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.

BaiY Application Platform - 1

- **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.

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

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
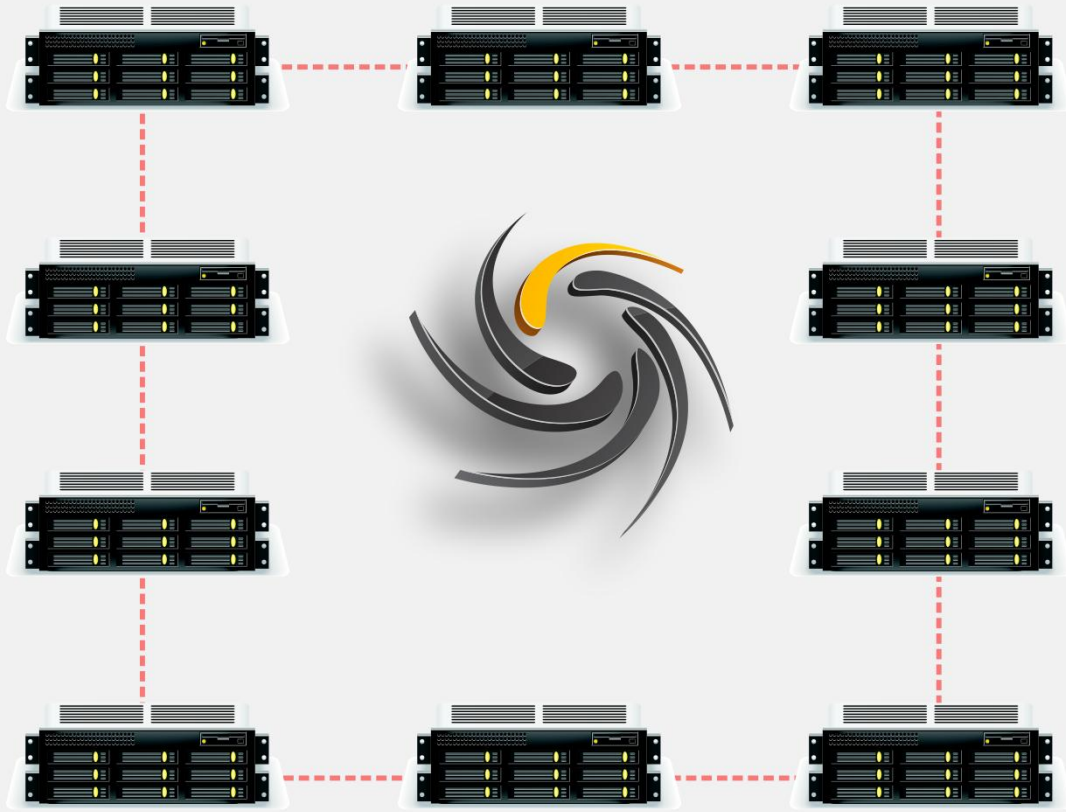
- Distributed coordination services provide functions such as service discovery, service election, fault detection, failover, failback, distributed lock, task scheduling, message routing and message dispatching.

