The Datagram newsletter

April, 2017 Volume 2, No. 4

From the Chair...

I was reading a paper (A Messy State of the Union: Taming the Composite State Machines of TLS) on software validation of the TLS. The paper explained the result of, and the procedures and software used, to validate the correctness of various TLS implementations.

TLS is the means to establish a secure communication channel to transport data over an insecure internet. The paper points out that many implementations have faulty state machines, allowing illegal transitions to occur with hackable consequences. The paper also points out that the validation effort has complexities in determining the root cause of some failures.

This led me to wonder about TLS. One aspect is the incorporation of a new web page (INFO Sec->Transport Layer Security) on our web site. But there are questions on the statement that the implementation-state machines are complex and that there is some difficulty in establishing the path of failure' for the validations software.

Finite State Machines (FSM) are rather simple devices (the best

Continued on page 2

Next meeting:

April 26, 2017

6:30 PM Dinner and Networking
7:00 - 8:00 PM Presentation
8:00 - 8:30 PM Q & A
8:30 - 9:00 PM Meet & Mingle

Dinner: FREE

ATEP, 15445 Lansdowne Road, Tustin, CA, Room #D106 (Room number subject to change)

Speaker: Irvin Lemus

This Month's Topic: CyberPatriot: Engaging Middle School, High School, and Community College Students

This presentation will overview Southern California Cybersecurity Community College Consortium (SoCal CCCC)'s involvement with the local K-12 districts and the community colleges that participate in CyberPatriot. It will be informative for anyone interested in cyber defense competition volunteering, sponsorship, and gameplay. The presentation will cover the event lifecycle for colleges hosting in our region, training and team development for K-12, the CyberPatriot competition timeline and training timeline, along with some examples from the competition and hands-on preview.■

About the Speaker

Irvin Lemus has been in the Information Technology industry for 10 years, focusing on Cybersecurity, Virtualization, Systems and Network Management for small and medium sized businesses ranging from clinics, law firms, investment advisors, manufacturing to energy efficient experts, non-profit organizations and after school K-12 programs.

Irvin has been involved with CyberPatriot for three years as a coach, mentor and as the Regional Coordinator for the Southern California Cybersecurity Community College Consortium.

He leads the participating community colleges in the consortium by training, mentoring and supporting the K-12 schools from various districts across Southern California.■

From the Chair, Cont'd.

"dumb" software I know). There are two basic implementations, a Mealy Machine and Moore Machine.

The Mealy Machine implements actions on events (FSM arcs). The Moore Machine implements actions on states. Pragmatically, the Moore Machine lacks flexibility and needs to carry global information to recover path information, whereas the Mealy Machine is better behaved. The "state" of the FSM for a Mealy machine is a single variable continuing the current state, but the Moore Machine may also need to track the FSM arcs (paths).

My implementations of an FSM consist of an n x m matrix, where the rows represent events and columns states. The complexity is one of size, not of algorithmic complexity. During design, each matrix cell requires some consideration, so e.g., a 20 x 30 matrix requires 600 individual decisions. This is onerous, but not complex. I had a professor who used to say that "counting from 1 to 10 is easy. Counting from one to a million is no more difficult, it just takes more time. And that is the case here.

So, I am puzzled. A properly constructed FSM is not complex. If it is necessary to reduce the size of the machine, then an FSM can be constructed for each disjoint part of the FSM, with a consequent reduction in overall size and a minimal increase in algorithmic complexity.

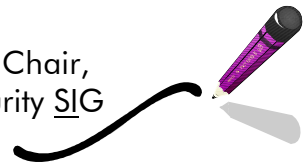
In the TLS case, each event can carry data. The data needs validation and can lead to a semantic generated event transiting the FSM to a new state. Not very complex.

So I remain puzzled by the statements about incorrect implementations because of "complexity." It seems more that the implementations are faulty because of poor software practices. I also remain a bit puzzled by the authors' issues with determining the cause of a failure in some cases.

Unfortunately, I will attempt to learn enough to implement TLS and validation software. When done, the software will be available and additional insights presented. If you would like to contribute to this effort, then please contact the chair.

