INTERNET2 2017 global SUMMIT

BRINGING NETWORKS TOGETHER

GS 17

CINC UP: COLLABORATIVE INNOVATION COMMUNITY MEETING: IOT, E2ET&S, SMART CAMPUS

April 25, 2017

CINC UP: Collaborative Innovation Community Meeting: IoT, E2ET&S, Smart Campus

AGENDA

- Welcome
- Collaborative Innovation Community (CINC UP) Working Groups Update: Internet of Things (IoT), End-to-End Trust & Security (E2ET&S), Distributed Big Data & Analytics (DBDA), Emily Nichols, Internet2
- Smart Campus Initiatives Update, Emily Nichols, Internet2
- Smart Campus: IoT Systems Risk Management Task Force Update, Chuck Benson, University of Washington and Jan Cheetham, University of Wisconsin-Madison
- Trust, Identity, Privacy, Protection, Safety & Security (TIPPSS) for IoT: ITANA Collaboration and White Paper, Ken Klingenstein, Internet2 and Ed Aractingi, Marshall University
- Smart Campus Cybersecurity Transition to Practice (TTP) Researchers, Aranya Chakrabortty, NCSU, Raju Gottumukkala, University of Louisiana-Lafayette, Fareena Saqib, FIT
- IoT Pedagogy, Ed Aractingi, Marshall University
- Next Steps, Florence Hudson and Emily Nichols, Internet2

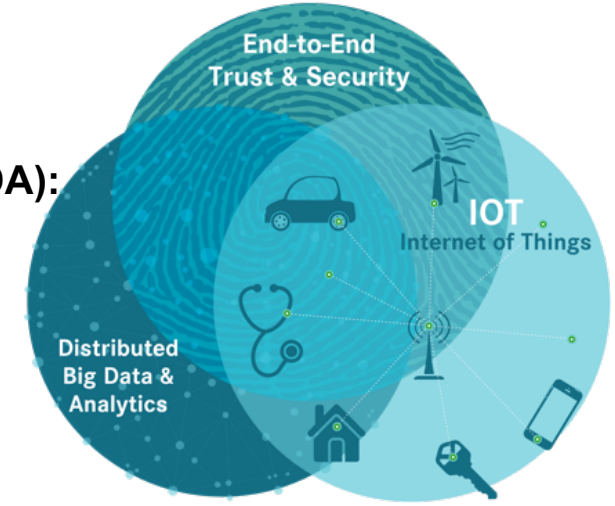
Collaborative Innovation Community is the combination of three member-led innovation working groups, focused on areas related to our top two priorities of advanced networking plus trust & identity.

E2E Trust & Security (E2ET&S):

- TIPPSS for IoT – Trust, Identity, Privacy, Protection, Safety, Security
- NSF EAGER Cybersecurity Transition to Practice (TTP) Acceleration
- SDP (Software Defined Perimeter), Network Segmentation for IoT

Distributed Big Data & Analytics (DBDA):

- Health & Life Sciences / Genomics
- Smart Campuses and Cities
- NSF Big Data Hub Collaboration



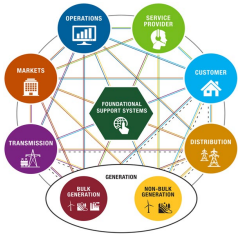
Internet of Things (IoT):

- IoT Sandbox
- Smart Campuses and Cities
- Smart Grid Testbed

Collaborative Innovation Community (CINC UP) includes Special Interest Groups pertinent to use cases identified by members.

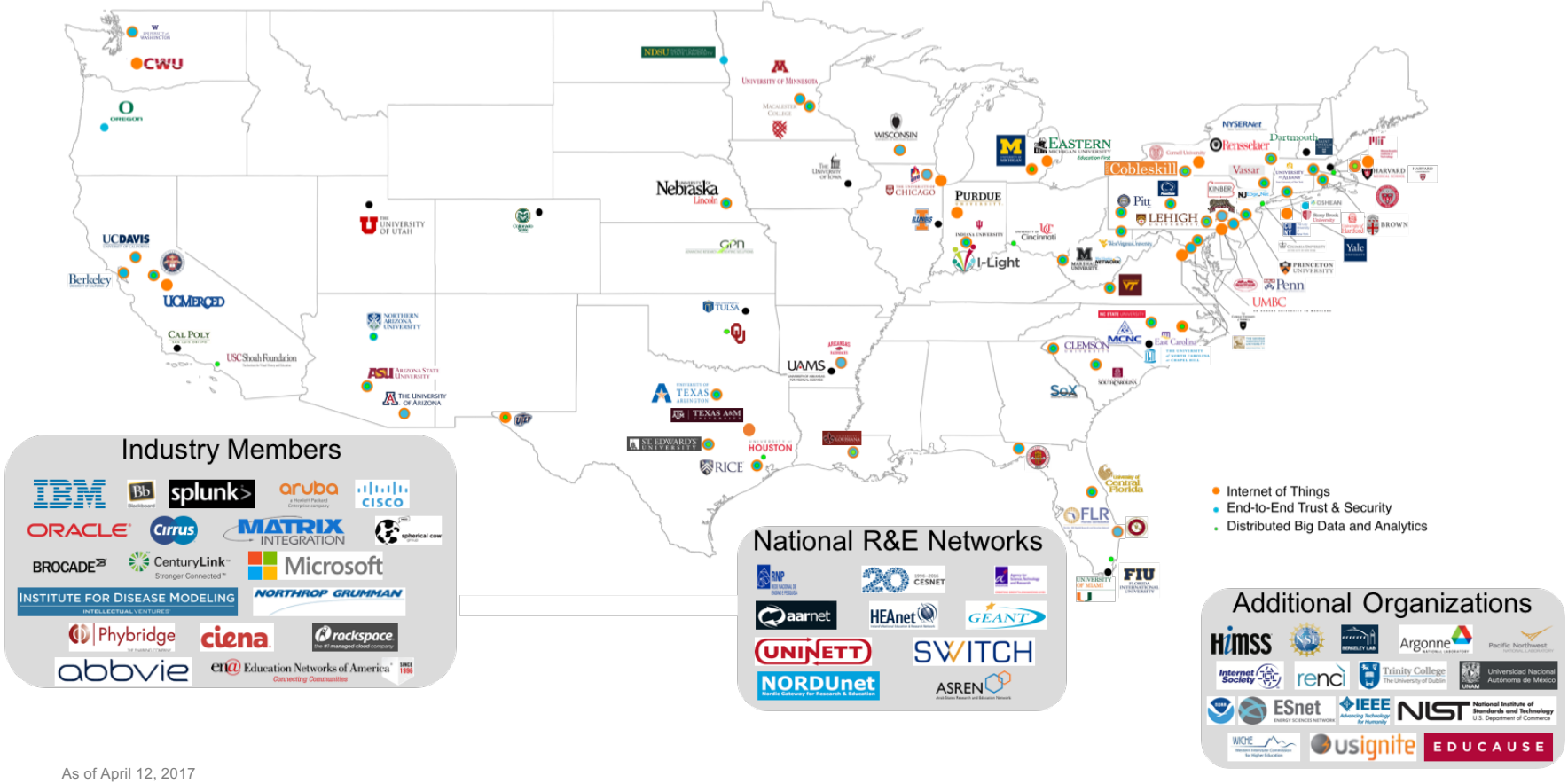
- Healthcare & Life Sciences / Genomics
- Smart Campus
- Smart Grid
- IoT Ethics
- Cybersecurity TTP

Join us! Email CINO@Internet2.edu



INTERNET2 2017 global SUMMIT Washington DC April 23-26

Internet2 Collaborative Innovation Community has grown to 335+ individuals representing 135 institutions.



As of April 12, 2017

CINC UP Community and CINO Deliverables

- **Collaborative Innovation Community / Innovative Working Group Monthly CINC UP Calls**
  - Presentations & discussions from members, SMEs on topics of interest to CINC UP Community
- **Cybersecurity Research Transition to Practice Acceleration Matchmaking**
  - 2016: TechEx 2016 kickoff, Matchmaking Webinar November with cyber researchers and practitioners
  - 2017: Workshop and Showcase at Global Summit, Regional Workshops, more webinars
- **Develop & Communicate Key Information Communications & Technology Trends for R&E**
  - Present broadly – 30 times across regional and university meetings
- **Internet2 Smart Campus Initiative**
  - Share best practices and recommendations to deploy IoT and Smart Campus capabilities
  - Global Summit and TechEx meetings
  - Engage industry members in collaboration with universities/regionals: IBM, Microsoft, Cisco
  - Microsoft Campus Connections Summit enabling new smart campus initiatives with Internet2 members
- **IoT Systems Risk Management Task Force**
  - Goal is to increase IoT systems risk awareness and provide deliverables to address risks, including:
    - Brochure on leveraging Shodan and Censys.io
    - IoT Systems Vendor Requirements Document
- **Member-led Thought Leadership**
  - ITANA / Internet2 led Enterprise IoT working group and TIPPSS for IoT whitepaper effort
  - Enable collaboration across R&E in focal areas. e.g., Smart Grid and Smart Campus/Communities
- **Connect member-led innovation initiatives to Internet2 services organizations to inform future services**

INTERNET2 2017 global SUMMIT Washington DC April 23-26

Smart Campus Initiative created based on member input & innovation working group use cases, with kickoff meeting at Global Summit 2016.

- Share best practices and recommendations to deploy Smart Campus capabilities
- Guided by a Smart Campus CIO Advisory Council
- Commissioned IoT Systems Risk Management Task Force
- Microsoft and Internet2 co-convened first annual Campus Connections Summit, Feb 2017, 140+ university “CIO + 1” attendees from around the world

ASU Arizona State University · Princeton University · UMBC · University of Pittsburgh · Marshall University · Virginia Tech

Indiana University Bloomington · University of Michigan · CUNY · The University of Wisconsin Madison · University of Washington

Research & Education activities are growing in Smart Campus, IoT, End-to-End Trust & Security, Big Data & Analytics, Smart Grid.

ASU Arizona State University Smart Campus operations & data analytics research	Colorado State University Advanced Networking / Cybersecurity Research	Lehigh University Smart Grid research	NC State University Smart Grid research network testbed
The University of Wisconsin Madison; Marshall University IoT Lab for Research and Pedagogy	Stanford University Smart transportation / IoT ethics research	Rensselaer Smart Grid research	Texas A&M Smart Grid research and data sharing
Princeton University IoT Security, Privacy & Ethics	UMBC An Honors University in Maryland Trust, Identity, Protection, Privacy, Safety, Security	University of Washington IoT Systems Risk Management & Security	VirginiaTech Smart Campus operations, trust and security

Grey - IoT research and pedagogy
Red - IoT Smart grid research
Blue - IoT security, privacy, ethics

February 2017 Microsoft Campus Connections Summit identified initiatives to further the Smart Campus journey.

- **Student Success & Data Analytics**
  - The Agile University
  - Global Talent Profile
  - MentorBot Personal Tutor for Student Success
- **Safety & Security**
  - Cybersecurity Learning Hub
  - Digital Literacy
- **Energy & Sustainability**
  - Campus as a Living Lab Breaking Cultural Barriers
  - Achieving Carbon Neutrality SCOPE ME
- **Collaborative Research**
  - Research Portal “1 Portal for All”

The Agile University

Cybersecurity Learning Hub

IoT Lab Contest

Research Portal

SMART CAMPUS: IOT SYSTEMS RISK MANAGEMENT TASK FORCE UPDATE

CHUCK BENSON
University of Washington

JAN CHEETHAM
University of Wisconsin-Madison

Internet2 IoT Systems Risk Management Task Force 2016-2017 Outcomes

Internet2 IoT Systems Risk Management Task Force
2016-2017 Outcomes

- Explore notion of ***a lifecycle of IoT Systems risk & operational management*** in Higher Ed institutions

- **Develop 2 tools/practices as starting place**:
  - HE practice of using Shodan and Censys tools to develop IoT Systems risk exposure for an HE institution
  - IoT Systems Vendor Management document/checklist to guide multiple departments/orgs within an HE institution on selection, procurement, management of IoT Systems

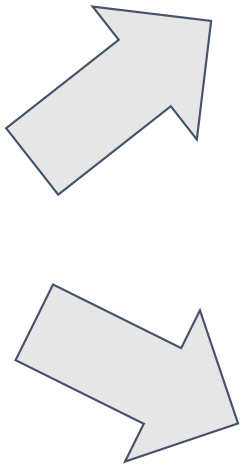
- Identify potential for future work

- Identify & share other resources

Developing an IoT Systems Risk Mitigation Life Cycle

pre-IoT Systems Implementation --
Risk Mitigation

IoT Systems Vendor Management Guidance Document
-- questions to guide purchaser/future owner of IoT Systems



post-IoT Systems Implementation --
Operational Risk Management

Institutional leadership, policy, oversight, resourcing for known systems

post-IoT Systems Implementation --
Cybersec Risk Management/Mitigation

Shodan/Censys/Other tools?
- Systems identification (there can be surprises)
- Risk mitigation

Jan Cheetham
Research Cyberinfrastructure Liaison
Office of the CIO
University of Wisconsin-Madison

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

IoT research initiatives

Internet of Things
SYSTEMS RESEARCH CENTER
UNIVERSITY OF WISCONSIN–MADISON

CloudLab

WiNEST

Template for a model wireless city

Arizona State University · CWU · Clemson · HEAnet · Indiana University · Princeton University · Texas A&M University · University of Michigan · Nebraska · University of Pittsburgh · University of Washington · University of Wisconsin–Madison · VirginiaTech · WICHE Western Interstate Commission for Higher Education · Yale

IoT Vulnerabilities: DDoS attacks

Mirai, BASHLITE, and evolving malware

OVH

9/18/16
1.1 Tbps

krebsonsecurity.com

9/20/16
620 Gbps

DVRs, CCTV cameras, home routers

ORACLE + Dyn

10/21/16
1.2 Tbps

Un-named US University
Late 2016

Campus vending machines, light sensors, refrigerators

Arizona State University · CWU · HEAnet · Indiana University · Princeton University · Texas A&M University · University of Michigan · University of Nebraska · University of Pittsburgh · University of Washington · University of Wisconsin-Madison · VirginiaTech · WICHE Western Interstate Commission for Higher Education · Yale

IoT Vulnerabilities: Industrial control systems

2008
Turkish oil pipeline

BBC News

2014
German blast furnace

Industrial Control & Critical Infrastructure in Higher Ed

Utility distribution

Building/Room environment control (HVAC)

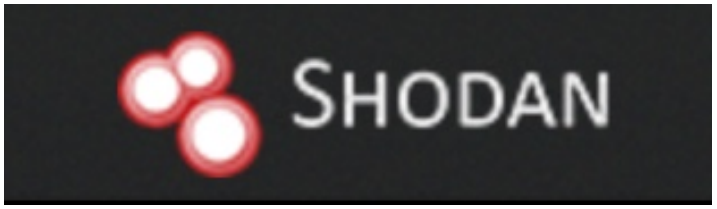
We also care about these:

