Návrh a implementace bezpečnosti v podnikových aplikacích

Pavel Horal <pavel.horal@orchitech.cz>

Obsah přednášky

- úvod do problematiky
  - aplikace, bezpečnost, …
- základní pojmy
  - informační bezpečnost, řízení přístupů, řízení bezpečnosti
- kryptosystémy a PKI
  - šifrování, hashe, razítka
  - PKI a související standardy
- protokoly a implementace
  - HTTP, OpenID, OAuth, SAML, Kerberos, WSS
  - Linux, Windows, OSX
- bezpečnostní standardy
  - ISO, CC, …

Podnikové aplikace

- *podpora fungování podniku* (ERP, CRM, BI, CMS, …)
- řízená obchodními požadavky
- *integrace s okolními systémy*
- zpracování a správa dat
- *implementuje obchodní procesy*
- konkrétní skupina uživatelů, různé role

Minesweeper, SAP, Office, SharePoint, Facebook, stackoverflow.com, bbc.co.uk, MySQL, ICQ, OpenWrt

Bezpečnost obecně

Stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí. Je to tedy míra stability systému a jeho primární a sekundární adaptace.

Zdroj: http://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx

Aplikační bezpečnost

Application security is the use of software, hardware, and procedural methods to protect applications from external threats.

Zdroj: http://searchsoftwarequality.techtarget.com/definition/application-security

Application security encompasses measures taken throughout the code's life-cycle to prevent gaps in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application.

Zdroj: https://en.wikipedia.org/wiki/Application_security

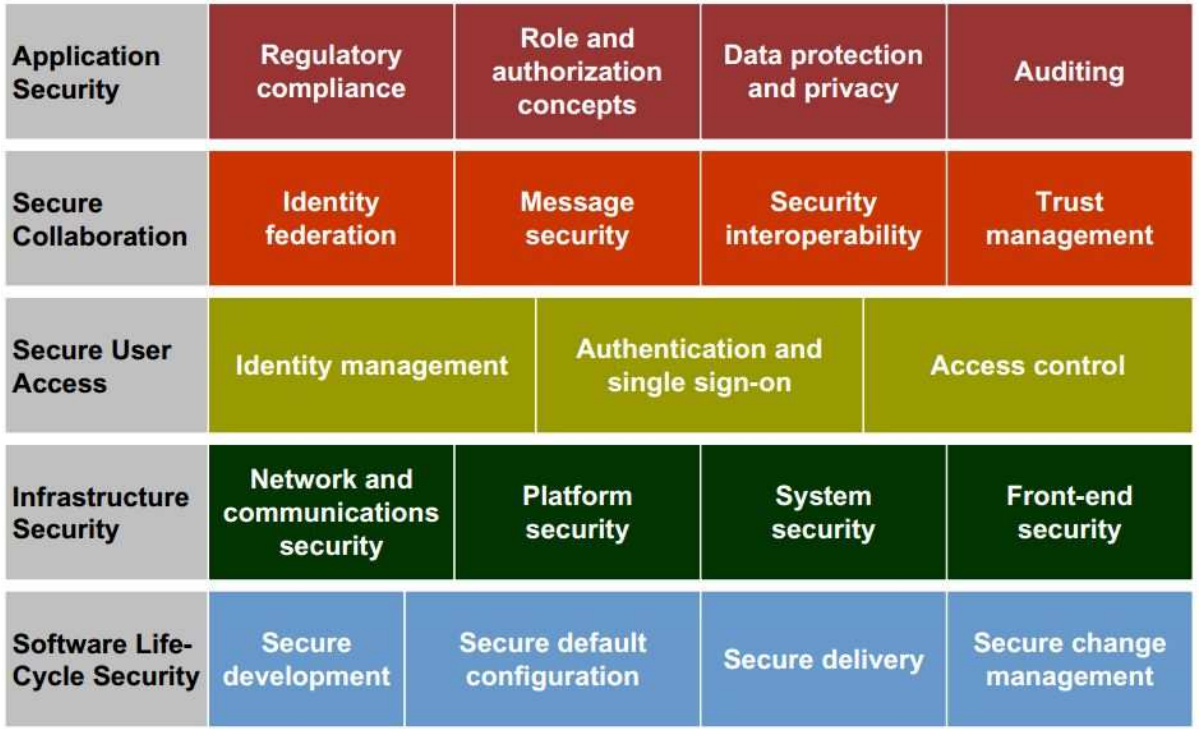
Co to znamená?

- Aplikace by měla zamezit odcizení dat.
- Aplikace by měla zamezit poškození dat.
- Aplikace by měla zajistit dostupnost dat.
- Aplikace by měla odolat chybovým stavům.
- Aplikace by měla fungovat správně.
- Aplikace by měla umožnit prokázání správné funkčnosti.
- Aplikace by měla, …

Pro zamyšlení: protokol z výslechu, corpus delicti, zatykač, vojenská informace?

