Львівський державний університет безпеки життєдіяльності

Кафедра управління проектами, інформаційних технологій та телекомунікацій

Лекція

з курсу:

" Безпека інформаційно-комунікаційних систем"

на тему: **" Основи безпеки інформації в комп'ютерних мережах "**

(для курсантів та студентів 5-го курсу спеціальності «Комп'ютерні науки»)

ПЛАН ЛЕКЦІЇ

1. Основні відомості про комп'ютерні мережі.
2. Загрози безпеці інформації у мережах.
3. Безпека взаємодії відкритих систем.

ЛІТЕРАТУРА

1. **Богуш В.М., Кудін А.М.** Інформаційна безпека від А до Я. - К.: МОУ, 1999. – 456 с.
2. **Гайворонський М.В., Новіков О.М.** Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. іл.
3. **Прохоров И.В., Толстой А.И.** Телекоммуникационные сети: Учебное пособие. – М.: МИФИ, 1996. – 64 с.
4. **Тимошенко А.О.** Методи аналізу та проектування систем захисту інформації: Курс лекцій. - К.: Політехніка, 2007. – 174 с.
5. **Зегжда Д.П., Ивашко А.М.** Как построить защищенную информационную систему. Том 1. - СПб: НПО «Мир и семья - 95», 1997. - 312 с.
6. **Олифер В.Г., Олифер Н.А.** Сетевые операционные системы – СПб.: Питер, 2001. – 672 с.

1. Основні відомості про комп‘ютерні мережі.

Комп'ютерна, або обчислювальна, мережа - це сукупність комп'ютерів, пов'язаних між собою лініями зв'язку, які утворюються за допомогою кабелів і комунікаційних пристроїв (адаптерів, комутаторів тощо). Комп'ютерна мережа - це окремий випадок (складова) розподіленої, або децентралізованої, обчислювальної системи. Основною ознакою розподіленої обчислювальної системи є наявність кількох центрів оброблення даних, розподілених у просторі. На основі розподілених обчислювальних систем будують розподілені інформаційно-комунікаційні системи.

Важливою характеристикою мережі є її топологія. Топологія - це конфігурація графа, вершинам якого відповідають вузли мережі (комп'ютери і, можливо, комутаційні пристрої), а ребрам - зв'язки між ними. Розрізняють фізичну і логічну топології. Фізична топологія описує конфігурацію фізичних зв'язків між комп'ютерами (електричних проводів, оптичних кабелів тощо), а логічна топологія - конфігурацію можливих маршрутів обміну повідомленнями.

Фізична і логічна топології деякої мережі можуть суттєво відрізнятися. Наприклад, мережа Token Ring має фізичну топологію «зірка», у центрі якої знаходиться спеціальний комутаційний пристрій, а її логічна топологія - «кільце» кожна станція отримує повідомлення лише від однієї, розташованої попереду, станції та передає повідомлення одній - розташованій за нею). Мережа 10Base-T Ethernet так само має фізичну топологію «зірка», а логічну топологію - «спільна шина» (усі станції мають рівноправний доступ до спільного середовища передавання даних).

Також важливою характеристикою мережі є принцип, за яким здійснюється з'єднання (комутація) абонентів між собою, - комутація каналів (Circuit Switching) або комутація пакетів (Packet Switching). Із послідовно з'єднаних ділянок утворюється неперервний фізичний канал, який монопольно використовують два кінцеві вузли. Комутація пакетів передбачає, що всі дані, які передаються мережею, подрібнюються на окремі порції (блоки) даних, які у різних технологіях називають пакета.ми (Packet), кадрами (Frame) або комірка.ми (Cell). Кожний пакет передається по мережі окремо і незалежно від інших пакетів. У подальшому ми розглядатимемо переважно мережі, побудовані на принципі комутації пакетів.

