Towards Security in Cyber Physical Systems

Dawn Song

UC Berkeley

Berkeley
UNIVERSITY OF CALIFORNIA

Massachusetts
Institute of
Technology

MICHIGAN

VANDERBILT
UNIVERSITY

The world is becoming more and more connected

- 1.1 Billion smart phones
- 244 Million smart meters
- 487 Million e-readers and tablets
- 2.37 Billion networked office devices
- 86 Million medical devices
- 45 Million connected automobiles
- 547 Million connected appliances
- 45 Million supervisory control and data acquisition (SCADA)
- 5+ Billion other (non-phone/tablet/e-reader) electronic devices
- Over 50 Billion connected devices by 2020

The world is becoming more and more connected

Malware enters new landscape as more parts of the world get connected

Malware enters new landscape as more parts of the world get connected

* Legacy, traditional vulnerabilities & attacks in new landscape

First Security Analysis on Medical Devices

* Cardiac Science G3 Plus model 9390A
* Analysis
  * Manual reverse engineering using IDA Pro
    * *MDLink*, *AEDUpdate* and device *firmware*
  * Automatic binary analysis
    * BitBlaze binary analysis infrastructure
    * BitFuzz, the dynamic symbolic execution tool
* Vulnerabilities lead to distributed worm in AED
  1. AED Firmware - Replacement
  2. AEDUpdate - Buffer overflow
  3. AEDUpdate - Plain text user credentials
  4. MDLink - Weak password scheme

The case for Software Security Evaluations of Medical Devices [HealthSec'11]

Malware enters new landscape as more parts of the world get connected

* Legacy, traditional vulnerabilities & attacks in new landscape

* New classes of vulnerabilities & attacks on new platform

Automatic In-depth Analysis of 3M+ Android Apps

- UC Berkeley/Ensighta Security Inc./FireEye Inc.

Malware

Adware

Vulnerable apps

Apps with undesired/unintended Security Consequences

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Case Study in Android: JS Binding & JBOH Vulnerability

* JavaScript (JS) Binding
  * JS binding in WebView is designed to allow JS to access certain Java objects & interfaces exposed to JS

* JavaScript (JS) Binding vulnerability
  * JS binding in WebView can be abused to execute arbitrary code on device from JS
    * JS binding allows JS to use Java reflection to acquire a reference to a runtime object
    * then execute arbitrary commands on the device
  * E.g., Adobe pdf reader
    * A malicious PDF can read your files (accessible to Adobe PDF reader) on Android and send them over the Internet

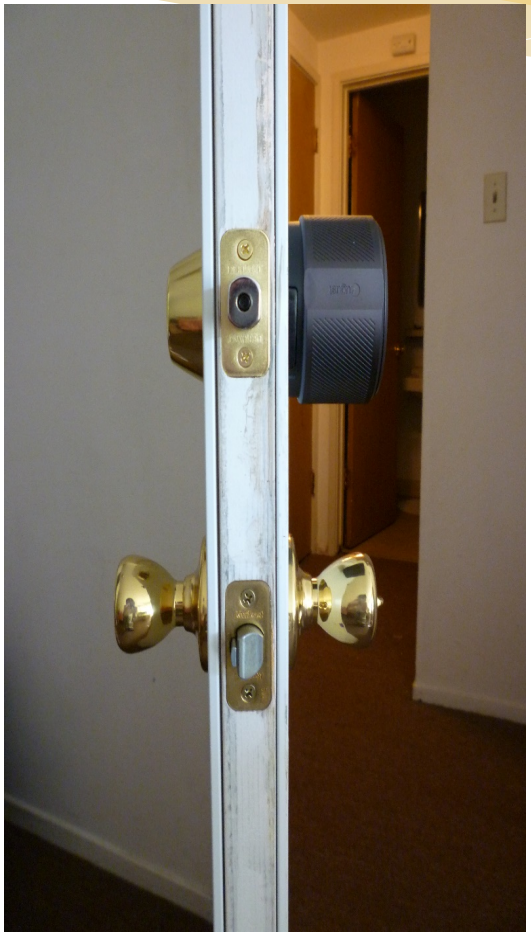
JBOH Vulnerability

* JavaScript-Binding-over-HTTP (JBOH) vulnerability
  * JS binding + WebView traffic going over HTTP
  * If you control one of these:
    * HTTP traffic, DNS, BGP…
  * You can:
    * Steal SMS (including two-factor auth token), take photo, record audio, etc., if the app has needed permissions

* Finding: JBOH in Android Ad Libraries
  * 18 out of the top 40 ad libs are JBOH (47%)
  * Affect more than 5.2 billion Google Play downloads (>18%)

