UPnP mapping

Daniel Garcia
(FormateZ)
Toor.do

Introduction

- Who am I ?
- What is UPnP(Universal Plug and Play) ?
- What is an IGD(Internet Gateway Device) ?
- How many IGD devices are on on-line ?

UPnP hacking timeline

2001 – Ken from FTU – Three windows UPNP DoS attacks

2001 – Eeye – Multiple remote BoF XP/ME/98

UPnP

2003 - Björn Stickler - Netgear FM114P UPNP information

Disclosure

2006 – Armijn Hemel (www.upnp-hacks.org)

2008 – GNUCitizen(Adrian Pastor, Petko Petkov)

Main problems

- It uses the words “Plug and Play”

- No authentication

- Most stacks don't validate data

- Allowing indiscriminate WAN requests

- Some devices don't log UPnP requests

Devices affected(So far)

Manufacturer	Model	Version
Linksys	WRT54GX	< 4.30.5
Edimax	BR-6104K	< 3.21
Sitecom	WL-153	< 1.39
Speedtouch/Alcatel/Thomson	5x6	< 6.2.29
Thomson	TG585 v7	< 7.4.3.2

Umap / What is it ?

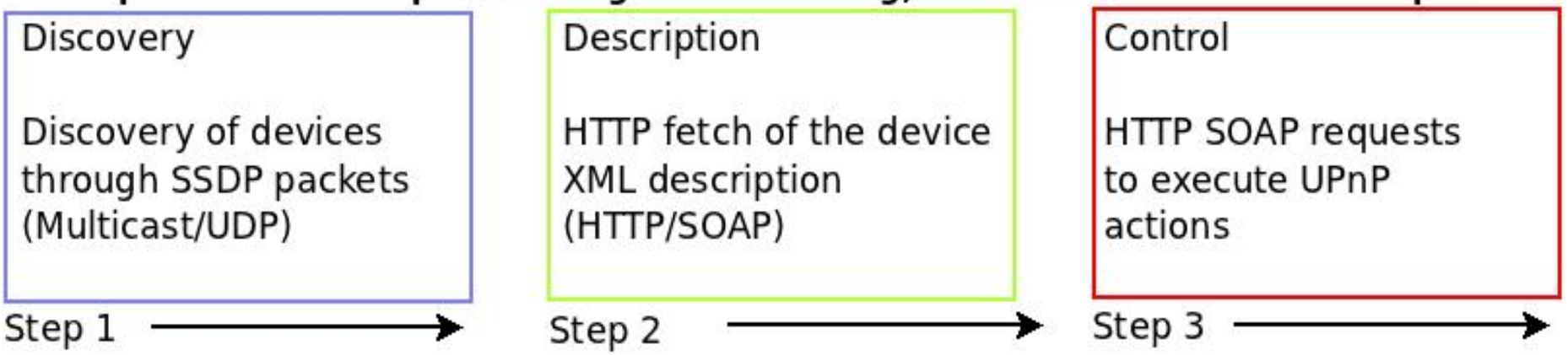
- SocksV4 proxy server that automatically forward's Requests through UPnP devices