Research Systems

Building, Internal Space, Animal Facility, BSL3 Access

And others …

Taskforce benchmarking activity

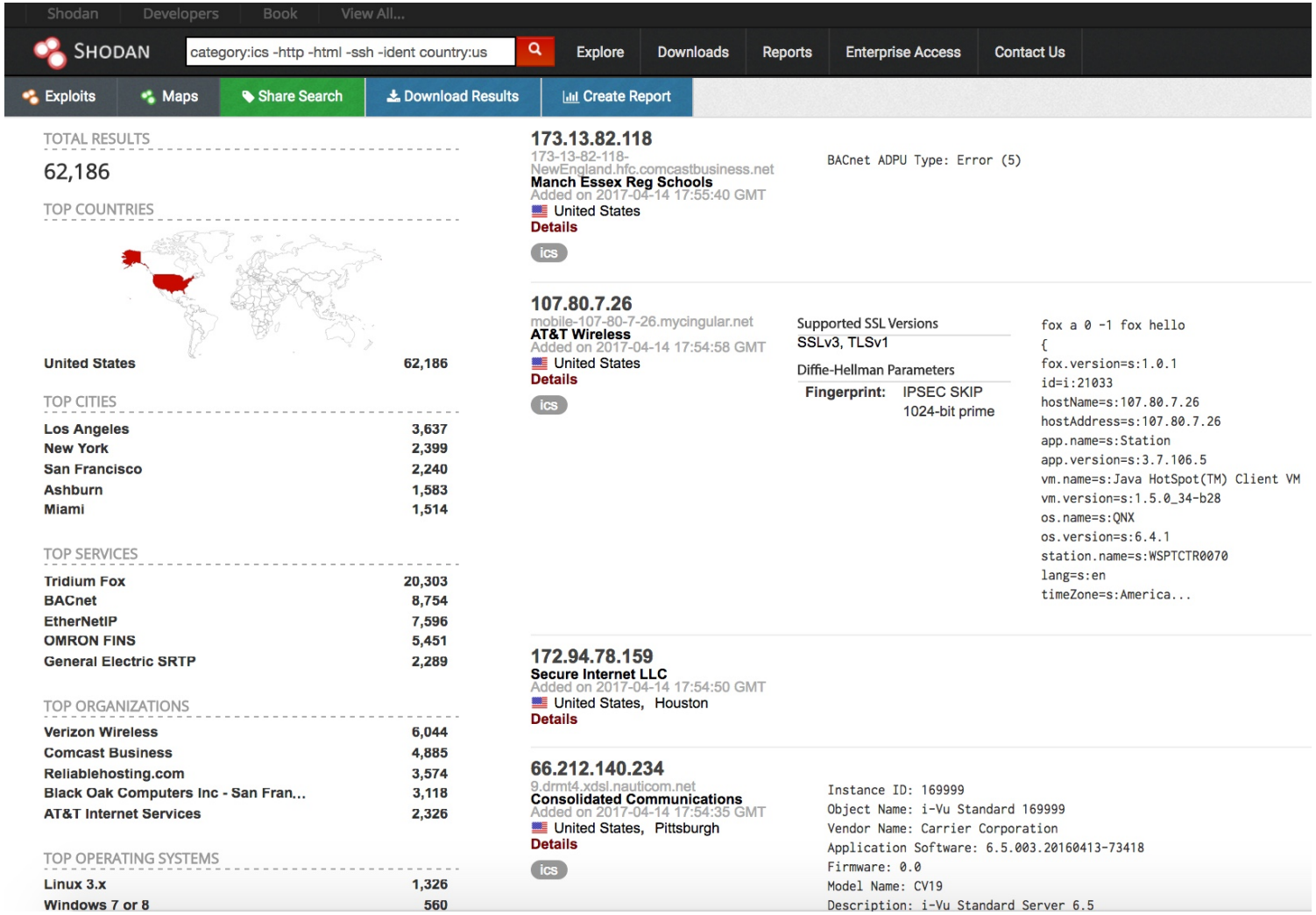


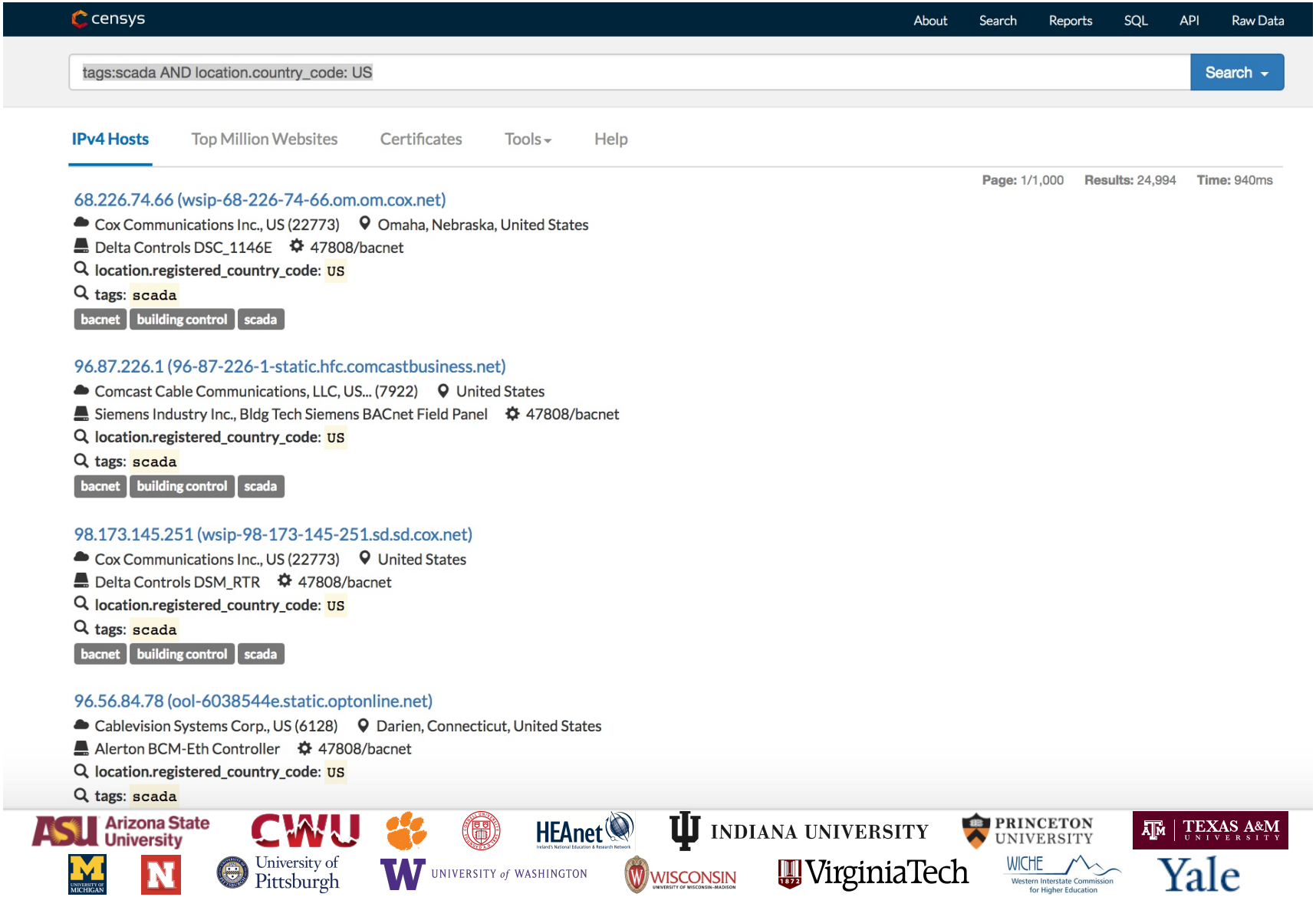
- Proprietary
- Developed by former UCSD student
- Used by private sector and academia

- Open source
- Developed at Univ of Michigan/Illinois
- Daily ZMap and ZGrab scans of IPv4 address space across important ports and protocols

Both do full text searching on protocol banners and other metadata on websites, servers, devices

WARNING: Consult your CISO office before using! Prior notice and authorization may be required.


Shodan
Developers
Book
View All...
SHODAN
category:ics -http -html -ssh -ident country:us
Explore
Downloads
Reports
Enterprise Access
Contact Us
Exploits
Maps
Share Search
Download Results
Create Report
TOTAL RESULTS
62,186
TOP COUNTRIES
United States 62,186
TOP CITIES
Los Angeles 3,637
New York 2,399
San Francisco 2,240
Ashburn 1,583
Miami 1,514
TOP SERVICES
Tridium Fox 20,303
BACnet 8,754
EtherNetIP 7,596
OMRON FINS 5,451
General Electric SRTP 2,289
TOP ORGANIZATIONS
Verizon Wireless 6,044
Comcast Business 4,885
Reliablehosting.com 3,574
Black Oak Computers Inc - San Fran... 3,118
AT&T Internet Services 2,326
TOP OPERATING SYSTEMS
Linux 3.x 1,326
Windows 7 or 8 560
173.13.82.118
173-13-82-118-NewEngland.hfc.comcastbusiness.net
Manch Essex Reg Schools
Added on 2017-04-14 17:55:40 GMT
United States
Details
ics
BACnet ADPU Type: Error (5)
107.80.7.26
mobile-107-80-7-26.mycingular.net
AT&T Wireless
Added on 2017-04-14 17:54:58 GMT
United States
Details
ics
Supported SSL Versions
SSLv3, TLSv1
Diffie-Hellman Parameters
Fingerprint: IPSEC SKIP 1024-bit prime
fox a 0 -1 fox hello
{
fox.version=s:1.0.1
id=i:21033
hostName=s:107.80.7.26
hostAddress=s:107.80.7.26
app.name=s:Station
app.version=s:3.7.106.5
vm.name=s:Java HotSpot(TM) Client VM
vm.version=s:1.5.0_34-b28
os.name=s:QNX
os.version=s:6.4.1
station.name=s:WSPTCTR0070
lang=s:en
timeZone=s:America...
172.94.78.159
Secure Internet LLC
Added on 2017-04-14 17:54:50 GMT
United States, Houston
Details
66.212.140.234
9.drmt4.xdsl.nauticom.net
Consolidated Communications
Added on 2017-04-14 17:54:35 GMT
United States, Pittsburgh
Details
ics
Instance ID: 169999
Object Name: i-Vu Standard 169999
Vendor Name: Carrier Corporation
Application Software: 6.5.003.20160413-73418
Firmware: 0.0
Model Name: CV19
Description: i-Vu Standard Server 6.5


censys
About
Search
Reports
SQL
API
Raw Data
tags:scada AND location.country_code: US
Search
IPv4 Hosts
Top Million Websites
Certificates
Tools
Help
Page: 1/1,000
Results: 24,994
Time: 940ms
68.226.74.66 (wsip-68-226-74-66.om.om.cox.net)
Cox Communications Inc., US (22773)
Omaha, Nebraska, United States
Delta Controls DSC_1146E
47808/bacnet
location.registered_country_code: US
tags: scada
bacnet
building control
scada
96.87.226.1 (96-87-226-1-static.hfc.comcastbusiness.net)
Comcast Cable Communications, LLC, US... (7922)
United States
Siemens Industry Inc., Bldg Tech Siemens BACnet Field Panel
47808/bacnet
location.registered_country_code: US
tags: scada
bacnet
building control
scada
98.173.145.251 (wsip-98-173-145-251.sd.sd.cox.net)
Cox Communications Inc., US (22773)
United States
Delta Controls DSM_RTR
47808/bacnet
location.registered_country_code: US
tags: scada
bacnet
building control
scada
96.56.84.78 (ool-6038544e.static.optonline.net)
Cablevision Systems Corp., US (6128)
Darien, Connecticut, United States
Alerton BCM-Eth Controller
47808/bacnet
location.registered_country_code: US
tags: scada

What we found

	Cameras	Building Automation	Sensors
		 device servers  ICS/SCADA	
Search terms	”camera”	”scada,” “ICS,” “HVAC,” “Tridium Fox,” “BACnet,” “Modbus”	”AMQP” “RabbitMQ” “MQTT”
Potential Risk	Weak, hard-coded passwords	Components of building control systems exposed on Internet, protocols lacking authentication, encryption	Complex, layered systems with physical security issues, protocols lacking authentication

May be others

Other types of devices we didn't search for

- Vending machines
- Refrigerators
- Health care monitors

Image sources: MegaLab, AlerSense, UAI Vending

Brief background

Chuck Benson

Facilities Services IT, UW
Drone policy working group, UW
Chair Internet2 IoT Systems Risk Management Task Force
Former Chair UW-IT Service Management Board, UW
Former Chair Protection of Industrial Controls (PICS) Task Force

Chair Internet2 IoT Systems Risk Management Task Force

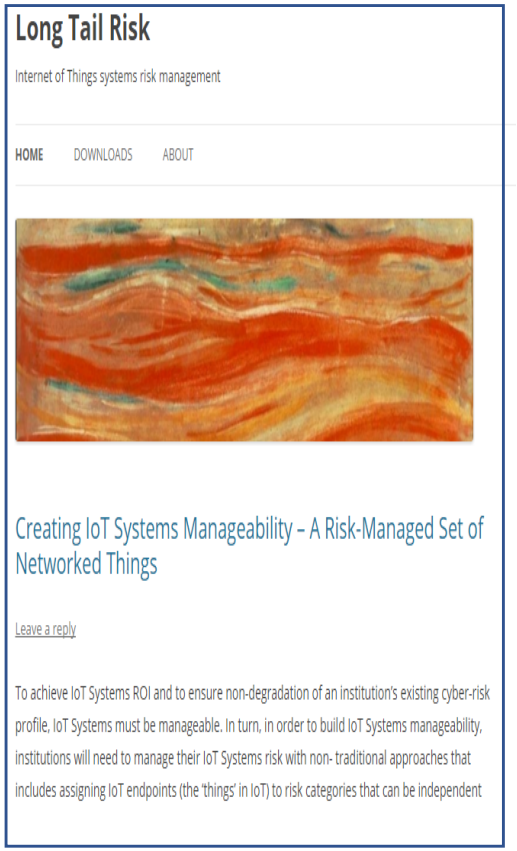
Why IT Matters to Higher Education
EDUCAUSEreview

Articles June & July 2016 –

"Internet of Things, IoT Systems, and Higher Education" &
"Raising Expectations for IoT Systems Vendors"

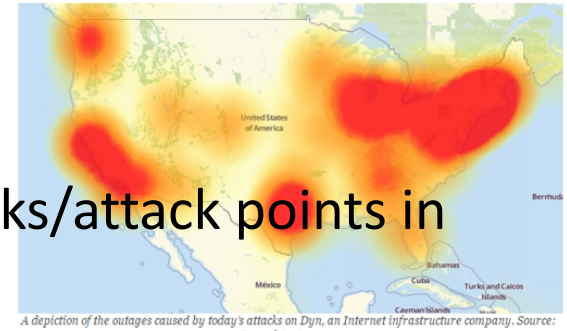
King's College London
Book Chapter on Smart Cities – part of Systems Science/Systems Thinking Series

"IoT Systems – Systems Seams & Systems Socialization – Considerations for Managing IoT Systems Risk in Smart Cities and Institutions"



(and the obligatory twitter feed -- @cabenson361)

IoT Systems Vendor Management Document

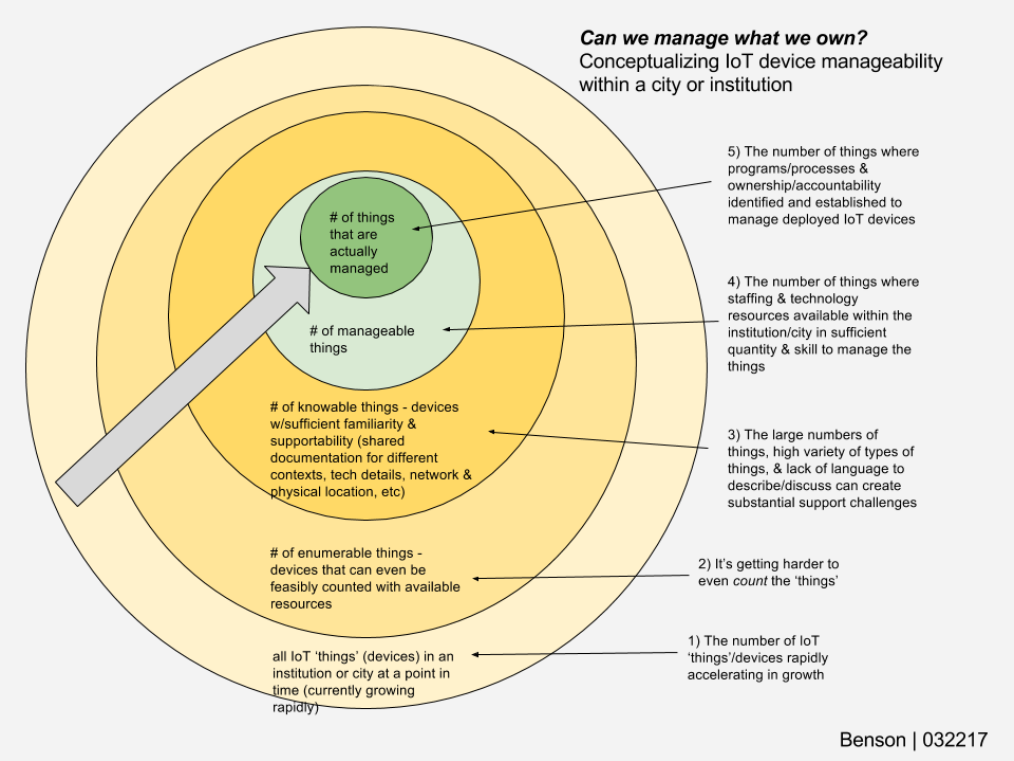


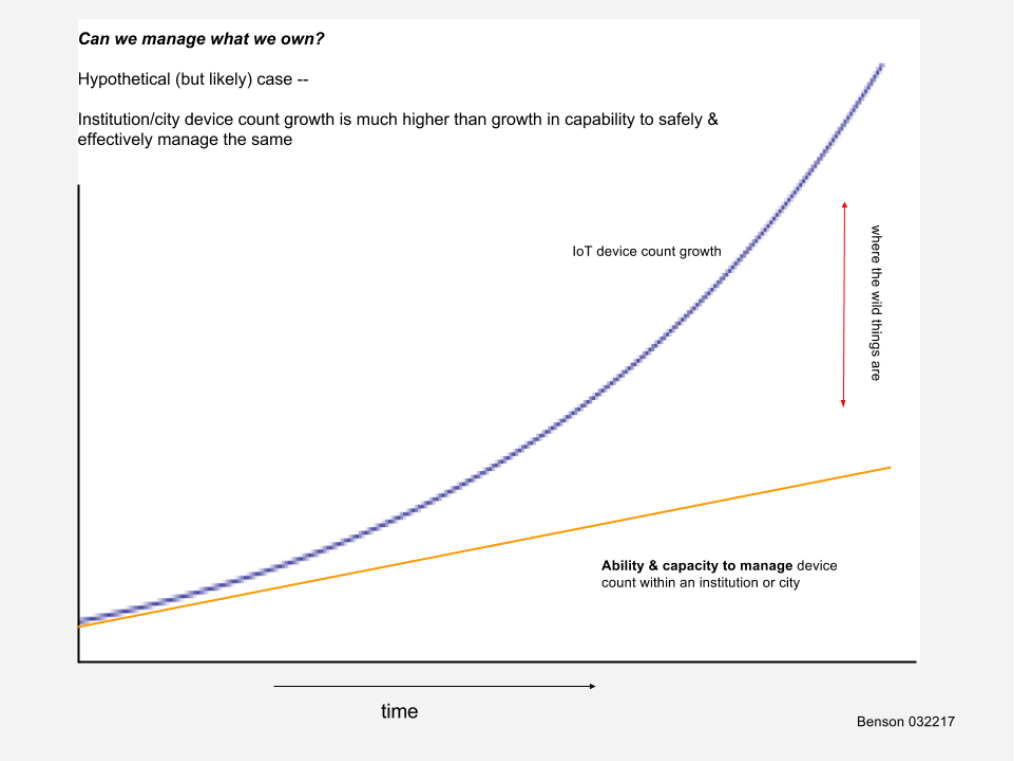
A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

