浙江大学 360 校园版定期安全简报（2015 年 2 月）

一、 360 虚拟服务器全网等级情况

目前，浙大使用了 2 台服务器为 360 天擎校园版的服务器，一台总控中心，一台分控中心。

1.1 服务器安全等级概况：

1) 10.203.2.93

2) 10.203.2.92

截止至 2015 年 3 月 1 日 9 点止，10.203.2.92 为 360 的总控中心，只负责分发漏洞补丁

事宜，安装客户端 2 台，10.203.2.93 服务器安装客户端 202 台，卸载 62 台。

1.2 受感染用户前 10 名（总排行 2015 年）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名
1	violin-lcl	192.168.1.100	45	VPN
2	YeZhiguo	10.71.123.36	38	紫金港-医学院综合楼
3	PC2013101815TCN	10.75.0.128	28	紫金港农生环大楼
4	ZhenyiNi-PC	10.18.3.98	27	玉泉硅材料实验室 3
5	zju-HP	10.51.120.163	27	之江-主楼
6	PC-201410101953	10.189.111.121	18	紫金港-无线网
7	user-PC	10.75.40.30	17	紫金港农生环大楼
8	LENOVO-19B00A36	10.214.147.141	15	玉泉-计算机学院
9	PC	10.180.77.218	14	玉泉-无线网
10	sufangwang	10.12.105.79	13	玉泉求是村综合楼

1.3 受感染用户前 10 名（本月排行）

序号	计算机	IP 地址	病毒/恶意软件数	楼宇名	处理措施
1	violin-lcl	192.168.1.100	45	VPN	清除成功
2	zju-HP	10.51.120.163	10	之江-主楼	清除成功
3	GongJian	10.189.132.167	5	紫金港-无线网	清除成功
4	DELL-PC	10.71.163.112	4	紫金港-东 3 教学楼	清除成功
5	PC-201202141043	10.12.215.249	3	玉泉-产业部	清除成功
6	cao-PC	192.168.1.102	2	VPN	清除成功
7	Huang-PC	222.205.55.244	2	玉泉-31 舍	清除成功
8	Sym-PC	210.32.146.124	2	VPN	清除成功

9	YeZhiguo	10.71.123.36	2	紫金港-医学院综合楼	清除成功
10	dqc-ws	10.78.62.1	1	紫金港西四	清除成功

二、 安全简讯

2.1 11 月检测统计

360 天擎自 10 月初部署以来，随着每天的人数的增多，漏洞补丁、木马、系统危险项日益增多，本月所有统计如下表所示：

日期	终端总数	活跃终端	体检分数	漏洞	木马	插件	系统危险项	安全配置项
2015-02-28	197	57	65	69	1	2	12	7
2015-02-27	197	52	63	0	1	2	7	0
2015-02-26	199	46	58	0	1	3	8	0
2015-02-25	198	38	67	20	1	2	7	0
2015-02-24	199	31	60	0	0	1	6	7
2015-02-23	199	31	56	0	0	1	6	7
2015-02-22	200	30	66	0	1	1	11	7
2015-02-21	202	26	57	0	0	0	7	0
2015-02-20	202	30	57	9	1	0	14	0
2015-02-19	202	26	57	0	0	1	8	7
2015-02-18	203	26	63	0	2	1	9	7
2015-02-17	202	38	67	1	2	3	16	7
2015-02-16	201	42	59	0	2	2	13	0
2015-02-15	202	47	60	0	1	3	13	0
2015-02-14	202	40	57	0	1	2	14	7
2015-02-13	202	52	76	1	0	5	10	7
2015-02-12	201	61	66	14	3	5	10	7
2015-02-11	201	56	70	8	0	4	7	0
2015-02-10	202	57	71	1	1	4	10	0
2015-02-09	203	72	68	1	1	4	15	0

2015-02-08	204	58	65	1	0	4	18	0
2015-02-07	205	56	70	1	1	5	19	7
2015-02-06	205	72	60	1	2	4	20	0
2015-02-05	207	82	68	4	1	5	15	0
2015-02-04	208	108	77	1	7	6	23	6
2015-02-03	210	115	75	31	10	8	25	0
2015-02-02	210	119	78	1	9	8	26	0
2015-02-01	210	76	68	15	6	7	15	9

