COMS W4180 – Spring, 2016

Written Assignment 4

Shivam Choudhary (sc3973)

1. **Answer:** top and netstat are related by PID(process id's) so an abrupt increase in a metric can be cross verified vice-versa. Since the system given to us is a predictable in terms on number of processes running so we just need to monitor the resources the system is using.

   (a) **IDS Design**

   - **Parameters to monitor:**
     - **top command:** PID, Command, %CPU, Memory, Disk Usage.
     - **netstat:** PID(using -p flag in netstat),Proto, Local Address, Foreign Address, State.
   - **How often to collect data:** We should maintain a running time average of data sampled every T seconds and P packets where these parameters depend on the amount of expected traffic in T seconds. For example if the server is a DNS server and we expect around 500 queries per 10 seconds then we should sample every 500 packets for netstat and for top every 10 seconds and compute the weighted running time average.
   - **Methodology:** Weighted running time average means that the parameters (Memory, Disk Usage etc) are scaled to place appropriate importance on each parameters. Since the number of processes is constant the state of the system can be approximately bound in terms of average resources. So if we observe that a process is using more memory or CPU(using proper weights to unify them into one parameters) and then we observe that the process(using it's PID) is also sending connections to unknown IP addresses then that process is malicious and can be put into Alert List. Furthermore for many connections if we observe sudden increase in number of open connections(using netstat) then that is certainly an indication of attack.
   - **Accuracy**

     False Positives When the admin does some routine maintenance work it might lead to False Positives because the admin might be updating the system and it might be downloading data simultaneously from different connections(like Canonical repositories) which may lead to surge in traffic. Furthermore admin might try to stress test some of the processes which might increase the CPU usage and then it would again be reported which is clearly False Positive.

     False Negatives A malware can be designed which replicates slowly using only minimal network resources which are aligned with the times the network expects the most traffic. Since this would not be detected in the running time average (as it would gel perfectly),though it was a malware.

   (b) If the developers are given access to the system then the IDS will observe surge in open number of connections in the system(ssh or otherwise) and this would be corroborated with high disk usage and cpu which will lead to generations of False positives. Now since

the number of users who are accessing the system is not bound the state of the system cannot be defined accurately(users may be running different processes and can update different components). This would lead to increase in both the number of False positives(users upgrading) or may lead to False negatives since we might need to introduce room to accomodate different processes to reduce False positives which might lead to some malwares being undetected.

2. **Answer:** Following security issues were identified in Zigbee:-

   (a) While it's assumed that the keys are securely stored(devices are preloaded with them) but if a non-preconfigured device joins the network then one-time transmission of key (albeit for a short interval) is required which opens a window for exploitation.An attacker can jam the signals to trick re-joining and then sniff the key.

   (b) The hardware is not tamper resistant given their relatively cheaper cost of manufacturing. So attacker can get physical access to a device revealing secret keying material and other privileged information and access to software and hardware.

   (c) The use of the default TC link key ZigBeeAlliance09 introduces a high risk to the secrecy of the network key.This allows for the case where alternative pre-configured link keys specifically associated with a device can be used as well.If an attacker is able to sniff a device join using the default TC link key, the active network key is compromised and the confidentiality of the whole network communication can be considered as compromised.

   (d) Devices in ZLL use ZigBee network layer.During classical ZigBee commissioning where a non-ZLL device is being joined to a ZLL network without a trust center, a pre-installed link key is used to secure the transfer of the network key when authenticating. The ZLL pre-installed link key is a secret shared by all certified ZLL devices. It will be distributed only to certified manufacturers and is bound with a safekeeping contract. Additionally, if the decryption of the APS message fails with the key described above, ZLL devices shall try to decode the APS message using the known default trust center link key.This leads also to the same vulnerable initial key exchange.

   (e) ZLL devices support a feature called Touchlink Commissioning that allows devices to be paired with controllers. As the default and publicly known TC link key is used, devices can be stolen

   (f) No automatic key rotation could be policy is implemented in Zigbees

3. **Answer:** Via TA(traffic analysis) the length of the packet can be identified which can then be used to classify the packets. The authors further claim that the none of the previously described claims aimed at traffic morphing is effective in real scenario.

   According to the authors none of the countermeasures can prevent this kind of identifications.

   The authors considered the following countermeasures

   (a) **Type-1: SSH/TLS/IPSec-Motivated Countermeasures** The countermeasures like Pad to MTU and Session Random 255 obfuscate the bandwidth usage but since the noise is added only to the lower order bits of total bandwidth hence the change in bandwidth usage is too small realative to what would be needed to make two websites bandwidths

likely to overlap significantly. The authors further claim that this is true for all padding based countermeasures(Type-1 and Type-2)

(b) Type I and Type 2 do not directly modify the total time taken by traces. On the other hand Distribution-based counter measures (Type 3) potentially inject dummy packets into a trace,but this is most often about 10-12 packets in succession hence not changing the total time significantly.

(c) Type 3 do not substantially change the total bandwidth of the data transmitted in each direction,nor the duration of the trace with regards to the time.

(d) Furthermore the coutermeasures don't conceal the burstiness of the data which maybe correlated to higher level structure of the underlying HTTP traffic.

4. **Answer:**

(a) `TCP` was used in the traffic that the authors analyzed.

(b) For each TCP connection they extracted Packet Size, Arrival Time and Direction(from/to server)

(c) The protocols they used were (number in bracket indicates port):

i. SMTP(25)
ii. HTTP (80)
iii. HTTP over SSL (443)
iv. FTP (20)
v. SSH (22)
vi. Telnet (23)
vii. outbound SMTP
viii. AOL Instant Messenger traffic

5. **Answer:**

(a) **Hacking IOT Baby monitors.**
Date: Published September 29, 2015
URL: https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf
Issues: Following were the issues which allowed the device to be hacked

i. **Cleartext Local API** : Local communications are not encrypted. They were sent in either plaintext or in a way that can be easily modified/sniffed by an attacker so it allowed easy network key access.
ii. **Cleartext Cloud API** : Remote communications are not encrypted so it was sniffed in the network and data uploaded from monitor was modified.
iii. **Unencrypted Storage**: Data collected is stored on disk in the clear so it allows easy access in case one device is physically compromised(in case the password is stored in plain).
iv. **Remote Shell Access** : A command-line interface was available on a network port which allowed easier password guessing,the manufacturers kept a shell with elevated privelges.

v. **UART Access** : Physically local attackers can alter the device. Since UART protocol typically tend to run under elevated privileges it became easier for attacking and modifying the firmware of Baby monitor.

(b) **Cherokee Jeep Hack**

Date: Published August 6,2015

URL: https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/

The attackers were able to apply brakes on in the Jeep using the CAN bus protocol.

Issues:

i. Hack password through Wifi connection as it was generated using time the multimedia and car was started the first time.

ii. Hacked the multimedia system which was running Linux using vulnerable attacks known particular to that version.

iii. Can control music using this.

iv. The V580 controller talks to a component which is connected to the CAN bus of the car. So using multimedia system they controlled the CAN bus which in-turn gave them control over the car's brakes and engines.

v. The main issue was that the CAN bus was not isolated from the vehicle's subsystem so they were able to hack it using multimedia system