



# Botnets and Internet of Things Security

Elisa Bertino, Purdue University

Nayeem Islam, Qualcomm

*Recent distributed denial-of-service attacks demonstrate the high vulnerability of Internet of Things (IoT) systems and devices. Addressing this challenge will require scalable security solutions optimized for the IoT ecosystem.*

**T**he large number of insecure Internet of Things (IoT) devices with high computation power make them an easy and attractive target for attackers seeking to compromise these devices and use them to create large-scale botnets. A botnet is a network of infected machines or bots, also called zombies, that has a command-and-control infrastructure and is used for various malicious activities such as distributed denial-of-service (DDoS) attacks (see the “Botnets” sidebar).

In November 2013, Symantec researchers discovered the Linux.Darll0z worm, which exploited a PHP vulnerability to propagate to IoT devices such as home routers, TV set-top boxes, security cameras, printers, and

industrial control systems. In January 2014, a variant of the worm was found to include a cryptocurrency mining tool.<sup>1</sup>

In September 2016, an IoT botnet built from the Mirai malware<sup>2</sup>—perhaps the largest botnet on record<sup>3</sup>—was responsible for a 600-Gbps attack targeting Brian Krebs’s security blog (krebsonsecurity

.com). Mirai’s strategy is quite simple; it uses a list of 62 common default usernames and passwords to gain access primarily to home routers, network-enabled cameras, and digital video recorders, which usually have less robust protection than other consumer IoT devices. The same month, a Mirai-based attack against the French webhost OVH broke the record for the largest recorded DDoS attack—at least 1.1 Tbps, and perhaps as large as 1.5 Tbps.<sup>4</sup>

## IoT SECURITY RISKS

These DDoS attacks weren’t a surprise. Compared to conventional computing systems, IoT systems are at higher security risk for several reasons:<sup>5</sup>



- › IoT systems don't have well-defined perimeters and continuously change due to device and user mobility.
- › IoT systems are highly heterogeneous with respect to communication medium and protocols, platforms, and devices.
- › IoT devices could be autonomous entities that control other IoT devices.
- › IoT systems might include "things" not designed to be connected to the Internet.
- › IoT systems, or portions of them, could be physically unprotected and/or controlled by different parties.
- › Unlike smartphone applications, which require permission for installation and many user interactions, granular permission requests might not be possible in IoT systems because of the large number of devices.

Consequently, many IoT systems lack even elementary security. Table 1 lists the most common IoT vulnerabilities identified by the Open Web Application Security Project (OWASP; [www.owasp.org](http://www.owasp.org)). A July 2014 report on IoT device security by HP found, on average, 25 vulnerabilities per device. For example, 80 percent of devices failed to require passwords of sufficient complexity and length, 70 percent didn't encrypt local and remote traffic communications, and 60 percent contained vulnerable user interfaces and/or vulnerable firmware.<sup>6</sup>

## PROTECTION TECHNIQUES

Ensuring that IoT devices aren't exploited as zombies requires adopting a few well-known security practices that address the most common vulnerabilities. An October 2016 alert by the US Computer Emergency Readiness Team (US-CERT) about the Mirai botnet<sup>4</sup>

## BOTNETS

A botnet is a robot network of compromised machines, or bots, that run malicious software under the command and control of a botmaster. Botnets have a wide range of nefarious purposes including email spam delivery, distributed denial-of-service (DDoS) attacks, password cracking, key logging, and cryptocurrency mining.

Bots can automatically scan entire network ranges and propagate themselves using known vulnerabilities and weak passwords on other machines. Once a machine is compromised, a small program is installed for future activation by the botmaster, who at a certain time can instruct the bots in the network to execute actions such as sending requests to a target website with the intent of rendering it unable to serve requests by legitimate users, resulting in DDoS.

Early botnets used a centralized architecture in which the botmaster would reside on one or more central servers. Because such botnets could be disabled by shutting down these servers, alternative architectures based on peer-to-peer (P2P) networks emerged. Example P2P botnets include GameOver Zeus, Sality, ZeroAccess, and Kelihos.

As communication is a critical botnet function, domain fluxing is widely used. In domain fluxing, each bot independently computes a list of pseudorandom domain names using a domain-generation algorithm. The bot then attempts to contact the domains in a certain order until one attempt is successful—that is, the domain name resolves to an IP address and the corresponding server provides a valid reply according to the botnet's protocol. The botmaster, however, need only register a few domains in the list to serve as command-and-control servers.

provides a comprehensive list of such practices, which include:

- › ensuring that all default passwords are changed to strong passwords;
- › updating IoT devices with security patches;
- › disabling Universal Plug and Play (UPnP) on routers unless absolutely necessary;
- › monitoring IP ports 2323/TCP and 23/TCP for attempts to gain unauthorized control over IoT devices using the network terminal (Telnet); and
- › monitoring for anomalous traffic on port 48101, as infected devices often attempt to spread

malware by using this port to send results to the threat actor.

