Paweł Rajba
pawel@ii.uni.wroc.pl
http://kursy24.eu/

Application Security Access Control

Agenda

- Basic concepts
- Authentication
- Obvious threats
- Access Control Models
- A&A in ASP.NET MVC

Basic concepts

- Identification
- Authentication
  - Identification + proof
  - Examples
    - Username + password
    - Security token
    - Smart card + PIN
    - Biometrics
- Authorization
  - Examples
    - File permissions
    - Encryption (only privileged get the key)
    - Boarding pass
    - Driver licence

Basic concepts

- Access Control System
  - Combining AuthN & AuthZ with additional rules
  - Examples
    - Rules on passwords (complexity, regular changes, history)
    - Object owner is able to determine object perms
    - Object owner is able to define object perms
    - Access denied by default
    - User ID can't be transferred
      - E.g. give to a new employee a login a someone fired

Authentication

- Types of proofs
  - Something..
    - you know
    - you have
    - you are
- Type of authentication
  - Single factor
  - Dual-, multi-factor
    - E.g. smartcard + PIN

Authentication

- Centralized vs. decentralized
- SSO
  - Concept
  - Protocols supporting SSO
    - XTACACS, TACACS+, Kerberos, SAML2, WS-Trust, WS-Federation, OAuth2

Obvious threats

- Password (sth you know)
  - Attacker may see or record when one is typing
  - Keyloggers
  - Sniffing (e.g. local network)
  - Phishing
  - Dictionary and brute force attack
  - Social attack
  - Re-use attack
    - E.g. the same password in different places

Obvious threats

- Smart cards (sth you have)
  - Steal card
  - Hack an issuer of cards
- One-time passwords (sth you have)
  - We consider both
    - Synchronic (generators on both sides)
    - Asynchronic (challenge-response protocol)
  - Again, steal device, hack device
  - Find a initial value for generator
    - Through hacking an issuer server

Obvious threats

- Biometrics (sth you are)
  - Retina scan, finger print, voice recognition, signature recognition
  - Main problem: biometrics accuracy
    - False Rejection Rate (FRR) – false negative
    - False Acceptance Rate (FAR) – false positive
  - Accuracy problem implies that one may pretend by getting e.g. victims fingerprints
  - Accuracy ranking
    - retina > fingerprint > signature > voice

Access Control Models

- Discretionary Access Control
  - Owner of an object is able to decide who is allowed to access it
  - Common example: file system ACL
- Mandatory Access Control
  - Access rules defined centrally
  - Hard to manage, but offers higher security
  - Usually based on hierarchical sensitive labels
  - Two methods for applying MAC usually
    - Rule-based
    - Lattice-based (for more complicated scenarios)

