Тема 5

Контрол на достъпа (идентификация, автентикация и оторизация)

Увод

- **Техническият контрол** е от съществено значение за една добре планирана програма за информационна сигурност, по-специално за прилагане на политиката за много ИТ функции, които **не са под прекия човешки контрол**.
- Компютърните мрежи и компютърни системи взимат милиони решения и действат по начини и при скорости, които хората **не могат** да контролират в реално време.
- Техническите решения за контрол, правилно имплементирани, могат да **подобрят** способността на организацията да балансира често **противоречащи** си цели 1) на превръщане на информацията в лесно и широко достъпна и 2) за запазване на конфиденциалността и интегритета на информацията.

. . .

- Един от най-често прилаганите технически методи за защита при компютърните системи е първоначално установяване на това „**кой**“ стои зад или управлява системата в момента и чак след това да му се **позволят** определени действия.
- Методите от тази категория са познати като **контрол на достъпа** и за висока сигурност се прилага т.нар. **zero-trust model**.
- На първо място стои **идентификацията**. Представлява заявка кои сме или коя е системата(в рамките на компютърна мрежа). Средства за идентификация са например лична карта, шофьорска книжка, име или адрес в компютърна мрежа и др.
- За да се осъществява контрол от техническа гледна точка първоначално на всеки потребител се присвоява т.нар. **идентификатор**. Така може да се осъществи проверка дали искащия достъп до даден ресурс или система е от **множеството** от легитимни потребители.
- На следваща стъпка се използват две други техники - на **автентикация** и **оторизация** за защита от неоторизиран достъп до информационни ресурси.
- Автентикацията се отнася до **установяване** на човека, системата или процеса и дали в действителност са тези за които се заявяват при идентификацията. Например в БД да се провери дали данните от личната карта съответстват.
- Оторизацията спомага да се установи какво им е **позволено**.

Идентификация

- Идентификацията се случва, когато потребител претендира за самоличност / се представя за някого.
- Например в релността човек се представя с името си. Когато срещаме някого за първи път се представяме, като казваме „Аз съм Иван Петков“. Дали в действителност съм се установява на следващ етап, например с лична карта.
- В дигиталния свят, вместо това име, може да се представим с потребителското си име или имейл адрес, заявявайки например самоличността на наш акаунт.
- Идентификацията е първата стъпка от контрола на достъпа.

Автентикация (Authentication)

- Автентикацията/удостоверяване е процес на доказване от страна на човека, процеса или системата, че в действителност е/са тези, за които се представят.
- Има три широко използвани механизма (**authentication factors**) за автентикация/удостоверяване:

➢ Нещо, което искащият достъп **знае** (парола, ПИН, код, ...);

➢ Нещо, което искащият достъп **има** (ID карта, смарт карта, смарт устройство);

➢ Нещо, което искащият достъп **е** (пръстов отпечатък или други биометрични данни).

Автентикация (Authentication)

- Процесът на автентикация се изразява в **Потвърждение** (може да бъде парола, код за достъп, т.нар. смарт карта, биометрични данни и др.) на идентичността на потребител.
- Най-често използвания метод днес е с парола (нещо, което само конкретния човек знае). Този метод е пример за т.нар. едно-факторна автентикация.
- Този метод обаче не е сигурен, тъй като паролата може да бъде разгадана, забравена или откраднатa.
- От друга страна методът е най-лесен за реализация.

Системи за автентикация

- При разисквания метод за автентикация с парола е характерно, че системата валидира автентичността като сравнява паролата със съхранена вече парола използвана преди.
- Съществуват различни системи за автентикация с пароли:

- Локално съхранение и верификация;
- Централизирано съхранение и верификация;
- Kerberos;
- One-time password (OTP);
- …

Автентикация (2)

- По-добри и препоръчителни са други методи на автентикация, чрез смарт карти или биометрични данни.

Мулти-факторна автентикация

- Най-сигурният метод за автентикация е мулти-факторният.
- Използват се два или повече метода за потвърждение/доказване на идентичността.
- Методът включва комбинации от вече дискутираните:

✓ Нещо, което знам (парола или PIN код);

✓ Нещо, което имам (като карта или телефон за да потвърдя с SMS);

✓ Нещо което съм (уникална физическа характеристика).

