Spencer Harbar

Kerberos Part One:

No ticket touting here, does SharePoint add another head?

SOFTWARE DEVELOPMENT NETWORK

About the speaker…

- Spencer Harbar - www.harbar.net | spence@harbar.net
  - Microsoft Certified Master | SharePoint 2007
  - Microsoft Certified Master | SharePoint Instructor & Author
  - Most Valuable Professional | SharePoint Server
  - SharePoint Patterns & Practices Advisory Board Member
  - 15 years in Enterprise IT
  - ISPA Board Member
  - Enterprise Architect working with Microsoft's largest customers deploying Office SharePoint Server 2007.

Microsoft CERTIFIED Master

SDN SOFTWARE DEVELOPMENT NETWORK

MVP Microsoft Most Valuable Professional

Agenda

- Two-part session
- Part One (this session!)
  - Authentication Methodologies
  - Kerberos Overview
  - Why Kerberos with SharePoint?
  - Implementing Kerberos with SharePoint
  - Common Problems
  - Best Practices
- Part Two (16.15)
  - Troubleshooting
  - Shared Service Providers
  - Search
  - “Advanced” Scenarios
  - Kerberos Only?
  - More Tools
  - Q&A/Discussion

Authentication Mechanisms

- Trusted Subsystem
- Impersonation/Delegation

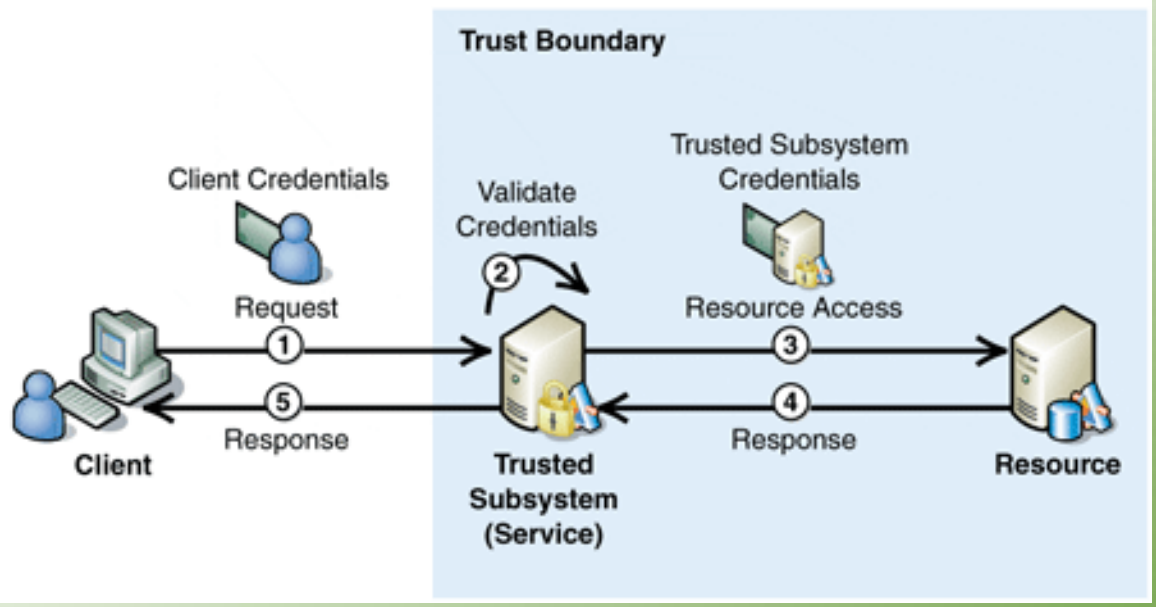
- Core concepts that underpin every web application, ever!

Essential Reading:
Designing Secure Web Based Application for Windows 2000
Michael Howard
www.microsoft.com/mspress/books/4293.aspx

