全面接触 WSE 3.0 和 Windows Communication Framework (Indigo)

莫淘
软件架构专家

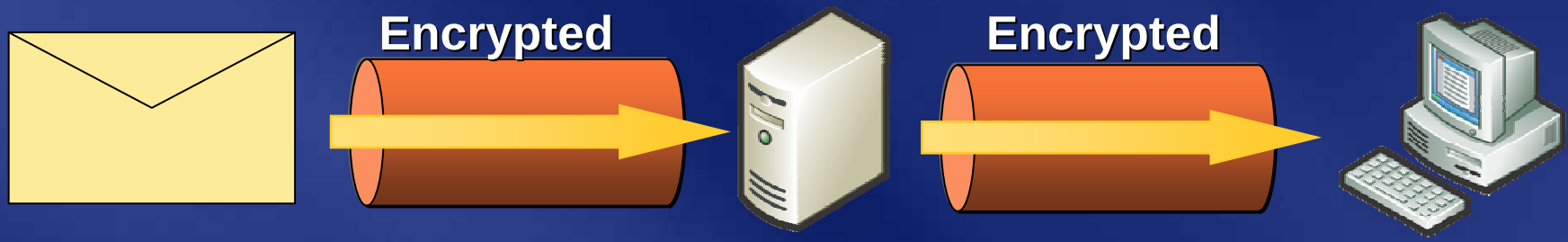
Developer & Platform Evangelism
Microsoft Corporation

.NET Web Services

- ASMX 是 .NET Framework 级别上对WEB服务的实现
  - 支持基本的规范(Basic profile)
  - 对简单的服务的支持
  - 没有实现 WS-* 规范 (WS-* specification)
- WSE 是对ASMX的扩展
  - 可以用来对ASMX行为进行扩展
  - 提供对一些 WS-* specs 的支持
  - 支持完全的客户化
- Indigo 提供对下一代 Web Services的实现
  - 提供了对WS-*, Messaging, Queuing, Transactions 等规范的一致性的编程模型