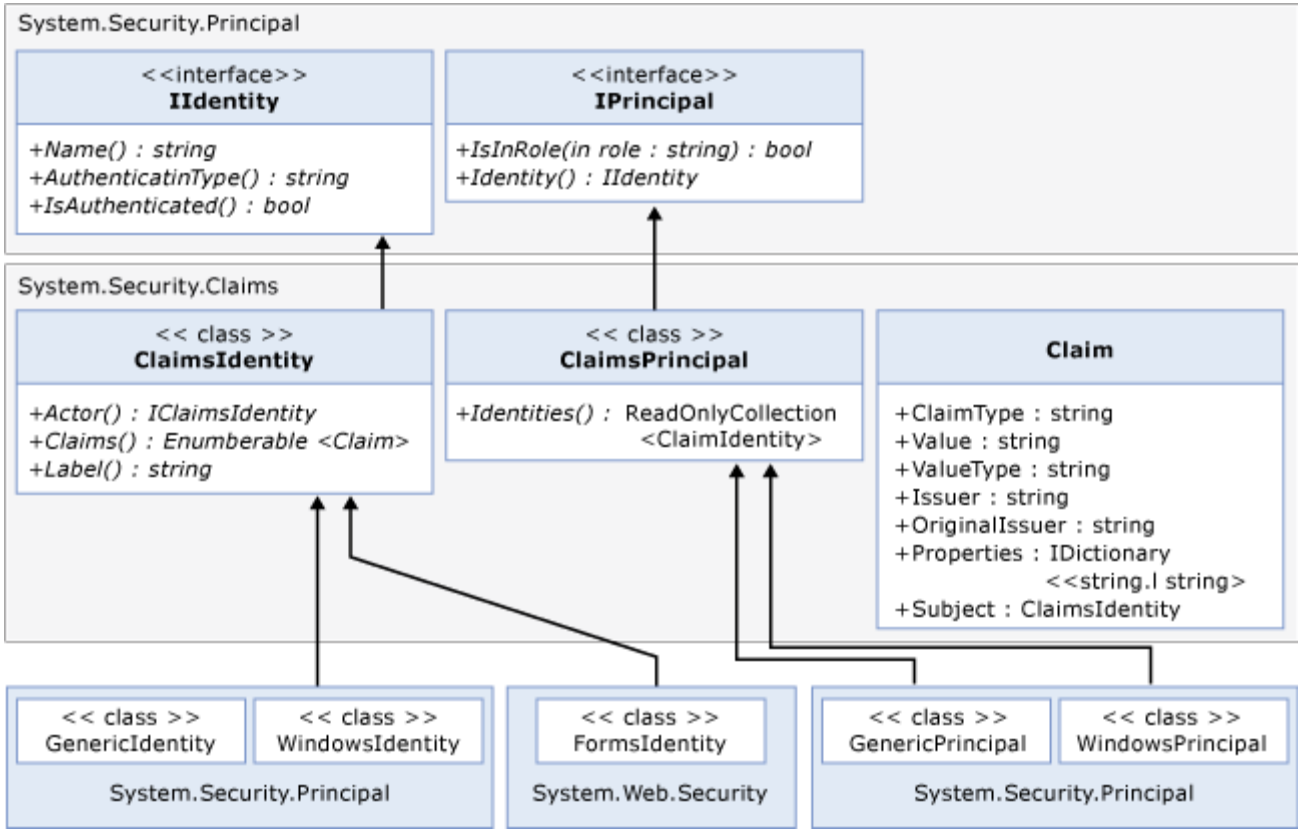
Access Control Models

- Role-based access control
  - Based on roles/groups
  - Roles are usually organized in a hierarchy
  - Roles are controlled centrally
    - MAC model is intended for only read and write
    - Roles are considered as set of permissions and give more flexibility
  - A lot of systems implement RBAC
- Attribute-based access control
  - Not based on rights assigned to subject
  - Based on attributes which are used to prove the truth of statements (i.e. claims)
  - Example:
    - Claim: „older than 18"
    - Anyone, who can prove that statement, has granted access

Source: http://en.wikipedia.org/wiki/Computer_access_control

A&A in ASP.NET MVC

- Classes related to security model in ASP.NET



Source: http://msdn.microsoft.com/en-us/library/hh873304(v=vs.110).aspx

A&A in ASP.NET MVC

- Methods for authentication
  - Anonymous
  - HTTP Basic
  - Windows
    - NTLM, Kerberos
  - Forms

A&A in ASP.NET MVC

- Entries in configuration file (web.config)
  - Authentication
    - <system.web>
      <!-- mode=[Windows|Forms|Passport|None] -->
      <authentication mode="Windows" />
      </system.web>
  - Authorization
    - <authorization>
      <allow .../>
      <deny .../>
      </authorization>
    - Meaning of * and ?

A&A in ASP.NET MVC

- HTTP Basic
  - A client sends a request to a protected resource
  - A server answers with 401 HTTP status
    - Additionaly a Realm (area description) is attached
  - In the client's browser usually a prompt for a login and password pops up
    - With every subsequent request a new header is attached Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
      - In data login:password sequence is encoded using Base64 algorithm
  - After providing a correct credentials the client is able access the resource on the server