- TCP/UDP scanner for hosts behind an IGD NAT

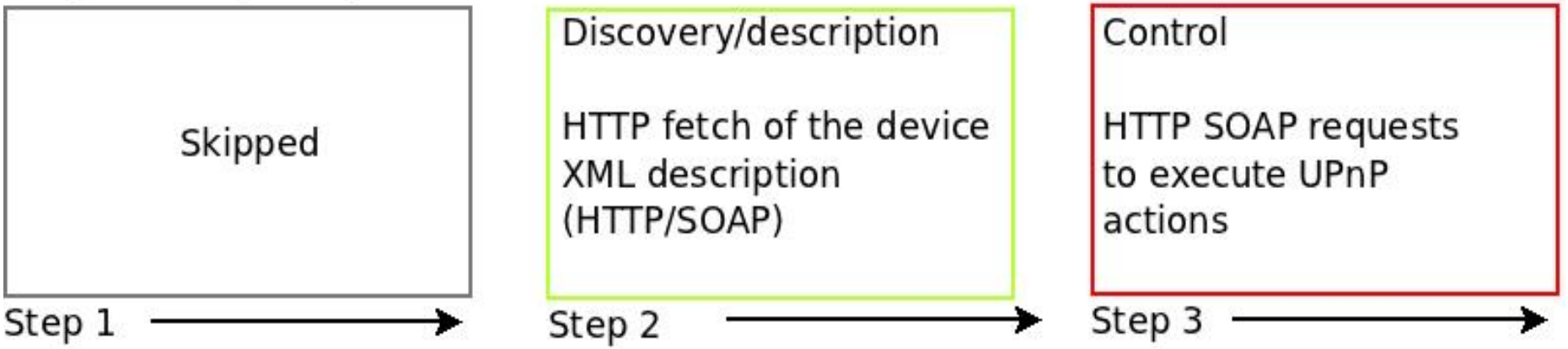
- Manual port mapper for UPnP devices

Umap / How does it work ?

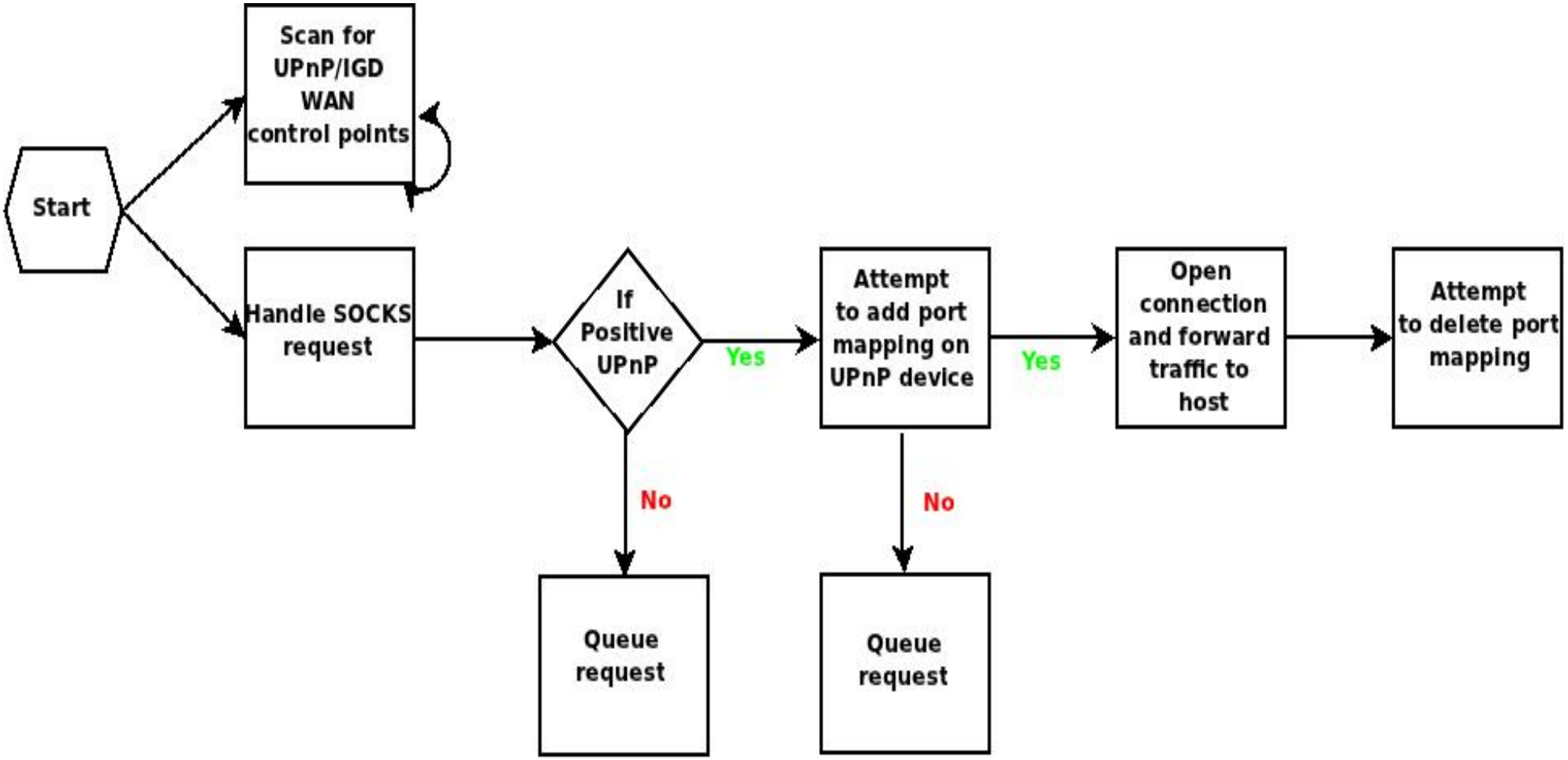
UPnP protocol v1.0 steps excluding the Addressing, Events and Presentation steps.



