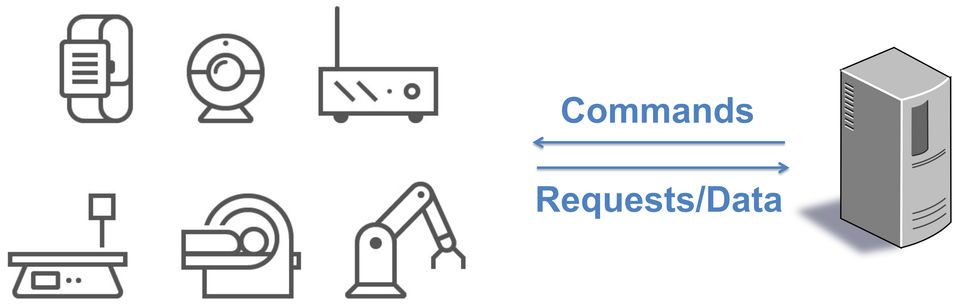
OAT: Attesting Operation Integrity of Embedded Devices

PI: **Long Lu**, Northeastern University

NSF Award# 1748334 -- CAREER: Rethinking Mobile Security in the New Age of App-As-A-Platform

The problem: Controllers' unverifiable (blind) trust on remotely deployed IoT devices



- *Issued commands executed faithfully w/o interruption?*
- *Incoming requests & data produced w/o manipulation?*

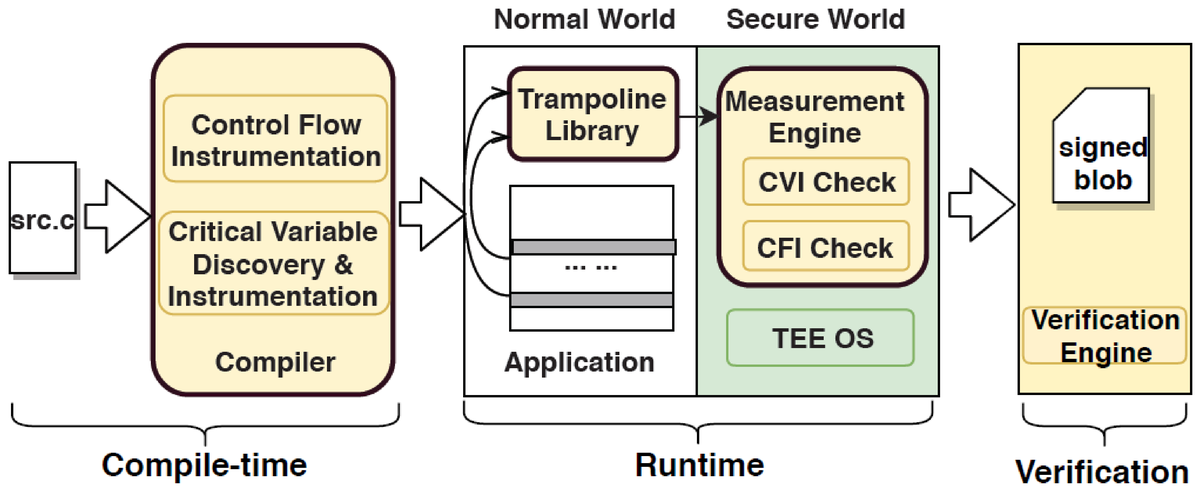
Our Solution: Remote attestation of **Operation Execution Integrity (OEI)**

A new security property formulated for embedded devices

OEI = { Operation-scoped CFI; Critical Variable Integrity }

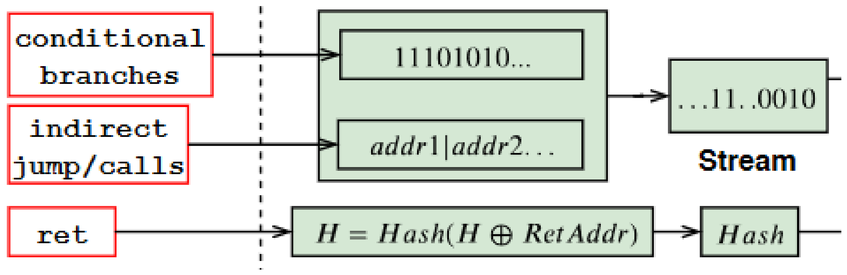
Efficiently capturing: (1) operation control flow deviations, and (2) corruption of critical data

A prover-verifier framework for attesting OEI



Scientific Contributions

- First formulation of a security property for capturing dynamic integrity of embedded devices
- A novel control flow attestation scheme, that is lightweight and deterministically verifiable



- A novel data integrity checking method, enforcing def-use-based value consistency, rather than heavy address-based checking

Result Highlights

- Runtime & verification overhead on real firmware

Prog.	Operation Exec. Time w/o OEI (s)	w/ OEI (s)	Overhead (%)	Blob Size (B)	Verification Time (s)
SP	10.19	10.38	1.9%	69	5.6
HA	5.28	5.36	1.6%	44	0.61
RM	10.01	10.13	1.3%	913	1.74
RC	2.55	2.66	4.5%	10	0.13
LC	5.33	5.56	4.4%	205	1.35
Avg.	N/A	N/A	2.7%	248	1.89

- OAT vs trace-based CFI checking

	SP	HA	RM	RC	LC	Avg.
R1	69	44	913	10	205	-
R2	42941	3772	13713	585	13725	-
R1 / R2	0.2%	1.1%	6.7%	1.7%	1.5%	2.24%

- OAT vs address-based data integrity checking

	SP	HA	RM	RC	LC	Avg.
R1	56	37	57	20	41	-
R2	140	388	842	45	131	-
R1 / R2	40%	9.5%	6.8%	44.4%	31.2%	26%

For more details, please refer to our IEEE S&P 2020 paper, preprint available at www.longlu.org/downloads/OAT.pdf