

Technical Advantages

Introduction

- Shanghai PHILO-TECH has leading technology for cross-platform and efficient software development. Over the years, we have completed a number of self-owned products with independent intellectual property rights, such as [BaiY Application Platform](#), [BlueWhale Telecom Billing System](#), [WhiteDolphin ERP platform](#), [BYCDN](#) and [BYST](#). At the same time, we also undertook and participated in the construction of many major projects such as [Taobao cloud computing platform \(the predecessor of Alibaba Cloud\)](#), [Shanghai subway reconstruction project](#), [SIP softswitch system](#), [ZhiYeJing.com talent platform](#), and [intelligent IoT warehousing](#).



Product Architecture

BMOD

...

WD ERP

BW Telecom 4A

Taobao Cloud

...

BaiY Application Platform (BAP)

BaiY Application Platform - 1



- See details:
http://baiy.cn/doc/asp_whitepaper_en.pdf

- BaiY Application Platform contains millions of lines of assembly, C / C + + code and **thousands of mature general-purpose components**. It has been tested in the real production environment of numerous Fortune 500 companies. It has been used in multiple high-load telecommunications, Internet and distributed computing environments for more than a decade.
- Supports most mainstream operating systems such as Windows, Linux, BSD, IBM AIX, HP-UX, Solaris, MAC OS X, vxWorks, QNX, DOS, WinCE (Windows Mobile), NanoGUI, eCos, RTEMS, Android, iOS, etc.
- Support mainstream hardware platforms such as x86/x64, ARM, IA64, MIPS, POWER, SPARC and so on.

BaiY Application Platform - 2

We have strong and consistent multi-active IDC high-availability, high-reliability and high-performance distributed cluster components protected by a number of national and international invention patents, core technologies such as distributed file systems that support real-time strong encryption and data compression. It can provide high availability, reliability and security guarantees for key services beyond Alipay, Google GCE, WeChat and other services.

Products based on the BaiY Application Platform can use the distributed database platform and data query and analysis engine independently developed by us to perform data storage and management. Its strongly consistent 6-copy technology across multiple IDC ensures extremely high data reliability.

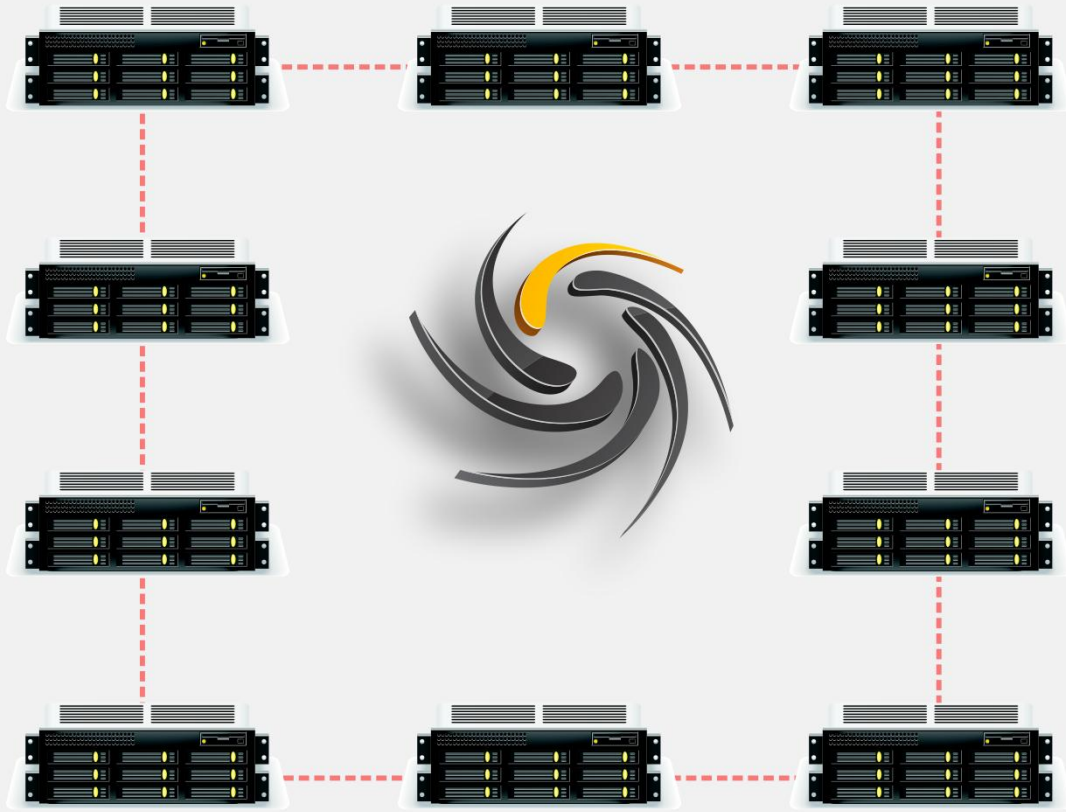
BaiY Application Platform - 3

The Application Platform uses assembly and asynchronous IO to optimize the network service components. These components enable **high performance network services** through the memory zero-copy and asynchronous IO mechanisms via DMA + hardware interrupts.

On an entry-level 1U PC Server (with dual-socket Intel Xeon 56xx) manufactured in 2011 (at that time, the price of the machine was less than 20,000 CNY or 2850 USD), **a single node can permit tens of millions of TCP / HTTP concurrent connections**. Correspondingly, with the same machine, a general server development by Java or .NET can only support up to 3000 to 5000 concurrent connections, PHP is even lower.

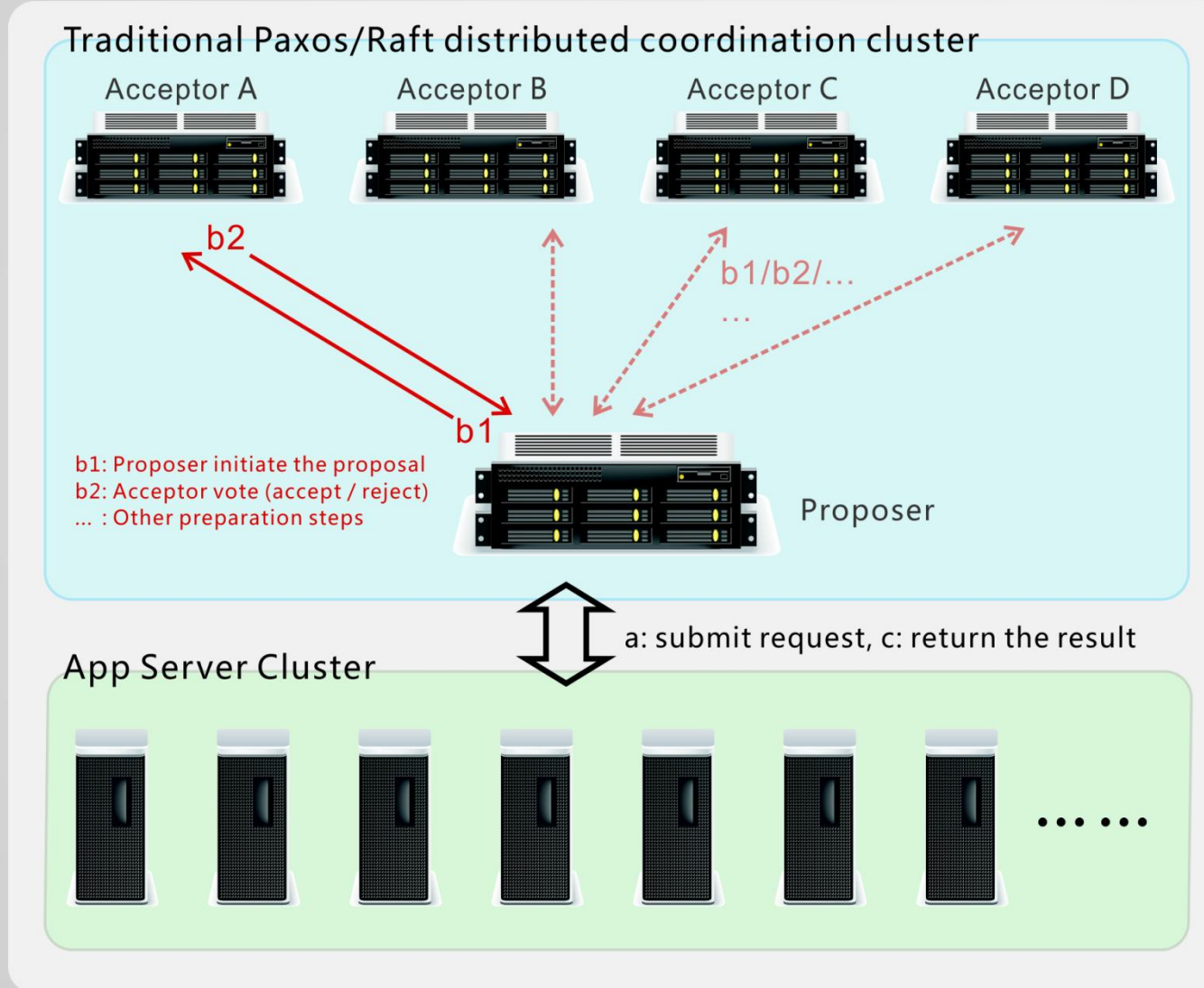
Thanks to the **extremely high single-point performance** and the **distributed high-performance cluster architecture** that can be scaled out on a large scale, the capacity of the product built based on the BaiY Application Platform has virtually no upper limit.