Smart Locks

OUTSIDE View



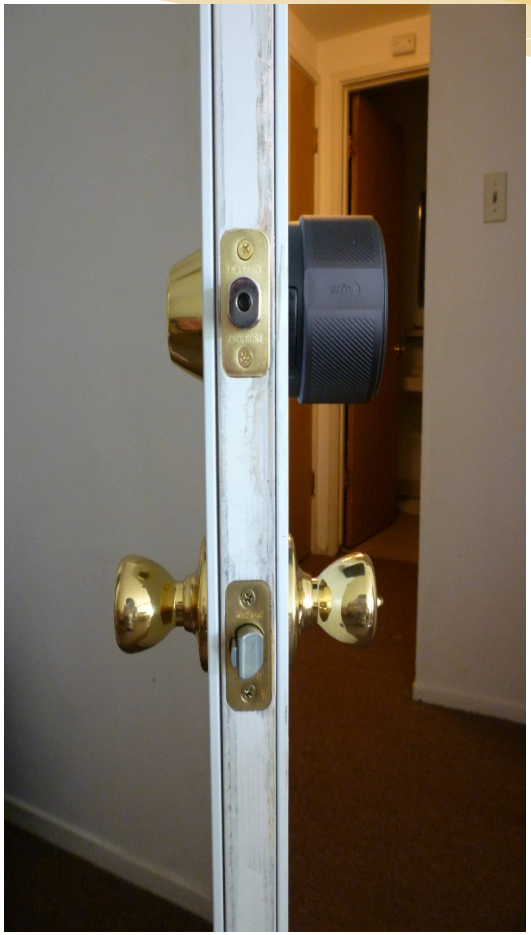
Side View

INSIDE View

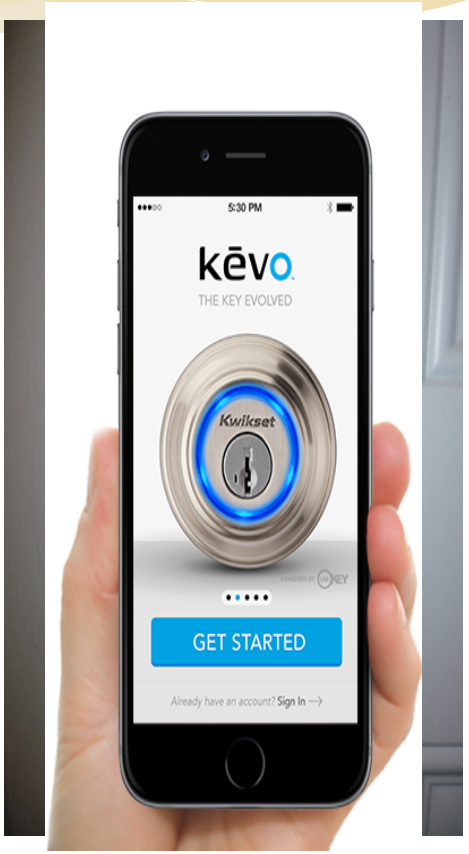
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Smart Locks

OUTSIDE View



Side View



INSIDE View

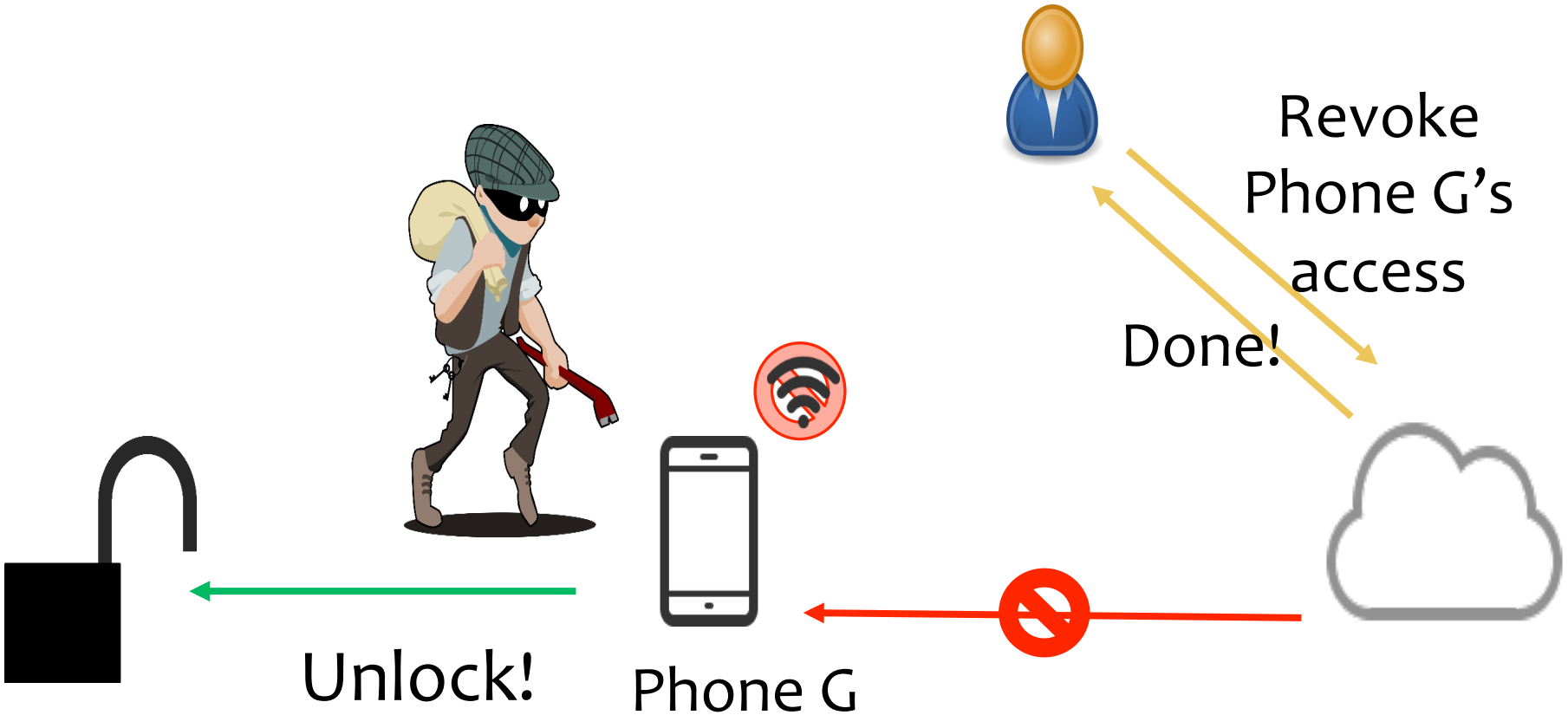
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Case Study: Revocation Evasion

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Case Study: Revocation Evasion

Mallory steals phone and switches it offline



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Malware enters new landscape as more parts of the world get connected

* Legacy, traditional vulnerabilities & attacks in new landscape
* New classes of vulnerabilities & attacks on new platform
* New threat models with new technology

Consumer-grade BCI Devices

* Price: ≈ 300 USD

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

HEADSET & ACCESSORIES

DEVELOPER & RESEARCH PACKAGES

APP STORE

BLINKCHALLENGE
Uses a Emobot interface and it can catch your blink immediately. Try to beat your longest stare! Or how fast can you blink? You just wear the headset and try this game

Rate this product:

$4.95

BUY NOW

ARENA
This is a game that requires you to use the power of your mind against your opponent. To play the game, you must first train your mind to shoot fireballs using the Emotiv PUSH command.

