès	La prévention de l'utilisation non autorisée d'une ressource (c.-à-d., Ce service contrôle qui peut avoir accès à une ressource, dans quelles conditions l'accès peut se produire et ce que les personnes qui ont accès à la ressource peuvent faire).	N/A	N/A

La confidentialité des données	La protection des données contre la divulgation non autorisée.	Confidentialité de la connexion	La protection de toutes les données de l'utilisateur sur une connexion.
		Confidentialité sans connexion	La protection de toutes les données de l'utilisateur dans un seul bloc de données.
		Confidentialité de champ sélectif	La confidentialité des champs sélectionnés dans les données de l'utilisateur sur une connexion ou dans un seul bloc de données.
		Confidentialité du flux de trafic	La protection de l'information pourrait être dérivée depuis l'observation des flux de trafic.
L'intégrité des données	L'assurance que les données reçues sont exactement comme envoyées par une entité autorisée (c'est-à-dire ne contiennent aucune modification, insertion, suppression ou reproduction).	Intégrité de connexion avec récupération	Fournit l'intégrité de toutes les données utilisateur sur une connexion et détecte toute modification, insertion, suppression ou réponse.
		Intégrité de la connexion sans récupération	Comme ci-dessus, mais ne fournit qu'une détection sans récupération.
		Intégrité de connexion du champ sélectif	Fournit l'intégrité des champs sélectionnés dans les données utilisateur d'un bloc de données transféré sur une connexion et prend la forme de déterminer si les champs sélectionnés ont été modifiés, insérés, supprimés ou reproduits.
		Intégrité sans connexion du champ sélectif	Fournit l'intégrité des champs sélectionnés dans un seul bloc de données sans connexion ; Prend la forme de déterminer si les champs sélectionnés ont été modifiés.
Non répudiation	Fournit une protection contre le déni par l'une des entités impliquées dans une communication d'avoir participé à tout ou partie de la communication.	Non répudiation - Origine	Preuve que le message a été envoyé par la partie spécifiée.
		Non répudiation - Destination	Preuve que le message a été reçu par la partie spécifiée.

L’authentification

- Le service d'authentification est chargé d'assurer qu'une communication est authentique. Dans le cas d'un seul message, tel qu'un signal d'avertissement ou d'alarme, la fonction du service d'authentification est d'assurer au destinataire que le message provient de la source qu'il prétend être. Dans le cas d'une interaction continue, comme la connexion d'un terminal à un hôte, deux aspects sont impliqués. Tout d'abord, au moment de l'initiation de la connexion, le service garantit que les deux entités sont authentiques, c'est-à-dire que chacune est l'entité qu'elle prétend être. Deuxièmement, le service doit s'assurer que la connexion n'est pas entravée de telle sorte qu'un tiers peut se faire passer comme l'une des deux parties légitimes aux fins d'une transmission ou d'une réception non autorisée.
- Deux services d'authentification spécifiques sont définis dans X.800:
  - Authentification par entité intermédiaire
  - Authentification d'origine de données

Contrôle d'accès

- Dans le contexte de la sécurité du réseau, le contrôle d'accès permet de limiter et de contrôler l'accès aux systèmes hôtes et aux applications via les liaisons de communication. Pour ce faire, chaque entité qui tente d'accéder doit d'abord être identifiée ou authentifiée, de sorte que les droits d'accès peuvent être adaptés à l'individu.

Confidentialité des données

- La confidentialité est la protection des données transmises contre les attaques passives. En ce qui concerne le contenu d'une transmission de données, plusieurs niveaux de protection peuvent être identifiés. Le service le plus large protège toutes les données transmises entre deux utilisateurs sur une période de temps. Par exemple, lorsqu'une connexion TCP est configurée entre deux systèmes, cette protection large empêche la sortie de toute donnée utilisateur transmise sur la connexion TCP. Des formes plus étroites de ce service peuvent également être définies, y compris la protection d'un seul message ou même des champs spécifiques dans un message. Ces améliorations sont moins utiles que l'approche générale et peuvent même être plus complexes et coûteuses à mettre en oeuvre.
- Il y’a un autre aspect de la confidentialité, qui est la protection des flux de trafic liés à l'analyse. Cela nécessite qu'un attaquant ne puisse pas observer la source, la destination, la fréquence, la longueur ou d'autres caractéristiques du trafic dans une installation de communication.

Intégrité des données

- Comme pour la confidentialité, l'intégrité peut s'appliquer à un flux de messages, un seul message ou des champs sélectionnés dans un message. Encore une fois, l'approche la plus utile et la plus simple est la protection totale des flux.
- Un service d'intégrité axé sur la connexion, qui traite d'un flux de messages, assure que les messages sont reçus comme envoyés, sans : duplication, insertion, modification, réorganisation ou répétition.

