HKUST Business School | Thompson Center for Business Case Studies 康信商業案例研究中心

HBP Product ID: ST32A

UST032/A/1608

KAI LUNG HUI
MINYI HUANG
PING FAN KE
ANTHONY LAI

PopVote: Assessing the Risks of DDoS (A)

> *Before the 2012 cyber-attack, we thought the system should be OK, but the attackers were so strong. We didn't expect that type of attack. It was fear. What if stronger attackers came? We did not have enough knowledge and resources to fight the cyber-war.*
>
> Robert Chung, director of Public Opinion Programme[1]

PopVote, launched in 2012, immediately became the target of a serious distributed denial of service (DDoS) attack [see **EXHIBIT 1** for background on DDoS]. PopVote was the electronic voting system used by the Public Opinion Programme (POP) at the University of Hong Kong. Jazz Ma, the IT manager of POP and architect of PopVote, had expected some form of cyber-attack on the e-voting system and had prepared accordingly. The scale of the DDoS attack, however, was completely unexpected. The university's Information Technology Services department (HKU ITS), which oversaw the IT infrastructure and support services of POP, immediately suspended the Internet connection to PopVote to protect the integrity of the university's Internet infrastructure. This had a significant impact on POP's other operations. Internet services to POP, including basic e-mail and the Computer Assisted Telephone Interview System (CATIS), resumed only two days later.

Clearly POP would have to better protect itself against cyber-attacks if it was to use the PopVote system in the future. After spending six months to systematically improve the system, POP successfully used an updated PopVote for a small-scale voting event on 1 January 2014. But the real test would come in June 2014, when PopVote was to be used to conduct an electronic vote sponsored and organized by the protest group Occupy Central, which had received significant public attention.[2] Occupy Central and the vote were

[1] Robert Chung, interview by Hui Kai Lung, Jeroen van den Berg, Ke Ping Fan, and Huang Minyi, Hong Kong, 23 September 2014.

[2] "Hong Kong votes in unofficial democracy referendum," BBC News, 20 June 2014, http://www.bbc.com/news/world-asia-china-27936340, accessed 8 September 2014.

Dr Minyi Huang, Ping-fan Ke and Anthony Lai prepared this case under the supervision of Professor Kai-lung Hui solely as a basis for class discussion. The authors may have disguised certain data to protect confidentiality. Cases are written in the past tense; this is not meant to imply that all practices, organizations, people, places or facts mentioned in the case no longer occur, exist, or apply. Cases are not intended to serve as endorsements, sources of primary data, or illustration of effective or ineffective handling of a business situation.

Inquiry on ordering and permission to reproduce the case and its materials, write to bmcase@ust.hk or visit cbcs.ust.hk

Last edited: 16 August 2016

politically controversial.[3] Robert Chung, director of POP, and Jazz expected massive cyber-attacks. They had to assess all possible security threats and consider possible solutions to ensure the vote could be conducted successfully.

Public Opinion Programme of the University of Hong Kong

Robert Chung established POP in 1991 as part of the Social Sciences Research Centre, the Faculty of Social Sciences of the University of Hong Kong.

POP used telephone, street intercept, and online surveys to collect and study public opinion on topics of interest to academics, journalists, policymakers, and the general public. It published poll results and research reports, such as quarterly reports on the popularity of the top-ten political groups in Hong Kong. Twenty full-time staff people worked for POP in 2014, including seven in senior positions [see **EXHIBIT 2** for POP's organizational chart]. Normally, they handled about 8 to 10 projects at the same time.

IT Department

Jazz was the IT manager of POP. He obtained his first degree in electronic engineering and computer science from the Chinese University of Hong Kong and his master's degree in electronic commerce and Internet computing from the University of Hong Kong. Before joining POP, Jazz had worked for the Hong Kong Federation of Youth Groups as a systems analyst for three years.

When Jazz joined POP in 2012, he had two full-time IT subordinates. His first task was to help improve the CATIS. POP used telephone surveys as its key survey tool. Telephone interviews were normally done by part-timers in the evening after all the IT staff had left the office. With an average of 50 pollsters using the phones on a typical evening, a system failure could cause significant damage.

By 2014, the POP's IT department had grown from three to four full-time staff, which included a system analyst, a programmer, a web developer, and Jazz. In addition to CATIS, the department was responsible for PopVote, the main POP website, and an online public opinion platform (POPCON).

> *We are a public opinion research institution emphasizing data accuracy, not an IT company. Most of the data held in the system are not confidential, and some survey results and sample data are available on our website. We are not too concerned with data breach, unless the data are related to personal privacy. Anyway, a system can't be 100% secure.*
>
> Jazz Ma, IT manager of POP[4]

HKU had provided the network infrastructure for POP's IT systems, until PopVote suffered from the cyber-attack in 2012. Since the network resources required to withstand the attacks were enormous, the PopVote platform was outsourced to Amazon Web Services (AWS), while other internal systems remained within the HKU ITS network.

[3] M. Yan, "June 22 poll is a political fraud by 'Occupy' heads," *China Daily*, 6 June 2014, http://www.chinadailyasia.com/opinion/2014-06/06/content_15138863.html, accessed on 8 September 2014.

[4] Jazz Ma, interview by Hui Kai Lung, Jeroen van den Berg, Ke Ping Fan, and Huang Minyi, Hong Kong, 23 September 2014.

