How IPv6 may affect IoT Security

Fernando Gont

SI6 NETWORKS

FIRST TC

Montevideo, Uruguay. September 18, 2017

About...

- Security Researcher and Consultant at SI6 Networks
- Published:
  - 30 IETF RFCs (15+ standards on IPv6)
  - 10+ active IETF Internet-Drafts
- Author of the SI6 Networks' IPv6 toolkit
  - https://www.si6networks.com/tools/ipv6toolkit
- Admin of a few mailing-lists:
  - {**ipv6hackers**, **iot-hackers**, **sdn-hackers**}**@lists.si6networks.com**
- More information at: https://www.gont.com.ar

IPv6 and the Internet of ...Things

What this presentation is about

- More and more devices connected to the Internet
- “Internet of Things” -- not all of them really “constrained devices”
- How IPv6 may affect the security of these devices?
- How could we possibly mitigate the associated security implications?
- **Mostly a challenge to ideas you usually hear on the topic**

Characteristics of IoT Devices

Some characteristics of these devices

- Generally “cheap”
- May or may not be “constrained” devices
- Non-managed devices
- No automatic updates
- May have default login credentials (some in firmware)
- Use of insecure protocols
- Many assume “secure” local network and insecure Internet

Some sample “smart” devices

TP-Link Smart Plugs (HS110, HS100)

HS110

- Allow remote operation of on/off switch
- Allow timers, event scheduling, etc.
- Some (HS110) are able to measure power consumption
- Can be locally-operated (WiFi)
- Also allow for “cloud” operation

TP-Link Smart Plug Operation

- Main protocol: TP-Link Smart Plug Protocol
  - Local protocol
  - “Obfuscated” rather than properly encrypted
  - Used for:
    - Device discovery
    - Device configuration
    - Polling and/or modifying device state
    - Available on port 9999 for both TCP and UDP
- Also support TDDP, a local debugging protocol
- Also allow for “cloud” operation
  - Via cloud server with HTTPS