This game supports single and dual player modes. For dual player mode (DUEL) each player will

Rate this product:

$14.95

BUY NOW

SPIRIT MOUNTAIN DEMO GAME
Experience the fantasy of having supernatural powers and controlling the world with your mind. Your journey will take you through a mythical landscape of forests, temples and an environment that adjusts itself based on how you feel.

Rate this product:

FREE

FREE

DOWN LOAD

MASTER MIND
Master Mind allows users to play their favorite PC games with the power of their mind. Existing PC games such as World of Warcraft™ and Call of Duty™ can now be played with the power of your mind.

$99.00

BUY NOW

MIND MOUSE
Mind Mouse is a revolutionary thought-controlled software application which allows the user to navigate the computer, click and double click to open programs, compose email and send with the power of their mind.
*** "NON 'AA

$99.00

BUY NOW

EMOTIV EPOC UNITY3D™ DEVELOPER SUPPORT PACK
This package contains a full Unity3D™ Wrapper for the Emotiv EPOC EmoEngine API and a working demonstration game project and assets.

$79.95

BUY NOW

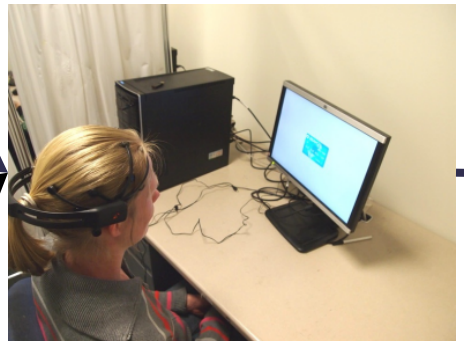
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

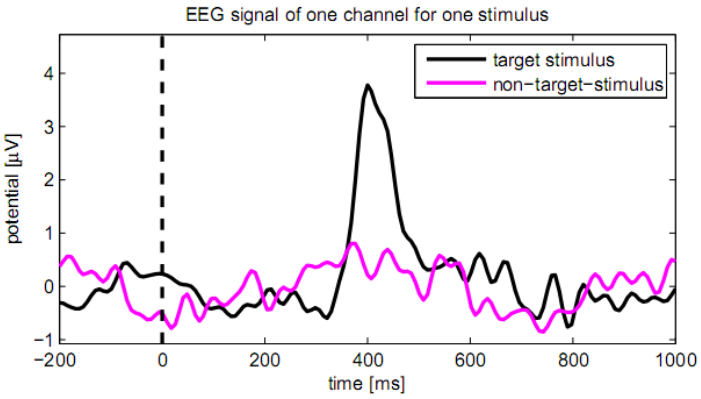
What if an EEG gaming app is malicious?

Secretly reading your mind?

BCI as Side-Channel to the Brain

Training Stimuli (known)





Signal Processing/ Classifier

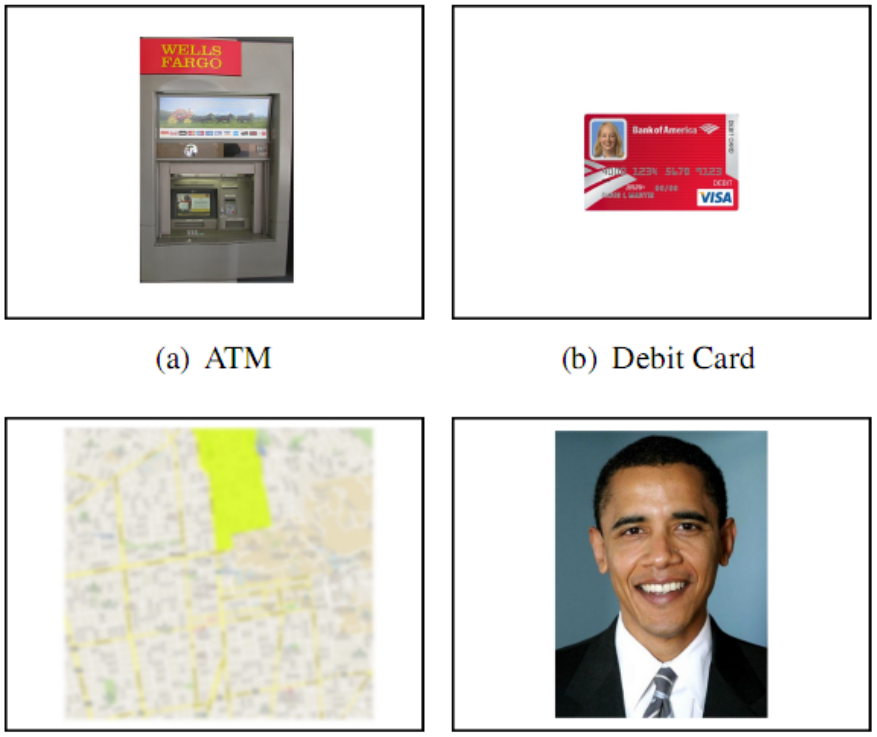
Stimuli Ranking

Attack Stimuli (unknown)

On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces [USENIX Security'12]

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Attack Stimuli



(a) ATM (b) Debit Card

Information tested:

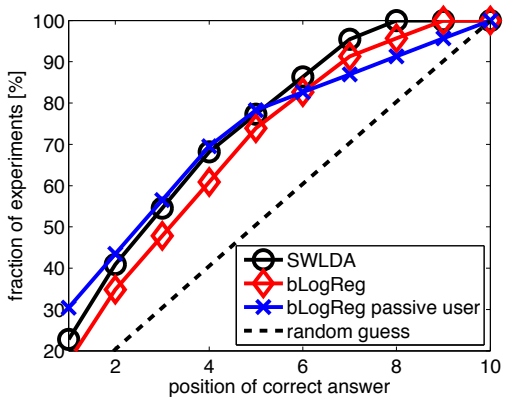
- First digit of PIN
- Do you know this person?
- Do you have an account at this bank?
- What month were you born in?
- Where do you live?