Zdroj: http://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx

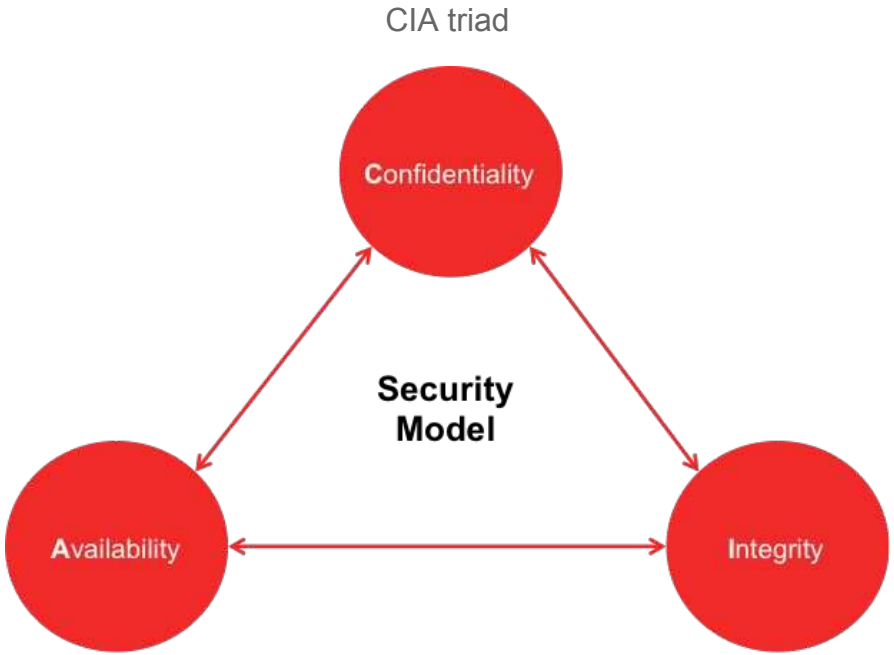
Oblasti bezpečnosti



Zdroj: Markus Schumacher, SAP AG

Informační bezpečnost

- Základní principy
  - autenticita
  - integrita
  - důvěrnost
  - dostupnost
  - nepopiratelnost
  - zodpovědnost
  - důvěryhodnost
  - sledovatelnost
- Řízení přístupů
  - identifikace
  - autentizace
  - autorizace



Zdroj: https://guardtime.com/blog/big-data-governance-and-security-for-the-fortune-500

Analýza rizik

- identifikace a ohodnocení zdrojů
- odhalení zranitelnosti a hrozeb
- návrh protiopatření pro minimalizaci rizik

- připuštění rizika, odstranění rizika, přenesení rizika

- každé protiopatření má svoji cenu (ne nutně finanční)
- vypůjčené pojmy z biometrie
  - false acceptance rate
  - false rejection rate

Obvyklé hrozby

- Validace / ošetření vstupů
  - buffer overflow, injection attacks, denormalizace
- Modifikace kódu systému
- Útok na autentizační schéma
  - odposlech, brute foce, slovníkový útok, reply, odcizení přihlašovacích údajů
- Útok na autorizační schéma
  - zvýšení práv, získání důvěrných dat, manipulace s daty
- Konfigurační řízení
  - získání konfiguračních dat, přístup k administrativním rozhraním, chybějící zodpovědnost

Zdroj: https://en.wikipedia.org/wiki/Application_security

Obvyklé hrozby

- Citlivá data
  - přístup k citlivým datům, odposlech, manipulace
- Session management
  - odcizení session, reply, man in the middle
- Kryptografie
  - špatné generování nebo správa klíčů, slabá kryptografie
- Parameter manipulation
  - query, form, cookie, header
- Exception management
  - zobrazení citlivých dat, nedostupnost
- Auditing and logging
  - odmítnutí zodpovědnosti, nedetekovatelný útok

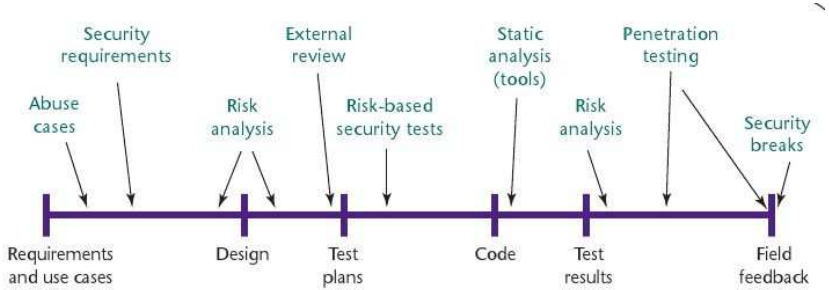
Metody zabezpečení

- procesní bezpečnost (politiky, …)
- fyzická bezpečnost (zámky, …)
- síťová bezpečnost (topologie, aktivní prvky, …)
- bezpečnost operačních systémů
- aplikační bezpečnost (řízení přístupu, …)
- datová bezpečnost (zálohy, …)

- *bezpečnost při vývoji*

Řízení bezpečnosti

- kontinuální vyhodnocování a zajišťování bezpečnosti



Zdroj: Gary McGraw: Software Security

"Cílem bezpečnostního projektu je docílení takového stavu, aby úsilí, riziko odhalení a finanční prostředky potřebné na narušení bezpečnostního systému byly adekvátní v porovnání s hodnotou, která je bezpečnostním systémem chráněna."

Zdroj: cs.wikipedia.org

Základní principy

- Určení a oddělení zodpovědnosti
- Zajištění nejslabšího článku
- Zabezpečení chybných stavů
- Jednoduchost návrhu
- Opatrnost v důvěře
- Princip nejmenšího práva
- Princip čtyř očí a obecně dvojité kontroly
- Auditní stopa
- Použití ověřených technologií

Autentizace

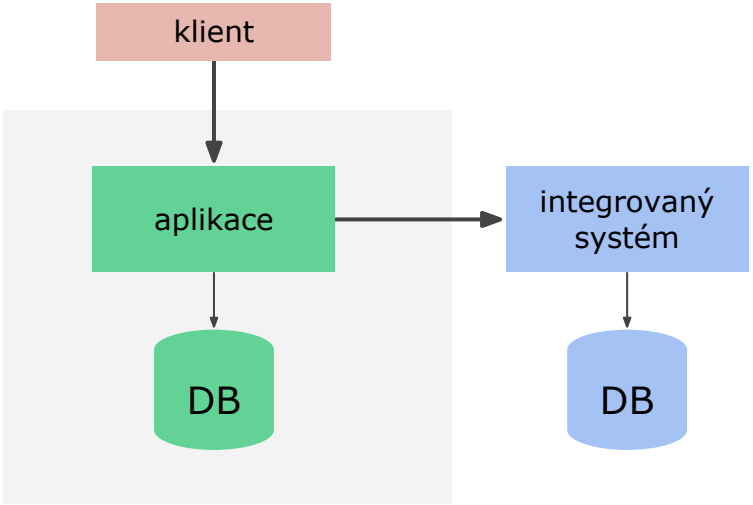
- ověření proklamované identity
- autentizace vs. identifikace

