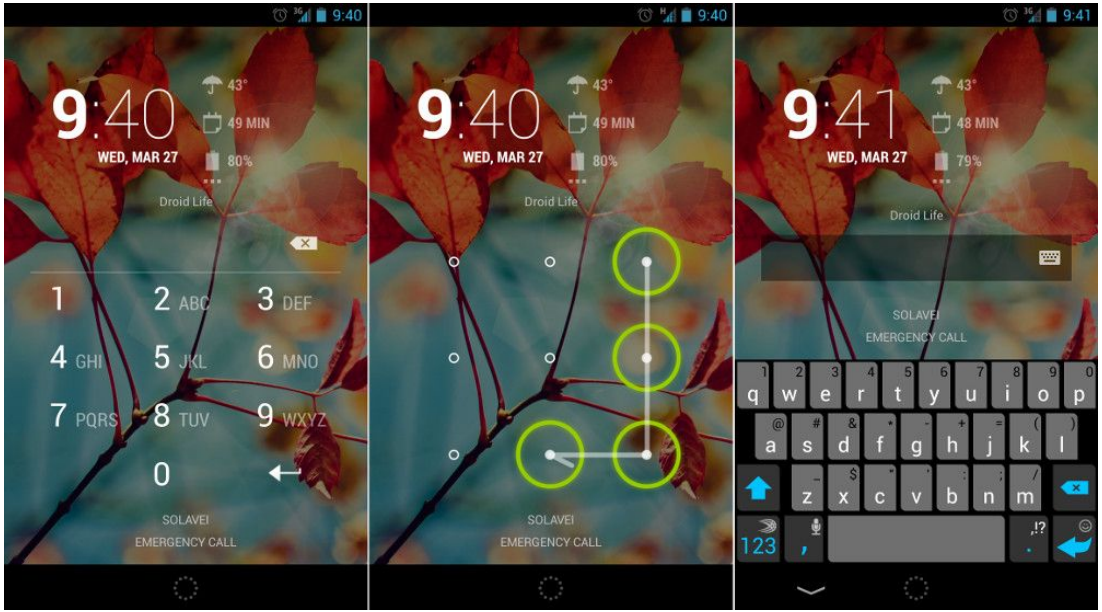
Smartphone and Cloud Security

Creating a secure cloud-based continuous implicit authentication application for mobile devices

Mike Freyberger & Paul Jackson

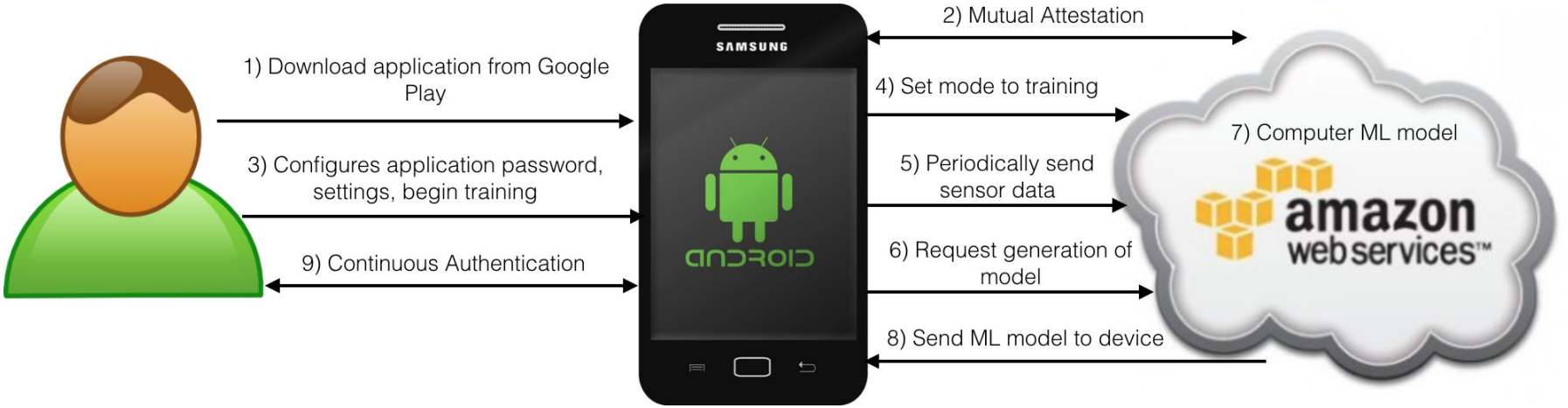
Introduction and Motivation

- PIN code, swiping pattern, and passwords are typically used for explicit authentication
- Many phones use biometrics like fingerprint recognition and facial recognition



http://www.droid-life.com/2013/03/27/an-overview-of-android-lock-screen-security-options-beginners-guide/

