Securing IoT Devices

Part of our mission here at the CyberSecurity & Networking Division is advancing applied cybersecurity and networking research and anticipating future security trends and threats. Working towards that end is the Science DMZ Actionable Intelligence Appliance (SDAIA) project—currently in development—which collects data from allocated but unused networking space. The data is analyzed for potential threats and shared with participating partners.

Large amounts of data have been collected from many thousands of unused IPs and we noticed several trends. All of the data collected so far have been SSH brute-force attacks, where automated attackers attempt to guess user and password combinations, giving them access to devices listening with an SSH service. We have noticed that a lot of the user/password combinations indicate an attacker preference for connected, embedded or “smart” devices—often referred to as the Internet of Things, or IoT. For example, within the 20 most common hits we found:

User	Password	Device
ubnt	ubnt	"wireless networking equipment"
root	openelec	"Linux based media center"
root	dreambox	“Linux based set-top box receiver"
root	raspberrypi	"single board computer, typically running Linux"
root	000000	"imaging, webcam"
pi	raspberry	"single board computer, typically running Linux"
root	xmhdipc	"imaging, webcam"
root	anko	"imaging, webcam"
root	welc0me	“Linux based NAS device"
root	rpitc	"raspberrypi thin client"
root	uClinux	"linux on embedded microcontrollers"
root	seiko2005	“unknown"
root	nosoup4u	”Linux based NAS device"
root	alpine	“smart phone"
root	ubnt	"wireless networking equipment"

These attacks point to the pervasiveness of these devices, which are projected to be over 7 billion by the end of this year. As these scans indicate, there has been little attempt to secure these devices, let alone change the default password—despite a large number of high profile denial of service attacks and worryingsecurity vulnerabilities. As has been pointed out by many experts, changing the default password on these devices can often prevent them from being infected by malicious software.

How can you ensure that you can quickly identify these devices on your networks? There are two possibilities. A passive solution relies on constant examination of traffic in and out of your networks using software such as the Bro IDS. The downside to this technique is that Bro will only detect insecure devices once they have been compromised. An active solution relies on scanning all parts of your network and testing whether the devices are actually vulnerable. SSH-auditor is an example of software that can do this efficiently and can be found at NCSA’s github repository collection. Seeding this software with the most common user/password combinations and scheduling frequent scans of your network can very quickly identify vulnerable devices.