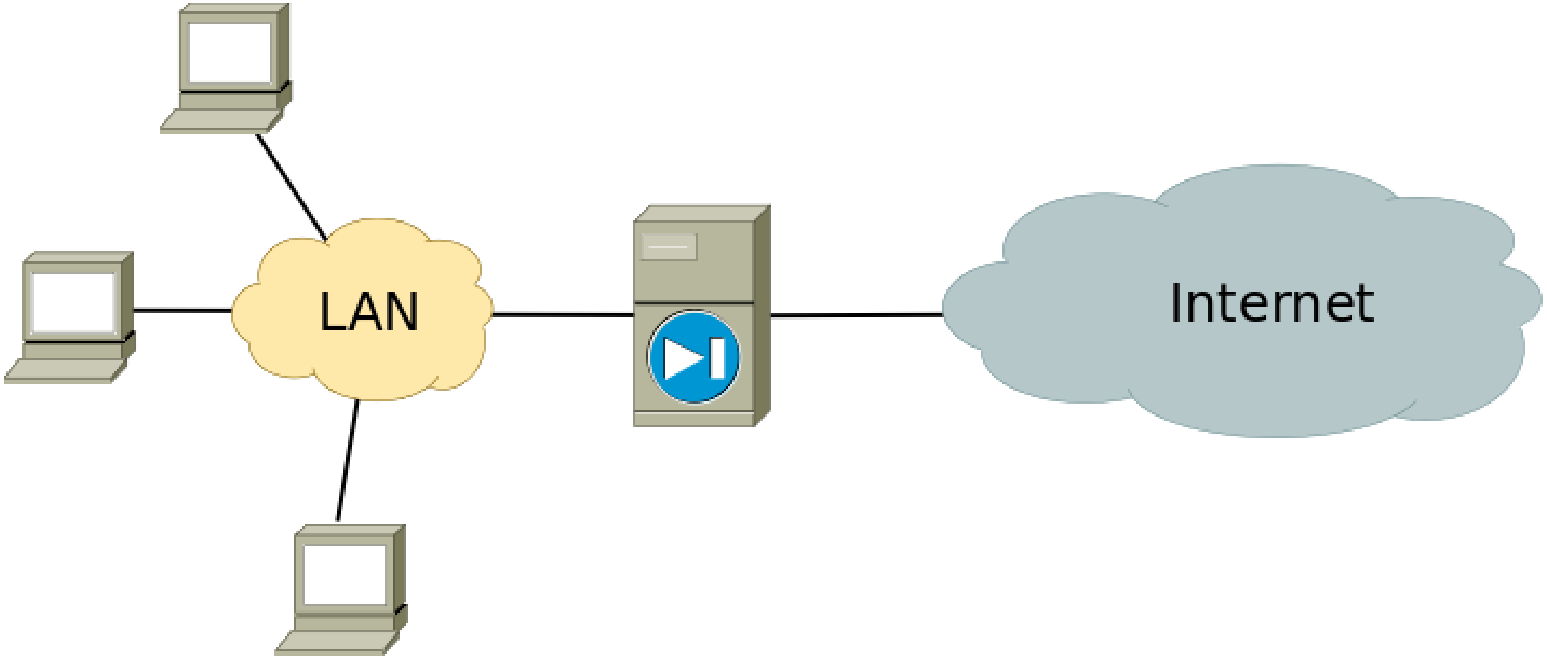
Some problems with these devices

- Two total different scenarios: local vs. remote attacker
- Local attacker:
  - Has **full** control of these devices
- Remote attacker:
  - Needs to authenticate with cloud server (*)
  - Relying on “cloud” support is questionable

Deployment model for IPv4

Deployment model for IPv4

- NATs partition the network into inner and external realm



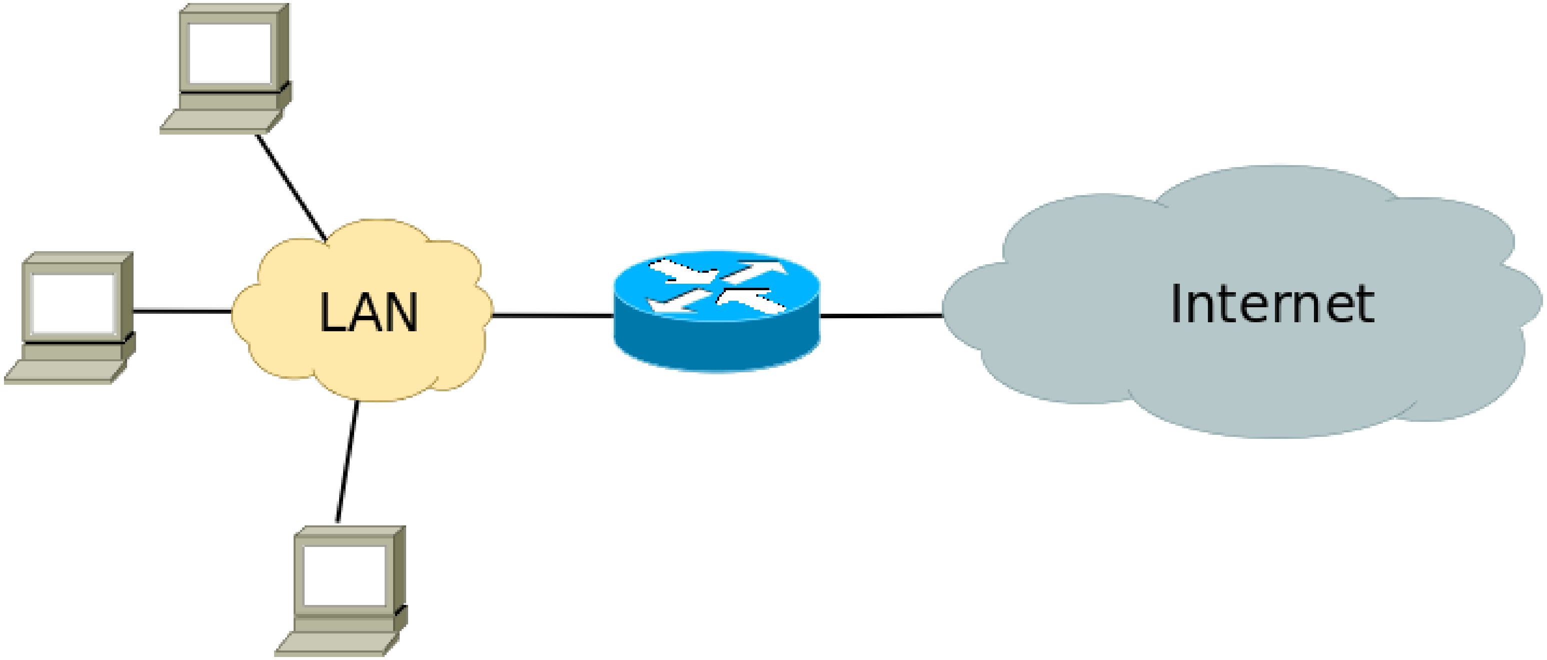
Deployment model for IPv4 (II)