І комутацію каналів, і комутацію пакетів здійснюють динамічно (тобто за запитом абонентів - як правило, таке з'єднання триває від кількох секунд до кількох годин) і постійно (комутацію здійснює персонал, що обслуговує мережу, типовий термін підтримки з'єднання - кілька місяців). Постійні з'єднання у мережах із комутацією каналів називають виділеними лініями (Dedicated Line).

Відкриті системи

Одним із головних напрямів розвитку інформаційних технологій є технологія систем з відкритою ар:хітектурою (відкритих систем). Ця технологія забезпечує мобільність прикладних програм - можливість їх перенесення на різні платформи і взаємодії різних систем між собою. Цього досягають використанням лише тих програмних і апаратних інтерфейсів, що відповідають міжнародним стандартам.

Згідно з визначенням Національного інституту стандартів США (National Institute of Standards and Technology, NIST): «Відкрита система - це система, що здатна взаємодіяти з іншою системою за допомогою реалізації міжнародних стандартних протоколів. Відкритими системами є як кінцеві, так і проміжні системи. Однак відкрита система не обов'язково може бути доступна іншим відкритим системам. Цю ізоляцію можна забезпечити фізичним відокремленням системи або використанням технічних можливостей, спрямованих на захист інформації в комп'ютерах і засобах комунікацій».

Модель взаємодії відкритих систем

Завдання забезпечення взаємодії сутностей (об'єктів), що входять до складу ІКС і об'єднані у мережу, полягає у вирішенні багатьох проблем. Це й вибір способу адресації об'єктів у мережі, узгодження електричних сигналів під час встановлення електричного зв' язку та забезпечення надійного передавання даних, оброблення повідомлень про помилки, формування повідомлень, що надсилаються, інтерпретація отриманих повідомлень тощо. Завдання такого рівня складності звичайно розбивають на кілька під-завдань і для виконання

кожного з них призначають окремий модуль. У сі модулі, що виконують підзавдання, поділяють на ієрархічно впорядковані групи - рівні. Для кожного рівня визначають набір функцій-запитів, з якими до його модулів можуть звертатися модулі, які належать до вищого рівня, задля виконання своїх завдань. Такий формально визначений набір функцій і формати повідомлень, якими обмінюються два сусідні рівні під час взаємодії, називають інтерфейсом.

Правила взаємодії двох об'єктів у мережі описують у вигляді набору процедур для кожного з рівнів. Такі формалізовані правила, що визначають послідовність і формат повідомлень, якими обмінюються мережні компоненти, розташовані на одному рівні але в різних вузлах мережі, називають протоколами. Погоджений набір протоколів різних рівнів, достатній для організації міжмережної взаємодії, називають стеком протоколи.

За сприяння Міжнародної організації зі стандартів (International Organization for Standardization, ISO) було розроблено модель, в якій чітко визначено різні рівні взаємодії систем і надано їм стандартні імена; тут також визначено, які функції має виконувати кожен рівень. Це модель взаємодії відкритих систем (Open Systems Interconnection, OSI), яку ще називають еталонною моделлю (Reference Moded).

Ця модель взаємодії складається із семи рівнів. Кожен рівень відповідає за забезпечення одного певного аспекту взаємодії та підтримує інтерфейси із сусідніми рівнями. Рівні моделі OSI нумерують, починаючи з нижнього. Посилання на певний рівень роблять як за його назвою, так і за номером (наприклад, «обладнання другого рівня~, «протокол третього рівня»). У табл.1 наведено перелік основних функцій, що реалізуються на різних рівнях.