Non répudiation

- La non répudiation empêche l'émetteur ou le récepteur de refuser un message transmis. Ainsi, lorsqu'un message est envoyé, le destinataire peut prouver que l'expéditeur présumé a en effet envoyé le message. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le prétendu séquestre a effectivement reçu le message.

Service de disponibilité

- Les deux X.800 et RFC 2828 définissent la disponibilité pour être la propriété d'un système ou une ressource système accessible et utilisable à la demande par une entité système autorisé, selon les spécifications de performance du système. Une variété d'attaques peut entraîner la perte ou la réduction de la disponibilité. Certaines de ces attaques sont soumises à des contremesures automatises, telles que l'authentification et le cryptage, tandis que d'autres nécessitent une sorte d'action physique pour éviter ou se remettre de la perte de disponibilité des éléments d'un système distribué.
- X.800 traite en outre la disponibilité en tant que propriété d'être associée à divers services de sécurité. Un service de disponibilité est celui qui protège un système pour assurer sa disponibilité. Ce service répond aux problèmes de sécurité soulevés par les attaques de déni de service.

Les mécanismes de sécurité

- Le tableau suivant énumère les mécanismes de sécurité définis dans X.800. Les mécanismes sont divisés en ceux implémentés dans une couche de protocole spécifique et ceux qui ne sont pas spécifiques à une couche de protocole ou à un service de sécurité particulier.
  - *Mécanismes de sécurité spécifiques* : Peuvent être incorporé dans la couche de protocole appropriée afin de fournir certains des services de sécurité OSI.
  - *Mécanismes de sécurité omniprésents :* Mécanismes qui ne sont pas spécifiques à un service de sécurité OSI ou à une couche de protocole particulier.

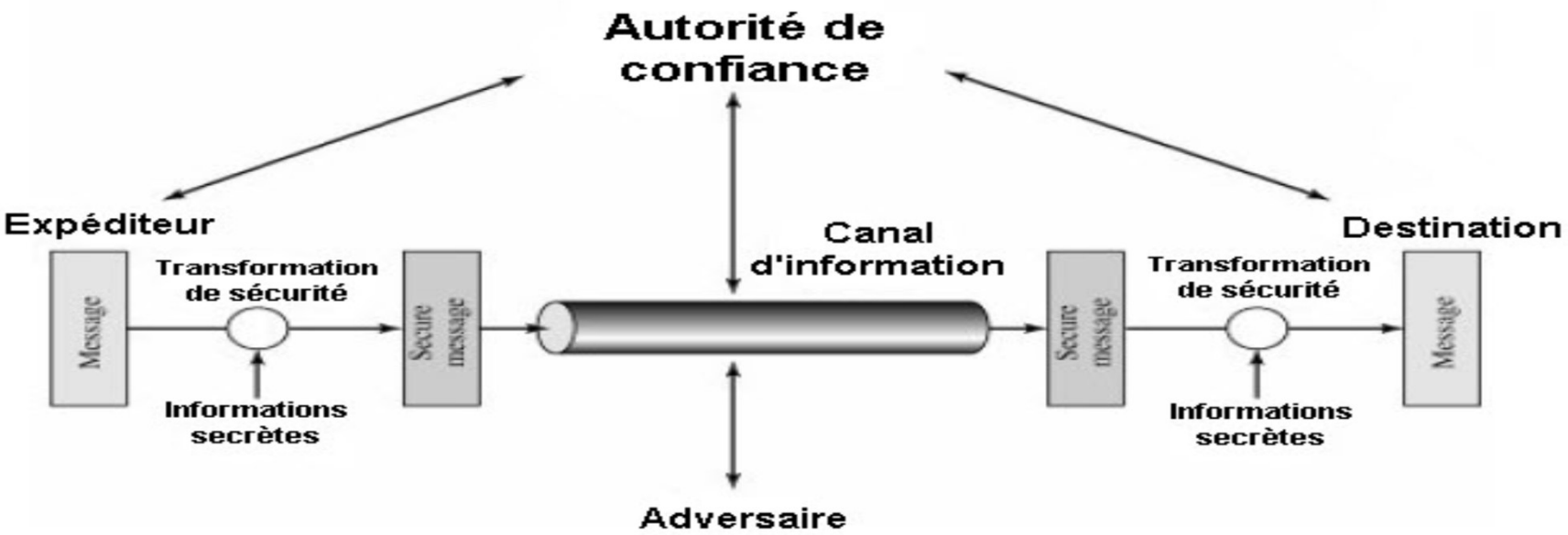
	Mécanisme	Description
Mécanismes De Sécurité Spécifiques	Le chiffrement	L'utilisation d'algorithmes mathématiques pour transformer les données en une forme qui n'est pas facilement intelligible. La transformation et la récupération ultérieure des données dépendent d'un algorithme et de clés de cryptage.
	Signature numérique	Les données sont ajoutées, ou une transformation cryptographique d'une unité de données.
	Contrôle d'accès	Divers mécanismes qui imposent les droits d'accès aux ressources.
	Intégrité des données	Divers mécanismes utilisés pour assurer l'intégrité d'une unité de données ou d'un flux d'unités de données.
	Echange d'authentification	Un mécanisme destiné à assurer l'identité d'une entité au moyen d'un échange d'informations.
	Remplissage du trafic	L'insertion de bits dans des intervalles dans un flux de données pour éviter les tentatives d'analyse de trafic.
	Contrôle de routage	Permet de sélectionner des routes physiquement sécurisées particulières pour certaines données et permet des modifications de routage, en particulier lorsqu'une violation de sécurité est suspectée.
	Notarisation	L'utilisation d'un tiers de confiance pour assurer certaines propriétés d'un échange de données.
Mécanismes de sécurité omniprésents	Fonctionnalité de confiance	Ce qui est perçu comme correct par rapport à certains critères (par exemple, tel qu'établi par une politique de sécurité).
	Étiquette de sécurité	Le marquage lié à une ressource (qui peut être une unité de données) qui nomme ou désigne les attributs de sécurité de cette ressource.
	Détection d'événement	Détection des événements liés à la sécurité.
	Sentier d'audit de sécurité	Les données recueillies et utilisées pour faciliter une vérification de la sécurité, qui est un examen et un examen indépendants des dossiers et des activités du système.
	Récupération de sécurité	Aborde les demandes de mécanismes, telles que la gestion des événements et prend des mesures de récupération.

