Min Wu
University of Maryland, College Park
minwu@umd.edu

Fernando M. Quintão Pereira
UFMG, Brazil
fernando@dcc.ufmg.br

Jie Liu
Microsoft Research
jie.liu@microsoft.com

Heitor S. Ramos
UFAL, Brazil
heitor@ic.ufal.br

Mário S. Alvim
UFMG, Brazil
msalvim@dcc.ufmg.br

Leonardo B. Oliveira
UFMG, Brazil
leob@dcc.ufmg.br

– New Direction –

Proof-Carrying Sensing:
Towards Real-World Authentication in CPS

Cyber-Physical Systems are Under Attack and Attacking

A DEEP FLAW IN YOUR CAR LETS HACKERS SHUT DOWN SAFETY FEATURES

CHNOLOGY

Massive IoT-Based DDoS Attack Could Affect Millions Of Devices: Cybersecurity Experts

BY **RISHABH JAIN** ON 10/25/17 AT 9:50 AM

SECURITY

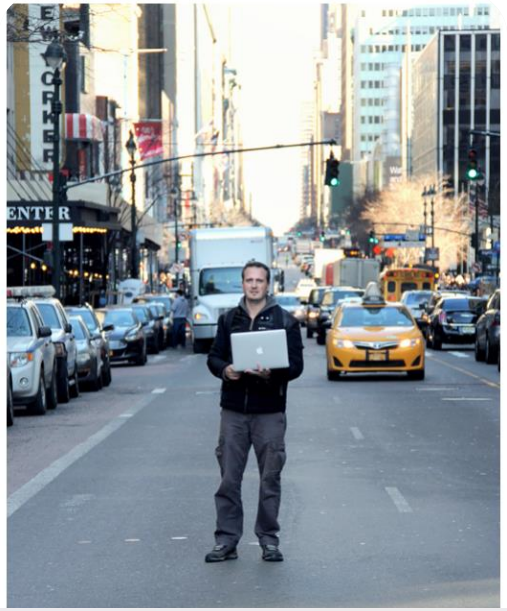
Report: IoT attacks exploded by 280% in the first half of 2017

A report from F5 labs showed how IoT devices have been targeted through botnets, many from a single hosting provider. Here are the results, and what they mean for the enterprise.

By Hope Reese | August 9, 2017, 11:35 AM PST

KIM ZETTER SECURITY 04.30.14 06:30 AM

HACKERS CAN MESS WITH TRAFFIC LIGHTS TO JAM ROADS AND REROUTE CARS



Cyber Security Paradigms Today

- Build walls
- Secure pipes
- Control accesses

Open Cyber-Physical Systems (aka Reality as a Service)

- Separation of decision makers and information providers
- Fusion of local and remote, public and private information
- “Journeys” across many administrative domains
- Ill-suited for sensor-edge-cloud architecture

Open CPS Vulnerabilities

Cyber

- The gap between device resources and attacker resources is rapidly increasing.
- Vulnerabilities are easily replicated due to mass production and hard to patch once deployed.

Physical

- Sensors can be physically moved to produce wrong data.
- Adversaries can physically access sensors to tamper its configuration or data

