Putting the Personal Health Information Securely "on the Internet” by Integrating Biosensor with Networked Information System

Tian Wu (u7075880)

Introduction

Diabetes is a kind of commonly known chronic disease characterised by disturbances of fat, sugar, and protein metabolism. Typically, diabetes leads to a high blood sugar level in the human body due to the failure of insulin secretion and action. Statistics have shown that approximately 1.7 million Australians have diabetes, including both type 1 and type 2 diabetes, and this number is increasing by 280 every single day. [diabetes australia website]. Diabetes can cause various symptoms, such as blindness, amputations, and heart disease, which seriously affect people's health and life quality. [d a website] In 2010, data collected from nearly 400,000 people revealed that only 50% of Australians with diabetes are reaching the healthy glycaemic target level, meaning the remaining 50% are faced with higher risks of medical complications resulted from diabetes. [d a web] Another serious fact is that compared with non-Indigenous Australians, Indigenous Australians experience a much higher possibility of developing diabetes partly due to the inequality in access to health and poor use of health services in remote areas. [diabetes au pdf, 5, 6] On top of this, a large number of people with diabetes are unaware of the situations they are facing until they show some severe symptoms after many years. [3] However, researchers found that early detection of diabetes contribute substantially to the treatment of chronic diseases including diabetes, [valentine 2011] which implies that if people with diabetes can get treatment in the early stage, the risks of developing diabetic complications will reduce considerably.

The idea is to take advantage of the rapid development in the Internet technologies together with the booming emerging market of portable/wearable devices. Building novel, miniaturised sensors attached in household items can be the key to solve the problem of monitoring chronicle diseases such as hypertension and diabetes in a cost-effective way. Over 30 years after the first Internet connection was set up in Australia, now more than 86% of Australian families have access to the Internet at home.[ABStastics] Moreover, 91% per cent of the connected households have used mobile or smartphones to gain access to the Internet. [ABS] Meanwhile, the Federal Government has been encouraging telecommunication enterprises like Telstra to get involved in the Mobile Black Spot Program to expand mobile coverage in remote areas in Australia since 2015.[Telstra web] On the other hand, the booming biosensor market has gained an enormous development combined with powerful artificial intelligence and big data technologies in fields like health informatics and precision therapy. For example, cloud-based communication for health monitoring and emergency assistance integrated with wearable devices helps doctors to monitor their patients' health situations. [sinnapolu]

Our goal is to design a networked information system which uses wireless biosensor-integrated toothbrushes to collect data from people with diabetes. When it comes to the invaluable privacy behind the data, the designed network must have sufficient resources and abilities to deal with related network threats to ensure the security of these data. Furthermore, integrated with the latest AI and ML technologies, the system can analyse the data to offer them with early diagnoses and precision medicine therapy advice regardless of people's social backgrounds and geographical locations.

2. Methods

When developing a secure network, our first step is to identify all risks and threats existing in our designed network system. Then we conduct a risk assessment to provide strategies for analysing and prioritising risks to information systems and networks. The very next step for developing a secure network is to ensure business continuity. Third, we take into consideration of the concrete methods for intrusion prevention.

Meanwhile, developing security controls is a critical part of developing a secure network. We address these controls in our network and come up with approaches to mitigate and prevent threats. Finally, in light of the emerging global trend of combining health information with the network system, we compare five other context-relevant apps/websites using a similar idea of a networked information system. By addressing all the security threats, we have carefully designed our integrated networked information system with all necessary security controls.

3. Results

3.1 Security Issues and Risk Assessment

3.1.1 Security Threats

Generally, security threats in a network system can be categorised into two broad categories which are ensuring business continuity and preventing unauthorised access.

Three kinds of threats exist in ensuring business continuity in our health information system (HIS). First of all, disruptions such as network switch failures will cause the loss of or reduction in HIS. Second, Events like hard disk breakdowns will cause destruction of data in HIS. Third, natural/human-made disasters including fires, earthquakes and terrorist attack can also lead to catastrophic consequences to HIS.