- Shodan, Censys, and non-published tools reveal cracks/attack points in our institutions
  - Creating potentially substantial additional risk
- We can lower that risk
  - By raising the bar & setting expectations of the IoT Systems vendor
  - RFI, RFP, contract negotiation, & relationship management phases with the vendor

ASU Arizona State University · CWU · Clemson · HEAnet · INDIANA UNIVERSITY · PRINCETON UNIVERSITY · TEXAS A&M UNIVERSITY · University of Michigan · Nebraska · University of Pittsburgh · UNIVERSITY of WASHINGTON · WISCONSIN · VirginiaTech · WICHE Western Interstate Commission for Higher Education · Yale

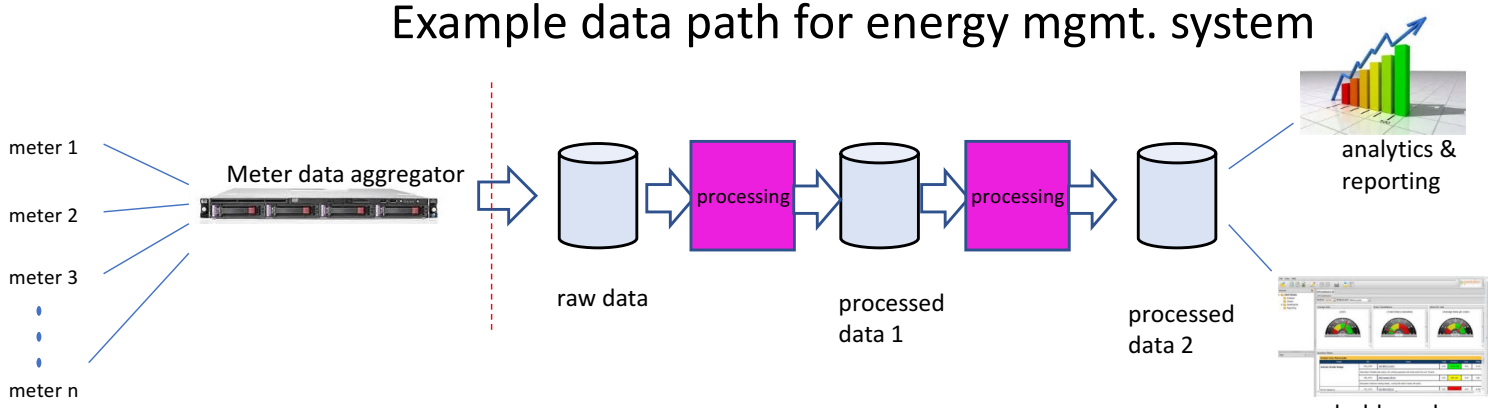
Can we manage what we own?





And the IoT System is deployed in a system of human & technical systems …

Example data path for energy mgmt. system



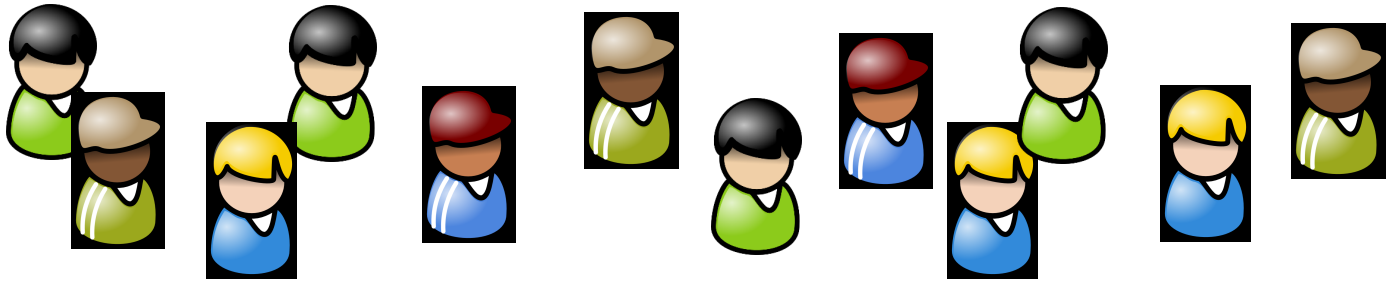
Technical infrastructure

Existing IT/Info Mgmt Infrastructure (e.g., physical network & physical implementation points)

Organizational structure

Central IT | Distributed IT | Facilities Mgmt | Institution Leadership | Acad/Admin Dept 1 | Acad/Admin Dept n | Vendor 1 | Vendor n

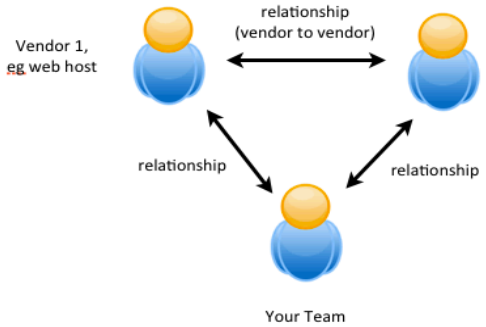
People – with roles, expectations, patterns, routines, opinions



Arizona State University · CWU · Clemson · HEAnet · Indiana University · Princeton University · Texas A&M University · University of Michigan · Nebraska · University of Pittsburgh · University of Washington · Wisconsin · VirginiaTech · WICHE Western Interstate Commission for Higher Education · Yale

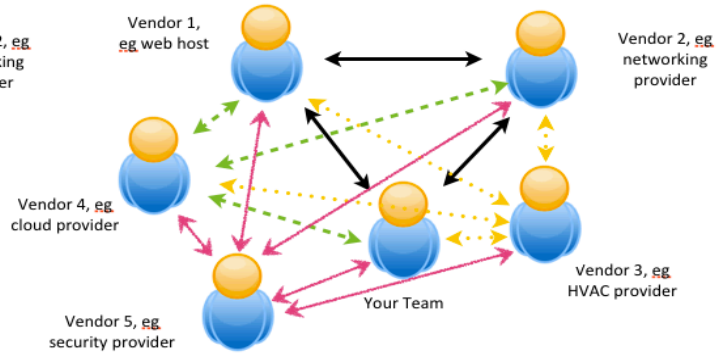
Increasing vendor/system count increases systems complexity & management overhead

the old days
-- smaller number of providers --



# of endpoints	potential # of relationships requiring management
3	3
...	...

the new world
-- IoT innovation & growth increases vendor count & relationships requiring management --



# of endpoints	potential # of relationships requiring management
3	3
4	6
5	10
6	15
7	21
...	...

Note: addition of a *single* endpoint later in the series creates *many* more relationships to be managed. This is the part that can sneak up on us. (Same reason why growing committee size gets unwieldy).

ChuckBenson@longtailrisk.com | 051415

Vendor management complexity grows rapidly with #IoT systems @cabenson361 #risk #i2summit17

IoT Systems Vendor Management Document

- Acknowledge that:
  - IoT Systems increasingly ***entering institution in non-traditional ways***
    - e.g., not central IT – but end-users/PI's, facilities, capital planning, planning/budgeting
  - IoT Systems are ***deployed in non-traditional ways***
    - These are not traditional enterprise systems
    - Often not with central IT
    - Often with vendor-heavy influence
  - Generally, ***limited vetting for IoT Systems***
    - Many, most? of these systems will not be managed by central IT

- IoT Systems Vendor Management Doc
  - Designed to assist:
    - selection
    - RFI
    - RFP
    - contraction negotiation
    - systems management

  - Doc needs broad utility & consumability -- Needs to be readable or 'parseable' by organizations fulfilling multiple different roles – not just IT

IoT Systems Vendor Management Document

-- example items --

operational risks (eg resourcing & planning)

- ❑ Does vendor need 1 (or more) data feeds/data sharing from your organization?
  - ❑ Are the data feeds well-defined?
  - ❑ Do they exist already?
    - ❑ If not, who will create & support them
- ❑ Who pays for vendor systems requirements (eg hardware, supporting software, networking, etc?)
  - ❑ Does local support (FTE) exist? Is it available? Will it remain available?
  - ❑ If hosted in a data center, who pays for those costs?
  - ❑ If cloud-hosted, eg AWS, who pays for those costs?
  - ❑ Above questions answered for both implementation & long term support?
- ❑ What is total operational cost after installation?
  - ❑ Licensing
  - ❑ Support contracts
  - ❑ Hosting requirements
  - ❑ Business resilience requirements (eg redundancy, recovery, etc for OS, db, other)
- ❑ Can IoT system vendor maintenance contract offset local IT support shortages?
  - ❑ for 10's, 100's, 1000's of new endpoints ?

cybersec (bad guy) risks

- ❑ Is there a commissioning plan? Or have installation expectations otherwise been stated?
  - ❑ Default logins & passwords changed & recorded?
  - ❑ Non-required default ports closed?
  - ❑ Devices port scanned (or similar) after installation
- ❑ For remote support, how does vendor safeguard login/account information?
  - ❑ Is it in contract?
- ❑ Who, in your organization, will manage the IoT system vendor contract?
  - ❑ Central IT?
  - ❑ Facilities?
  - ❑ Tenant/customer dept ?
  - ❑ Other? PD/security? CISO? CSO?

both

- ❑ How many endpoint devices will be installed?
  - ❑ Is there a patch plan? Who manages this?
- ❑ How many IoT systems are you already managing?
  - ❑ Are you anticipating more in next 18 months?
- ❑ Is the IoT vendor system implementation documented?
  - ❑ Architecture diagram ?
    - ❑ w/IP addresses & physical location of devices?
    - ❑ w/required ports documented
- ❑ Does this vendor's system have dependencies on other systems?
- ❑ Is a risk sharing agreement in place for shared institutional information?

Many other resources (some longer to read than others)

- NIST Cybersecurity for IoT Program
  - https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
- FTC & IoT Privacy
  - https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
- Industrial Internet of Things Security Framework
  - http://www.iiconsortium.org/IISF.htm
- GSMA IoT Security Guidelines
  - http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
- OWASP IoT Security Guidance
  - https://www.owasp.org/index.php/IoT_Security_Guidance
- DHS Strategic Principles for Securing the Internet of Things
  - https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
- Others …

Possible future work in area

- IoT Systems Costing
  - Few, if any, institutions have a handle on this
- Network segment portfolio strategies
  - Segmentation is all the rage, but how are those segmentation portfolios managed
- Internal ICS & IoT exposure
  - Shodan/Censys do public addresses
    - Internal VLAN's, VRF's, etc not covered
- Benchmark/standard for exposure in HE

Questions/Comments?

TRUST, IDENTITY, PRIVACY, PROTECTION, SAFETY & SECURITY (TIPPSS) FOR IOT: ITANA COLLABORATION AND WHITE PAPER

KEN KLINGENSTEIN
Internet2

ED ARACTINGI
Marshall University

Enterprise Managed IoT

Enterprise Managed IoT: Topics

- ITANA and I2 T&I + CINO
- Distinctive R&E Use cases
- A Layered View of IoT
- An Overlayered View of Enterprise Managed IoT
- What we might do

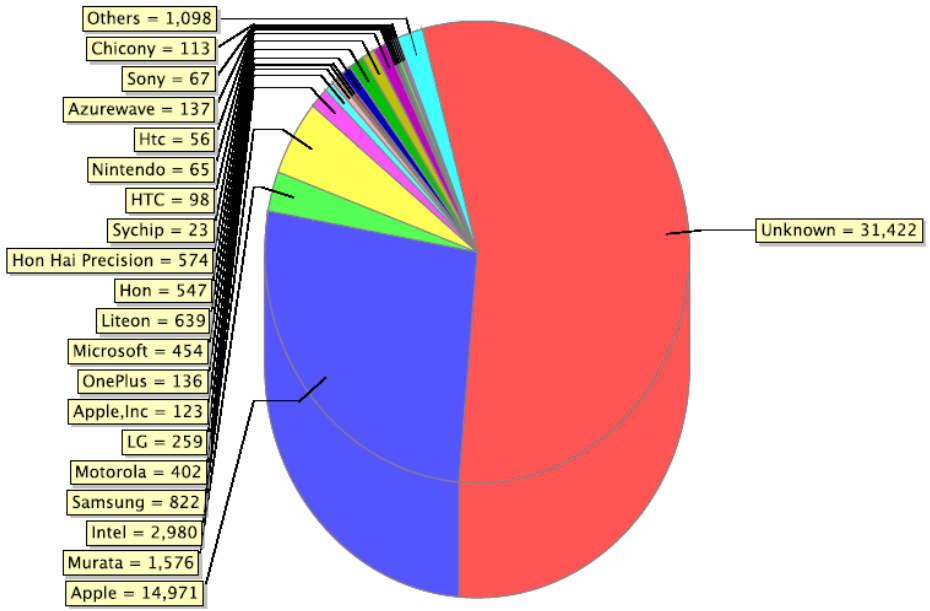
ITANA, T&I, CINO

- ITANA – A group of enterprise architects, supported by Internet2 and Educause
- Trust and Identity – the division of Internet2 that does federation and enterprise middleware software
  - InCommon
  - TIER
- CINO – Chief Innovation Office – A catalytic agent for innovation within Internet2

Distinctive R&E IoT Considerations

- Supporting the researchers in CS and Engineering
- Supporting the applied researchers in Medical Schools
- Decentralized purchasing
- Transient populations of students and faculty
- Distinctive privacy requirements
- 20,000 entrepreneurs whose only concern about the institution is parking

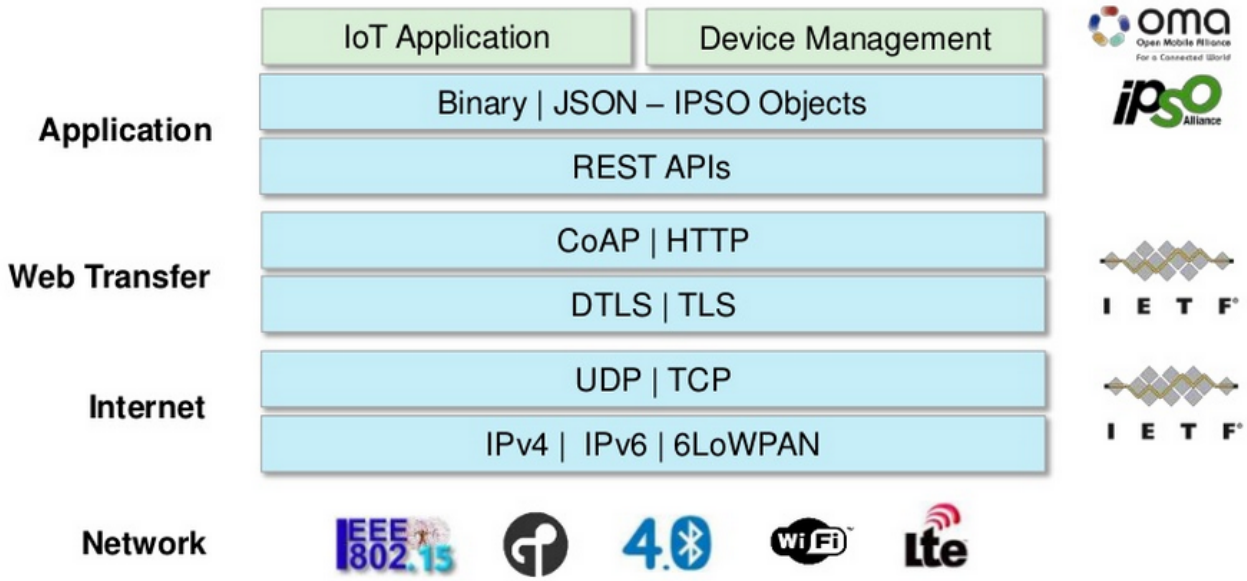
Distinctive – What's on Your Network



Unknown = 31,422 Apple = 14,971 Murata = 1,576 Intel = 2,980 Samsung = 822 Motorola = 402 LG = 259
Apple,Inc = 123 OnePlus = 136 Microsoft = 454 Liteon = 639 Hon = 547 Hon Hai Precision = 574 Sychip = 23
HTC = 98 Nintendo = 65 Htc = 56 Azurewave = 137 Sony = 67 Chicony = 113 Others = 1,098

One Layered View

Remember the I in IoT!



