ROOT OF TRUST - SOMETHING WHICH WE BLINDLY TRUST
↳ UNVERIFYABLY TRUSTWORTHY

TRUST IS TRANSITIVE
↳ IF YOU TRUST SOMETHING, YOU TRUST WHAT IT TRUSTS

TRUSTED COMPUTING BASE
↳ OF A COMPUTER SYSTEM IS THE SET OF ALL HW, FIRMWARE, & SOFTWARE THAT COULD CREATE VULNERABILITIES
↳ KEEP SMALL & SIMPLE

SECURITY OBJECTIVES
↳ CONFIDENTIALITY - PREVENT/DETECT/DETER — DISCLOSURE
↳ ~~AVAILABILITY~~ INTEGRITY - " " " MODIFICATION
↳ AVAILABILITY - " " " ACCESS
↳ AUTHENTICITY - ENSURES THAT IT COMES FROM RIGHT SOURCE
↳ NON-REPUDIATION - CANNOT LIE ABOUT HAVING GIVEN INFO

BOOTING:
↳ HW DOESN'T KNOW WHERE OS IS
↳ USE BOOTSTRAP LOADER
↳ FINDS KERNEL, LOADS TO MAIN MEM, BEGINS EXECUTING

PC BOOT PROC. (BIOS)
↳ USER SWITCH ON
↳ PSU DOES SELF CHECK
↳ CPU EXECUTES 0XFFFF0
↳ BIOS ROM
↳ ONLY 20 BITS
↳ BACKWARDS COMPATIBILITY BACK TO 8086
↳ ROUTINE IN BIOS TESTS HW & INIT
↳ SEARCH FOR ROMS & RUNS
↳ IF COLD BOOT IT RUNS POST
↳ BIOS LOOKS FOR BOOT DEVICES
↳ UPON FINDING BOOT DEVICE IT LOADS THE BOOT SECTOR & LOADS IT
↳ OFTEN CALLED MBR (MASTER BOOT RECORD)
↳ LOADS TO 0X7C00
↳ MBR CHECKS PARTITION TABLE FOR AN ACTIVE PARTITION
↳ LOADS THAT PARTITION'S BOOT SECTOR

SECURE BOOT

- AEGIS [AFS97]
  - USES A CHAIN OF INTEGRITY CHECKS TO ENSURE BOOT IS SAFE
  - ASSUMED MOBO, PROC, BIOS VERIFICATION CODE, BOOTSTRAP EXPANSION CARD ARE TRUSTED

PROJECT

- FIND TEAM
- ROWHAMMER ATTACK TOOLS & LAB?

TPM - TRUSTED PLATFORM MODULE

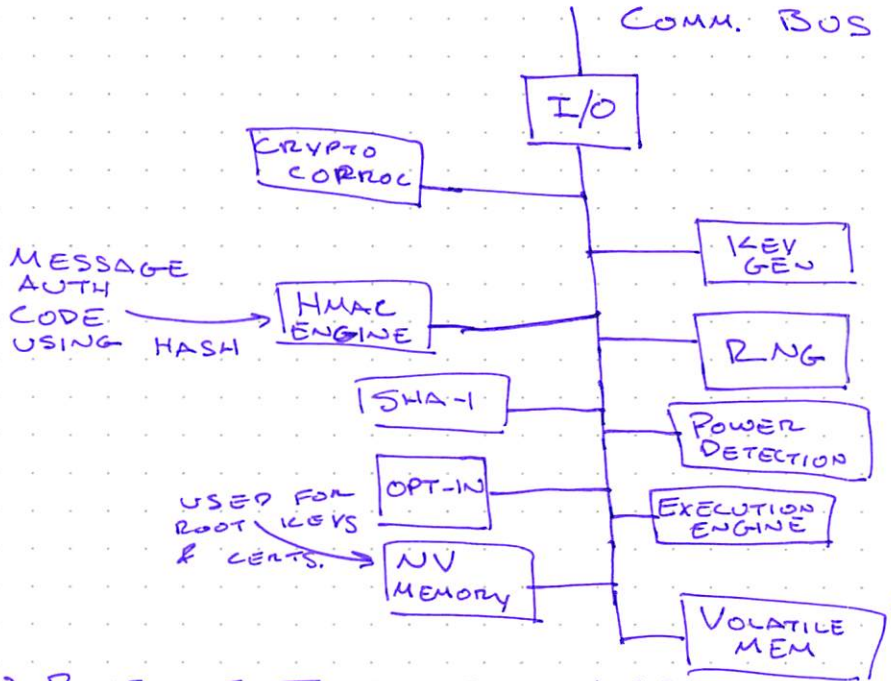
- A CRYPTO COPROC., NOT A CRYPTO ACCELERATOR
  - NOT A GPP
- A HARDWARE ANCHOR FOR SYSTEM (APP LEVEL) SECURITY
- MOST THINGS USE TPM FOR SECURE BOOT.
  - NOT APPLE ...