BaiY Application Platform - 4



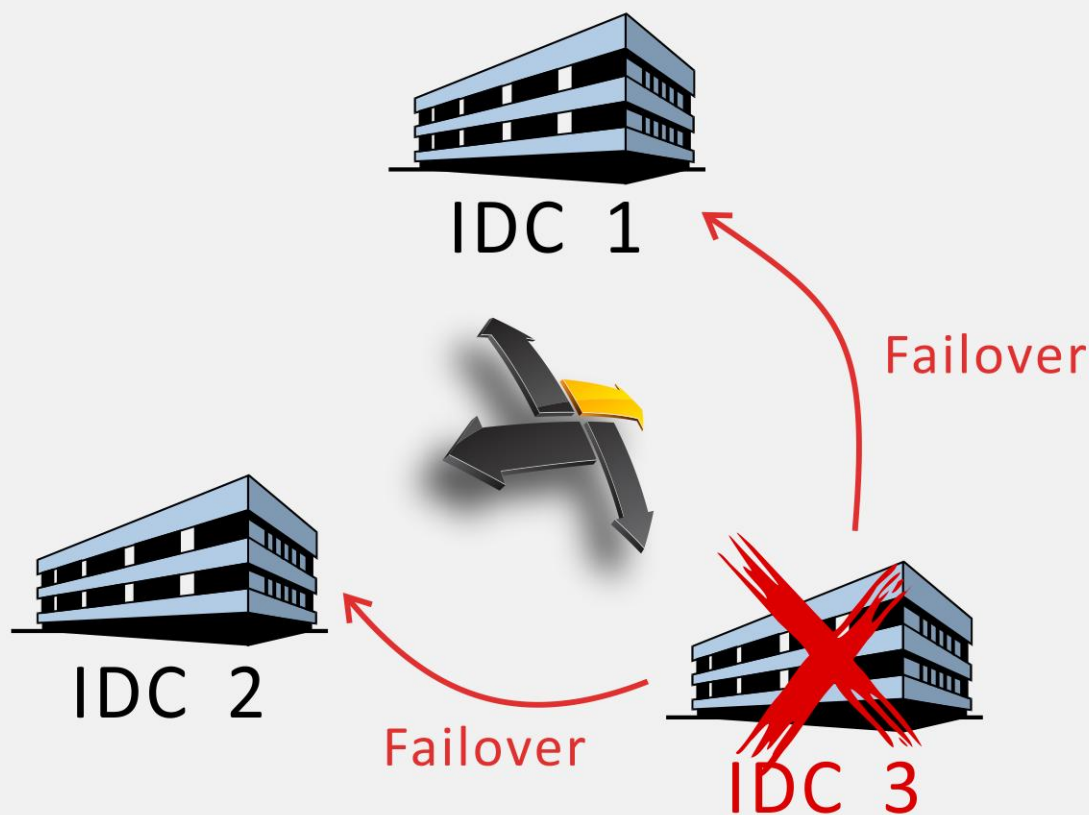
- Distributed coordination services provide functions such as **service discovery**, **service election**, **fault detection**, **failover**, **failback**, **distributed lock**, **task scheduling**, **message routing** and **message dispatching**.
- The distributed coordination service is the **brain of a distributed cluster** that is responsible for coordinating all the server nodes in the cluster. Make distributed clusters into an organic whole that works effectively and consistently, making it a linear scalable high performance (HPC) and high availability (HAC) distributed clustering system.

BaiY Application Platform - 5



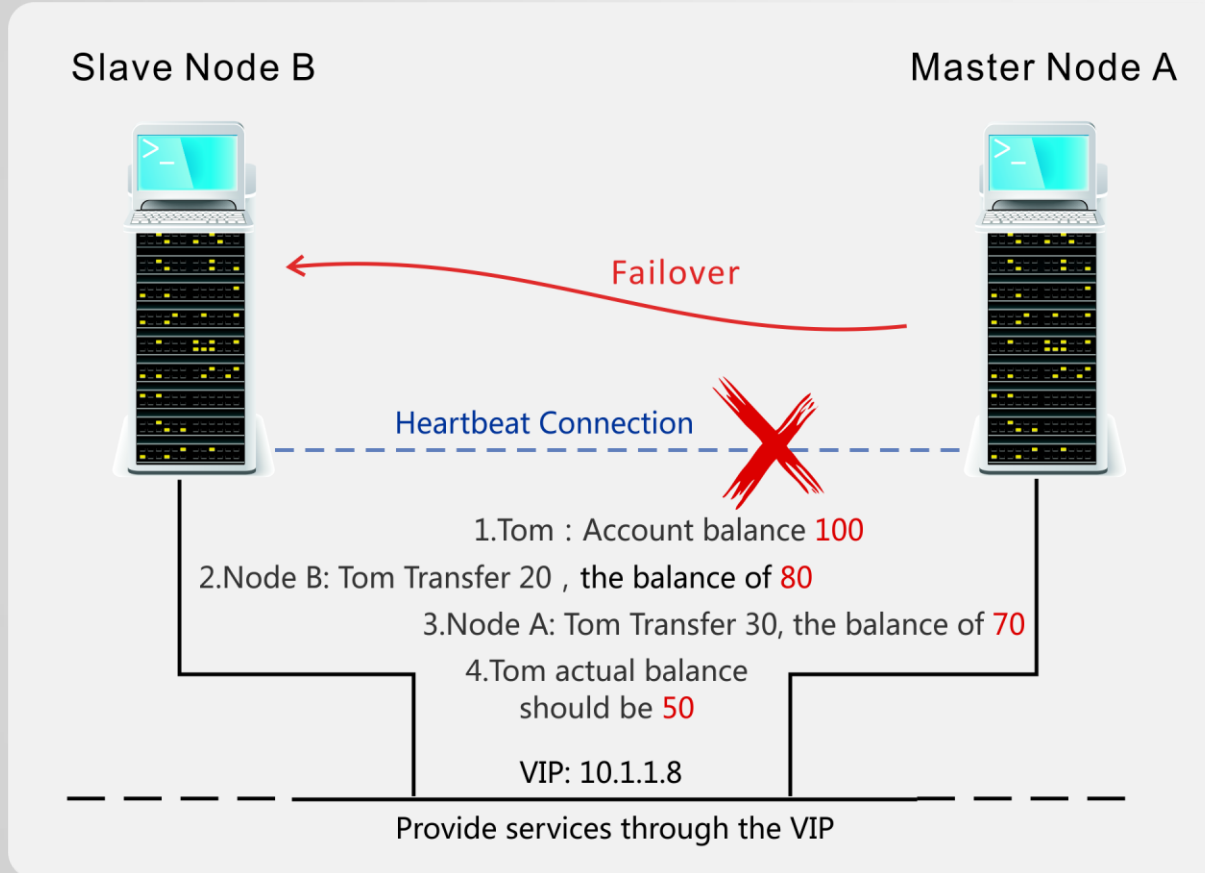
- The traditional Paxos / Raft distributed coordination algorithm **initiates voting for each request, generating at least 2 to 4 broadcasts (b1, b2...) and multiple disk IO**. Making it highly demanding on network throughput and communication latency, and cannot be deployed across multiple data centers.
- Our **patent algorithm completely eliminated these overheads**. Thus greatly reducing the network load, significantly improve the overall efficiency. And makes it easy to deploy clusters **across multiple data centers**.

BaiY Application Platform - 6



- Based on our unique distributed coordination technology, the high performance, strong consistency cluster **across multiple data centers** can be implemented easily.
- Fault detection and failover can be done **in milliseconds**. The system is still available even if the entire data center is offline.
- We also providing a **strong consistency** guarantee: even if there is a network partition, it will not appear split brain and other data inconsistencies.

BaiY Application Platform - 7



- In the traditional dual fault tolerance scheme, the slave node automatically promotes itself as the master node after losing the heartbeat signal and continues to provide services to achieve high availability.
- In this case, **split brain** problem occurs when both the master and slave nodes are normal, but the heartbeat connection is accidentally disconnected (network partition).
- At this time, node A and B both think that the other party is offline. As a result, both nodes upgrade themselves to the master node and provide the same service, respectively. This will **result in inconsistent data that is difficult to recover**.

BaiY Application Platform - 8

Our BYPSS service provides the same level of consistency as the traditional Paxos / Raft distributed algorithm **on the cross-IDC scale, fundamentally eliminates the occurrence of inconsistencies such as split brain.**

Similarly: ICBC, Alipay and other services are also have its own **remote disaster recovery** solutions (Alipay: Hangzhou → Shenzhen, ICBC: Shanghai → Beijing). However, in their remote disaster recovery schemes, there is no paxos and other distributed coordination algorithms between the two data centers, so **strong consistency cannot be achieved.**

For example, a transfer transaction that has been successfully completed at Alipay may take **several minutes or even hours** to be synchronized from the Hangzhou main IDC to the disaster recovery center in Shenzhen. When the Hangzhou main data center offline, **all of these non-synchronized transactions are lost** if they switch to the disaster recovery center, leads a large number of inconsistencies. Therefore, ICBC, Alipay and other institutions **would rather stop the service for hours or even longer, and would not be willing to switch to the disaster recovery center in the major accidents of the main IDC.** Operators will consider turning their business into a disaster recovery center only after a devastating accident such as a fire in the main data center.

Therefore, the remote disaster recovery schemes and **our strong consistency, high availability, anti-split brain multi-IDC solution** is essentially different.

BaiY Application Platform - 9

Due to the elimination of a large number of broadcast and distributed disk IO and other high-cost operation brought by the Paxos / Raft algorithm. Making BYPSS distributed coordination component also provides more excellent features in addition to the above advantages:

- **Bulk operation:** Allows each network packet to contain a large number of distributed coordination requests at the same time. **Network utilization greatly improved**, from the previous less than 5% to more than 99%. Similar to the difference between a flight only can transport one passenger each time, and another one can transport full of passengers. In the actual test, in a single Gigabit network card, BYPSS can achieve **4 million requests per second** performance. In the dual-port 10 Gigabit network card (currently the mainstream data center configuration), the throughput of **80 million requests per second** can be reached. There is a huge improvement compared to the Paxos / Raft cluster which performance is usually **less than 200 requests per second** (restricted by its large number of disk IO and network broadcast).
- **Large capacity:** usually **every 10GB of memory can support at least 100 million ports**. In a 1U-size entry-level PC Server with 64 DIMM slots (8TB), it can support at least **80 billion objects** at the same time. In a 32U large PC server (96TB), it can support about **1 trillion distributed coordinating objects**. In contrast, traditional Paxos / Raft algorithms can only effectively manage and schedule **hundreds of thousands of objects** due to their limitations.

BaiY Application Platform - 10

In addition, Paxos / Raft cannot guarantee the strong consistency of data during the process of simultaneous failure and recovery of more than half of the nodes, and **may cause inconsistencies such as phantom reading**.

For example, in a three-node cluster, node A goes offline due to power failure, and after one hour, nodes B and C go offline because of disk failure. At this point, node A resumes power supply and goes online again, and then the administrator replaces the disks of nodes B and C and restores them to go online. At this point, the data modification of the entire cluster in the last hour will be lost, and the cluster will fall back to the state before the A node goes offline at 1 hour ago.

BYPSS fundamentally avoids such problems, so BYPSS has a stronger consistency guarantee than Paxos / Raft.

BaiY Application Platform - 11

Efficient high-strength cryptographic components: includes basic functions such as public-key algorithms, symmetric encryption algorithms, data encoding and decoding, hash and message authentication algorithms, data compression algorithms, and etc.

In addition, the application platform also provides a number of highly abstract advanced components, such as:

The **Virtual File System (VFS) supports data encryption and compression on-the-fly**. VFS supports dozens of strong encryption algorithms, including AES (128/256), SM4, TwoFish, etc., optimized using AES-NI, SSE4 and other assembly instruction set, with high efficiency. We use this component to provide on-the-fly data compression and strong encryption protection for the whole database and configuration categories in our products like BlueWhale, WhiteDolphin, ZhiYeJing.com and so on. It also includes strong cryptographic communication protection components based on Public Key Infrastructure (PKI) and etc.

