سیگنال‌های افشا کننده
سیگنال‌های وای‌فای از روی دست شما تقلب می‌کنند!

پژوهش‌گران موفق به طراحی سامانه‌ای شده‌اند که می‌تواند کلیدهای تایپ شده توسط کاربر را شناسایی کند. این سامانه از سیگنال‌های وای‌فای به منظور استخراج کلیدها استفاده می‌کند. زمانی که در حال فشار دادن کلید خاصی هستید، دستان و انگشتان شما قالب و مسیر حرکت منحصر به فردی به خود می‌گیرند و به این شکل یک الگوی منحصر به فرد را به وجود می‌آورند که این الگو باعث به وجود آمدن طول موجی در مقادیر CSI می‌شود که اکنون پژوهش‌گران می‌توانند آن‌را روبایش کنند.

تیمی متشکل از دانشمندان علوم کامپیوتر دانشگاه ایالتی میشیگان و دانشگاه نانجینگ پکن در مقاله‌ای به تشریح سامانه‌ای پرداختند که آن‌را WiKey نام‌گذاری کرده‌اند. سامانه‌ای که با اکثر دستگاه‌های وای‌فای (از قبیل روترها) مجهز به قابلیت چند ورودی/چند خروجی (multiple-input and multiple-output) سازگاری دارد. هر کانال مایمو بین هر یک از آنتن‌های ارسال-دریافت (TX-RX) متعلق به یک جفت گیرنده و فرستنده قرار گرفته و چندین زیرحامل (sub-carriers) را در معرض تهدید قرار می‌دهد.

مطلب پیشنهادی

در خدمت سرویس مخفی میکروفون
حملات فیزیکی برای استخراج کلیدهای رمزنگاری

این دستگاه‌های وای‌فای به طور پیوسته وضعیت کانال وای‌فای را برای انتقال موثر و بهبود نرخ سازگاری برای هر یک از MiMostreamها تحت نظارت قرار می‌دهند. اکثر روترها این توانایی را دارند تا وضعیت یک کانال وای‌فای را تحت نظر گرفته و اطلاعات حالت کانال (CSI) سرنام channel state information را برداشت کنند. این مقادیر CSI، به نوبه خود، توصیف کننده اطلاعاتی هستند که ما آن‌ها را پاسخ کانال فرکانس (CFR) یا نوسانات موجود در سیگنال به نمایش گذاشته شده میان هر یک از آنتن‌های زیرحامل می‌نامیم. نوساناتی که به شدت پیرامون یک کانال وای‌فای قرار دارند. همان‌گونه که ممکن است حدس زده باشید، CFR حتا این قابلیت را دارد تا حرکت دست و

انگشتان را که به واسطه تایپ کلیدها طول موجی را به وجود می‌آورد، شناسایی کند.

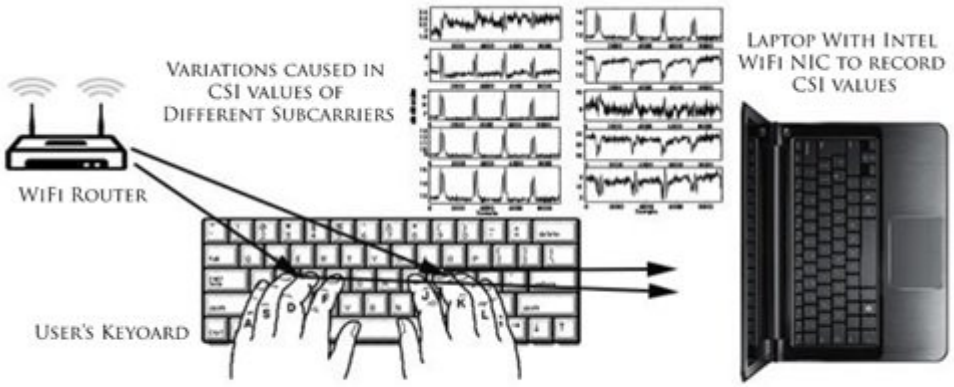

Figure 1: WiKey System

در این آزمایش، پژوهش‌گران یک روتر وای‌فای TP-Link TL-WR1043ND و یک لپ‌تاپ لنوو مدل X200 را مورد استفاده قرار دادند. زمانی که کاربر در حال تایپ یک موضوع بود، پژوهش‌گران از آنتن‌های روتر برای جمع‌آوری تمامی مقادیر مربوط به اطلاعات حالت کانال استفاده کردند. بعد از جمع‌آوری داده‌ها با استفاده از چند فیلتر مختلف پارازیت‌هایی که از منابع مختلف دریافت شده بود را حذف کردند و کلیدها را به صورت ایزوله شده، استخراج کردند. با استفاده از یک الگوریتم ویژه محققان توانستند هر ضربه‌ای که به کلیدها وارد می‌شوند را دریافت کنند. اطلاعات به دست آمده، نشان داد که آن‌ها موفق شده‌اند، یک ابزار واقعی که قادر است کلیدهای تایپ شده را استخراج کند، طراحی کنند.