Continuous Authentication System



Client Side Threat Model

- Attacks on confidentiality and integrity of sensitive data
- Physical Attacks
  - Attacker picks up unlocked phone
  - Attacker bypasses default locking mechanism
  - Ability to probe memory
- Software Attacks
  - Malicious software snooping and deleting data
- TCB
  - TrustZone, CryptoCell
  - Secure monitor, trusted os, secure firmware
- Side channel attacks not considered

Server Side Threat Model

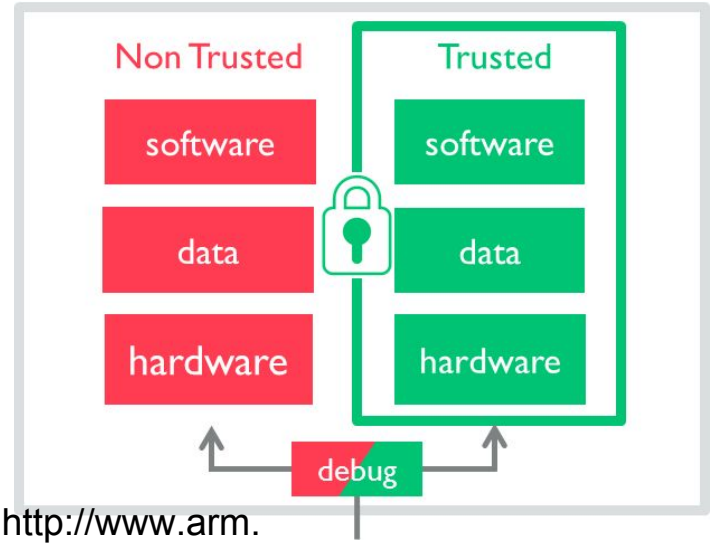
- VM level attacks
  - Malicious Guest OS
  - Malicious applications running inside of VM
  - Same application leaking secrets
- Server level attacks
  - Malicious VM’s on the same server
  - Malicious hypervisor
  - Hardware probing attacks
- Cloud Attacks
  - Attacks from machines within the cloud subnet
  - Attacks from machines outside of the subnet
- TCB: SGX Hardware and Software resources, CPU & Caches

Communications Threat Model

- Considering active and passive attackers
  - Snooping Attack
  - Spoofing Attack
  - Splicing Attack
  - Replay Attack
- Not considering DoS attacks

