A Look at the Hardware Security of Wireless Communication

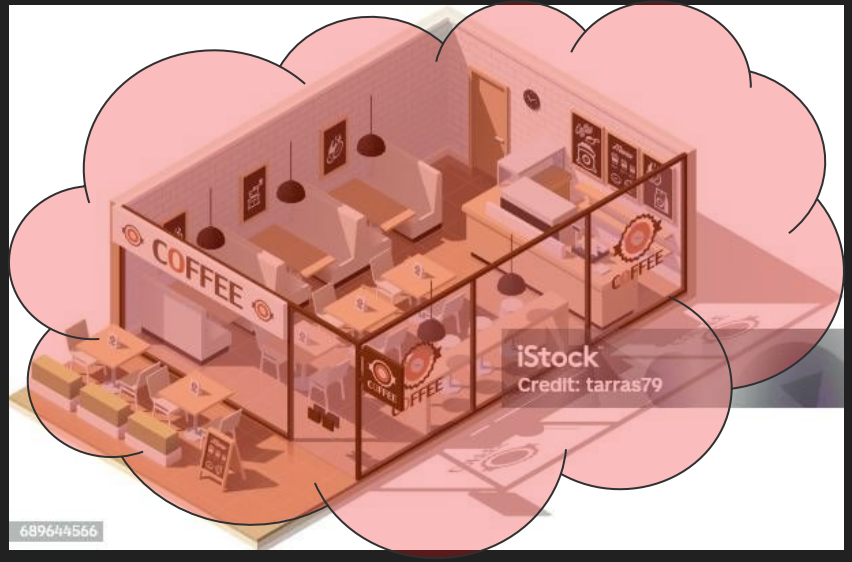
Barak Binyamin

Contents

- Security Analysis
- Attacks in Action
- Patch
- Closing Comments

Security Analysis: Attack Surface

Wired



Wireless

Security Analysis

What happens when we physically expose our communications to the air?

Security Analysis

What happens when we physically expose our communications to the air?

- Spoofing
  Malicious router broadcasting the same name/ssid as a trusted router
- Tampering
  Man in the middle altering data
- Information disclosure
  Man in the middle capturing data
- Repudiation
  Malicious router can imitate authorship credentials
- Denial of Service
  Flooding a communication channel with noise or sending Deauth udp packets
- Elevation of Privilege
  User device can become a malicious router