HISTORY OF TPM

- TPM 1.1b - 2003
  - RSA KEYGEN & STORAGE
  - SECURE AUTH
  - DEVICE HEALTH ATTESTATION
  - OFFERED PCRs TO ~~ACCOM~~ MAINTAIN BOOT SEQ. SECURITY
  - HARDCODED SHA-1
  - ~~DIRECT ANON~~
- TPM 1.2 - 2005 - 2009
  - STD SOFTWARE INTERFACE
  - STD HARDWARE PACKAGE PINOUT
  - PROTECT AGAINST DICT. ATTACKS
  - SMALL (2KB) NON-VOLATILE STORAGE TO STORE CERT. FOR ENDORSEMENT KEY
  - HARDCODED SHA-1
  - DIRECT ANONOMOUS ATTESTATION (DAA)
  - IN MOST PCs BY 2005
- TPM 2.0 - 2005
  - DIGEST AGILITY
    - CAN USE ANY HASH ALG.
- ISSUES TPM 1.2 TRIED TO ADDRESS
  - ID DEVICE
  - SECURE KEYGEN
  - SECURE KEY STORAGE
  - NVRAM STORAGE
  - DEVICE HEALTH ATTESTATION
- ISSUES TPM 2.0 TRIED TO ADDRESS
  - ALG. AGILITY
  - ENHANCED AUTH.
  - QUICK KEY LOADING

APPLICATION INTERFACES USED TO TALK TO TPMs
- PROPRIETARY APPS WRITTEN DIRECTLY TO TPM
- LEGACY APPS THAT USE MIDDLEWARE
  - PUBLIC KEY CRYPTO STANDARD (PKCS) #11
  - MICROSOFT CRYPTO API (CAPI)
- APPS WHICH USE TCG SOFTWARE STACK (TSS)
- JAVA LIBRARIES

TPM 1.2
- PROVIDES ROOT OF TRUST FOR
  - STORAGE
  - REPORTING
    - "IS SYSTEM IN A GOOD STATE?"
    - ROT OF MEASURING CHECKED, ROT OF ~~THE~~ REPORTING TELLS YOU
      - TPM IS ROT FOR REPORTING BUT NOT ~~RECORDING~~ MEASURING
  - ROT OF STORING



SPECIAL TO TPM
- PLATFORM CONF. REG.
  - USED FOR SYSTEM MEASUREMENTS
  - ALWAYS RESET @ BOOT
  - HAS SPECIFIC OPERATIONS

- ROOT OF TRUST FOR MEASUREMENT
  - TPM CAN'T MEET "WHAT IS THE STATE OF THE SYSTEM?"
  - OTHER THINGS MUST BE USED AS ROT