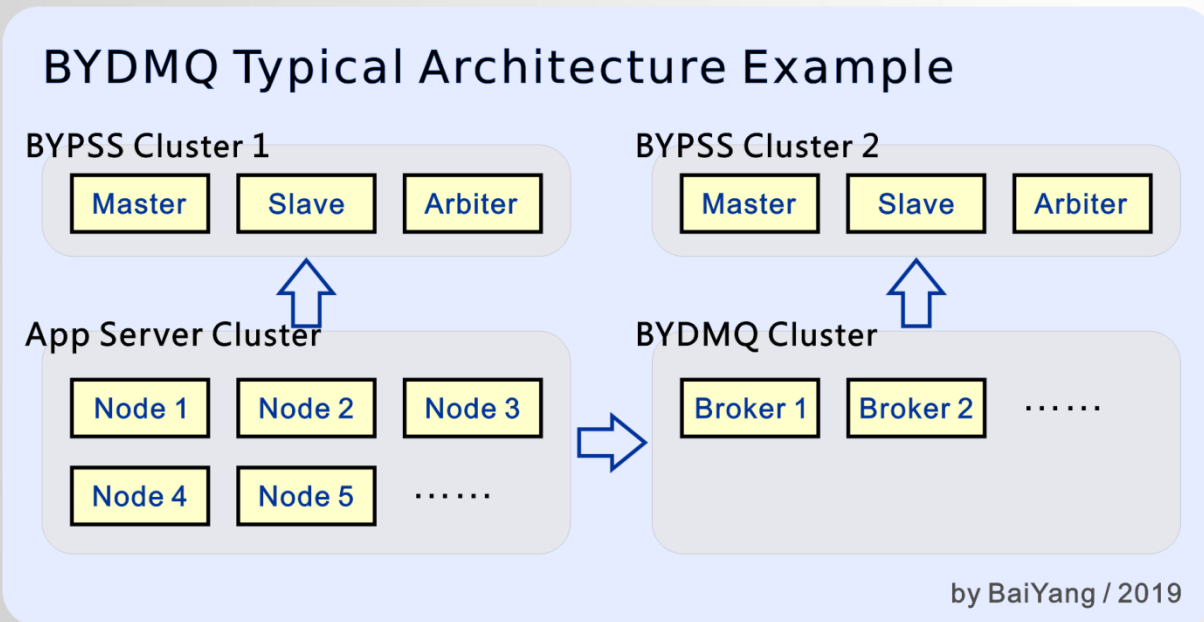
BaiY Application Platform - 12

The application platform also includes a [Query Engine](#). Its ability is better than SQL language. Having own query engine gives us the flexibility to switch between RDBMSs such as MySQL, MS SQL Server, Oracle, DB2, SQLite, and NoSQL databases like MongoDB and Cassandra. In addition to making applications database-independent, the query engine also provides a variety of advanced characteristics that are not supported by SQL language, such as ARE (Advanced Regular Expressions) query with support for Unicode charset, join query with support for nested tables, mix query of business data and configuration data, virtual field query, and other customized queries.

The query engine was implemented using C/C++, and its hotspot codes were optimized using assembly language for mainstream hardware platforms. [13 million times of evaluation of expressions per second](#) can be achieved on a ThinkPad W510 notebook (having 4 cores and 8 threads @1.6GHz) produced in 2010, using a single core and a single thread only.

BaiY Application Platform - 13

The [BaiY Distributed Message Queuing Service \(BYDMQ\)](#) is a distributed message queue service with strong consistency, high availability, high throughput, low latency and linear scale-out. It can support [a single point](#) of tens of millions of concurrent connections and [a single point](#) of tens of millions of message forwarding performance per second, and [supports linear horizontal scaling out of the cluster](#).



BYDMQ focuses on high-throughput, low-latency delivery of large amounts of business messages. Through the use of [mature and efficient network IO components](#), as well as [automatic message packing](#), [pipelining](#) and other mechanisms, it significantly reduces command processing delay, improves network throughput, and effectively increases network utilization rate. At the same time, it also supports advanced functions such as specifying [TTL](#), [maximum number of retries](#) and [automatic dispersed delivery](#) at single message level.

BaiY Application Platform - 14

The **BYST** component provides users with an end-to-end secure tunnel service. BYST supports dozens of strong encryption and data verification algorithms, which can provide users with **safe, reliable and consistent data communication tunnel services**.

At the same time, thanks to our mature high-performance network IO components, batch message packing and unpacking mechanism, patented distributed N:M:N dynamic connection pool mapping, real-time data compression and other algorithms, BYST has significantly improved the network Utilization (high load ratio) and network throughput. In typical daily office scenarios (email, OA, file services, online meetings), BYST **can save users up to 50% of network traffic**, significantly reducing the cost of renting expensive dedicated line networks.



Different from all existing VPN solutions, thanks to the impact of the above strong encryption, batch IO packaging and unpacking, connection pool random remapping and data compression algorithms, **BYST can be completely featureless** (There are no clear text fields that can be analyzed, nor any flow characteristics). So there is no need to worry about being accidentally injured by the firewall.

At the same time, BYST is **transparently compatible with various existing solutions such as OpenVPN, CISCO VPN, v2ray, ss, etc.** There is no need to replace and redeploy existing solutions.

BaiY Application Platform - 15

BYCDN can save 95% of the traffic cost and avoid lag. No App or hardware box is needed, No need to change the original architecture such as the application and CDN, just add a line of code to the page.

Relying on the above BYPSS components, BYCDN tailored a set of patented distributed, ultra-fine-grained real-time tracking, matching, and scheduling algorithms for the p2p CDN environment. The algorithm can simultaneously manage the massive online resources in a very fine granularity (data chunk level) at the same time in a very large-scale concurrent user scenario with real-time tracking, matching, analysis statistics and scheduling. It can greatly improve the real-time performance and success rate of p2p sharing, and significantly enhance the adaptability of the overall p2pcdn system to changes in unpredictable p2p network nodes and cache status.

Cooperate with our self-developed "Region/Country -> ISP -> State/City" three-level and five-layer peer matching algorithm, network QoS adaptation, and strong data encryption. BYCDN can provide secure and powerful data distribution capabilities for various services such as audio and video live broadcast and on-demand, file sharing, and online office. At the same time, it saves 95% of traffic and costs, and avoids the problem of lag (the more concurrent users, the smoother it is).

BaiY Application Platform - 16

We do not rely on "trade secrets" to protect our core competitiveness. Instead, we use more open and transparent trademarks, certifications, copyrights, patents and notarization to protect our legal rights. Therefore, all of our technical details are disclosed in the corresponding documents. For details, please refer to the “BaiY Application Platform Whitepaper”:

http://baiy.cn/doc/asp_whitepaper_en.pdf

And other documents, including Hacker News (the world's largest computer science news website), Google Blogger, CSDN, and cnblogs, many domestic and foreign media have reproduced or reported these papers. Compared with "strictly keeping secrets", we believe that a large number of peer reviews under openness and transparency, combined with the harsh tests in the actual production environment, are more conducive to the improvement of product quality.

BaiY Application Platform - 17

证书号第 4249374 号

证书号第 2776194 号

(12) United States Patent
Bai

(10) P
(45) E

(54) PORT SWITCH SERVICE SYSTEM

(56)

证书号第 3400663 号

发明专利

發明專利

發明名稱: 消息端口交换服务系统

發明人: 白楊

專利號: ZL 2016 1 0323880.5

專利申請日: 2016 年 05 月 16 日

專利權人: 白楊

地址: 200092 上海市楊浦區控江路 2202 號

授權公告日: 2019 年 06 月 04 日

國家知識產權局依照中華人民共和國專利法進行公告並在專利登記簿上予以登記。專利權自授權公告之日起算。

專利證書記載專利權登記時的法律狀況。專利權利權人的姓名或名稱、國籍、地址變更等事項記載在

局長
申長雨

第 1 頁 (共 2 頁)

發明專利之延伸註冊證
Título de Extensão de Patente de Invenção
澳門特別行政區政府
Governo da Região Administrativa Especial de Macau
經濟局
Direcção dos Serviços de Economia

編號 N.º: J/003824
頁 Págs: 1 / 2
FOLH

延伸申請日期 Data do pedido de extensão: 2019/09/04
延伸批給日期 Data da concessão de extensão: 2019/10/23
專利權人 Titular: 白楊

US101700948B2

(12) United States Patent
Bai

(10) Patent No.: US 10,700,948 B2
(45) Date of Patent: Jun. 30, 2020

(54) SERVICE-ORIENTED MODULAR SYSTEM ARCHITECTURE

(58) Field of Classification Search
CPC H04L 41/5048; H04L 41/5051; H04L 41/5054; H04L 9/32; G06F 9/18; G06F 9/44; G06F 9/44526

(71) Applicant: Yang Bai, Shanghai (CN)

See application file for complete search history.

REPUBLIC OF SINGAPORE
THE PATENT ACT (CHAPTER 221)
CERTIFICATE ISSUED UNDER SECTION 35

I HEREBY CERTIFY that under the provisions of the Patent Act, a patent has been granted in respect of an invention having the following particulars:

TITLE : PORT SWITCH SERVICE

APPLICATION NUMBER/ PATENT NUMBER : 11201808659V

DATE OF FILING : 8 AUGUST 2016

PRIORITY DATA : 16 MAY 2016 - PATENT APPLICATION NO. 201610323880.5 (CHINA)

NAME OF INVENTOR(S) : BAI, YANG

NAME(S) AND ADDRESS(ES) OF PROPRIETOR(S) OF PATENT : BAI, YANG

DATE OF GRANT : 19 July 2021

DATED THIS 19th DAY OF JULY 2021

知識產權署專利註冊處
Patents Registry
Intellectual Property Department

香港特別行政區政府
The Government of the Hong Kong
Special Administrative Region

批予轉錄標準專利證明書
《專利條例》(第 514 章)
CERTIFICATE OF GRANT OF STANDARD PATENT
BY RE-REGISTRATION
Patents Ordinance (Chapter 514)

茲證明下述轉錄標準專利根據《專利條例》第 2 部在今日批予:
I hereby certify that a standard patent by re-registration with the following particulars has been granted under Part 2 of the Patents Ordinance today:

專利編號 Patent No.: HK1259712 申請編號 Application No.: 19119473.7

專利所有人姓名或名稱及地址 Name and Address of Proprietor:
Bai, Yang

發明專利證書

發明名稱: 基于 N:M 连接动态映射的网络连接加速转发方法

512 B
期限, 颁发发明专利
期限为二十年, 自
终止、恢复和专

WO 2016/169529
PCT/CN2016/093880
EAU
ECTUAL PROPERTY
teping District
OTICE
y 2016 (16.05.2016)
s made to INID codes

Safety and Reliability

- Products based on BaiY application platform can pass multiple technologies, such as strong consistent online replication (distributed file system), multi-version control system, disk snapshots, automatic backup and automatic recovery, strong data encryption, CHAP authentication, BYST end-to-end authentication secure transmission, TLS (HTTPS) security Transmission, and high-availability cluster (HAC) to ensure the security, reliability, stability and robustness of the service from various aspects such as data storage, network transmission, and node fault tolerance.