PopVote

The version of PopVote used for the voting on 23 March 2012 was developed by Jazz with the help of two full-time developers and one part-time developer in less than three months. When designing the system, they wanted to ensure that the system was available during the event period, would prevent duplicate votes, and would verify the voter's identity[5] [see **EXHIBIT 3** for PopVote system design].

23 March 2012 Vote[6]

Voting Arrangements

On 8 February 2012, HKU POP held a press conference to announce its first e-voting event to be held on 23 March 2012. To promote the event, it built a PopVote website and started a promotion campaign using a Facebook page, video clips, posters, flyers, and banners.

The targeted voters were Hong Kong permanent residents[7] aged 18 and older. To familiarize the public with PopVote and online voting in general, POP conducted two phases of public testing, from 16 to 20 March and on 21 March, respectively. The first phase was a performance test to check the system's stability and responsiveness by allowing those people who were interested in testing to enter the system and vote once per hour. The second phase was a functional test conducted by staff to ensure the different functionalities of the system worked as required.

Voters could choose between off-site and on-site e-voting. If voting off-site, participants could vote through the PopVote website or mobile applications[8] between 00:00 and 20:00 on 23 March. They had to follow the instructions on the screen by entering their HKID[9] and mobile numbers and declaring their eligibility to vote by ticking a box on the screen. After submitting this information, they would see a telephone number displayed on the screen. They were given three minutes to send a blank SMS to the given telephone number for verification. If successful, they could enter the voting interface to cast their votes.

To vote on-site, voters had to visit a designated polling station between 09:00 and 21:00 on 23 March. Station staff used voters' HKID cards to verify their identities and entered their HKID card information into the system. Voters could then proceed to voting booths where they could vote electronically. The e-voting system in polling stations was installed with a log-on mechanism, which allowed only station staff to log on to the e-voting system right before the polling stations started running, using an ID and password provided by POP.

To avoid double-voting, the online system displayed the message "duplicated vote" if a voter's HKID card number or mobile number had already been registered and used for voting, no matter whether the previous vote was done off-site or in a polling station. If a voter cast his or her first vote off-site, the system

[5] Jazz Ma, Winnie Lee and Robert Chung, "PopVote: A Revolution in Gathering Opinions in Hong Kong," World Association for Public Opinion Research (WAPOR) 66th Annual Conference, Boston, May 14-16, 2013.

[6] This voting event was named by the event organizers "3.23 Civil Referendum."

[7] HK permanent residents refers to those who were born in Hong Kong or continuously live in Hong Kong for no less than seven years, no matter whether they have Chinese nationality or not.

[8] Mobile applications had iOS and Android versions.

[9] HKID refers to Hong Kong Identity Cards. All Hong Kong residents aged 11 or over are required to register for an identity card that contains their name, date of birth, residency status, photo, and a unique identification number.

allowed the voter to vote again in the polling station to replace the previous vote, using the same HKID card. POP believed that on-site voting was the most reliable voting method.

Several measures, such as a virtual keyboard and a Secure Sockets Layer (SSL) connection, were used to protect voters' personal information. Data were also hashed and encrypted to prevent hackers from obtaining voters' HKID numbers. All processed data were stored only in the system, and all personal information was destroyed after the 23 March vote.[10]

The system had four servers, two cloud and two physical. All of them were located on the HKU campus and protected by the security facilities of HKU ITS. HKU's external network was equipped with a firewall and an intrusion detection and prevention system. The system used the Linux platform. The firewall of the platform opened only relevant ports for websites to connect.

Cyber-Attacks and Responses

On 21 March, during the second phase of testing, HKU ITS found that POP's server was under suspected DDoS attacks at a speed of 1 million requests per second and notified POP.[11] POP referred the attack to the network service provider, which implemented measures to successfully block the abnormal data transfer.[12]

On 22 March, two POP IT staff e-mail accounts were hacked twice in succession. After the passwords were changed, someone logged into one of the accounts from an unknown Internet Protocol (IP) address.[13] The hackers might have wanted to plant malware on the staff's machines or to steal important system information, such as the system's infrastructure design.[14]

Off-site Voting

The official voting commenced at 00:00 a.m. on 23 March. At 3 a.m., a DDoS attack took place that paralyzed the system for 15 minutes.[15] Around 7 a.m., the voting website came to a complete halt as a result of the DDoS attacks. Voters were unable to log on to the website or carry out SMS verification.

Meanwhile, POP made the following attempts to repair the system:[16]

- Reduced the system workload by optimizing and removing irrelevant web data.
- Reduced the use of system resources by giving lower priority to the SMS verification process.
- Tightened the firewall connection limit.
- Investigated the root cause of the problem by examining the system record.
- Double-checked the source code of the system to ensure it contained no error.
- Prepared for immediate reallocation by renting four more cloud servers from HKU ITS.

[10] HKU POP, "3.23 Civil Referendum Project Activity Report," 23 May 2012.

[11] HKU POP, "Contingency Plan Invoked for '6.22 Civil Referendum,'" Public Opinion Programme, University of Hong Kong, 18 June 2014, http://hkupop.hku.hk/english/release/release1152.html, accessed 8 September 2014.

[12] HKU POP, "3.23 Civil Referendum Project Activity Report."

[13] HKU POP, "Contingency Plan Invoked for '6.22 Civil Referendum.'"

[14] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."