Локално съхранение и верификация

- С развитието на компютърните системи са налага защита на ресурсите по отношение на **множество** потребители.
- До неотдавна данните за автентикация (потребителско име и парола се съхраняваха **некодирани** в бази от данни или файлове.
- Достъп до тези бази и файлове имаха множество администратори или потребители с познания в областта, което компрометира сигурността.
- Този подход се използва и днес, но само за приложения, които изрично изискват вътрешна/локална автентикация, а на разработчиците на приложения се оставя отговорността да защитят файловете с паролите.
- Например за Windows криптирани данни се съхраняват в регистрите или във файлове в папка **Credentials.**
- Днес най-често се използват централизирани системи, като OpenLDAP и Active Directory или клауд решения (**Azure Active Directory**, **Amazon Cognito**).

Централизирани системи

- Разработваните днес системи използват криптирани данни.
- Вместо да се прави просто сравнение на въведената парола и съхранената се налага да се криптира въведената и да се сравни с тази в базата данни.
- Голямото предизвикателство тук е, че не всички информационни системи **могат или са създадени така**, че да предават по мрежата кодираните пароли и някои ги изпращат като обикновен текст.
- Добрите новини са, че дори и в малките организации се използват клиентски системи изискващи централизирана автентикация позволяващи кодиране на данните при изпращане по мрежата.

Как става кодирането? Какво е хеш?

- Хеш функция е математическа формула, която преобразува низ от символи(текст или цифри) към цифров код (обикновено се наричат хеш).
- Тези функции са много важни методи за криптиране, и по този начин за системите за автентикация, които изискват данни, например парола, да бъдат скрити при предаване по мрежата.
- На теория, хеш е еднопосочен код, което означава, че можете да го създадете, но не и обратно.
- Когато един компютър създава хеш, друг компютър може да използва точно същия входен низ за създаване на друг хеш. Сравняването на двата хеша дава успех или неуспех при автентикация.
- Secure Hash Algorithm версия 1 (SHA-1) и Message Digest версия 5 (MD5) са широко използвани хеш функции.

Керберос (Kerberos)

- Kerberos е протокол за автентикация на мрежата. Той е предназначен да осигури сигурна автентификация за клиент / сървър приложения с помощта на криптография чрез таен ключ.
- Kerberos се базира на използването на билети. Обикновено тези системи се използват в незащитени мрежи и Интернет.
- Системата използва трета страна наречена Център за дистрибуция на ключове или на английски - key distribution center (KDC), който предоставя две теоритично независими услуги: Удостоверителн Сървър Authentication Server (AS) и Билето предоставящ сървър -Ticket Granting Server (TGS)..
- KDC подържа база данни от тайни ключове, всеки елемент от мрежата, без значение клиент или сървър, споделя таен ключ известен само на него и на KDC. Притежаването на този ключ служи за доказване на идентичността на елемнта. За целта на комуникацията, KDC генерира сесиен ключ, който се използва от комуникиращите страни за защита на техните трансмисии.

Как работи?

- Ако се използва Kerberos, клиента (обикновено е или потребител или услуга) изпраща искане за билет до т.нар. Key Distribution Center (KDC).
- KDC създава билет (ticket-granting ticket TGT) за клиента, криптира билета с помощта на паролата на клиента като ключ, и изпраща криптирания билет TGT обратно на клиента.
- След това клиентът се опитва да декриптира TGT, използвайки своята парола. Ако клиентът успешно декриптира TGT (т.е., ако клиентът даде правилната парола), се запазва декриптирания TGT билет, като става доказателство за самоличността на клиента.
- Този вид автентикация се поддържа от Windows, Apple OS, FreeBSD, UNIX, and Linux системи.