Safety and Reliability - Data Reliability

- [The cross-IDC strong consistency distributed 6 replica technology](#) On the premise of ensuring strong consistency, the reliability of all user data is as high as 99.999999999999999% (17 “9”s). No data will be lost even if the entire IDC is completely destroyed catastrophically.
- It can automatically complete snapshot backups every day and keep disk snapshots within a specified time range. [Snapshot data can be based on reliable multiple copy technology or multiple EC algorithms](#), which can effectively recover data loss caused by user misoperation or malicious operation. Backup snapshots can be stored alternately in different IDCs to further improve their reliability. With [unlimited version control technology](#), it can easily audit and restore the historical state of the system.
- Data can be centrally stored in a [virtual file system \(VFS\)](#) independently developed by us with on-the-fly compression and strong encryption protection. Every time there is a change, the data can be [backed up automatically](#). Before each data access, an integrity check will be performed, and if an error occurs, it will be [automatically restored](#).

Safety and Reliability - Service Availability

- Based on our [strong consistent and split-brain resistant multi-active IDC high-availability cluster \(HAC\) patent architecture](#), the overall service availability can reach 99.9999% (6 “9” s). Ensure that even if the entire IDC goes offline due to municipal construction, natural disasters, human error, etc., it can complete the failover in seconds and automatically switch to other available IDCs to provide uninterrupted services.
- The strong consistency guarantee provided by the well-designed distributed coordination and data synchronization algorithms such as fault detection, service discovery, service election, distributed locks, and message routing ensures that [cross-IDC failover will not cause data consistency problems](#).

Note: Our high-availability (HAC) and high-performance (HPC) distributed architecture and algorithms are protected by a number of national and international invention patents.

Safety and Reliability - Reliability Supplement

- Multi-active IDC technology with strong consistency guarantee is the key technology of modern high-performance and high-availability clusters, and it is also a major difficulty recognized in the industry. As examples: September 4, 2018, the cooling system failure of a **Microsoft** data center in South Central US caused Office, Active Directory, Visual Studio and other services to be offline for nearly 14 hours; August 20, 2015 **Google** GCE service interrupted for 12 hours and permanently lost part of data; May 27, 2015, July 22, 2016 and Dec 5, 2019 **Alipay** interrupted for several hours; As well as the July 22, 2013 and Mar 29, 2023 **WeChat** service interruption for several hours, and etc. These major accidents are due to product not implement the multiple active IDC architecture correctly, so a single IDC failure led to full service off-line.
- We have over 10 years of experience in the distributed computing field. We hold the related distributed architecture and algorithms which protected by a number of national and international patents. Thanks to these leading distributed clustering algorithms and architectures, we can deploy multiple active IDC cluster with strong consistent, high availability, and high-performance guarantee easily. **We have been implemented the truly multiple active IDC cluster on full range of our products, providing our customers with unparalleled data reliability and service availability assurance.**

Safety and Reliability - High Availability Counterexamples

- WeChat did not implement multi-active IDC, resulting in unavailability for several hours

微信全面瘫痪：服务器故障 国内外均无法连接

中国网 www.china.com.cn 2013-07-22 10:02

 打印 |  转发 |  评论

中国网7月22日讯(记者 乔红康)7月22日早间,有大量用户反映腾讯微信发生故障,包括微信信息无法发出、无法刷新朋友圈、无法登陆公众账号平台、无法连接微信网页版等。

从网友反馈的结果来看,包括北京、广东、浙江、山东、黑龙江、河南等地区在内,微信均发生全面故障。有用户表示,目前他人在美国,但也连不上微信。

腾讯微信官方微博对此发布回应称,由于服务器基础网络故障导致出现收发问题,并表示正在恢复中。截至22日上午10:00整,该故障仍未修复。

近期,微信多次出现相关故障,仅在上个月就连续出现多次登录、公众平台、连接服务器等方面的故障。

Safety and Reliability - High Availability Counterexamples

- WeChat and QQ did not implement multi-active IDC, resulting in unavailability for several hours



中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

工业和信息化部 新闻动态 政务公开 政务服务

首页 > 工业和信息化部 > 机关司局 > 信息通信管理局 > 应急通信与互联互通

工业和信息化部信息通信管理局指导重要业务系统安全稳定运行

间：2023-04-14 16:57 来源：信息通信管

工信部听取“3·29”微信业务异常情况汇报，腾讯：已处罚相关负责人

红星新闻 2023-04-14 21:28

红星资本局4月14日消息，据工信部官网，工信部信息通信管理局听取腾讯公司关于“3·29”微信业务异常情况汇报，要求腾讯公司进一步健全安全生产管理制度、落实网络运行保障措施，坚决避免发生重大安全生产事故，切实提升公众业务安全稳定运行水平。

对此，腾讯方面的相关负责人向红星资本局表示，3月29日凌晨，由于机房配套设施故障，部分用户使用微信相关功能时出现异常。事故发生后，微信内部快速拉起了专项团队，对问题予以解决，并进行全链条梳理、优化产品保障机制。

腾讯微信团队 3-29 10:50

工程师淋汗以报：现在微信、微信支付相关功能已恢复。

腾讯微信团队 3-29 08:44

今天凌晨部分用户使用微信、微信支付相关功能出现异常，经工程师抢修，系统正在逐步恢复，很抱歉给大家带来不便。

1079 6604 1.8万

腾讯微信团队 3-29 08:44

今天凌晨部分用户使用微信、微信支付相关功能出现异常，经工程师抢修，系统正在逐步恢复，很抱歉给大家带来不便。

1079 6604 1.8万

局听取腾讯公司关于“3·29”微信业务异常情况汇报，要求腾讯公司进一步健全安坚决避免发生重大安全生产事故，切实提升公众业务安全稳定运行水平。

局将深入贯彻落实党的二十大报告关于提高公共安全治理水平的决策部署，统筹发展管力度，指导电信业务经营者严格落实主体责任、完善保障措施、强化事故应急处置行业高质量发展。

Safety and Reliability - High Availability Counterexamples

- Alipay did not implement multi-live IDC, resulting in multiple unavailability for several hours

支付宝故障最新消息

发布时间：2015-05-28 编辑：1037 手机版

27日，支付宝因杭州市政道路建设导致网络光缆被挖断，使部分用户在当天下午短时出现

回复了几个大家关

，但支付宝也会

支付宝出现大面积故障 官方称已在恢复中

腾讯科技 微博 王潘 2016年07月22日12:11

我要分享

腾讯科技讯（王潘）7月22日11时许，支付宝出现较大范围的故障，转账、付款和提现等功能均出现无法操作的情况，出现“网络不给力，暂时无法获取付款结果”“提现系统维护中，请稍后重试”“人气太旺啦，请稍后再试试”等提示语。

而在微博微信等社交平台，更是有大量用户表示遇到同样的问题，比如在饿了么订餐时出现无法支付。

支付宝 突发紧急事件我们也能理解，但你知道？全国有多少人靠着你们生活啊！！离了一会活不下去啊！！拜托你们快点处理啊！

11分钟前 来自 OPPO智能手机

收藏 转发 评论 点赞

支付宝 为啥这样 杭州·领SHOW



11分钟前 来自 iPhone 6

知乎 推荐 关注 热榜

2019年12月5日支付宝疑似崩溃，你们的支付宝还好吗？发生了什么？

支付宝 已认证的官方帐号

7,741 人赞同了该回答

谢谢。

利益相关：利益相关

各位亲，今天下午4点多，支付宝某

可能对部分用户的使用造成影响，

目前，该机房的网络已恢复正常。

此前受到影响的用户可以继续正常使

请放心，大家的资金和信息安全不会

您的余额余额宝会员卡优惠券花呗账

2019年12月5日支付宝疑似崩溃，你们的支付宝还好吗？发

更多回答

再也无法相遇的你

3,338 人赞同了该回答

在海底捞和妹子吃饭，

准备付钱走人了

付了五分钟还不行

尴尬的让妹子付了

然后妹子回家了

发布于昨天 17:41

已赞同 3.3K

327 条评论

分享

收藏

感谢

...

Safety and Reliability - High Availability Counterexamples

- Google cloud computing service crashes for 12 hours and permanently loses data

谷歌数据中心遭雷劈 部分数据永久丢失

腾讯科技 [微博] 2015年08月20日18:19

我要分享

[摘要]雷电天气引起电力中断，导致数据中心磁盘受损和云存储系统断线。

腾讯科技讯 8月20日，比利时布鲁塞尔西南郊的St.Ghislain小镇日前遭遇了强雷电天气，而这一恶劣天气的出现也让谷歌(微博)位于当地的数据中心不幸“躺枪”。

谷歌方面表示，当时的雷电天气引起了电力中断，导致磁盘受损、部分云存储系统断线、数据丢失。虽然数据中心很快便切换到了备用电源，但这一切换却依旧导致0.000001%的数据遭到了删除，且无法恢复。

对此，一家名为‘Azendoo’的法国初创企业负责人查尔斯-大卫(Charles David)表示，因为谷歌数据中心遭遇雷击，自己公司的服务遭遇了长达12小时的中断。

在随后发布的官方事故报告中，谷歌表示自己需要为这一事件负上全部责任，同时鼓励受到影响的企业用户考虑将数据备份到其他谷歌存储服务中。

谷歌云计算引擎的此次事故表明，企业将所有数据存储于单一数据中心会不可避免的在遭遇数据中心级别意外时候面临巨大风险。谷歌在自己的官方声明中说道。

对于谷歌的这一说法，Proper Villains公司合伙人阿隆-图比克(Aaron Trubic)也非常赞同。

Safety and Reliability - High Availability Counterexamples

- QQ mailbox does not implement multiple active IDC, and the service is unavailable on a large scale

就 QQ邮箱等产品大规模瘫痪 作出说明

发布时间：2015-03-20 更新时间：2015-03-31 来源：网络 作者：natty

关键词：[腾讯 公告](#) [网络故障](#)

[技术资料](#) [云计算](#) [云服务器ECS](#) [rds](#) [大数据](#) [建站](#) [com域名](#) [软件安装](#) [域名注册](#)

1月21日中午消息，[腾讯客服](#)今日发布公告，就 QQ邮箱等产品大规模瘫痪 作出说明。公告指出，由于网络系统故障，QQ空间、QQ邮箱等16款腾讯旗下产品受到影响，目前相关服务正在恢复中。

今日早些时候有消息指出，本次QQ邮箱无法正常登陆的原因是，腾讯第三方登录服务器出现了宕机，但腾讯官方未就此作出回应。

今天上午，多家媒体及微博大号报道了腾讯多款产品无法正常使用情况，不少[网友](#)调侃称“腾讯出事了，出大事了，年终奖发少了，技术把服务器格式化了！”

截至记者发稿，此次网络故障所影响的产品已经基本恢复正常。（木南）

腾讯公告原文：

关于网络故障造成部分业务无法正常使用的通知

尊敬的用户：

您好，非常抱歉，由于网络系统故障，导致您的部分服务使用可能受到影响，目前相关服务正在恢复中，请您稍后再使用，由此给您带来的不便敬请谅解！感谢您的支持。

Safety and Reliability - High Availability Counterexamples

- Multiple failures of Alibaba Cloud data center cause service interruptions

尊敬的阿里云用户：

您好，杭州可用区D网络故障确认由于市政施工导致运营商光纤受损，现场正在紧急抢修，目前部分链路已经恢复，请您协助我们一起测试观察，详细情况我们稍后给出。

给您
阿里云
2014年

3月3日凌晨，阿里云开始出现大规模故障。位于华北地区的多家互联网公司的IT运维人员发现一批程序员赶往公司加班。这起宕机事故持续了三个小时左右，事后观察了两个小时。