[15] Ming Pao, "Voting Site Got Attacked," 24 March 2012, http://news.sina.com.hk/news/20120324/-1-2616158/1.html, accessed 8 September 2014.

[16] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."

At 17:00, invited IT security experts arrived and, after four hours, successfully stabilized the system at 21:00. Since the scheduled e-voting ended at 20:00, those people who intended to vote off-site but did not vote between 0:00 and 7:00 had lost the opportunity to do so.

On-site Voting

At the polling stations at 8 a.m., station staff found that there was a problem connecting to the system located in the POP office. They were either unable to connect to the server or got disconnected intermittently. Since the location of the server was not disclosed to the public, the POP IT team knew the connection problems could be caused by errors when typing the website address, mobile network reception problems, inappropriate firewall settings, or vicious attacks. POP immediately modified the firewall, only allowing selected fixed lines or station staff mobiles' IP addresses to access POP's servers. By the time the problem was alleviated at around 11:00 a.m., most polling stations had already made the decision to close. [17]

Press Conference

POP decided to hold a press conference at noon on 23 March to inform the media of the situation and announce the switch to paper ballot voting in polling stations in the afternoon until the e-voting system recovered. In paper ballot voting, the voter first marked his or her vote clearly on a piece of paper and wrote his or her HKID card number on top of an envelope. Then, the voter put the paper into the envelope and sealed it. Finally, the voter put the envelope into the ballot box after HKID card verification by station staff. In a follow-up press conference, held at 22:00, POP announced it would extend the voting time for both on-site and off-site voting by one day, simultaneously ending at 18:00 on 24 March.[18]

On 24 March, online voting was relatively smooth and any remaining log-on problems were caused mainly by general network congestion. E-voting also resumed in the polling stations.

Reflections on the March 23 Voting

After hours of investigation, IT security experts found that four suspected IP addresses launched DDoS attacks on the system.[19] POP reported the case to the Hong Kong Police Force, which later arrested two males. One was convicted of criminal damage and given an order of 160 hours of service.[20]

Reflecting on the design of the PopVote system, the IT community in Hong Kong discussed and suggested how to improve the system:

- The SMS verification process slowed down mobile and website applications. Automatic timeout and the attempts to log in led to heavy website traffic, creating a small-scale "One DDoS oneself" [21] [see **EXHIBIT 4** for related comments].

[17] HKU POP, "3.23 Civil Referendum Project Activity Report."
[18] HKU POP, "3.23 Civil Referendum Project Activity Report."
[19] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."
[20] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."
[21] Charles Mok, "Facebook Comments," 22 March 2012, https://www.facebook.com/charles.mok/posts/10150865795529186, accessed 8 September 2014.

- The real traffic and self-feedback loop were underestimated when designing the system. A robust system should have been designed to tolerate peak usage and a certain level of DDoS.[22] In terms of software, a lightweight and efficient language, such as Node.js, to handle web requests was recommended.[23]
- The programming of the voting website was relatively weak. There should have been functions to allow the system to filter and block those Internet addresses that abnormally contacted the website during a short time.[24]
- To improve security, POP should have used more secure hashing [see the **Glossary**]. For example, adding a random salt to data before hashing would make it difficult to work out the original data by the hashed pattern. After iterating the hashing process several times, the difficulty of hacking would increase.[25]
- POP should not have revealed the website's real address to the public.[26] The suggestion was that POP have a fault-tolerant system. Once the system failed, it could continue to operate, such as by displaying the status of the server to the web visitors.[27]
- POP should have more external support. Since HKU ITS had been incapable of handling the attacks, POP should have used cloud service providers with reliable firewalls and cloud-filtering techniques to help to defeat attacks.
- POP should not have delayed in reporting to the police, no matter how short the attack. Instead, the police should have been contacted immediately, as the personal details of online voters might have been stolen by the hackers.[28]

After this event, POP believed that preparing paper ballots in advance for emergency use would be a good idea, just in case the e-voting system underwent severe disruptions or was unavailable. The paper ballot system might also suit those citizens who were unfamiliar with e-voting or had no confidence in it.[29]

April 2013 to December 2014: Improving the System

System Improvements

> *In terms of management and manpower . . . we just didn't have enough manpower, even when designing the system, because it is a huge system prone to attacks. We need IT experts, but we could not afford to hire them. To overcome this challenge, we established the IT Advisory Group. They are volunteers. . . . The group should help us to redesign and enhance the e-voting system.*
>
> —Robert Chung, director of POP[30]

In a press conference on 23 January 2013, POP announced the establishment of the IT Advisory Group of PopVote [see **EXHIBIT 5** for the list of advisers] to strengthen the cooperation between POP and the IT

[22] Mok, "Facebook Comments."
[23] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."
[24] Pao, "Voting Site Got Attacked."
[25] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."
[26] Pao, "Voting Site Got Attacked."
[27] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."
[28] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."
[29] Ma et al., "PopVote: A Revolution in Gathering Opinions in Hong Kong."
[30] Chung, interview by Hui Kai Lung et al.

sector. Supported by the IT Advisory Group, Jazz and his team spent about six months making improvements to the PopVote system. They wanted to ensure that PopVote could withstand possible future attacks aimed at paralyzing the system and stealing or changing information.

Changes included rewriting the system using another programming language—Python—that was more scalable, offered more functionality, and was easier to manage. More secure hashing was implemented to ensure that the data were transferred safely without being intercepted or modified.