2.2 XP 加固日志数据

2014 年 4 月 8 日微软对 XP 系统停止服务以来，360 盾甲对 XP 的安全，防护，系统加固产生了至关重要的作用。

360 天擎校园版自 2015 年以来，2 月份累计修复 5874 条。

2.3 本月终端插件情况统计

本月来累计统计的插件情况如下：

插件名称	危险级别	终端数量	上报日期
带推广标记的网址导航图标	高	7	2015-02-03 13:01:08
百度地址栏搜索插件	高	5	2015-02-28 13:31:53
百度杀毒所附带的浏览器插件	高	4	2015-02-13 14:10:06
捆绑安装的小广告图标	高	3	2015-02-02 02:05:37

伪装的浏览器图标	高	2	2015-02-28 02:09:35
捆绑安装的网址导航图标	高	2	2015-02-03 09:55:31
腾讯应用宝附带功能组件	高	2	2015-02-26 09:59:00
恶意的篡改程序	高	1	2015-02-27 20:10:52
腾讯搜索插件	高	1	2015-02-04 16:03:13
Ask 工具条	高	1	2015-02-03 02:30:32
捆绑安装的购物类广告图标	高	1	2015-02-02 02:05:37

2.4 Microsoft 2015 年 2 月安全更新

安全公告编号:CNTA-2015-0004

2 月 10 日，微软发布了 2015 年 2 月份的月度例行安全公告，共含 9 项更新，修复了 Microsoft Windows、Internet Explorer、Office 和 Server 软件中存在的 56 个安全漏洞。

其中，3 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行远程代码，提升权限，绕过安全功能限制，获得敏感信息。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

下表所示为了微软本月安全公告详情（按严重性排序），更多情况请参阅微软的官方网站。

公告 ID	公告标题和摘要	最高严重等级和漏洞影响	重新启动要求	受影响的软件
MS15-009	**Internet Explorer 的安全更新 (3034682)** 此安全更新可解决 Internet Explorer 中一个公开披露的漏洞和四十个秘密报告的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看经特殊设计的网页时允许远程执行代码。成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。	严重 远程代码执行	需要重新启动	Microsoft Windows，Internet Explorer
MS15-010	**Windows 内核模式驱动程序中的漏洞可能允许远程执行代码 (3036220)** 此安全更新解决 Microsoft Windows 中一个公开披露的漏洞和五个秘密报告的漏洞。如果攻击者诱使用户打开特制文档或访问包含嵌入 TrueType 字体的不受信任的网站，则	严重 远程代码执行	需要重新启动	Microsoft Windows

	其中最为严重的漏洞可能允许远程执行代码。			
MS15-011	**组策略中的漏洞可能允许远程执行代码（3000483)** 此安全更新可解决 Microsoft Windows 中一个私下报告的漏洞。如果攻击者诱使用户将配置域的系统连接到受攻击者控制的网络，此漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。	严重 远程代码执行	需要重新启动	Microsoft Windows
MS15-012	**Microsoft Office 中的漏洞可能允许远程执行代码（3032328)** 此安全更新可修复 Microsoft Office 中的三个秘密报告的漏洞。如果用户打开经特殊设计的 Microsoft Office 文件，那么这些漏洞可能会允许远程代码执行。成功利用这些漏洞的攻击者可以获得与当前用户相同的用户权限。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。	重要 远程代码执行	可能要求重新启动	Microsoft Office
MS15-013	**Microsoft Office 中的漏洞可能允许安全功能规避（3033857)** 此安全更新可修复 Microsoft Office 中的一个公开披露的漏洞。如果用户打开经特殊设计的 Microsoft Office 文件，那么此漏洞可能会允许安全功能规避。该安全功能规避本身不允许执行任意代码。但是，攻击者可以将此安全功能规避漏洞与另一个漏洞（如远程代码执行漏洞）组合使用，从而运行任意代码。	重要 安全功能规避	可能要求重新启动	Microsoft Office
MS15-014	**组策略中的漏洞可能允许安全功能规避（3004361)** 此安全更新可解决 Microsoft Windows 中一个私下报告的漏洞。如果攻击者通过中间人攻击的方式导致目标系统上的组策略安全配置引擎策略文件已损坏或不可读，该漏洞可能允许安全功能规避。这将导致系统上的组策略设置恢复到他们默认的可能较不安全的状态。	重要 安全功能规避	需要重新启动	Microsoft Windows
MS15-015	**Microsoft Windows 云中的漏洞可能允许特权提升（3031432)** 此安全更新可解决 Microsoft Windows 中一个私下报告的漏洞。漏洞可能允许攻击者利用模拟级别安全检查的缺失，在进程创建过程中提升特权。成功利用此漏洞的经过身份验证的攻击者可能会获取管理员凭据，并可能使用	重要 特权提升	需要重新启动	Microsoft Windows