- TWO ROOT KEYS
  - ENDORSE
  - STORAGE

GET TPM READY TO USE & LEARN THE KEY HIERARCHY
- TURN ON (BIOS)
  - ACTIVATED
  - ENABLED
  - OWNED

} DIFF COMBINATIONS

SOME BIOSES ALSO PROVIDE A CLEAR OPTION
↳ ERASES STORAGE ROOT KEY & OWNER

ENDORSEMENT KEY
↳ ROOT KEY FOR REPORTING
↳ SHOULD BE CREATED IN MANUFACTURING
↳ SHOULD SHIP W/ CREDENTIALS WHICH CERT EK
↳ MANY MANUFACTURERS DO NOT DO THIS ^
↳ IF THEY DO INCLUDE EK, THEY PROBABLY DON'T INCLUDE THE CERT

CREATE EK:
↳ TPM_CREATEENDORSEMENTKEYPAIR
↳ SOME PLATFORMS OFFER MORE USER-FRIENDLY TOOLS
↳ CREATES PERMANENT EK
↳ TPM_CREATE REVOKABLE...
↳ MAKES A REVOKABLE EK

↳ TPM_READ PUBEK
↳ READS PUBLIC PART OF EK
↳ NO WAY TO GET PRIVATE PART

TPM MUST SHIP W/ NO OWNER INSTALLED
↳ OWNER ≠ ROOT

TPM_TAKEOWNERSHIP
↳ CREATES SRK

TPM OWNERSHIP
↳ 1.2 CAN ONLY HAVE 1 OWNER
↳ BEFORE IT HAS AN OWNER, ANYONE CAN BECOME THE OWNER
↳ OWNER HAS EXCLUSIVE RIGTH TO MAKE IDENTITIES

DICT. ATTACKS:
↳ TPM LOGS ALL AUTHORIZATION ATTEMPTS

↳ WHEN TAKING OWNERSHIP, 2 PASSWDS ARE REQUIRED
↳ OWNER
↳ SRK

TYPES OF TPM KEYS
↳ IDENTITY KEY
↳ SIGN DATA FROM TPM
↳ SIGNING KEY - SIGN
↳ STORAGE KEY - ENCRYPT
↳ BINDING KEY - DECRYPT
↳ LEGACY KEYS (DON'T USE)
↳ SIGN OR ENCRYPT