One-time password (OTP)

- При този метод на автентикация потребителя може да използва една парола **само веднъж**.
- Или с други думи една парола е валидна само в рамките на **една потребителска сесия** или **една трансакция**.
- Обикновено е част от метода на много-факторната автентикация.
- Основното предимство на този метод е, че система, която е защитена с този метод не е податлива на атаки, които се основават на периодичното опитване да се налучка паролата или дори и да се научи по някакъв начин, то тя ще е валидна само за кратък период от време.
- В момента банковите системи в България достъпни за клиенти през Интернет използват предимно този метод.

Сертификати

- Сертификатът е сбор на информация, която свързва потребител, компютър, информационна услуга, или устройство с публичен ключ от двойка публичен / частен ключове. Двата ключа се използват за криптиране и декриптиране, както и за предотвратяване на подмяна и фалшифициране на предоставената информация.
- Типичният сертификат включва информация за самоличността и определя целите, за които сертификатът може да се използва, сериен номер и място, където има повече информация за органа издал сертификата.
- Сертификатът е цифрово подписан от орган за сертификати наречен certificate authority (CA).

Сертификати (прод.)

- **Публичен и частен ключове**

  Публичният и частния ключове са две числа, генерирани от специален математически алгоритъм. Използват се за криптиране и декриптиране на информация. Информацията, криптирана с публичен ключ, може да бъде декриптирана със съответстващия частен ключ. А информацията, криптирана с частния ключ, може да бъде декриптирана само със съответстващия публичен ключ.

- Сертификата освен, че се съхранява от потребителя-притежател, може да се експортира като файл, да се изпраща по електронна поща, да се разпространява като допълнение към софтуер или да се съхранява в централизиран сървър.

- Сертификати се използват при две системи за автентикация SSL/TLS и смарт карти.