SOFTWARE DEVELOPMENT NETWORK

Trusted Subsystem

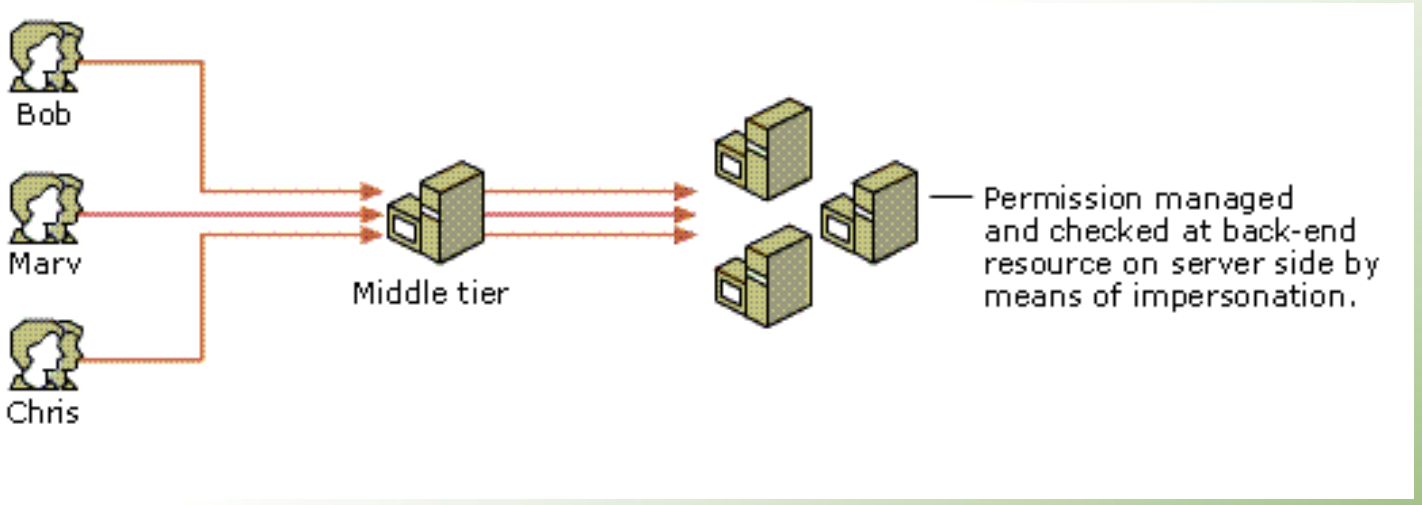
- Resources are accessed by a “service account”
- Caching & SQL Connection Pooling
  - Application Pools enable:
    - with Windows Credentials
    - zero credential storage
- SharePoint is predominately a Trusted Subsystem



SOFTWARE DEVELOPMENT NETWORK

Impersonation/Delegation

- Resources are accessed using client credentials
- Allows end to end auditing etc
- Caching / Pooling not possible



SOFTWARE DEVELOPMENT NETWORK

What is Kerberos?

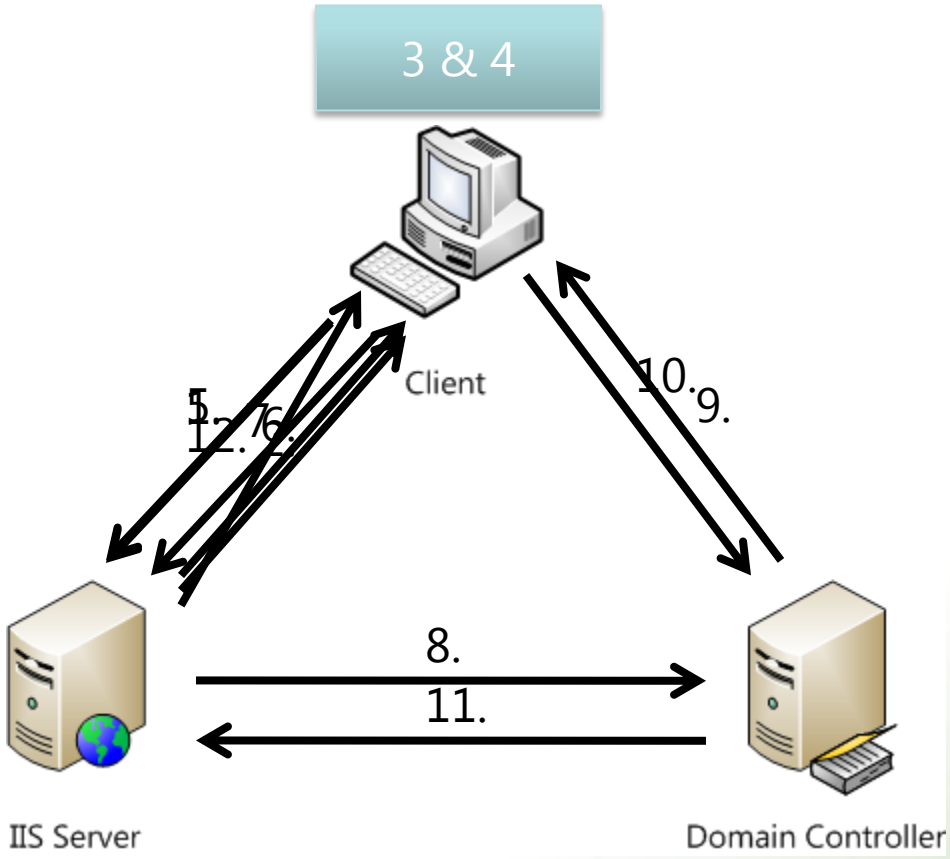
- Open, Extensible ***Authentication*** Protocol developed at MIT
- Implemented in Windows 2000 and above Domains
- Implemented as a Security Support Provider (SSP) and accessed through the SSP Interface (SSPI)
- Default Authentication Protocol in Windows 2000 and above Domains
- Windows 2003 adds support for certificate based smart cards

