**Spoofing SSDP and UPnP Devices with EvilSSDP**

## **SSDP & UPnP Overview**

SSDP (Simple Service Discovery Protocol) is utilized for network service advertising and discovery, operating on UDP port 1900 without needing DHCP or DNS configurations. It's fundamental in UPnP (Universal Plug and Play) architecture, facilitating seamless interaction among networked devices like PCs, printers, and mobile devices. UPnP's zero-configuration networking supports device discovery, IP address assignment, and service advertising.

## **UPnP Flow & Structure**

UPnP architecture comprises six layers: addressing, discovery, description, control, eventing, and presentation. Initially, devices attempt to obtain an IP address or self-assign one (AutoIP). The discovery phase involves the SSDP, with devices actively sending M-SEARCH requests or passively broadcasting NOTIFY messages to announce services. The control layer, vital for client-device interaction, leverages SOAP messages for command execution based on device descriptions in XML files.

## **IGD & Tools Overview**

IGD (Internet Gateway Device) facilitates temporary port mappings in NAT setups, allowing command acceptance via open SOAP control points despite standard WAN interface restrictions. Tools like **Miranda** aid in UPnP service discovery and command execution. **Umap** exposes WAN-accessible UPnP commands, while repositories like **upnp-arsenal** offer an array of UPnP tools. **Evil SSDP** specializes in phishing via spoofed UPnP devices, hosting templates to mimic legitimate services.

## **Evil SSDP Practical Usage**

Evil SSDP effectively creates convincing fake UPnP devices, manipulating users into interacting with seemingly authentic services. Users, tricked by the genuine appearance, may provide sensitive information like credentials. The tool's versatility extends to various templates, mimicking services like scanners, Office365, and even password vaults, capitalizing on user trust and network visibility. Post credential capture, attackers can redirect victims to designated URLs, maintaining the deception's credibility.

## **Mitigation Strategies**

To combat these threats, recommended measures include:

* Disabling UPnP on devices when not needed.
* Educating users about phishing and network security.
* Monitoring network traffic for unencrypted sensitive data.

In essence, while UPnP offers convenience and network fluidity, it also opens doors to potential exploitation. Awareness and proactive defense are key to ensuring network integrity.