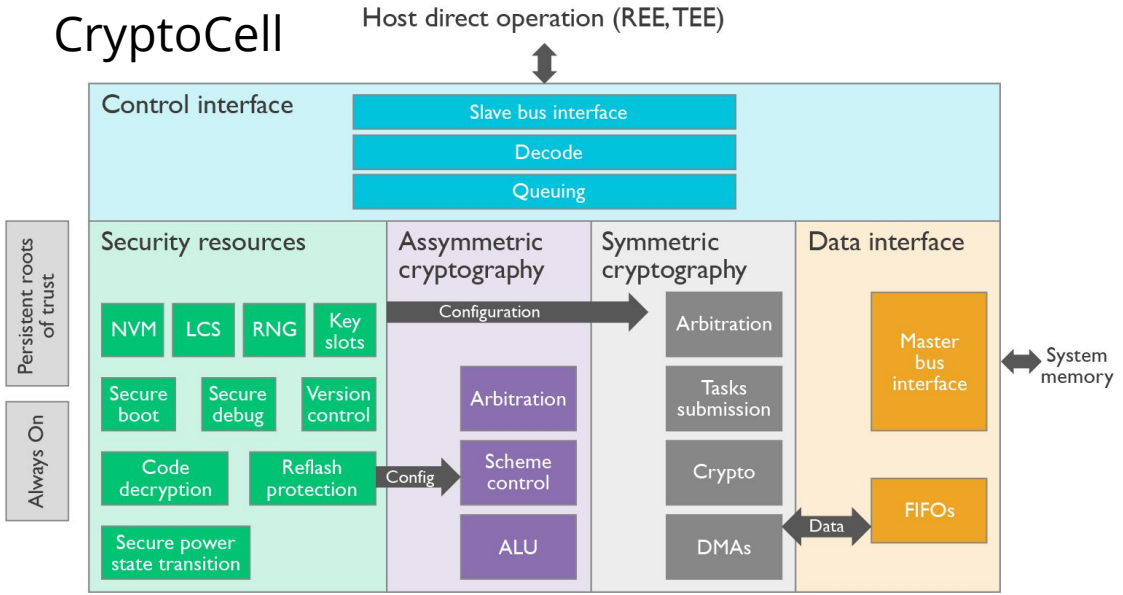
TrustZone and Cryptocell

TrustZone



http://www.arm.com/products/processors/technologies/trustzone/

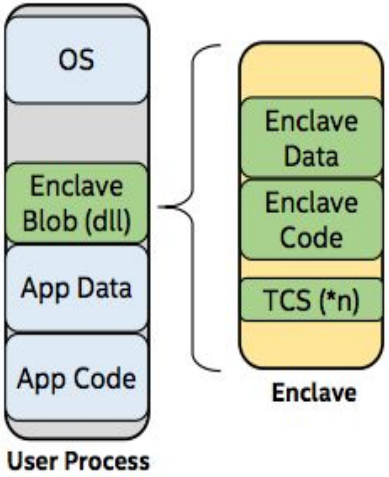
CryptoCell



http://www.arm.com/assets/images/TrustZone_CryptoCell.jpg

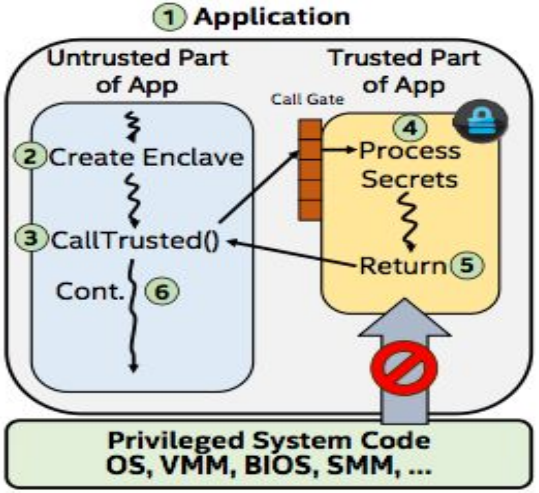
SGX

Process View



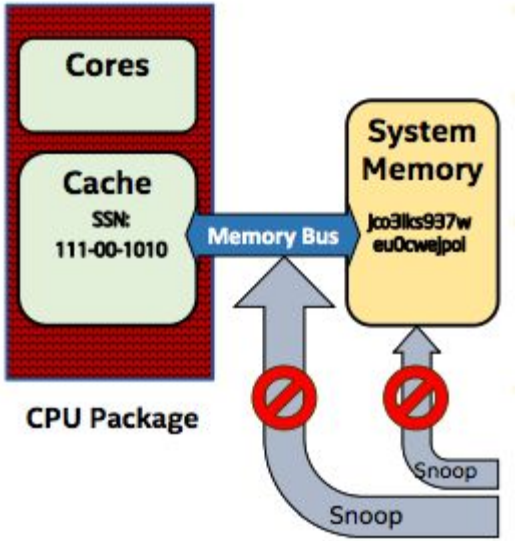
https://software.intel.com/sites/default/files/managed/3e/b9/SF15_ISGC003_81_SGX_DL_100_small.pdf

Execution View



https://software.intel.com/sites/default/files/managed/3e/b9/SF15_ISGC003_81_SGX_DL_100_small.pdf