WSE 是安全的

安全的通讯
协议级别的安全

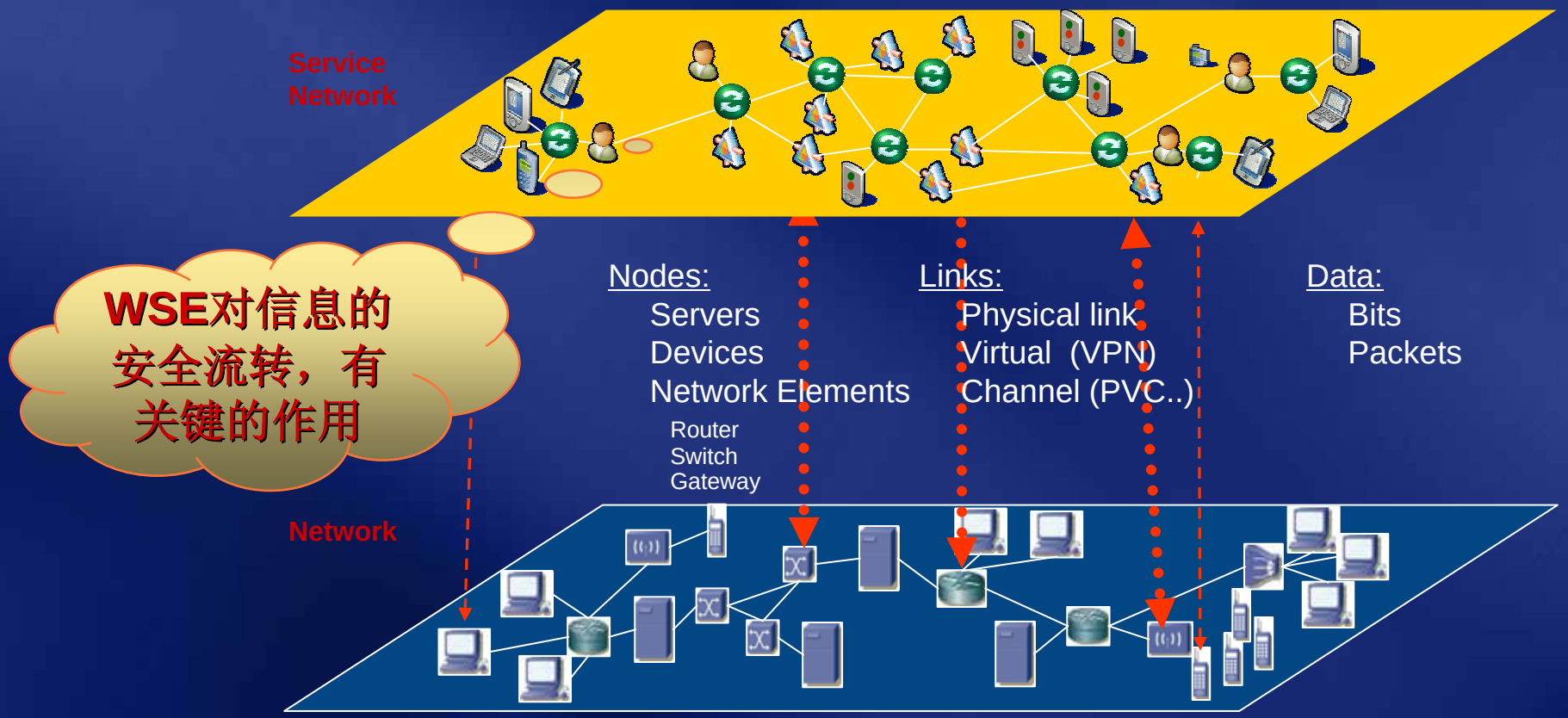


- 发送者必须信任仲裁者
- 信息由仲裁者解密
- 信息的整体被加密
- 在可以被使用的协议和加密方法上，有局限性

安全的通讯
端对端的安全

- 独立于传输，提供端对端的信息安全
- 支持多种协议和加密机制
- 提供对部分信息的加密
- 发送者只需信任最终接受者
- 签名和数据可以存储在一起

安全的通讯
将数据和用户耦合在一起

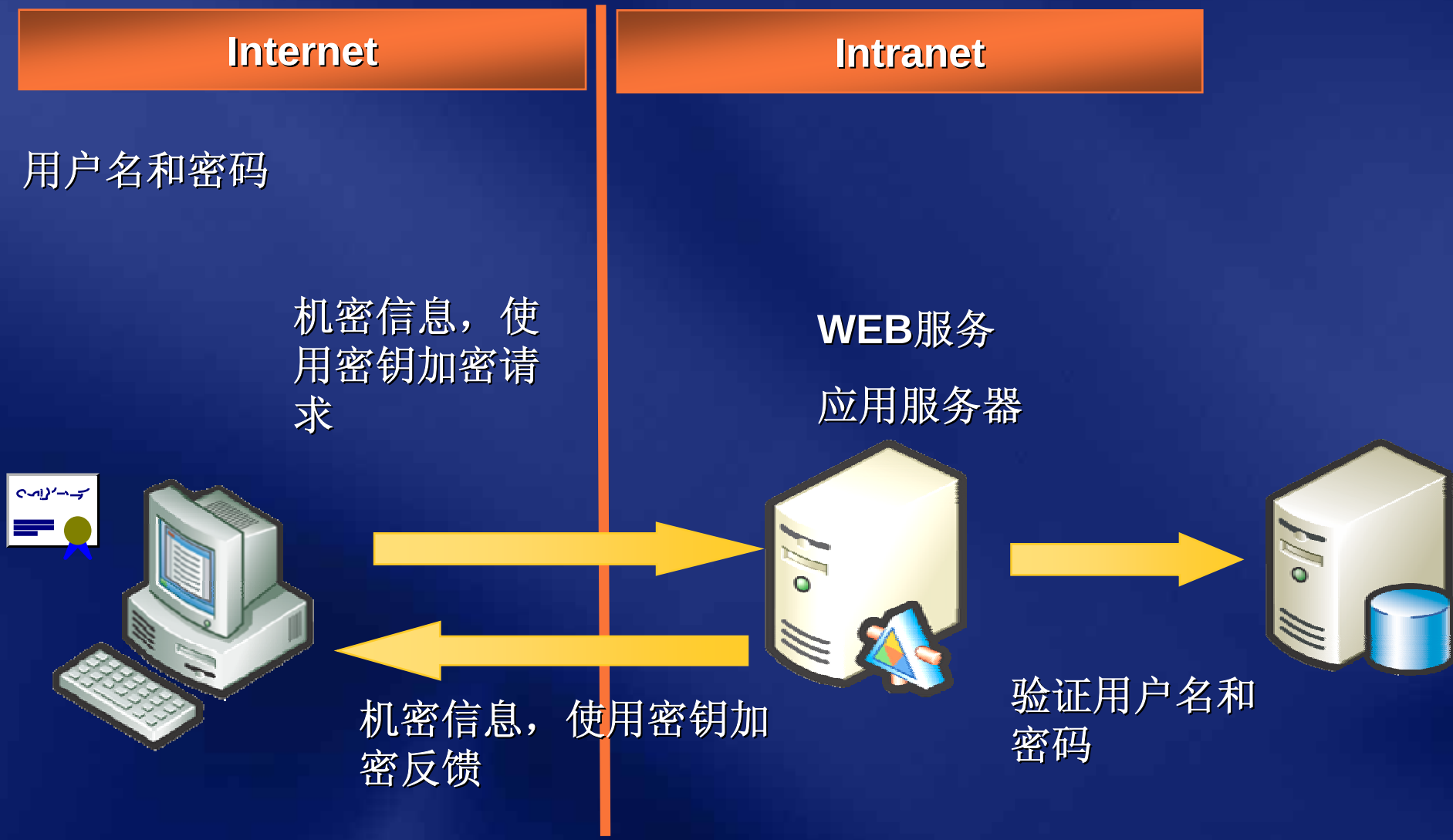


WSE 3.0 支柱

- 方便和简单的构造安全的WEB服务
- 可以非常方便的利用WS-* 规范和.NET Framework v2.0 面向服务的系统(Service Oriented System)的开发