- Incoming communications to the internal realm not allowed
  - (compartmentalization)
- This can help mitigate some problems
  - You may not exploit a vulnerability if you can't reach the device
  - This does not fix the underlying issues, but may impede their exploitation

Deployment model for IPv6

Deployment model for IPv6

- The whole point of IPv6 is its increased address space
  - Large enough to provide multiple addresses to each connected device
- Many people assume that IPv6 implies total host exposure
  - any-to-any communication between all connected devices



How IPv6 may affect IoT security

How IPv6 may affect IoT security

- The ~~dream~~ nightmare of fully-connected ~~IoT~~ IoSh*# network made real!
- Zillions of flawed devices directly reachable from the public Internet
    - Lightbulbs, cameras, DVDRs, fridges... you name it.
- Insecure protocols meant for local use may now become usable in global/remote context
- Connectivity requirements essentially depend on:
    - Push vs pull model
    - Most of these IoT devices employ the pull model!

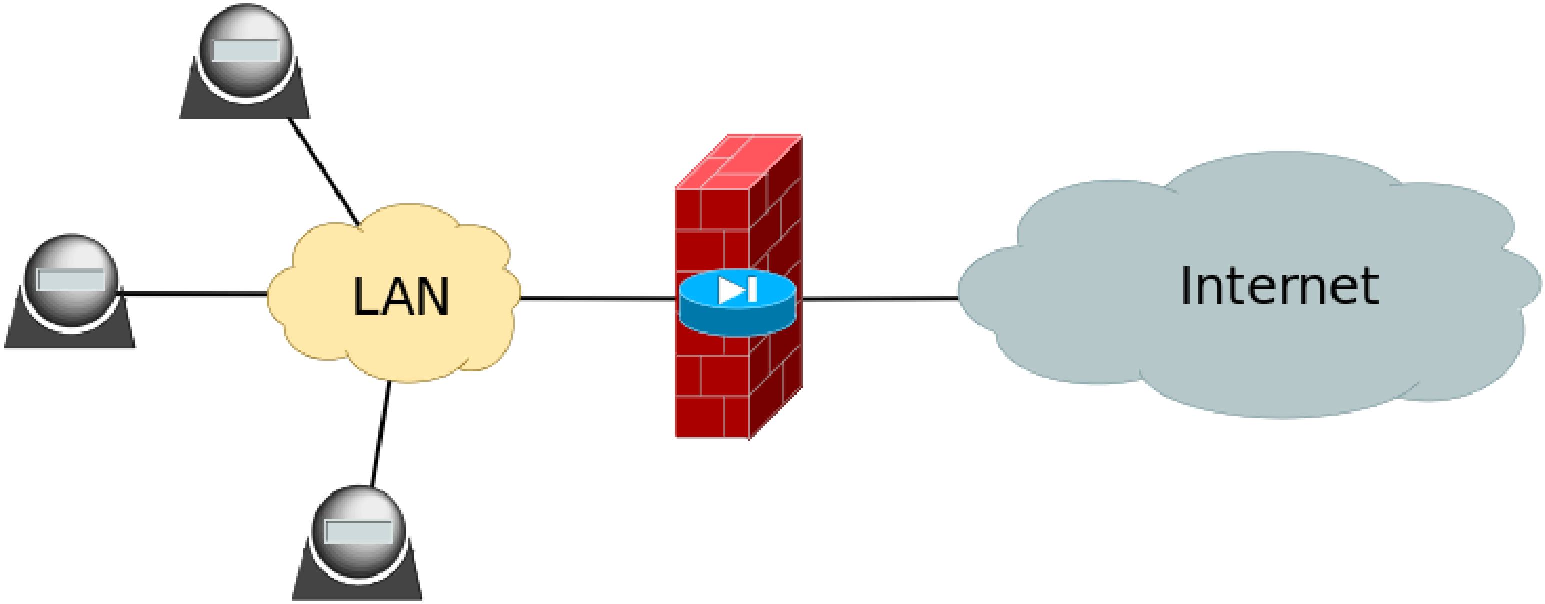
Do we actually need global reachability?