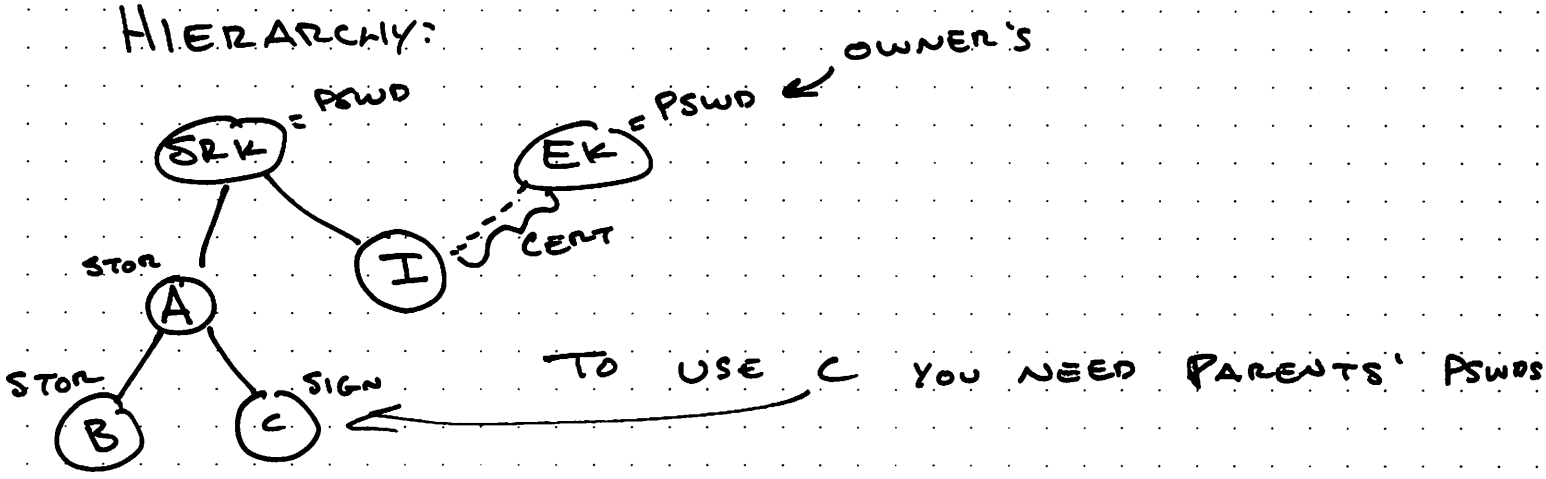
CREATING WRAP KEYS

- TPM_CREATEWRAPKEY
  - ANY TYPE OTHER THAN IDENTITY
  - MUST PROVIDE PARENT KEY, ALREADY LOADED INTO TPM
  - OUTPUTS KEY BLOB
    - USER NEEDS TO STORE

LOADING KEYS

- TPM_LOADKEY2
  - 2 ARGS
    - ENCRYPTED KEY BLOB
    - PARENT

HIERARCHY:



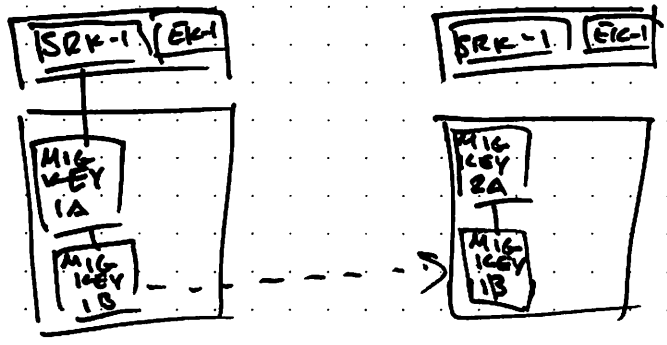
TYPES OF TPM KEYS:

- WRAP KEYS
  - STORAGE: ENCRYPT DATA & OTHER KEYS
  - BINDING: DECRYPT DATA
  - SIGNING: SIGN DATA
  - LEGACY: ENCRYPT OR ~~DECRYPT~~ SIGN
- IDENTITY KEY
  - ATTESTATION IDENTITY KEY (AIK)
  - SIGN DATA FROM TPM
  - TPM QUOTES & CERTS
  - CAN HAVE MANY IDENTITIES
- ALSO CLASSIFIED BY MIGRATABILITY
  - (NMK) NON-MIGRATABLE KEY
  - (MK) MIGRATABLE KEY
  - (CMK) CERTIFIABLE MIGRATABLE KEY
    - MIGRATABLE, BUT HIGHLY CONTROLLED
    - TPM CAN ATTEST/CERTIFY ITS PROPERTIES

CREATING IDENTITY KEYS
- ↳ TPM OWNER MUST AUTHORIZE COMMAND
- ↳ AUTH VALUES TO USE
  - ↳ PCR AND/OR LOCAL CONSTRAINTS
  - ↳

KEY MIGRATION
- ↳ CRITICAL FEATURE
  - ↳ BACKUP & SYSTEM REPLACEMENT

- ↳ CREATE MIGRATABLE KEY K ON TPM A
- ↳ CREATE MIGRATION BLOB, RE-ENCRYPTING K TO KEY ON TPM B
- ↳ REQUIRES OWNER AUTH
- ↳ K IS STILL USABLE ON A
  - ↳ MORE LIKE A CLONE / BACKUP