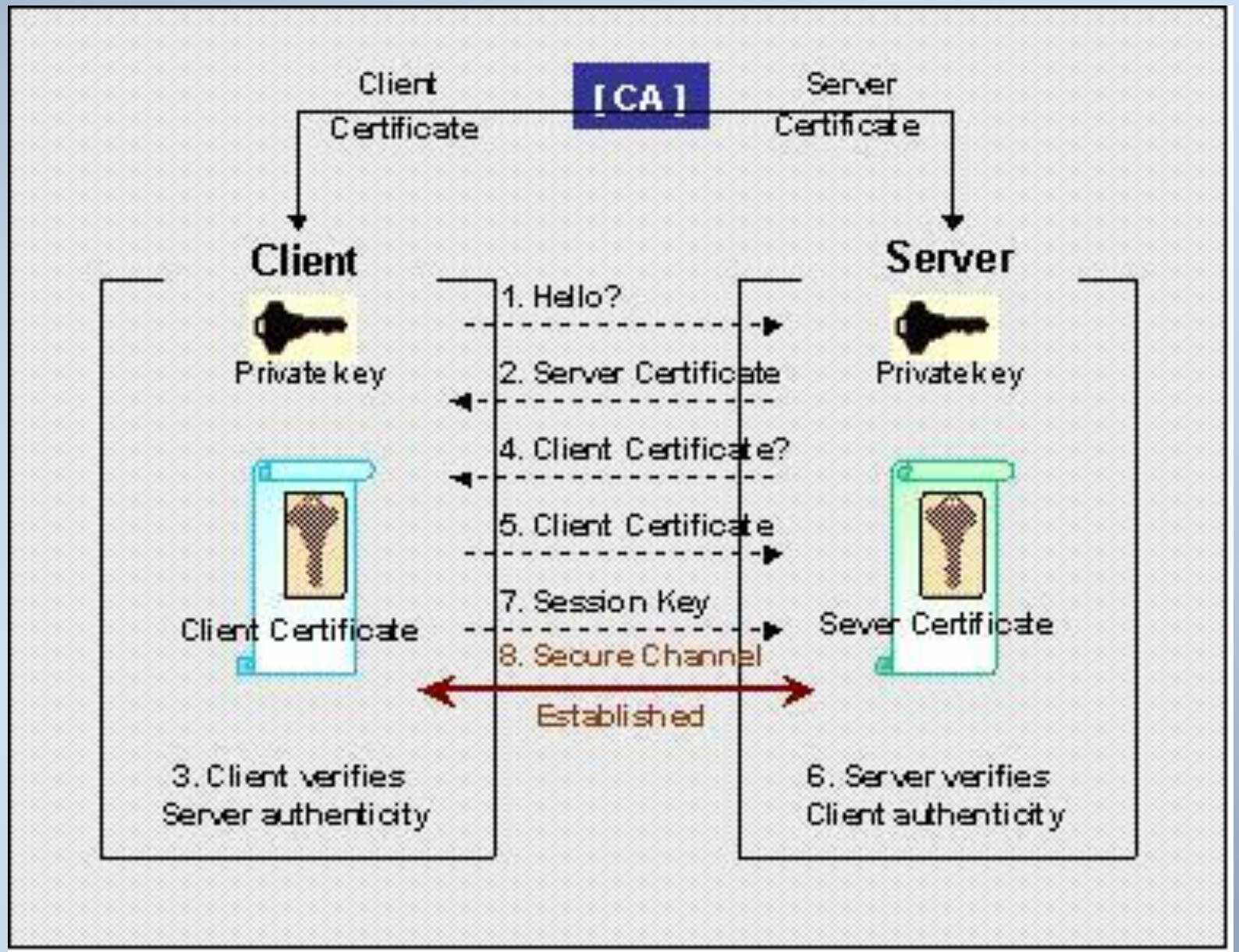
SSL/TLS

- Secure Sockets Layer (SSL) е система(протоколи) за автентикация на базата сертификати.
- Използва се за сигурна комуникация между уеб сървъри и клиенти и за споделяне на криптиращи ключове между сървъри и клиенти.
- Версии на протоколите се използват широко при сърфиране в интернет, електронна поща, instant messaging и voice-over-IP (VoIP).
- Transport Layer Security (TLS) е наследник на SSL. Макар че и двете TLS и SSL изпълняват същата функция, те не са съвместими-сървъра, който използва SSL не може да установи защитена сесия с клиент, който използва само TLS.
- SSL/TLS позволява на клиентски / сървърни приложения да комуникират в мрежата по начин предназначен за предотвратяване на подслушване и подправяне.
- За използването на SSL, организацията получава сървърен SSL сертификат от публичнен CA, като например Symantec, и инсталира сертификата на своя уеб сървър.

Как работят – пример при сърфиране?

1. Потребителят въвежда URL адреса уеб сървъра в браузъра.
2. Искането на клиента за уеб страницата се изпраща на сървъра.
3, Сървърът получава искането и изпраща своя сървърен сертификат на клиента.
4. Браузъра на клиента проверява сертификата в собственото хранилище за сертификати от CA.
5. Ако се намери сертификата, браузърът валидира сертификата, като проверява подписа на сертификата на сървъра с помощта на публичния ключ, предоставен от CA.
6, Ако този тест е успешен, браузърът приема сертификата на сървър, като валиден.
7. Генерира се и се криптира симетричен ключ, като се използва публичния ключ на сървъра.
8. Криптирания ключ се връща на сървъра.
9. Сървърът декриптира ключа със собствен частен ключ. И двата компютъра вече разполагат с ключ за криптиране, който може да се използва за осигуряване на комуникации между тях.

digital certificates - web site https://tender.eprocurement.gov.in/DigitalCertificate/faqs/gfaqs.htm



Смарт карти и други устройства

- Защитата на частния ключ е от първостепенно значение в системите за автентикация чрез сертификат.
- Ако един хакер може да получи частния ключ, то може да подправи самоличността на клиента.
- Реализациите на тези системи осигуряват защита на частния ключ, но в крайна сметка, ако ключът се съхранява на компютъра, има потенциал за компрометирането му.
- От една добра система би трябвало да се изиска частният ключ бъде съхранен отделно от компютъра.
- Смарт картите могат успешно да бъдат използвани за тази цел.

Смарт карти и други устройства

- Макар, че има много видове смарт карти, тези използвани за автентикация приличат на кредитна карта,

но съдържат компютърен чип,
който се използва за съхраняване
на частния ключ и копие на сертификата.