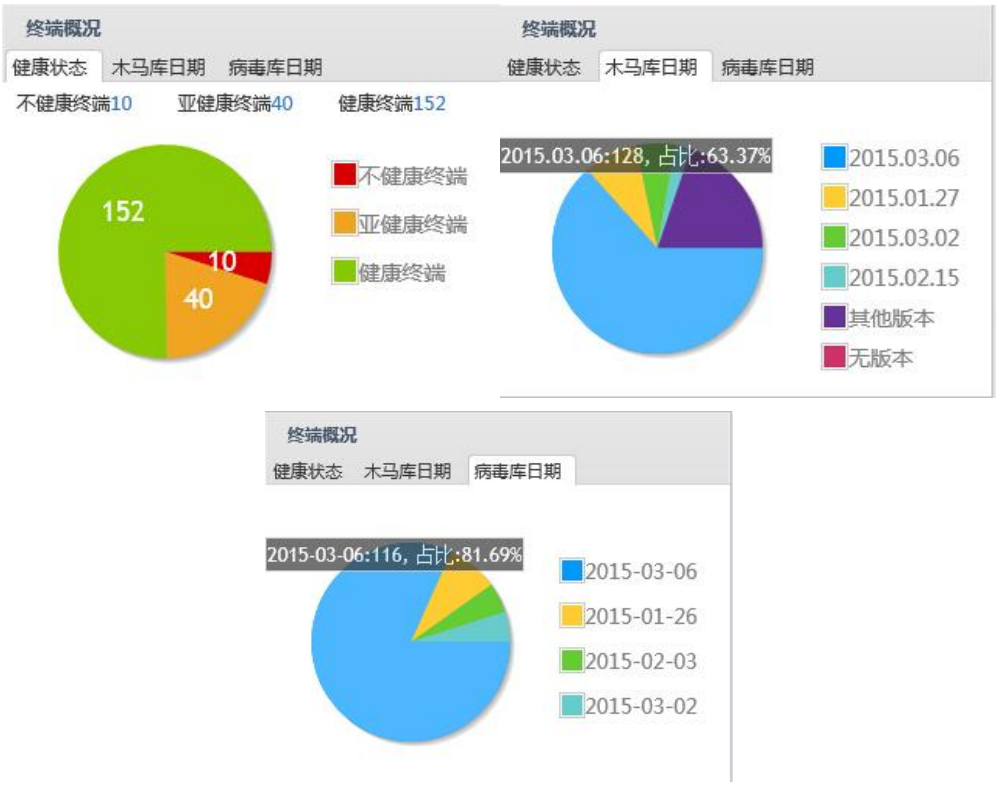
	它们来提升特权。攻击者随后可安装程序；查看、更改或删除数据；或者创建拥有完全管理权限的新帐户。			
MS15-016	**Microsoft Graphics 组件中的漏洞可能允许信息泄露（3029944）** 此安全更新可解决 Microsoft Windows 中一个私下报告的漏洞。如果用户浏览包含经特殊设计的 TIFF 图像的网站，该漏洞可能允许信息泄露。虽然攻击者无法利用此漏洞来执行代码或直接提升他们的用户权限，但此漏洞可用于获取信息，这些信息可用于试图进一步危及受影响系统的安全。	重要 信息泄露	可能要求重新启动	Microsoft Windows
MS15-017	**Virtual Machine Manager 中的漏洞可能允许特权提升（3035898）** 此安全更新可解决 Virtual Machine Manager (VMM) 中一个秘密报告的漏洞。如果攻击者登录受影响的系统，该漏洞可能允许特权提升。攻击者必须拥有有效的 Active Directory 登录凭据，并能够使用那些凭据登录以利用此漏洞。	重要 特权提升	需要重新启动	Microsoft Server 软件