Le tableau de relation entre les services de sécurité et les mécanismes de sécurité.

Mécanisme								
Service	Chiffrement	Signature numérique	Contrôle d'accès	Intégrité des données	Echange d'authentification	Remplissage du trafic	Routage	Contrôle de la notarisation
Authentification	X	X			X			
Authentification d'origine des données	X	X						
Contrôle d'accès			X					
Confidentialité	X						X	
Confidentialité des flux de trafic	X					X	X	
Intégrité des données	X	X		X				
Non répudiation		X		X				X
Disponibilité				X	X			

Un modèle pour la sécurité réseau

Modèle:



Un modèle pour la sécurité réseau

- La figure précédente présente un modèle de sécurité réseau. Un message doit être transféré d’une partie à une autre à travers l'Internet. Les deux parties, qui sont les principaux de cette transaction, doivent coopérer pour que l'échange se produise. Un canal d'information logique est établi en définissant un itinéraire via Internet entre la source et la destination et par l'utilisation coopérative de protocoles de communication (par exemple, TCP / IP).

Documents recommandés

- [RChp11] fournit les bases de la compréhension de la sécurité matérielle et de la confiance, qui sont devenues des préoccupations majeures pour la sécurité nationale au cours de la dernière décennie. La couverture comprend les problèmes de sécurité et de confiance dans tous les types de dispositifs et systèmes électroniques tels que ASIC, COTS, FPGA, microprocesseurs / DSP et systèmes embarqués. Cela constitue une référence inestimable à la recherche de pointe qui revêt une importance cruciale pour la sécurité et la confiance dans les infrastructures soutenues par la microélectronique de la société moderne.
- [RChp12] est intéressant si vous êtes impliqué dans n'importe quel aspect du cloud computing.
- [RChp13] présente des concepts modernes de sécurité informatique. Il introduit l'arrièreplan mathématique de base nécessaire pour suivre les concepts de sécurité informatique. Les développements modernes en cryptographie sont examinés, à partir du cryptage de clé privée et de clé publique, en passant par le hachage, les signatures numériques, l'authentification, le partage secret, la cryptographie axée sur le groupe, la pseudo-émanation, les protocoles clés d'établissement, les protocoles de connaissance zéro et l'identification.

Documents recommandés

- [RChp14] vous guide dans les principes fondamentaux, en commençant par la façon dont la plupart des personnes rencontrent d'abord des réseaux informatiques - à travers l'architecture Internet. La partie 1 couvre les applications Internet les plus importantes et les méthodes utilisées pour les développer. La partie 2 traite du bord du réseau, composé d'hôtes, de réseaux d'accès, de réseaux locaux et de médias physiques utilisés avec les couches physiques et de liaison. La partie 3 explore le noyau du réseau, y compris les commutateurs de paquets / circuits, les routeurs et le backbone Internet, et la partie 4 examine le transport fiable et la gestion de la congestion du réseau.
- **[RChp11]** Tehranipoor, M., & Wang, C. (2011). *Introduction to hardware security and trust*. Springer Science & Business Media.
- **[RChp12]** Krutz, R. L., & Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing.
- **[RChp13]** Pieprzyk, J., Hardjono, T., & Seberry, J. (2013). *Fundamentals of computer security*. Springer Science & Business Media.
- **[RChp14]** Wu, C. H. J., & Irwin, J. D. (2016). *Introduction to computer networks and cybersecurity*. CRC Press.