- **Други устройства се базират**

на USB интерфейс.

Как работи?

1. Потребителят слага смарт картата в четеца или включва USB устройството.
2. Компютърът реагира, чрез подканване на потребителя за неговия уникален PIN.
3. Потребителят въвежда своя ПИН.
4. Ако ПИН съвпада, приложението (компютъра), може да комуникира със смарт картата/ USB устройството. Частният ключ се използва за криптиране на необходимите данни.

5. Криптираните данни се прехвърлят към компютъра и евентуално до сървър в мрежата.
6. Публичният ключ се използва за декриптиране на данните.
Тъй като само притежателя на смарт картата/ USB устройството има частен ключ и валиден PIN, който трябва да се въведе, за да започне процеса изобщо, идентичността на конкретния потребител е гарантирана.

Биометрика

- **Биометриката** използва биометрична информация от човек и я свързва еднозначно с личността му, като по този начин дигитализира биометричната му идентичност.
- Използва се следната биометрична информация:

- **Пръстови отпечатъци -** пръстовите отпечатъци се формират още в утробата. На четвъртия месец от развитието на плода, той вече има пръстови отпечатъци. С възрастта на човека отпечатъците стават все по-големи. Независимо от това обаче, съотношенията между отделните елементи на всеки отпечатък се запазва.
- **Ирис –** сканирането на ириса е една от най-надеждните форми на биометрична идентификация. Тя осигурява анализ на пръстените, браздите и луничките в цветния пръстен, който обгражда зеницата на окото. Повече от 200 точки се използват за сравнение.
- **Лице -** лицевите характеристики включват размера и формата на лицето, както и връзката между тях. Макар този метод за биометрична идентификация да е най-разпространения между самите хора, той не е лесен за автоматизация и дигитализация. Обикновено този метод използва относителните разстояния между специфични лицеви характеристики за да генерира уникален лицев отпечатък.

Оторизация

- Важно за защитата на информационните ресурси е не само да се установи кой е потребителят, но и **какво му е позволено**.
- Оторизацията представлява именно това.
- Обикновено това е начин за управляване на достъпа до ресурси, като например файлове, но е и набор от **позволения**, които потребителят може да има върху системата или в мрежата.
- Има различни видове оторизиращи системи, използващи правата на потребителите, базирани на **роли**, **списъци** за контрол на достъпа и такива базирани на **правила**.

Оторизация (прод.)

- Оторизацията е **съотнасяне** на вече автентикиран потребител към списък с информационните активи и съответстващи на нива на достъп. Този списък е обикновено т.нар. ACL или матрица за контрол на достъпа.
- В общи линии, оторизацията може да работи по един от следните **три** начина:

1. Оторизация за **всеки** автентикиран потребител, за който системата извършва оторизация, за да се провери всеки субект и след това предоставя достъп до исканите ресурси.
2. Оторизация за членове на **група**, в която се проверява съответствие на потребителя и след това предоставяне достъп до ресурси на базата на права на достъп на групата. Това е най-често срещаният метод за оторизация.
3. Оторизация **в няколко системи**, в които централизирани системи за автентикация и оторизация проверява потребителската идентичност и след това се предоставя набор от позволения (например Google акаунт позволява достъп до поща, място за съхранение на файлове или работа с документи).

Потребителски права (User Rights)

- Потребителските права предоставят **разрешението** на даден потребител да извършва неща, които могат да влияят на цялата система.
- Способността да се създадат групи, присвояване на потребителите към групи, логин в системата, както и много други права могат да бъдат присвоявани.
- Типичен пример е система Unix, при която пълни права се предоставят на т.нар. root акаунт. Този акаунт е оторизиран да направи всичко със системата. Потребителите, от друга страна, имат ограничени права, като възможността за вход в системата, достъп до определени файлове и за стартиране на определени приложения.