Jazz and the team moved the PopVote system to a cloud server provider, AWS, to speed up data handling and cope with a sudden increase of network traffic. The system was uploaded to a cloud server, which had an integrated firewall to block DDoS attacks. At the same time, they integrated the system with security service providers' network monitoring and real-time blocking equipment. They also developed a real-time system-monitoring platform that allowed staff to monitor real-time network usage. When encountering extraordinary network traffic, staff could take immediate action.

They used modular designs to break the system into subsystems with different functionality, including a verification code check function, application programming interface request processing, electronic queuing, receiving SMS messages, physical polling stations data exchange, vote count, and system logging and monitoring. Using more than 40 servers, this modular design strengthened the system's ability to manage usage allocation and, when a subsystem was under attack, minimized its impact on the whole system.

As for improving the verification process for off-site voting, POP considered several options, namely:

Electronic certification. This option was declined because of the low popularity of the personal electronic certificate in Hong Kong and a compatibility problem with mobile applications.

Registering voters beforehand, which allowed them to check the validity of their HKID cards in person and distribute voting passwords. But Hong Kong had more than 3 million registered voters. There were not enough resources to set up adequate registration booths.

Requiring voters to upload their HKID card copies, which would be automatically checked by the system. But the team gave up this idea, because the voters had to go through a complicated verification process and submit very detailed personal information, which raised security and privacy concerns.

After balancing the pros and cons of each option, Jazz and the team decided to maintain the original mobile messaging method for ID verification for two reasons. First, the uniqueness of the HKID card number ensured one person, one vote. The HKID card had a check digit in brackets to facilitate computer processing, which was the only way to check the number's validity. But using HKID card numbers alone had its limitations. Nongovernment organizations, including POP, were unable to access the government databases that provided personal information for HKID cardholders. The HKID number itself contained no information about a person's identity and age. Tools were available to generate "valid" HKID card numbers, which people could use to fool the system. Jazz hoped that people would not purposely do this in a civil society.[31]

Second, since the vast majority of people owned a mobile phone, the project team found that a mobile SMS onetime password (OTP) was often used by sizable websites to prevent the abuse of network resources and to ensure that the registered person really existed and had only one account. Therefore, combined with

[31] Jazz Ma, "A study of 'Civil Referendum Voting Programme' Electronic Voting System," *Media Digest,* February 2014.

SMS authentication, the system could significantly reduce the number of nonexistent users.[32] Once the team made a decision, they discussed their requirements with the SMS service provider in order to choose a suitable text-messaging service package to improve the identity verification process.

They also decided to prepare back-up paper ballots for future e-voting events, in case technical failure or malicious attacks took place.

2014 New Year Vote[33]

The 2014 New Year Vote was organized by POP and the Centre for Social Policy Study of the Hong Kong Polytechnic University to encourage the general public to express views on the principles for electing the chief executive and to learn to use the e-voting system.

Though the voting arrangements were similar to those in 2012 and offered the voters on-site and off-site voting options, there were some differences.[34]

Since both on-site and off-site data management depended on the system, if the system had problems, it could affect the normal operation of on-site polling stations. Therefore, the project team placed servers in the polling stations and wrote the same information security programs, which allowed the polling stations' servers to work independently without connecting to the Internet. Even if the system was under cyber-attack, the polling stations were still able to operate normally. When the servers from the polling stations were connected to the system successfully, the hashed personal information and encrypted voting information would be automatically transferred to the system and saved.

Only three authorized, nontechnical personnel had the partial decryption keys to access the database. In order to read the vote data from the electronic voting box, two of the three keys had to be used at the same time. This design was to prevent the loss and theft of keys.

On voting day, the system was running smoothly. Among approximately 62,000 votes received, over 40,000 were made using mobile applications and more than 19,000 voted via the website[35].

Reflections on the 2014 New Year Voting

After reflecting on the voting event, POP was considering possible ways to improve PopVote.[36]

In terms of the SMS verification process, the integration of mobile message distribution and the system was not adequate. The speed of sending out mobile messages was relatively slow, and most voter complaints were related to the long waiting time when sending and receiving SMS messages. The system had an electronic queuing mechanism to allocate vote quota and to arrange voting. If it took longer than three minutes to complete the verification process, the system's electronic queuing mechanism would immediately start a people clearance management process. The delay of SMS messages meant some voters were unable

[32] Ma, "A study of 'Civil Referendum Voting Programme' Electronic Voting System."

[33] Event organizers called this voting event "New Year Civil Referendum."

[34] HKU POP, "Arrangements for the 'New Year Civil Referendum," 27 December 2013, http://hkupop.hku.hk/english/release/release1092.html, accessed 8 September 2014.

[35] Ma, "A study of 'Civil Referendum Voting Programme' Electronic Voting System."

[36] Ma, "A study of 'Civil Referendum Voting Programme' Electronic Voting System."

to complete the verification process, which was a waste of time and messaging costs [see **EXHIBIT 6** for off-site voting verification process].

To solve this problem, POP was considering the possibility of enhancing cooperation with the SMS service provider by choosing more scalable and more effective SMS services. The team was also considering possible longer verification times, more people allowed by the system, and the addition of a reminder function to the verification process. When the system received the mobile message, it would automatically remind the votes to enter the voting interface, without the need to pay attention to the verification interface. Additionally, POP was looking into alternative verification methods to replace mobile messaging services. To solve this problem, POP was considering an increase in the number of people allowed in the system by expanding the system's voting quotas.