Intrusions can also be a threat to our HIS from both outside networks and within the organisations. External attackers can gain access to organisational data from across the Internet, while employees inside the companies can also steal critical information on purpose.

Out of all the security threats mentioned above, we find our major threats are centred around the user information which can be compromised mostly by malware attacks, denial of services attacks and theft of information.

3.1.2 Risk Assessment

In dealing with security threats, it is of critical importance to conduct a risk assessment to view the whole picture of our designed system.

There are five steps required to complete a risk assessment: developing risk measurement criteria, inventorying IT assets, identifying threats, documenting existing controls, and identifying improvements.

The following table is a complete risk assessment targeted at addressing the three major threats: DoS attacks, theft of information and the malware attacks.

| Assets | Health Monitoring Applications/Services | | | Customer Database | | | Servers (e.g. web servers, mail servers) | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Asset Importance | High | | | High | | | High | | |
| Threat | DoS attacks | | | Theft of information | | | Malware attacks (viruses, ransomware, etc.) | | |
| Description | Attackers try to disrupt our service by flooding it with messages so we can not process requests from normal users | | | External hackers or inside employees attempt to gain access to customer database without authorization and sell it to make profits | | | Intruders or hackers try to distribute viruses, worms, or trojans for extortion | | |
| Likelihood | Medium (2) | | | High (3) | | | High (3) | | |
| Impact on | Availability | | | Availability, integrity and confidentiality | | | Availability, integrity and confidentiality | | |
| Impact Areas | Priority | Impact | Score | Priority | Impact | Score | Priority | Impact | Score |
| Financial | High (3) | Medium (2) | 6 | High (3) | Medium (2) | 6 | High (3) | Medium (2) | 6 |
| Productivity | Medium (2) | High (3) | 6 | Medium (2) | High (3) | 6 | Medium (2) | High (3) | 6 |
| Reputation | High (3) | Medium (2) | 6 | High (3) | High (3) | 9 | High (3) | Medium (2) | 6 |
| Legal | Medium (2) | Low (1) | 2 | Medium (2) | Medium (2) | 4 | Medium (2) | Medium (2) | 4 |
| Impact Score | 20 | | | 25 | | | 22 | | |
| Risk Score (Likelihood x Impact Score) | 40 | | | 75 | | | 66 | | |
| Adequacy of Existing Controls | Low | | | Medium | | | Medium | | |
| Risk Control Strategy | Mitigate | | | Mitigate | | | Mitigate | | |
| Risk Mitigation Controls | Description | | | Description | | | Description | | |
|  | Traffic filtering | Configure main router to verify the incoming source addresses | | Encryption | Encrypt the database | | Backup of database | Backup daily the whole database to a remote and independent data centre | |
|  | Router and firewall configurations | Configure main router to limit the number of incoming packets | | Firewall | Install a packet-level firewall on the router | | Disaster Recovery Plan | Regularly test the recovery plan to ensure the alternate database can restore full data successfully | |
|  | Traffic anomaly detectors and analysers | Add devices (detectors and analysers) to monitor normal traffic | | Personnel Policy | Any employee leaving the company will be removed of the log-in credentials | |  |  |  |
|  |  |  |  | Training | Regular training on network security with hands-on practice | |  |  |  |
|  |  |  |  | Other Security Measures | Secured door system from theft; password log-in to organisation network | |  |  |  |

3.1.3 Security Controls

When we build a network for HIS based on the health data we gather from our users, it is of importance that we develop a set of security controls to reduce or eliminate the threats. The controls are comprised of anything ranging from software, hardware to rules or procedures, which ultimately help prevent, detect, and/or correct insecure situations from happening. Network controls can be categorised into the following three aspects: preventive controls, detective controls, and corrective controls.

Preventive controls are a set of basic control methods which aim to mitigate or prevent a person from acting or an event from occurring. For instance, we can set up strong passwords in our system to keep intruders away. Meanwhile, we ask our users to create robust passwords for their accounts or bind their mobile devices for the two-step authentication. In the context of disruptions, it is also a good practice if we can set up a second circuit and a backup server just to ensure our network will keep working even if one of the service servers is down.