Kerberos Benefits

Delegated Authentication	• e.g. allows a web server to impersonate a client when accessing a database resource • a.k.a. "double-hop authentication"
Interoperability	• with other implementations, open (IETF based) • mature (10+ years)
Efficient	• renewable session tickets • avoids unnecessary roundtrips to domain controllers
Mutual Authentication	• allows verification of server identity
Secure	• Assumes network is **un-trusted** • Real encryption!

COMPARING NTLM AND KERBEROS

Windows Authentication (NTLM)



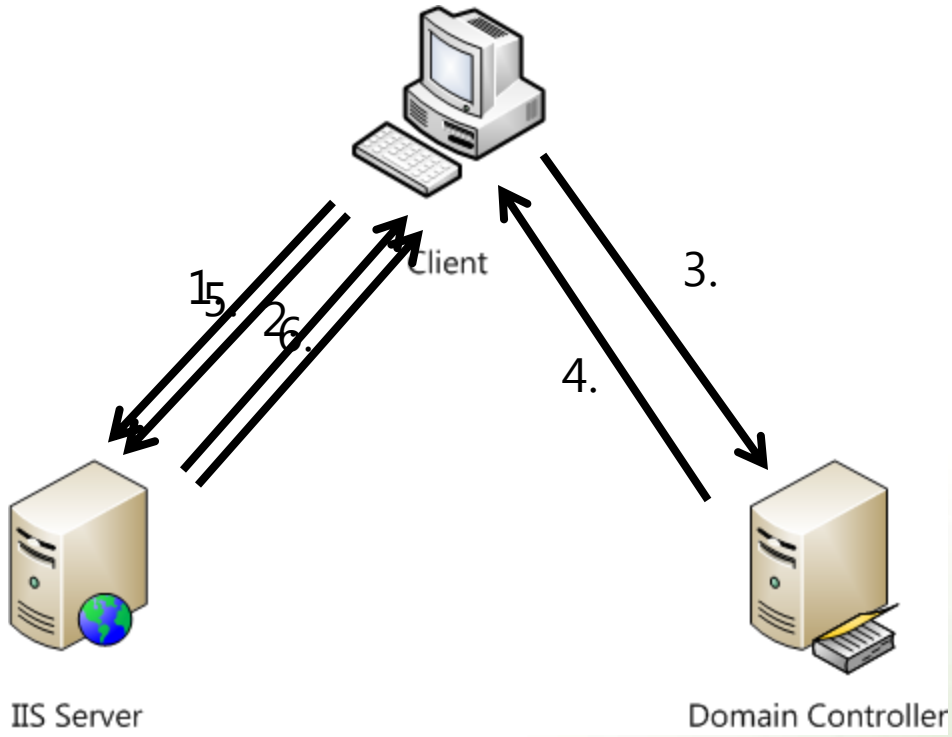
1. HTTP GET
2. HTTP: 401 WWW-Authenticate: NTLM Header
3. Acquire Credentials
4. Construct AuthN Token
5. HTTP GET with Username
6. HTTP 401: NTLM Challenge
7. NTLM Challenge Response
8. Username Token *
9. NTLM Challenge *
10. NTLM Challenge Response *
11. Authentication Success
12. HTTP 200: OK

- Doesn't Scale
- Doesn't Perform
- Shared Secret over the wire

SOFTWARE DEVELOPMENT NETWORK

* Max NTLM Auths (2 by default) can be tweaked, but can tank your DCs

Windows Authentication (Kerberos)



1. HTTP GET
2. HTTP: 401 WWW-Authenticate: Negotiate or Kerberos
3. Request Service Ticket from KDC
4. Service Ticket returned
5. HTTP GET with authenticator
6. HTTP 200 OK

Approx one authN every five minutes

SOFTWARE DEVELOPMENT NETWORK

Comparing NTLM & Kerberos

	NTLM	Kerberos
Cryptography	Symmetric	Symmetric and/or Asymmetric
Trusted 3rd Party	Domain Controller	Domain Controller with KDC Domain Controller and Enterprise CA
Supported Clients	Windows 9x, Me, NT4, 2000 and above	Windows 2000 and above
Features	Slow auth (pass thru)	Ticketing
	No mutual AuthN	Mutual AuthN
	No delegation	Delegation
	Proprietary	Open Standard
	Lamer data protection	Cryptographic data protection

WHY KERBEROS WITH SHAREPOINT?