Таблиця 1. Рівні моделі OSI та реалізовані на них функції

№	Рівень	Функції
7	Прикладним (Application)	Набір протоколів доступу користувачів до ресурсів мережі. Саме до цього рівня звертаються прикладні програми
6	Представницький (Presentation)	Узгодження форми подання інформації, що передається, зокрема, узгодження різних наборів символів
5	Сеансовий (Session)	Керування діалогом: визначення активної сторони, синхронізація
4	Транспортний (Transport)	Доставляння даних до кінцевого вузла із заданим рівнем надійності сервісу (з підтвердженням або ні. 3 відновленням або ні)
3	Мережний (Network)	Утворення єдиної транспортної системи, що об'єднує кілька підмереж, які у загальному випадку можуть бути побудовані на різних технологіях. І іа цьому рівні вирішують такі завдання: ♦ універсальної адресації, яка забезпечує унікальні адреси у всій мережі; ♦ просування (Forwarding) пакета даних об'єднаною мережею крізь послідовність підмереж до кінцевого вузла; ♦ маршрутизації, тобто визначення шляху, за яким пакет даних може досягти кінцевого вузла
2	Канальний (Data Link)	Утворення каналу, яким передаються блоки даних у межах одної підмережі. Па цьому рінні реалізується багато функцій, шо стало причиною подальшого його поділу на два підрівні: ♦ верхній — рівень керування логічним з'єднанням (Logical Link Control, LLC), який забезпечує коректне передавання кожного кадру, підтвердження доставления, контроль послідовності; ♦ нижній - рівень керування доступом до середовища (Media Access Control, MAC), на якому здійснюється перевірка доступності середовища передавання, доступ до передавання та приймання кадрів, виявлення та корекція помилок
1	Фізичний (Physical)	Передавання бітів даних фізичними каналами зв'язку. Специфікації протоколів цього рівня мають узгоджувати тип і параметри сигналів, способи аналогової модуляції або цифрового кодування, типи кабелів і роз'єднувачів

У табл. 2 наведено кілька класифікацій протоколів різних рівнів, що дають змогу чітко визначити особливості цих протоколів.

Таблиця 2. Класифікації протоколів моделі OSI

Рівень моделі OSI	Рівень протоколу	Реалізація	Залежність від технологи
Прикладний Представницький	Протокол верхнього рівня	Програмна	Протоколи, що не залежать від технології мережі
Сеансовий Транспортний Мережний	Протокол середнього рівня		
Канальний Фізичний	Протокол нижнього рівня	Апаратна	Протоколи, що залежать від технології мережі

Стеки протоколів

На підставі запиту прикладної програми до прикладного рівня програмне забезпечення цього рівня формує повідомлення (пакет, або кадр) стандартного формату, де розміщує службову інформацію (заголовок) і, можливо, передані дані. Потім це повідомлення спрямовується до представницького рівня, який додає до повідомлення свій заголовок і передає результат униз, сеансовому рівню, що також додає заголовок і т. д. Зрештою, повідомлення досягає найнижчого, фізичного, рівня, який передає його по мережному каналу зв'язку.

Коли повідомлення потрапляє на інший об'єкт (комп'ютер), воно послідовно просувається вгору з рівня на рівень. На кожному рівні повідомлення аналізується та обробляється, з нього видаляється заголовок цього рівня і виконуються відповідні функції. Після цього повідомлення передається рівню, що розміщений вище. Сукупність протоколів, які забезпечують взаємодію двох систем і передавання повідомлень між ними, утворює стек протоколів.

Розглянемо стеки мережних протоколів, які використовують найчастіше, та порівняємо їх із рівнями еталонної моделі OSI (табл. 3)

.

Таблиця 3. Стеки мережних протоколів та їх порівняння із стеками протоколів рівнів моделі OSI

Рівні моделі OSI	IBM/Microsoft	TCP/IP		Novell	Стек OSI
Прикладний	SMB	Telnet, FTP, SMTP, NNTP, HTTP. SNMP		NCP, SAP	X.400, X.500, VTP, FT A M
Представницький					Протокол подання OSI
Сеансовий	NetBIOS	TCP			Сеансовий протокол OSI
Транспортний			UDP	SPX	Транспортний протокол OSI
Мережний	—	IP, ICMP, RIP. OSPF		IPX, RIP, NLSP	IS-IS
Канальний	Ethernet (802.3), Token Ring (802.5), FDD1, SLIP, PPP, X.25, ATM, LAP-B, LAP-D				

Стек протоколів NetBIOS/SMB було створено для невеликих локальних мереж, де його і використовують. Стек протоколів IPX/SPX було розроблено на початку 80-х років минулого століття для мереж, побудованих із персональних комп'ютерів, що мали обмежені ресурси, завдяки чому він тривалий час домінував у локальних і корпоративних мережах.

