Title: Smart Things

Below is the detailed challenge. CACI will bring the hardware but the students need to have their own laptops.

This challenge involves activating the provided smart outlet by bypassing the Smart Things Cloud and associated security. The challenge sponsor is providing the following to facilitate this challenge:

1.A SmartThings Hub properly configured and registered with the Samsung Cloud/ Service using the following e-mail address:CACIChallenge@gmail.(the password will be provided to teams that choose this challenge) The CACI Team expects participants to install the free SmartThings app on their own devices in order to interact with the environment.

2.A wireless router setup with an SSID CACI_Challenge_LAN. This network will simulate a home network that the challenge teams have penetrated. The Router will be configured as a NAT behind the GMU provided LAN architecture. (passcode will be provided to participant teams)

3.A Sumsung SmartThings Outlet – the goal is to be able turn this off/on

4.A USB based dongle that will allow challenge teams to interact with the RF Protocol used between the Hub and the Outlet. (There are 4 available – 1 per team)

This challenge can be completed by compromising any of the links between the SmartThings Phone App, an external service like Echo or Google Home, the Samsung Cloud, the SmartThings hub or the Smart Outlet itself. The provided environment allows for both TCP/IP and RF based attacks.

Automatic Disqualification:

a.Challenge teams will NOT attempt to penetrate the Amazon, Google or Samsung online systems as this is clearly illegal and they are likely far more secure than you have resources or expertise to succeed in the 48 hours allotted.

b.Attacks focused on compromising the registration userID and password since we are providing both the registration ID and passwords so that teams may interact with the available devices in their intended manner. Obviously if you can compromise the registration credentials, this challenge is trivial and that would be the easiest to make the attack successful.

c.Any attack that requires physical access to the devices since a potential “bad guy” will not have physical access to the devices since they will be inside a locked consumer’s house.

d.The attack must not render the device unusable as stealth is very important so that you can compromise and then lie in wait until the exact right time to cause the device connected to the outlet to turn off. Besides 4 teams may be competing against each other and must not interfere with each other.

e.Use of code, tools, research developed by 3rd parties that is not credited in the final presentation since in School, Plagiarism is grounds for failing.
f.Any activity that actively interferes with the efforts of another team.

Once again, the goal is to be able to turn on/off the outlet by bypassing the default security inherent in the SmartThings architecture.

Points will be awarded for the following:

- Successfully installing and activating the USB dongle to view RF Traffic
- Completing the attack w/o using 3rd party products
- First team to successfully conduct the attack
- An assessment of each of the attack vectors suggested with viable courses of action to include the steps necessary to successfully complete the attack using that COA
- A protocol definition and possible attack vectors for the ZigBee protocol
- Conducting an Internet Search and reporting on previous successful attacks and suggested vulnerabilities today and how they may be mitigated
- Successfully spoofing the SmartThings Hub
- ID'ing any encryption in use and successfully breaking it
- The furthest physical distance from the outlet to conduct a successful attack
- The most creative approach that would likely succeed but did not due to resource constraints (time or material)