SOFTWARE DEVELOPMENT NETWORK

Security

- Inter-server communications
- End user authentication
- Applications that require Delegation

Performance & Scalability

- More RPS *can* be possible
  - due to dramatically less AuthN round trips
  - Primarily for long user sessions
- Reduction in impact on Domain Controllers
- Helps address multi-domain scenarios

- Performance myths:
  - “Kerberos makes SharePoint faster”
  - “One DC for every three WFEs”

SOFTWARE DEVELOPMENT NETWORK

Performance Comparison

	Ave RPS	Ave PRT
"Standard" Session		
Kerberos	35.6	4.18
NTLM	**42.6**	**3.29**
"Long" Session		
Kerberos	**58.2**	**3.16**
NTLM	42.3	3.89

- RPS = Requests Per Second (Higher is better)
- PRT = Page Response Time (Lower is better)

SOFTWARE DEVELOPMENT NETWORK

Functionality

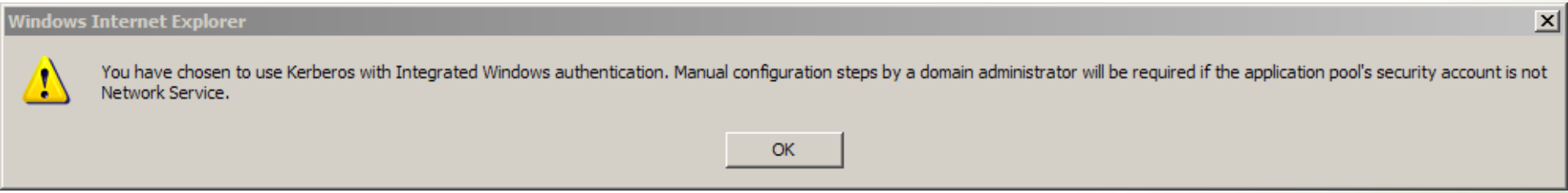
- Delegation
  - RSS Viewer
  - Excel Services to SQL Analysis Services
  - SQL Server Reporting Services
  - Other applications (e.g. SAP via BDC)
  - Custom code

IMPLEMENTING KERBEROS WITH SHAREPOINT

SOFTWARE DEVELOPMENT NETWORK

SharePoint Comedy

- You've all seen the lamer dialog:



- SharePoint books say:
  "we recommend Kerberos but we're not gonna tell you how to set it up, here's a link to a non SharePoint KB"
- Detailed terribly on the "interweb"
  - Focus on single server scenarios
  - Dozens of erroneous blog posts, articles etc
- Fixed with technet.microsoft.com/en-us/library/cc263449.aspx

SOFTWARE DEVELOPMENT NETWORK

Requirements

- Windows 2000 and above
- a TCP/IP Network
- DNS (hosts files still work)
- an Active Directory Domain
- Consistent Time Service
- Service Principal Names (SPNs)

Where?

SQL Communications	• SQL Server Service Account • Farm SQL Connections
Web Applications	• Inc. Central Admin & SSP Admin • End user authentication
Shared Services	• For each SSP • Web Services

SOFTWARE DEVELOPMENT NETWORK

How?

DNS

- Always use A records!
- Don't use Aliases (CNames) for Web Applications

Active Directory

- Implement "Service Accounts" for Application Pool Identities

How?

Active Directory Attributes	• Service Principal Names (SPNs) • Delegation (if needed)
SharePoint	• STSADM • Central Administration
IIS7	• Configure Kernel Mode Authentication

Service Principal Names

- Notation is key

  PROTOCOL/HOST:PORT

  e.g.

  http/intranet.sharepoint.com
  MSSQLSvc/sql.sharepoint.com:1433

- Port is **not** required when using default port for HTTP.
- Best Practice:
  SPN for both hostname and “fully qualified” name:

  http/intranet
  http/intranet.sharepoint.com

SOFTWARE DEVELOPMENT NETWORK

PAC Validation

- Privilege Attribute Certificate validation takes place by default (on Windows 2003)
- Still making use of Secure Channel
  - causes delays
  - perceived poor performance
- Windows 2003 SP2 introduces ability to disable (KB 906736)
- DWORD:
  HKLM\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters\ValidateKdcPacSignature = 0
- On Windows 2008 default is off (0)