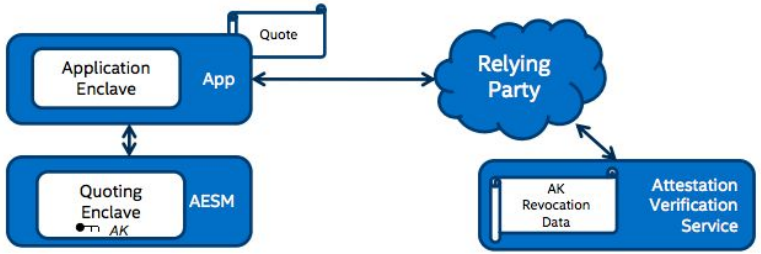
TCB



https://software.intel.com/sites/default/files/managed/3e/b9/SF15_ISGC003_81_SGX_DL_100_small.pdf

Mutual Attestation

- Client must trust the server execution environment and the server code
  - SGX provides remote attestation report
- Server must trust the client is running in secure environment with correct client side code
  - TrustZone with Cryptocell provide secure boot and TrustZone verification
  - Code verification is difficult on Android



Intel® Software Guard Extensions (Intel® SGX). Intel Corporation. June 2015. https://software.intel.com/sites/default/files/332680-002.pdf

Application Configuration

- Create application-specific password
  - Necessary to have trusted peripherals through TrustZone
  - Ensure password strength (complexity & dictionary checking)
- Configure application settings
  - Adjust default training period
  - What to do upon uninstallation
    - Reset password and unlock phone
    - Wipe phone data

Communications Protocol

Client → Server: GET /nonce; Header: DEVID.

Server → Client: *n*

Client → Server: POST /sensor. Header: DEVID. Body:

$E_{\text{Session Key}}$(Sensor Data), E_{SKC}[h(Sensor Data || n || DEVID)], E_{PKS}{Session Key}

Secure Storage

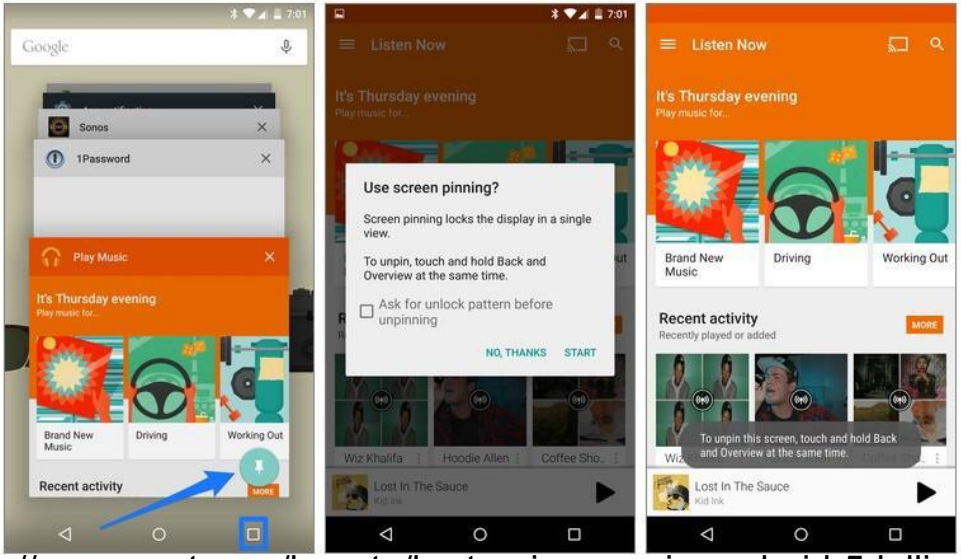
- Each SGX device has a root key fused as manufacturing time
- Each enclave can request a key that will be deriving based on enclave attributes and the root key
- Each user will have their own keys derived from the root key
- User Encryption Key = $HMAC_{Root\ Key}(Device\ ID)$
- User Authentication Key = $HMAC_{Root\ Key}(HMAC_{Root\ Key}(Device\ ID))$

Machine Learning

- Uses LibSVM Library
- Constructs one-class support vector machine
  - Only needs 1 user’s data to work
  - Creates boundary separating inliers of training set from outliers
  - Determines if test values are outliers for training set
  - Can account for outliers in training set
- Trained model returned to smartphone
  - Allows for continuous authentication without a data connection