2.5 截止至本月月底的全网安全状况如下：

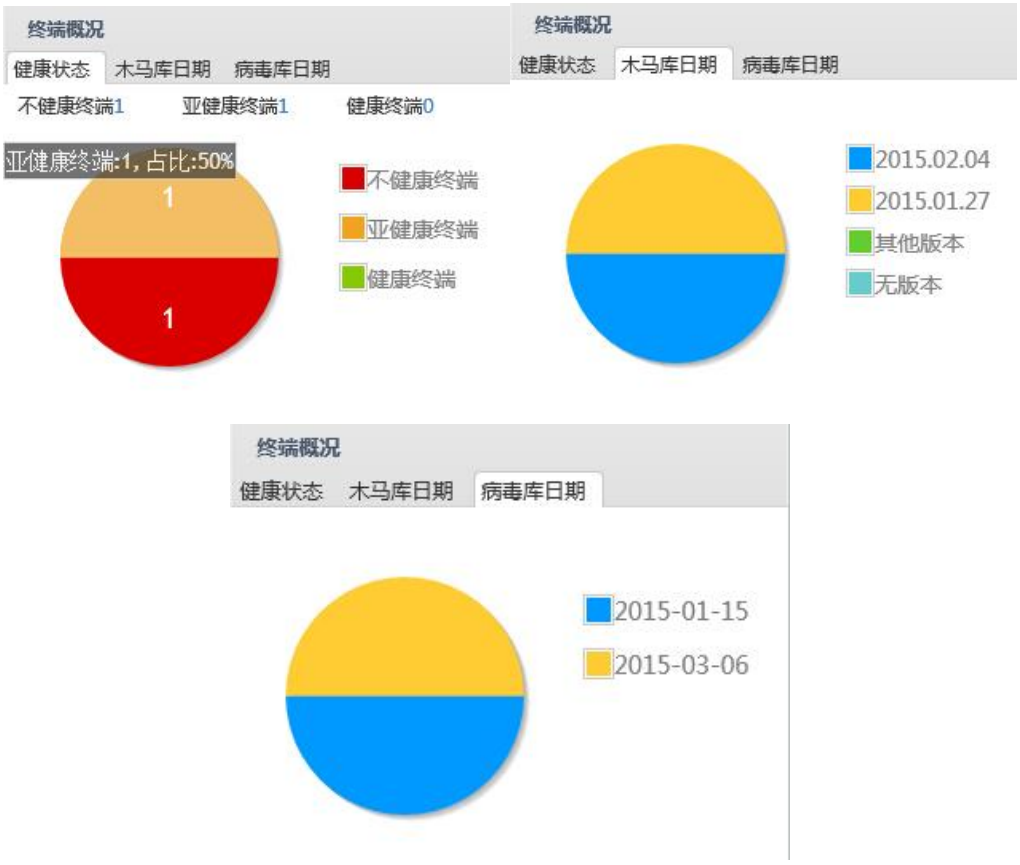
10.203.2.93　　10.203.2.92

2．6 终端概况如下

1）10.203.2.93


终端概况
健康状态
木马库日期
病毒库日期
不健康终端10
亚健康终端40
健康终端152
152
10
40
不健康终端
亚健康终端
健康终端
终端概况
健康状态
木马库日期
病毒库日期
2015.03.06:128, 占比:63.37%
2015.03.06
2015.01.27
2015.03.02
2015.02.15
其他版本
无版本
终端概况
健康状态
木马库日期
病毒库日期
2015-03-06:116, 占比:81.69%
2015-03-06
2015-01-26
2015-02-03
2015-03-02

2）10.203.2.92


终端概况
健康状态
木马库日期
病毒库日期
不健康终端1
亚健康终端1
健康终端0
亚健康终端:1, 占比:50%
1
1
不健康终端
亚健康终端
健康终端
终端概况
健康状态
木马库日期
病毒库日期
2015.02.04
2015.01.27
其他版本
无版本
终端概况
健康状态
木马库日期
病毒库日期
2015-01-15
2015-03-06