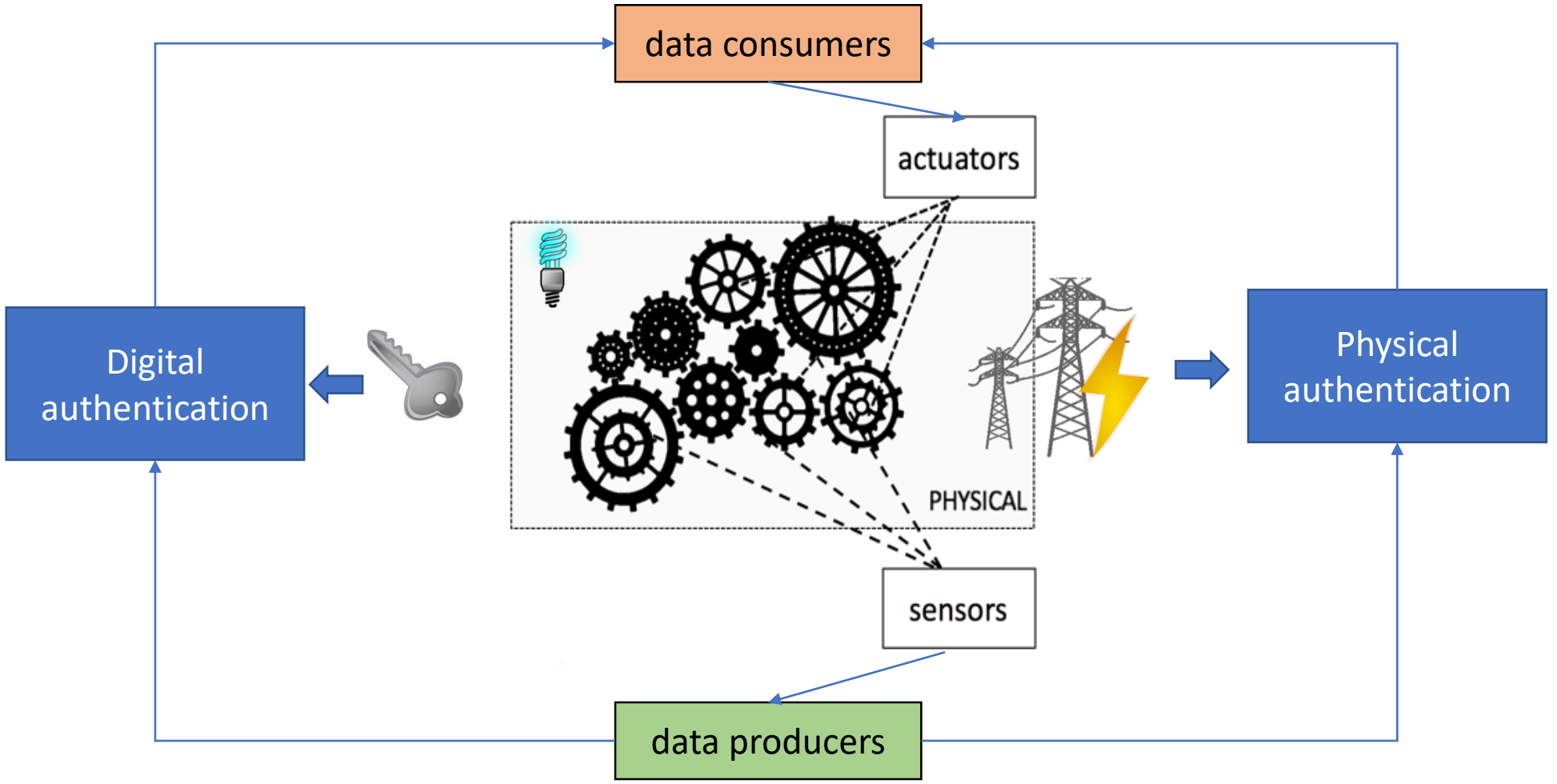
Human

- Domain-specific customization make best security practice hard to enforce.
- Disgruntled employees may leak system credentials and launch attacks from inside.

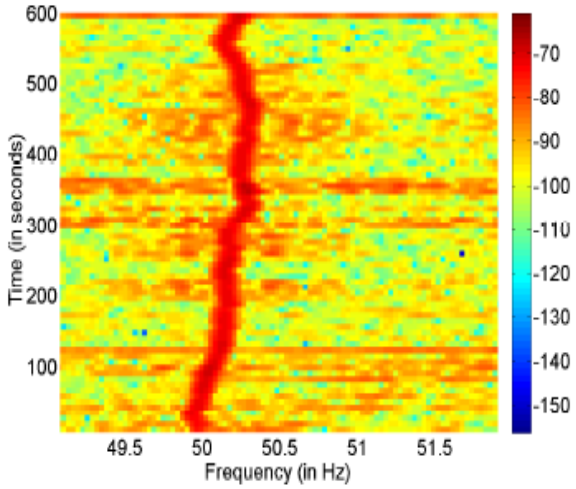
Data Authentication

How can we be sure that data is
from the right device,
in the right place,
at the right time?