Стек TCP /IP також було розроблено в кінці 70-х - на початку 80-х років минулого століття за ініціативи Міністерства оборони США для експериментальної мережі ARP Anet та її зв' язку з іншими мережами. Перевага цього стека протоколів полягає у його орієнтації на об'єднані гетерогенні мережі. Саме на цьому стеку протоколів базується Інтернет - нащадок проекту ARP Anet. Поступово, зі зростанням обчислювальної потужності комп'ютерів, стек TCP /IP суттєво потіснив інші стеки протоколів у локальних мережах і зараз є домінуючим у корпоративних мережах. Слід зазначити, що стек TCP /IP, на відміну від моделі OSI, має чотири рівні:

- верхній, що відповідає прикладному і представницькому рівням моделі OSI;
- транспортний, що містить транспортні протоколи, причому протокол TCP, від якого походить назва цього стека, реалізує ще й функції сеансового рівня;
- мережний, що відповідає мережному рівню моделі OSI;
- нижній, на якому реалізовано різні мережні технології, тобто функції фізичного і канального рівня.

Стек протоколів OSI - єдиний стек, який цілком відповідає 7-рівневій моделі. Він досі не набув широкого визнання, хоча існують реалізації відповідних протоколів для багатьох платформ. Окремі протоколи з цього стека використовують і в інших мережах. Серед таких можна назвати деякі протоколи прикладного рівня і протоколи маршрутизації.

2. Загрози безпеці інформації у мережах.

Комп'ютерні мережі через притаманні їм особливості створюють умови для виникнення численних загроз безпеці інформації. Розподіл ресурсів та інформації у просторі робить можливою наявність специфічного виду атак - так званих мережних (Network Attacks), або віддалених, атак (Remote Attacks). Під віддаленою атакою розуміють атаку на розподілену обчислювальну систему, що здійснюють програмні засоби каналами зв'язку. Така атака може бути здійснена на протоколи і мережні служби, а також на операційні системи та прикладні програми вузлів мережі.

Однією з основних причин потенційної вразливості мереж є принцип їхнього функціонування. Інформаційний обмін у мережі здійснюють за допомогою механізму повідомлень. Людина майже не бере участі в роботі мережі. У вузлах мережі розташовано апаратні та програмні засоби, які діють автоматично, без втручання оператора. Такі засоби призначені для передавання і приймання даних із мережі. Для цього вони мають відповідати на повідомлення-запити, що надходять із мережі та які регламентовано протоколами взаємодії. Спеціальним чином створені запити можуть викликати такі відповіді автоматичних засобів, які призводять до порушення політики безпеки. Крім того, атака може бути спрямованою не на комп'ютер у мережі, а на інформацію, що передається мережею.

Інтернет становить особливу небезпеку через свою доступність і глобальний масштаб. У цій мережі присутні та активно діють численні зловмисники – професіонали і просто допитливі підлітки, які знайшли інструменти зламу - доступне в мережі відповідне програмне забезпечення - і тепер намагаються їх випробувати. У глобальній мережі одночасно діють представники кримінальних структур, різних політичних партій і течій, правоохоронних органів і спецслужб різних країн. Атака на підключену до мережі систему може бути матеріально чи політично вмотивованою. А зловмисники, навіть якщо будуть вистеженими, можуть знаходитися в іншому правовому полі (в іншій державі) і бути недосяжними для покарання.