WSE 3.0 基于 .NET Framework 2.0，提供了面向 Indigo 的兼容能力

典型的安全场景（1）
使用 X509 证书进行用户验证



典型的安全场景（2）
安全场景的模式

- 这些模式是基于行业中的最佳时间而总结出来的
- 每一个场景代表了一种安全的断言
  - UsernameOverX509Security
  - AnnonymousOverX509Security
  - UsernameOverTransportSecurity
  - KerberosSecurity
  - MutualX509Security

安全策略

安全策略是一种部署时期考虑的问题

策略

- 只接受利用服务器证书结合**Username/Password**的方式
- 呼叫者需要具有管理员的权限

策略

- 只接受**Kerberos**的认证方式

WSE 3.0中的策略文件

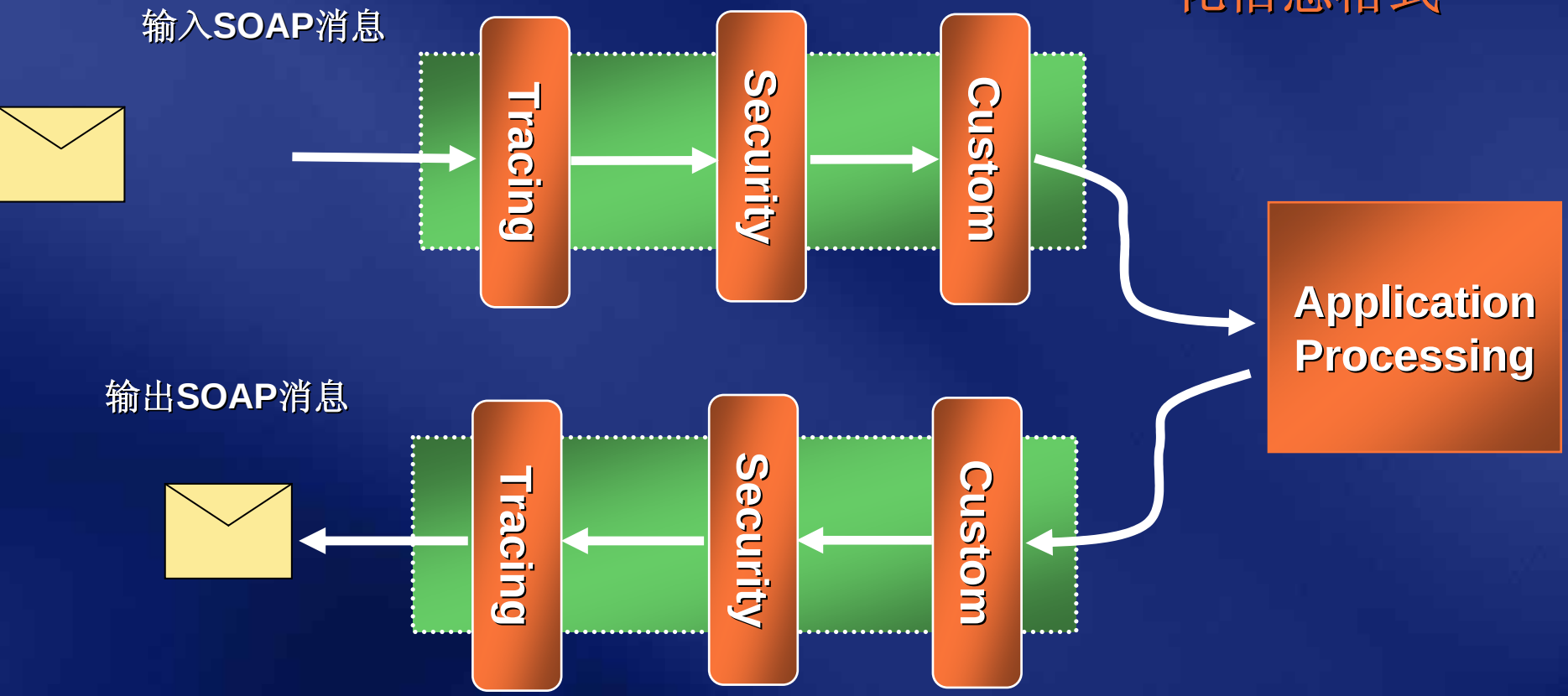
- 以一种策略断言(assertion)的方式，对传入和传出的信息的需求进行描述
  - 使得一部分安全问题，可以在部署时期进行考虑
- 策略文件很简单
  - 支持使用关守安全断言(Turnkey security assertions)的方式，在策略文件中描述安全需求
- 支持策略文件中的新的对象模型
  - 支持配置文件和代码两种方式(Declarative configuration or in code)

```
// Set the ClientPolicy onto the proxy
serviceProxy.SetPolicy("ClientPolicy");
```