公告

[阿里云首页](#) > [其他](#) > [【其它】关于华北2地域可用区C部分ECS](#)

【其它】关于华北2地域可用区C部分ECS服务器IO HANG通报

北京时间2019年3月3日凌晨，华北2地域可用区C部分ECS服务器等实例出现IO HANG，经紧急排查处理后已全部恢复。目前我们已经全面排查其他地域及可用区，未发现此类情况。

非常抱歉给您带来的影响！如有任何问题，可通过电报工单随时反馈，感谢您的理解和支持！针对本次故障，我们将根据SLA协议，尽快处理赔偿事宜。

阿里云计算有限公司
2019年3月3日

[阿里云官方公告](#)

阿里云香港机房为何瘫痪12小时

2015年06月23日 20:53 来源于 财新网

事故发生24小时后，阿里云和运营商对事故原因和细节仍莫衷一是，甚至无事的消防和电力部门也被拉来骑枪。阿里云作为国内最大的互联网云提供商是否已经准备好

相关报道

【财新周刊】以阿里云志IOE

【大家谈】阿里云：冲第一而来

阿里云海外扩张提速 借道拜拉避中东北非

中石化牵手阿里云 开启能源大数据

12306春运火车票查询75%由阿里云分流

中国雅虎邮箱转关 阿里云接管

阿里蚂蚁金服60亿建本地生活O2O平台

阿里CEO张勇：做生意的方式将深刻改变

歌华联手阿里、中影打造中国电视网络（更新）

阿里挑战CDN玩法

阿里当家 阿里的银行能飞多高

【财新网】（记者 屈运租 驻香港记者 王靖 见习记者 刘晓景）没有挖断光纤，也不是电力部门问题，更没有所谓的消防警报延误抢修时间，经过财新记者多方调查核实，阿里云在香港中止服务12小时就是一起由硬件故障引发、抢修和恢复严重超时的事故。

这类数据中心的电力事故原本是国内外云服务商普遍面临的一大问题，但用一位业内资深人士的话来说，“12小时才恢复实在太久了。应该几分钟就解决的。”

12小时的超长处理时间，以及过程当中阿里云与相关方陆续给出的五花八门甚至自相矛盾的解析引发了用户的不满和业内的质疑，也暴露了阿里云在故障处理和公众沟通中存在的问题。有部分用户甚至反映15个小时业务才恢复。

Safety and Reliability - High Availability Counterexamples

- British Airways crashes system for days due to power failure in data center



Safety and Reliability - High Availability Counterexamples

- A Microsoft data center air conditioner failure caused Office, AD, VS and other services to be offline and unavailable for nearly 14 hours

Azure status

Last updated 48 seconds ago

Get a personalised view of the health of your Azure services

[Go to your personalised dashboard >](#)

Multiple Services - Applying Extended Mitigation

UPDATE AS OF 15:00 UTC: Engineers have restored storage availability for the majority of impacted services, and customers should be continuing to see improvements to service availability.

CUSTOMER IMPACT: Starting at 09:29 UTC on 04 Sep 2018, customers with resources in South Central US may experience difficulties connecting to resources hosted in this region. A complete list of impacted services can be found below.

PRELIMINARY ROOT CAUSE: A severe weather event, including lightning strikes, occurred near one of the South Central US datacenters. This resulted in a power voltage increase that impacted cooling systems. Automated datacenter procedures to ensure data and hardware integrity went into effect and critical hardware entered a structured power down process.

ENGINEERING STATUS: Engineers have restored access to storage resources for the majority of services, and most customers should be seeing signs of recovery. Engineers are continuing to work on any residual storage impact to fully mitigate this issue. We are also working with the impacted service teams to validate their service health in order to update this status page.

NEXT UPDATE: The next update will be provided by 20:00 UTC 05 Sep 2018 or as events warrant.


Safety and Reliability - High Availability Counterexamples

- The failure of China's national foreign exchange system caused the suspension of foreign exchange business of all domestic banks for several hours




Safety and Reliability - High Availability Counterexamples

- Shanghai Telecom's optical fiber was cut and several businesses including Tencent League of Legends (LoL) were suspended for several hours




新闻综合

腾讯公司 


15分钟前 来自 微博 weibo.com

置顶 【最新进展】经过上海当地运营商... 恢复。业务恢复正常中，部分产品可能存在... 成的不便，我们深表歉意。祝大家周末愉快

@腾讯公司 

【紧急公告】各位用户，2019年03月23日16时左右... 故障，腾讯多个产品业务使用受到影响。目前运营... 处理，业务陆续恢复中。后续修复进展会及时向... 今天 16:32 来自 专业版微博

☆ 收藏 8




知乎 首页 发现 等你来答 极速救援

电子支付 微信 支付 微信支付

10月29日微信支付问题是什么原因导致的？

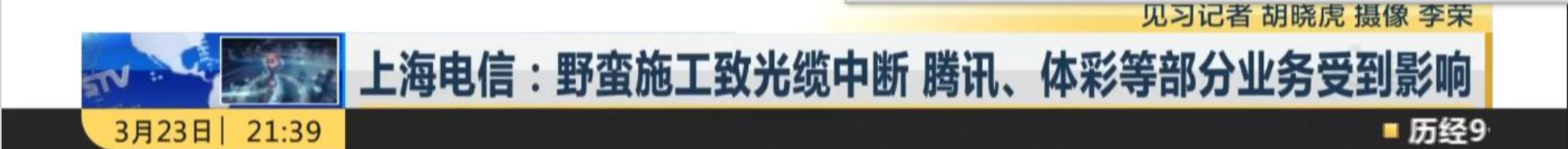
相关问题：

如果微信支付或支付宝等电子支付一个月不能使用，生活会发生哪些变化？ 

www.zhihu.com

最新进展：

网传微信故障通告：由于微信官方与银联系统... 对接的网络宕机，20:10-20:35之间，全国微信支付交易无法正常进行。



见习记者 胡晓虎 摄像 李荣

上海电信：野蛮施工致光缆中断 腾讯、体彩等部分业务受到影响

3月23日 | 21:39

■ 历经9

Safety and Reliability - Data Security 1

- Our self-developed virtual file system (VFS) supports on-the-fly data compression and strong encryption. It can provide strong encryption protection at the [entire database level](#) for all data, and supports dozens of industry-recognized strong encryption algorithms including AES, SM4, and BlowFish.

Note: Ordinary, encryption based on database records usually converts the same plaintext into the same ciphertext.

For example: if there is a field named "Name" in the user table in the database to store the name of the employee, and the plaintext "James" is encrypted and the ciphertext is "ABCD", then for the row by row (field by field) encryption algorithm, every time an employee named "James" appears in the table, it will be encrypted as "ABCD" (ECB-like mode).

All types of ECB modes have weak protection against cracking methods such as static analysis, differential analysis, and known (partial) plaintext attacks, and cannot ensure data security.

Our VFS uses an [entire database-level encryption](#) technology based on secure encryption modes such as CTR and CBC and strong encryption algorithms such as AES to provide mathematically provable strong security (reliability, consistency, confidentiality) protection. Even if it is the same plaintext, it will be transformed into a different and completely unrelated ciphertext, thus eliminating the above-mentioned attack methods.

Safety and Reliability - Data Security 2

- The application platform supports the storage of user passwords with a salted secure hash value. Then this information will be compressed and strongly encrypted before being saved in the configuration storage.
- The support platform supports unified management of user permissions with a strict role-based authorization mechanism and [access control list \(ACL\)](#). After the entire database encryption function is turned on, even network administrators cannot peek into corporate data.

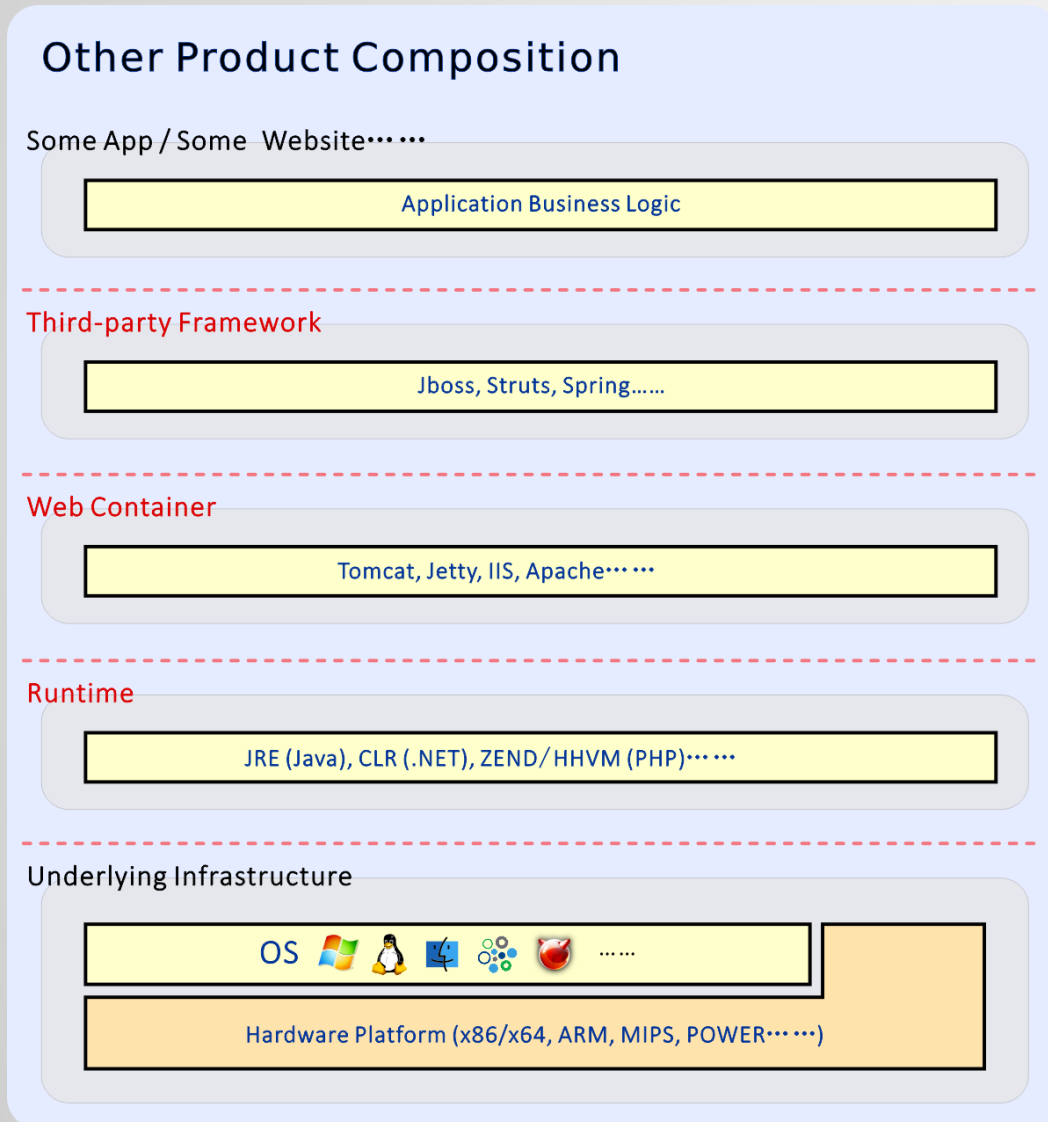
Safety and Reliability - Transmission Security