- 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
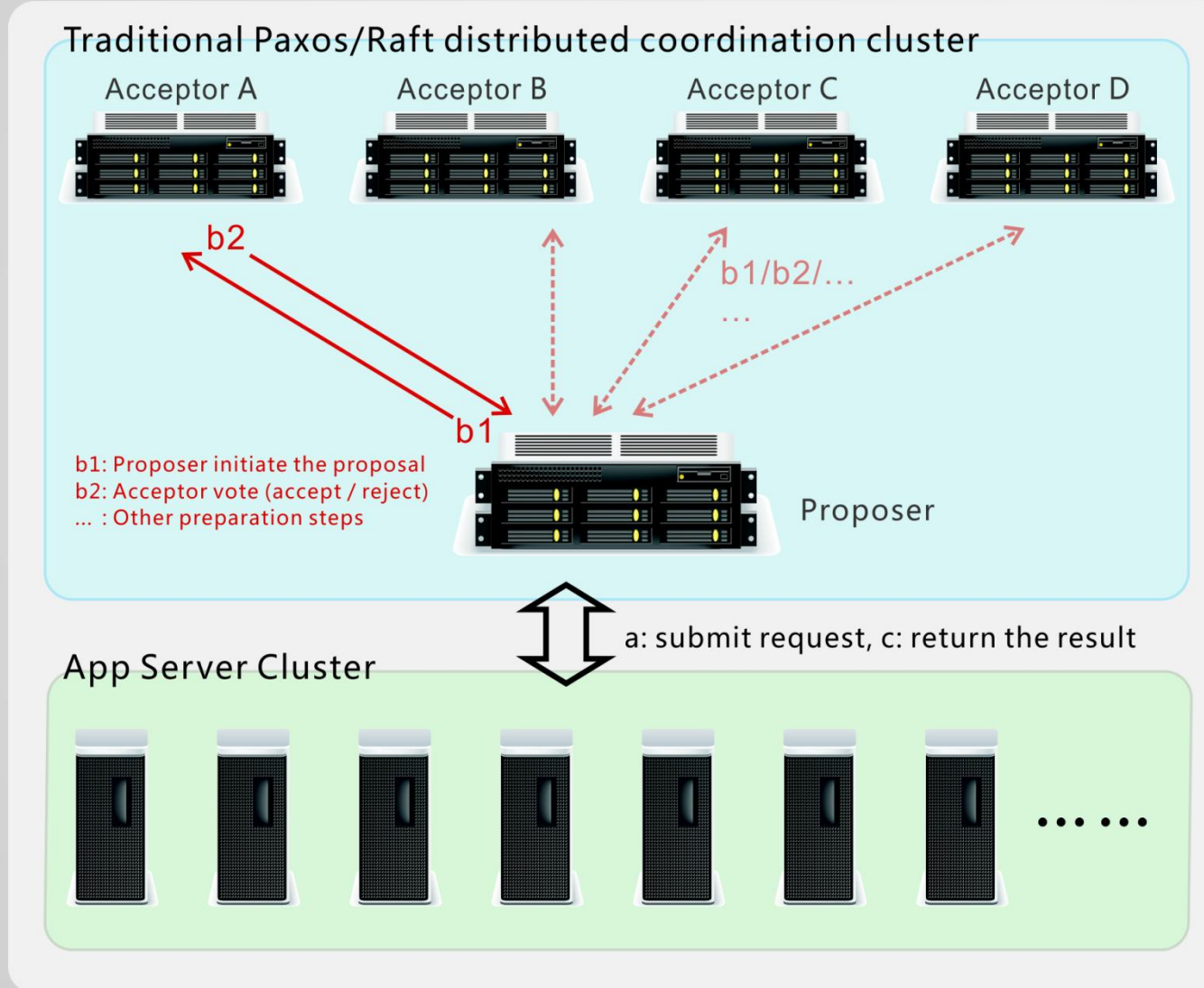
- The traditional Paxos / Raft distributed coordination algorithm initiates voting for each request, generating at least 2 to 4 broadcasts (b1, b2...) and multiple disk IO. Making it highly demanding on network throughput and communication latency, and cannot be deployed across multiple data centers.