- autentizace je dokazovacím procesem
- důkaz je vlastnictví, znalost nebo vlastnost
- vícefaktorová autentizace

- úspěšná autentizace má své vlastnosti
  - úroveň a typ autentizace
  - autentizační kanál
  - …

Aplikace a jejich prostředí

- desktopová aplikace
  - běží v OS
  - nativní vs. VM
- *webová aplikace*
  - běží na serveru
  - tlustý vs. tenký klient
- mobilní aplikace
  - běží v mobilním zařízení
  - práva na HW a data



Webové aplikace

- aplikace běžící v prohlížeči (tenký klient)
- aplikace postavené na webových technologiích (HTTP)

- HTTP (RFC 2068)
  - request / response protokol
  - metoda + URI, response kód a status
  - hlavičky a tělo

Webová autentizace

- BASIC
  - jméno a heslo zakódované v BASE64
  - posílá se s každým requestem
- DIGEST
  - HA1=MD5(username:realm:password) v BASE64
  - HA2=MD5(method:URI)
  - MD5(HA1:nonce:HA2) – posílá se s každým requestem
  - nonce (reply attack)
- Formulářová autentizace
  - HTML formulář na jméno a heslo
  - speciální URI na zpracování autentizace
  - uložení autentizace?

Webová autentizace

- Klientské SSL
  - autentizaci na úrovni SSL
  - autentizace privátním klíčem (využití asymetrické kryptografie)
  - uložení autentizace?
- Další metody
  - SPNEGO / Kerberos
  - OAuth
  - OpenID Connect
  - SAML
  - CAS
  - JWT
  - …

Návrh a implementace bezpečnosti v podnikových aplikacích

Pavel Horal <pavel.horal@orchitech.cz>

Kryptologie

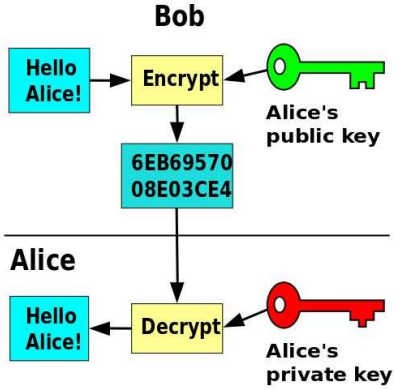
- nauka zkoumající metody dosažení cílů informační bezpečnosti
  - důvěrnost, integrita, autenticita, nepopiratelnost, …
- kryptografie vs. kryptoanalýza
- produkty jsou *kryptografické služby* s komponenty
  - kryptografické protokoly (např. výměna klíčů)
  - kryptografická schémata (např. módy blokových šifer)
  - atomické primitivy (např. blokové šifry nebo hashovací funkce)
- bezpečnost komponent je
  - prokazatelná vs. neprokazatelná (ekvivalence s obtížným problémem)
  - podmíněná vs. nepodmíněná (neschopnost provést útok v reálném čase)

Šifrování

- algoritmus pro šifrování a dešifrování textu / dat za použití tajného klíče
- ve výsledku jde o funkce `c=E(k,m)` a `m=D(k,c)`
- základní vlastností je délka klíče (bruteforce attack)
  - 128, 256, 512, 1024, … O(N) pro šifrování, $O(2^N)$ pro útok
- symetrické vs. asymetrické šifry (prokazatelná bezpečnost)
  - IDEA, Blowfish, DES, AES, RSA, RC4, DH, OTP, …
- proudové vs. blokové šifry
  - Kolik dat zašifrují blokové šifry?
- vlastnosti konfuze a difuze

Asymetrická kryptografie

- 2 klíče, jeden pro šifrování a druhý pro dešifrování
- nazýváno též jako *kryptografie s veřejným klíčem*
- vzájemný matematický vztah klíčů, obtížně odvoditelné
- šifrování, podpis, razítko



RSA

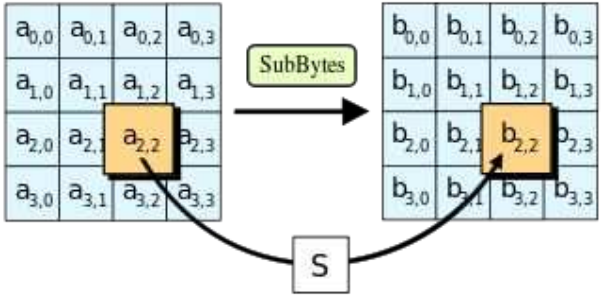
- malá Fermatova věta $a^{p-1} \equiv 1 \pmod{p}$
- aritmetika v Z_n, kde $n = p \cdot q$
- veřejný klíč
  - e; $1 < e < \varphi(n)$
- soukromý klíč
  - b; $e \cdot b \equiv 1 \pmod{\varphi(n)}$
- šifrování
  - $E(m) = m^e \bmod n$
- dešifrování
  - $D(c) = c^d \bmod n$
- nalezení d je ekvivalentní problému faktorizace, RSA však nemusí být

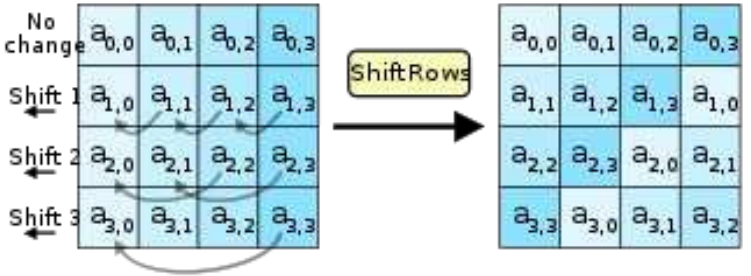
D-H Key Exchange

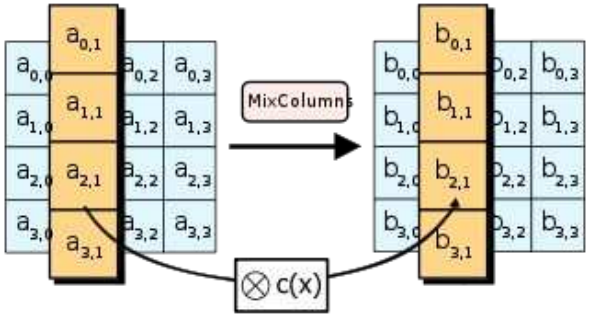
- založeno na problému diskrétního logaritmu
  - $a^x \equiv c \pmod n$
- základní průběh
  - dohoda na cyklické grupě Z_n a generátoru g
  - Alice má privátní klíč **a** a Bob má privátní klíč **b**
  - z pohledu Alice (Bob obdobně):
    - Alice dostane g^b
    - Alice vypočítá finální klíč $(g^b)^a = g^{ab}$
  - útočník se znalostí n, g, g^a, g^b není schopen jednoduše zjistit g^{ab}