- Products based on the support platform can use digital certificates issued by recognized authorities to provide online [banking-level TLS \(HTTPS\) network data transmission protection and BYST-based end-to-end secure transmission capabilities](#).
- User passwords are stored in the form of a [salted secure hash](#). Use the [CHAP authentication](#) protocol based on SHA and HMAC security algorithms to complete the network authentication process. Even if it does not rely on TLS encryption protection (full plaintext transmission), there will be no key leakage.
- It can be configured to [force the cooling](#) for M minutes after the same user fails to log in consecutively for N times, and cooperate with intrusion detection and malicious request filtering technology to prevent brute force cracking. In addition, the administrator can also customize the [password complexity requirements](#) such as the minimum length, uppercase and lowercase letters, and numbers.
- [EAL5+ level dedicated smart card](#) can be used to achieve hardware-level security authentication.

Safety and Reliability - System Security 1

- Environments such as Java (JRE), C# (.NET), and Tomcat have a large number of serious security vulnerabilities, and there are extremely high security risks. Through the CVE database published by the International Security Organization, it can be found that the above-mentioned products have multiple new vulnerabilities with the highest severity level being disclosed almost every year. For example:
- Java : https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-19117/Oracle-JRE.html
- Tomcat : https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-887/Apache-Tomcat.html
- .NET : https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-2002/Microsoft-.net-Framework.html
- etc.

Safety and Reliability - System Security 2

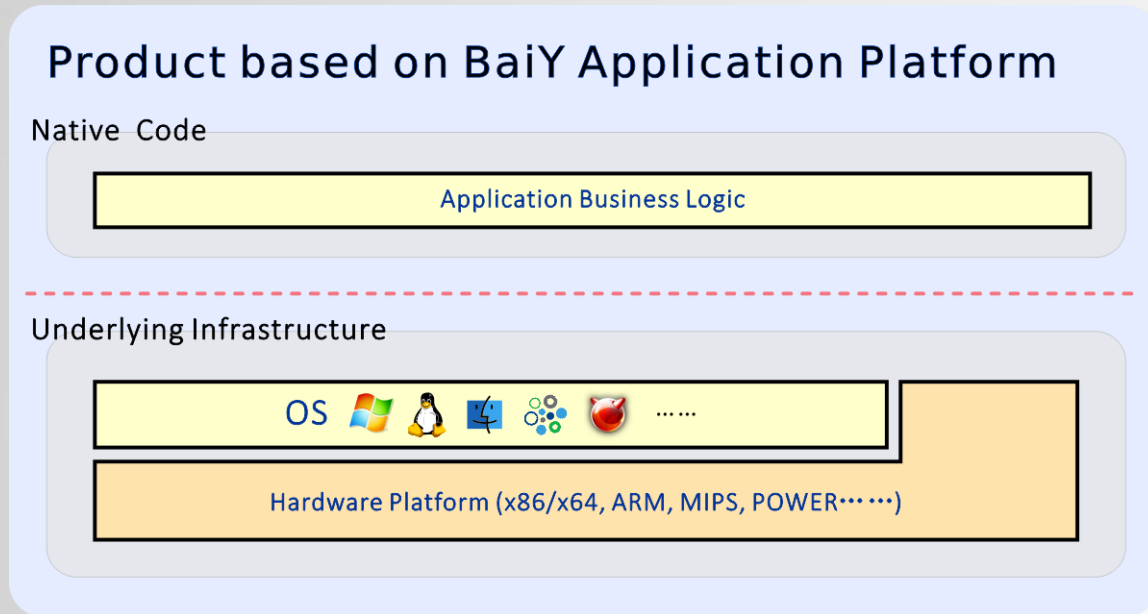


- As shown in the left figure: The dependence on dynamic runtime environments such as Java and .NET, containers such as Tomcat, and third-party frameworks such as Spring have led to the introduction of a large number of additional third-party components that are not controlled by the developer.
- Obviously, products developed using dynamic languages such as Java, .NET, and PHP include multiple additional layers such as third-party frameworks, web containers, and dynamic runtimes between the application and the underlying infrastructure. **These additional layers of third-party software that are not under the control of the developer contain a large number of well-known security vulnerabilities that can be easily exploited.**

Safety and Reliability - System Security 3

- Even ordinary users with a little common sense can simply find free and open source tools that can successfully exploit these vulnerabilities through search engines, and use them to invade corporate systems to complete illegal operations such as data theft, data tampering, and data destruction. Just try Google "vulnerability scan", "penetration tool" and other related keywords.
- It can be seen that the introduction of uncontrolled additional layers greatly increases the attack surface of the system and seriously increases the security risk of the system. At the same time, it greatly increases the workload of operation and maintenance personnel and increases the total cost of ownership (TCO) of the system.

Safety and Reliability - System Security 4



- As shown in the figure above: products based on the application platform are developed using tools such as assembly and C/C++.
- Built directly on the underlying operating system and hardware platform.

- Products based on the application platform run directly on the underlying infrastructure composed of bare metal and operating systems with efficient native code (**Native Code**), bringing unparalleled space-time efficiency and security guarantees for software products.
- Since there is no need to rely on uncontrollable third-party components such as dynamic runtimes and web containers, **the attack surface of the software and the hidden dangers of system security are greatly reduced**. At the same time, it greatly reduces the workload of operation and maintenance personnel and reduces the overall cost.

Safety and Reliability - Security Supplement

- In recent years, there have been frequent security issues. Amazon, Walmart, Yahoo, LinkedIn, , OpenAI (ChatGPT), Sony, JPMorgan Chase, UPS, eBay, JD, Alipay, CTrip, 12306, Netease, CSDN, China Life Insurance, and major hotel groups (such as Jinjiang, InterContinental, Sheraton, Marriott, and Huazhu) and other well-known companies frequently report a large number of serious security incidents involving the leakage of user information, and security assurance is urgent.
- The application platform supports storing all databases and local configuration data in our self-developed virtual file system (VFS) that supports on-the-fly data compression and strong encryption for comprehensive protection. Support dozens of industry-recognized strong encryption security algorithms, even system administrators can not peek into corporate data.
- The strong encryption algorithm based on industry standards guarantees that even if there are supercomputers that can complete one trillion key cracking attempts per second in the future, it will take an average of 54 trillion years to crack a key. Safety has been greatly guaranteed.

Safety and Reliability - Security Counterexamples

思科：Java 成 91% 恶意攻击的主要原因



Google

思科的

根据思
一项技

思科的

“在观澳
国互联

思科的

贡德特

击’（零
然，也

思科不

2013年

2018开源代码安全报告：每个代码库平均包含64个漏洞

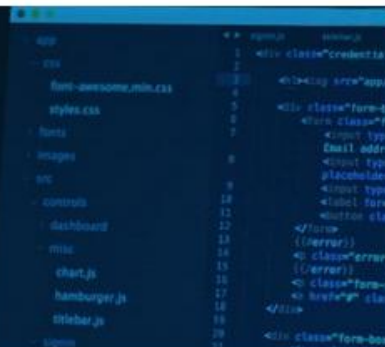


王练

发布于2018年07月06日 收藏 3 评论 2

Synopsys 公司近日发布了“**2018 年开源代码安全和风险分析**” Black Duck (黑鸭) 报告，深入考察了商业软件中开源安全性，许可证合规以及代码质量风险的状况。本次报告讨论的是从 2017 年审计的超过 1,100 个商业代码库中的匿名数据所得出的结果，行业包括汽车、大数据（主要是人工智能和商业智能）、网络安全、企业软件、金融服务、医疗保健、物联网（IoT）、制造业和移动应用市场。

2018 Open Source Security and Risk Analysis Report



Safety and Reliability - Security Counterexamples

- A glimpse of high-risk vulnerabilities in Java

Vulnerability Details : [CVE-2016-3443](#)

Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to 2D. NOTE: the previous information is from the April 2016 CPU. Oracle has not commented on third-party claims that this issue allows remote attackers to obtain sensitive information via crafted font data, which triggers an out-of-bounds read.

Publish Date : 2016-04-21 Last Update Date : 2016-12-02

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the system, resulting in the system being unavailable.)
Access Complexity	Low (Specialized access conditions are required, but they are not difficult to exploit.)
Authentication	Not required (Authentication is not required for the exploit to succeed.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerability.

Vulnerability Details : [CVE-2016-3427](#)

Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JMX.

Publish Date : 2016-04-21 Last Update Date : 2016-12-02

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the system, resulting in the system being unavailable.)
Access Complexity	Low (Specialized access conditions are required, but they are not difficult to exploit.)
Authentication	Not required (Authentication is not required for the exploit to succeed.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerability.

Vulnerability Details : [CVE-2016-0494](#)

Unspecified vulnerability in the Java SE and Java SE Embedded components in Oracle Java SE 6u105, 7u91, and 8u66 and Java SE Embedded 8u65 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.

Publish Date : 2016-01-20 Last Update Date : 2016-12-07

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

- CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)

Safety and Reliability - Security Counterexamples

- Security breach led to Yahoo leaking data of more than 3 billion users

雅虎再次曝出数据泄露事件：涉10亿帐户 有史以来最严重

2016年12月15日 09:07 新浪科技 微博

雅虎：5亿用户信息两年前被盗 或为最大网络信息泄露 东方新闻 160923



雅虎又泄露3200万账户数据，这次是因为“cookie伪造”攻击

孙毛毛 @2017-03-03 共39169人围观，发现18个不明物体 资讯

engadget 中国版

雅虎承认 2013 年的骇客攻击涉及了当时所有 30 亿个账户

受害者数量一下子变成了之前公布的三倍。



Sanji Feng

2017年10月4日, 下午08:00

在过去两年间，有入侵者进行“cookie伪造”攻击，造成3200万账户泄露。特别值得注意的是，和前几个月爆出的两次大规模数据泄露不一样（2016年12月曝10亿账户泄露，200万这个数字现在听起来根本就不算什么。

hacked hacked hacked hacked hacked hacked hacked hacked

ashed passwords (the vast majority with bcrypt and, in some cases, encrypted). The ongoing investigation suggests that stolen information did not include bank account information, payment card data and bank account information are not found to be affected. Based on the ongoing investigation, Yahoo believes that user accounts was stolen and the investigation has found no evidence that the work, Yahoo is working closely with law enforcement on this matter.