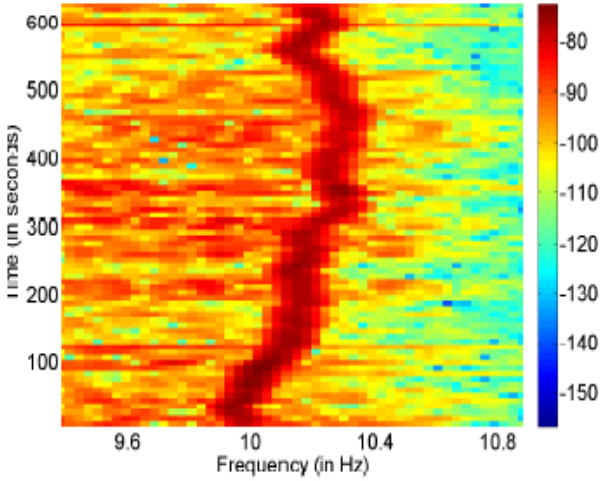
Proof-Carrying Sensing



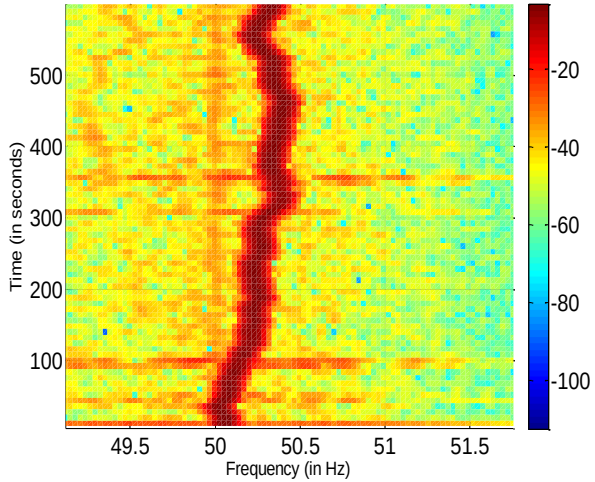
Intrinsic Signatures: Example Induced by Power Grid



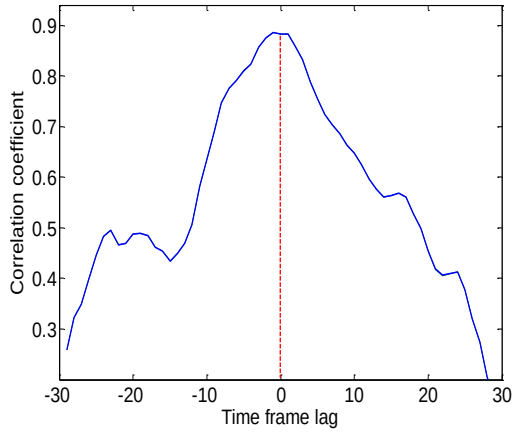
(a) ENF from audio track



(b) ENF from video track



(c) Concurrent power-line ENF



(d) normalized correlation (between video & power)

- Spectrograms show electric network frequency (*ENF*) signals induced by power grid in concurrent recordings of audio recording, visual recording and power main.
- Cross-correlation study shows the similarity between media and power line reference at different time lags, where the peak suggests their temporal alignment.