SOFTWARE DEVELOPMENT NETWORK

Kernel Mode Authentication

- Introduced with IIS7
- Significantly Improves Performance
- Eases configuration (except when using SharePoint!)
- HTTP.sys handles authentication
  - under LocalSystem regardless of the application pool identity
  - Means no SPN is required
  - No good in a farm (even a single SharePoint server)

- It's not SharePoint's fault (this time!)
- Disable (via IIS7 UI) not good!
- Best Practice: Configure via applicationHost.config
- BSOD Alert!!! Hotfix at KB962943

Configuring Kernel Mode AuthN

- `useAppPoolCredentials` attribute in `system.webServer/security/authentication/Windows-Authentication` configuration section to true.

```
<windowsAuthentication enabled="true"
useKernelMode="true" useAppPoolCredentials="true" />
```

- There is no ability to edit this value using the IIS Manager.
- Best Practice: on a per Web Site basis

```
appcmd set config "SharePoint - 80“
    /section:windowsauthentication
    /useAppPoolCredentials:true
    /commit:MACHINE/WEBROOT/APPHOST
```

SOFTWARE DEVELOPMENT NETWORK

Implementing Kerberos for SharePoint

DEMONSTRATION

SOFTWARE DEVELOPMENT NETWORK

Testing and Validation

- Don’t test from DC or Web Server!
- Windows Security Auditing
- Kerberos Auditing (more in Part Two)
- Kerbtray and Klist
- Netmon and Fiddler (etc)
- IIS Log Files, IIS7 Failed Request Tracing
- Above all, be patient!
  - Use IISRESET

Common Issues

Issue

- Mis-configured SPNs
- Duplicate SPNs
- Clock Skew
- PAC Validation
- Host name issues
- Load Balancing Myths
- IE6 Clients use NTLM

Resolution/Best Practice

- Use correct notation!
- Use new SETSPN –X switch
- Ensure Time Sync
- Disable PAC Validation
- Never use CNames!
- Setup Web App Correctly
- Don't use CNames!
  - or MSKB 911149

SOFTWARE DEVELOPMENT NETWORK

DON'T USE ALIASES (CNames) for Web Applications!

General Best Practices

- Windows Server 2008 if at all possible
- Install Infrastructure Updates (or later)
- Patience!
- NTLM first, then enable Kerberos
- Script configuration only after extensive testing
- Document your configuration! (no really!)

Essential Tools

- CLI: Setspn.exe
  - Windows Server 2008: installed by default
  - Windows Server 2003: part of Resource Kit or separate download
    http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd
- GUI: Adsiedit.msc
  - Windows Server 2008: installed by default
  - Windows Server 2003: part of support tools (on Windows CD)
- Kerbtray.exe
  http://www.microsoft.com/downloads/details.aspx?familyid=4E3A58BE-29F6-49F6-85BE-E866AF8E7A88
- Klist.exe
  http://www.microsoft.com/DownLoads/details.aspx?familyid=1581E6E7-7E64-4A2D-8ABA-73E909D2A7DC
  - Both part of the Windows 2003 Resource Kit Tools
    http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd
- Network Monitor 3.3
  http://www.microsoft.com/downloads/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f
- Fiddler http://www.fiddlertool.com/

SOFTWARE DEVELOPMENT NETWORK

More in Part Two

Takeaways

- **It's easy! Don't believe the hype!**
- However, tons of misinformation and myths on the 'net
  - DCOM Configuration – Delegation - Dodgy Blog Posts!

- The best links:
  - Configure Kerberos authentication (Office SharePoint Server)
    http://technet.microsoft.com/en-us/library/cc263449.aspx
  - Ken Schaefer's IIS & Kerberos FAQ Article Series
    http://www.adopenstatic.com/faq/
  - Kerberos Authentication Tools and Settings
    http://technet.microsoft.com/en-us/library/cc738673.aspx
  - Troubleshooting Kerberos Errors
    http://www.microsoft.com/downloads/details.aspx?FamilyID=7DFEB015-6043-47DB-8238-DC7AF89C93F1

In Part Two (at 16.15)

- Troubleshooting
- Shared Service Providers
- Search
- “Advanced” Scenarios
- Kerberos Only?
- More Tools
- Q&A/Discussion

SOFTWARE DEVELOPMENT NETWORK

Thank You!

Please complete your evaluations

It makes us better next time!

SOFTWARE DEVELOPMENT NETWORK