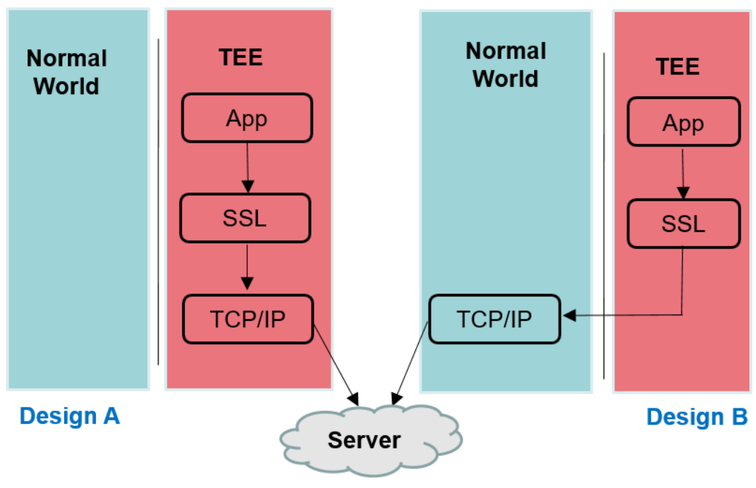
Expanding TrustZone in Android OS & Developing SEED Labs

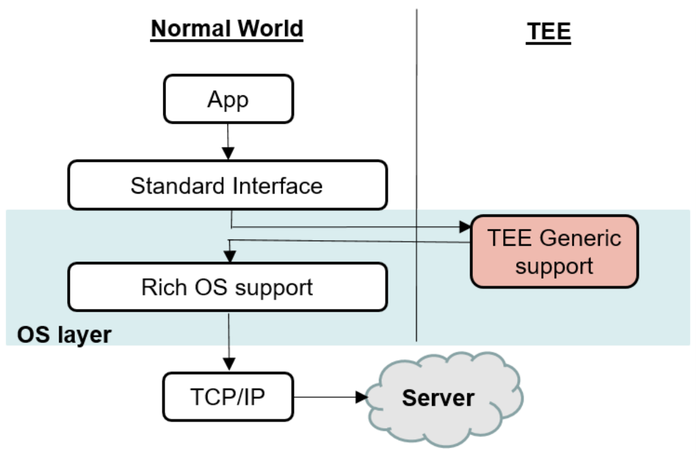
Wenliang (Kevin) Du, Syracuse University

Abstract: Over the last 7 years, the number of identified vulnerabilities in mobile operating systems has skyrocketed, posing a great threat to device users. Once a mobile device is compromised (e.g. rooted), all the sensitive data and operations on it will be compromised. To counter such a threat, mobile devices today provide a hardware-protected area called Trusted Execution Environment (TEE) to help protect users from a compromised OS. Unfortunately today's TEE is primarily leveraged by vendor applications, because non-vendor app code is considered untrusted inside TEE. We propose a novel design to integrate TEE with mobile OS to allow non-vendor apps to leverage TEE in a transparent way. We achieve this by incorporating TrustZone support at the operating system level, so apps can leverage TrustZone support without adding app-specific code into TEE. We implement our design TruZ-Droid by integrating TrustZone TEE with the Android OS. TruZ-Droid allows non-vendor apps to leverage TEE to protect: (i) user secret input & user acknowledgement, and (ii) sending of user secret to the authorized server. We build a prototype phone using the TrustZone-enabled HiKey board to evaluate our design. We demonstrate TruZ-Droid's effectiveness by adding new security features to existing applications to solve real-world problems.