Performing Continuous Implicit Authentication

- Measure sensor data at regular intervals
- Lock out user if multiple anomalies detected in a row
- Cannot simply lock phone
  - Use application pinning
- Account password reauthenticates user



http://www.cnet.com/how-to/ho-to-pin-apps-in-android-5-lollipop/

Retraining, Suspending Service, & Uninstallation

- Can retrain or temporarily suspend continuous implicit authentication upon request
  - Requires user's application password to prevent attackers from doing so
- Application cannot be uninstalled by default
  - Must first remove administrative privileges
- Administrative password required upon revocation of administrative privileges
  - Failing to do so triggers backup security mechanisms

Prototype

- Collaborated with David Gilhooley and Tony Jin
- Created cloud server using Amazon Web Services
  - Implemented REST API
  - Collected sensor data of multiple users
  - Stored encrypted data in MongoDB database
- Machine Learning
  - GCU Dataset

Conclusion

- The attack surface for cloud based smartphone applications is very large
- TrustZone with CryptoCell provides the necessary sub systems to support secure memory and secure storage
- SGX provides secure memory and secure execution
- SGX provides trusted key management necessary for secure storage
- There are many steps in designing a full secure system, all of which must be handled carefully in order to maximize usability without sacrificing security

Works Cited

[1] Wei-Han Lee and Ruby B. Lee, “Multi-sensor Authentication to Improve Smartphone Security”, in Proceedings of the International Conference on Information Systems Security and Privacy, 2015.
[2] L. Li, X. Zhao, and G. Xue. Unobservable reauthentication for smartphones. In Network and Distributed System Security Symposium. 2013.
[3] H. G. Kayacık, M. Just, L. Baillie, D. Aspinall, and N. Micallef. Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors. Mobile Security Technologies. 2014.
[4] Dan Branley. Informate Mobile Intelligence First to Measure Smartphone Usage Internationally, Report currently Tracks 12 Countries and Will Expand to 25 by the End of 2015. Informate Mobile Intelligence. February 2015. http://www.informatemi.com/newsletter10022015.html
[5] Intel® Software Guard Extensions (Intel® SGX). Intel Corporation. June 2015. https://software.intel.com/sites/default/files/332680-002.pdf
[6] Matthew Hoekstra. Intel SGX for Dummies (Intel SGX Design Objectives). Intel Developer Zone. November 2015. https://software.intel.com/en-us/blogs/2013/09/26/protecting-application-secrets-withintel-sgx
[7] B. Schölkopf, J. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson. Estimating the support of a high-dimensional distribution. Neural Computation. 2001.
[8] Android 5.0 APIs. Google. http://developer.android.com/about/versions/android-5.0.html#ScreenPinning
[9] Intel® Software Guard Extensions Programming Reference. Intel Corporation. October 2014. https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf
[10] H. Krawczyk and P. Eronen. HMAC-based Extract-and-Expand Key Derivation Function (HKDF). http://tools.ietf.org/html/rfc5869
[11] TrustZone. ARM. 2015. http://www.arm.com/products/processors/technologies/trustzone/
[12] Fundamentals of ARMv8. ARM Cortex-A Series Programmer’s Guide for ARMv8-A. 2015. http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.den0024a/CIHGCIDG.html
[13] Steven J. Vaughan-Nichols. Amazon EC2 cloud is made up of almost half-a-million Linux servers. DNet. March 2012. http://www.zdnet.com/article/amazon-ec2-cloud-is-made-up-of-almost-half-amillion-linux-servers/
[14] Amazon Web Services: Overview of Security Processes. August 2015. https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf
[15] Pramod Jamkhedkar, Jakub Szefer, Diego Perez-Botero, Tianwei Zhang, Gina Triolo and Ruby B. Lee. A Framework for Realizing Security on Demand in Cloud Computing. IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Bristol, UK. 2013.
[16] Signing Your Applications. http://developer.android.com/tools/publishing/app-signing.html
[17] David Champagne and Ruby B. Lee. Scalable Architectural Support for Trusted Software. The 16th IEEE International Symposium on High-Performance Computer Architecture (HPCA). January 2010.
[18] J. Christopher Bare. Attestation and Trusted Computing. CSEP590: Practical Aspects of Modern Cryptography. March 2006.
[19] Node.js Foundation. Node.js. https://nodejs.org/en/
[20] Express – Node.js web application framework. http://expressjs.com/

Thank You

Questions?