The US-CERT alert also recommends specific end-user actions such as only acquiring IoT devices from companies with a good security reputation and understanding the devices' communication capabilities, as they're at higher risk of malware infection.

These security practices are reasonable and would provide a first line of defense, but their application is clearly limited by the scalability of human interaction with IoT devices. Approaches are also needed that automatically manage security for such devices.

Another challenge of IoT devices is that even if they have known software

**TABLE 1.** Common Internet of Things vulnerabilities.\*

Vulnerability	Examples
Insecure web/mobile/cloud interface	Inability to change default usernames and passwords; weak passwords; lack of robust password recovery mechanisms; exposed credentials; lack of account lockout; susceptibility to cross-site scripting, cross-site request forgery, and/or SQL injection
Insufficient authentication/authorization	Privilege escalation; lack of granular access control
Insecure network services	Vulnerability to denial-of-service, buffer overflow, and fuzzing attacks; network ports or services unnecessarily exposed to the Internet
Lack of transport encryption/integrity verification	Transmission of unencrypted data and credentials
Privacy concerns	Collection of unnecessary user data; exposed personal data; insufficient controls on who has access to user data; sensitive data not de-identified or anonymized; lack of data retention limits
Insufficient security configurability	Lack of granular permissions model; inability to separate administrators from users; weak password policies; no security logging; lack of data encryption options; no user notification of security events
Insecure software/firmware	Lack of secure update mechanism; update files not encrypted; update files not verified before upload; insecure update server; hardcoded credentials
Poor physical security	Device easy to disassemble; access to software via USB ports; removable storage media

\*Table adapted from [www.owasp.org/index.php/Top\\_IoT\\_Vulnerabilities](http://www.owasp.org/index.php/Top_IoT_Vulnerabilities).

vulnerabilities, patches or work-arounds might not be downloaded for a very long period of time. Under these conditions, intrusion-detection techniques become even more important. In addition, as many of the devices themselves might not have powerful processors or sufficient memory, the intrusion-detection analysis will likely occur at a gateway device.

## A LONGER-TERM IOT SECURITY STRATEGY

Mirai is just the first of a novel category of botnets that exploit IoT devices and systems. Unfortunately, as history shows, the deployment of defenses against a given security threat is soon followed by new attack methods, such as recent DDoS amplification attacks that use spoofed source IP addresses to make it difficult for defenders to trace the attack's origin.<sup>7</sup> Thus, we can soon expect more sophisticated attacks than Mirai with even more devastating consequences. In particular, because many IoT systems and devices have actuation capabilities and can modify

the physical environment, attacks to such systems and devices could result in major safety risks and endanger human life. Devising IoT-specific security techniques must be a research priority.

Defenses against conventional botnets can be broadly categorized into prevention, monitoring, and response.

Preventing bot infections is the most effective defense. This can be accomplished through antivirus software complemented by intrusion-prevention systems, firewalls, content filtering and inspection technologies, and application whitelisting. User awareness is also critical, as malware often spreads because of user mistakes, such as clicking on email attachments. For example, Locky, a recent ransomware strain that also recruited infected machines into a botnet, was distributed via a large-scale email spam campaign.<sup>8</sup>

However, machines can become infected despite the use of security techniques. It's therefore critical to monitor network and device behavior for anomalous events or trends that might indicate the presence of a threat.

Network behavior analysis (NBA) programs—which can be installed and operated by administrators or provided by third-party services—continuously monitor data flows from routers and other sources and flag departures from established baselines for traffic volume, bandwidth use, protocol use, and other metrics. Users can also take a more active role in threat detection by reporting typical machine infection signs such as longer start-up or shut-down times, frequent crashes, unexplained error messages, and unusually slow operation.


If signs of a potential DDoS attack or infected machine are detected, a prompt response is critical to minimize damage and prevent the malware from spreading. Responses can vary from simple actions such as disconnecting a suspect machine from the network to tracking, analyzing, and taking down botnets. NBA tools can carry out some mitigation actions—for example, they can redirect potentially malicious traffic to other hosts using the Border Gateway Protocol or similar

routing mechanisms. However, advanced actions such as disabling a botnet might require the involvement of specialized security companies or law-enforcement agencies.

