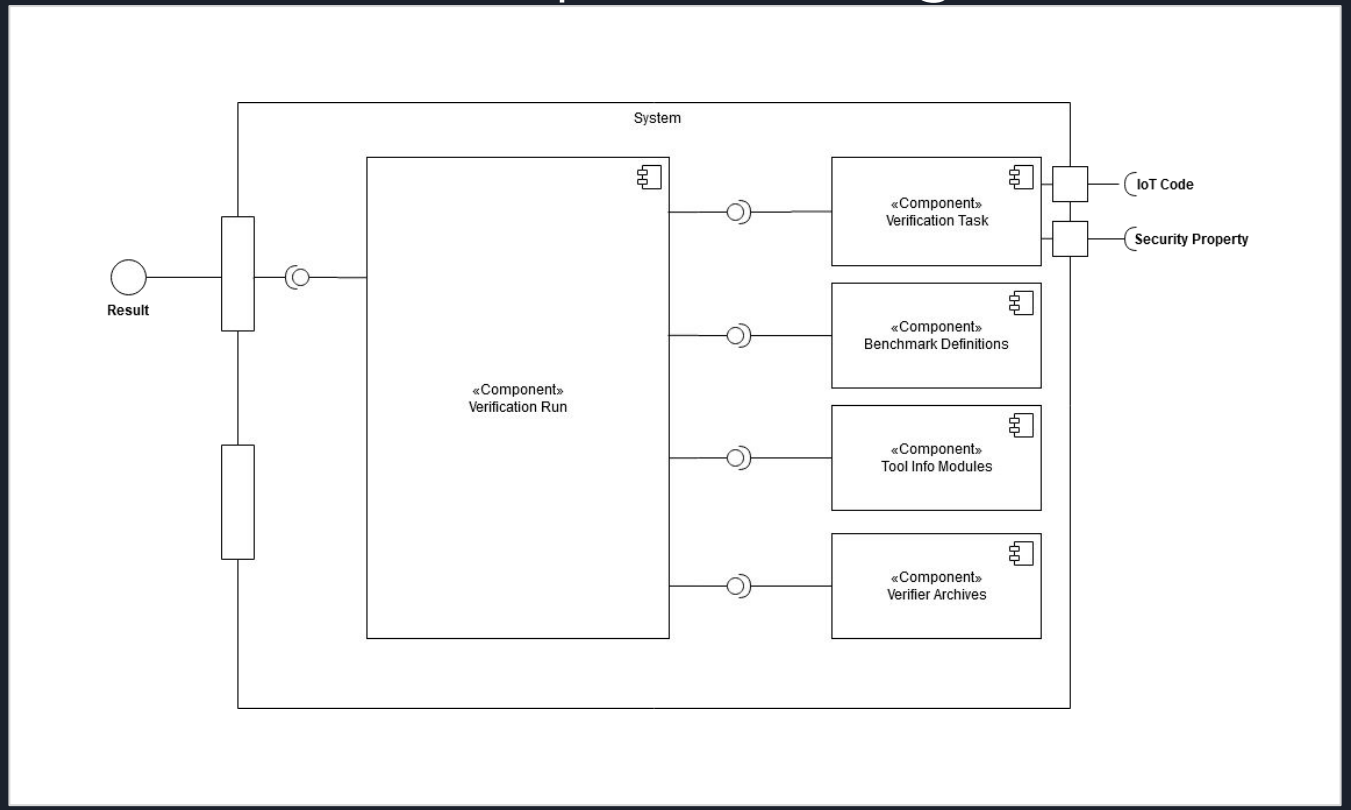
Sdmay21-41

Vincent Johnson - Team Lead: vincentj@iastate.edu
Joshua French
Jordan McKillip
Marcus Reecy

IoT Security Verification

The Internet of Things (IoT) is becoming more and more a part of people's everyday lives. Devices such as locks, cameras, and smart-speakers are just a very small view of all the ways our lives are going online. With all of these devices having important roles, being located in private places, and gathering loads of information, the security of them is much more prevalent as it would be problematic if it got into the wrong hands.

Benchmark Component Diagram



Technical Challenges

- Some tools are more successful at testing certain properties than others
- Some benchmarks may error out with some tools

CPA-SEQ			PredatorHP			VeriAbs		
No Overflows	Mem Safety	Reach Safety	No Overflows	Mem Safety	Reach Safety	No Overflows	Mem Safety	Reach Safety
T	T	T	T	T	?	T	T	T
T	U	T	U	U	?	T	T	T
T	U	?	U	U	?	T	T	T
T	U	T	?	?	?	U	U	T
T	T	T	?	U	?	?	T	T
T	T	?	?	?	?	U	T	T
T	U	T	?	U	?	T	U	T
T	T	T	?	U	?	?	T	T
T	U	?	?	?	?	U	U	T
T	U	T	?	?	?	T	T	T
T	U	T	?	U	?	T	T	T
						?	?	?
T	T	T	T	T	T	T	T	T
T	T	T	T	T	T	T	T	T
T	T	T	U	U	U	T	T	T
U	IF	U	T	T	T	T	T	T
T	T	T	T	T	T	T	T	T
U	T	T	U	U	U	T	T	T

Technical Challenges

- Analyzing libraries / creating benchmarks from them
- Adding new properties

```
fnet_ip6_multicast_list_entry_t *_fnet_ip6_multicast_find_entry(fnet_netif_t *netif, const fnet_ip6_addr_t *group_addr )
{
    fnet_index_t                    i;
    fnet_ip6_multicast_list_entry_t *result = FNET_NULL;

    /* Find existing entry or free one.*/
    for(i = 0u; i < FNET_CFG_MULTICAST_MAX; i++)
    {
        if((fnet_ip6_multicast_list[i].user_counter > 0u)
           && (fnet_ip6_multicast_list[i].netif == netif)
           && FNET_IP6_ADDR_EQUAL(&fnet_ip6_multicast_list[i].group_addr, group_addr))
        {
            result = &fnet_ip6_multicast_list[i];
            break; /* Found.*/
        }
    }

    return result;
}
```

Example benchmark

IEEE Standards

- IEEE 802.11ai-2016
  - The standard is about initial setup methods and their security.
- IEEE 1012-2016
  - This standard is about the verification and validation of systems, software, and hardware life cycles.

Engineering Constraints

- Utilization of the tools requires a lot of time
  - Average time for a single run could go from 15 minutes to several hours
  - Size of files paramount
- Certain benchmarks are written in different, but comparable languages
  - Shifting between C and C++
- To run benchexec and tools:
  - At minimum, memory limit of 15 GB (14.6 GiB) of RAM, a runtime limit of 15 min of CPU time, and a limit to 8 processing units of a CPU conforming to standard SV-COMP guidelines.
  - Must be able to download and install the different tools

Engineering Requirements

- Must be wireless compatible.
  - IoT compatible
- Must compile and be stable on their own
  - Archived properly within the zip
- Finalized within git with several files
  - Read me, declarations, etc.
- Requires:
  - Python 3.5 for testing and running (3.6 to be used when released)
  - Linux with a x86 or Arm machine for the architecture.