Art

(reluctant) Chair,
CyberSecurity SIG



March Meeting Report:

DELDroid: An Automated System for Determination and Enforcement of Least Privilege Architecture

by Carol J. Amato

Mahmoud Hammad gave us a very interesting and informative talk on the research project on which he is currently working: DELDroid. He explained Android has 85% of the marketshare because of the number of applications available. The Android Operating System allows the API to have over-privileged access at runtime. In other words, privileges are inherited and all used interfaces are granted the same ones as the parent app (see Figure 1 on the next page). "Not all components need these permissions," he stated.

These unnecessary permissions cause security consequences:

- It is hard to comprehend the security posture of an Android system
- They increases the attack surface
- They cause many security vulnerabilities
    - Privilege escalation attack
    - Hidden Inter-Component Communication (ICC) attack

To combat these problems, Hammad's group at UCI has developed DELDroid (see Figure 2), an automated approach for determining and enforcing the Limited Privilege (LP) architecture for an Android System.

The LP architecture narrows the attack surface and thwarts certain security attacks. It also has a multiple domain matrix (MDM). MDM models a complex system with multiple domains. Each domain is modeled as a Design Structure Matrix (DSM). DSM and MDM are very effective in capturing

Continued on page 3

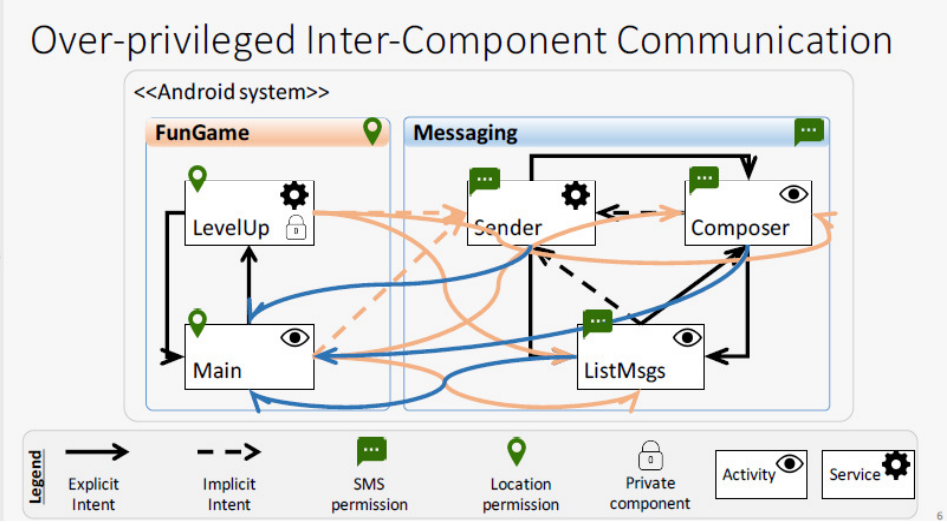


Figure 1. Over-privileged Inter-Component Communications

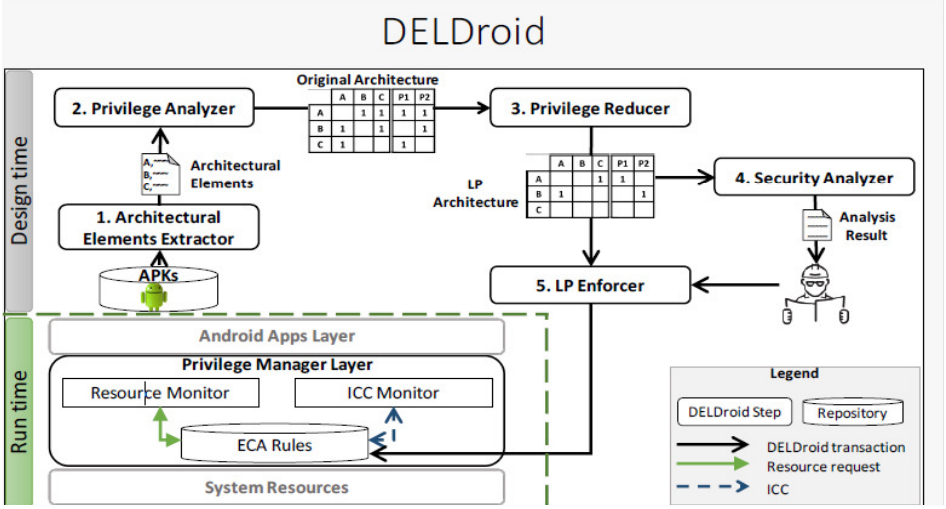


Figure 2. Deldroid

DELDroid, Cont'd.