三、 2015 年 2 月编程语言排行榜 TIOBE

希望以下数据能对正在学习或者将要学习一些编程语言的同学带来一些帮助。

在 2014 年最后一个月赢得年度语言奖之后，JavaScript 不断走强。本月它超过了 php，现在的位置排名第六。另外，Objective-C 的日子似乎已经结束。一年时间，Objective-C 份额下降超过 5%。现在排到第四的位置，在 C++之后。Objective-C 之前排在第三位的位置长达超过 2.5 年。

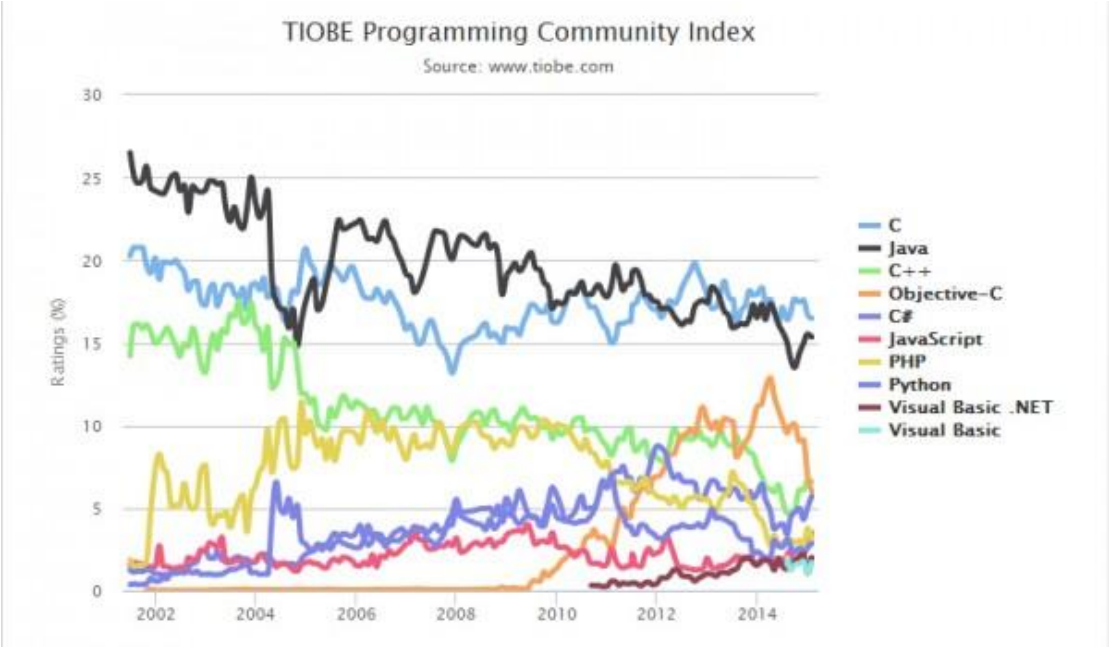
TIOBE 编程语言社区排行榜是编程语言流行趋势的一个指标，每月更新，这份排行榜排名基于互联网上有经验的程序员、 课程和第三方厂商的数量。排名使用著名的搜索引擎(诸如 Google、MSN、Yahoo!、Wikipedia、YouTube 以及 Baidu 等)进行计算。

该指数可以用来检查你的编程技能是否仍然是最新的或作出什么开始建立一个新的软件系统时，编程语言应采取的战略决策。在 TIOBE 指数的定义可以在这里找到。

编程语言排行榜 TOP 20 榜单：

Feb 2015	Feb 2014	Change	Programming Language	Ratings	Change
1	1		C	16.488%	-1.85%
2	2		Java	15.345%	-1.97%
3	4	↑	C++	6.612%	-0.28%
4	3	↓	Objective-C	6.024%	-5.32%
5	5		C#	5.738%	-0.71%
6	9	↑	JavaScript	3.514%	+1.58%
7	6	↓	PHP	3.170%	-1.05%
8	8		Python	2.882%	+0.72%
9	10	↑	Visual Basic .NET	2.026%	+0.23%
10	-	⇈	Visual Basic	1.718%	+1.72%
11	20	⇈	Delphi/Object Pascal	1.574%	+1.05%
12	13	↑	Perl	1.390%	+0.50%
13	15	↑	PL/SQL	1.263%	+0.66%
14	16	↑	F#	1.179%	+0.59%
15	11	⇊	Transact-SQL	1.124%	-0.54%
16	30	⇈	ABAP	1.048%	+0.69%
17	14	↓	MATLAB	1.033%	+0.39%
18	44	⇈	R	0.963%	+0.71%
19	17	↓	Pascal	0.960%	+0.41%
20	12	⇊	Ruby	0.873%	-0.05%

