College of Engineering and Applied Science
University of Colorado **Boulder**

Automatic Segregation of Network Traffic Using UPnP – A Consumer IoT Security Design

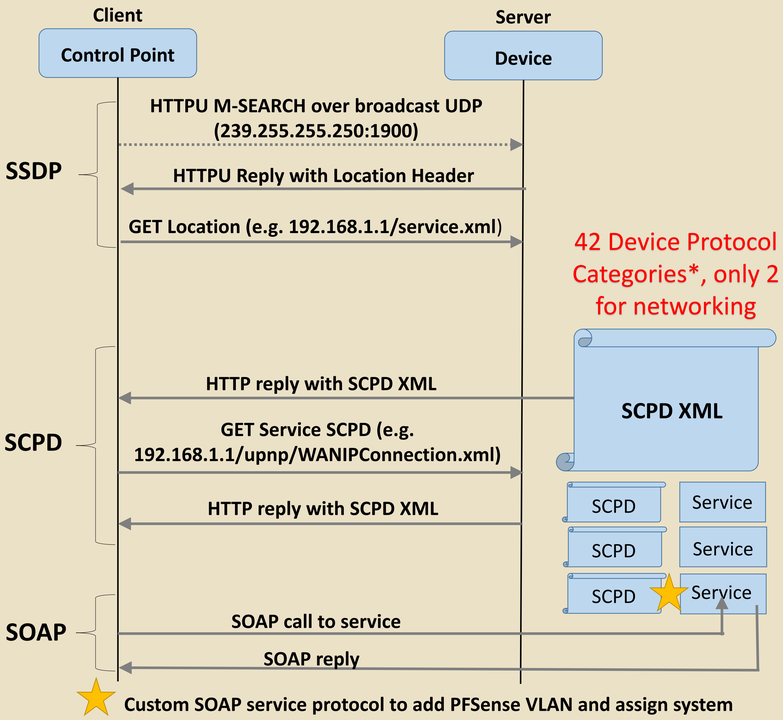
Karl Olson, Hima Boddupalli
Dr. Nolan Scaife – CSCI 7000-015 (Topics in Network Security) – Department of Computer Science

Background

- **UPnP and NAT-PMP are nearly ubiquitous device connectivity protocols used by many home routers and smart devices to streamline user connectivity and setup.**
- **Many flaws and shortcomings in protocol design and incorrect vendor implementations have resulted in high profile network and device vulnerabilities utilizing the protocol.**
- **With increase in prevalence of Internet of Things and smart devices within the home, security risks and user exposure will increase due to each connected device having full authenticated access to the local network.**
- **While solutions have been proposed that focus on improving the security of UPnP, no effort to date has questioned the need for devices to have full authenticated access to the network (Threat Model mismatch).**
- **Many IoT/Smart Home devices rarely are patched and may go their entire life without fixing a vulnerability**
- **Competing proposals to UPnP such as OCF, AllJoyn, UPnP+ and Thread continue to fail to address concerns in proper device segregation and network access.**