前被盗 或为最大网络信息泄漏 NEWS24

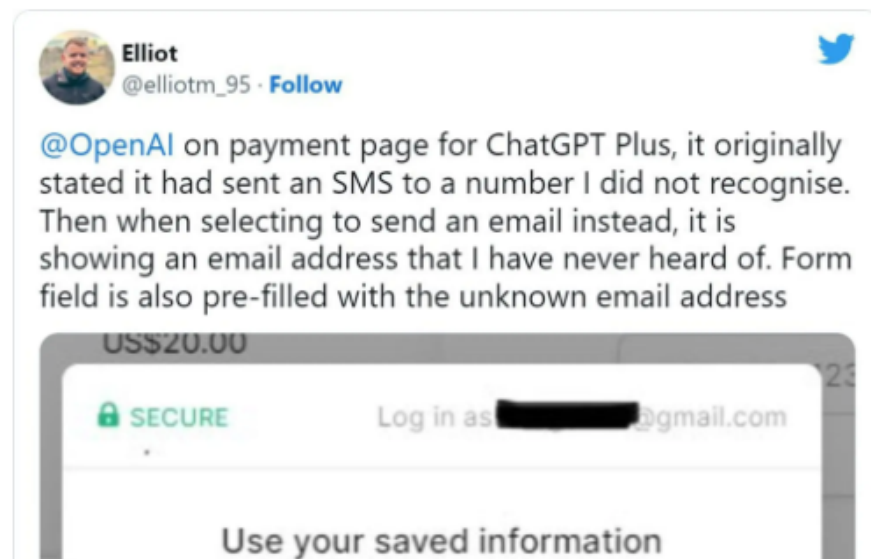
Safety and Reliability - Security Counterexamples

- Redis security flaws lead to ChatGPT leaking user privacy sessions

Redis 错误导致 ChatGPT 数据泄露，技术细节一并公布

来源: OSCHINA 编辑: Alias_Travis 2023-03-27 08:52:26 8

在上周一，ChatGPT 遭遇了一次用户数据泄漏事件，许多 ChatGPT 的用户都在自己的历史对话中看到了其他人的对话记录。不光是对话的历史记录，不少 ChatGPT Plus 用户还在 Reddit 和 Twitter 等平台发出了截图，表示在他们的订阅页面上看到了其他人的电子邮件地址。



Safety and Reliability - Security Counterexamples

- NetEase leaked data of over 100 million users

网易邮箱被曝过亿数据泄露

腾讯科技  [微博] 梁辰 2015年10月19日15:39 我要分享 ▼

腾讯科技讯（梁辰）10月19日，有用户“路人甲”在国内安全网络反馈平台WooYun（乌云）发布消息称，[网易163/126邮箱](#)过亿数据泄漏，涉及邮箱账号、密码、用户密保等。这一漏洞危害等级被标注为“高”。另有消息称，此次泄露规模或达5亿条的规模。同时也有人表示，已向[苹果](#)客服咨询，苹果客服称网易服务器被入侵。

不过，截至腾讯科技发稿时，乌云平台已将“网易邮箱”抹掉，改为“某邮箱”。目前的漏洞状态为已交由第三方合作机构(cncert国家互联网应急中心)处理。

导致此次安全事件的原因，疑似网易用户数据库泄露，影响数量总共数亿条。乌云方面称，目前已通过乌云漏洞平台第一时间通知到网易。

乌云平台披露，目前泄露的信息包括用户注名、MD5（一种算法）密码、密码提示问题和答案、注册IP、生日等。据悉，解开后测试大部分邮箱依旧还可登陆。

Safety and Reliability - Security Counterexamples

- Java Struts framework vulnerability causes sensitive data such as tens of millions of user account passwords and credit cards to leak

[资讯] 京东数千万用户信息遭外泄 东方新闻 2016-12-11

✓ 641

```
uid":1,"realname":"那落","username":"richard","email":"alrc@163.com","password":"6e5ea5  
uid":2,"realname":"魏其","username":"hg_jh","email":"hg_jh@163.net","password":"625bdd5  
uid":3,"realname":"田子明","username":"tianzhimi","email":"tianzhimi@126.com","password  
uid":4,"realname":"林林","username":"blob","email":"blob2000@163.com","password":"f3f15  
uid":5,"realname":"李一宇","username":"lyntom","email":"lyntom@163.com","password":"62  
uid":6,"realname":"魏志电子","username":"qlyy","email":"13051304881","password":"9f681b  
uid":7,"realname":"空军","username":"飞行器","email":"xy1234567@139.com","password":"0  
uid":8,"realname":"张涛","username":"Amiao","email":"amiao@vip.163.com","password":"8b  
uid":9,"realname":"吴彬","username":"justin0","email":"justin.wb@263.net","password":"039  
uid":10,"realname":"刘庆宇","username":"bdi","email":"sunth@163.com","password":"bab6  
uid":11,"realname":"岑玉","username":"70年代的人","email":"aiping2009@gmail.com","passw  
uid":12,"realname":"陈瑞","username":"cherolangq","email":"chenxiangq@hotmail.com","p  
uid":13,"realname":"陈奇","username":"qcsince","email":"burningq@163.com","password":"  
uid":14,"realname":"胡朝晖","username":"胡朝晖","email":"qdzouzhao@163.com","pass  
uid":15,"realname":"吴江","username":"wujohn","email":"xcstz@gmail.com","password":"8b  
uid":16,"realname":"王健文","username":"guru","email":"warrenbox@126.com","password":"  
uid":17,"realname":"邱宇","username":"wahaha","email":"qiyu@21cn.com","password":"26  
uid":18,"realname":"石树茂","username":"志豪","email":"whisperwoods@sina.com","passwo  
uid":19,"realname":"王翔翔","username":"tobyjacky","email":"tobyjacky@163.com","passw  
uid":20,"realname":"吕进俊","username":"odd","email":"esoddus@sina.com","password":"0e  
uid":21,"realname":"刘杰","username":"jasco","email":"jasco@126.com","password":"22ca6c  
uid":22,"realname":"王雷","username":"trillkum","email":"whist@mail.xpft.q.cn","password"  
uid":23,"realname":"陈强","username":"陈人","email":"fai ren_2@hotmail.com","password":"6  
uid":24,"realname":"朱磊","username":"我是替补","email":"41657634@qq.com","password":"  
uid":25,"realname":"田德浩","username":"清吧吧","email":"liandehao@tom.com","password"
```

18:42

东方卫视 戴晶磊 成奕霖

京东被指大量用户信息遭外泄

NEWS24

Safety and Reliability - Security Counterexamples

- Alipay leaked tens of millions of user data

支付宝数据泄露!工信部介入密码泄露调查

2011年12月30日11:06 来源: 太平洋电脑网 作者: 盛夏Veya [欢迎发表评论](#)

将本文转发至: [QQ](#) [微信](#) [微博](#) [人人网](#) [豆瓣](#) [贴吧](#) [更多](#) [纠错](#) [收藏](#)

12月30日消息,中国互联网正在遭遇一场最大规模的用户信息泄露事件,而此次“泄密门”事件波及的范围也越来越广,从互联网科技公司,到互联网电商企业,都难逃数据泄露的厄运。而如今,就连银行、出入境局登记数据也被传有泄露。目前,工信部已经介入此次大规模的密码泄露事件,强烈谴责窃取和泄露用户信息的行为,责令发生用户信息泄露的网站尽快发出警示,要求互联网站开展全面的安全自查。

不断扩大的互联网用户信息泄露阴影

继CSDN、天涯社区等论坛确认用户资料被泄露之后,一向被用户定义为“安全”的第三方支付平台也被爆料称上千万的用户信息外泄。

漏洞概要

漏洞编号: [WooYun-2011-03871](#) 关注度(8)

漏洞标题: 支付宝用户大量泄露,被用于网络诈骗

相关厂商: 支付宝

漏洞作者: 路人甲

提交时间: 2011-12-28

漏洞类型: 用户资料大量泄露

危害等级: 高

自评Rank: 20

漏洞状态: 等待厂商处理

漏洞来源: <http://www.wooyun.org>

Tags标签: 无

分享漏洞: [QQ](#) [微信](#) [微博](#) [人人网](#) [豆瓣](#) [贴吧](#) [更多](#)

漏洞详情

简要描述:

支付宝用户大量泄露,被用于网络诈骗 泄露总量达1500-2500W之多 泄露时间不明,里面只有支付宝用户的账号,没有密码

漏洞hash: 6701ae23372bbea6c1dd74f23d8c584e

支付宝用户信息也被泄露

日前,网络安全问题反馈平台“乌云漏洞”指出,支付宝部分账号信息被泄露,涉及邮箱数量在1500万至2500万。对此,支付宝公关经理朱先生否认支付宝存在漏洞一说,并称相关账号并非支付宝用户账号,且支付宝内没有用户的手机号、身份证号等敏感信息,但支付宝部分账号并非支付宝用户账号。

Safety and Reliability - Security Counterexamples

- Equifax leaked 143 million people's social security, credit card and other sensitive records due to Java Struts vulnerability

Cybersecurity Incident & Impact

[Consumer Notice](#) [FAQs](#) [Potential Impact](#) [Enroll](#) [Trust](#)

A Progress Update for Consumers

September 13, 2017

1) Updated information on U.S. website application vulnerability

Equifax has been intensely investigating the scope of the intrusion with information was accessed and who has been impacted. We know that Apache Struts CVE-2017-5638. We continue to work with law enforcement with law enforcement.

