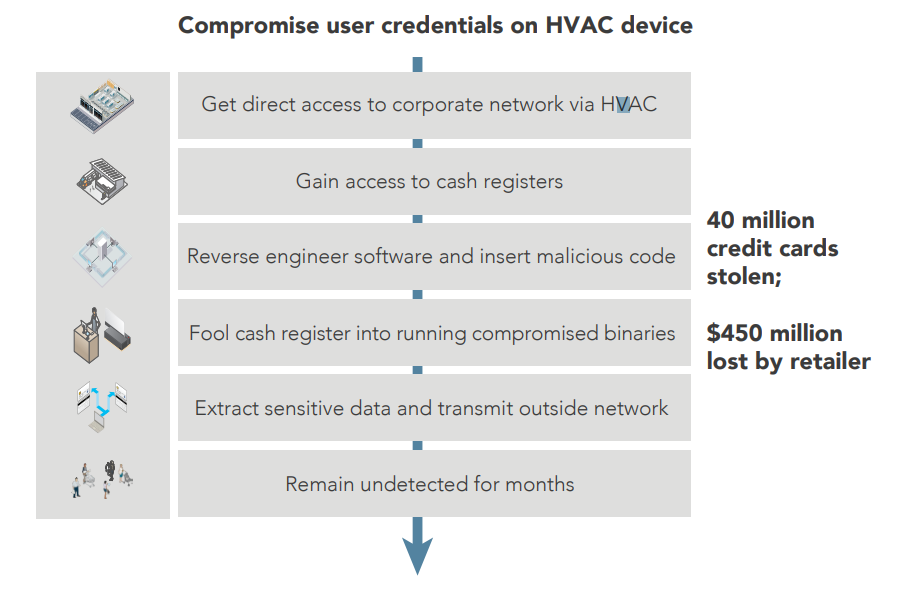
1. Introduction
2. Main Part
   1. Challenge
   2. Vulnerability
   3. Case study
3. case study 1:
   1. What happened?

A larger number of retailers from USA experienced a security breach that leads to a considerable customer credit and debit card numbers were stolen by cyber thefts. The point of sale (POS) was actually compromised and its information was also captured. How this actually happened, the image below show the step that was conducted by the hackers to obtain illegal . Firstly, the hackers access into  the HVAC (heating, ventilation, and air conditioning) system network, this network however is on the same network as the POS devices. Therefore, the hacker can remotely entered to the company cash register system, once breached the engineer code was reversely modified and inserted malicious code, these malicious code made the system by running weaken binary code. The system is then tracked then its transaction information was caught, extracted and transmitted as soon as the customers wiped their credit/debit card through the machines. Unfortunately, the hacked lasted for weeks after the vendors detected, the situations could went worse if there was no outside investigators joined and alerted the sellers.



* 1. What was the cause

There were plenty of causes rather than a single failure:

* The retailer did not detached the HVAC network from the main network
* The POS system were widely welcomed any devices to access into its system
* The running source code was not encrypted
* The operating system did not have the access control configured
* No monitoring system was installed
  1. Recommendation methods to prevent the causes
* Isolating the HVAC system into the separated networks, this method would close the interruption from entering the POS devices
* Enabling firewall on POS devices might blocked illegal access, the devices also can only run proper source code but not outside injected one
* Encrypting the application makes its harder for reverse engineering intrusion, with this configured, unoriginal malicious code  can not be executed and tricked the cash register machine itself.
* Installing proper access control system to prevent sensitive devices from running dangerous tasks as well as the unauthorized extracted data from broadcasting outside the network

1. Case study 2:  The Dyn Cyberattack
   1. What happened?

In October 26, the world has witnessed how fragile the internet is, many popular websites suddenly stop working properly. Many internet users can’t reach sites like Reddit, Paypal, Twitter, Pinterest, Netflix, etc. This attack involved multiple Denial-of-service attack (DoS attack) that targeted operating system by Domain Name System (DNS) by DYN - an internet performance management company.