TO MIGRATE:
- ↳ LOAD 1A, LOAD 1B
- ↳ ENCRYPT 1B W/ 2A PUB KEY → BLOB
- ↳ LOAD 2A, USE PRIV. KEY TO DECRYPT BLOB

ATTESTATION
- ↳ PRESENTATION OF VERIFIABLE EVIENCE ABT A MACHINE TO A REMOTE PARTY
  - ↳ IN TPM CONTEXT, THAT USUALLY MEANS PCRs
- ↳ VERIFIER CAN INSPECT PCRs, VERIFY CHAIN OF TRUST, ETC.
- ↳ PRIMARY TOOL IS QUOTE
  - ↳ SIGNED REPORT OF CURRENT PCR VALUES, ANY CRYPTOGRAPHICALLY VERIFIABLE ~~EVIDENCE~~ EVIDENCE OF PCR STATE COUNTS
- ↳ PCR CONTENTS ARE ALL HASH CHAINS

DATA PROTECTION & STORAGE

- TPM_SEAL
  - ENCRYPT DATA FOR LATER DECRYPTION W/ TPM_UNSEAL

MIGRATE EXAMPLE:

- TPM1 OWNER PWD: 0001, SRK PWD: 5581
- TPM2 OWNER PWD: 0002, SRK PWD: 5582

KEY 1A IS LOADED TO TPM1 & ITS HANDLE IS BBBBBBBB

[ON TPM1] migrate -hp BBBBBBBB -pwd 0001 -im 2A.key -pwdm bmig
-ik 1B.key -ok migrationblob.bin

[TPM2] loadkey

↓ REST OF EXAMPLE IN SLIDES

CERTIFIED MIGRATION KEYS (CMKs)

(SLIDES)

SEALING EXAMPLE IN SLIDES

BINDING:

- ANYONE ON ANY PLATFORM CAN BIND (ENCRYPT)
- ONLY TPM CAN DECRYPT USING TPM_UNBIND
  - THERE IS NO TPM_BIND COMMAND
- BINDING EXAMPLE ON SLIDES

~~NEXT~~

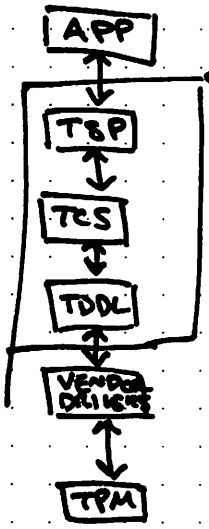
NVRAM:

- WEEK 4_1 NOTES

MACHINE AUTHENTICATION:

- REMOTELY VERIFIABLE PROOF OF MACHINE IDENTITY
  - SUBSET OF ATTESTATION
- MOST TPM KEYS CAN BE USED
- SIGNING BASED MACHINE AUTH
  - "MACHINE X SIGNED Y"
  - SIGNING OR IDENTITY KEY
  - CHOICE OF KEY PROPS CAN MAKE OR BREAK SECURITY
- SIGN-BASED AUTH EXAMPLE
  - (SLIDES)

PROGRAMMING TPM



TSS
↳ TCG SOFTWARE STACK

TSP - TCG SERVICE PROVIDER
TCS - TCG CORE SERVICES
TDDL - TCG DEVICE DELIVERY LIBRARY

TPM HARDWARE INTERFACE
↳ ATTACHED TO LOW PIN COUNT (LPC) BUS
↳ ACCESSED THROUGH BIOS INTERRUPT CALL

TSS
↳ AUTH SESSIONS
↳ KEYMGMT ABSTRACTIONS
↳ DEFINES USEFUL OBJECTS FOR INTERACTION

CODE EXAMPLE IN SLIDES 4_2

VIRTUALIZATION

↳ SYSTEM VIRTUALIZATION
↳ VIRTUAL MACHINE MODULE (VMM) OR HYPERVISOR
↳ 3 PROPERTIES OF INTEREST
↳ EQUIVALENCE
↳ PROGRAMS SHOULD RUN THE SAME
↳ RESOURCE CONTROL
↳ VMM MUST HAVE TOTAL CONTROL OF VIRTUAL RESOURCES
↳ EFFICIENCY / PERFORMANCE
↳ MOST INSTRUCTIONS MUST BE RUN W/OUT VMM INTERVENTION
↳ SUFFICIENT BUT NON-REQUIRED CONDITIONS (ISA INTO 2 GROUPS)
↳ PRIVILEGED INSTRUCTIONS
↳ TRAP IF PROC. IN USER MODE, NO TRAP IN SUPERVISOR MODE
↳ CTRL SENSITIVE INSTRUCTIONS
↳ THOSE THAT ATTEMPT TO CHANGE SYSTEM CONF
↳ BEHAVIOR SENSITIVE
↳ BEHAVIOR OR RESULT DEPENDS ON CONFIG OF RESOURCES