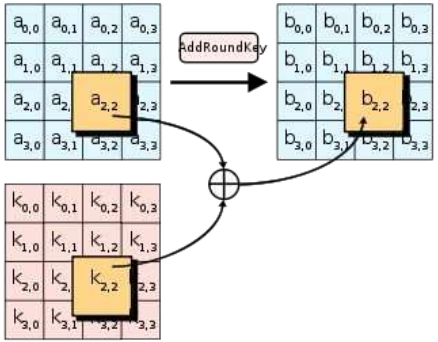
AES (Rijndael)

- délky klíč 128, 192 a 256 bitů





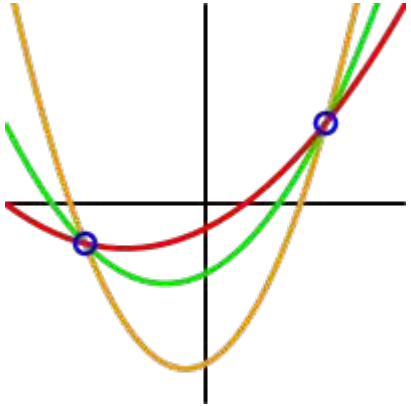




Shamirovo sdílení tajemství

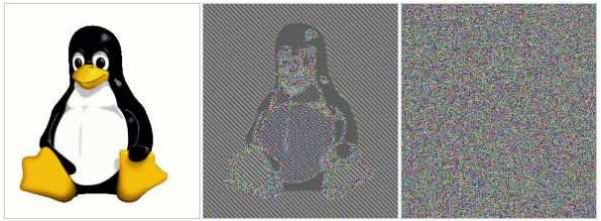
- cílem je tajemství S rozdělit na n částí tak, aby stačila znalost k částí k rekonstrukci S, ale ne $k-1$
- založeno na existenci unikátního polynomu stupně n pro $n+1$ bodů
  - $S = a_n a_{n-1} \dots a_1 a_0$
  - $a_n x^n + a_{n-1} x^{x-1} \dots a_2 x^2 + a_1 x + a_0$

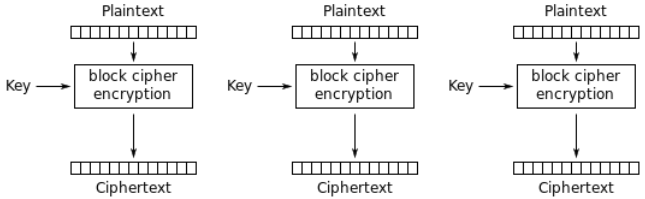
- použití v DVB nebo komplexních schématech



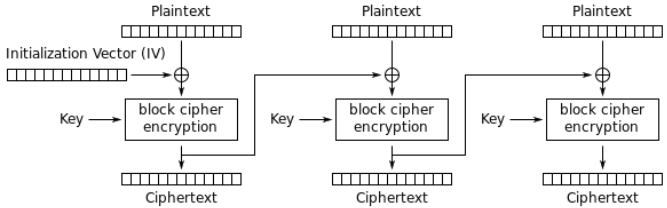
Módy blokových šifer

- Proč je problém *prostě jen šifrovat odděleně*?
- možnost generovat klíč a nebo řetězit šifrování
- ECB (Electronic Codebook)
- CBC (Cipher Block Chaining)
- CFB, OFB, CTR, (MAC), …





Electronic Codebook (ECB) mode encryption



Cipher Block Chaining (CBC) mode encryption

Padding a inicializační vektor

- inicializační vektor (veřejný, unikátní, náhodný)
- blokové šifry vyžadují plný blok → padding

- Mělo by být jasné, co znamená:
  - AES/CBC/PKCS5Padding
  - RSA/ECB/PKCS1Padding
  - …

Šifrování – útoky

- zlomení, narušení, malleability (ohebnost ŠT)
- útoky pomocí orákula
  - only ciphertext
  - known plaintext
  - chosen plaintext (adaptivní útok)
  - chosen ciphertext (adaptivní útok)
- Kreckhoffův předpoklad – útočník zná vše kromě klíče
  - porovnat se *security through obscurity*
- Lineární a diferenciální kryptoanalýza
- Útoky postranními kanály
  - time, power, EM, …

Hash

- funkce *VSTUP* → *OTISK* $(\mathbb{Z}^* \rightarrow \mathbb{Z}^k)$
- jednosměrná, bezkolizní
- kolize
  - Nalezení libovolných M a M´ tak, že h(M) = h(M´).
  - Pro M nalezení M´ tak, že h(M) = h(M´).