* 1. What was the cause

To achieve the objective by overwhelming the DNS systems with a flow of request from unique devices, botnets were used to take over routers,computers, internet cameras by hackers. Those accesses required many DNS lookup requests from 10 millions of IP addresses. The botnet is reported to be infected with Mirai malware. Investigators said that there was an estimated load of 1.2 Terabits/second, which is a largest DDoS attack has ever happened.  Mirai effectively scanned for IoT devices after injected to the insecure devices, it then looked for devices with simple, default password. With no surprise, many of these have original username and password like “admin”, “root”, “password”. Infected devices run normally except casually show sluggishness and big bandwidth was increasingly used.

* 1. Recommendation methods to prevent the causes
* Implement secure remote management, in company network environment. Network Segmentation method is recommended. By creating VLAN (Virtual Local Area Network), it brings a flexible and powerful control for remote users to access.
* VPN (Virtual private networks) is also a secure remote management methods, it brings a secure way to insecure and vulnerable devices
* Set secure password for better devices security. Devices should be changed with a combination of upper, lower cases characters, numbers, special characters to form passwords. Then use a password manager to tracking all your devices ‘s passwords.

1. Case study 3:  The Jeep Cherokee Hack
   1. What happened?

In July 2015, two security researchers Charlie Miller and Chris Valasek successfully hacked into a Jeep Cherokee manufactured in 2014 and able to steer the wheels, disable the brake, or even shut down the engine. They also said that there are still thousands of other smart vehicles are still using the Uconnect- a wireless entertainment and navigation system, developed by Dodge, Jeep and Chrysler vehicles This harmless  demonstration leads to a recall of 1.4 millions vehicles by Fiat Chrysler.



* 1. What was the cause

Mostly new smart vehicles come with impressive computers that connected to each other on certain networks. Firstly, a brute force attack was conducted to connect to the on-board Wifi within the vehicle system. The Linux based “head unit” in the vehicle system was hacked and allowed the two security researchers to modify the firmware inside the system. The firmware included an internal communications network (CAN bus), with this access, they could interrupt and prevent the vehicle in performing critical system like the braking system.

* 1. Recommendation methods to prevent the causes
* Add cryptography to enhance the communications and authentications process between the software systems and devices.
* Disable unused communication ports
* Prevent the firmwares, software alter to prevent the

1. Suggestion

---Minimize the IoT security vulnerabilities  for small business network--

* Every devices should change or update the password from its default one, devices that are having constant password should not be use. Complex and unique password are recommended to use.
* Create or split into multiple network zones for IoT devices, especially along with firewall monitoring for IoT devices if available. This therefore create an extra security layers help prevent possible vulnerable devices from reaching, accessing into core/main network that might leaking important information or being hacked. In certain cases, you might consider stronger firewalls like a next-generation (NGFW) or Unified Threat Management (UTM) that support organization level of protection.
* Encryption devices is also recommended, encrypted send and receive data are always better to protect your information.
* Keep software update to make sure the current devices or networks have newest technology, one of the standing benefit in updating version is the hotfixes and security improvement releases by developers. Updating devices should be checked monthly or enable auto update, therefore devices that can not received updates should not be used.
* Disable unused and unnecessary functions/ components, display devices like TV, cameras tend to have a voice-recognition function, hacker can use that way to exploit to breach into the system, so it a good idea to disable its microphone.

---

X)References

<https://www.networkworld.com/article/3269184/internet-of-things/10-best-practices-to-minimize-iot-security-vulnerabilities.html>

<https://www.securitysales.com/integration/6_tips_for_reducing_internet_of_things_security_risks/>

<https://www.windriver.com/whitepapers/documents/2583-Securing-Devices-in-the-Internet-of-Things-White-Paper.pdf>

<http://ec.europa.eu/information_society/newsroom/image/document/2017-11/generic_security_and_privacy_principles_to_ensure_a_trusted_iot_environment_by_gsma_0B65C49E-D8A9-037B-2E9A3587227071F9_43658.pdf>

<http://cse.unl.edu/~qyan/paper/MobiSec17_AugustLock.pdf> --- Chua xai