THEOREM 1: AN EFFECTIVE VMM CAN BE MADE WHEN THE SET OF SENSITIVE INSTRUCTIONS IS A SUBSET OF THE PRIVILEGED INSTRUCTIONS
↳ CAN MAKE TRAP-AND-EMULATE STYLE VMM

TYPE 2: BINARY REWRITE
- RUNS FROM W/IN OS
- READ IN CODE & LOOK FOR BASIC BLOCKS
- IF A BLOCK WOULD NOT GENERATE A TRAP, IT REPLACES THE BLOCK

TYPES OF MACHINE VIRTUALIZATION:
- BARE METAL
  - RUNS IN USER MODE
  - VM RUNS GUEST OS
  - IF OS CALLS SENSITIVE INSTRS, VMM TRAPS & EXECUTES

VIRTUALIZING TPM
- SO EACH APP CAN USE ITS OWN TPM
  - NOT AS SECURE

ARM

- AS OF 2005 98% OF PHONES USE ARM
- IT'S VERY POPULAR
- BASED ON RISC
  - NOW COMPETING W/ RISC V
- ARM FAMILIES
  - A
    - APPLICATION PROCESSOR
    - SUPPORTS OS & HIGH PERF. APPS
      - SMARTPHONES, TVS, ETC
  - R
    - REAL-TIME PROCESSORS
    - HIGH PERF & HIGH RELIABILITY
  - M
    - MICROCONTROLLERS
    - COST SENSITIVE
      - NO MMU (NO VIRTUAL MEM)

CORTEX A
- 30+ GEN. PURPOSE REG.
- 1 PC
- 1 CPSR (CURRENT PROG. STATUS REG)
- 1 SPSR (SAVED " " ")
- HAS A HYPERVISOR MODE
  - VIRTUALIZE TRUSTZONE

CORTEX A BOOT ← FINISH FROM NOTES
- HAS CODE BURNED TO CHIP (NO BIOS)
- MEM-MAPPED I/O
- DIFF. MEM. COMPONENTS (SRAM, DRAM, ROM)
  - CONTAINS SETUP CODE

CORTEX M BOOT:
↳ MAIN STACK POINTER @ 0x00000000
↳ PC (POINTS TO RESET HANDLER) @ 0x00000004

ARM INSTRUCTIONS
↳ REVIEW ARM...

LAB ~~#~~ 1 PT 2: DUE OCT. 31ST
↳ WILL GET ANOTHER LAB NEXT WEEK

MIDTERM AFTER COLUMBUS DAY

PROJECT PRESENTATION SOON

LOOK @ SLIDES FOR ARM INSTRUCTIONS

TRUSTED EXECUTION ENVIRONMENT
~~↳ APPSTRAND~~
↳ HARDWARE-BASED
  ↳ SECURE, ISOLATED, INTEGRITY-PROTECTED
  ↳ HAS PROCESSING, MEMORY, & STORAGE
  ↳ ISOLATED FROM NORMAL ENVIRONMENT

↳ GOALS OF TEE
  ISOLATED EXECUTION
  ↳ TEE MAY BE MALICIOUS
  SECURE STORAGE

↳ EXAMPLE APPS
  ↳ CRYPTO
    ↳ KEY STORAGE
    ↳ KEY USAGE POLICY ENFORCEMENT

ARM TRUST ZONE
↳ PROVIDE COMPLETE VIRTUAL SYSTEM FOR SECURE COMP.
↳ DIVIDE HW ~~[illegible]~~ & SW INTO SEC "WORLDS"
  ↳ ONE TRUSTED ("SECURE WORLD")
  ↳ ONE NOT ("NORMAL " ")
↳ LIMITED & TIGHTLY DEFINED WAYS TO GO BTWN THEM
↳ EACH SECURITY STATE HAS SYSTEM REGISTERS & MEM ADDRS