2) Temporary interruption to credit freeze sign-up link.

sina 新浪财经 新浪财经 > 美股 > 正文

美国1.43亿人个人信息被泄露

2017年09月08日 08:40 新浪科技 微博 我有话说(10人参与) 收藏本文



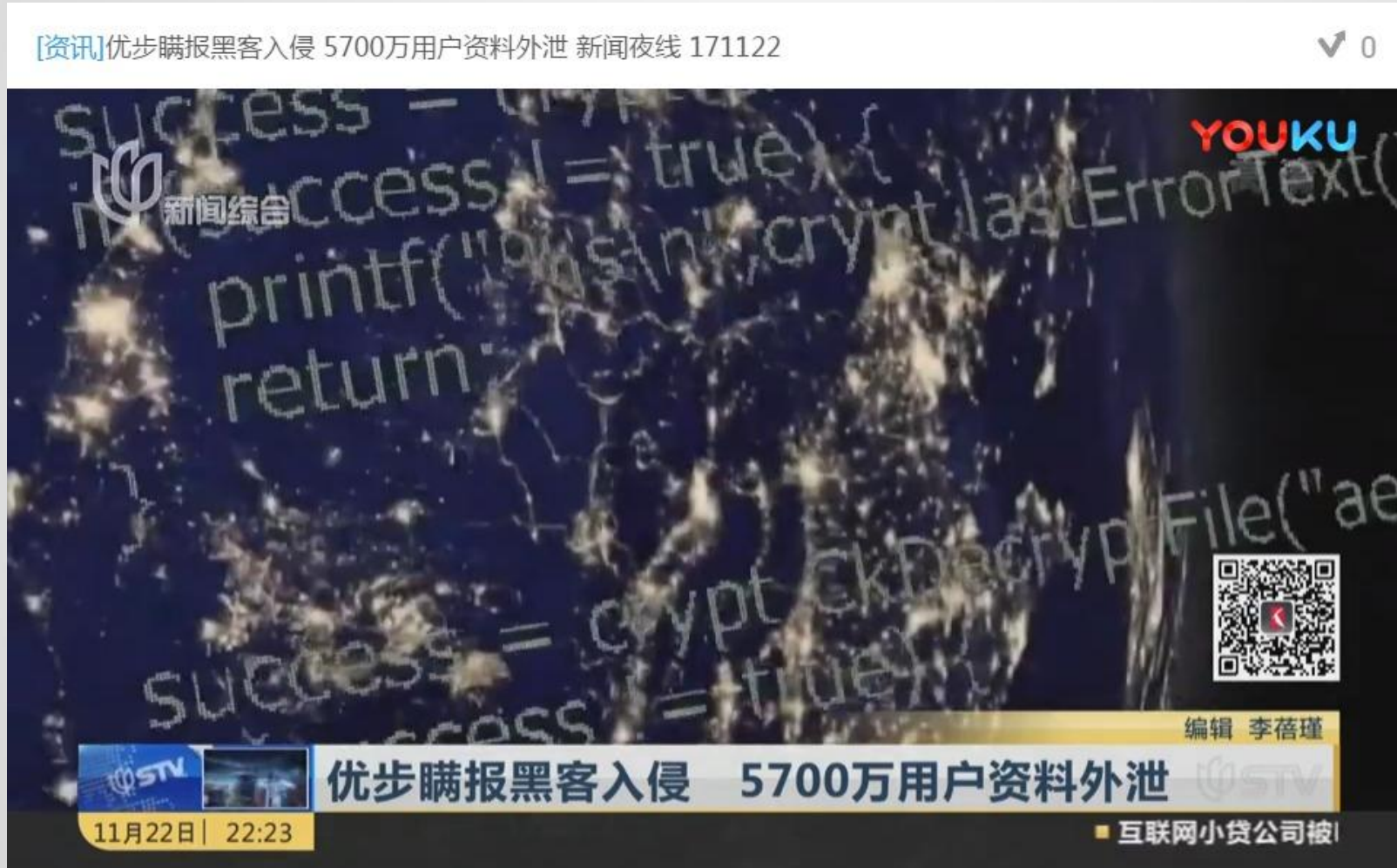
美股行情中心: 独家提供全美股行业板块、盘前盘后、ETF、权证实时行情



新浪科技讯 北京时间8日早间消息，美国征信企业Equifax披露称，其网站遭遇黑客攻击，造成1.43亿人的个人信息泄露，包括社会保障号码和驾照信息等。这可能是近年来最大的一起泄露事故。之前雅虎虽然泄露了10亿帐户信息，但里面没有包含社会保障号和驾照信息。


Safety and Reliability - Security Counterexamples

- Uber concealed hacking and leaked data of 57 million users




Safety and Reliability - Security Counterexamples

- Major security incident of WeChat Pay "Buy at Zero Dollars" caused by the XXE vulnerability in Java XML component




www.news.cn
新华网
NEWS
www.xinhuanet.com


让新闻离你更近




关注新华网



微信



微博



Qzone

0
评论

微信支付曝“0元购”漏洞 安全

2018-07-04 15:04:57 来源：新华网

新华社厦门7月4日电（记者颜之宏）3日，有网络安全机构曝光了一组微信支付技术漏洞，据称攻击者可利用该漏洞将自己伪装成微信支付平台，通过篡改获得“0元购”特权。记者3日晚间从微信支付官方渠道获悉，该漏洞已修复，目前暂未发现商户有异常，商户无需恐慌。

据网络安全专家谢忱介绍，从当前被公开的漏洞信息来看，网络攻击者通过微信支付官方SDK（软件工具开发包）存在的漏洞，将自己伪装成“微信支付平台”，通过微信的漏洞伪造与商户的直接通信，在篡改微信支付的正常通信信息后，达到“换柱”的目的。

谢忱表示，正常的支付流程应该是由用户发起，经由微信支付平台到达商户，会有一个与微信支付平台确认支付结果的过程，而网络攻击者恰恰是利用了这个漏洞，通过篡改微信支付的数据包，伪造了与商户的通信，从而实现了“0元购”等操作。谢忱认为，一些商家的安全防护水平较低，攻击者还可通过获取商户的密钥等信息，再通过这个漏洞就可以实现“将订单设置为0元”等操作，导致该商户的消费者信息等数据内容泄漏。

网络支付安全专家于迪则认为，接入微信支付的商户不必过度恐慌。于迪表示，该

关于20180704微信支付漏洞的分析

kanmars
一个不懂生活的人，正在补习前半生的失误

+ 关注他

2 人赞了该文章

今天看新闻，说微信官方SDK有漏洞。

微信支付曝漏洞：可发伪造信息使购物无需付费

7月4日消息，近日有网友在国外安全社区发帖称微信支付官方SDK存在的严重漏洞，攻击者可通过此漏洞侵入商家服务器，获得商家关键安全密钥，通过发送伪造信息来欺骗商家而无需付费购买任何东西。

腾讯对此表示，微信支付技术安全团队已第一时间关注及排查，对官方网站上该SDK漏洞进行更新，修复了已知的安全漏洞，并在此提醒商户及时更新。

```
Example vivo :
attack:
  notify url: https://pay.vivo.com.cn/webpay/wechat/callback.oo
  cmd: /home/

result:
  tomcat

attack:
  notify url: https://pay.vivo.com.cn/webpay/wechat/callback.oo
  cmd: /home/tomcat

result:
```

Safety and Reliability - Security Counterexamples

- Many hotel groups such as China Lodging Group Hanting, Orange and other hotel groups leaked 130 million people's sensitive information and 240 million room opening records

helen250

帖子: 10
注册时间: 2018年-08月-28日 00:34
联系:

华住旗下酒店开房数据 (汉庭, 桔子, 全季等)

由 helen250 » 2018年-08月-28日 06:00

出售华住旗下所有酒店数据 (汉庭/美爵/禧玥/漫心/诺富特/美居/CitiGO/桔子/全季/星程/宜必思尚品/宜必思/怡莱/海友)

附件当中为测试数据, 各提供10000条数据供大佬测试。

crm.txt为华住官网注册资料, 包括姓名, 手机号, 邮箱, 身份证号, 登陆密码等信息。全部资料共53G, 大约1.23亿条记录

cusinfo为酒店入住时登记的身份信息, 主要包括姓名, 身份证号, 家庭住址, 生日, 内部id号。全部资料共22.3G, 大约1.3亿人身份证信息

history 为酒店开房记录, 包括内部id号 (可与cusinfo做关联查询), 同房间关联号, 姓名, 卡号, 手机号, 邮箱, 入住时间, 离开时间, 酒店id号, 房间号, 消费金额等信息。共66.2G, 大约2.4亿条记录。

以上数据脱裤时间为2018年8月14号。

欢迎各位有需要的大佬购买, 以上全部信息打包价为8比特。

联系我邮箱或者暗网私信我, 我把数据的下载地址和解压密码。

据还可以免费发给已购买的大佬。

程	C01, 3101	, 1974-10-06 00:00:00, 上海市黄浦
胡	, C01, 23	, 1, 1968-09-12 00:00:00, 黑龙江省
	, C01, 46	, 1,, 海南省海口市美兰区中贤村二村
	, C01, 42	, 1, 1967-03-07 00:00:00, 武汉市蔡
	, C01, 37	, 1, 1965-07-06 00:00:00, 济南市天
	C01, 6103	, 1984-10-02 00:00:00, 陕西省扶风
	C01, 3209	, 1976-08-11 00:00:00, 江苏省无锡
	, C01, 33	, 1, 1988-11-01 00:00:00, , , , ,
	, C01, 33	, 1,, 浙江省瑞安市桐浦乡山平村,,
	, C01, 23	, 1, 1967-03-11 00:00:00, 黑龙江省
	, C01, 46	, 2,, 海南省海口市美兰区中贤村二村
	C01, 1401	, 1977-10-20 00:00:00, 山西省太原
	C01, 1301	, 1983-10-04 00:00:00, 北京市石景
	, C01, 33	, 1,, 浙江省金华市婺城区长山乡石
	C01, 3101	, 1958-02-03 00:00:00, 上海市普陀
	C01, 3206	, 1980-11-13 00:00:00, 江苏省启东
	, C01, 46	, 2,, 海南省海口市龙华区八灶村80号
	, C01, 33	, 1, 1969-08-14 00:00:00, 浙江省金
	, C01, 61	, 1,, 陕西省岐山县凤鸣镇北杨村张
	, C01, 33	, 1, 1979-01-31 00:00:00, 浙江省瑞
	, C01, 37	, 2,, 山东省临邑县临盘街道办事处
	, C01, 46	, 2, 1953-04-04 00:00:00, 海南省海
	, C01, 35	, 1, 1985-05-10 00:00:00, 福建省南

08:02

看东方 Morning

华住酒店集团上亿用户数据疑泄露 警方已介入调查

涉及汉庭、桔子、全季、宜必思

08:02

看东方 Morning

华住酒店集团上亿用户数据疑泄露 警方已介入调查

涉及入住登记身份约1.3亿条 开房记录约2.4亿条

Safety and Reliability - Security Counterexamples

- The Sheraton, Westin, W and many other hotels of the Marriott Group leaked the sensitive information and room opening records of 500 million people

The background image is a blurred screenshot of a Marriott press release. It features the Marriott logo (a red circle with a white star) and text that reads: "Marriott has not finished identifying duplicate information up to approximately million of these guests' email address, past arrival and departure also includes pay".

Overlaid on the background is a video player. The video title is "3.83 亿开房记录被泄露后，万豪又又又泄露用户数据了" (After 383 million room records were leaked, Marriott leaked user data again and again). The author is "作者: 万佳" (Author: Wan Jia) and the view count is "阅读数: 3041 | 2020 年 4 月 1 日 16:36". The video content shows a close-up of a "Boggle" sign.

At the bottom of the image is a red banner with white text. It includes a QR code on the left, the time "18:55", and the text "东方卫视 邢晓宇 编辑 朱晓涵" (Oriental TV, Editor: Xu Xiaoyu, Editor: Zhu Xiaohan). The main headline on the banner is "万豪旗下喜达屋数据遭窃" (Marriott's Starwood data was stolen). To the right of the banner, there is another video player showing a news report with the headline "万豪旗下喜达屋数据遭窃 信息泄露或涉5亿宾客" (Marriott's Starwood data was stolen, information leak may involve 50 million guests).



重玄科技
PHILO-TECH

philo-tech.com