In terms of participation, the system was connected directly with Hong Kong Internet Exchange Centre via an Internet security company, which allowed only HK local networks to enter for security reasons. On the voting day, some HK citizens overseas expressed their willingness to vote through non-HK networks. POP also considered whether to set up a server especially to serve non-HK networks; then the two systems could bear different security risks.

What Next?

The June vote[37] was sponsored and organized by the protest group Occupy Central to draw attention to its civil disobedience movement. It encouraged the public to participate in the vote as a way to support candidate nomination by universal suffrage in the 2017 chief executive election. Occupy Central and the vote were legally and politically controversial. The mock vote and preregistration of the June vote were scheduled to start on 13 June with the actual voting to take place from 20 to 22 June.

Jazz and Robert had a brainstorm meeting with the members of the IT Advisory Group. Based on past experience [see **EXHIBIT 7** for the timeline of major events], they felt it was likely PopVote would be the target of cyber-attacks to disrupt the vote.

Jazz and the advisory group had limited time to identify all possible security threats and ensure solutions were in place. After the meeting, Jazz was considering various options that would ensure the smooth operation of the mock voting on 13 June. How could they assess the potential risks systematically and properly address these risks? How could he justify his recommendations to the various stakeholders?

[37] The voting event was named by the event organizers the "6.22 Civil Referendum."

EXHIBIT 1: DDoS ATTACKS

Distributed denial of service (DDoS) attacks attempt to consume all available resources of a target computer system so that it cannot handle service requests from legitimate users. Typically, DDoS attacks are executed by a robot network, or "botnet," containing a large number of "zombies," or Trojan-infected computers, which can be remotely accessed and controlled by a hacker without the knowledge of their owners.[38] The zombies receive instructions from a command-and-control (C&C) server to bombard the target computer system simultaneously with a large number of service requests. The target system can become too busy responding to these malicious requests and so will be unable to handle legitimate users' requests. This results in long delays and sometimes complete service outage.[39]

DDoS attacks take advantage of the characteristics of the Internet. Designed as a simple, fast, data communications network with high bandwidth, the Internet moves packets around quickly but cannot detect and stop misbehavior in the absence of a global security and privacy management mechanism.[40] The security of a system on the Internet depends not only on in-house investments in firewalls, intrusion detection systems, network vulnerability scanners, and encryption technologies, but also on the security of other systems, because the Internet facilitates autonomous data transmission among organizations.[41] User-friendly DDoS tools available online and an increasing number of personal computers adopting high-bandwidth, always-on Internet-access technologies make DDoS attacks easier. At the same time, the distributed nature of DDoS and IP spoofing make it very difficult to identify and trace the hackers.

To defend against DDoS attacks, some people suggest using cloud computing because cloud providers with a global network of traffic scrubbing centers can help detect and mitigate large-scale attacks. An organization can also engage cloud security service providers that have the scale and professional skills to help fight the battle. Internet service providers (ISPs) and anti-DDoS service providers may also help. Though there is no silver bullet, organizations should plan ahead and invest in redundant servers, data monitoring, log-inspection tools, and IT training to mitigate the impacts from DDoS attacks.[42]

DDoS attacks can be categorized into four types:[43]

- TCP (transmission control protocol) connection attacks aim at occupying all the available connections in infrastructure devices, like load-balances, firewalls, and application servers.
- Volumetric attacks aim at using up the bandwidth either within the target system or between the target system and the rest of the Internet.
- Fragmentation attacks aim at overwhelming the target system's ability to reassemble the streams by sending a flood of TCP or user datagram protocol (UDP) fragments.

[38] The only difference a user might notice is that the computer is not working as fast as it used to when it was engaging in a DDoS attack.

[39] Prolexic, "What is DDoS denial of service?," 2014, http://www.prolexic.com/knowledge-center-what-is-ddos-denial-of-service.html, accessed 8 September 2014.

[40] Jelena Mirkovic and Peter Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," *ACM SIGCOMM Computer Communication Review* 34, no. 2 (2004): 39–53.

[41] Lee Garber, "Denial-of-Service Attacks Rip the Internet," 2000, ftp://mail.im.tku.edu.tw/assistant/bearhero/00839316.pdf, accessed 8 September 2014.

[42] S. Lam and C. Ko, "The PopVote attack aftermath," *Computerworld Hong Kong,* July/August 2014, pp. 30–31.