Detective controls are more focused on revealing events that can bring out unwanted results. For instance, it is an excellent idea to install software tools that keep looking for illegal network attempts. The tools will automatically spot the unwanted entries, keep logs and even report the events for future analysis. Take data destruction for example, in the event of a virus wiping out data or a hard disk failure due to natural disasters, and we can still recover from the damage with the help of a backup data plan if the backup service regularly runs in our HIS.

Corrective controls are a series of remedies dealing with unanticipated events or intrusions. Ideally, security software in our system can fix the problems on the spot and make patches immediately to prevent reoccurrences of such issues in the future. In other cases, a system administrator must keep an eye for these security breaches by unauthorised intruders and fix the errors.

Moreover, when designing a health network system, every engineer needs to take responsibility for their operations. Security controls need to be tested and updated regularly to keep up with the continually emerging threats and intrusions.

3.2 Business Continuity

Business continuity means that HIS data and applications will continue to operate in the face of disruption, destruction, or disaster. A business continuity plan has two major parts: the development of controls that will prevent these events from having a significant impact on the organisation, and a disaster recovery plan that will enable the organisation to recover if a disaster occurs.

Though there is much in common underneath threats and intrusions, the differences between threats and intruders are worth discussing.

A threat is any potential occurrence that can harm, interrupt the systems using the network, or cause a monetary loss to the organisation. An intruder is one who attempts to gain unauthorised access to computer networks regularly. Therefore, when faced with threats, we can do a thorough risk assessment to spot and identify the potential risks in our physical and virtual systems. We can come up with preventions to minimise the effects by either mitigating risks, sharing risks or other possible methods. While with intrusions, the critical element is the proactive measures we take in the first place. We need to bear in mind that no network is of complete safety and routinely check, test and upgrade our security systems before any intruders spot any opportunities and utilise the loopholes. One of uttermost principle about storing our customers' health data online is to isolate the data in a specialised data server guarded with the most advanced types of equipment.

3.2.1 Mitigating and preventing threats

We aim to prevent, reveal, and remedy the threats and have come up with five different levels of protection plans: virus protection, denial-of-service protection, theft protection, device failure protection and disaster protection.

According to a survey, every organisation experiences malware attacks in a typical year[textbook]. Installing antivirus software and keeping them updated will protect the system against numerous viruses and ransomware.

Several approaches are effective in dealing with DoS attacks, including traffic filtering, traffic limiting and installing sophisticated traffic anomaly detector and analyser. Since our HIS is based on the connections between our servers and the users, it is critical to invest our resources on defending such attacks.

When it comes to theft protection, physical security plays a crucial role in preventing essential devices from being stolen. Every department needs to make sure the devices are safely protected by locked doors and other safety measures.