Стисло розглянемо типові вразливості розподілених систем. У документі «Інструкція із захисту базового рівня інформаційних технологій~ («IT Baseline Protection Manual») як типові атаки, що можуть бути застосовані для нападу на розподілені системи та які слід моделювати під час випробувань стійкості до них систем, названо такі:

- угадування паролів, або атаки за словником;
- реєстрація та маніпуляції з мережним трафіком;
- імпорт фальшивих пакетів даних;
- експлуатація відомих уразливостей програмного забезпечення (мови макросів, помилки в ОС, служби віддаленого доступу тощо).

Проаналізувавши успішні атаки на мережні системи, можна визначити причини, через які такі системи є вразливими:

- використання спільного середовища передавання (наприклад, Ethernet, радіоканал);
- застосування нестійких алгоритмів ідентифікації віддалених активних і пасивних об'єктів;
- використання протоколів динамічної (адаптивної) маршрутизації;

- застосування алгоритмів віддаленого пошуку;
- можливість анонімного захоплення активним об'єктом багатьох фізичних або логічних каналів зв'язку.

З-поміж типових віддалених атак виокремлюють такі:

- аналіз мережного трафіку;
- підміна довіреного об'єкта в розподіленій системі;
- упровадження в розподілену систему фальшивого об'єкта через нав'язування фальшивого маршруту;
- упровадження в розподілену систему фальшивого об'єкта шляхом використання недоліків алгоритмів віддаленого пошуку;
- відмова в обслуговуванні.

3. Безпека взаємодії відкритих систем.

Захищати інформацію так чи інакше мусять усі користувачі ІКС, зокрема й користувачі відкритих систем. При цьому різні користувачі та системи потребують різних рівнів захисту. Інколи високий ступінь захисту системи заважає здійснювати легкий доступ до неї. З одного боку, наявність засобів захисту може впливати на продуктивність системи в цілому, на зручність її використання, на взаємодію прикладних програм і загальне керування системою. З іншого боку, такі властивості відкритих систем, як здатність забезпечити спільну роботу з прикладними системами на локальних і віддалених платформах, а також мобільність застосувань, стають джерелом додаткових уразливостей, на кшталт небезпеки внесення вірусів і «троянських коней~ або полегшення неавторизованого доступу.

Захист інформації в ІКС, реалізованих відповідно до технології відкритих систем, є проблемою, яку не так просто вирішити. Зараз частково розроблено стандарти (робота над їх створенням триває), спрямовані на забезпечення захисту інформації у відкритих системах, і відповідні механізми захисту. Базовими документами у сфері захисту розподілених систем стали технічно узгоджені документи ISO/IEC 7498-2 і Рекомендації CCITT (The International Telegraph and Telephone Consultative Committee) X.800 «Архітектура безпеки взаємодії відкритих систем для застосувань CCITT». Розглянемо більш докладно останній документ.

Сервіси безпеки

У рекомендаціях X.800 увагу закцентовано на таких функціях (сервісах) безпеки:

- автентифікація;
- керування доступом;
- конфіденційність даних;
- цілісність даних;
- унеможливлення відмови від авторства.

Розглянемо ці функції детальніше. Скрізь, де інше не вказано явно, йдеться про реалізацію сервісу безпеки, що надає послуги на певному рівні моделі OSI засобами цього ж рівня. ~дані користувача» у цьому розумінні - це дані, які є корисним навантаженням для окремого блоку даних або всієї послідовності блоків даних, тобто йдеться про дані протоколу вищого (вищих) рівня.

Автентифікація

Цей сервіс забезпечує автентифікацію сторін, що спілкуються (Communicating peer Entity), і автентифікацію джерела даних.

Автентифікацію сторін здійснюють у момент встановлення з'єднання та іноді під час передавання даних з метою підтвердження автентичності сутностей з'єднання. Завдяки використанню цього сервісу можна бути впевненим, що суб'єкт не влаштує ~маскарад» і не використає повторно попередній несанкціонований сеанс зв'язку. Застосовують різні схеми автентифікації, які забезпечують різний ступінь захисту.

