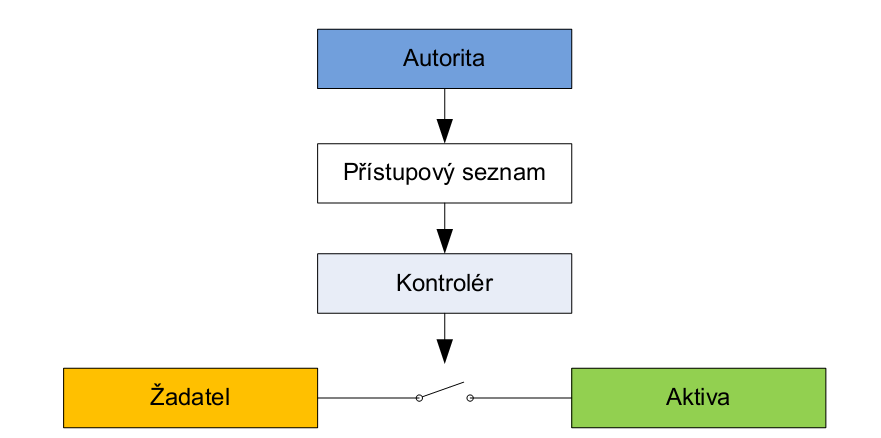
**Autentizace**

Autentizace pochází z německého slova die Authentisierung. Obecně autentizace slouží k ověření žadatelem předložených identifikačních údajů, tzn. ověření jeho proklamované identity a následnému řízení přístupu k některé z jeho poskytovaných služeb, nebo dat (aktiv). Z toho vyplývá, že hlavním úkolem autentizace je zamezení přístupu nepověřených osob, popř. útočníků, k chráněným službám a datům,nebo povolení přístupu osobám k tomu oprávněným.

Schéma řízeného přístupu:

* Žadatel - je to osoba nebo zařízení, žádající o přístup k aktivům,
* Autorita - je to osoba nebo orgán, který rozhoduje kdo a v jakém rozsahu smí k aktivům přistupovat,
* Přístupový seznam - zde jsou uvedeny identifikační údaje uživatelů spolus právy, která jim náleží,
* Kontrolér - osoba nebo zařízení povolující přístup k aktivům,
* Aktiva - cokoliv, co je organizací považováno za cenné (informace, zařízení,budovy, pověst organizace. . . ).

**Princip řízeného přístupu je následující:** Žadatel žádá o přístup k aktivům, při té příležitosti předá kontroléru svoje identifikační údaje. Ten ověří, zda tyto údaje náleží danému uživateli. Pokud souhlasí, tak si kontrolér v přístupovém seznamu najde daného žadatele, zjistí jeho přístupová práva a na jejich základě povolí žadateli přístup k aktivům. Pokud identifikační údaje nesouhlasí, je žadateli přístup k aktivům zamítnut



**Typy autentizace**

Autentizaci dělíme na fyzickou, kdy jsou identifikační údaje žadatele o aktiva kontrolovány nějakou fyzickou osobou a na základě jejího rozhodnutí je žadateli povolen přístup k aktivům, nebo na automatizovanou, kde největším problémem je ověření, zda se žadatel nevydává za někoho jiného.

Autentizaci dělíme na tří základní části:

* Autentizace znalostí: žadatel svoji identitu dokazuje znalostí (např. PIN,heslo),
* Autentizace předmětem: žadatel svoji identitu dokazuje předmětem (např.ID karta, Token, platební kartou, čipem. . . ),
* Autentizace žadatelem: žadatel svoji identitu dokazuje svými charakteristickými vlastnostmi (např. otisky prstů, hlasem. . . ).

Všechny třídy mají své výhody či nevýhody, proto se v praxi setkáváme nejčastějis jejich různými kombinacemi.

**Autentizace znalostí**

V této oblasti autentizace je žadatel před povolením přístupu k aktivům dotazován na znalost určité přístupové informace, na jejímž základě je žadateli povolen přístup. Tuto informaci by měl znát pouze autorizovaný uživatel a před případnými útočníky by měla zůstat utajena. Uživatelé tuto informaci smějí mít uloženou pouze ve své paměti, proto musí být daná přístupová informace snadno zapamatovatelná. Což je v dnešní době plné informačních systémů velmi obtížné, protože uživatel většinou disponuje hned několika hesly (řetězec alfanumerických znaků) nebo autentizačních kódů (řetězce numerických znaků) od různých systémů (např. emailové schránky, ICQ, různých sociálních sítí, pinu od platební karty. . . ). Proto se nelze divit, že si je uživatelé buďto někam zapisují, nebo používají stejná, většinou velmi jednoduchá hesla. Vezmeme-li v potaz další požadavky, které jsou v dnešní době kladeny na hesla:

* dlouhé aspoň 8 znaků,
* kombinace malých, velkých písmen, číslic i ostatních textových znaků,
* pro každý kontrolér jiné heslo,
* heslo nesmí mít nějaký význam,
* pravidelná obměna hesla,

zjistíme, že tento způsob autentizace představuje velké bezpečnostní riziko, proto se začal používat převážně v kombinaci i s jinou další třídou autentizace.

Druhou a silněji chráněnou metodou u autentizace znalostí je typ výzva odpověď. Principem této metody je, že žadatel potvrdí vhodnou odpovědí kontroléru znalost reakce na jeho výzvu. Bezpečnost této metody je založena na tom, že kontrolér posílá výzvu pouze jednou a nikdy ne stejnou. Třetí a dnes posledním známým typem je autentizace nulové znalosti (v ang. Zero-Knowledge). Žadatel v této metodě prokazuje pouze svoji znalost hesla, ale nevyzrazuje žádnou jeho část kontroléru, ten na rozdíl od výše zmíněných metod heslo žadatele nezná. Metoda zachovává anonymitu uživatele.

**Použitá literatura:**

*Burda, Karel*. Bezpečnost informačních systémů. 1. vydání Brno: FEKT VUT, Brno, 2005

*HAJNÝ, Jan*. Úvod do Zero-knowledge protokolů. Elektrorevue [online].16.10.2008, [cit. 2013-01-03]. Dostupný z WWW: www.elektrorevue.cz/cz/download/uvod-do-zero-knowledge-protokolu. ISSN 1213-1539

*HAJNÝ, Jan*; MALINA, Lukáš. Anonymní Autentizace. SeCReG [online]. [cit.2013-01-03]. Dostupný z WWW: secreg.utko.feec.vutbr.cz/cs/content/

anonymn%C3%AD-autentizace.