- MD5 (128b), SHA (190b), SHA-2 (256b/512b)
- Použití v podpisech, hesla (k čemu je sůl?), MAC, …

Zabezpečená komunikace

- Handshake
  - Kdo jsi a kdo jsem já?
  - Co umíš za šifru? Čím budeme šifrovat?
  - Jaký hash budeme používat?
- Domluva na klíči
- Posíláme data

http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite

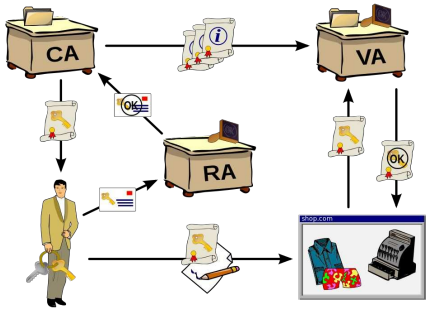
https://wiki.mozilla.org/Security/Server_Side_TLS

Další relevantní oblasti

- Steganografie
  - postupy pro ukrytí dat v jiných datech
- Samoopravné kódy
  - BCH, Hamming, RS, …
- Linked hash a witness value

Public Key Infrastructure

- Důvěryhodnost certifikátů
  - Jak mohu věřit certifikátu?
- Certifikační autorita
  - Kdo to je? Kdo se jí může stát?
- Vydávání certifikátů
  - Jak předat certifikát k podpisu bez vyzrazení klíče?
  - Jak autorita ověří, že nevydává certifikát podvodníkovi?
- Odvolání certifikátů
  - Jak se dozvím o odvolaných certifikátech?
- …



X.509

- X.509
  - struktura certifikátu
- ASN.1
  - obecná struktura
- DER
  - kódování

Certificate:
  Data:
    Version: 1 (0x0)
    Serial Number: 7829 (0x1e95)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
        OU=Certification Services Division,CN=Thawte Server CA/emailAddress=server-certs@thawte.com
    Validity:
      Not Before: Jul 9 16:04:02 1998 GMT
      Not After: Jul 9 16:04:02 1999 GMT
    Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
        OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
          66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
          16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
          8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
          e8:35:1c:9e:27:52:7e:41:8f
        Exponent: 65537 (0x10001)
  Signature Algorithm: md5WithRSAEncryption
    93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
    ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
    0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
    8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:68:9f

PKCS

- Standardy pro kryptografii s veřejným klíčem

- PKCS#7
  - Cryptographic Message Syntax (.p7, .p7s)
- PKCS#10
  - Certificate Signing Request (.p10)
- PKCS#12
  - Personal Information Exchange Syntax (.pfx, .p12)

OWASP

- Projekty s vazbou na Internetovou bezpečnost
- Auditní projekty
  - ASVS – hodnocení bezpečnosti
  - OWTF, … – (automatizované) testování
- Bezpečnostní frameworky
  - HDIV – integrita v rámci tzv. HTTP konverzací
  - …
- Žebříčky zranitelností
  - TOP 10 pro webové aplikace
  - TOP 10 pro mobilní aplikace

Návrh a implementace bezpečnosti v podnikových aplikacích

Pavel Horal <pavel.horal@orchitech.cz>

@include X

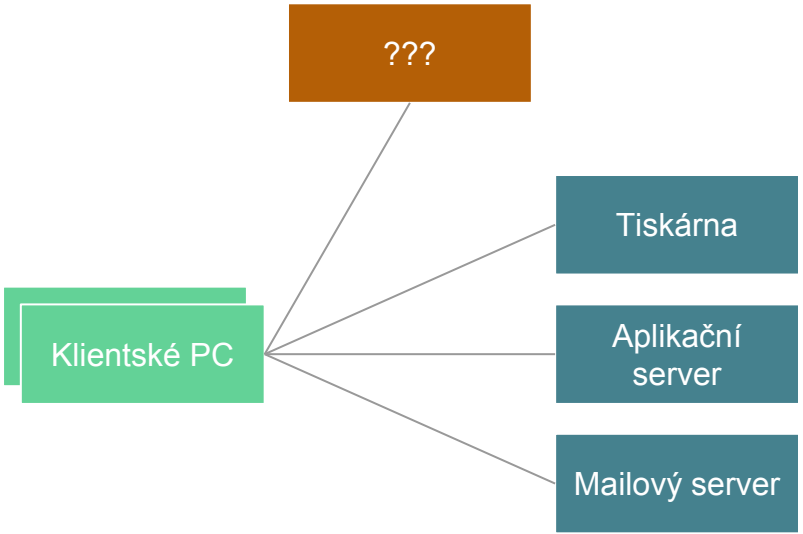
- Technologie a OS
  - HSM, AD, AGLDP, PAM, JAAS
- WSS
- **Data lifecycle**
- Provozní bezpečnost
  - IDS, IPS
- Audit

Téma na test

- OAuth
- OpenID Connect
- SAML
- SASL
- NTLM
- CAS
- JWT
- PEP / PAP
- PKCS #7, #12

Situace – organizace

- discovery
- autentizace
- autorizace

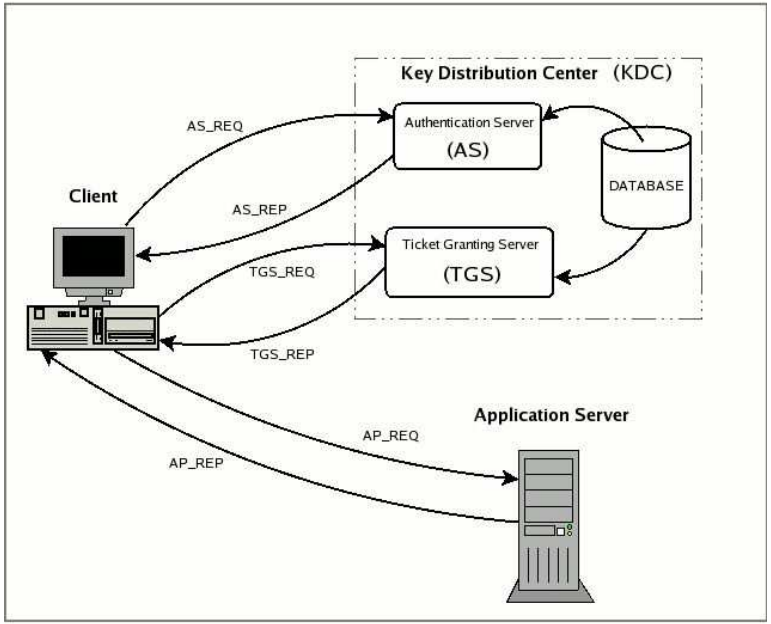


Kerberos

- KDC – key distribution center
  - AS – autentizační server
  - TGS – autorizační server
- AP – aplikační server

- Centrální autorizace
- REALM a jeho význam
- Využívá na transportní vrstvu

- Reply attack?
- Man in the middle attack?