Автентифікація джерела даних - це підтвердження автентичності джерела блоку даних. Сервіс, який реалізують засобами певного рівня моделі OSI та надають для сутностей

вищого рівня, підтверджує автентичність сутності цього ж таки рівня. Слід зауважити, що сервіс не забезпечує захист від повторення або пошкодження даних.

Керування доступом

Цей сервіс забезпечує захист від несанкціонованого використання ресурсів, доступних через взаємодію відкритих систем. Керування доступом може застосовуватися до різних типів доступу до ресурсу (наприклад, використання комунікаційного ресурсу, читання, записування або видалення інформаційного ресурсу, виконання ресурсу оброблення).

Конфіденційність даних

Цей сервіс забезпечує захист даних від їх несанкціонованого розкриття. Розрізняють кілька сервісів конфіденційності даних:

- конфіденційність даних під час обміну зі встановленням з'єднання - цей сервіс захищає всю інформацію користувачів, окрім даних щодо запиту на встановлення з'єднання (це залежатиме від рівня моделі OSI);
- конфіденційність даних під час обміну без встановлення з'єднання - цей сервіс захищає всю інформацію користувачів;
- конфіденційність окремих полів даних - цей сервіс забезпечує захист інформації в окремих обраних полях даних у сеансі зі встановленням з'єднання або без нього;
- конфіденційність трафіку - цей сервіс забезпечує захист інформації", яку отримують під час здійснення аналізу трафіку.

Цілісність даних

Цей сервіс спрямований на протидію активним загрозам. Розрізняють такі сервіси цілісності даних:

- цілісність даних під час обміну зі встановленням з'єднання з відновленням -цей сервіс забезпечує цілісність усіх даних користувача шляхом виявлення будь-якої модифікації даних (додавання, видалення та повторення) і здійснює спробу відновити дані;
- цілісність даних під час обміну зі встановленням з'єднання без відновлення - так само, як і попередній сервіс, забезпечує цілісність усіх даних, але без спроби їхнього відновлення;
- цілісність окремих полів даних під час обміну зі встановленням з'єднання - цей сервіс забезпечує цілісність окремих обраних полів даних у сеансі зі встановленням з'єднання і визначає, чи не було ці поля модифіковано (додано, видалено та повторено);
- цілісність даних під час обміну без встановлення з'єднання - цей сервіс на відміну від попередніх у разі його реалізації на певному рівні моделі OSI забезпечує цілісність даних за запитом сутності вищого рівня; сервіс забезпечує цілісність окремого блоку даних, що передається без встановлення з'єднання, і може визначати, чи було блок даних модифіковано, крім того він може виявляти дані, що повторюються;
- цілісність окремих полів даних під час обміну без встановлення з'єднання - цей сервіс забезпечує цілісність окремих обраних полів в окремому блоці даних, що передається без встановлення з'єднання, і визначає, чи було модифіковано обрані поля.

Унеможливлення відмови від авторства

Сервіс забезпечує такі можливості (кожну окремо або обидві разом):

+ унеможливлення відмови від авторства з підтвердженням справжності джерела даних - цей сервіс захищає одержувача даних від будь-якої спроби відправника відмовитися від факту відправлення ним даних чи справжності їхнього вмісту;

+ унеможливлення відмови від авторства з підтвердженням про отримання - цей сервіс сповіщає відправнику даних про їх отримання, що не дає одержувачу відмовитися від факту отримання даних або викривити їх.

У табл. 4 показано, на яких рівнях моделі OSI реалізують сервіси безпеки.

Слід зазначити, що прикладні процеси можуть самі забезпечувати сервіси безпеки, що доповнюють або заміняють сервіси 7-го рівня.