On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces [USENIX Security'12]

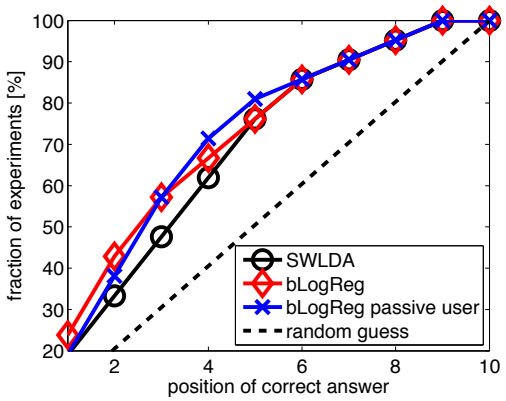
FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

BCI as Side-Channel to the Brain

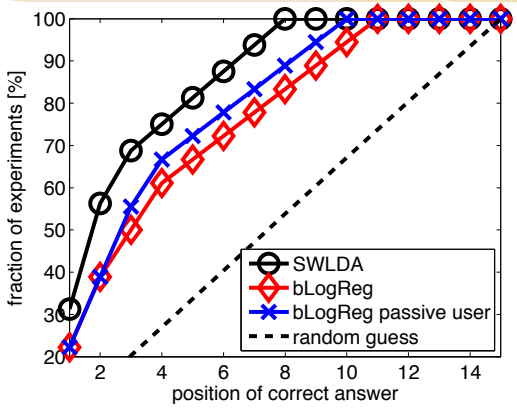
Experimental results from 30 participants



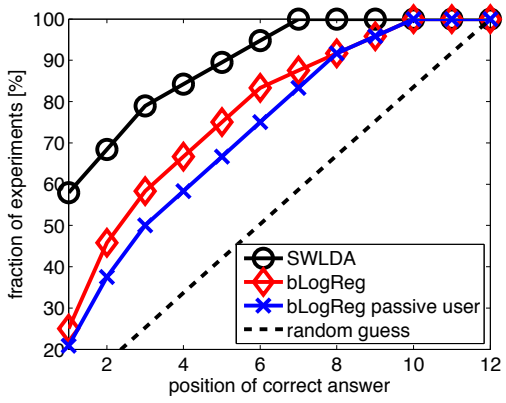
(a) 1st digit PIN



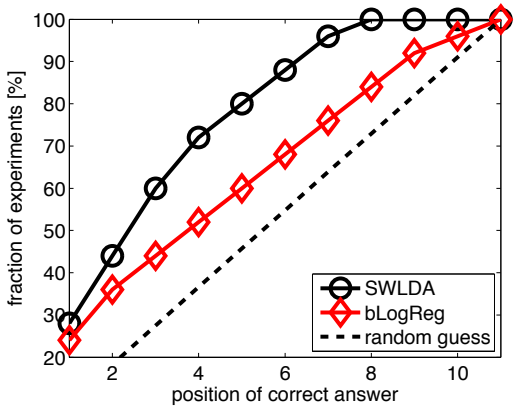
(b) Debit card



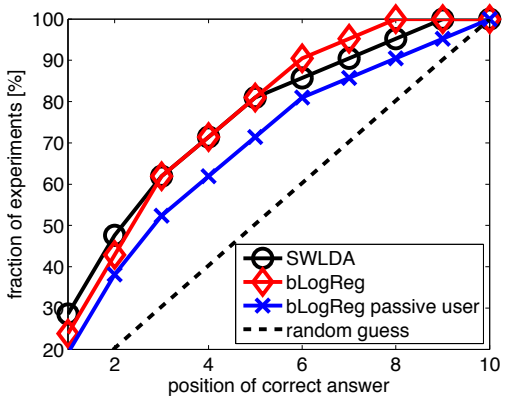
(c) Location



(d) Month of birth



(e) People



(f) ATM machine

On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces [USENIX Security'12]

The Dual

The More Powerful Consumer-grade BCI devices are ↑

↓

The More Powerful the attacks are ↑

Malware enters new landscape as more parts of the world get connected

* Legacy, traditional vulnerabilities & attacks in new landscape
* New classes of vulnerabilities & attacks on new platform
* New threat models with new technology

Traditional Defenses

Reactive Approaches

* Detecting and blocking malware
* Patching exploited vulnerabilities
* Most of commercial security solutions today
  * Network-based security solution
  * Host-based security solution

Reactive Defense Is Insufficient

* Cat-&-mouse game
  * Needs to change as attacks change
* Malware can cause real physical damage
* Deploying patches may be difficult
  * May require additional certification

Proactive Defense

* Making it easier to build secure systems
  * Free of certain classes of vulnerabilities
* Approach 1: reducing vulnerabilities by automatic bug finding
* Approach 2: secure by construction

Proactive Defense
Bug Finding

Proactive Defense
Secure by Construction

Approach 1: Automatic Bug Finding

Proactive Defense
Bug Finding

* Challenges:
  * Cannot guarantee finding all vulnerabilities
    * High false positive/false negative
  * Asymmetry
    * Attacker only needs to find one vulnerability
  * Race with the attacker
    * Who finds the vulnerability first

Approach 2: Secure by Construction

Proactive Defense
Secure by Construction

* Define security properties
  * Many possibilities

* Security mechanisms at different stages to ensure property
  * Compilation stage
  * Program instrumentation & transformation post compilation
  * (Provably secure) security primitives