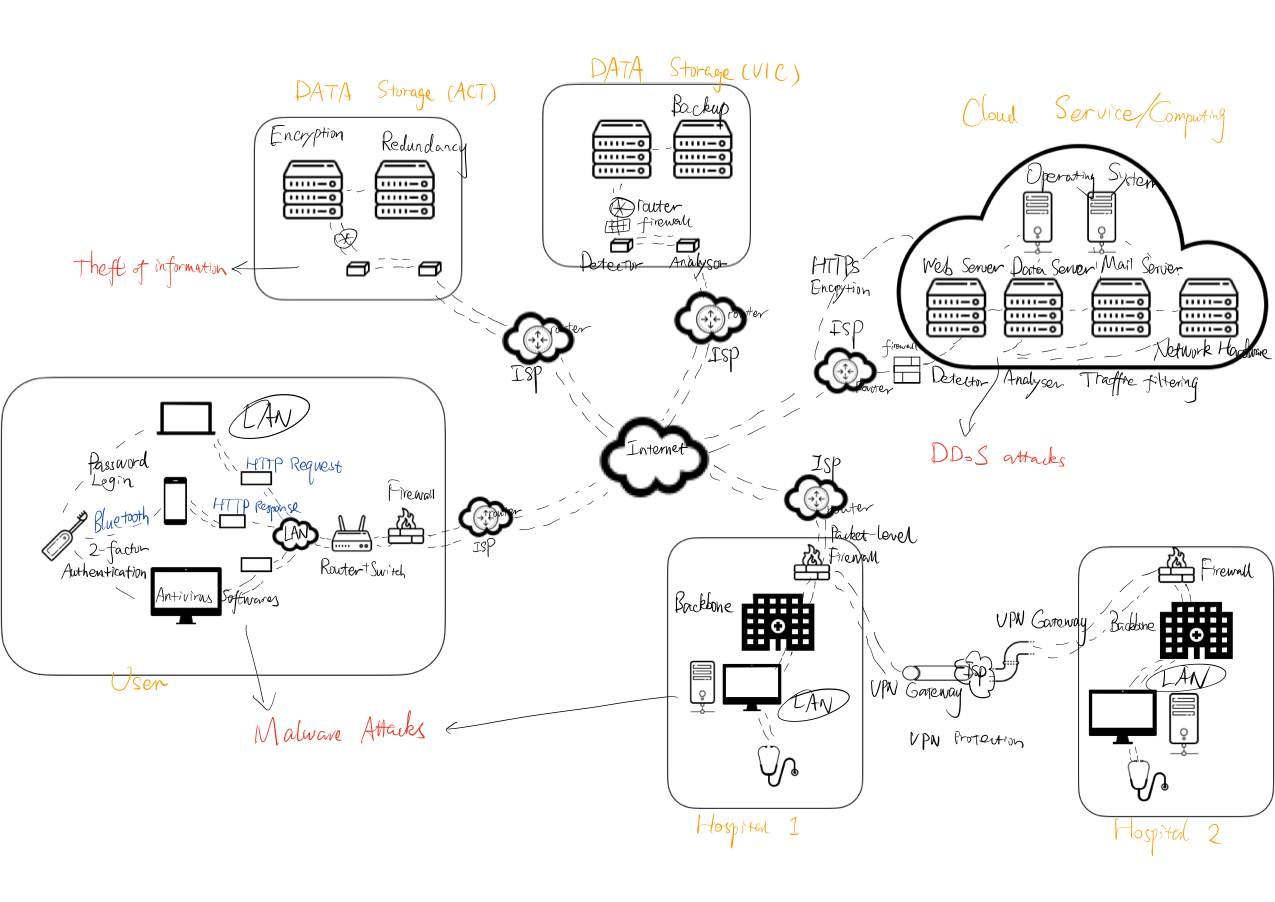
Moreover, building redundancy into the network will make HIS more reliable against hardware failures. Our network service is of great importance to the successful operation of the system; therefore, adding extra web servers will maximise the stability of the network connections.

Regarding the disaster protection, while avoiding disaster can be a difficult task, an essential part is a disaster recovery plan addressing various levels of possibilities.

3.2.2 Context-relevant networked information system

Due to both the intense demands in the wearable device market and the state-of-the-art technology breakthroughs in fields such as Artificial Intelligence (AI) and IoT, multiple platforms and systems have emerged during recent years.

