

Have a secure RIOT

Eric Sesterhenn <eric.sesterhenn@x41-dsec.de>

2017

X41 D-SEC GmbH

- Eric Sesterhenn
- Principal Security Consultant
- Pentesting/Code Auditing at X41 D-Sec
- Father of a daughter



- A lot of people know RIOT better than I do
- Intended to be positive criticism
- This is a spare time project for me
- Spent 2hr/week from June to mid August

“RIOT implements all relevant open standards supporting an Internet of Things that is connected, **secure**, durable, and privacy-friendly.”

Motivation

- Good friend asked me ;-)
- Drunk in Warsaw... one thing leads to another

Security

The image shows a screenshot of a tweet by Amity Dan (@popshark1) from July 1st. The tweet text reads: "TP-Link forgot to buy the domain tplinklogin.net. Exploit can be made, the domain is for sell for 2.5m\$". Below the tweet is a photograph of a TP-Link router. To the right of the router is a Das Keyboard SQ, with a text box describing it as a cloud-connected, open API RGB mechanical keyboard. Below the router is another text box explaining a security vulnerability: "This is a huge problem. If anybody knows the MAC address of one of your sockets, they can control it from anywhere in the world. You can't set a password to stop them, and a normal home router configuration won't block this. You need to explicitly firewall off the server (it's 115.28.45.50) in order to protect yourself. Again, this is completely unrealistic to expect for a home user, and if you do this then you'll also entirely lose the ability to control the device from outside your home." At the bottom of the slide, there are three small text boxes: "RIOT Summit 2016", "Kai Beckmann and Michael Frey", and "We Predict A RIOT".

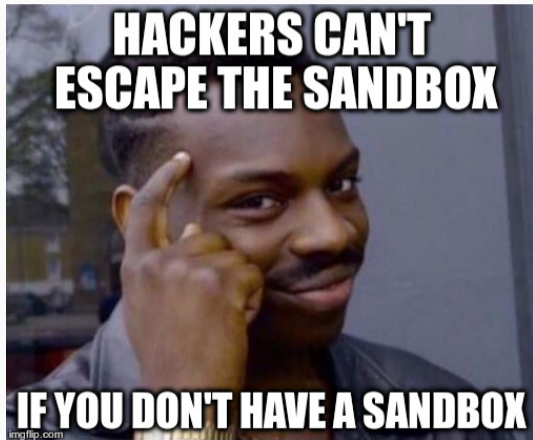
Amity Dan (@popshark1) · Jul 1
TP-Link forgot to buy the domain tplinklogin.net
Exploit can be made, the domain is for sell for 2.5m\$

Das Keyboard SQ is a cloud-connected, open API RGB mechanical keyboard that allows each key to be color-controlled over the Internet. It is built with ground-breaking electronics that provide superior RGB LED brightness and unsurpassed response time. Along with the Das Keyboard Q application, the Das Keyboard SQ makes you more productive by streaming information directly to your keyboard.

This is a huge problem. If anybody knows the MAC address of one of your sockets, they can control it from anywhere in the world. You can't set a password to stop them, and a normal home router configuration won't block this. You need to explicitly firewall off the server (it's 115.28.45.50) in order to protect yourself. Again, this is completely unrealistic to expect for a home user, and if you do this then you'll also entirely lose the ability to control the device from outside your home.

RIOT Summit 2016 Kai Beckmann and Michael Frey We Predict A RIOT

- Sandboxing - nah
- ACL - nah
- Fancy User Separation - nah
- DEP, ASLR... - nah



- Secure Language - nah
- C has tons of issues



What is already happening?

- Hard to find out, no Wiki page...
- Coding guide
- Static Analysis (cppcheck, clang)



- Fuzzing just for SPIFFS
- In the dumbest version, throw random garbage at parsers
- Tools: American Fuzzy Lop, Libfuzzer, Radamsa, Honggfuzz...

I THROW POOP ON YOU!!!



memecenter.com 



Name	Issues reported
RIOT OS Core	3
Wakaama	3
Tiny-ASN1	5
SPIFFS	4
TinyDTLS	7
CCN-Lite	>15
OONF	3

- Classic Integer Overflow
- Fixed in glibc and others in 2002
- Used by MSP430

```
1 void __attribute__((weak)) *calloc(size_t
   ↳ size, size_t cnt)
2 {
3     void *mem = malloc(size * cnt);
4     if (mem) {
5         memset(mem, 0, size * cnt);
6     }
7     return mem;
8 }
```



- Type Confusion
- `lwm2m_data_free()` depends on the type
- Data reinterpreted as pointer and array size

```
1 targetP->type = LWM2M_TYPE_MULTIPLE_RESOURCE;
2 targetP = prv_extendData(targetP);
3 if (targetP == NULL) goto error;
4 ...
5 error:
6 lwm2m_data_free(size, *dataP);
```

- Should have been picked up by static analysis
- Bugs in error handling are common
- Crashes are different for IoT

```
1 if(encryption_algorithm_identifier == NULL
   ↳ ||
   ↳ encryption_algorithm_identifier->type
   ↳ != ASN1_TYPE_OBJECT_IDENTIFIER) {
2   fprintf(stderr, "ERROR: ...%d\n",
   ↳ encryption_algorithm_identifier->type
   ↳ );
3   return 1;
4 }
```



```
1 dtls_ticks(&now);
2 /* if (defined(WITH_CONTIKI) || defined(RIOT_VERSION)) */
3 /* FIXME: need something better to init PRNG here */
4 dtls_prng_init(now);
5 /* else /* WITH_CONTIKI */ */
```

- Randomness infrastructure missing (just PRNGs exist)
- Guess this is known...

- Use with care...
- Rewrite is happening

```
1 int i, maxi, vallen;
2 int typ;
3 ...
4 if (typ < NDN_TLV_MAX_TYPE &&
    ↪ ndntlv_recurse[typ]) {
5     *len -= vallen;
```

```
1 struct key_s *k = (struct key_s *)
    ↪ calloc(1, sizeof(struct key_s*));
```

```
1 cp = ccnl_malloc(strlen(pending)+1);
2 strcpy(cp, pending);
```

- Properly checked, that no OOB Read occurs?
- Whats missing?

```
1  if (*ptr + tail_len > eob){
2      /* not enough buffer for head */
3      return RFC5444_END_OF_BUFFER;
4  }
5
6  /* copy address tail into buffer */
7  memcpy(addr_entry->addr +
      ↪ tlv_context->addr_len - tail_len, *ptr,
      ↪ tail_len);
```

- Port parts to secure language (lua?)
- Proper Audits
- Proper Fuzzing Infrastructure
- Use -m32 to find integer overflows easier
- Use asan, usan, msan and friends



- GPG key for the security contact would be nice
- List with security issues/advisories (I didnt see a changelog entry, CVE-ID, ... about the issues reported)
- List the stuff that is happening
- Talk with upstream - just two of five upstream kept the CC

“Actually, I wasn’t even aware

██████████ was a part of riot os until now”

- Q & A
- eric.sesterhenn@x41-dsec.de
- Sorry no Twitter... stalk me on linkedin if you must