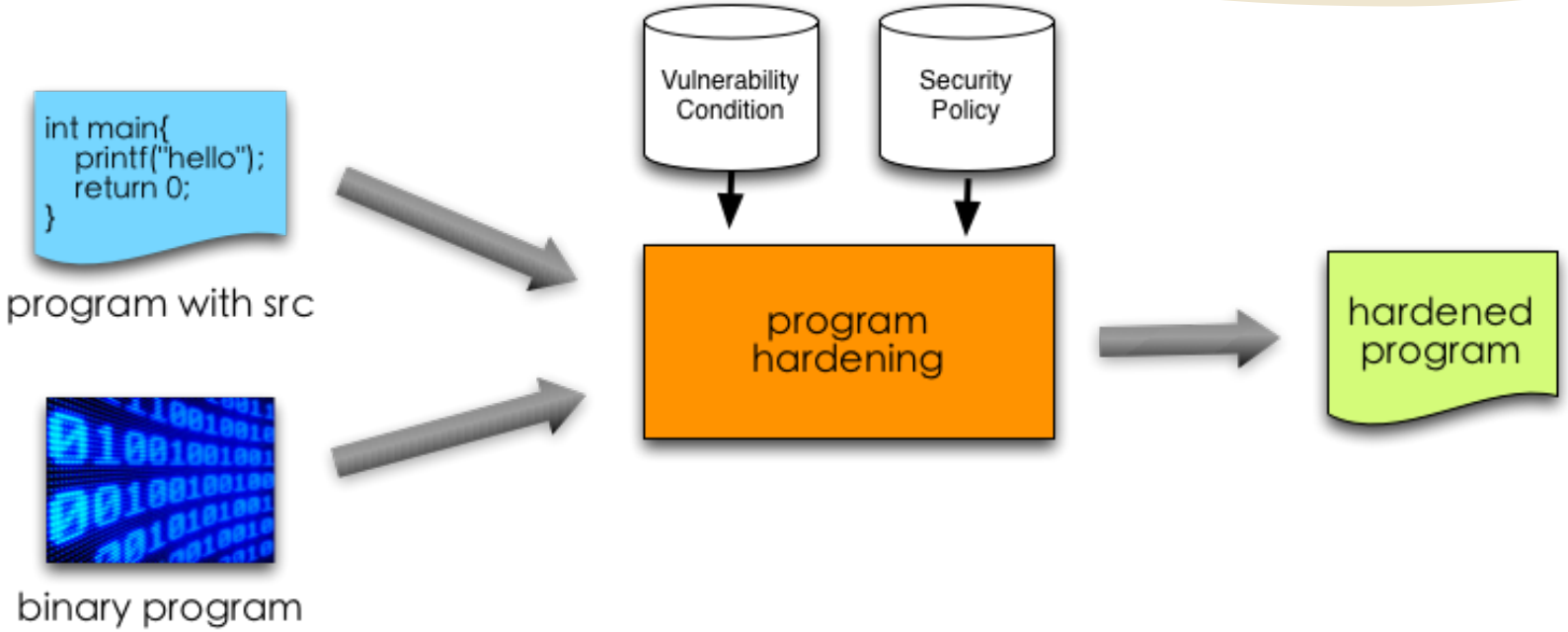
* Practical
  * Low performance overhead
  * Compatibility
  * Little to no effort from developer

Towards Building Secure Cyber Physical Systems by Construction

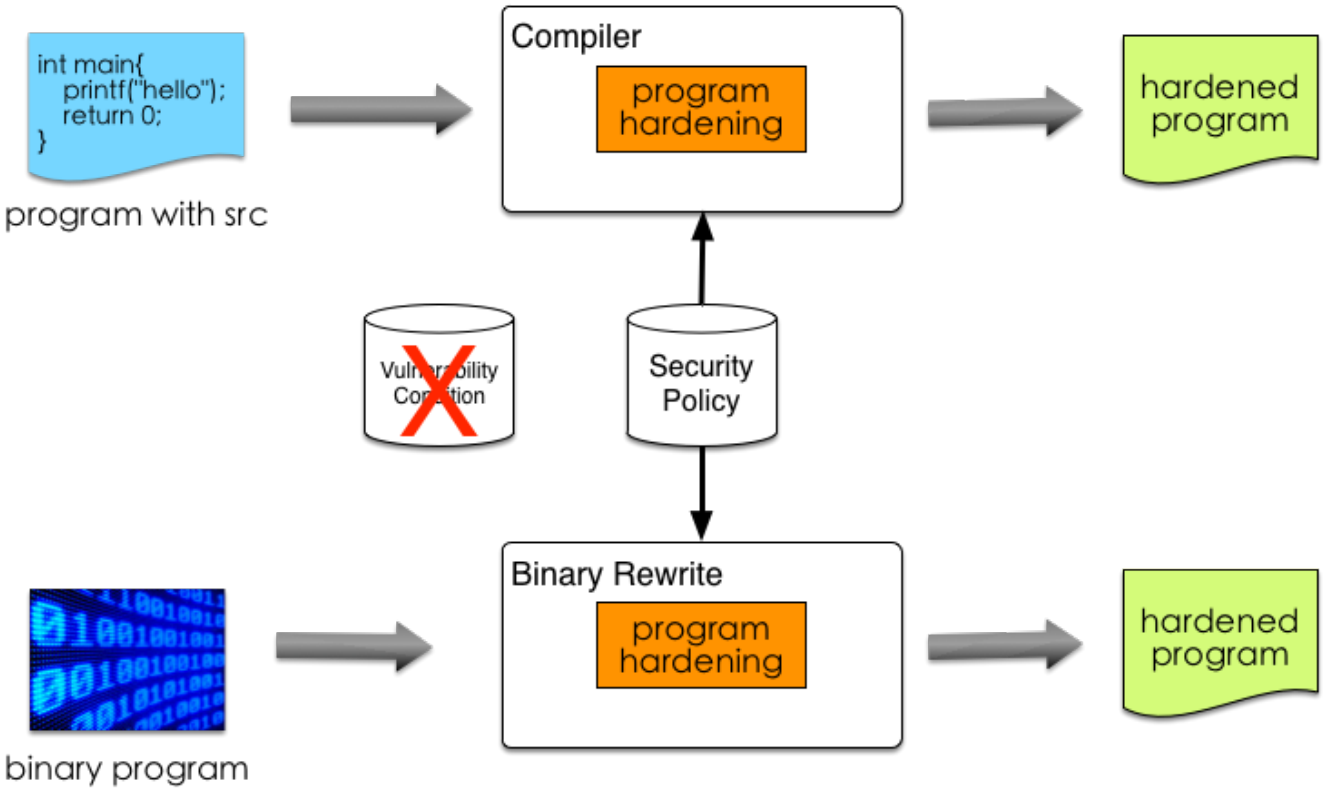
* Program hardening to protect against exploits