- 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
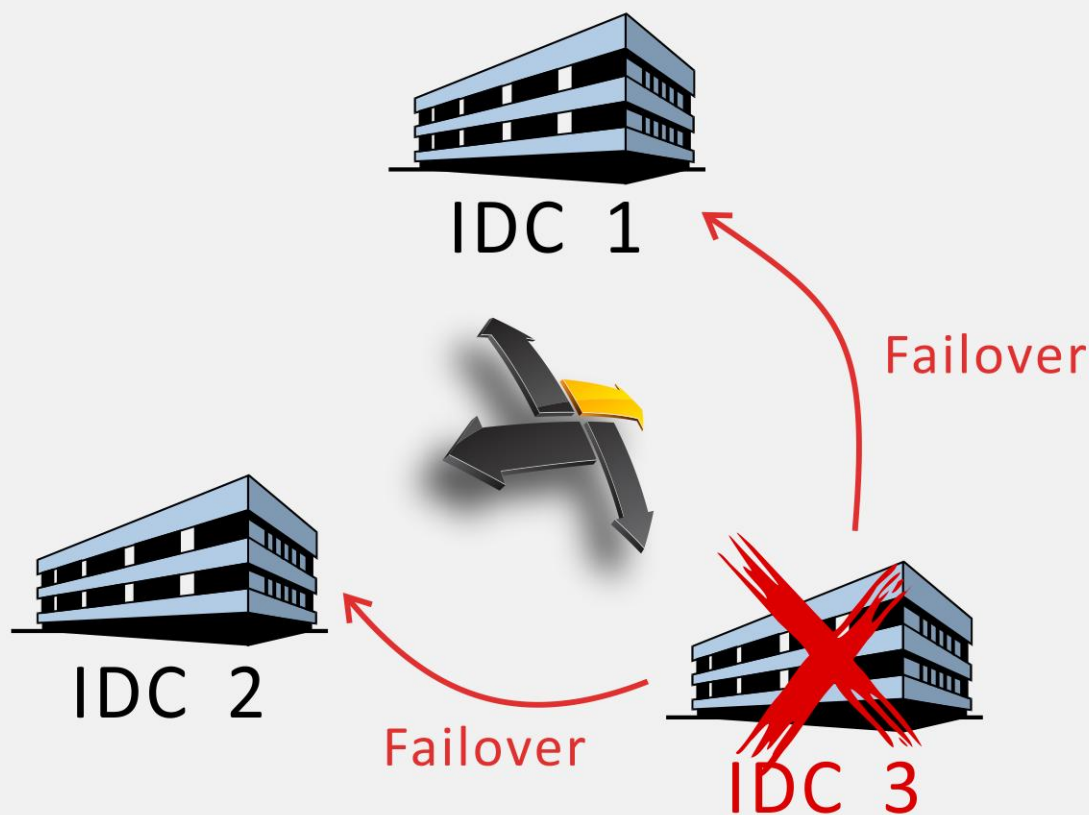
- Based on our unique distributed coordination technology, the high performance, strong consistency cluster across multiple data centers can be implemented easily.

- 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

Slave Node B   Master Node A

Failover

Heartbeat Connection

1.Tom : Account balance 100
2.Node B: Tom Transfer 20 , the balance of 80
3.Node A: Tom Transfer 30, the balance of 70
4.Tom actual balance should be 50