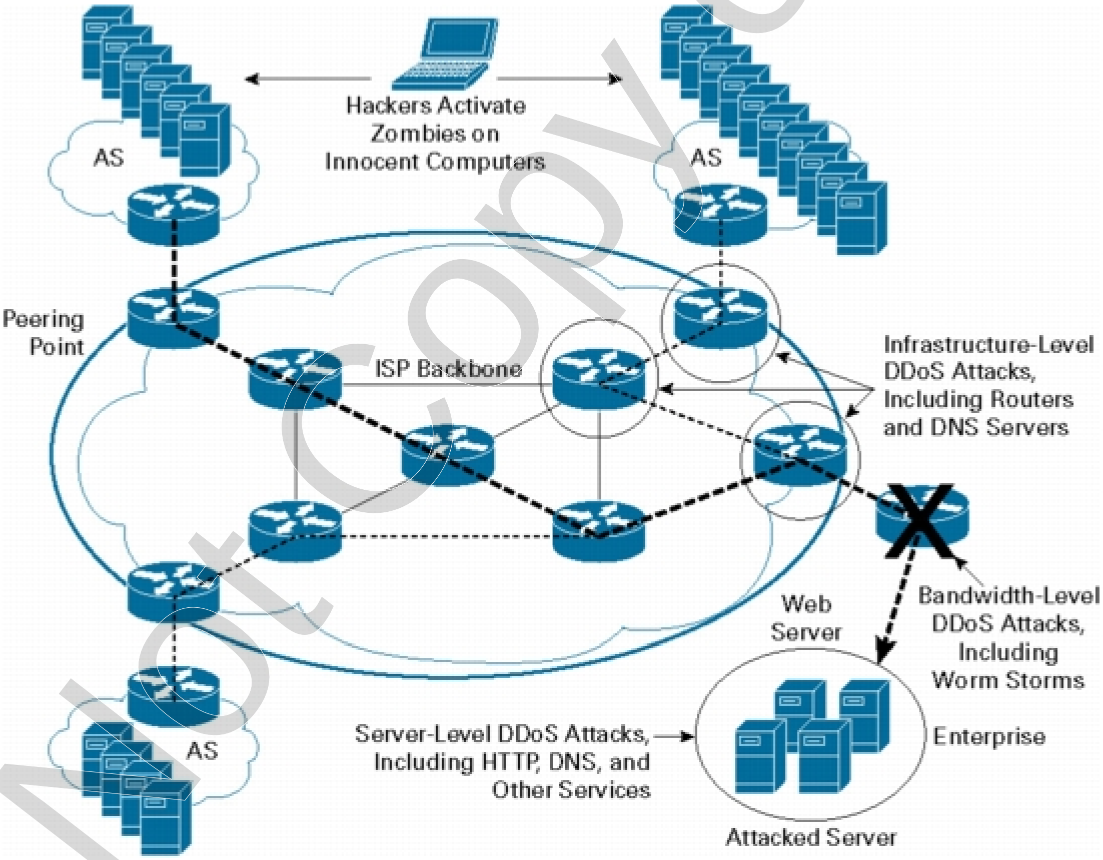
[43] Digital Attack Map, "What is a DDoS Attack?," 2014, http://www.digitalattackmap.com/understanding-ddos/, accessed 8 September 2014.

- Application attacks aim at attacking a specific aspect of an application or service, which could be effectively achieved using very few attacking machines generating a low traffic rate. This makes it very difficult to detect and mitigate.

Besides using botnet, attackers can multiply the attack traffic in the following two ways:

- DNS (domain name system) reflection forges the target system's IP address to send small requests to its botnet, overwhelming the target system with large replies that can be amplified as much as 70 times the size of the original requests.[44]
- Chargen reflection uses Chargen, an outdated testing service supported by most computers and Internet-connected printers to ask the target system to reply with a steady stream of random characters.[45]

The diagram below shows a system's vulnerable points prone to DDoS attacks.


AS
Hackers Activate Zombies on Innocent Computers
AS
Peering Point
ISP Backbone
Infrastructure-Level DDoS Attacks, Including Routers and DNS Servers
Web Server
Bandwidth-Level DDoS Attacks, Including Worm Storms
Server-Level DDoS Attacks, Including HTTP, DNS, and Other Services
Enterprise
AS
Attacked Server

Sources: Adopted from the website of CISCO. Cisco, "Defeating DDoS Attacks," 2004, http://www.cisco.com/c/en/us/products/collateral/security/traffic-anomaly-detector-xt-5600a/prod_white_paper0900aecd8011e927.html, accessed 8 September 2014.

[44] Digital Attack Map, "What is a DDoS Attack?"

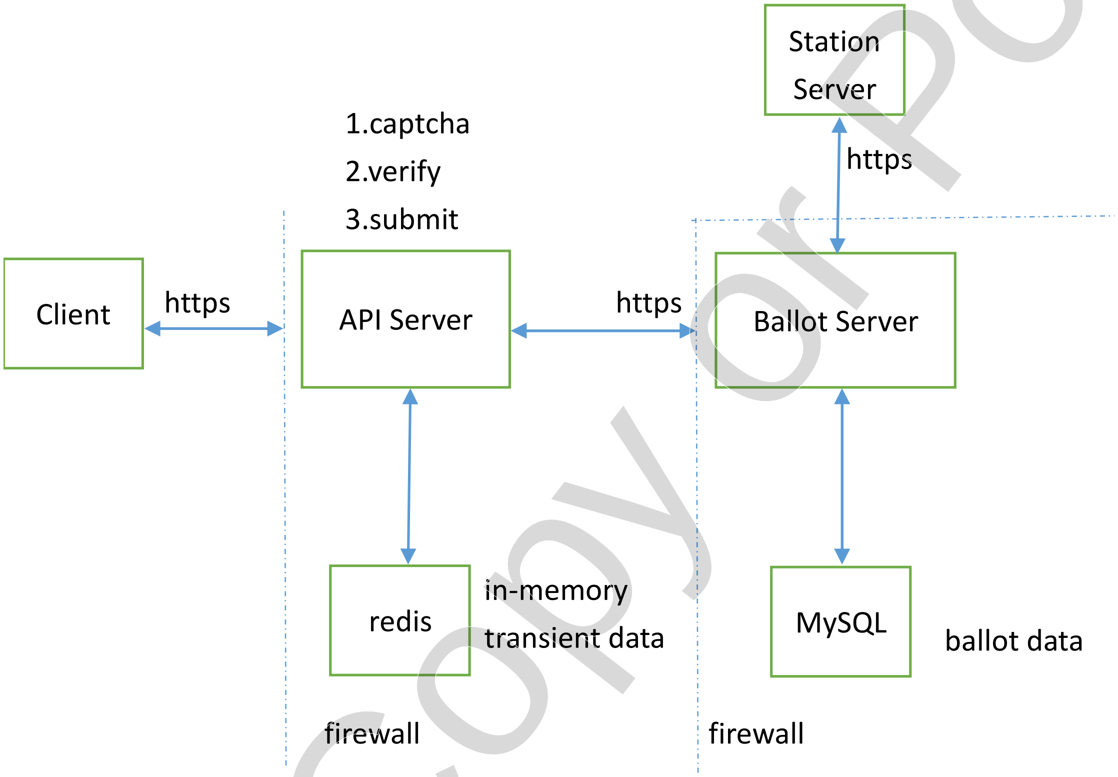
[45] Digital Attack Map, "What is a DDoS Attack?"