Deploying these various defenses won't be trivial given the large number of IoT devices and their inherent vulnerabilities. It's thus essential to extend existing security mechanisms such as encryption, authentication, access control, network security, and application security to fit the IoT ecosystem. For example, techniques and tools are needed to analyze firmware for flaws such as authentication bypass back doors.<sup>9</sup> Devising methods for discovering, identifying, and monitoring IoT devices is also critical. For example, the adoption of stronger passwords and/or a whitelist of addresses from which it's possible to log into IoT devices and to which IoT devices can send traffic would have prevented the exploitation of such devices by the Mirai botnet.

However, understanding which combination of techniques and tools should be used to protect IoT systems is challenging due to the wide diversity of IoT applications and scenarios. In addition, the selection might depend on the processes in place for managing software. It's reasonable to assume that companies creating IoT devices for privacy-sensitive or safety-critical applications would perform firmware analysis, but many companies in the consumer IoT space might not do so. Thus, a security strategy must also include a thorough risk assessment.

An important advantage to keep in mind, however, is that many of today's IoT devices have specialized functions with very limited input, and thus they behave quite predictably. This makes it easier to establish baseline actions within monitoring tools to detect anomalies that could indicate potential attacks or compromised devices. To keep such an approach scalable, such monitoring activities could be carried out by IoT routers or gateways.

Although most IoT systems are closed and tailored to specific applications, such systems pose formidable security challenges because of the large number and diversity of devices, communication media, communication protocols, and software. So even testing IoT systems might be very difficult. In addition to scalability and interoperability issues, IoT ecosystems contain many different parties, each performing security-relevant functions—assigning identifiers to IoT devices, patching device software, and so on. Keeping track of information, such as device cryptographic keys and who is responsible for which security aspects of devices, in massive distributed systems with multiple security/administration domains is complex and yet critical. 

## REFERENCES

1. S.K. Bansal, "Linux Worm Targets Internet-Enabled Home Appliances to Mine Cryptocurrencies," *The Hacker News*, 19 Mar. 2014; [thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html](http://thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html).
2. D. Goodin, "Record-Breaking DDoS Reportedly Delivered by >145K Hacked Cameras," *Ars Technica*, 28 Sept. 2016; [arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever](http://arstechnica.com/security/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever).
3. "KrebsOnSecurity Hit with Record DDoS," blog, 21 Sept. 2016; [krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos](http://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos).
4. US Computer Emergency Readiness Team, "Heightened DDoS Threat Posed by Mirai and Other Botnets," alert TA16-288A, 14 Oct. 2016 (revised 30 Nov. 2016); [www.us-cert.gov/ncas/alerts/TA16-288A](http://www.us-cert.gov/ncas/alerts/TA16-288A).
5. E. Bertino, "Data Security and Privacy in the IoT," *Proc. 19th Int'l Conf. Extending Database Technology (EDBT 16)*, 2016; [openproceedings.org/2016/conf/edbt/paper-a.pdf](http://openproceedings.org/2016/conf/edbt/paper-a.pdf).
6. "HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack," press release, HP Inc., 29 July 2014; [www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WEWz17IrKos](http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676#.WEWz17IrKos).
7. J. Krupp, M. Backes, and C. Rossow, "Identifying the Scan and Attack Infrastructures behind Amplification DDoS Attacks," *Proc. 2016 ACM SIGSAC Conf. Computer and Comm. Security (CCS 16)*, 2016, pp. 1426–1437.
8. Symantec Security Response, "Locky Ransomware on Aggressive Hunt for Victims," Symantec Corp., 18 Feb. 2016; [www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims](http://www.symantec.com/connect/blogs/locky-ransomware-aggressive-hunt-victims).
9. Y. Shoshitaishvili et al., "Firmalice—Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware," *Proc. 2015 Network and Distributed System Security Symp. (NDSS 15)*, 2015; [www.lastline.com/papers/2015\\_ndss15\\_firmalice-2.pdf](http://www.lastline.com/papers/2015_ndss15_firmalice-2.pdf).

**ELISA BERTINO** is a professor of computer science and a courtesy professor of electrical and computer engineering at Purdue University, where she is also director of the Cyber Space Security Lab (Cyber2Slab). Contact her at [bertino@purdue.edu](mailto:bertino@purdue.edu).

**NAYEEM ISLAM** is a vice president and head of corporate research and development at Qualcomm Research Silicon Valley. Contact him at [nayeem.islam@gmail.com](mailto:nayeem.islam@gmail.com).

**myCS** Read your subscriptions through the myCS publications portal at <http://mycs.computer.org>