前 10 名编程语言长期走势图：



以下是 21-50 编程语言排名：

Position	Programming Language	Ratings
21	ML	0.861%
22	COBOL	0.858%
23	SAS	0.832%
24	PostScript	0.801%
25	Logo	0.796%
26	Assembly	0.751%
27	Swift	0.723%
28	OpenEdge ABL	0.704%
29	ActionScript	0.692%
30	D	0.619%
31	Fortran	0.543%
32	Lisp	0.519%
33	Groovy	0.502%
34	RPG (OS/400)	0.469%
35	Ada	0.445%
36	Awk	0.433%
37	Scratch	0.411%
38	Scheme	0.391%
39	Max/MSP	0.363%
40	Lua	0.353%
41	Scala	0.318%
42	Prolog	0.317%
43	Go	0.302%
44	Inform	0.300%
45	PL/I	0.293%
46	Haskell	0.266%
47	LabVIEW	0.250%
48	(Visual) FoxPro	0.250%
49	C shell	0.249%
50	VBScript	0.233%

后 50 名编程语言如下：

下面的列表表示#51 至#100。由于差异比较小，编程语言只列出(排名不分先后)。

4th Dimension/4D, ABC, Alice, Apex, Arc, Bash, bc, Bourne shell, cg, CL (OS/400), Clean, Clojure, Dart, DiBOL, Erlang, EXEC, Factor, Forth, Icon, IDL, Io, Ioke, J, J#, JADE, JScript, Korn shell, Ladder Logic, M4, Magic, Mathematica, Moto, NATURAL, NXT-G, OpenCL, Oz, PILOT, Programming Without Coding Technology, Pure Data, Q, S, SPARK, SPSS, SQR, Standard ML, Stata, Tcl, TOM, VHDL, Z shell

本月变动的指数

This month the following changes have been made to the definition of the index:

Iskander Sabaev suggested to add MQL5 to the MQL4 entry. This has been done.

Due to a bug in the January edition of the TIOBE index, some programming languages such as Visual FoxPro and COBOL had a higher rating than usual. This has been fixed.

There are lots of mails that still need to be processed. As soon as there is more time available your mail will be answered. Please be patient.

Programming Language Hall of Fame

The hall of fame listing all "Programming Language of the Year" award winners is shown below. The award is given to the programming language that has the highest rise in ratings in a year.

Year	Winner
2014	JavaScript
2013	Transact-SQL
2012	Objective-C
2011	Objective-C
2010	Python
2009	Go
2008	C
2007	Python
2006	Ruby
2005	Java
2004	PHP
2003	C++

必须声明，这个榜单本身采集的是英文世界的数据，虽然在反映趋势上有一些参考意义，但与中国的实际情况不完全符合，而且，这张采样本身也有相当大的局限性。

【说明】

TIOBE 编程语言社区排行榜是编程语言流行趋势的一个指标，每月更新，这份排行榜排名基于互联网上有经验的程序员、课程和第三方厂商的数量。排名使用著名的搜索引擎(诸如 Google、MSN、Yahoo!、Wikipedia、YouTube 以及 Baidu 等)进行计算。请注意这个排行榜只是反映某个编程语言的热门程度，并不能说明一门编程语言好不好，或者一门语言所编写的代码数量多少。

这个排行榜可以用来考查你的编程技能是否与时俱进，也可以在开发新系统时作为一个语言选择依据。

四、 技术交流

欢迎老师和同学们前来交流问题，多提建议，希望下期简报内容更加接近大家的需求。

咨询服务电话：87951669
邮箱: netsafe@zju.edu.cn

工程师联系方式：
13588277982 章荣伟