VIP: 10.1.1.8
Provide services through the VIP
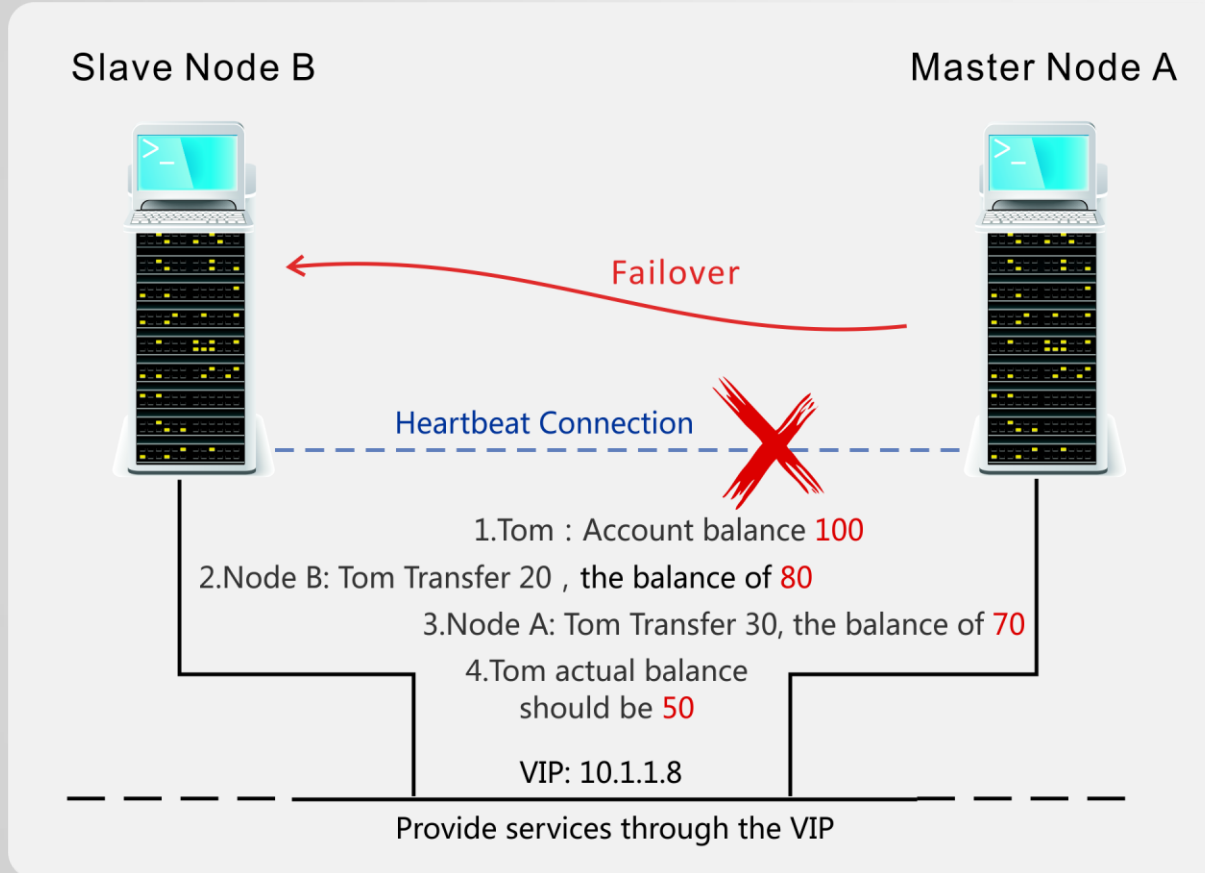
- In the traditional dual fault tolerance scheme, the slave node automatically promotes itself as the master node after losing the heartbeat signal and continues to provide services to achieve high availability.

- 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.
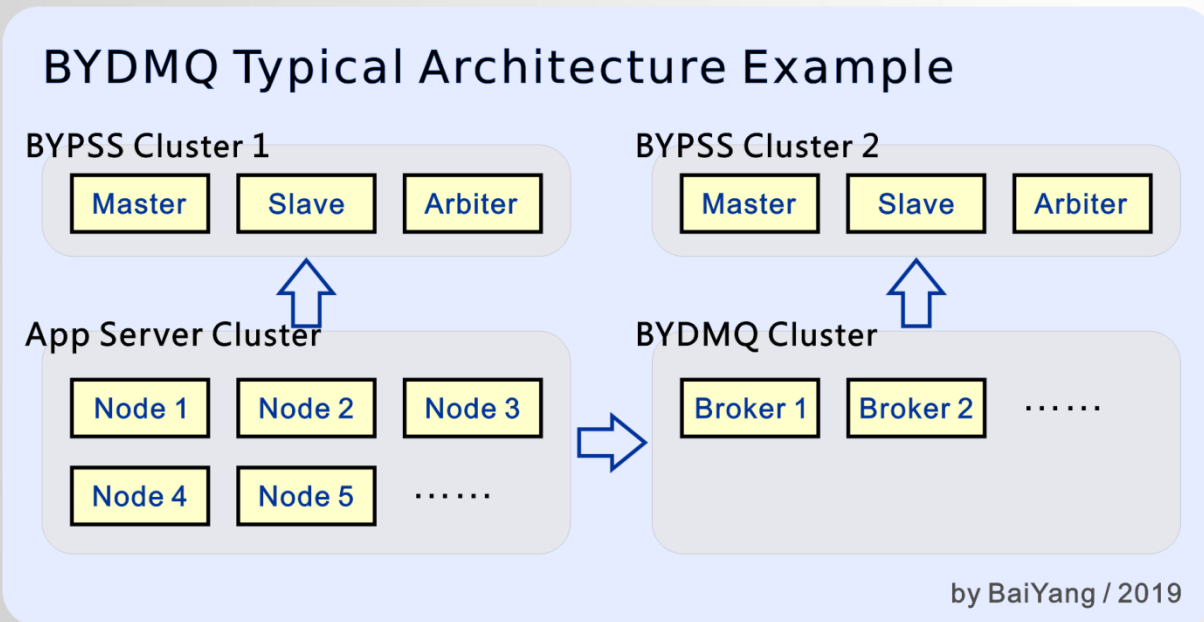
BYDMQ focuses on high-throughput, low-latency delivery of large amounts of business messages. Through the use of mature and efficient network IO components, as well as automatic message packing, pipelining and other mechanisms, it significantly reduces command processing delay, improves network throughput, 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.