EXAM 1 - OCTOBER 17
↳ LECTURE NOTES THROUGH TODAY
↳ LAB 1 PART 1

TODAY: TRUSTZONE SOFTWARE ARCHITECTURE

SOFTWARE DESIGN OPTIONS:
- RUN FULL SECURE WORLD OS
- USE TRUST ZONE AS A SECURE LIBRARY
- SOMETHING IN BETWEEN

ENTERS MONITOR MODE W/ SMC INSTRUCTION

MONITOR MODE SOFTWARE
- MANAGES SWITCHING BTWN SECURE & NON-SECURE WORLDS
- CONTEXT SWITCHES SIMILAR TO OS CONTEXT SWITCHING, BUT NOT QUITE THE SAME
  - STORE GENERAL PURPOSE REG
  - ANY NON-BACKED UP COPROC REGISTERS
  - ANY WORLD SPECIFIC INFO
  - SOURCE CODE EXAMPLE ON MYCOURSES
    - EACH WORLD NEEDS TO DO ITS OWN INIT OF STACK & MMUs
    - CPS INSTRUCTION CHANGES MODES

GO THROUGH & UNDERSTAND WHAT'S GOING ON

PROJECTS USING TRUSTZONE
- CORTEX A
  - NORMAL WORLD CODE CAN'T ACCESS SECURE WORLD RESOURCES
  - SWITCH IS DONE BY SMC. SECURE WORLD CAN'T DO TRAP-EMULATE
- REAL TIME KERNEL PROTECTION FROM SECURE WORLD
  - SAMSUNG KNOX
- TRADITIONAL & PREVIOUS KERNEL PROTECTIONS
  1) SEC. TOOL RUNS IN SAME ADDR SPACE & PRIVILEGE LEVEL AS KERNEL
  2) HYPERVISOR BASED APPROACHES: USE VIRTUALIZATION TO PROVIDE SEC. TOOLS W/ HIGH PRIVILEGE & ISOLATION
  3) HARDWARE APPROACHES: AMD SVM, INTEL TXT, ARM TZ
- LIMITATIONS OF HW APPROACHES
  1) INABILITY TO CLOSELY MONITOR EVENTS IN TARGET KERNEL
  2) CAN ONLY TO PERIODIC KERNEL CHECKING
     - ONLY DETECT ATTACKS AFTER THEY'VE HAPPENED OR NOT AT ALL
     - NOT EVENT DRIVEN MONITORING
- TECHNICAL CHALLENGES
  - TZ SEC WORLD CANNOT INTERCEPT CRITICAL EVENTS
- THREAT MODEL
  - EXECUTING UNAUTH PRIVILEGED CODE
    - AIM TO INJECT MALICIOUS CODE
    - MODIFY PRIVILEGED CODE
    - ESCALATE PRIV. OF USER SPACE CODE
  - BOOTING PHONE

USENIX 2016 - fTPM: A SOFTWARE-ONLY IMPLEMENTATION OF A TPM CHIP
↳ MICROSOFT
↳ DEPLOYED IN WINDOWS PHONE
↳ EMULATE TPM IN TZ SECURE WORLD