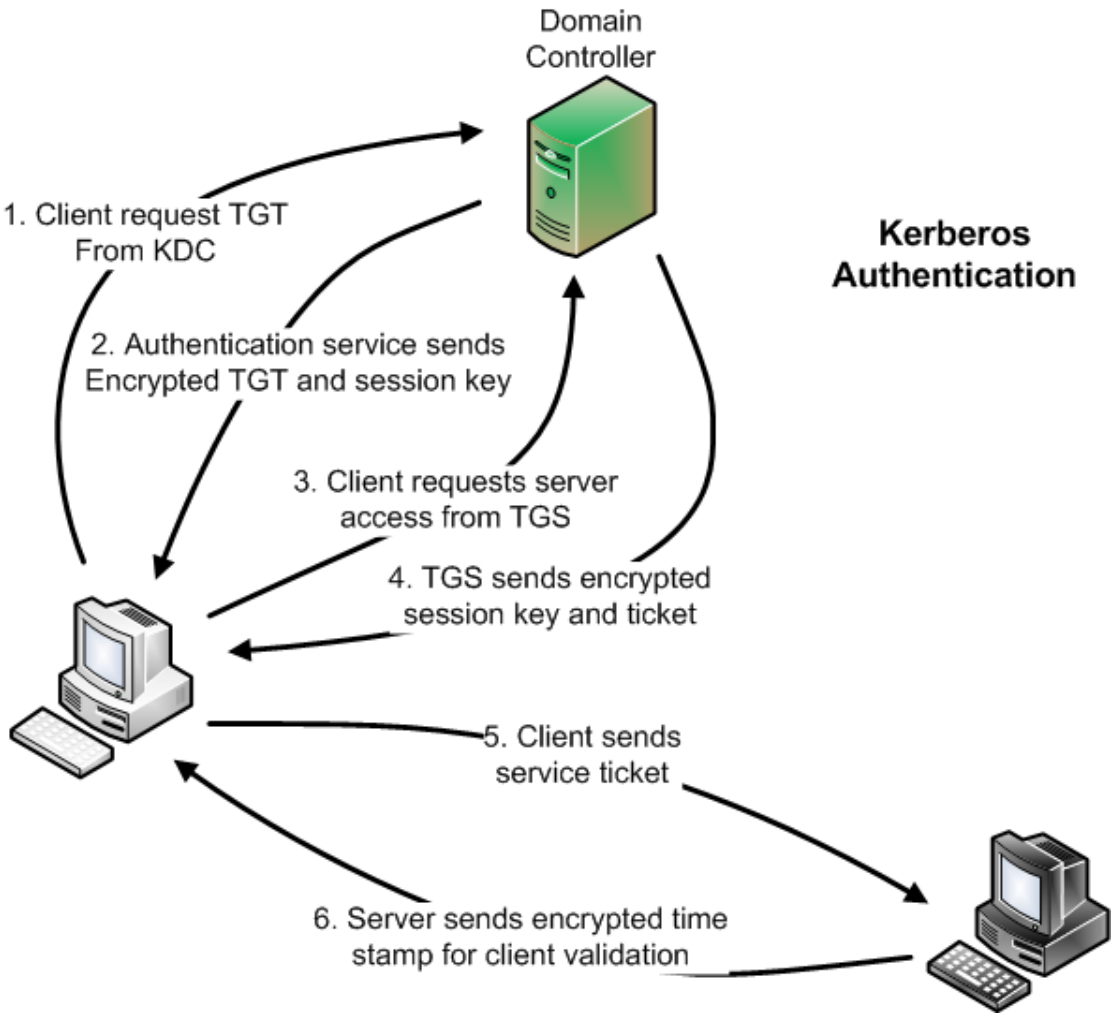
A&A in ASP.NET MVC

- Windows
  - NTLM – challenge response protocol
  - Handshake
    - 1: C → S
      - GET …
    - 2: C ← S
      - 401 Unauthorized
        WWW-Authenticate: NTLM
    - 3: C→ S
      - GET …
        Authorization: NTLM <base64-encoded type-1-message>
    - 4: C ← S
      - 401 Unauthorized
        WWW-Authenticate: NTLM <base64-encoded type-2-message>
    - 5: C → S
      - GET …
        Authorization: NTLM <base64-encoded type-3-message>
    - 6: C ← S
      - 200 Ok

Source: http://www.innovation.ch/personal/ronald/ntlm.html

A&A in ASP.NET MVC

- Windows
  - Kerberos



Source: http://digital-forensics.sans.org/blog/2012/09/18/protecting-privileged-domain-accounts-network-authentication-in-depth

A&A in ASP.NET MVC

- Windows
  - NTLM, Kerberos and headers
    - One can encounter the following headers
      - Authorization: NTLM message-encoded-in-base64
      - Authorization: Negotiate message-encoded-in-base64
    - Of course NTLM means NTLM, however…
    - Negotiate can be both NTLM and Kerberos

A&A in ASP.NET MVC

- Forms authentication
  - Based on login form and authentication cookie
  - Authentication cookie has several parameters
    - Protection: None | All | Encryption | Validation
  - Meaning of
    - MembershipProvider
    - RoleProvider

A&A in ASP.NET MVC

- Authorization
  - Authorize attribute
  - User.IsInRole()
  - Roles.IsUserInRole()
- Claim-based approach

A&A in ASP.NET MVC

- DEMO: IntegratedSecurity
  - Different deployments
    - Local IIS, IIS Express (see properties tab), built-in server
  - Web.config
  - Global.asax and review of authenticated user
  - IIS Manager and check different options
  - Template view

A&A in ASP.NET MVC

- DEMO
  - FormsBasedSecurity
  - FormsBasedOldSecurity
- Review of code
- Review of auth cookie
- Playing with users and roles
- Review of users database

References

- Biometrics
  - http://en.wikipedia.org/wiki/Biometrics
- NTLM & Kerberos
  - http://www.innovation.ch/personal/ronald/ntlm.html
  - http://blogs.technet.com/b/tristank/archive/2006/08/02/negotiate-this.aspx
  - http://digital-forensics.sans.org/blog/2012/09/18/protecting-privileged-domain-accounts-network-authentication-in-depth
- ASP.NET
  - Provider model http://www.hanselman.com/blog/IntroducingSystemWebProvidersASPNETUniversalProvidersForSessionMembershipRolesAndUserProfileOnSQLCompactAndSQLAzure.aspx
  - WIF programming model http://msdn.microsoft.com/en-us/library/hh873304(v=vs.110).aspx
  - Roles http://msdn.microsoft.com/en-us/library/system.web.security.roles_methods.aspx