Kerberos

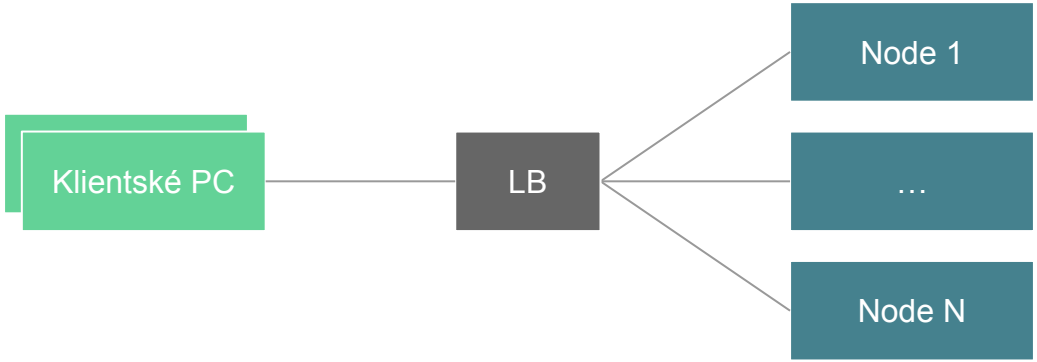
- Ticket
  - zašifrovaný (částečně – čím?)
  - **session key**
  - timestamp
- Flagy
  - Post-dated tickets
  - Proxy tickets
  - Forwardable tickets
- Example
  - klist
  - https://www.ietf.org/rfc/rfc4120.txt
  - http://web.mit.edu/kerberos/krb5-1.12/doc/admin/enctypes.html

Kerberos

- GSS API / JGSS
  - Kdo komunikuje s KDC (aplikace nebo OS)?
- SPNEGO
  - Chci to použít na webu!
- Cross-realm autentizace
  - TRUST jako specifický konstrukt.

Situace – distribuovaná aplikace

- autentizace
- session

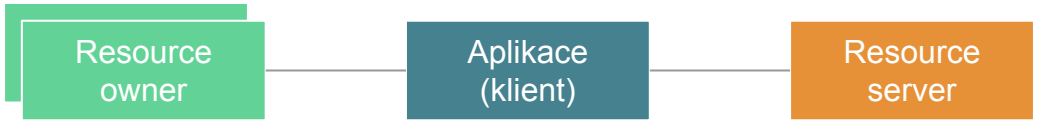


JSON Web Token

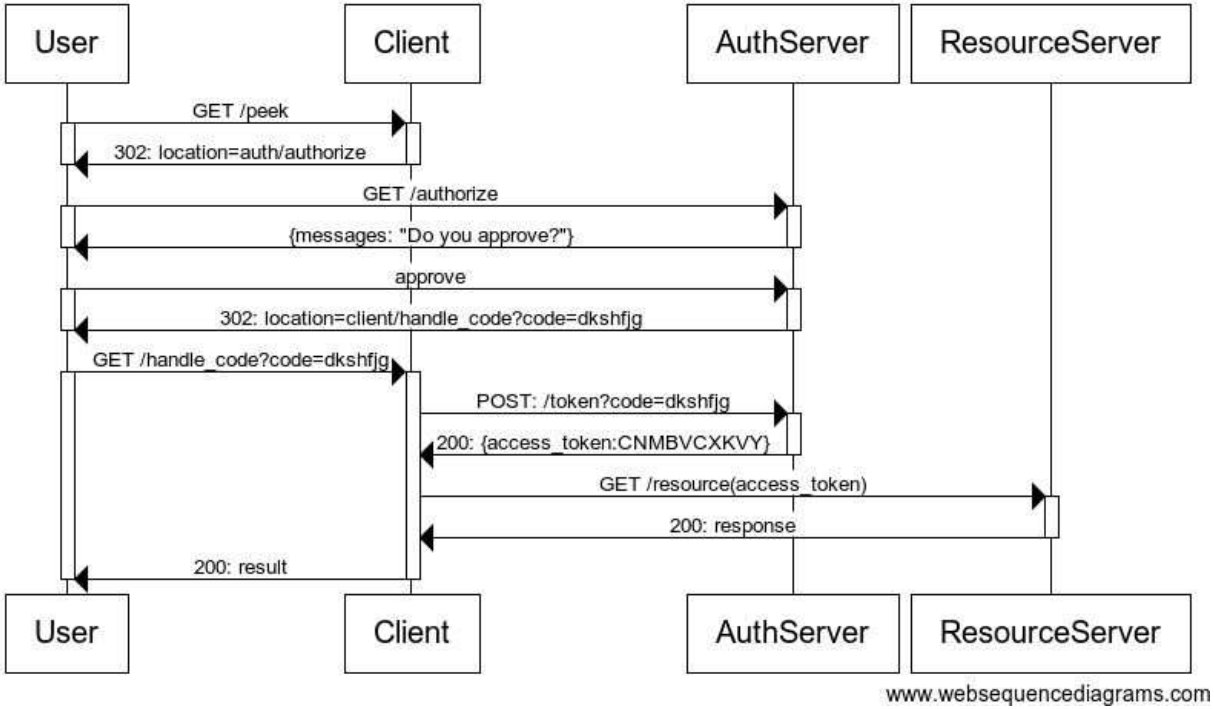
- Struktura pro zabezpečné přenášení tzv. claims
- Součásti
  - hlavička (typ, alg)
  - payload (claims)
  - podpis
- Možnost zašifrovat paylout

