禪

[[[[

[illegible]

Algorithm 1 ModulateOOK

1: procedure ModulateOOK(nLED, data, T)

2: openLED(nLED); //opens the LED file for writing

3: while(data[i] !=0)

4: if(data[i] == ‘0’) //modulate 0 by turning the LED off

5: setLEDOff(nLED);

6: if(data[i] == ‘1’) //modulate 1 by turning the LED on

7: setLEDOn(nLED);

8: i++;

9: sleep(T); // sleep for time period of T

10: closeLED(nLED); // closes the LED file descriptor

[illegible]

```
// Method #1

// turn the LED on

1: echo 0 > /sys/class/leds/led_name/brightness

// turn the LED off

2: echo 255 > /sys/class/leds/led_name/brightness

// Method #2
```

```
3: echo 1 > /proc/gpio/X_out // turn the LED on

4: echo 0 > /proc/gpio/X_out // turn LED off
```

این گروه از پژوهشگران امنیتی کد اثبات مفهومی خود را که بر پایه این تکنیک قادر است اطلاعات را فاش کند در قالب یک فایل ویدویی منتشر کردهاند . این ویدیو به وضوح نشان میدهد که آنها برای سرقت اطلاعات از چه بردار حملهای استفاده کردهاند . اگر یک هکر بتواند سیگنالهای ائیدی را از طریق یک دوربین دیجیتالی ضبط کند و در ادامه به دنبال جمعآوری اطلاعات از روی این فیلم ضبط شده باشد، در این حالت نرخ دستیابی به دادهها برای او به یک کیلوبیت بر ثانیه محدود خواهد شد .

یک دوربین GoPro Hero5 قادر است چشمک زدن چراغهای الئیدی را با نرخ 960 بیت در ثانیه ضبط کند، اما اکثر دوربینها تنها با نرخ 120 بیت بر ثانیه قادر به انجام اینکار هستند . همچنین اگر هکری به مسیریاب دسترسی فیزیکی داشته باشد، به شکل کارآمدتری قادر خواهد بود این بردار حمله را اجرایی کند . در این حالت نرخ دسترسی به دادهها از یک کیلوبیت بر ثانیه به 3.5 کیلوبیت بر ثانیه افزایش پیدا خواهد کرد . اینگونه به نظر میرسد که بهترین تکنیک برای حمله ضبط سیگنالهای الئیدی و کار روی میانافزارها و سیستمعامل روتر است .

نویسنده :
حمیدرضا تائبی
دسته بندی:
امنیت
تاریخ انتشار :
21:50 - 20/03/1396
برچسب:
امنیت - روتر - مسیریاب - کانال جانبی - هک - هکر - آسیبپذیری

نشانی
□□□□:https://www.shabakeh-mag.com/security/8150/%DA%86%D8%B1%D8%A7%D8%BA%E2%80%8C%D9%87%D8%A7%DB%8C-%D8%B1%D9%88%D8%AA%D8%B1%D9%87%D8%A7-%D8%A7%D8%B7%D9%84%D8%A7%D8%B9%D8%A7%D8%AA-%D9%85%D9%87%D9%85%DB%8C-%D8%B1%D8%A7-%D9%81%D8%A7%D8%B4-%D9%85%DB%8C%E2%80%8C%DA%A9%D9%86%D9%86%D8%AF