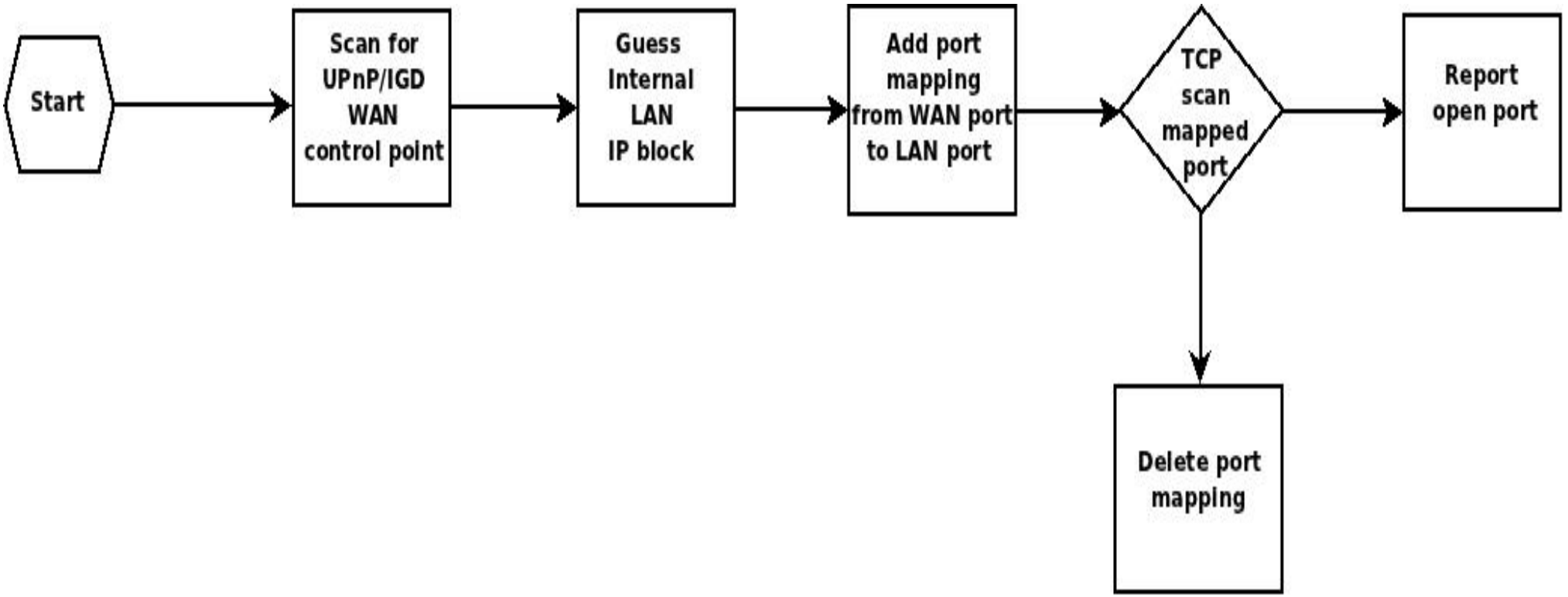
Steps used by Umap



Umap / How does it work ?



Umap / How does it work ?



UPnP mapping cons

- UPnP stacks are buggy/unstable

- Limited bandwidth

- Protocols with heavy amounts of connections don't work well

- Some devices actually report having the port mapping functionality, but don't do anything

Umap Demo
SOCKS Proxy mode

Umap Demo
Internal LAN scanning

Umap Demo
Manual port mapping

Mitigation

- Disabling UPnP actions from being executed on the WAN

- Operators using base configurations with UPnP disabled

- On some cases, disabling UPnP (things might break)