|  |
| --- |
| CS3609 CYBERSECURITY COURSEWORK  STUDENT NUMBER: \_\_1516552\_\_ |
| COUNTERMEASURES ( 1 PAGE ):  *Describe 3 countermeasures that you recommend for the below systems architecture [150 words per countermeasure].*  Countermeasure 1:  Access control is one of the utmost countermeasure required to maintain a safe level of security within any system, since the most crucial step of cyber kill chain is to gain access to the system through exploiting the given system.  Especially for a system like the Brunel Smart Home system, which entities will be able to access what functions and what permissions each entity will have is crucial.  Access control can also be physical limits to the assets. However, the main threat arises within the logical access control. ABAC (Attribute-based access control) a type of logical access control manages access via enforcing a set of rules or policies using attributes of users, systems and environmental conditions which would benefit the Brunel Smart home system. Enabling a Firewall would also regulate the flow of traffic between LAN-to-WAN domain and enable protection from external source trying to gain access to the system.    Countermeasure 2:  Second countermeasure I would recommend is to heighten the authentication protocol of the Brunel Smart Home system. The Exploitation is arguably the most threatening stage of the cyber kill chain and it can be challenged through providing an adequate level of authentication process.  The first stage of authenticating a connection of a terminal to a host is to verify that the two entities involved are the legitimate. Secondly, the protocol must ensure that connection is not interfered by third party who can masquerade as one of the two legitimate entities.  Due to the internet-enabled devices on BRUNEL Smart home system, each access point is a potential intrusion point therefore, it is important for each IP connected devices to have a strong machine authentication. A VPN (Virtual Private Network) is also used in a Certificate-based authentication to ensure the identity of entities joining the network through means of digital certificate and where CA (Certification Authority) plays a vital role.  Countermeasure 3:  Data confidentiality/privacy is yet another vital countermeasure that needs attention. As shown in the System diagram below, the data collected from the smart home system is sent to BRUNEL’s remote web service. Ensuring that third parties do not have access to confidential information while the data is being transmitted between two entities, in this case between Brunel Smart home system and the remote web server in BRUNEL is crucial. The risk of information leakage could mean an easier execution of Reconnaissance and Weaponization stage of the cyber kill chain.  Encrypting sensitive files, data acquisition and utilization are some of the few suitable way to manage data confidentiality for the Brunel Smart home system. Sensitive Information such as user’s pattern of use of the home devices needs to be encrypted. The IP connected devices specifically requires a basic cybersecurity hygiene of using anti-virus software, updating and patching software, enabling firewall etc.  by gaining more infor-  mation about its customers’ energy consumption. As a result,  consumers could find themselves in yet another situation where  they are expected to emit personal information regarding the  activity in their home environment.  by gaining more infor-  mation about its customers’ energy consumption. As a result,  consumers could find themselves in yet another situation where  they are expected to emit personal information regarding the  activity in their home environmen  SYSTEM ARCHITECTURE DIAGRAM ( 1 PAGE ):  *Produce a diagram depicting the vignette environment – including 3 additional IP connected devices. The diagram should help you to identify risks, support decision making and countermeasure choice [Hint! Annotate the diagram with labels].* |
| DECISION MAKING (UP TO 2 PAGES ):  *Describe your decision making in determining risks and countermeasures. Reference literature where appropriate to support your decisions.*  *Justify the countermeasures and relate it to kill chain*  *How the intruders will behave?*  *What actions will they take*  *How the countermeasures put in place will fight the attacks?*  Brunel Smart Home system (BSH) is a type of home automation system which uses elements of home network to control the heating, lighting, smart fridge and in-room music in a home environment.  The security countermeasures that I recommended for this system are access control, authentication and data confidentiality. The reason behind the selected countermeasures is mainly because it addresses the early stages of the cyber kill chain which is arguably the most vital part as with the saying “Prevention is better than cure”. Once the system has been exploited and the infected program has been installed, the system will already have suffered ample damage. Therefore, I strongly recommended the access control, authentication and data confidentiality countermeasures to tackle the potential risks to the system.  Firstly, according to Stallings, “Access control is the ability to limit and control the access to host systems and applications via communication links.” A weak access control is an open gateway for attackers to deliver and exploit the system with the weapon that they have created to conduct malicious activities.  According to a 2017 Data Breach Investigations Report by Verizon, about 96% of the attacks are via an ‘External’ breaches i.e. Unauthorized access of the system from a third party source. It is not as different for a Home network environment where the devices connected will be access public domain which is a potential intrusion point for attackers. This is completely viable for the BSH system since there are three IP connected devices which shares the same WAN router. If the attackers gained access into the system, they will begin the exploitation phase of the kill chain whereby the weapon/malware is ‘detonated’. In BSH system’s case, if system isn’t updated and current to stop malware installation then the system can get compromised letting the attackers to move on to ‘Command & Control’ phase of the cyber kill chain. Once they are in this stage the attackers will be able to control the home devices controlled through the BSH system such as lighting, heating and so on.  The ABAC (Attribute-Based Access Control) is a type of logical access control which evaluates the rules against attributes of entities, operations and the environment relevant to a request. This means that the user of BSH system  And the leakage could include information such as the energy consumption or types of music the user listens to and their patterns of use of their home devices. |
| BIBLIOGRAPHY ( UP TO 1 PAGE ):  *Harvard format*  [*http://dtpr.lib.athabascau.ca/action/download.php?filename=scis-07/open/evanwagnerEssay.pdf*](http://dtpr.lib.athabascau.ca/action/download.php?filename=scis-07/open/evanwagnerEssay.pdf)  [*https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2017.pdf*](https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun-2017.pdf)  [*https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf*](https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf)  [*https://searchsecurity.techtarget.com/definition/access-control*](https://searchsecurity.techtarget.com/definition/access-control)  [*https://www.researchgate.net/publication/289415256\_On\_the\_Risk\_Exposure\_of\_Smart\_Home\_Automation\_Systems*](https://www.researchgate.net/publication/289415256_On_the_Risk_Exposure_of_Smart_Home_Automation_Systems)  [*https://www.ndss-symposium.org/wp-content/uploads/sites/25/2018/06/eurousec2018\_11\_Nthala\_paper.pdf*](https://www.ndss-symposium.org/wp-content/uploads/sites/25/2018/06/eurousec2018_11_Nthala_paper.pdf)  [*http://www1.udel.edu/security/data/confidentiality.html*](http://www1.udel.edu/security/data/confidentiality.html)  [*https://core.ac.uk/download/pdf/81064359.pdf*](https://core.ac.uk/download/pdf/81064359.pdf)  [*https://www.mdpi.com/2313-576X/4/3/36/pdf*](https://www.mdpi.com/2313-576X/4/3/36/pdf)  [*https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain*](https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain)  [*http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings\_Cryptography\_and\_Network\_Security.pdf*](http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5680/material-cripto-seg/2014-1/Stallings/Stallings_Cryptography_and_Network_Security.pdf) |