Таблиця 4. Співвідношення сервісів безпеки і рівнів моделі ISO

Сервіс	Рівень						
	1	2	3	4	5	6	7
Автентифікація сторін			+	+			+
Автентифікація джерела даних			+	+			+
Керування доступом			+	+			+
Конфіденційність даних під час обміну зі встановленням з'єднання	+	+	+	+		+	+
Конфіденційність даних під час обміну без встановлення з'єднання		+	+	+		+	+
Конфіденційність окремих полів даних						+	+
Конфіденційність трафіку	+		+				+
Цілісність даних під час обміну зі встановленням з'єднання з відновленням				+			+
Цілісність даних під час обміну зі встановленням з'єднання без відновлення			+	+			+
Цілісність окремих полів даних під час обміну зі встановленням з'єднання							+
Цілісність даних під час обміну без встановлення з'єднання			+	+			+
Цілісність окремих полів даних під час обміну без встановлення з'єднання							+
Унеможливлення відмови від авторства з підтвердженням справжності джерела даних							+
Унеможливлення відмови під авторства з підтвердженням про отримання							+

Специфічні механізми безпеки

Реалізувати сервіси безпеки можна, впровадивши на певному рівні моделі OSI такі механізми:

- шифрування;
- цифровий підпис;
- керування доступом;
- контроль цілісності даних;
- автентифікаційний обмін;
- заповнення трафіку;
- керування маршрутом;
- нотаризація.

Шифрування

Цей механізм, який захищає окремі дані або потік даних (шифрування трафіку), може бути використаний іншими механізмами або може замінити деякі з них.

Застосовують симетричні й асиметричні алгоритми шифрування. Використання алгоритму шифрування майже завжди передбачає впровадження механізму керування ключами.

Цифровий підпис

Механізм цифрового підпису складається із двох процедур:

- підписання блоку даних;
- перевірки підписаного блоку даних.

Процедура *підписування блоку даних* полягає у шифруванні блоку даних або обчисленні криптографічної контрольної суми з використанням приватної (унікальної та конфіденційної) інформації користувача, що здійснює підпис.

Для *перевірки підписаного блоку даних* використовують процедури та інформацію, що є загальнодоступними, але з яких неможливо здобути приватну інформацію про того, хто підписує. Ця процедура, фактично, дає змогу перевірити, чи справді цифровий підпис було зроблено з використанням приватної інформації того, хто підписав блок даних.

Керування доступом

Ці механізми використовують ідентифікацію сутності або деяку інформацію про сутність (як належність до певної відомої множини сутностей), а також посвідчення, надане сутністю для визначення і встановлення її прав доступу. Якщо сутність намагається здійснити неавторизований (несанкціонований) доступ (використати неавторизований ресурс або недозволений метод доступу до авторизованого ресурсу), функція керування доступом

перешкодить цьому і, можливо, згенерує повідомлення про інцидент (для ініціювання протидії або з метою аудита).

Механізми керування доступом можуть використовувати один чи кілька із зазначених нижче видів та джерел інформації:

- бази даних керування доступом, в яких зберігаються права доступу сутностей; Ці бази підтримуються централізовано або на кінцевих системах; права доступу зберігаються у вигляді списків керування доступом або матриці ієрархічної чи розподіленої структури (використання бази даних керування доступом передбачає, що сутності перед цим було автентифіковано);
- інформація автентифікації, володіння якою і надання якої є доказом авторизації (наприклад, паролі);
- посвідчення, володіння якими і подання яких є доказом дозволу доступу до сутності або ресурсу, вказаних у посвідченні;
- мітки безпеки, асоційовані із сутностями (суб'єктами та об'єктами доступу), які використовують для надання або заборони доступу, як правило, на основі політики безпеки;
- момент часу, коли було здійснено спробу доступу;
- маршрут спроби доступу;
- тривалість спроби доступу.

Механізми керування доступом можуть бути задіяні на будь-якій із сторін, що здійснюють зв'язок, а також у проміжній точці. Механізми, задіяні у точці, яка ініціює доступ, і у проміжних точках, мають перевіряти, чи відправник авторизований для зв'язку з одержувачем та (або) для використання комунікаційних ресурсів.