* Security as a service for managing security life cycle

Program Hardening



Our Solutions



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Code Pointer Integrity (CPI)

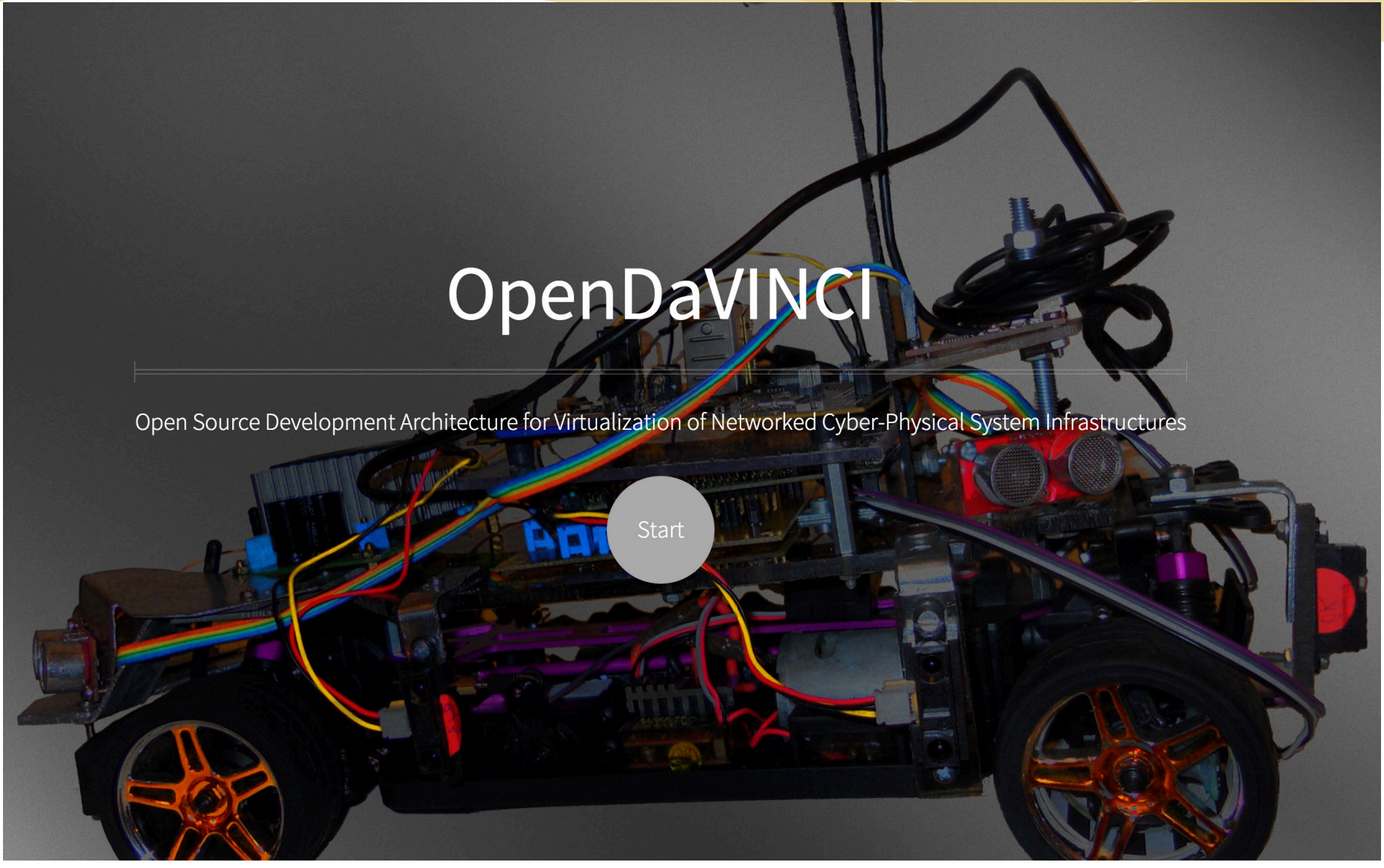
* Harden complete FreeBSD distribution (modulo kernel)
  * Protecting against control-flow hijacking attacks
* >100 extra packages

VTint: Defending against VTable Hijacking

* VTable hijacking is popular and critical
  * Real-world exploits against COTS applications exist.
  * CPS applications also have a large attack surface.
* Existing solutions are not perfect
* VTint is a lightweight, binary-compatible and effective defense against VTable hijacking, similar to DEP

defense solution	*vtable hijacking*			info leakage	binary support	perf. overhead
	corrupt	inject	reuse			
VTGuard	N	N	Y	N	N	0.5%
SD-vtable	N	Y	Y	N/A	N	30%
SD-method	Y	Y	Y	N/A	N	7%
DieHard	partial	partial	partial	N/A	N	8%
VTint	Y	Y	partial	Y	Y	2%

Program Hardening in Cyber Physical Systems



Attack Surface of OpenDaVINCI

	#vtable	#vcall
RuntimeControl~1	175	1325
RuntimeControl~2	161	826
RuntimeControl~3	155	780
QueueTestSuite	63	650
ControlFlowTes~	138	643
ConferenceClie~	124	607
TCPTestSuite	55	465
ConferenceFact~	74	447
DMCPConnection~	76	421
ConnectionTest~	62	417
DMCPDiscoverer~	60	411
DataStoreTestS~	61	401
AbstractCIDMod~	58	365
UDPTestSuite	43	346
CommandLinePar~	34	343
KeyValueConfig~	35	332