策略文件工作体系架构

一个策略文件描述了一个输入管道

由策略文件转化信息格式



demo

使用策略文件和关守断言加密ASMX WEB服务

与Visual Studio 2005的集成性

- 集成在Visual Studio 2005 开发工具环境中
- 扩展了ASMX的编程模型
  - 支持使用TCP作为传输方式
  - 支持多种宿主环境－例如使用Console应用作为宿主
- 性能的提升
  - 支持更快的签名和XML的处理
- 支持的消息API
  - **SoapClient, SoapService**

扩展ASMX编程模型

Demo Code

```
public class StockService
        System.Web.Services.WebService
 {
        [WebMethod]
        public StockQuote[] StockQuoteRequest([string[]          symbols)
         { }
 }
static void Main(string[] args)
 {
        Uri to = new Uri( "soap.tcp://StockService/StockQuote");
        EndpointReference EPR = new EndpointReference(to);
        SoapReceivers.Add (EPR, typeof (StockService));
}
```

demo

通过TCP调用ASMX WEB服务

大量数据在消息级别的安全性问题(1)

- 消息传输优化机制(MTOM) —Message Transmission Optimization Mechanism
- 在WSE3.0中，MTOM 代替了 DIME & WS-Attachments
- 好处
  - 使用 WS-Security 规范，象保护SOAP信息一样来保护附件信息
  - 简单的编程模型
  - 有助于在传输级别减小消息的尺寸

大量数据在消息级别的安全性问题(2)

- 基于服务级别的MTOM的支持
  - 通过配置文件可以指定一个服务端点(Endpoint)如何支持 MTOM
  - *never*
  - *Always*
  - *optionally*
- 任何*byte[ ]类型的*、超过一定尺寸临界的数据，都将被序列化成为MTOM类型

```
[WebMethod]
    public byte[ ] GetFileAsBytes (string fileName)
    {
       return CreateFileAsBytesResponse (fileName);
    }
```

demo

使用 MTOM 发送大型数据

Secure Conversation Session

安全会话的管理

- 有状态的安全会话令牌(SCT)
  - 在WSE中，需要由服务来维护一个SCT的状态
    - 服务端和客户端，有 2n 个SCT
  - 在WSE 3.0中，状态信息可以被保留在 SCT 中
    - 典型应用1 — 支持使用 SCT 重建一个会话
    - 典型应用2 — 对Web farm的支持
- SCT 取消
  - 在 WSE 2.0 中的 SCT 是基于时间过期的机制
  - 在 WSE 3.0 提供了一种取消的机制

WSE 的兼容性

- WSE 2.0 在 .NET v2.0 还可以存在，但是…
  - 只是支持运行时(Runtime Time),没有设计时(Design Time)支持
  - 只支持32位
- WSE 3.0 是WSE 2.0的一个全面的替代品
- WSE的主要版本之间，有兼容性
- WSE 2.0 与 WSE 3.0 或者 Indigo 之间的互操作是不支持的
- WSE 3.0 与 Indigo之间的互操作是支持的

WSE 3.0 — 通向 Indigo之路

- WSE3与indigo Beta1之间，支持报文级别的互操作性
  - WSE 3.0 是一种投资保护
- 支持标准的互操作安全场景
  - 例如，WSE 关守应用断言 == Indigo 安全绑定元素
- WSE 3.0 可以与 Indigo 并行
- WSE 3.0 将会提供到 Indigo 的升级向导

discussion

Turnkey Security Assertions

- Scenarios based on industry best practices
- UsernameOverX509
  - Client authenticates with username/password
  - Confidentiality provided by server certificate
- AnnonymousOverX509
  - Client is not authenticated by the server
  - Confidentiality provided by server certificate
- UsernameOverTransport
  - Client authenticates with username/password

Turnkey Security Assertions

- Kerberos
  - Client and server authentication and confidentially provided by Windows Key Distribution Center (KDC)
- MutualX509
  - Client and server authenticate each other via certificates, which are used for confidentiality
  - Requires WS-Security 1.1 support
- X509MutualAuthenticationProfile
  - Client and server authenticate each other via certificates, which are used for confidentiality
  - WS-Security 1.0 compliant

Microsoft®

您的潜力，我们的动力