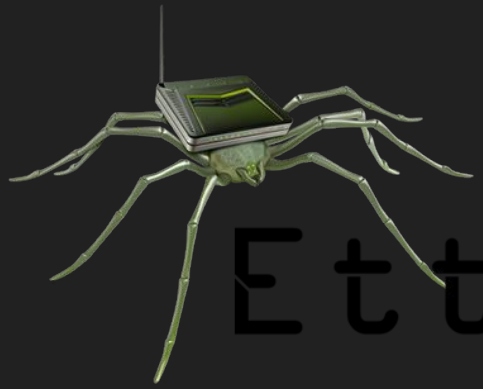
Free Wireless Analysis & Attack Tools

MARAUDER

TCPDUMP & LIBPCAP

fing

WIRESHARK



Ettercap

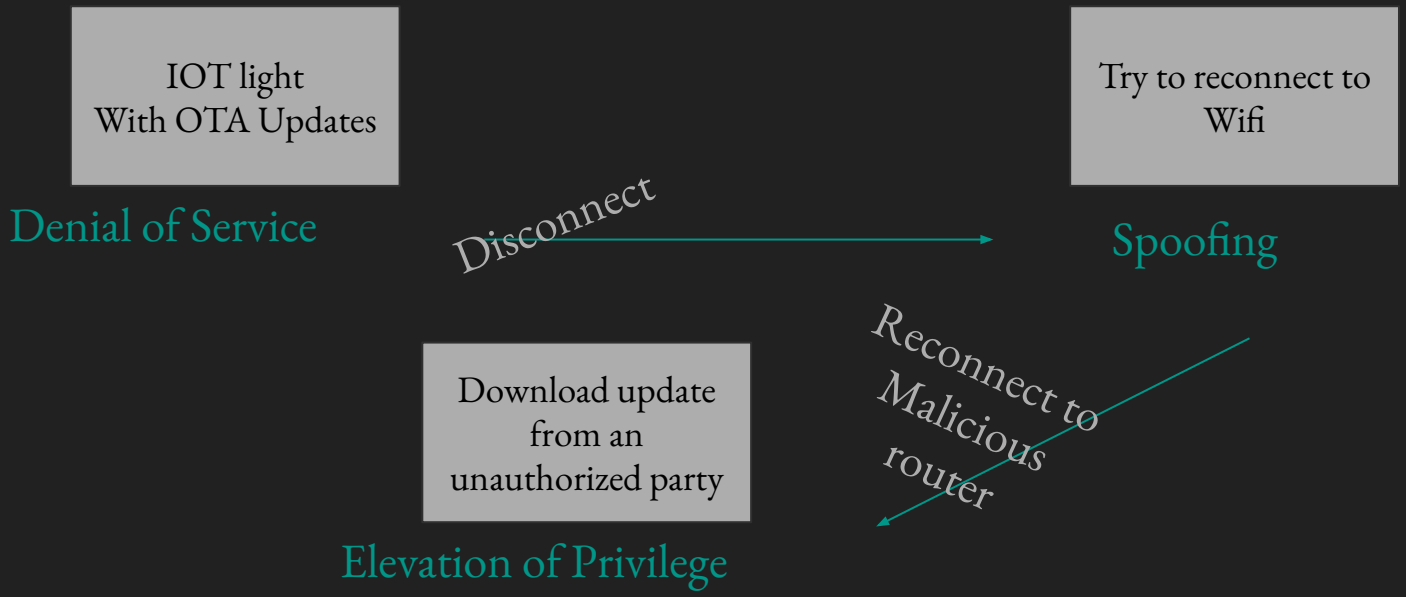
Attacks in Action

Denial of Service

Disconnect

Attacks in Action

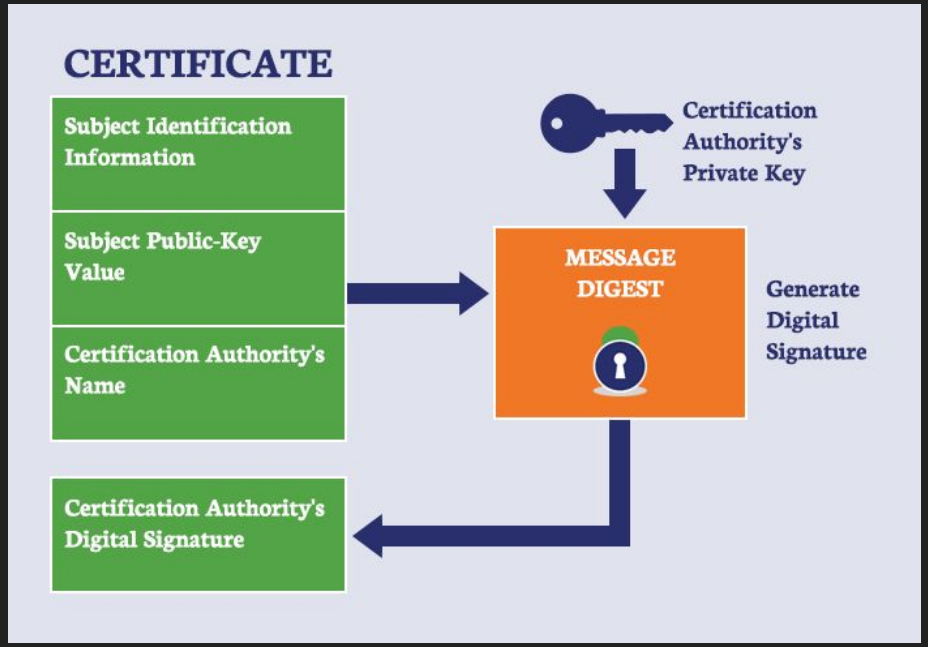
Attacks in Action



Similar Attack in Action

A Patch For Verifying Authorship

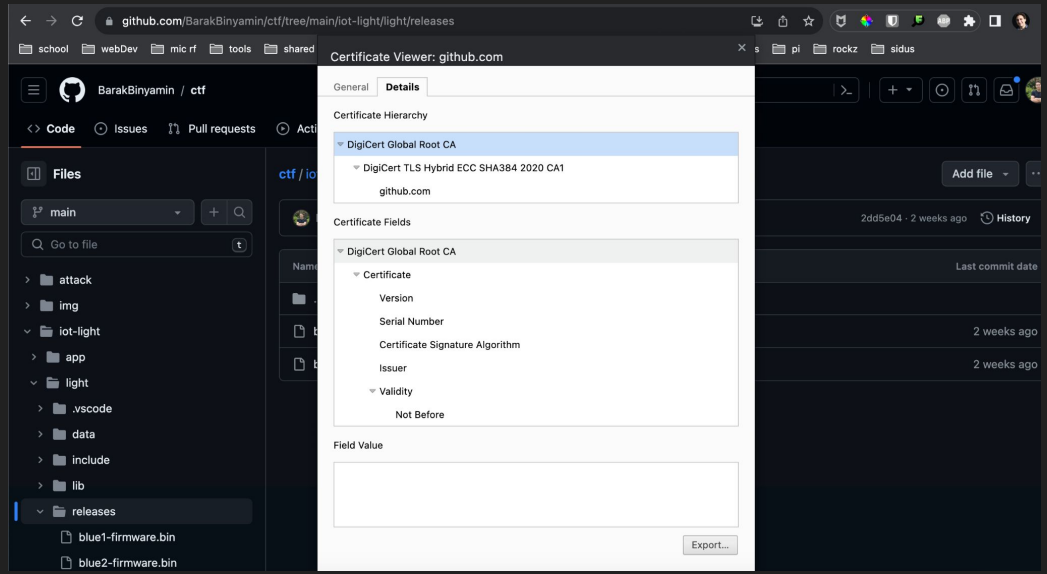
Use TLS to the fullest, by verifying the certificate signature



[1]

```
110
111  // Get the firmware
112  HTTPClient client;
113  bool success = false;
114  client.begin(updateURL.c_str(), root_certificate);
115  int httpResponseCode = client.GET();
116  if (httpResponseCode>0 && httpResponseCode == HTTP_CODE_OK) {
117    int totalBytes      = client.getSize();
118    int bytesLeftToRead = client.getSize();
119    uint8_t      buff[2048] = { 0 };
120    WiFiClient * stream     = client.getStreamPtr();
121    while(client.connected() && bytesLeftToRead > 0) {
122      // get available data size
123      size_t size = stream->available();
124      if(size) {
125          int numBytesToWrite = stream->readBytes(buff, ((size >
```