	#vtable	#vcall
TimeFactoryTes~	40	329
SharedPointerT~	31	325
DisposalTestSu~	30	309
TimeStampTestS~	34	306
ConditionTestS~	39	302
ClockTestSuite	27	297
NetstringsProt~	35	290
RunnerTestSuit~	27	290
FalseSerializa~	37	288
ContainerTestS~	36	287
ServiceTestSui~	40	286
SerializationT~	32	279
StringProtocol~	33	275
SharedMemoryTe~	25	273
MutexTestSuite	28	259
TreeNodeTestSu~	25	250

* Most modules have virtual calls and VTables
* The attack surface is large enough for real world attacks.

Towards Building Secure Cyber Physical Systems by Construction

* Program hardening to protect against exploits

* Security as a service for managing security life cycle
  * Device onboarding/pairing
  * Device authentication/access control
  * Device removal/transition
  * Secure software update
  * Secure key management

Access Control on IoT Devices is Important

* Sensitive information on them
* Control other connected IoT devices

Smartphone

Wearable

Healthcare Monitor

Smart lock

Current Solutions

* Password
  * Limited applicability: Some IoT devices do not have touchscreen or keyboard
  * Tedious: Need to type in password every time
  * Insecure: Users select weak passwords/reuse passwords
* Biometrics
  * Unreliable, e.g., fingerprint on smartphones might require multiple trials.
  * Insecure: Vulnerable to forgery attacks

Emerging Scenarios in IoT

* A user carries a IoT device which has already authenticated the user's identity.
  * Vouching device
* Authentication on another IoT device
  * Authenticating device
* Examples
  * Vouching device=wearable, authenticating device=smartphone
  * Vouching device=smartphone, authenticating device=smart lock

Key Observation

Vouching device=wearable

Authenticating device=smartphone

Small *d*

Close when the legitimate user uses the smartphone

Large *d*

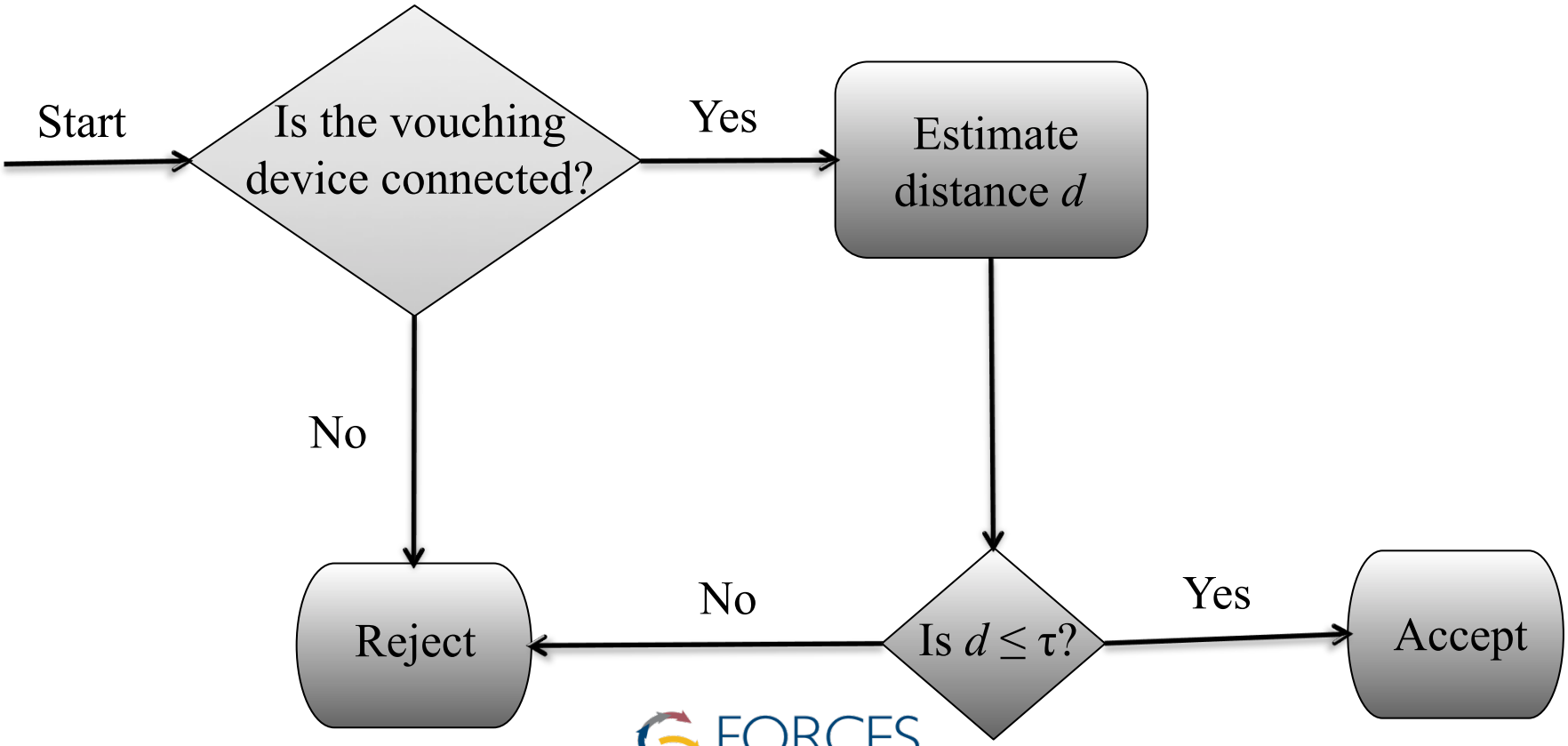
Far away when an attacker tries to access the smartphone