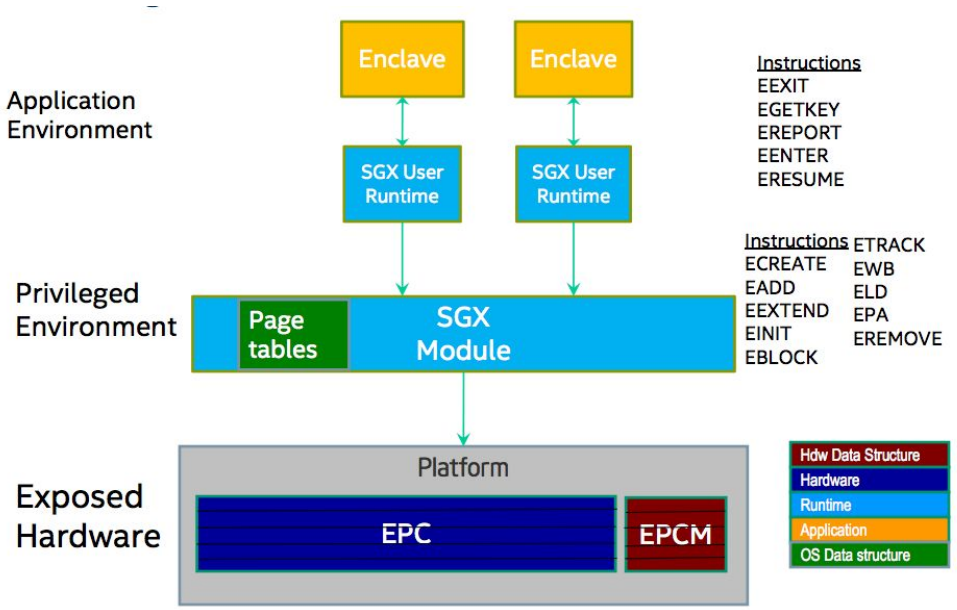
Motivation

- Smartphone authentication is explicit and one time
- This does not protect against an attacker stealing an unlocked device or an attacker who knows the user's PIN

http://www.data-directions.com/View.aspx?page=asktheppropellerheads/articles/consumergroup/lostphone

Server Side TCB

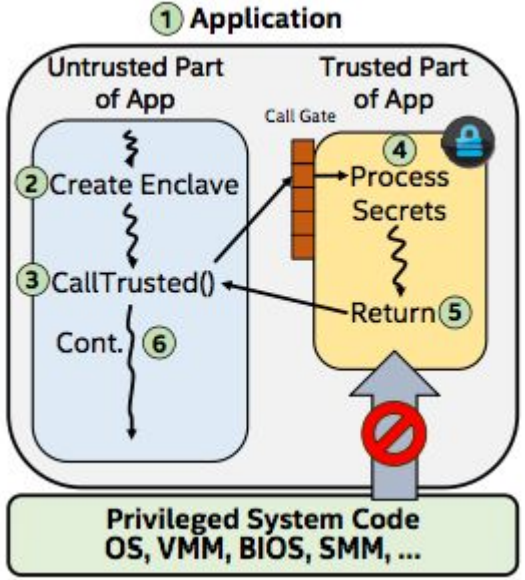
- SGX software and hardware resources
- CPU and caches



Intel® Software Guard Extensions (Intel® SGX). Intel Corporation. June 2015. https://software.intel.com/sites/default/files/332680-002.pdf

SGX Execution

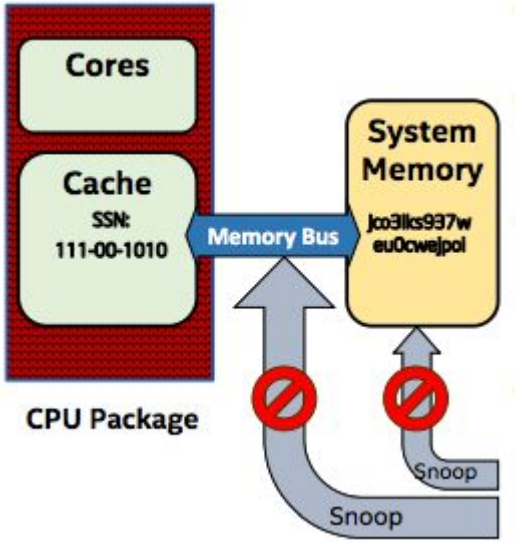
- Application begins with all code and data
- Code and data are transferred to the enclave during enclave creation
- Enter into enclave through defined entry point
- Memory access is denied to enclave data is denied from outside of the enclave



https://software.intel.com/sites/default/files/managed/3e/b9/SF15_ISGC003_81_SGX_DL_100_small.pdf