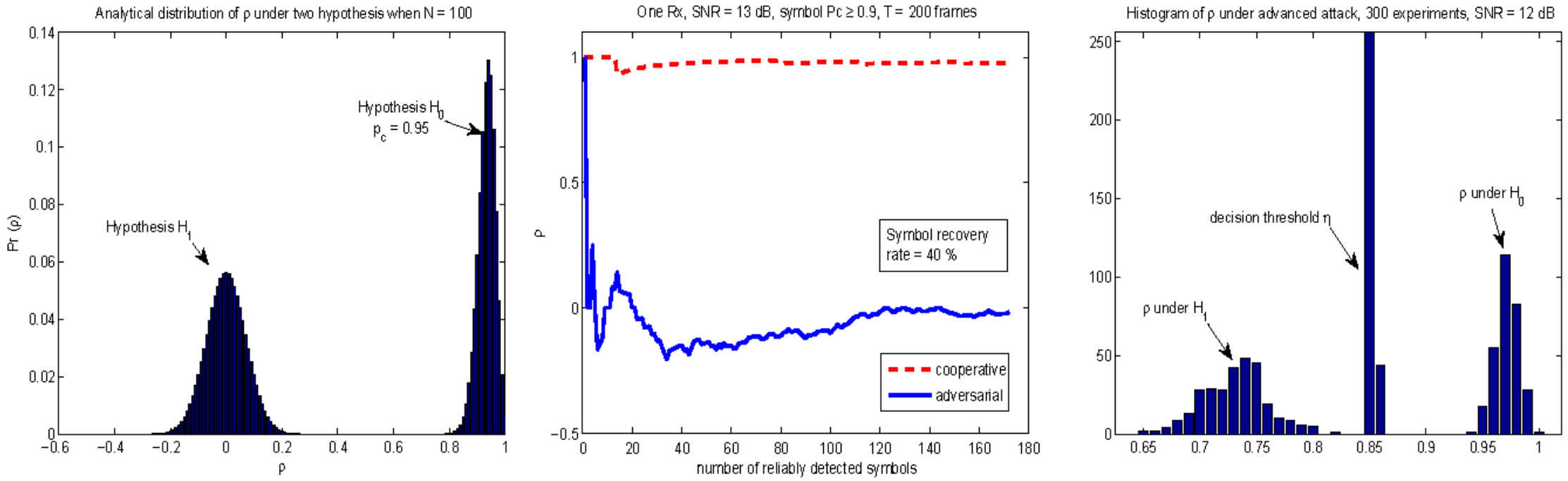
Extrinsic Signature

Signals and data injected and monitored by a system

- In the form of physical-layer watermarks, of physical- or digital-layer pilot sequences, or of challenges

- Exmaple-1: Watermarking CPS actuator (Satchidanandan, Bharadwaj & Kumar, 2017)
  - An actuator injects into the system a probing signal unknown to other nodes
  - Based on knowledge of the CPS' properties (dynamics etc.), the actuator can examine the sensors and infer whether there is malicious activity in the system or not, and where and how.
- Example-2: Identifying malicious behavior of relay nodes (Mao-Wu 2007)
  - Injection guided by cross-layer system modeling or crypto. random number generation
  - By design of known value or by proactive learning => establish the expected outcome of these signatures => A deviation from it indicates a potential abnormality

Extrinsic Signatures: Example



An example of injecting pseudo-random tracing symbols for relay-node authentication in cooperative wireless communications. (a) the distribution of detection statistic ρ (for N = 100 tracing symbols) measuring the normalized similarity between observed/estimated tracing symbols and the ground truth of such a signature, where the expected value of ρ is zero under adversarial relay (H1 hypothesis) and approaches one for cooperative relay (H0 hypothesis); (b) One realization of sequentially computed ρ as the number of reliably detected symbols grows; (c) histogram of ρ under partial-corruption attack by a sophisticated adversarial relay node, leading to an increased mean ρ value under attack.

Example: Smart Transportation

Example: Voting Machine/Smart Retail

Challenges ahead

Challenge 1: Suitable Physical Signatures.