28

ARM

Another Layered View

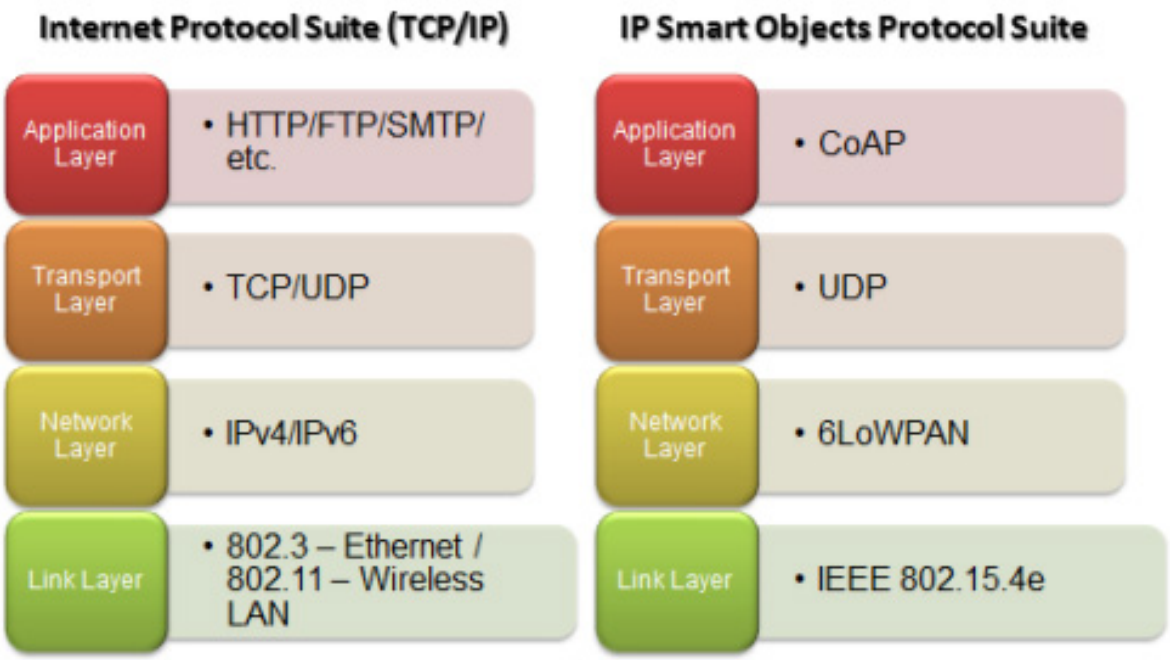
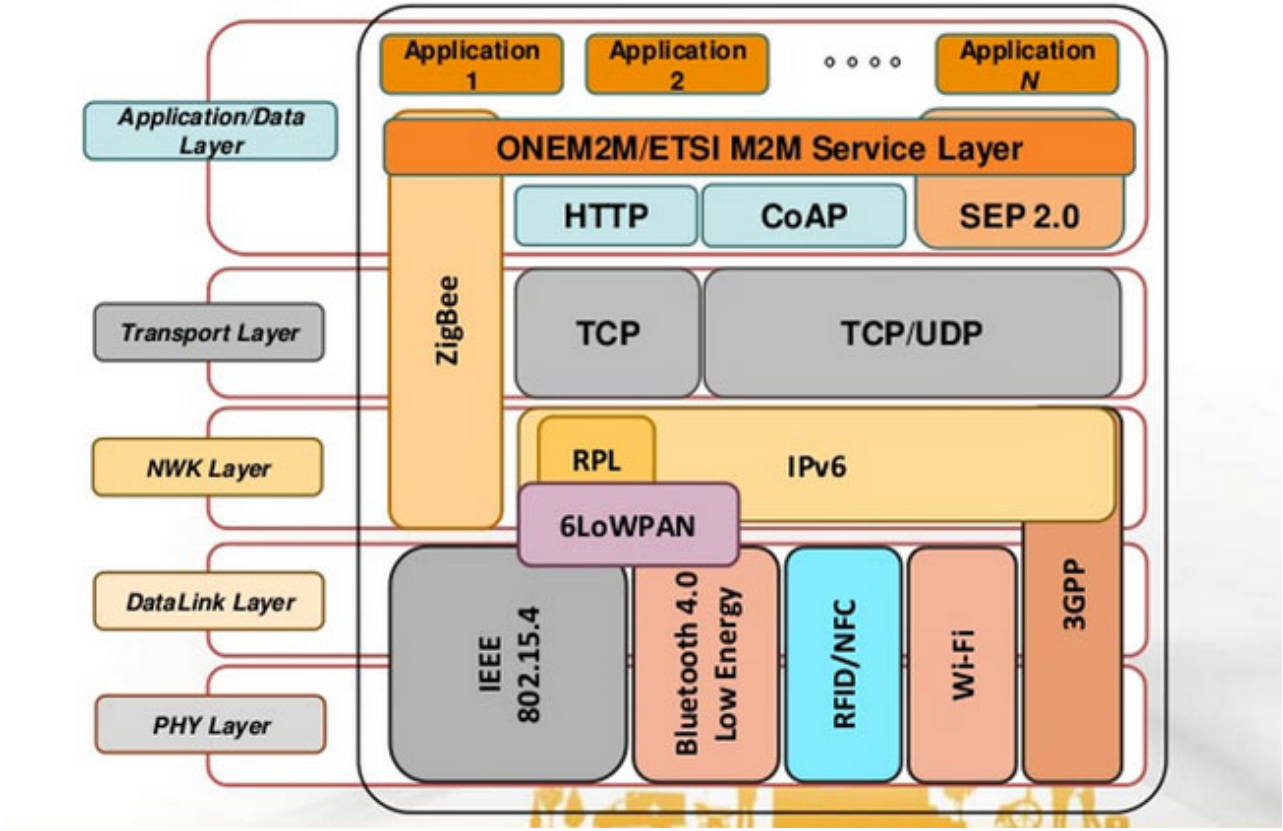


Figure 1 TCP/IP Stack and IP Smart Objects Protocol Stack

And this


Application 1
Application 2
Application N
Application/Data Layer
ONEM2M/ETSI M2M Service Layer
HTTP
CoAP
SEP 2.0
ZigBee
Transport Layer
TCP
TCP/UDP
NWK Layer
RPL
IPv6
6LoWPAN
DataLink Layer
IEEE 802.15.4
Bluetooth 4.0 Low Energy
RFID/NFC
Wi-Fi
3GPP
PHY Layer

Where can the enterprise help manage IoT?

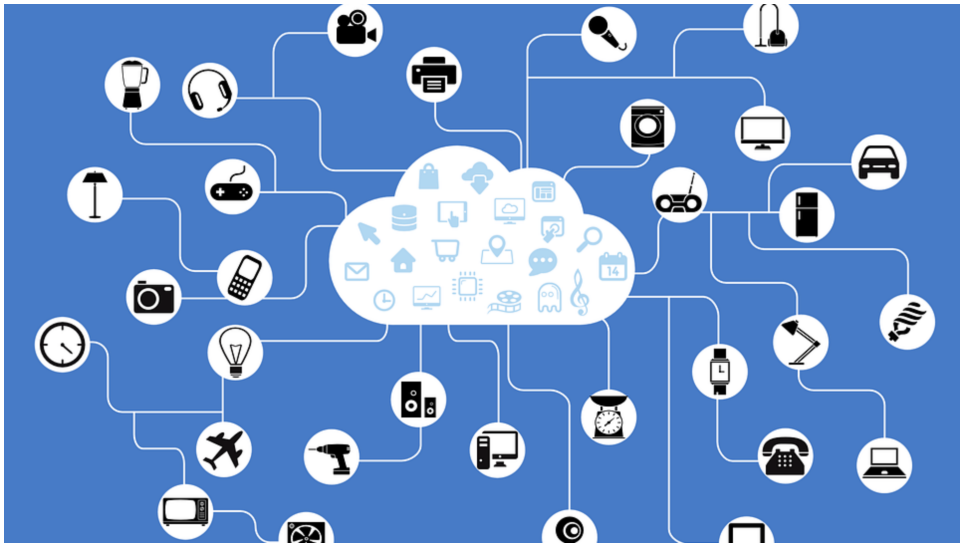
- Where and how to put management?
  - The IP network?
  - Data link layer controls?
  - REST API's
- Who does management?
  - Facilities
  - Campus IT
  - Purchasing
- What's the business model
  - Governance
  - Funding

Next Steps

- Enterprise-IoT will contribute some distinctive use cases to other CINO White Paper activities
- Will investigate several areas:
  - Registries – what's needed for things?
    - May feed into TIER activities
  - How do our central middleware concepts- authentication, authorization, delegation, etc. add value to IoT?
  - Is the work within IETF useful and ready?
    - CORE - Constrained RESTful Environments
    - ACE - Authentication and Authorization for Constrained Environments
- Lots of interest in checklists for vendors and purchasing

Campus IoT Whitepaper Topics

- Overview of IoT on Campus
- IoT in Pedagogy
- IoT in Research
- IoT in Administrative Areas
- IoT in Campus Facilities
- IoT in Campus Safety & Security
- IoT in Student Life
- IoT in Campus Health
- IoT in Campus Sports
- IoT in Campus Residential Communities
- IoT for Visitors and Public on Campus
- IoT for Recruitment and Alumni Relations
- IoT Interaction between Campuses and Business Partners
- Campus IoT Technical Considerations and Architectures



Participate in these IoT whitepaper efforts

Email CINO@Internet2.edu

INTERNET2 2017 global SUMMIT Washington DC April 23-26

SMART CAMPUS CYBERSECURITY TRANSITION TO PRACTICE RESEARCH

ARANYA CHAKRABORTTY
North Carolina State University

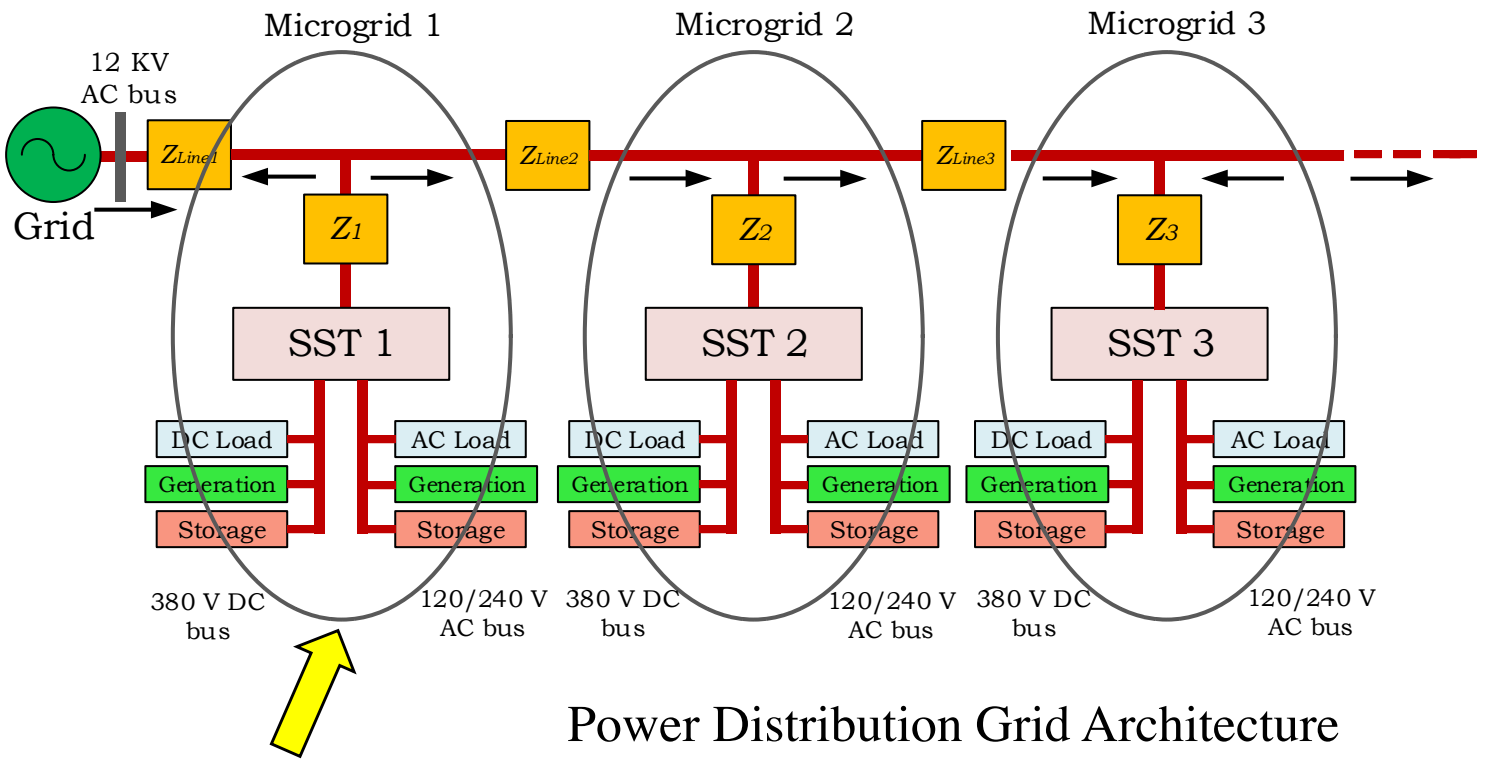
Cyber-Security Challenges for Power Distribution in Smart Campuses

Aranya Chakrabortty
North Carolina State University

Internet2 Global Summit

April 25, 2017, Washington DC

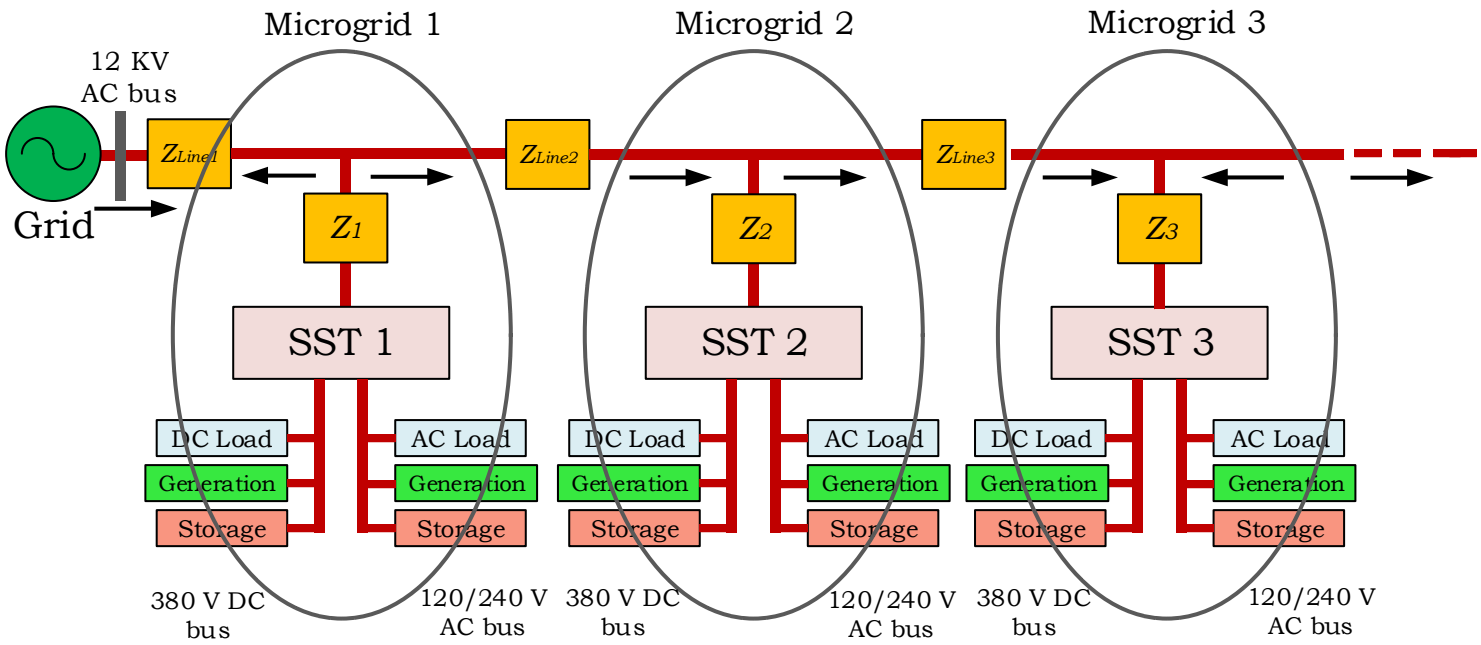
Why is Communication So Important for Controlling Power Systems?



Power Distribution Grid Architecture

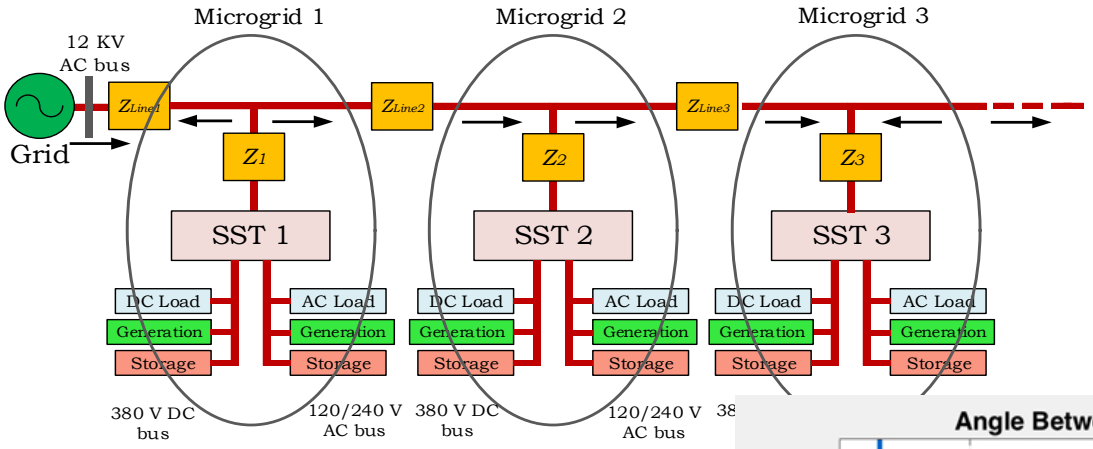
Can be a campus micro-grid

Why is Communication So Important for Controlling Power Systems?