Do we need global connectivity?

- Connectivity requirements essentially depend on push vs. pull model. e.g.,
  - Should a device be polled for information or “pushed” actions?
  - Or, should the device just report updates to and pull actions from, e.g., central server?
  - Or, maybe, contact all devices via central server?
- Virtually all IPv4 smart devices currently employ pull model, or communicate via server
- Same “model” could apply to IPv6, and hence IoT devices may be connected to the Internet with a “diode” firewall
  - This is a side-effect in IPv4 NAT

Do we need global connectivity?

- By default, consider connecting your devices to the Internet via a “diode” firewall



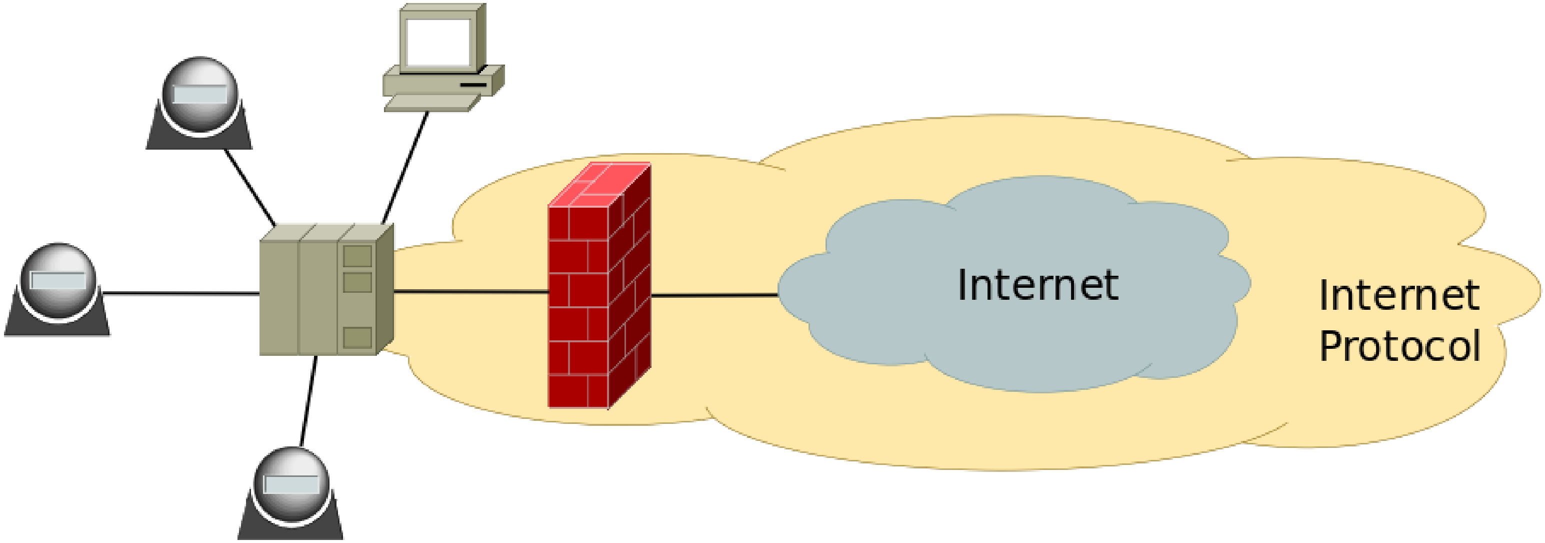
Do we actually need global addressability?

Do we need global addressability?

- Global addressability implies that each device gets global routable address
- Needed if one expect devices to “talk” directly to other devices
  - Is this really needed?

Do we need global addressability? (II)

- An alternative model:



Do we need global addressability? (III)

- Benefits:
  - Less code at devices (possibly no IP stack)
  - Communications go through (hopefully more secure) gateway
- “Drawbacks”:
  - “*Part of the network is not IP*” -- think of that part as a single distributed system!

Conclusions

Conclusions

- IPv6 could potentially increase the exposure of insecure systems and protocols
- Apply the “principle of least privilege” to mitigate potential issues

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IoT Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com