Advanced Topics in IP Networks
Lecture 12

Lecture by Dr. Anat Bremler-Barr
Typeset by Steven Karas

2019-01-03
Last edited 20:59:56 2019-01-03

Disclaimer These notes are based on the lectures for the course Advanced Topics in IP Networks, taught by Dr. Anat Bremler-Barr at IDC Herzliyah in the fall semester of 2018/2019. Sections may be based on the lecture slides prepared by Dr. Anat Bremler-Barr.

1 Agenda

- IoT security
- DNS
- Project ideas

2 IoT security

The internet of things is a buzzword that describes all the non-personal computing devices that are network-connected. There are many types of IoT devices, from home appliances to industry specific devices such as agritech, retail, and transportation. One of the visions of IoT is direct device to device communication.

Industrial IoT devices are typically pushed into their own field, as they often do not use the same protocols, have different connectivity requirements, etc.

IoT will typically use mostly standard protocols such as WiFi, Bluetooth, Zigbee, etc. There are however many custom protocols to bridge IoT specific needs such as LoRa, 6LowPAN, NB-IoT, MQTT, etc.

There are many new devices, from many vendors, at low price points, low in resources, and seldomly updated, if at all. As such, this presents a huge attack surface.

Privacy is a major concern with IoT, as the large attack surface and abundant sensors can allow massive data leakage. **Safety** is another concern, as some IoT devices may control essential safety systems, such as elevators or cars. **Sabotage** is yet another major issue because even if people aren't hurt, improperly heating a building can ruin or destroy property.

Mirai Attack Leading up to October 21, 2016 the attackers used default or common credentials to compromise over 500K IoT devices. On October 21, 2016 the botnet mounted a DDoS attack on DyN, a major DNS provider, which took down Netflix, Spotify, Twitter, and others.

2.1 IoT connectivity

IoT devices being accessed on the local network is typically a non-issue. However, when trying to access the devices remotely for example from your work computer, several solutions are used. The first generation of IoT solutions relied on fixed IPs or DDNS to route, and configured Port Forwarding/UPnP to route the remote traffic to the device. The currently favored approach is cloud-based, in that the device connects to the vendor's servers, and then client devices connect to the vendor's servers. In more modern devices, a hybrid solution is used which prefers direct communication when locally based. Home/SMB networks have a tendency to have complex topologies, with multiple hubs and different link types.

A SOTA attack uses DNS rebinding to attack devices by pivoting around the firewall/NAT. This means that security should be designed assuming that the firewall/NAT does not protect it explicitly.

2.2 What can we do?

Tracking and managing devices is the first step. Once we understand which devices need connectivity, we can monitor and restrict access to them. We can also understand the normal behavior and alert on anomalous behavior or even automatically block it. We can set stronger credentials in order to access devices.

When designing products, we can ensure that they only require connectivity if absolutely necessary. We can also design them with stronger authentication.

Governmental regulation is also beginning to take a larger role. The "Internet of Things Cybersecurity Improvement Act of 2017" is an example of incoming regulation, however this only affect American vendors. The FTC fined ASUS and D-Link in separate cases for failing to properly implement security controls for home routers. Similarly, the ISP/CSP/Telco can proactively secure their customers in preventing malicious traffic and contacting customers with infected devices.

2.3 Security as a Service - IoTica

Dr. Bremler-Barr's current venture provides a NFV cloud solution for ISP/CSPs that automatically categorizes traffic. For example, collecting the list of domains and hard coded IPs a device connects to, the packet flow rates, etc. Current research directions are learning how to automatically classify IoT devices as opposed to personal computing devices.

Heimdall is a competing approach that uses a blacklist rather than a whitelist.

3 DNS security

The basic concept of DNS is that of an address book, translating human names into machine addresses. DNS uses a hierarchical structure, with root servers that point to the authoritative server for each top level domain, and so on. As such, it is a distributed global database. Using anycast, many servers can handle the requests for a given authoritative DNS server. DNS by default runs over UDP in a largely text format. For reliability, we also allow querying multiple servers and don't care which one responds first.

Recursive servers will make multiple requests and return an authoritative answer. Iterative servers will just return an answer with a more authoritative server for the query.

3.1 DNS caching

DNS replies are cached according to the TTL field. The recent trend is to use a much shorter TTL than in the past, with major websites such as cnn.com using a TTL of 60 seconds. Each layer of DNS will also keep an independent cache, for example at the ISP level, the OS, and the browser.

3.1.1 DNS Cache Poisoning

If we know that a client is asking a DNS query, an attacker can respond before the server and effectively steal the entire domain. This is a practical attack, for example when attacking another device on the same wireless network.

4 Next week

More on DNS, and disposable domains.

References

[1] Mark Crovella and Balachander Krishnamurthy. *Internet Measurement: Infrastructure, Traffic and Applications*. John Wiley & Sons, Inc., New York, NY, USA, 2006.

[2] James F. Kurose and Keith Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edition, 2002.

[3] George Varghese. *Network Algorithmics,: An Interdisciplinary Approach to Designing Fast Networked Devices (The Morgan Kaufmann Series in Networking)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2004.