A Patch For Verifying Authorship




```
const char*      root_certificate = "-----BEGIN CERTIFICATE-----\n"        \
"MIIDrzCCApegAwIBAgIQCDvgVpBCRrGhdWrJWZHHSjANBgkqhkiG9w0BAQUFADBh\n"  \
"MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3\n"  \
"d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD\n"  \
"QTAeFw0wNjExMTAwMDAwMDBaFw0zMTExMTAwMDAwMDBaMGExCzAJBgNVBAYTAlVT\n"  \
"MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxGTAXBgNVBAsTEHd3dy5kaWdpY2VydC5j\n"  \
"b20xIDAeBgNVBAMTF0RpZ2lDZXJ0IEdsb2JhbCBSb290IENBMIIBIjANBgkqhkiG\n"  \
"9w0BAQEFAAOCAQ8AMIIBCgKCAQEA4jvhEXLeqKTTo1eqUKKPC3eQyaKl7hLOllsB\n"  \
"CSDMAZOnTjC3U/dDxGkAV53ijSLdhwZAAIEJzs4bg7/fzTtxRuLWZscFs3YnFo97\n"  \
"nh6Vfe63SKMI2tavegw5BmV/Sl0fvBf4q77uKNd0f3p4mVmFaG5cIzJLv07A6Fpt\n"  \
"43C/dxC//AH2hdmoRBBYMql1GNXRor5H4idq9Joz+EkIYIvUX7Q6hL+hqkpMfT7P\n"  \
"T19sdl6gSzeRntwi5m3OFBqOasv+zbMUZBfHWymeMr/y7vrTC0LUq7dBMtoM1O/4\n"  \
"gdW7jVg/tRvoSSiicNoxBN33shbyTApOB6jtSj1etX+jkMOvJwIDAQABo2MwYTAO\n"  \
"BgNVHQ8BAf8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUA95QNVbR\n"  \
"TLtm8KPiGxvDl7I90VUwHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUw\n"  \
"DQYJKoZIhvcNAQEFBQADggEBAMucN6pIExIK+t1EnE9SsPTfrgT1eXkIoyQY/Esr\n"  \
"hMAtudXH/vTBH1jLuG2cenTnmCmrEbXjcKChzUyImZOMkXDiqw8cvpOp/2PV5Adg\n"  \
"06O/nVsJ8dWO41P0jmP6P6fbtGbfYmbW0W5BjfIttep3Sp+dWOIrWcBAI+0tKIJF\n"  \
"PnlUkiaY4IBIqDfv8NZ5YBberOgOzW6sRBc4L0na4UU+Krk2U886UAb3LujEV0ls\n"  \
"YSEY1QSteDwsOoBrp+uvFRTp2InBuThs4pFsiv9kuXclVzDAGySj4dzp30d8tbQk\n"  \
"CAUw7C29C79Fv1C5qfPrmAESrciIxpg0X40KPMbp1ZWVbd4=\n"                  \
"-----END CERTIFICATE-----\n";
```

Demo Time

Step 1	Step 2	Step 3
Start Malicious Router and Server	**Deauth** Your Devices, Some Will Auto Connect to the Malicious Router	An RIT Login Page May Pop Up on Your Devices

Closing Comments: Trusted Access Points

Trusted parties are a large source of risk

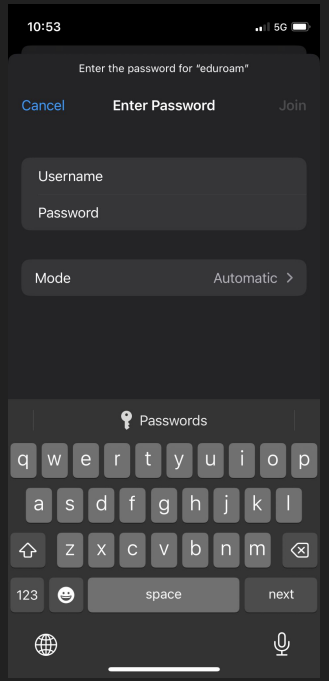
- Can we trust who we are communicating with (both sides?)

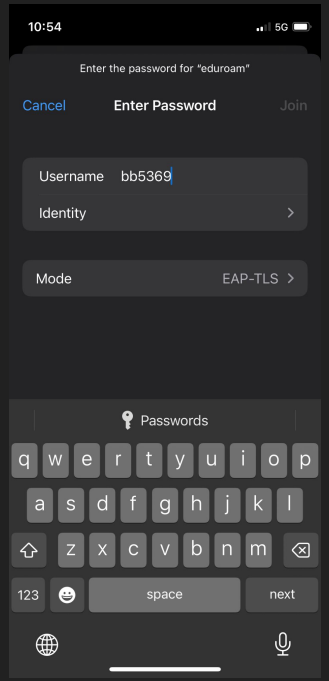
Our devices automatically connect to WiFi with familiar SSID and Password, no verification of authorship needed, which is a risky