- Characterize suitable intrinsic and extrinsic signatures.
- Quantitative models for normal and abnormal behavior of CPS.

Possible approaches:

- Physical models to yield analytic approximations of quantitative properties.
- Data-driven learning approaches to gather statistical data of behaviors.
- Metrics to assess the appropriateness of signatures in authenticating CPS.

Challenges ahead

Challenge 2: Formal Model and Certification. (Probabilistic?)

- Ensure authentication mechanisms based on local physical information are sound.
- Degree of tolerance for small variations between expected and received certificates.

Possible approaches:

- Probability theory and algebra techniques to the rescue!

Challenges ahead

Challenge 3: Safeguarding Physical Data.

- Leaks of physical data to outside network of trust.
- Adversaries who can read physical data in real time.
- Physical data shared among many devices.
- Time: old physical data might not need to be secured.

Possible approaches:

- Information-flow framework to preserve the confidentiality of data.
- Temporal logic techniques.

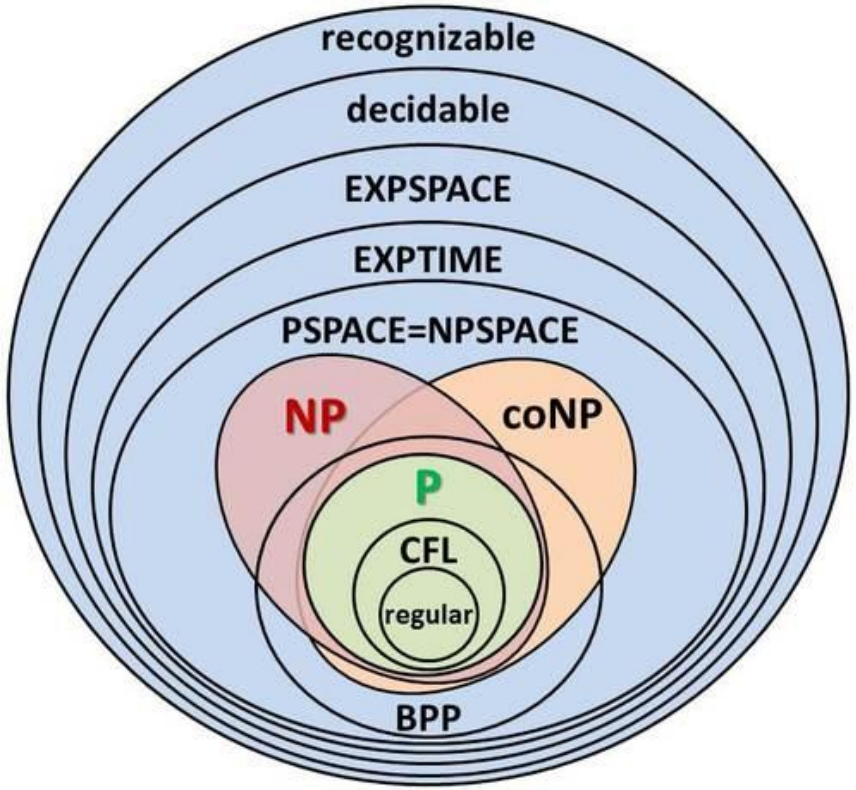
Challenges ahead

Challenge 4: Computational Complexity.

- Complexity results (space and time) for certifications, schemes, and mechanisms.
- Distributed algorithms running on low-power devices have online, adaptive behavior.

Possible approaches:

- Apply online and real-time algorithms.



Challenges ahead

Challenge 5: Dependable Software Engineering.
(mitigate human errors)

- Tools to implement, test, and deploy certification mechanisms?
- Polyglot programming vs. creating a domain-specific language?
- Ordinary programmers, not necessarily experts in software security, should be able to use our tools.

Possible approaches:

- Simulators to ease the effort of testing this kind of certification protocol.