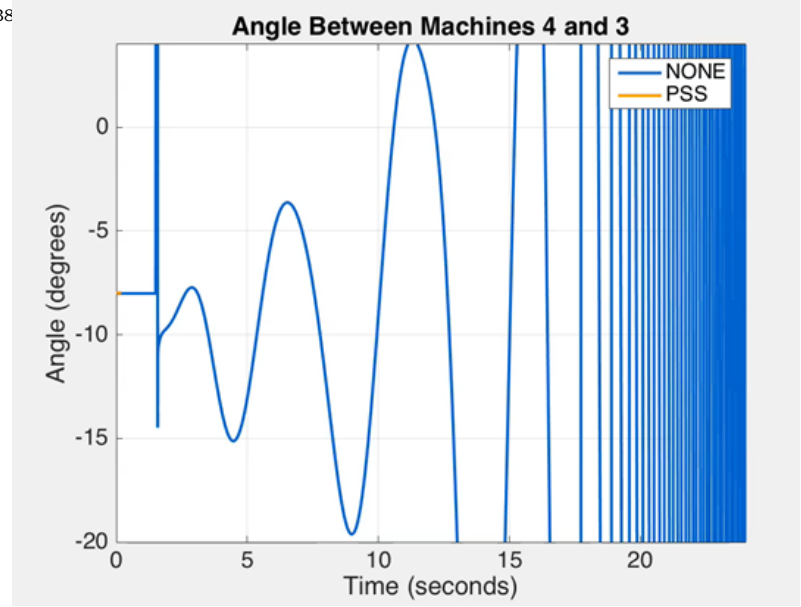


Companies and asset owners take control actions inside their regions agnostic of the health of other parts of the grid

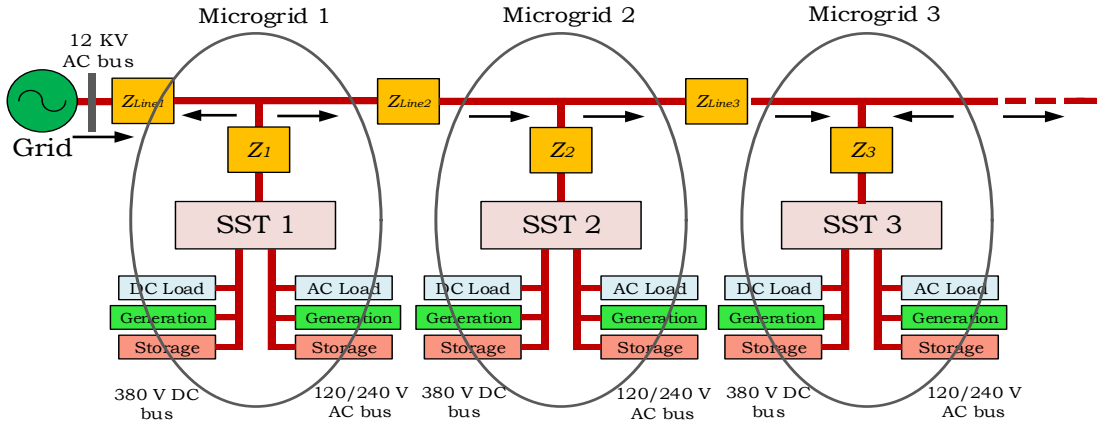
Why is Communication So Important for Controlling Power Systems?

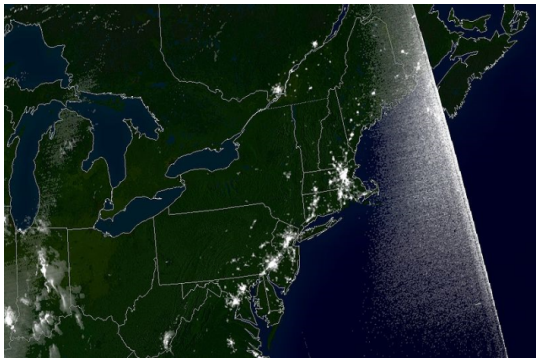


Agnostic local control actions can easily lead to instability



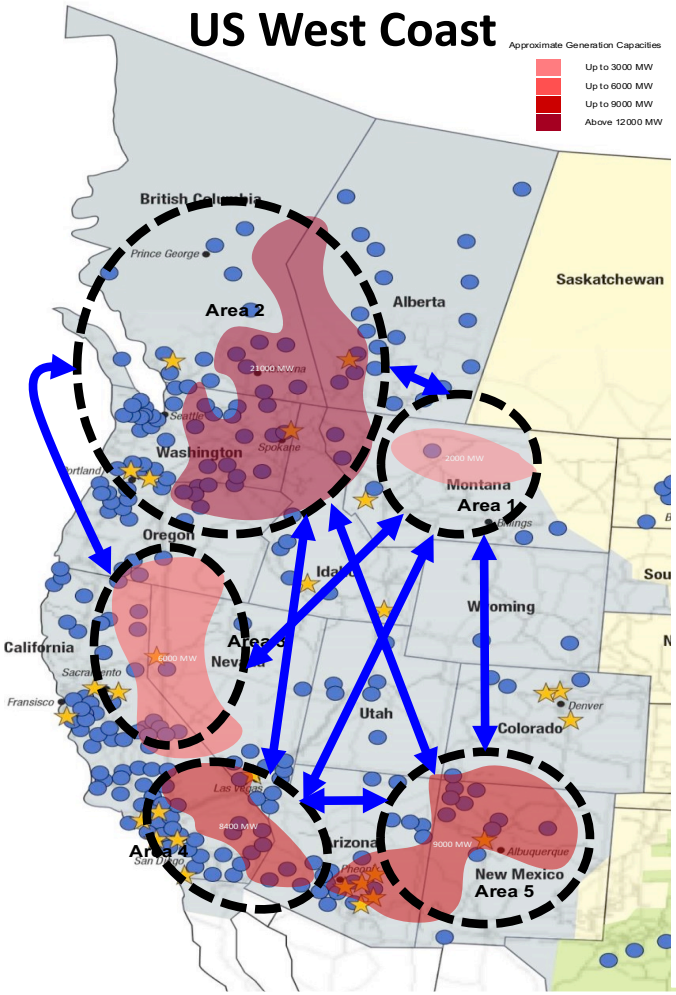
Why is Communication So Important for Controlling Power Systems?





2003 Northeast blackout

Why is Communication So Important for Controlling Power Systems?



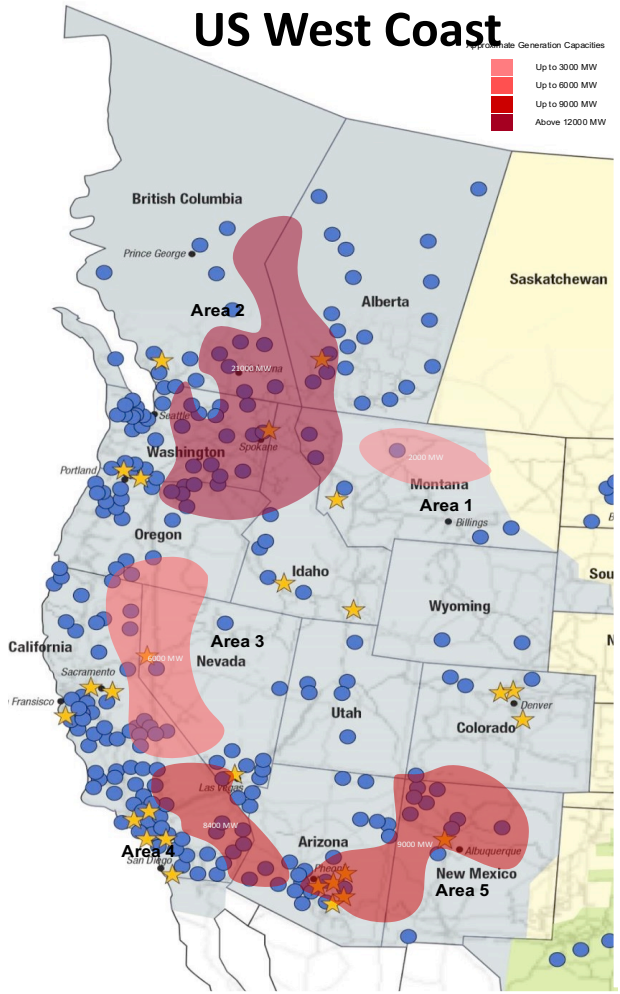
- Continuous status updates between the

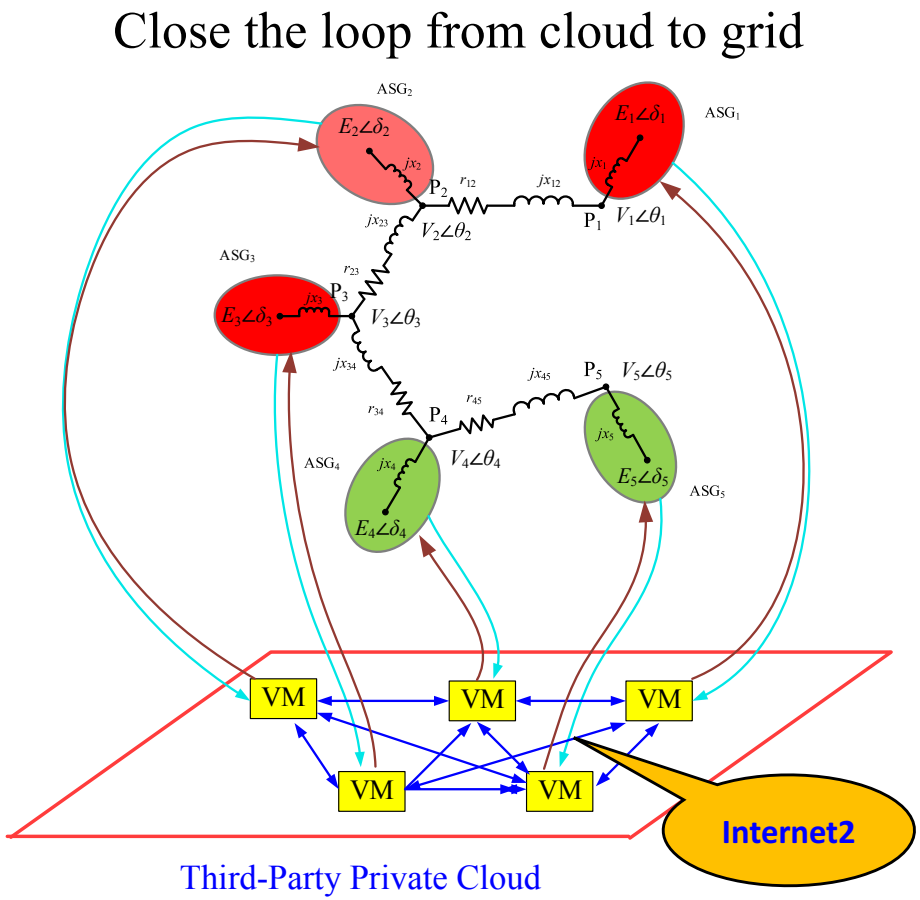
micro-grids are necessary

- Need a robust, secure, communication network

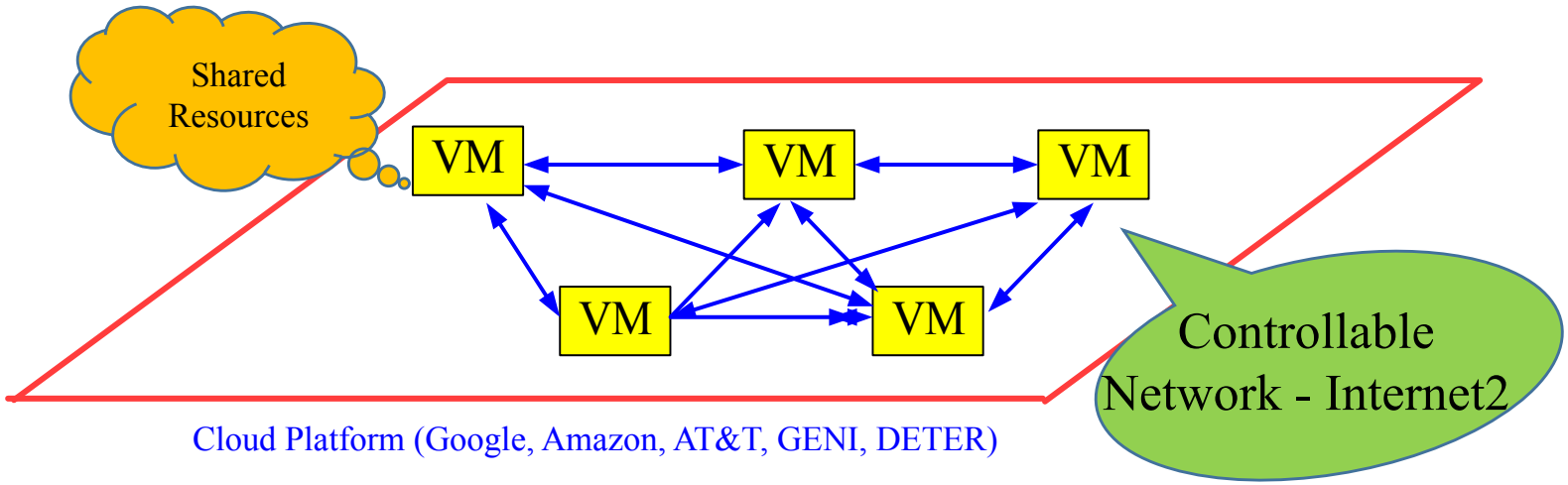
- SDN, cloud computing, Internet2

Balancing Regions are Sensitive to Data Privacy!





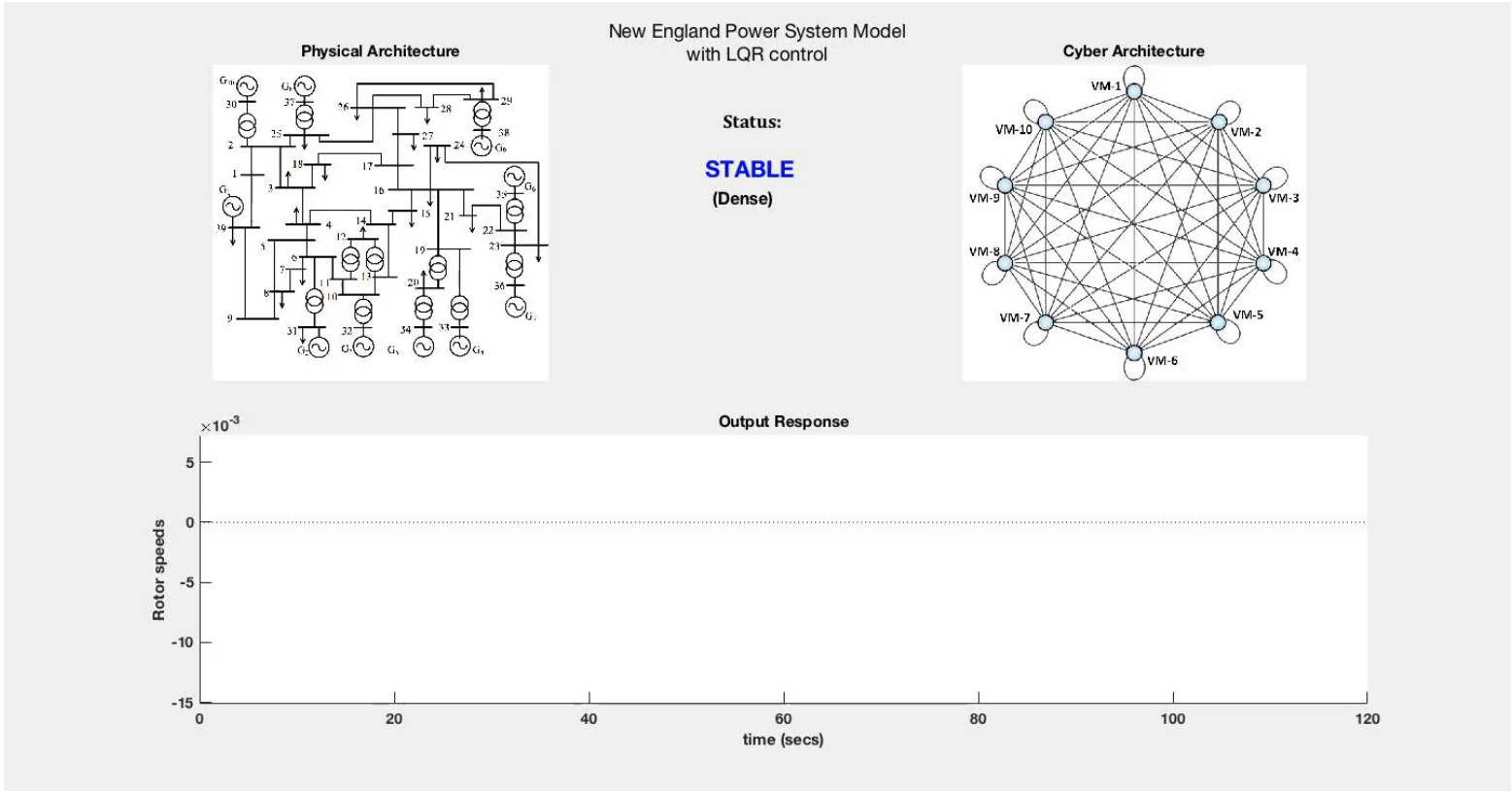
Interesting Things Going on in the Communication Plane