مطلب پیشنهادی

صفحه‌کلیدهای آسیب‌پذیر
آیا صفحه‌کلیدهای بی‌سیم عامل افشای اطلاعات هستند؟

به طور کلی میزان موفقیت WiKey در شناسایی درست کلیدها زمانی که کلیدها به صورت تکی فشرده می‌شوند، 96.4 درصد بود است. البته این نرخ موفقیت، زمانی که کلیدها به طور مداوم و برای تایپ یک جمله مورد استفاده قرار می‌گیرند، به نرخ 93.5 درصد می‌رسد.

Table 1: Average values of features extracted from keystrokes of keys a-z collected from user 10

Features	a	b	c	d	e	f	g	h	i	j	k	l
Mean amplitude	-0	-0.04	0.0124	-0.03	0.045	-0.043	-0.076	-0.06	0.014	-0.03	0.03	-0.01
Second central moment	0.08	0.133	0.0801	0.083	0.156	0.1818	0.6523	0.263	0.12	0.231	0.33	0.11
Third central moment	0.02	-0.03	0.0036	-0.01	0.029	-0.06	-0.919	-0.05	-0.01	-0.1	0.05	0.02
RMS deviation	0.27	0.359	0.2782	0.285	0.385	0.4244	0.7899	0.506	0.332	0.472	0.57	0.32
Energy	71.5	116.6	69.788	73.34	137.5	159.43	570.8	232.1	104.8	201.4	288	95.2
Entropy	9.76	9.762	9.7616	9.762	9.762	9.7616	9.7616	9.762	9.762	9.762	9.76	9.76
Zero Crossings	11.8	6.913	12.363	6.225	6.4	4.375	4.075	3.4	12.08	9.088	6.05	13.7

m	n	o	p	q	r	s	t	u	v	w	x	y	z
-0	0.032	0.02	0.03	-0.012	0.008	0.054	7E-04	-0.013	-0.02	-0	-0.1	-0.02	0.06
0.1	0.108	0.09	0.19	0.1022	0.051	0.245	0.192	0.062	0.12	0.097	0.26	0.09	0.21
-0	0.01	0.01	0.04	-0.006	0.003	0.098	-0.101	-0.01	0.029	0.023	-0	-0.02	0.04
0.3	0.323	0.29	0.43	0.3137	0.222	0.472	0.434	0.242	0.335	0.306	0.5	0.3	0.45
83.7	94.98	75.6	167	88.928	44.22	215.5	167.1	54.56	104.4	84.48	227	81.5	182
9.76	9.762	9.76	9.76	9.7616	9.762	9.762	9.762	9.762	9.762	9.762	9.76	9.76	9.76
10	9.063	13.8	12.9	11.85	15.41	6.35	12.85	16.75	11.88	14.3	6.48	10.1	7.55

مجرمان سایبری و پژوهش‌گران امنیتی در سال‌های اخیر به امنیت صفحه‌کلیدها توجه ویژه‌ای از خود نشان داده‌اند. با تلاش‌های مداوم و گاهی اوقات تعامل با یکدیگر، آن‌ها نشان داده‌اند که بدافزارها نه فقط این توانایی را دارند تا کلیدهای تایپ شده را با استفاده از سیگنال‌های FM از یک کامپیوتر ایزوله شده برداشت کنند، بلکه ثابت کرده‌اند که می‌توان هویت یک کاربر را شناسایی کرده و بر اساس آن چیزی که تایپ می‌کند به ردیابی او پرداخت.

لازم به گفتن نیست که این سامانه با محدودیت‌هایی همراه است. برای این آزمایش، پژوهش‌گران مجبور شدند تعدادی از متغیرها را به طور ویژه تنظیم کنند. آماده‌سازی محیطی با حداقل پارازیت‌ها، دستگاهی که در فاصله دو متری میان روتر و صفحه‌کلید قرار دارد، ارائه آموزش لازم به افراد به طوری که در طول روز سر یا دیگر اعضا بدن خود را حرکت ندهند، از جمله این فاکتورها به شمار می‌روند. پژوهش‌گران امیدوار هستند در آینده مشکل عدم کارایی سیگنال‌ها که به واسطه پارازیت‌های محیطی ضعیف هستند را با اتکا بر فناوری‌های استخراج ژست‌های حرکتی بهبود بخشند.

تاریخ انتشار:
14 شهریور 1395

نشانی منبع: https://www.shabakeh-mag.com/security/4441