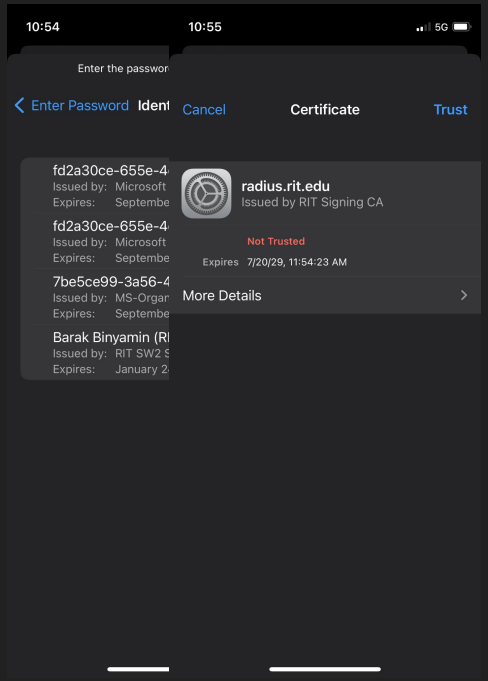
What is if wifi could use use the same principles to verify the authorship of various access points?

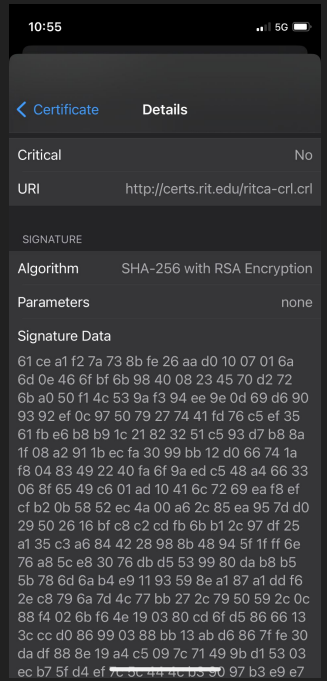
WPA-Enterprise: TLS option

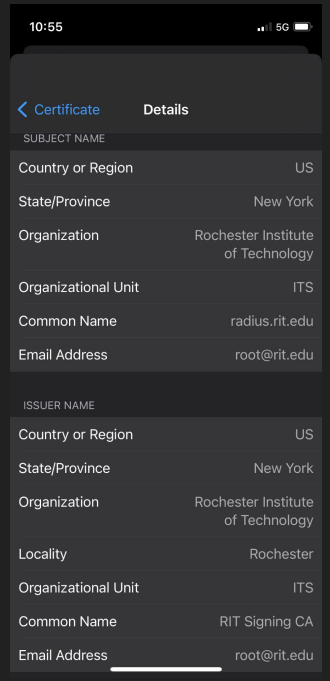
Trusted Access Points do exist, they're an option under WPA-Enterprise











Github

README.md

Capture The Flag

Attack surface, attack tooling, and patch included

Directory

- Project Directory
- Quickstart
- Motivation
- Resources
- References

LinkedIn

References

[1] Thesslstore, TLS Certs Image,
https://www.thesslstore.com/blog/ssltls-certificate-its-architecture-process-interactions/

[2] Ke2therm.com, Ethernet Network Topologies,
https://ke2therm.com/wp-content/uploads/2015/08/w-5-2_Understand_Ethernet_topologies.pdf

[3] Istockphoto, Free Coffee Shop,
https://www.istockphoto.com/vector/vector-isometric-low-poly-coffee-shop-gm689644566-127053561

[4] CDFER, Captive Portal ESP32,
https://github.com/CDFER/Captive-Portal-ESP32/blob/main/src/main.cpp

Q&A

What is the difference between SSL and TLS?

Transport Layer Security (TLS) is the upgraded version of SSL (Secure Socket Layer) that fixes existing SSL vulnerabilities

What is EAP?

Extensible Authentication Protocol, a protocol for wireless networks that expands the authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the internet

How do apps normally share WiFi?

Apps can prompt the user then share the way it wants, for apple devices, they can apply to join a special club called MFI which will allow the user to press a button to share all wifi credentials