Situace – delegace

- trust
- delegace



OAuth 2.0

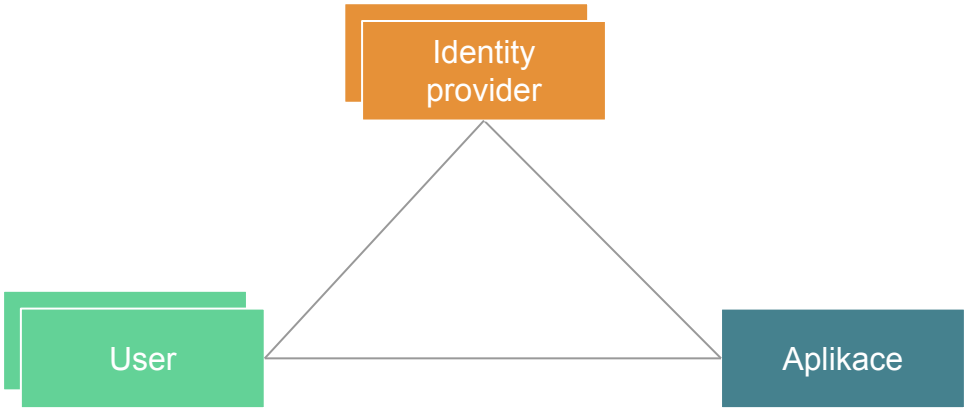

User
Client
AuthServer
ResourceServer
GET /peek
302: location=auth/authorize
GET /authorize
{messages: "Do you approve?"}
approve
302: location=client/handle_code?code=dkshfjg
GET /handle_code?code=dkshfjg
POST: /token?code=dkshfjg
200: {access_token:CNMBVCXKVY}
GET /resource(access_token)
200: response
200: result
User
Client
AuthServer
ResourceServer
www.websequencediagrams.com

OAuth 2.0

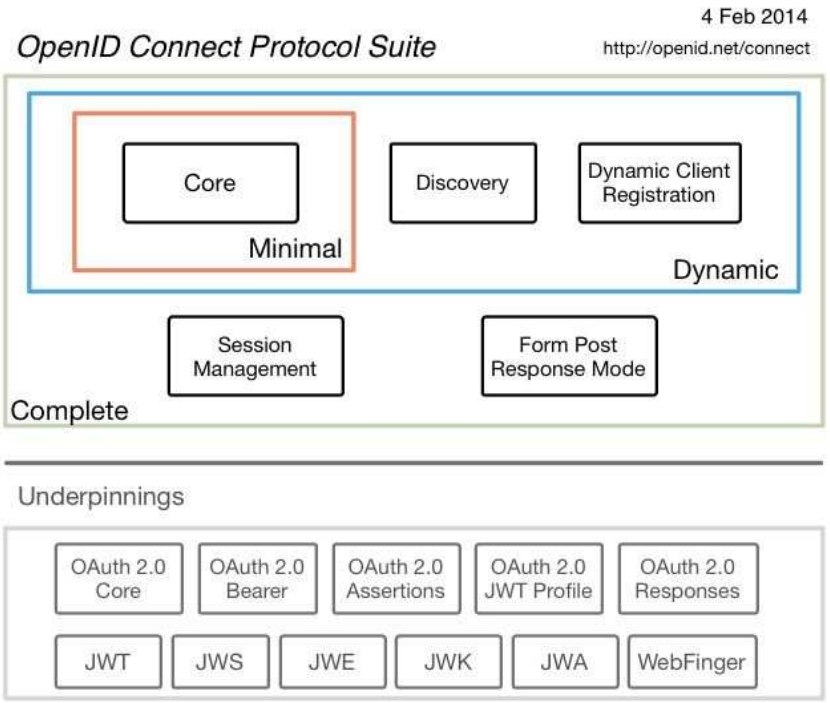
- Authorization grant – povolení přístupu
  - authorizatization code
  - implicit
  - password
  - client credentials
- Access token
- Refresh token