30 Gbps

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

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

Safety and Reliability - High Availability Counterexamples

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

Safety and Reliability - High Availability Counterexamples

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

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的情况，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

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
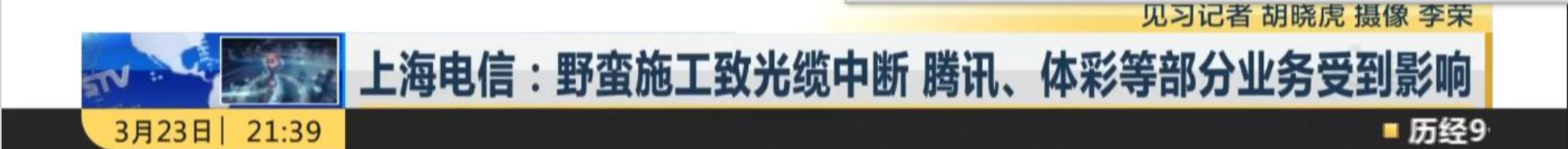
Safety and Reliability - Data Security 1

- 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

Other Product Composition

Some App / Some Website······

| Application Business Logic |

Third-party Framework

| Jboss, Struts, Spring…… |

Web Container

| Tomcat, Jetty, IIS, Apache······ |

Runtime

| JRE (Java), CLR (.NET), ZEND/HHVM (PHP)······ |

Underlying Infrastructure

| OS ······ |

| Hardware Platform (x86/x64, ARM, MIPS, POWER······) |
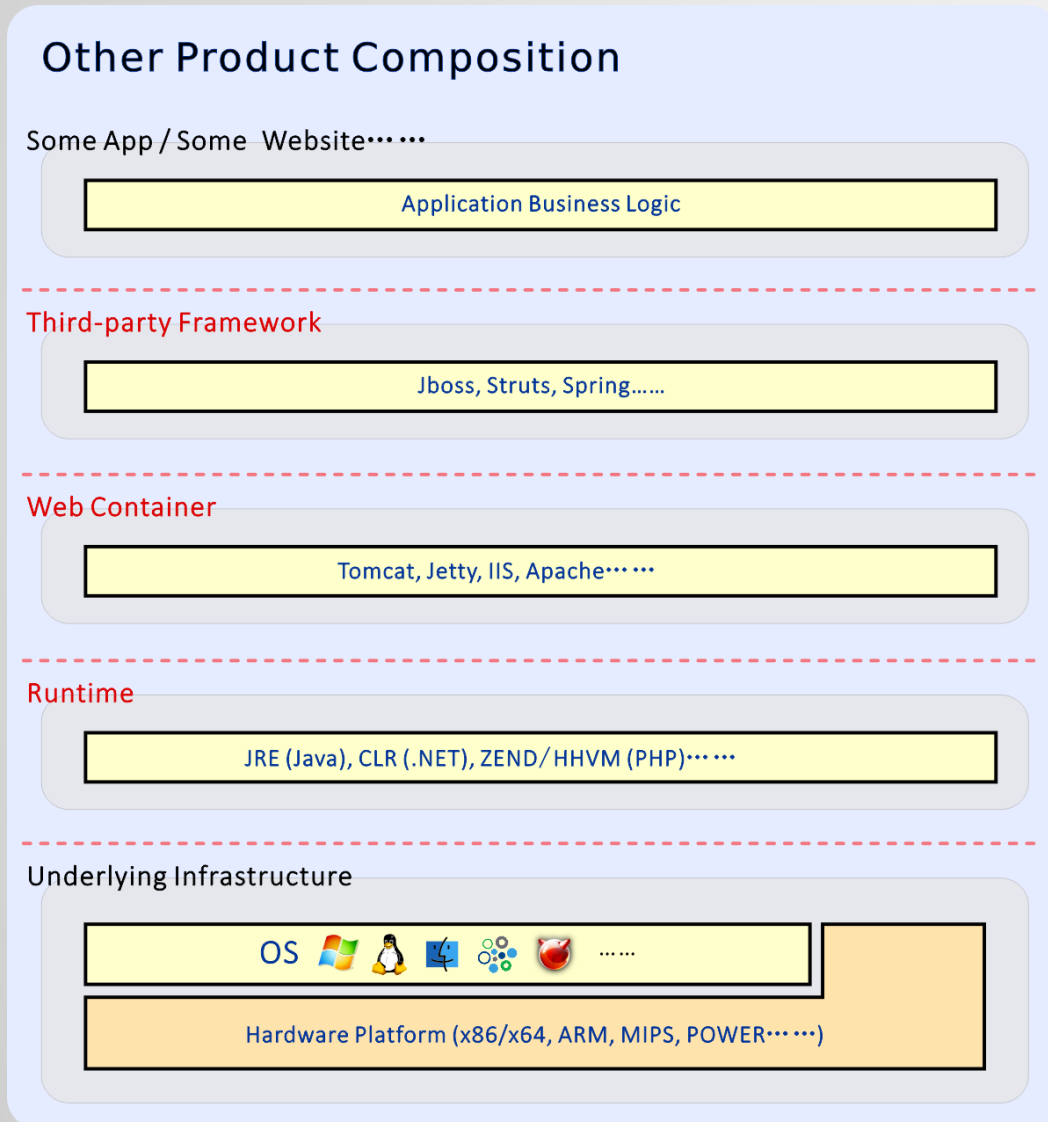
- As shown in the left figure: The dependence on dynamic runtime environments such as Java and .NET, containers such as Tomcat, and third-party frameworks such as Spring have led to the introduction of a large number of additional third-party components that are not controlled by the developer.

- 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

Product based on BaiY Application Platform

Native Code

Application Business Logic

Underlying Infrastructure

OS ......