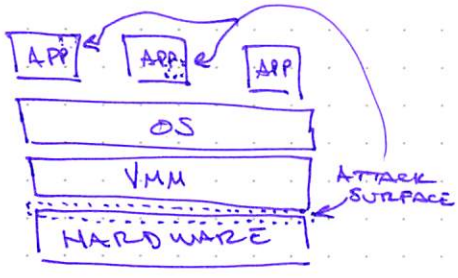
TRUST ZONE PROPERTIES
↳ ISOLATED RUNTIME THAT BOOTS FIRST
↳ CURTAINED MEMORY
  ↳ NOT ENCRYPTED, BUT HIDDEN FROM NORMAL OPERATION
↳ ABILITY TO MAP INTERRUPTS DELIVERED TO SECURE WORLD
  ↳ SECURE MONITOR DISPATCHES INTERRUPTS
↳ INSTRUCTION SMC FOR WORLD SWITCH

TZ VS. TPM LIMITATIONS
↳ TZ DOES NOT HAVE ISOLATED/TRUSTED STORAGE
↳ TZ LACKS SECURE ENTROPY & PERSISTENT COUNTERS
  ↳ CAN'T GEN RANDOM #S
↳ LACK OF VIRTUALIZATION
  ↳ TZ DOESN'T HAVE BUT ARM DOES SOMETIMES
↳ NO SECURE CLOCK & OTHER PERIPHERALS
↳ LACK OF ACCESS (DON'T OPEN TZ TO 3RD PARTIES)
↳ NO MEMORY ENCRYPTION

WHAT CAN TZ OFFER?
↳ CONFIDENTIALITY & INTEGRITY OF MEM FROM ATTACKS FROM NORMAL WORLD
TZ CAN'T PROTECT FROM MEMORY ATTACKS

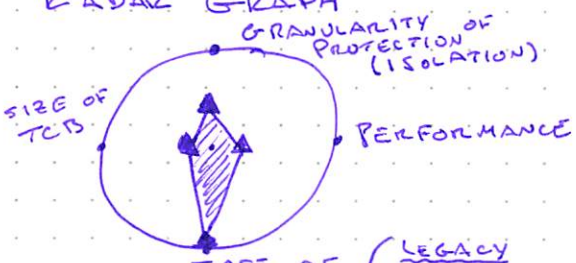
MIDTERM 2 - DEC 3RD
LAB 2 - LATER THIS WEEK
NEXT WEEK - GUEST SPEAKERS

SGX



SGX SECURE ENCLAVE SIMILAR TO TZ
↳ SEC. ENCLAVE CAN'T DO AS MUCH
  ↳ CAN'T RUN OS, JUST SOME PROCESSES
  ↳ ONLY @ APPLICATION LEVEL

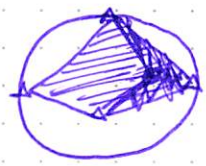
RADAR GRAPH



HAVEN
- ~~LEGACY~~
- ~~BINARY~~
- ~~SOURCE~~
- ~~ANNOTATION~~
- RE-DESIGN

SCONE

GLAMDRING



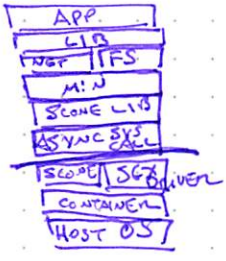
SCONE: SECURE LINUX CONTAINER ENVIRONMENTS USING SGX

TRUST ISSUES:
- ↳ CLOUD OWNERS ~~DON'T~~ TRUST USERS
- ↳ USERS ~~DON'T~~ TRUST CLOUD PROVIDERS

CONTAINERS
- ↳ W/OUT SGX, HAS SAME ISSUES AS VMs

GOALS:
- ↳ RUN UNMODIFIED LINUX APPS
- ↳ IN CONTAINERS
- ↳ IN UNTRUSTED CLOUD
- ↳ SECURELY
- ↳ AND W/ MINIMAL PERF. ~~HIT~~

SCONE ARCH:



GLAMDRING

WHAT DID WE DISCUSS?

1) TRUST, TRUSTED TCB
2) TPM
3) TRUSTZONE
4) SGX

VULNERABILITIES:

TPM-FAIL: TPM MEETS TIMING & LATTICE ATTACKS
- ↳ SOME TPM 2.0 VULNERABILITIES
  - ↳ LEAKING DATA FROM ECC