Оторизация, чрез роли

- Да вземем за пример една организация, в нея всяка задача се извършва от човек или група от хора, които имат строго определени позволения, достъп до определени ресурси и т.н.
- Съвременните информационни системи използват подхода с роли, за да дефинират специфични права и позволения, а на отделните потребители се присвояват **специфични роли**.
- Ако вземем за пример една информационна система използвана в университет, то може да се дефинират роли на студент, преподавател, администратор, ректор, счетоводител и други. Всеки студент регистриран в системата, например студента Петко Дончев ще „играе“ роля на студент и ще има достъп до информация касаеща само него, например оценките му, но не и да кажем счетоводна такава.

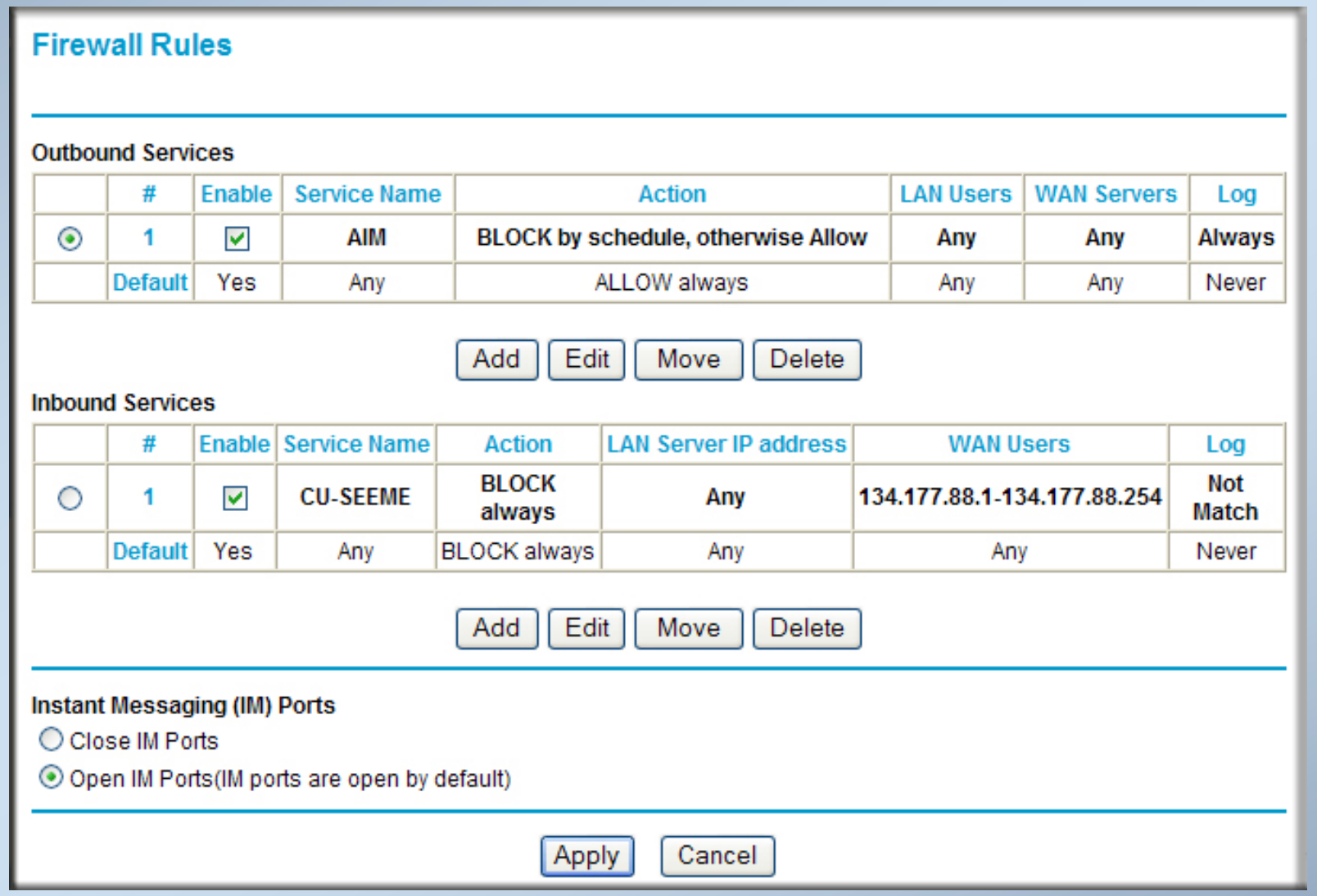
Списък за контрол на достъпа (Access Control Lists)