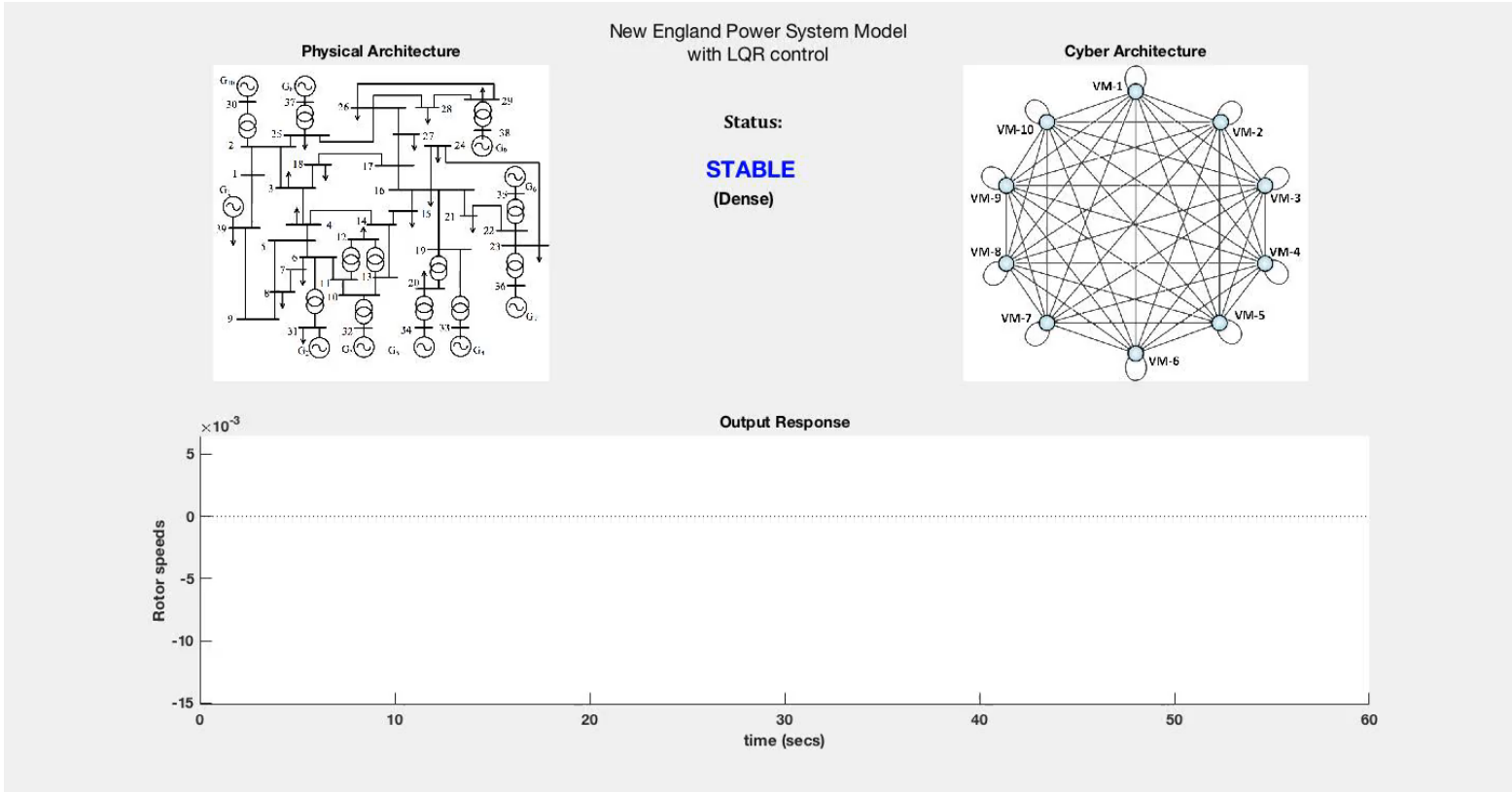
Different types of attacks:

1. Denial-of-Service
2. Data manipulation
3. GPS spoofing
4. Replay attacks

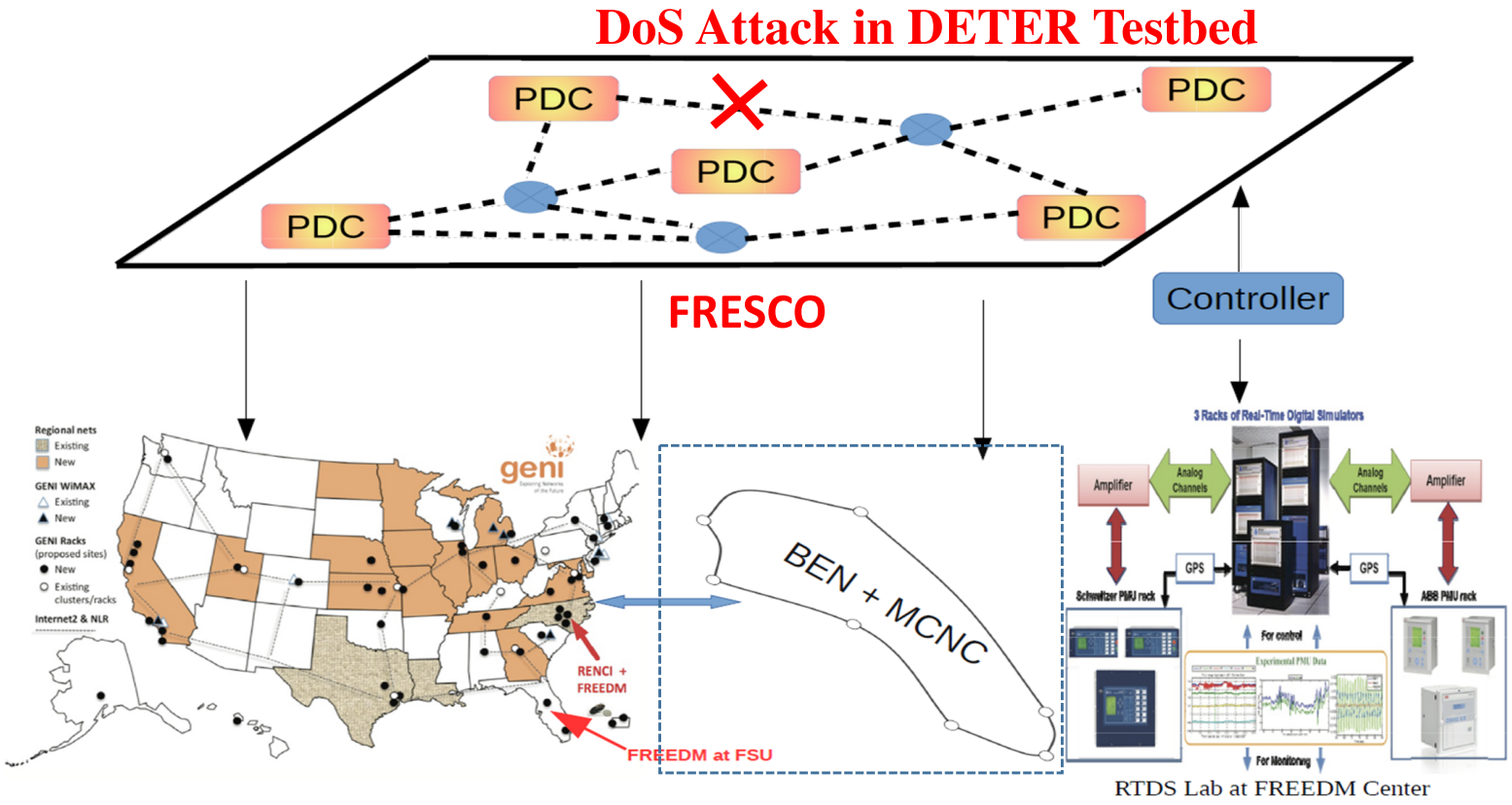
Denial-of-Service Attack



Denial-of-Service Attack



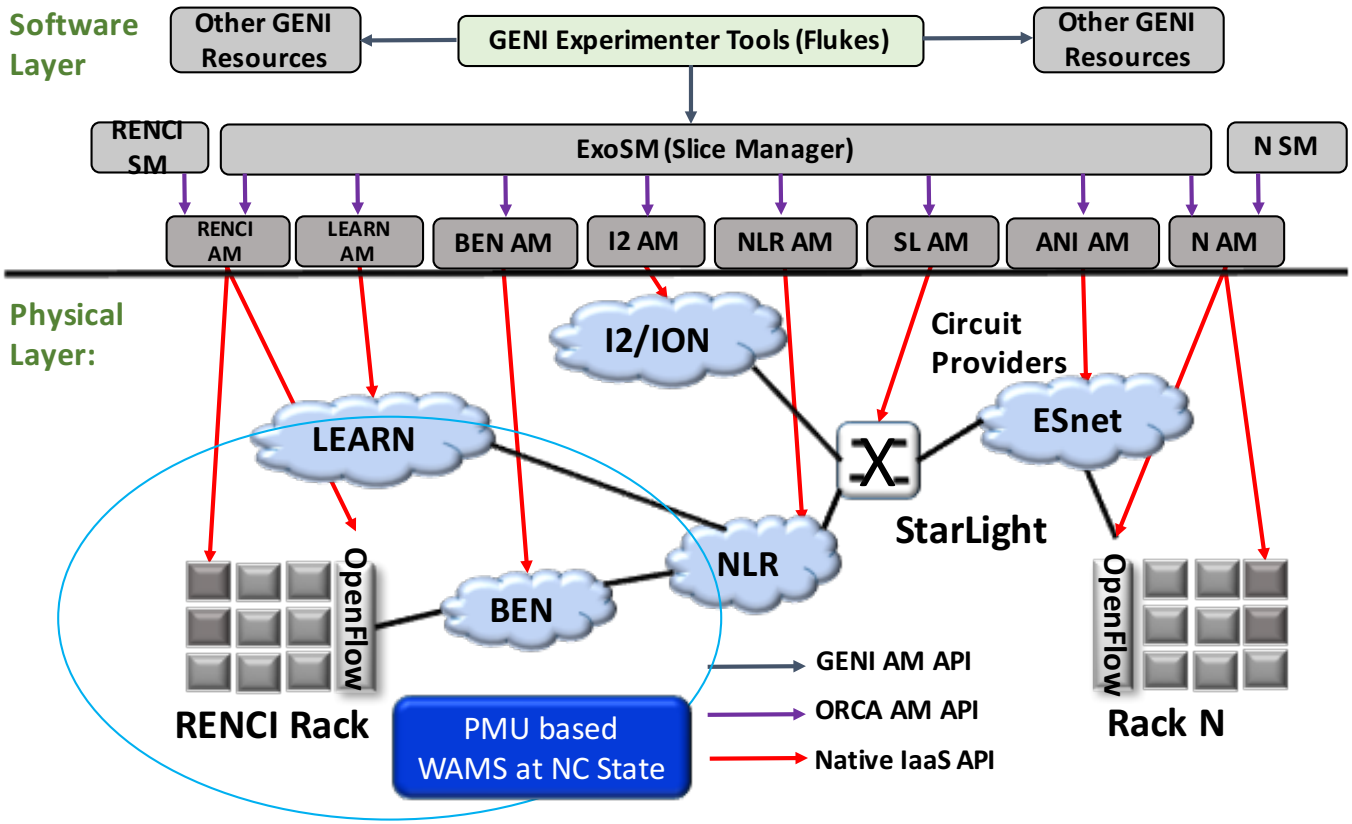
ExoGENI-DETER-WAMS Testbed at NC State



Middleware provided by Green Energy Corporation and RTI

Networked Cloud Computing Testbed - ExoGENI

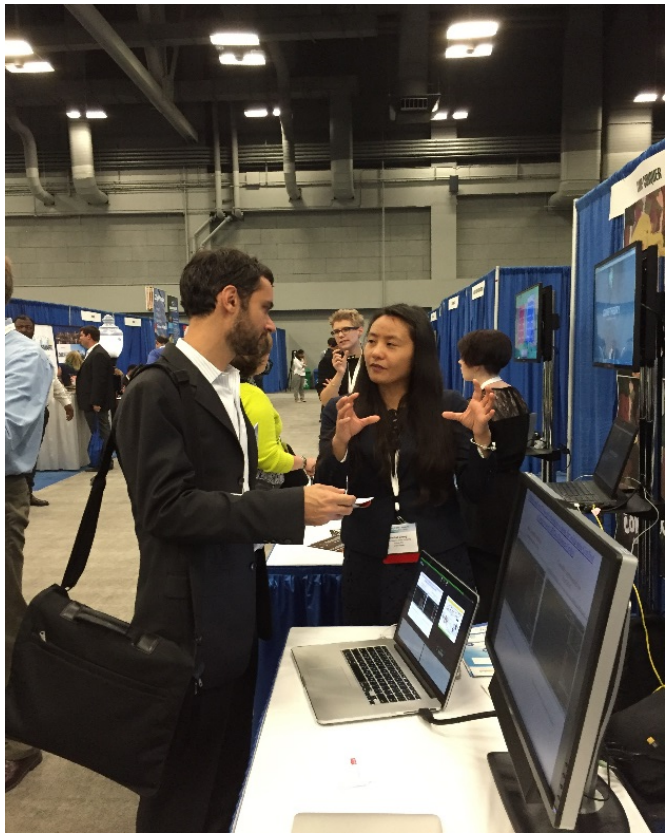
ExoGENI provides in virtual IaaS services for innovative research on distributed applications for Wide-Area Monitoring and Control (14 rack sites at universities & labs over the US)



Project Impacts:

DETER Demo at NIST & Smart-America 2014

Best Energy App Award at US Ignite 2015



US Ignite & NIST
Smart Cities Application
Summit, Austin, TX, 2016

Thank You

Email: achakra2@ncsu.edu

Website: http://people.engr.ncsu.edu/achakra2

INTERNET2 2017 global SUMMIT Washington DC April 23-26

SMART CAMPUS CYBERSECURITY TRANSITION TO PRACTICE RESEARCH

RAJU GOTTUMUKKALA
University of Louisiana-Lafayette

Cybersecurity Risks of EV Charging

Raju Gottumukkala, Ph.D

Director of Research, Informatics Research Institute

Site Director, NSF Center for Visual and Decision Informatic

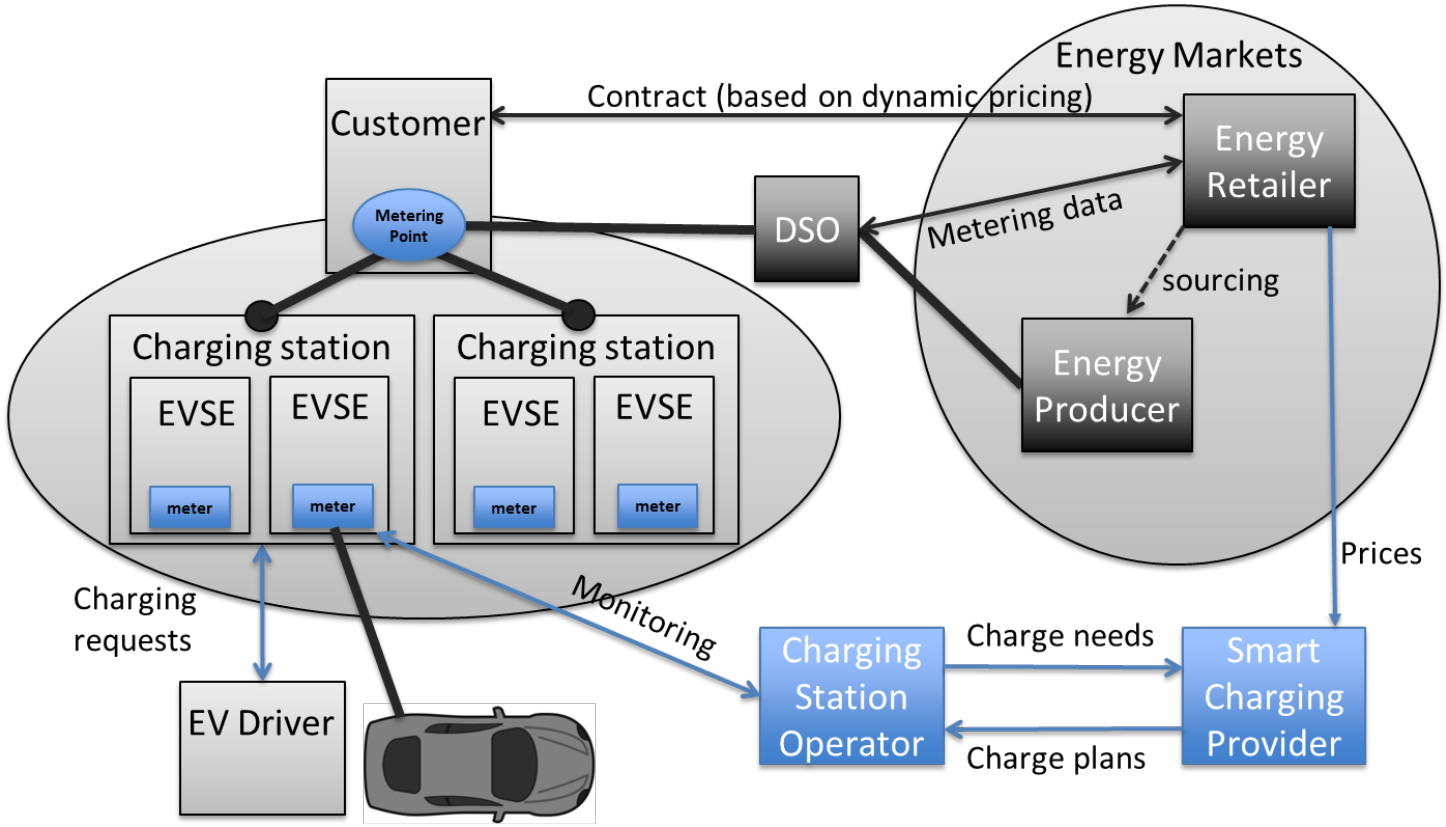
Assistant Professor, College of Engineering