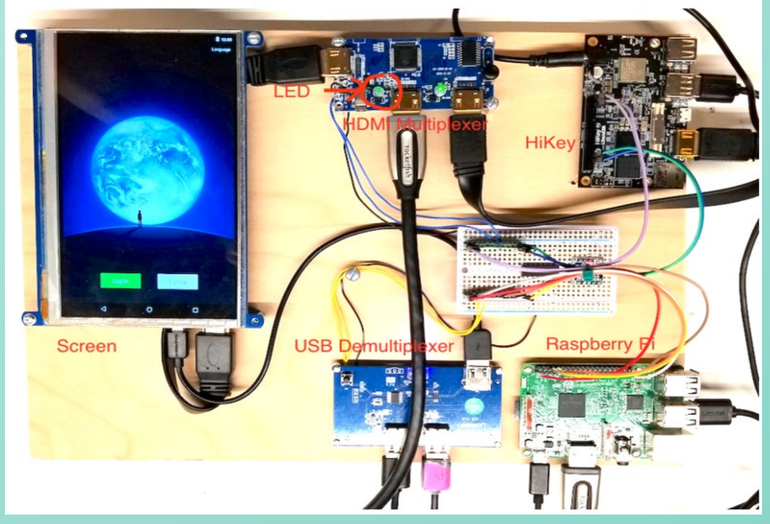
Existing Solutions



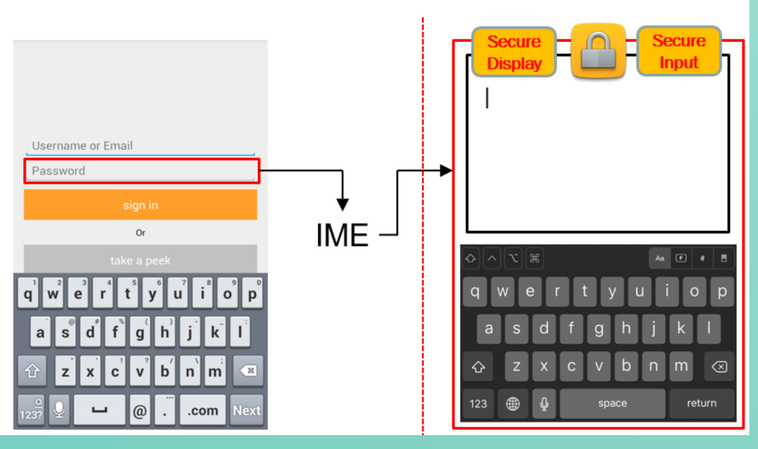
Our Design



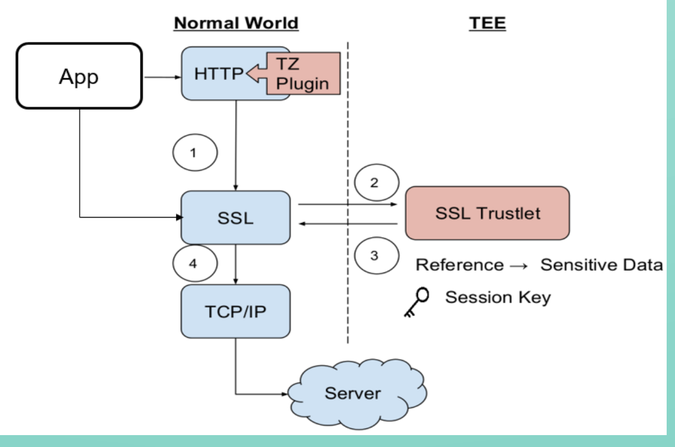
Hardware Implementation



Protecting User Interaction – Example



Split HTTPS/SSL Design Overview



Evaluation

Table 1: Evaluation Results for Open-Source Apps

Test Case	Client	Server	Time Spent
Drupal Attested Post	4 LOC	20 LOC	1 hour
Elgg Attested Payment	4 LOC	12 LOC	30 mins
Elgg Authenticator	3 LOC	4 LOC	30 mins
Drupal Login	3 LOC	4 LOC	30 mins
GNUSocial Login	3 LOC	4 LOC	40 mins
Kandroid Login	3 LOC	4 LOC	30 mins
Redmine Login	3 LOC	4 LOC	30 mins
Owncloud Login	3 LOC	4 LOC	40 mins
Seafile Upload	3 LOC	4 LOC	50 mins

Table 2: Evaluation Result for Closed-Source Apps

Test Case	Login	Payment	Upload	Attestation
Success/Total	13/15	5/5	2/2	9/9

Performance Evaluation

- Input: 123 ms
- UI confirmation: 53 ms
- Split SSL: 304 ms
- Overall: the delay is barely noticeable

Usability Evaluation

- Amazon Mechanical Turk (161 responses)
- Identify secure world

SEED: Hands-on Labs for SEcurity EDucation

OBJECTIVES

- Developing hands-on lab exercises.
  - Interesting, effective, and timely
  - Open-source and free
  - Easy (for instructors) to adopt
  - No need for dedicated hardware

Classical Attacks

Buffer-Overflow Attack
CTF: Buffer-Overflow Attack
Return-to-libc Attack
Format-String Attack
CTF: Format-String Attack
Race Condition Attack
Packet sniffing and spoofing
Mitnick Attack (TCP attack)
ARP Cache Poisoning Attack
Kaminsky Attack (DNS attack)
SQL Injection Attack
Cross-Site Request Forgery
Samy Worm (Cross-Site Scripting)
MD5 Collision Attack
Hash Length Extension Attack

More Recent Attacks

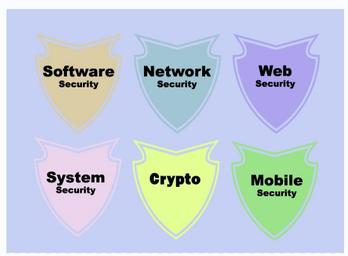
Meltdown Attack Lab
Spectre Attack Lab
Dirty COW Attack Lab
Shellshock Attack Lab
Heartbleed Attack Lab
Android Repackaging Attack Lab
Android Rooting Attack Lab
BGP Attack Lab
Blockchain Attack Lab

Exploration and Design Labs

Set-UID Program Lab
Firewall Exploration Lab
Firewall Evasion Lab
Secret-Key Encryption Lab
Public-Key Encryption Lab
PKI Lab
VPN Lab
Linux Capability Lab
Linux Container Lab
Bitcoin and Blockchain Lab

Easy Lab Setup

Students just need to download our pre-built virtual machine image to their personal computers or run it from a cloud. There is no need for a physical lab space or dedicated computers. All the software we use for the lab environment setup is open-source and free.



Over 30 Labs

We have developed over 30 labs that cover a wide range of topics in computer and information security, including software security, network security, web security, operating system security and mobile app security. More labs are currently being developed.

Free Workshops

2015: 60 faculties
2016: 70 faculties
2017: 70 faculties
2018: 80 faculties
2019: 100 faculties

Textbook (New)

I have written a textbook based on the SEED labs and my teaching experience. The book takes a hands-on approach, i.e., for each security principle, specially designed activities are used to help explain the principle. The book can be ordered from Amazon.

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 | Alexandria, Virginia

Award ID#: 1718086 and 1303306