- Присъствието на някои социални събития, се ограничава само до поканените. За да се гарантира, че само поканени присъстват се създава списък на поканите и охраната допуска само тях.
- Когато гост пристигне, името му се проверява в този списък, и влизането е позволено или отказано.
- Информационни системи могат също да използват ACL-ци, за да се определи дали исканата услуга или ресурс е разрешен.
- Достъп до файлове на отдалечен сървър, често се контролира от информация - списък, която се поддържани за всеки файл.
- Аналогично, възможността на различни видове комуникация да премине през мрежово устройство също може да се контролира така. Обикновено ACL се присвояват на порт на устройство, като се избира кой трафик преминаващ през порта да ограничава списък за достъп – входящия или изходящия.

Оторизация базирана на правила

- Оторизация, базирана на **правила** изисква разработването на правила, които предвиждат **какво**, специфичен потребител, може да направи с една система.
- Тези правила могат да предоставят информация като "User Алекс има достъп до ресурс X, но не може да получи достъп до ресурс Y. „.
- Типичен пример е настройката на една защитна стена, там се използват правила затова коя програма какъв достъп има входящ или изходящ трафик на кой порт и т.н.

Netgear Firewall Rules



Firewall Rules

Outbound Services

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
◉	1	☑	**AIM**	**BLOCK by schedule, otherwise Allow**	**Any**	**Any**	**Always**
	Default	Yes	Any	ALLOW always	Any	Any	Never

Add Edit Move Delete

Inbound Services

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
○	1	☑	**CU-SEEME**	**BLOCK always**	**Any**	**134.177.88.1-134.177.88.254**	**Not Match**
	Default	Yes	Any	BLOCK always	Any	Any	Never

Add Edit Move Delete

Instant Messaging (IM) Ports

○ Close IM Ports

◉ Open IM Ports(IM ports are open by default)

Apply Cancel

Отчетност

- Освен описаните процеси на контрол на достъпа е необходимо да се **следи** и цялостно какво се случва при тях, например успешни – неуспешни автентикации и т.н.
- Отчетността най-често се осъществява с помощта на генериране на **системни дневници(Logs)** и дневници за базите данни, както и одитът на тези записи.
- Системите дневници съхраняват конкретна информация, като неуспешни опити за достъп и модификациите на системите.
- Дневниците имат много приложения, като например за откриване на проникване, определяне на основната причина за системен отказ или просто за проследяване на използването на конкретен ресурс.

Заключение

- Автентикацията и оторизацията са едни от най-често прилаганите методи за защита при компютърните системи.
- Те позволяват да се контролира кой потребител има достъп до системата и какво му е позволено да прави с нейните ресурси.
- Тези два подхода следва да се използват заедно с други методи, за да се осигури възможно най-високо ниво на защита на информационните ресурси.

Identity management systems (IMS) или identity and access management (IAM)

- За имплементиране на механизми за контрол на достъпа за големи организации често са налага да се използват отделни специализирани информационни системи.
- Системите за управление на идентичността/самоличността се занимават със създаването, администрирането и внедряването на:
- Идентификатори: Данни, използвани за идентифициране на субект.
- Credentials - Удостоверения: Данни, предоставящи доказателства за твърдения за самоличности или части от тях.
- Атрибути: Данни, описващи характеристики на субект.

Практически упражнения

- В рамките на един учебен час потърсете в Интернет пространството информация за разглежданите в темата понятия, дефиниции и аспекти. Търсенето може да направите и на чужди езици, които владеете.
- Анализирайте намерената информация и я сравнете с поднесената тук.
- Опишете как във Вашата практика(вкл. и като разработчици) имплементирате мерки за контрол на достъпа.