and analyzing the architecture of a complex system. The permissions can be set for each component.

DELDroid modifies the Android architecture by adding a Privilege Manager layer. DELDroid can be configured to remove a malicious communication and to prevent hacker attacks.

Hammad's group is researching three questions:

1. How effective is DELDroid in reducing the attack surface?

2. How effective is DELDroid in detecting and preventing attacks in real-world apps?

3. What is the performance of DELDroid?

Experimental results show that there is between 97% and 99% attack surface reduction; that there is a 97% precision and 100% recall in detecting and preventing security attacks; and that there is negligible runtime performance overhead.

At present, however, DELDroid is a research tool that is not commercially available. The government has more interest than commercial companies.

DELDroid, Cont'd.

They hope to use it for soldiers who are in the field so they can't be tracked. ■

Why Cybercriminals Love Health Records

Many people don't understand why cybercriminals would want their medical data. According to Peter Vogel, Eric Levy, and Eddie Block (http://www.technewsworld.com/story/84417.html), the reason is that health records never expire, whereas credit cards do and can be maxed out or canceled, rendering them useless.

Health records not only contain social security numbers, but they "can be used to acquire prescription drugs, falsify insurance claims, file fraudulent tax returns, open credit accounts, obtain official government documents such as passports and drivers' licenses, and even create new identities" (Trend Micro, 2017). Over 113 million records were stolen in 2015.

This poses a problem for health practitioners, who are expected to protect health information. According to Vogel, Levy, and Block, keeping it safe has to be a top priority for every entity responsible for it. Small businesses that can't afford the technology on their own can hire what HIPAA calls a "business associate" to safeguard the information for them. ■

Place Your Ads in The Datagram

Do you have information about an academic program, seminar, work-shop, symposium, presentation, or job listing related to cybersecurity? Consider placing an ad in The Datagram.

Ads are currently FREE and will be published for three months, after which they are renewable. They will appear simultaneously on the CyberSecuritySIG's website at sites.ieee.org/ocs-cssig for maximum exposure.

Submit a camera-ready, business-card-sized (3.5" x 2") JPG file to Carol Amato at stargazer@stargazerpub.com. ■

Contact Information

Website: sites.ieee.org/ocs-cssig

Meetup.com/CyberSecuritySIG

Newsletter Editor: stargazer@stargazerpub.com

Request for Articles

This newsletter is open for article or information submission by all mem-bers of the CyberSecurity SIG. If you have something to say or leads on information that would be of benefit to the SIG, the members would love to read it.

Articles must be a maximum of 500 words. For articles over 500 words, please provide a double-spaced abstract for publication in *The Datagram*, and the full article, single-spaced, as a .doc, .docx, or .rtf file to Carol J. Amato, Newsletter Editor, at stargazer@stargazerpub.com. ■

Speakers Requested

If you know of an expert in cyber-security who is willing to speak to our CyberSecurity SIG, please contact our program chair, Irvin Lemus, at ilemus3@coastline.edu. ■

2017 CyberSecurity SIG Executive Committee

Chair	Arthur Schwarz
Co-Chair	Gora Datta
Treasurer	Brandon Young
Programming	Irvin Lemus
Newsletter	Carol J. Amato
Web Design	Ginson Samuel
Audio-Visual	Open

Please Provide Feedback on Our Website

We want your feedback on our new website. If you like what you see or have any changes to suggest, tell us and others. If you have any changes in mind, please let us know. We are open to any suggestions and would appre-ciate your comments. ■