Proximity-based Authentication

* Access is granted if and only if the distance between the authenticating device and the vouching device is no larger than an authentication threshold τ.
* Distance estimation techniques using radio signals such as Bluetooth, WiFi, and GPS have large errors on commodity devices
* Our goal: secure, reliable, passive, and efficient proximity-based authentication using acoustic signals

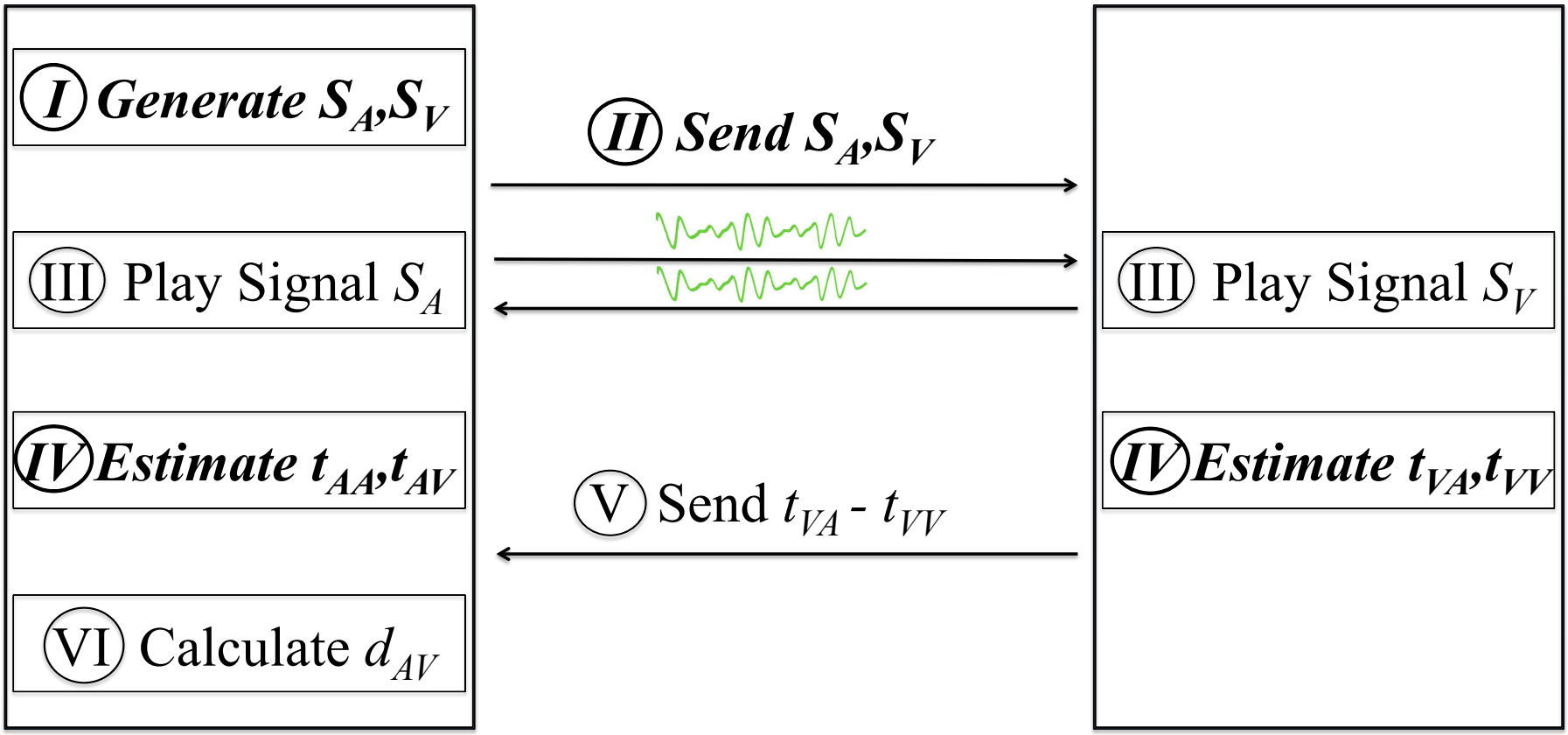
PIANO

* The two devices are already paired via a secure channel (e.g., Bluetooth)



FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Acoustic Signal Based Distance Estimation



$$d = \frac{1}{2} \cdot c \cdot ((t_{VA} - t_{VV}) + (t_{AV} - t_{AA}))$$

Results

FNRs in different environments and with different authentication thresholds

	0.5m	1.0m	1.5m	2.0m
Office	5.6%	2.8%	1.9%	1.4%
Home	9.5%	4.8%	3.2%	2.4%
Street	12.6%	6.3%	4.2%	3.1%
Restaurant	8.5%	4.2%	2.8%	2.1%
Multiple users	7.9%	4.0%	2.6%	2.0%

FPRs in different environments and with different authentication thresholds

	0.5m	1.0m	1.5m	2.0m
Office	0.3%	0.3%	0.3%	0.4%
Home	0.5%	0.5%	0.6%	0.6%
Street	0.7%	0.7%	0.7%	0.8%
Restaurant	0.4%	0.5%	0.4%	0.4%
Multiple users	0.4%	0.4%	0.5%	0.5%

* Efficiency
  * 3s per authentication
  * 100 times of authentication consumes 0.6% of smartphone battery

Malware enters new landscape as more parts of the world get connected

* Legacy, traditional vulnerabilities & attacks in new landscape
* New classes of vulnerabilities & attacks on new platform
* New threat models with new technology

Towards Building Cyber Physical Systems Secure by Construction

Reacting to Attacks **Racing with Attacks** **Eradicating Attacks**

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Towards Building Secure Cyber Physical Systems by Construction

* Program hardening to protect against exploits

* Security as a service for managing security life cycle
  * Device onboarding/pairing
  * Device authentication/access control
  * Device removal/transition
  * Secure software update
  * Secure key management