EXHIBIT 2: POP ORGANIZATIONAL CHART

Director	Robert Ting-Yiu Chung
Secretary	A. Lai
Clerical assistants	E. Ching
	R. So
Assistant Director	K. Pang
IT manager	Jazz Ma
System analyst	S. Lau
Programmer	F. Chan
Web developer	O. Yau
Research managers	F. Lee
	W. Lee
Research executives	J. Chan
	J. Li
	K. Chan
Research project assistant	S. Chu
Supervisors	K. Chan
	P. Wong
Senior data analyst	E. Tai
Senior statistical analyst	K. Yu
Statistical assistant	J. Yiu

Source: POP, "Team Members," 2014, http://hkupop.hku.hk/english/aboutpop/teams.html, accessed 8 September 2014.

EXHIBIT 3: POPVOTE SYSTEM DESIGN



Source: Adapted from Patrick Cheung, "Coding PopVote," PopVote System Technical Seminar, 20 September 2014, Hong Kong Polytechnic University, Hong Kong.

EXHIBIT 4: A PUBLIC VIEW OF HANDLING THE ATTACK

This time Dr. Chung Ting-Yiu, director of HKU POP, was responsible for organizing "3.23 Civil Referendum," and so far my views on the cyber-attack issues are: first, website and mobile application delays were mainly caused by the long waiting time during the SMS verification process, because automatic timeout as well as log-in and relog-in attempts proliferated the network traffic, resulting in the system's small-scale "DDoS itself." Additionally, the server might not be designed to accommodate such a high network traffic and self-feedback loop. This is the system's problem rather than an attack from outside the system. Second, DDoS attacks did exist and, as far as I know, came from inside and outside Hong Kong. But the system was already protected by HKU's network, which should have filtered the attacks. But I don't have the detailed information myself in this regard.

Our IT Voice 2012 made suggestions to POP, but they were responsible for the operations. We will continue to keep an eye on the situation and provide necessary assistance. We would suggest POP consider reporting to the police, especially if there is evidence to show the attacks are local or overseas. We also want to remind POP's colleagues of carefully keeping all the relevant evidence.

Sources: Charles Mok, "Facebook Comments," Chinese to English trans., 22 March 2012,
https://www.facebook.com/charles.mok/posts/10150865795529186, accessed 8 September 2014.

EXHIBIT 5: IT ADVISORY GROUP

Convenor of IT Advisory Group

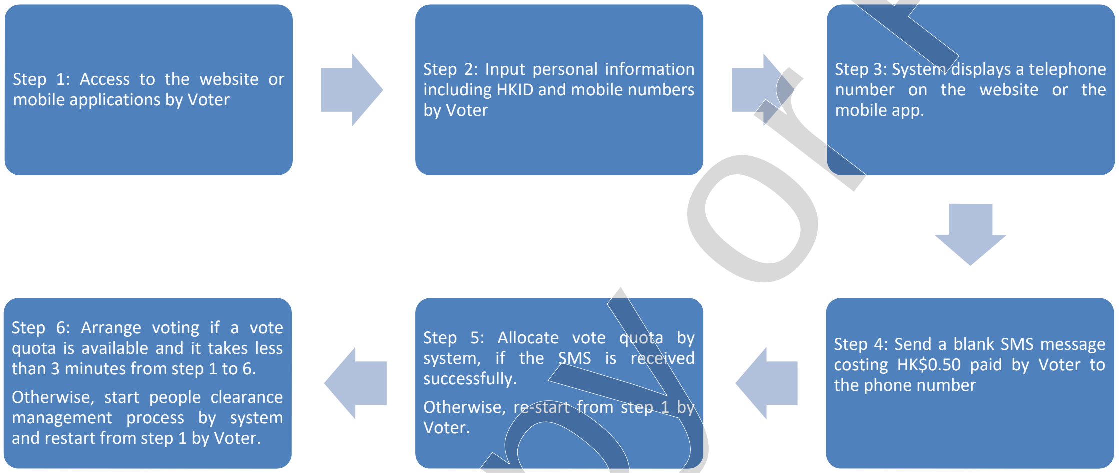
Mr. S. C. Leung	Director, Internet Society Hong Kong

