**Autentizace předmětem**

Jak je zřejmé z názvu této třídy, bude žadatel o přístup k aktivům prokazovat svoji identitu pomocí předmětu (tzv. Tokenu). Jelikož je přístupová informace uložena na paměťovém zařízení v Tokenu (např. čipová karta) nebo na jeho povrchu (např. průkaz totožnosti), je nutné, aby autorita zabezpečila daný předmět vhodnou technologií proti padělání a zároveň jej uživatel chránil před krádeží či ztrátou. Bezesporu největší výhodou tohoto typu autentizace je, že si uživatel nemusí pamatovat přístupovou informaci, která tím, že je uložena v Tokenu, může být delší a odolnější vůči slovníkovému útoku.

Rozdělení typů autentizačních prostředků:

1. Úložiště,
	1. s nechráněnými daty,
	2. s chráněnými daty,
		1. s přístupovou ochranou,
		2. s kryptografickou ochranou,

**Autentizátory**

Jako úložiště označujeme předměty, kde je autentizační informace pouze uložena, ale samotná autentizace se provádí na jiném zařízení. Úložiště se dělí na dvě třídy s nechráněnými a chráněnými daty. Z úložiště s nechráněnými daty lze autentizační informaci vyčíst bez jakéhokoliv omezení, použitím vhodného čtecího zařízení. Naopak u úložiště s chráněnými daty se už setkáváme s vyšším stupněm ochrany, kdy jsou autentizační informace chráněny jednoduchou kryptografickou šifrou (nutná znalost dešifrovacího klíče) nebo je k jejich vyčtení z paměti potřeba znalost hesla popř. klíče.

Autentizátory poskytují v sobě uloženým informacím nejvyšší možnou ochranu, protože se autentizační proces provádí přímo v nich a uložené autentizační informace se tak nemají jak dostat z autentizačního předmětu. Autentizátory jsou jednočipové počítače, které pro vykonávání své činnosti musí obsahovat procesor (8, 16 nebo 32 bitový), paměť (ROM/Flash, EEPROM, RAM), komunikační rozhraní a občas i kryptografický koprocesor, který slouží k provádění složitějších kryptografických výpočtů. Jedná se např. o Smartkarty nebo USB tokeny.

Autentizační předměty můžeme rozdělit podle:

1. tvaru
	1. karty,
	2. přívěsky,
	3. náramky,
2. typu paměťového úložiště pro autentizační informaci,
	1. magnetická páska / Wiegandův drát,
	2. paměťový čip,
	3. mikroprocesor,
3. komunikačního rozhraní,
	1. snímač magnetického záznamu,
	2. galvanické (kontaktní) rozhraní: ISO 7816, USB, I-Button,
	3. rádiové (bezkontaktní) rozhraní: ISO 14443

**Autentizace žadatelem**

Další možností je autentizace žadatelem. U toho způsobu autentizace dochází k porovnávání aktuálních charakteristik žadatele s uloženými záznamy, které se v terminálu nacházejí uloženy v kontejnerech nebo ve formě certifikátů autorizovaných příslušnou autoritou. Základními parametry pro to, aby se dal použit charakteristický rys žadatele k autentizaci, je jedinečnost a neměnnost dané charakteristiky. Kvůli požadavku na jedinečnost charakteristického rysu se používá tento typ autentizace pouze u osob. Autentizace založená na těchto údajích se nazývá Biometrická autentizace.

V současné době existují dvě třídy tohoto typu autentizace:

* fyziologické metody,
* behaviorální metody.

Fyziologické metody jsou metody, které se zaměřují na jedinečné a neměnné fyziologické charakteristiky člověka (např. otisky prstů, tvar obličeje. . . ), zatímco behaviorální metody jsou založeny na individuálnosti lidského chování (např. způsob psaní na klávesnici nebo způsob psaného podpisu). Mezi dnes nejpoužívanější biometriky patří ty založené na charakteristikách: otisky prstů, tvaru obličeje, oční duhovky, geometrie ruky, oční sítnice, hlasu, způsobu psaného podpisu, způsobu psaní na klávesnici.

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.