2017 Internet2 Global Summit (04/25/2017)

University of Louisiana Lafayette | Informatics Research Institute

U.S. Department of Energy | INL Idaho National Laboratory

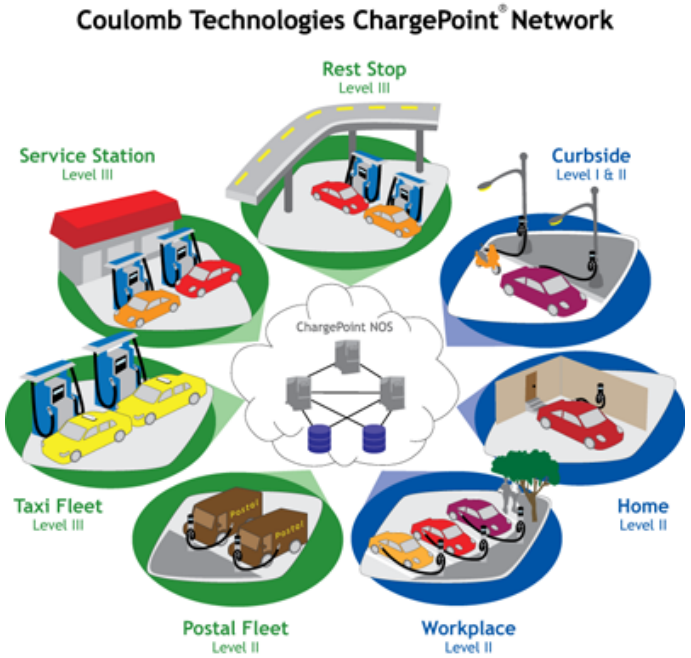
How Smart Charging Works?



Source: Lefrançois, Maxime, et al. "Outsourcing Electric Vehicle Smart Charging on the Web of Data." *Proceedings of the First International Conference on Green Communications, Computing and Technologies,(GREEN 2016), Nice, France*. 2016.

Components in a EVSE

- Electrical/Electronics
  - Metering & terminals
  - PSU, RCD, Smart socket
- Communications
  - RFID reader
  - Wifi/Zigbee/GSM/RS
  - RS-485
- Computing
  - PCB
  - Display unit
  - Firmware



Network of charging stations

What's Inside a PEV (for charging)

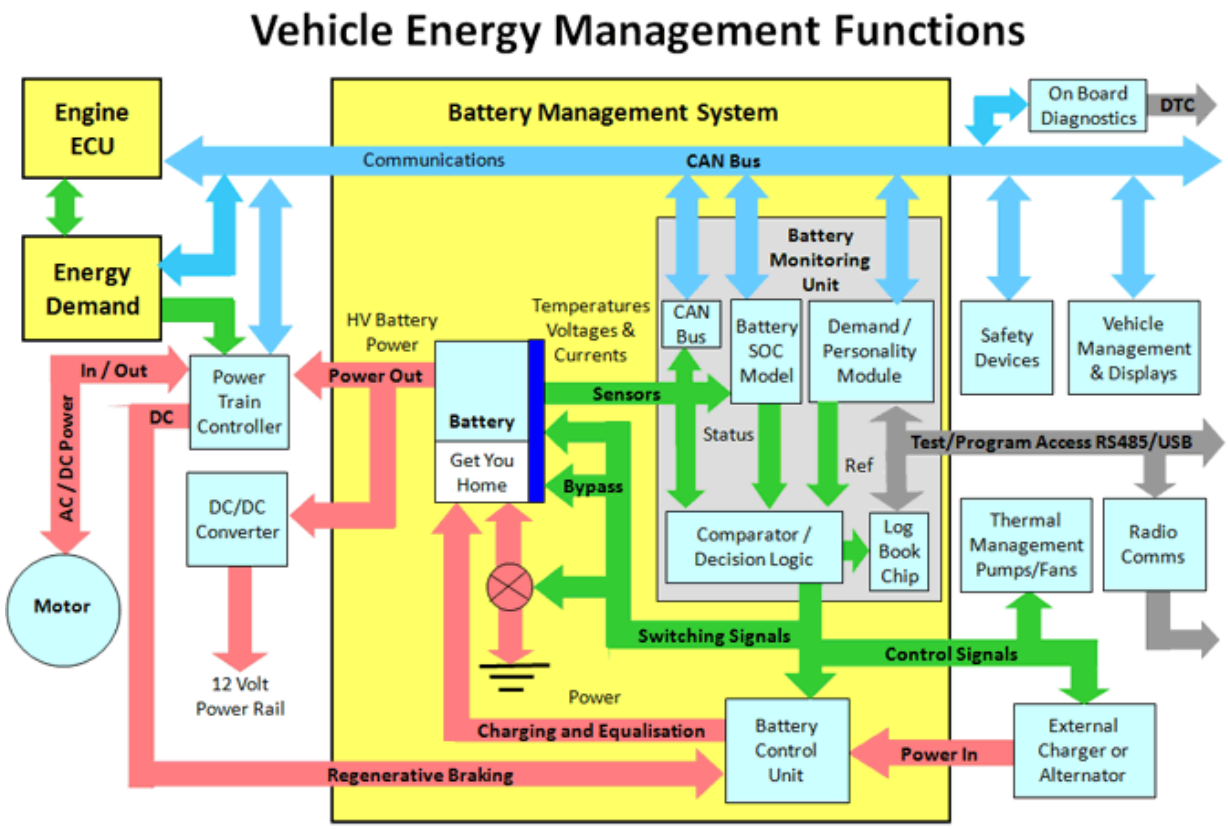


Image source: http://www.mpoweruk.com/bms.htm

RFIDs

- Key characteristics
  - Near short range
  - Convenient, more secure than user-id and password
  - Tamper-resistant – not tamper proof
- Types of attacks
  - Functional flaws (protocols, key management, cryptographic algorithms)
  - Physical attack
    - Mess with the card

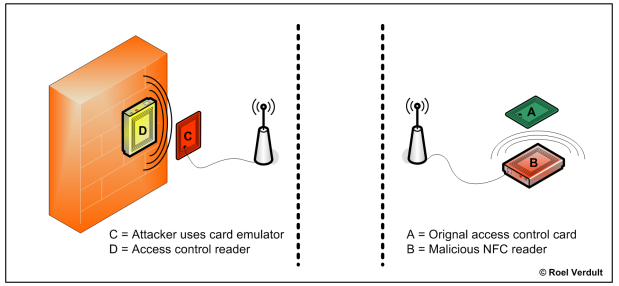
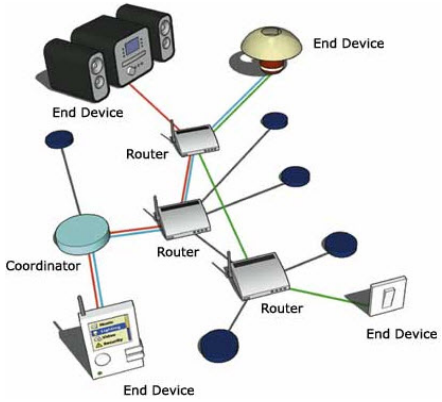


Image source: https://www.engadget.com/2008/10/07/oyster-card-rfid-hack-gets-detailed/

ZigBee

- Key characteristics
  - Short range (10 to 100 meters)
  - Simple, less expensive, low battery life & security
- Types of attacks
  - With key compromise
    - Eavesdropping, spoofing
  - Without key compromise
    - Replay
    - DoS attack



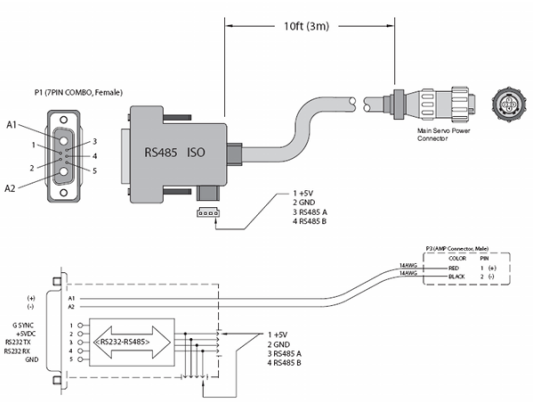
ZigBee communication

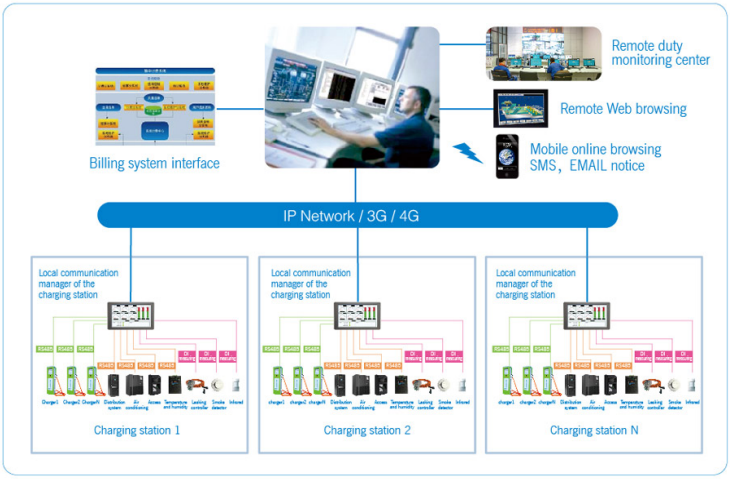
ZigBee modem

Image source: https://www.elprocus.com/what-is-zigbee-technology-architecture-and-its-applications/

RS-485 Communications

- Key characteristics
  - Low bandwidth, high latency multiplexing
  - Used to connect multiple charging stations
  - No in-built security for MODBUS (authentication / encryption)
- Attacks
  - Transceiver can monitor, disrupt and modify communications
  - Several known SCADA system attacks (i.e Stuxnet)



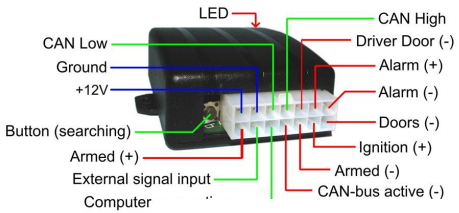


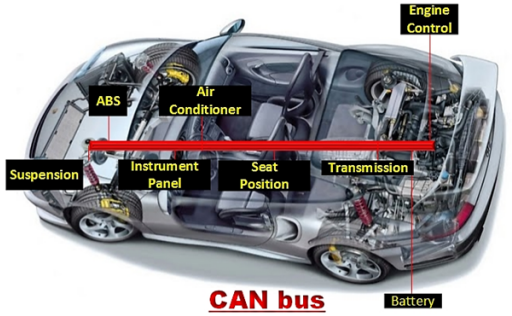
City charging station monitoring system diagram

Image source: http://www.kstarpower.com/index.php/cat/solutions/electric-vehicle-charging-solutions/monitoring-solution/

CANBUS

- Connects all major controls, sensors & actuators
- Attacks
  - Need Physical access without connectivity
  - All connected components are vulnerable



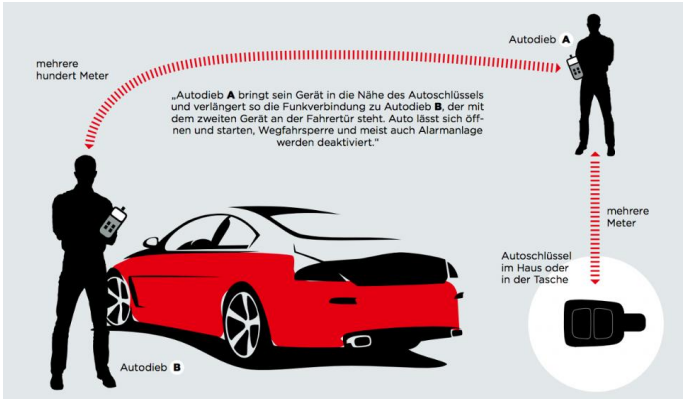


Source: http://thehackernews.com/2016/11/hacking-tesla-car.html

Charlie Miller • Chris Valasek • Work diligently since 2010 on DARPA funding • VIDEO DEMO Hacking Chrysler Jeep Remotely

Other Vulnerabilities

- Key Fob
- Bluetooth
- Wi-Fi
- Cloud security
- “People”



ADAC shows how two hackers with radio devices can harvest signals and crack cars.

Fahrzeug-hersteller	Modell	Erst-zulas-sung	Reichweite der Keyless-Verlängerung in Testhalle	Illegales Öffnen möglich?	Illegaler Motorstart möglich?
Audi	A3	10/2015	Max.	Ja	Ja
	A4	9/2015	Max.	Ja	Ja
	A6	9/2014	Max.	Ja	Ja
BMW	730d	8/2015	Max.	Ja	Ja
Citroen	DS4 CrossBack	11/2015	Max.	Ja	Ja
Ford	Galaxy	5/2014	Max.	Ja	Ja
	Eco-Sport	10/2015	Max.	Ja	Ja
Honda	HR-V	6/2015	Max.	Ja	Ja
Hyundai	Santa Fee	8/2015	Max.	Ja	Ja
KIA	Optima	11/2015	Max.	Ja	Ja
Lexus	RX 450h	12/2015	Max.	Ja	ja
RangeRover	Evoque	9/2015	Max.	Ja	ja
Renault	Traffic	11/2015	Max	Ja	Ja
Mazda	CX-5	3/2015	Max.	Ja	Ja
MINI	Clubman	8/2015	Max.	Ja	Ja
Mitsubishi	Outlander	12/2013	Max.	Ja	Ja
Nissan	Qashqai+2	11/2013	Max.	Ja	Ja
	Leaf	05/2012	Max.	Ja	Ja
Opel	Ampera	03/2012	Max.	Ja	Ja
SsangYong	Tivoli XDi	09/2015	Max.	Ja	Ja
Subaru	Levorg	8/2015	Max	Ja	Ja
Toyota	RAV4	12/2015	Max.	Ja	Ja
VW	Golf 7 GTD	10/2013	Max.	Ja	Ja
	Touran 5T	12/2015	Max.	Ja	Ja

ADAC's long list of vulnerable cars. It was able to start the engines and open doors of all those tested.

Cybersecurity Testbed @ UL Lafayette

Protecting “Smart Campus” Infrastructure

- It ain’t smart unless it is secure
- SCADA systems are not designed for IoT
- Lack of tools to detect potential entry points, and attack paths to SCADA systems
- 2015 NIST Industrial Control Systems (ICS) Security Guide

INTERNET2 2017 global SUMMIT Washington DC April 23-26

SMART CAMPUS CYBERSECURITY TRANSITION TO PRACTICE RESEARCH

FAREENA SAQIB
Florida Institute of Technology

HARDWARE BASED AUTHENTICATION AND TRUSTED PLATFORM MODULE FUNCTIONS(HAT) FOR IOTS

Fareena Saqib

fsaqib@fit.edu

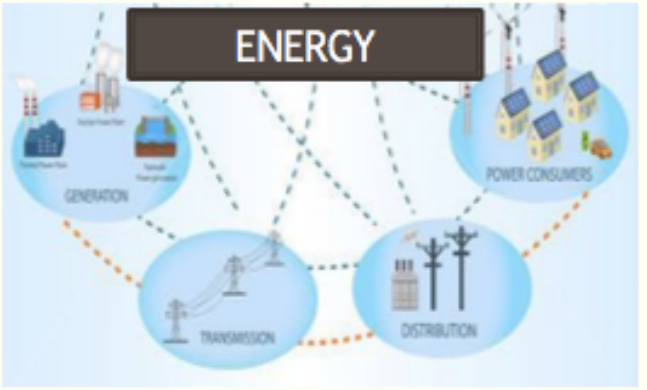
Electrical and Computer Engineering

Florida Institute of Technology

Outline

- Introduction to cybersecurity
- Hardware security attacks and countermeasures
- Research overview: Security challenges in IoTs.
- Q&A

Digital Transformation



Business Operations ⟷ Enterprise Culture ⟷ 3rd Party Ecosystem

Cyber security: Where and Why it is important

Cloud and distributed system security

IoT Security

Network Security

Biometrics and Security

Supply Chain Security

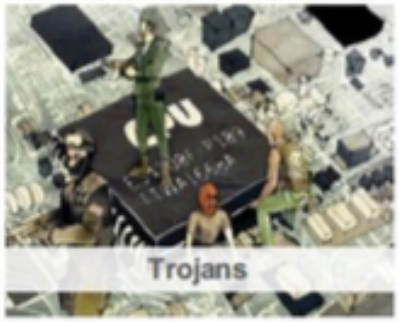
Nanoscale Security

4

Hardware Security

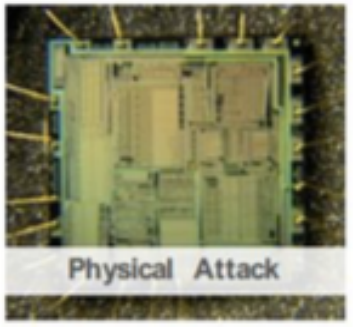
Cyber security traditionally meant software, network and data security considering hardware as root of trust. This assumption is no longer true with evolving semiconductor business landscape .