Hardware Platform (x86/x64, ARM, MIPS, POWER·····)
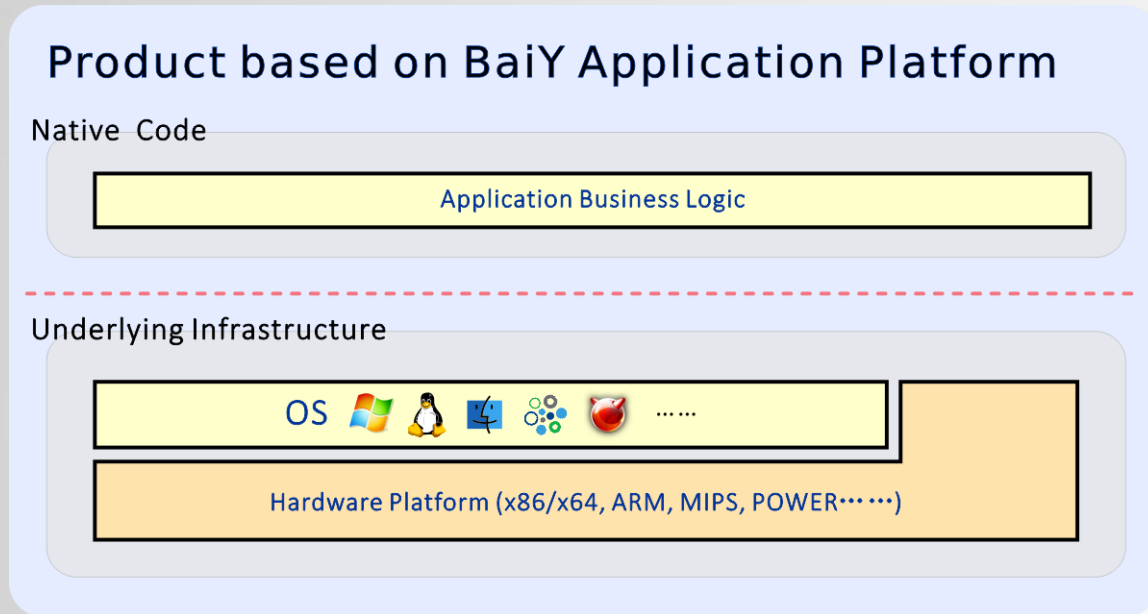
- As shown in the figure above: products based on the application platform are developed using tools such as assembly and C/C++.

- 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

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
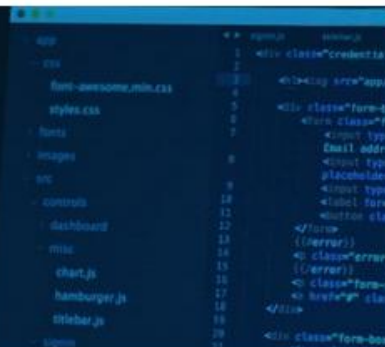
Safety and Reliability - Security Counterexamples

- A glimpse of high-risk vulnerabilities in Java

Safety and Reliability - Security Counterexamples

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

Safety and Reliability - Security Counterexamples

- Redis security flaws lead to ChatGPT leaking user privacy sessions
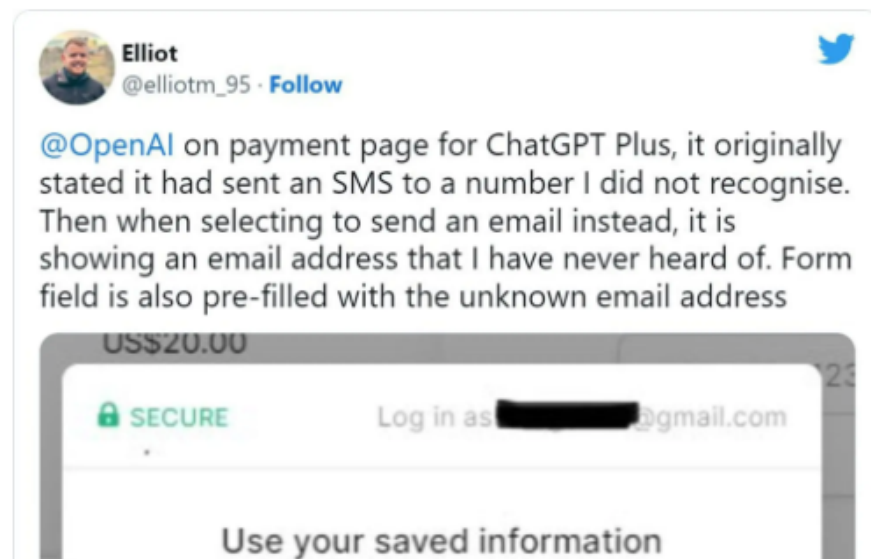
Safety and Reliability - Security Counterexamples

- 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"。目前的漏洞状态为己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