Members

Dr. K. P. Chow	Department of Computer Science, University of Hong Kong
Dr. Joe C. K. Yau	Department of Computer Science, Hong Kong Baptist University
Dr. Ricci Ieong	Director, Cloud Security Alliance HK & Macau Chapter
Mr. Henry Ng	Head of Consulting Service of an international consultancy firm
Mr. Vincent Ip	Council Member of Information Security and Forensics Society
Mr. Eric Fan	Vice Chairperson, Professional Information Security Association
Mr. Chester Soong	Chairperson, Internet Society Hong Kong
Mr. Ben Cheng	Vice Chairperson, Convenor, Startup Working Group, Internet Society Hong Kong
Mr. Sang Young	Director, Education; Convenor, Security & Privacy Working Group, Internet Society Hong Kong
Mr. Ken Lam	Director; Convenor, Internet Application Development Working Group, Internet Society Hong Kong)

Source: Jazz Ma, "POP Vote Technical Sharing Seminar," 22 September 2014, Hong Kong Polytechnic University, Hong Kong.

EXIBIT 6: OFF-SITE VOTING VERIFICATION PROCESS



Step 1: Access to the website or mobile applications by Voter

Step 2: Input personal information including HKID and mobile numbers by Voter

Step 3: System displays a telephone number on the website or the mobile app.

Step 4: Send a blank SMS message costing HK$0.50 paid by Voter to the phone number

Step 5: Allocate vote quota by system, if the SMS is received successfully.

Otherwise, re-start from step 1 by Voter.

Step 6: Arrange voting if a vote quota is available and it takes less than 3 minutes from step 1 to 6.

Otherwise, start people clearance management process by system and restart from step 1 by Voter.

EXIBIT 7: TIMELINE FOR MAJOR EVENTS

08 Feb 2012	POP announced to hold its first e-voting event on 22 March.
21 Mar 2012	POP’s server discovered an attack, and the network service provider solved the problem.
22 Mar 2012	Two IT staff’s e-mail accounts were hacked in succession.
23 Mar 2012	At 00:00, off-site voting using websites or mobile applications started. At 03:00, an attack came and paralyzed the system for 15 minutes. At 07:00, the system stopped working. At 08:00, ballot stations had problems connecting to the server in POP’s office. At 09:00, on-site voting was planned to start. At 11:00, mobile connection problems at ballot stations were solved. At 12:00, in a press conference, POP announced switch to paper ballots. At 21:00, IT experts successfully stabilized the system. At 22:00, POP announced extension of both on-site and off-site voting for one day.
24 Mar 2012	At 18:00, both on-site and off-site voting ended.
23 Jan 2013	POP announced the enhancement of PopVote and established the IT Advisory Group.
12 Mar 2013	A man was arrested and convicted of criminal damage in relation to the DDoS attacks in 2012.
1 Jan 2014	New Year Voting Event sponsored by Occupy Central Secretariat was held.

GLOSSARY

Anti-DDoS Service Providers

Anti-DDoS service providers, or DDoS mitigation service providers, use network appliances and intrusion detection systems to prevent the client's server network and application from being interrupted by DDoS attacks.

Cloud Computing[46]

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud Security Service Provider

Different from cloud providers that offer clients a computing platform such as operating system and web server, cloud security service providers offer cloud-based security services to customers, such as identity and access management, remote vulnerability assessment, and security information and event management.

E-Certificate or Digital Certificate[47]

Public-key container files that allow computer programs to validate the key and identify to whom it belongs.

Fault-tolerant System[48]

A fault-tolerant system is designed from the ground up for reliability by building multiples of all critical components, such as CPUs, memories, disks, and power supplies into the same computer. In the event one component fails, another takes over without skipping a beat.

Firewall

Firewalls examine each incoming and outgoing network packet and determine whether to forward it toward its destination, based on a set of predefined security rules. Firewalls can be hardware or software based and are designed to protect networks against hackers, viruses, worms, and other malicious traffic.

[46] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Special Publication 800-145, National Institution of Standards and Technology, US Department of Commerce, 2011.

[47] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 4th ed. (Singapore: Course Technology, 2012), p. 586.

[48] "Definition of fault tolerant," *PC Magazine*, 2014, http://www.pcmag.com/encyclopedia/term/43036/fault-tolerant, accessed 18 September 2014.

Hackers

Hackers are advanced computer users who use their IT skills to discover and exploit vulnerabilities in electronics, IT systems, and computer networks.

Hash[49]

The hash function is often incorporated into cryptosystems. Hash functions are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a specific message and to confirm that there have not been any changes to the content.

Modification Attack[50]

Modification attacks occur when someone makes unauthorized modifications to code or data, attacking its integrity.

Salt[51]

A salt is a random string used in conjunction with a password to make offline password-guessing attacks more difficult.

Source: Unless otherwise referenced, adopted from Prolexic, "DoS and DDoS Glossary of Terms," 2014, http://www.prolexic.com/knowledge-center-dos-and-ddos-glossary.html, accessed 8 September 2014.

[49] Whitman and Mattord, *Principles of Information Security*, p. 350.

[50] S. Northcutt, "Alteration Attacks," 2015, http://www.sans.edu/research/security-laboratory/article/alter-code, accessed 18 January 2015.

[51] C. A. Henk van Tilborg and S. Jajodia, *Encyclopedia of Cryptography and Security* (New York: Springer Science + Business Media, 2011), p. 1076.