Apple has developed its health platforms to fill the gap between medical professionals and developers through the innovation of the Internet. Wearables such as Apple Watches and Fitbit bands now can measure people's heart rate anytime, anywhere daily with almost no extra cost. [webs] For instance, The heart rate data gathered by optical sensors in Fitbit band will be stored in the Fitbit app installed on the phones, and data including all-day activity can be uploaded to the Internet by users to analyse. Since the Series 4 launched in September 2018, Apple Watch has also integrated an electrical heart sensor within the Health app to keep a record of electrocardiogram (ECG or EKG) which is of great help to spot any irregular rhythms. Besides, the new fall detection function in the Apple Watch takes full advantage of the network system. Whenever falling happens in an incident, if the person is unresponsive after one minute, the emergency call will be placed automatically by the app, and the location is sent using a mobile network connection through cellular for Emergency SOS. Another popular trend is the emergence of smart home devices centred around connecting all the electronic devices at home via Bluetooth or Wi-Fi, including health monitoring devices. The app MI Home acts as the data hub for all the hardware ranging from the air purifier to electronic sphygmomanometer [web]. For sensitive groups with hypertension, the sphygmomanometer collects data as usual. However, the app will send the data to the cloud where the analysis is generated based on history and the specific settings. In the field of sports, significant clubs have already embraced the state-of-the-art technologies to ensure the health and performance of their players since a decade ago. GPSports have designed a bespoke athlete management system called Catapult AMS which can "centralise football club's performance, medical and wellness information to streamline the management and communication of crucial information" by gathering data through tracking units integrated into the compression vests. [web] On the other hand, as far as personalised health technologies are concerned, more and more companies worldwide are investing in continuous non-invasive and miniaturised devices to take full advantage of new technologies such as AI for big data analysis, cloud computing on the Internet and ML modelling predictions. For instance, gene-sequencing company 23andme develops a home-based saliva collection kit for customers to send the sample of their DNA to the lab where the company uses next-generation sequencing together with powerful big data processing ability to analyse the data and offer tailored ancestry and health reports back to users. [web] In summary, all these apps and websites have taken advantage of the networked information system behind their different ideas to make use of the personal data gathered from users.

3.3 Health Information System (HIS) network design

We choose to design a biosensor integrated networked system based on the cloud computing architecture PaaS (Platform as a Service). PaaS is a three cloud computing model where developers create a diabetes monitoring application for users. PaaS rents the platform, including hardware (web servers, data servers, mail servers, network hardware) and software infrastructure (operating systems, database software) from the cloud provider. In this way, we manage the application and data while using the database software and operating system from the cloud provider.

4. Discussion

We have designed and built a networked information system by first using diabetes biosensor in a toothbrush to collect health information, and then utilising the mobile phones and computers to transmit the data to the cloud for detailed analysis. Wherever the user lives, he can access his health data and recommendations with an Internet connection in real-time.

We develop risk measurement criteria to evaluate the way a security threat could affect the organisation. In the case of setting up a networked information system for health monitoring, there are four most commonly considered impact areas to consider which are financial, productivity, reputation and legal. Then, we inventory all types of assets, including hardware, software, data, or applications. Of all these assets, there is one mission-critical application essential to the survival of our health monitoring system: the HIS application services we offer to our customers. Afterwards, we pivot our attention to identify threats, especially the major threats can help us create threat scenarios to assess likelihood, priority and impact in a quantifiable way. Then, we get the risk control strategy in place after identifying the specific assets, threats scenarios. In this process, we intend to address the risks by mitigating them by security controls.

Last but not least, our final objective is to identify what improvements our system needs by concentrating on the highest risks first. In the case of building and implementing HIS, we have identified three most urgent and significant risks emerging around us at this moment, which are malware attacks, theft of information and the DoS (denial-of-service) attacks. By addressing these three utmost risks, we designed a network system most suitable and reliable against the threats and intrusions.

However, there is no perfect network defending all threats and intrusions. Our HIS design still has its limitations. For example, attackers often use social engineering to break into users' database in which case users are exposed to threats without knowing. What's worse, experienced attackers can use man-in-the-middle attacks by eavesdropping from unencrypted access points and stealing the sensitive data. Furthermore, there are only two database centres in our network which limit our ability to reach out to more people in remote places. In the future, we need to integrate more secure encryption into our system while setting up more locations to offer our service to a border range of people with faster connections.

During this research, I gain a deeper understanding of the complexity of the networked systems in the world. Frankly, I appreciate all the efforts and thinkings behind the existing technologies, especially the security measurements that keep the whole system running all the time smoothly. In our daily experience, security issues may be ignored when we get used to the convenience of the Internet, however, as future engineers and computer scientists, we need to lay a reliable and secure foundation when designing the network in the first place.

5. References