Safety and Reliability - Security Counterexamples

- Alipay leaked tens of millions of user data

Safety and Reliability - Security Counterexamples

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

Safety and Reliability - Security Counterexamples

- Uber concealed hacking and leaked data of 57 million users
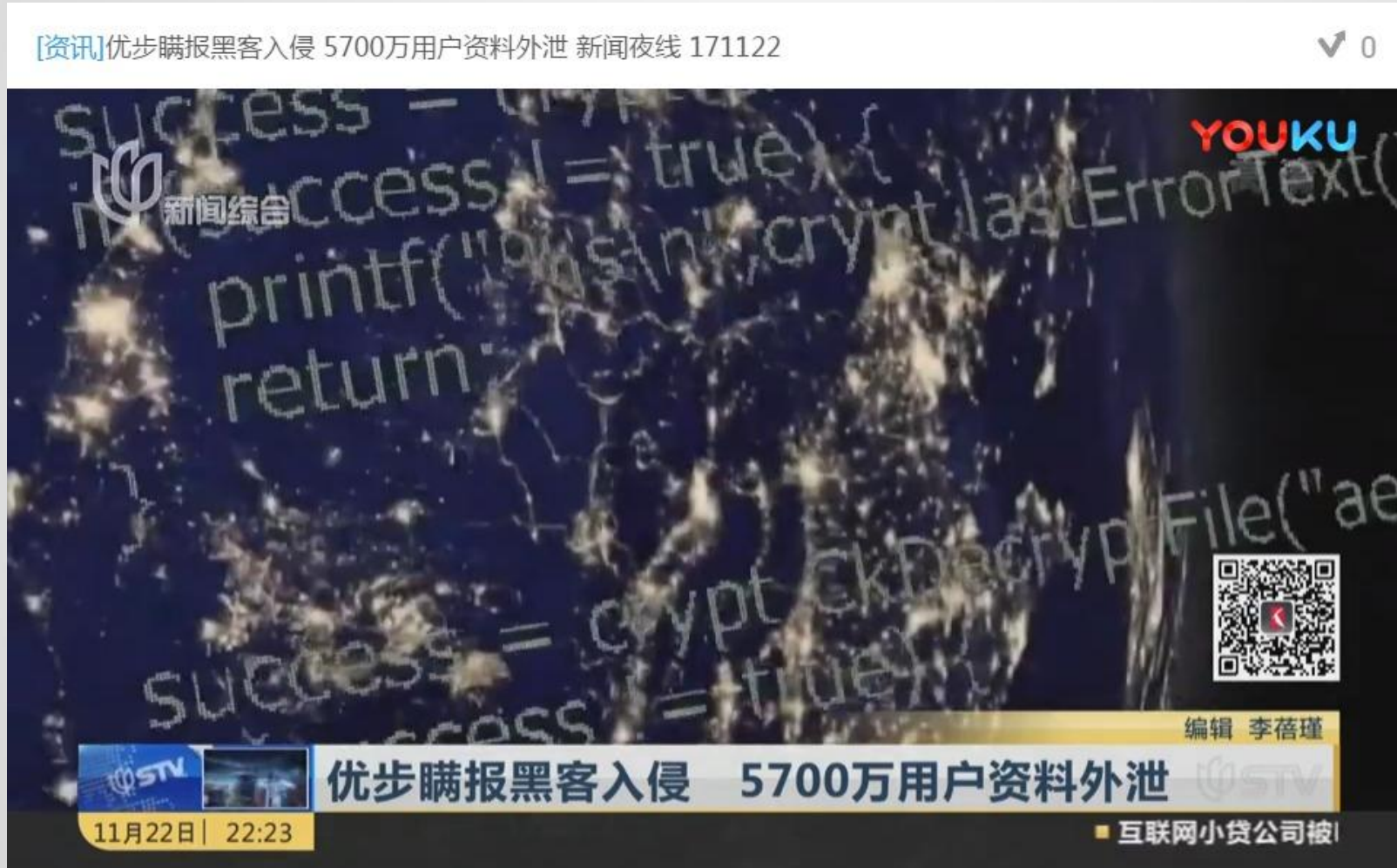
Safety and Reliability - Security Counterexamples

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

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

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

重玄科技
PHILO-TECH