Якщо зв'язок було здійснено без встановлення з'єднання, вимоги механізму, реалізованого у кінцевій точці, мають бути відомими у точці, що ініціює доступ, апріорі.

Контроль цілісності даних

Є два аспекти цілісності:

- цілісність окремого блоку даних або поля інформації;
- цілісність потоку блоків даних або полів інформації.

Для забезпечення цих двох видів сервісу цілісності у загальному випадку можуть бути задіяні різні механізми, але контроль цілісності потоку без контролю окремих блоків даних (полів) не є практичним.

Контроль цілісності окремого блоку даних (поля) здійснюють як на стороні, що передає дані, так і на стороні, що їх приймає. На стороні, що передає, до блоку даних додається інформація, яка є функцією від цих даних (циклічна або криптографічна контрольна сума, яка також може бути зашифрованою). На стороні, що приймає, генерується аналогічна контрольна сума, яка в подальшому порівнюється з отриманою. Зауважте, цей механізм не здатний захистити від повторення блоків даних.

Перевірка цілісності потоку блоків даних (тобто захист від втрати даних, їх перевпорядкування, дублювання, вставляння та модифікації) вимагає додаткового впровадження порядкових номерів, часових штампів або криптографічного зв'язування (коли результат шифрування чергового блоку залежить від попереднього).

Під час здійснення зв'язку без встановлення з'єднання використання часових штампів надає обмежений захист від дублювання блоків даних.

Автентифікаційний обмін

Механізми автентифікаційного обміну впроваджуються на певному рівні моделі OSI для підтвердження автентичності сутності. Якщо механізм не підтверджує автентичність сутності, з'єднання забороняється або закривається вже встановлене з'єднання, при цьому може бути згенероване повідомлення про інцидент (для ініціювання протидії або з метою аудита). Автентифікаційний обмін здійснюють у кілька способів:

- використовуючи автентифікаційну інформацію (на кшталт паролів), яку надає відправник і перевіряє одержувач;
- із застосуванням криптографічних методів;
- демонструючи характеристики або можливості сутності.

Щоб уникнути повторення даних, криптографічні методи іноді використовують разом із процедурами ~рукостискання~ (Handshaking) - обміну з квитируванням, підтвердження зв'язку.

Методи автентифікаційного обміну інколи (залежно від обставин) використовують разом із:

- часовими штампами і синхронізацією годинників;
- двох- і трьох-етапними процедурами «рукостискання» (відповідно для одно та двох-сторонньої автентифікації);
- сервісами унеможливлення відмови від авторства, що досягається використанням механізмів цифрового підпису та (або) нотаризації.

Заповнення трафіку

Механізми заповнення трафіку застосовують для забезпечення захисту від аналізування трафіку. Ці механізми ефективні лише в поєднанні із засобами забезпечення конфіденційності.

Керування маршрутом

Маршрути можна обирати динамічно або статично таким чином, щоб використовувати лише фізично безпечні підмережі, вузли комутації та канали. Кінцеві системи у разі виявлення неодноразових атак на маршруті мають можливість звернутися до провайдера мережних послуг для встановлення з'єднання за іншим маршрутом.

Передавання даних, що мають мітки безпеки, через певні підмережі, вузли комутації та канали може бути заборонено політикою безпеки. Ініціатор з'єднання, або відправник даних, які передаються без встановлення з'єднання, має можливість обмежити маршрут таким чином, щоб оминути певні підмережі, вузли комутації та канали.

Нотаризація

За допомогою механізму нотаризації завіряються характеристики даних, що передаються між двома (або більше) сутностями (їх цілісність, джерело, час передавання і пункт призначення). Достовірність таких даних стверджує третя сторона, якій довіряють сутності, що взаємодіють, і яка володіє достатньою для цього інформацію. Кожна сутність, що взаємодіє із застосуванням механізму нотаризації, використовує цифровий підпис, шифрування і контроль цілісності.