Situace – externí autentizace

- autentizace
- discovery
- registration
- attributes

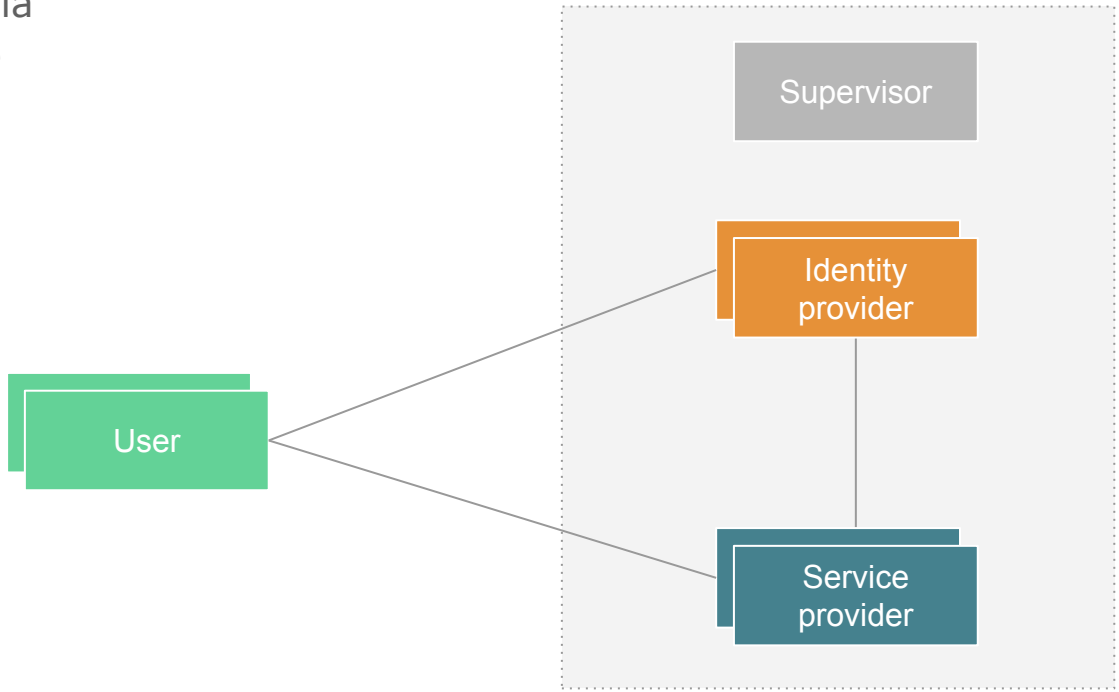


OpenID ~~1 2~~ Connect



Situace – trust

- společná pravidla
- ověření členové



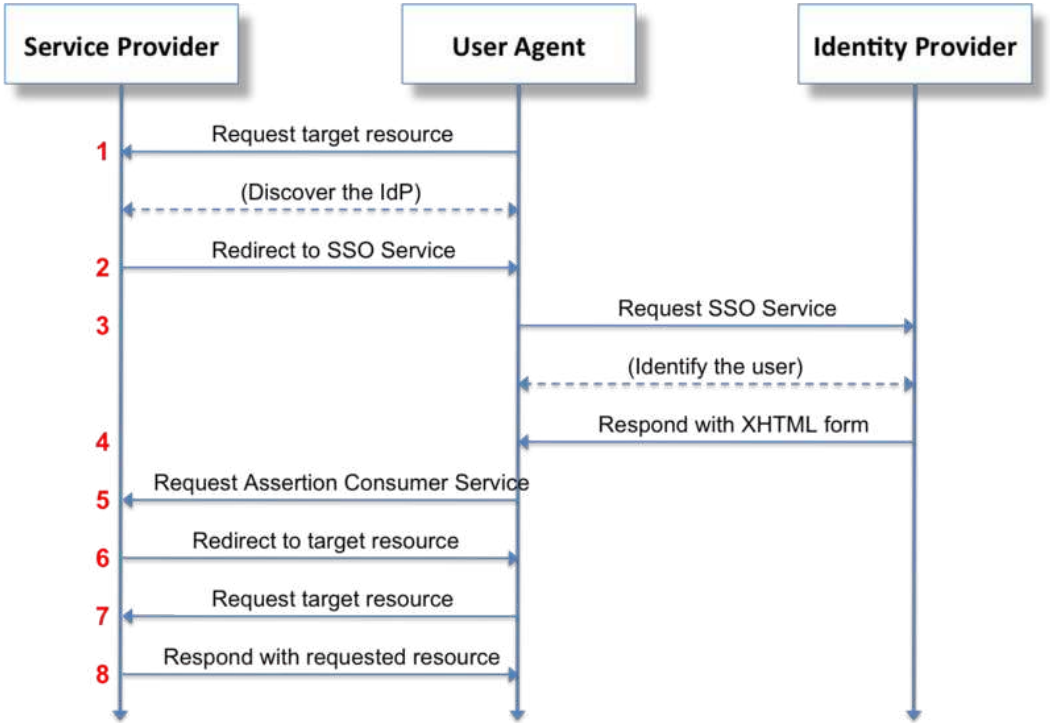
SAML

- Security Assertion Markup Language
- Tři základní účastníci:
  - Principal (uživatel)
  - Identity Provider (IdP)
  - Service Provider (SP)
- Assertion - ověření
  - Authentication statements
  - Attribute statements
  - Authorization statements

SAML

- SAML protocols
  - Assertion Query, Authentication, Artifact Resolution, Single Logout, ...
- SAML bindings
  - SOAP, HTTP Redirect, HTTP POST, HTTP Artifact, ...
- SAML profiles
  - Web Browser SSO, Identity Provider Discovery, Single Logout, Artifact Resolution, …
- SAML metadata

SAML


Service Provider
User Agent
Identity Provider
1
Request target resource
(Discover the IdP)
2
Redirect to SSO Service
3
Request SSO Service
(Identify the user)
4
Respond with XHTML form
5
Request Assertion Consumer Service
6
Redirect to target resource
7
Request target resource
8
Respond with requested resource

Situace – …

- WS komunikace
  - WSS
- centralizace autorizace
  - definice vs. vyhodnocování
- dohoda na autentizaci
  - SPNEGO, SASL, …
- single-sign-on a single-sign-out
  - IWA, CAS,
- …

XACML

- eXtensible Access Control Markup Language
- Komponenty
  - PAP, PDP, PIP, PRP
- Objekty
  - Subject, Resource, Action, Environment
- Struktura
  - PolicySet, Policy, Rule

ukázka

Spring Security

- principal – objekt reprezentující uživatele
- authentication – objekt reprezentující autentizaci
- granted authority – oprávnění v rámci aplikace

- security context – kontext běhu aplikace
  - standardně vázaný na vlákno
  - občas vázaný i na kód
  - v HTTP vázaný na HTTP požadavek

Spring Security

- SecurityContextHolder
  - ThreadLocal
  - InheritableThreadLocal
  - Global

- vše ostatní
  - inicializace contextu
  - autorizace na základě contextu

Spring Security

- Filter chain
  - sada filtrů s oddělenými úlohami a pravomocemi
  - více filter chainů dle patternu
  - může být i prázdný
- Základní sada filtrů
  - autentizační filtry (BASIC, SPNEGO, DIGEST, FORM)
    - processing URI
  - persistence filtry
  - autorizační filtry
  - zpracování chybových stavů
- AuthenticationEntryPoint
  - inicializace autentizačního protokolu

Spring Security

- Základní filtry
  - FilterSecurityInterceptor
  - ExceptionTranslationFilter
    - AccessDeniedHandler
    - AuthenticationEntryPoint
  - Processing filters
    - UsernamePasswordAuthenticationFilter
    - …
  - SecurityContextPersistenceFilter
    - SecurityContextRepository

Spring Security

- AuthenticationManager
  - autorita schopná ověřit Authentication objekt
- ProviderManager
  - DaoAuthenticationProvider
  - UserDetailsService
- PasswordEncoder
  - SaltSource

Spring Security

- Autorizace
  - pre-invocation vs post-invocation
  - FilterSecurityInterceptor vs MethodSecurityInterceptor (AOP)
- Expression-based access control
  - založeno na SpEL
  - hasRole()
  - hasPermission()
  - isAuthenticated()

Spring Security

- ACL – domain object security
- SecurityUtils a SecurityAdvisor
- LDAP, CAS, Kerberos