OPEN CONNECTIVITY FOUNDATION · UPnP · AllJoyn · Fairhair Alliance · THREAD

UPnP Protocol Operation

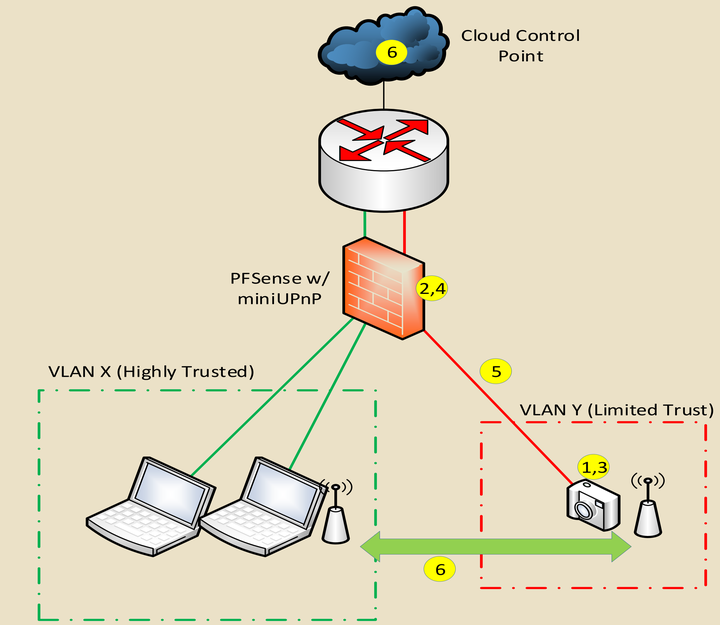


* Available in UPnP Specification, rarely are more than 2-3 ever implemented
SSDP - Simple Service Discovery Protocol (Discover UPnP Devices on Network)
SCPD - Service Control Point Definition (Defines services on control point)
SOAP - Simple Object Access Protocol (Calling actions on device)

Research Questions

1. **Can we improve security of a local network comprised of authenticated privileged systems and IoT/Smart Home devices without sacrificing the ease of consumer setup?**
2. **What levels of access do home devices require in order to operate under the concept of least privilege?**
3. **Can we utilize an automatic configuration protocol, such as UPnP, to segregate network access between privileged and unprivileged systems?**
4. **How can we identify a device appropriately to ensure it is placed on the right network segment for operation without involving user input?**
5. **How has the threat model changed since inception of UPnP and are we addressing current and emerging concerns correctly?**

Experimental Setup / Operation



1. **New device connects to network and initiates SSDP discovery.**
2. **miniUPnP server responds with location and SCPD xml list of services. Device obtains list of services on firewall.**
3. **Device Identifies itself as IoT Device and need for segregated network access through SOAP request**
4. **miniUPnP server utilizes SOAP instruction to create VLAN on Firewall and segregate traffic**
5. **Devices operates on segregated network. In case of compromise or vulnerability, device would not provie authenticated access to other home systems.**
6. **Recommendation for device configuration through *direct* wifi connection or through authenticated connection to cloud control point.**

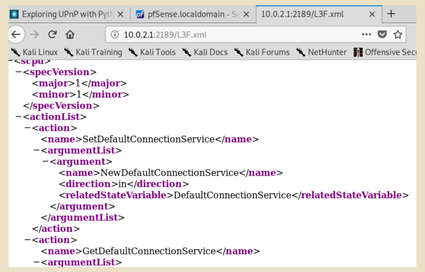
Results / Discussion

1) Not all UPnP Implementations are the same! Device/Vendor specific.

Some allow UPnP setup by VLAN – User intensive Configuration

With our program, we are able to scan network for UPnP devices, pull their service listing and call SOAP actions.

No DeviceSecurity:1 Implementation!



However, SOAP actions are tied to vendor implementation by UPnP standard. No opportunity to implement VLAN without modifying vendor source code.

2) Automating network segregation will require each vendor to implement independently.

-likely an unattainable proposition (thousands of patches, users, etc)
-demonstrates need to update threat model and standard

3) Appears vendors using advanced security features as business model

- **Future solutions for open connectivity need to consider device segregation; home router devices need to include support for this as a factory feature.**

Recommendations / Future Work

- **Create server module of SOAP instruction set to automate VLAN Creation and Segregation; integrate with miniUPnP server**
- **Review Applicability of Threat Model against other competing open connectivity protocols/frameworks to ensure completeness. Are protocols addressing appropriate threats and protecting user confidentiality and security in case of compromise?**
- **Assess devices against concept of least privilege based on operation need.**
- **Apply methods of consideration for contested and shared control environments**
- **Review cloud based security concerns and control options; do cloud connected devices change considerations?**

Acknowledgements:XXXXXXXXXX
Project Funded Under Grant#: XXXXXXXXX

For Presentation At:XXXXXXXXX
Date: XXXXXXXXX