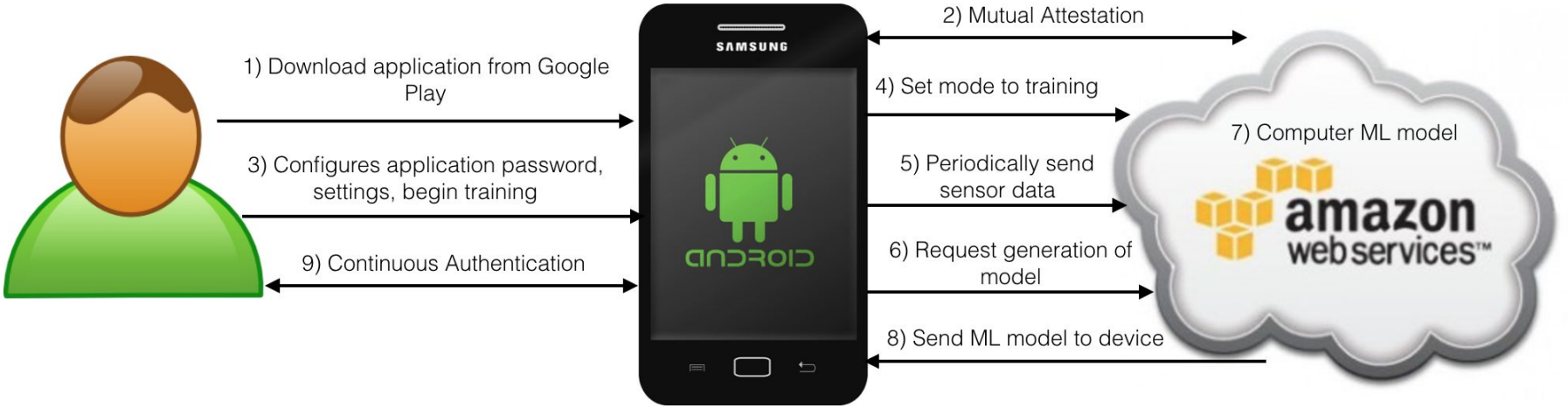
SGX TCB

- During enclave execution the data is only in plaintext while inside of CPU package
- Prevents snooping on memory bus or system memory



https://software.intel.com/sites/default/files/managed/3e/b9/SF15_ISGC003_81_SGX_DL_100_small.pdf

Full System


1) Download application from Google Play
3) Configures application password, settings, begin training
9) Continuous Authentication
SAMSUNG
ANDROID
2) Mutual Attestation
4) Set mode to training
5) Periodically send sensor data
6) Request generation of model
8) Send ML model to device
7) Computer ML model
amazon web services™

SGX Report Structure

Table 2-21. Layout of REPORT

Field	OFFSET (Bytes)	Size (Bytes)	Description
CPUSVN	0	16	The security version number of the processor.
MISCSELECT	16	4	SSA Frame specified extended feature set bit vector
RESERVED	20	28	Must be zero
ATTRIBUTES	48	16	The values of the attributes flags for the enclave. See Section 2.7.1 (ATTRIBUTES Bits) for the definitions of these flags.
MRENCLAVE	64	32	The value of SECS.MRENCLAVE
RESERVED	96	32	Reserved
MRSIGNER	128	32	The value of SECS.MRSIGNER
RESERVED	160	96	Zero
ISVPRODID	256	02	Enclave PRODUCT ID
ISVSVN	258	02	The security version number of the Enclave
RESERVED	260	60	Zero
REPORTDATA	320	64	A set of data used for communication between the enclave and the target enclave.This value is provided by the EREPORT call in RCX.
KEYID	384	32	Value for key wear-out protection
MAC	416	16	The CMAC on the report using report key

Intel® Software Guard Extensions Programming Reference. Intel Corporation. October 2014.https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf

Download Application

- Application signing
- Android uses developer signatures, not CA signatures
- Must keep signing key secure