Security Attacks on Hardware


Trojans

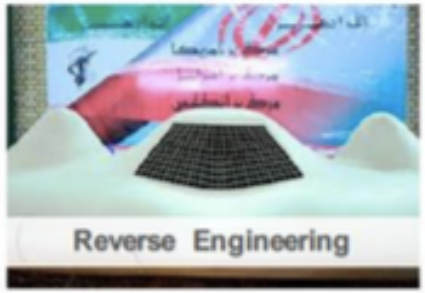

Untrusted Foundry


Counterfeit ICs


Physical Attack


Side-channel

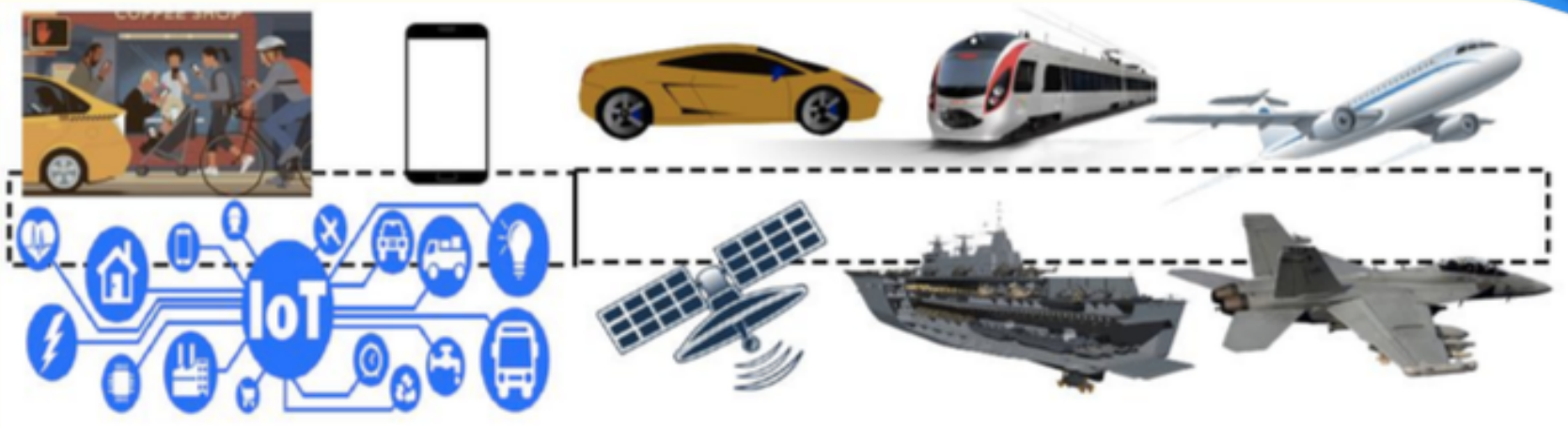

Fault Injection


Reverse Engineering

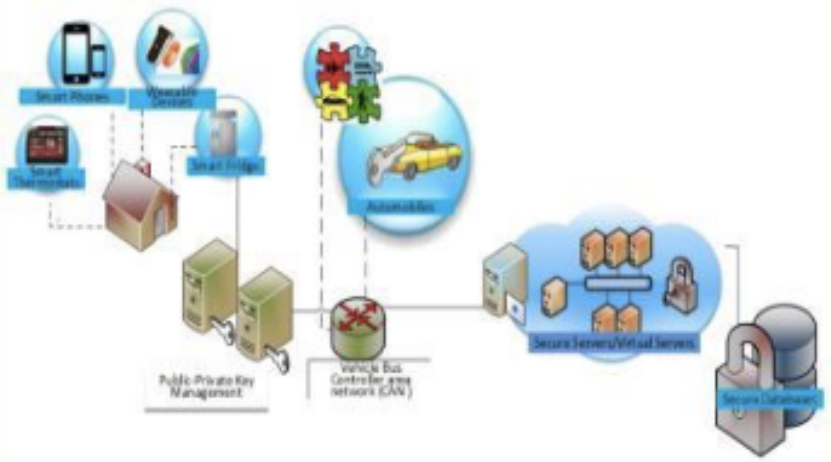
Fake Parts

Applications and Threats

Millions of chips are fabricated and tested in untrusted foundries, assemblies, and are currently in the supply chains



Hardware based Authentication and Trusted Platform Module Functions for IoTs (HAT for IoTs)



Project addresses the need for hardware-oriented capabilities and mechanisms for protecting the increasingly vulnerable microelectronic devices and systems in the internet of things (IoTs). The over-arching objective of the project is to investigate benefits to systems when constituent components are designed with the perspective of security and trust as a fundamental feature of the hardware.

Internet of things needs to be redefined as securely connecting devices, exchanging trusted data and delivering value through analytics and smart decisions

Research Projects

- **Hardware-Oriented Security and Trust (HOST)**
  - Physical Unclonable Functions
  - Authentication and Encryption
  - Differential power analysis countermeasures
  - Hardware Trojan Detection
  - Obfuscation of chip functionality
  - Secure Automotive ECU Design

- **Embedded Systems**
  - TrustZone based hardware isolation
  - FPGA-based embedded systems
  - Hardware acceleration

Supply Chain Issues

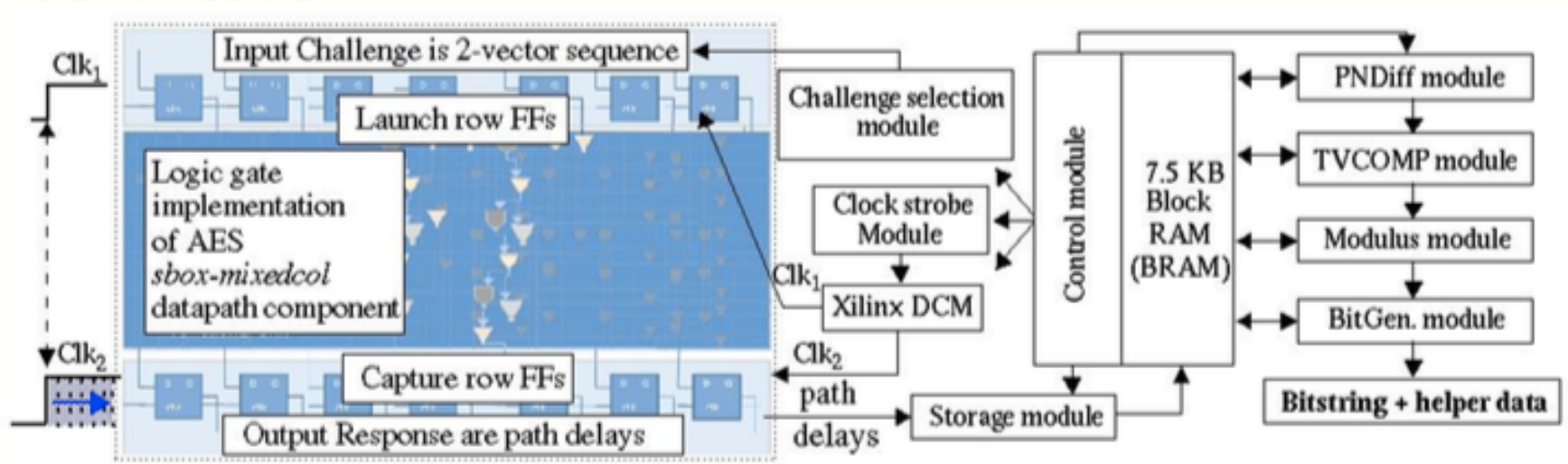
- **Supply chain threats imposed by grey markets**
  - Recycled components
  - Low reliability parts marked as high reliability
  - Older parts marked with newer date
  - Low quality clones that include malicious functionality
  - Component that are covertly repacked for unauthorized applications
  - Overbuilding of authorized components

- **Important aspect in addressing the supply chain threats is to assigning chips unique identifiers.**
  - Storing digital information in a device in a way that is resistant to physical attacks is difficult and expensive

Security Research: PUFs

HELP entropy is path delays of existing functional units.

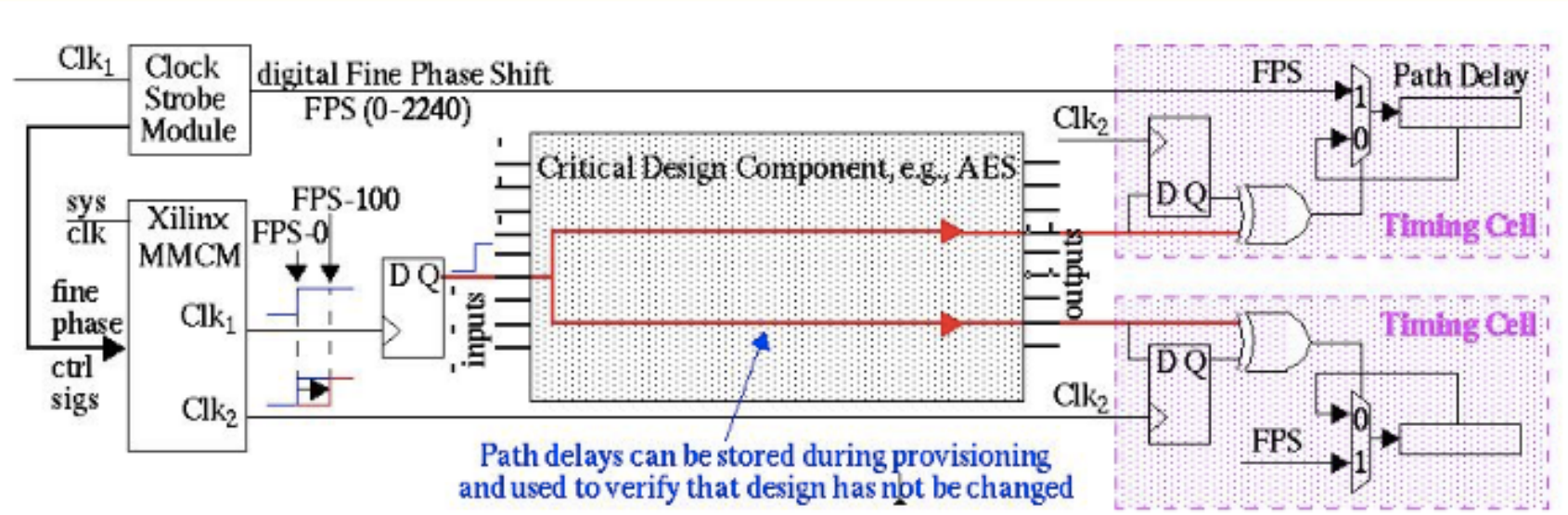
On-chip bitstring generation provides real-time identification.



Trust Research: Tamper Detection

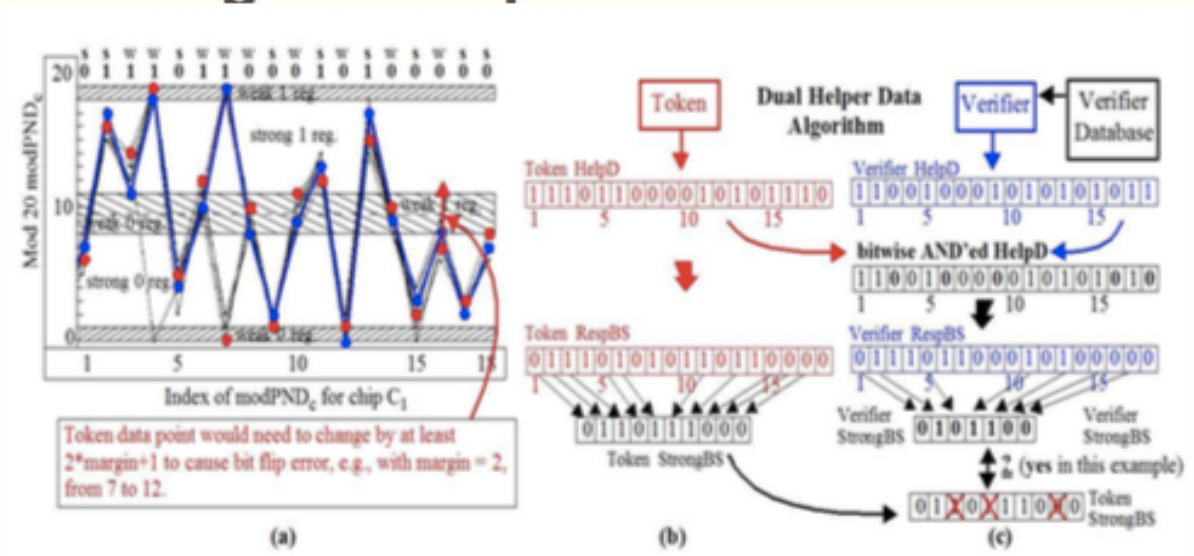
Devise a water-marking mechanism by profiling path delays

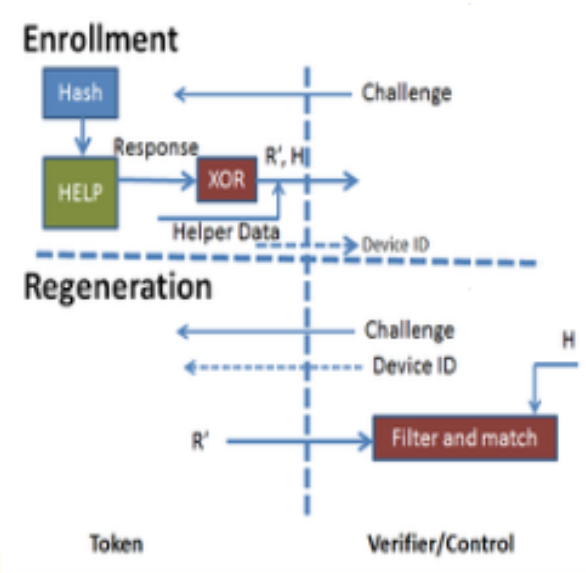
In-field chips compared with the time 0 to detect tamper



Privacy Preserved Authentication in Distributed Environment

A privacy-preserving, mutual authentication protocol using dual helper data

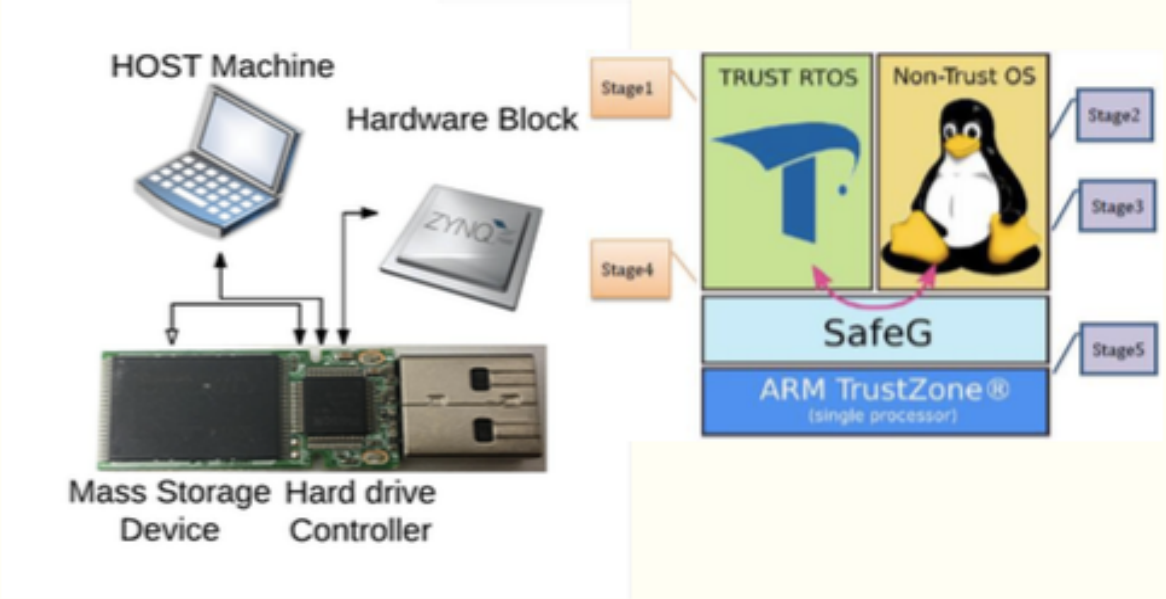




▪ Sponsored by NSF

Security based hardware isolation and Access Control

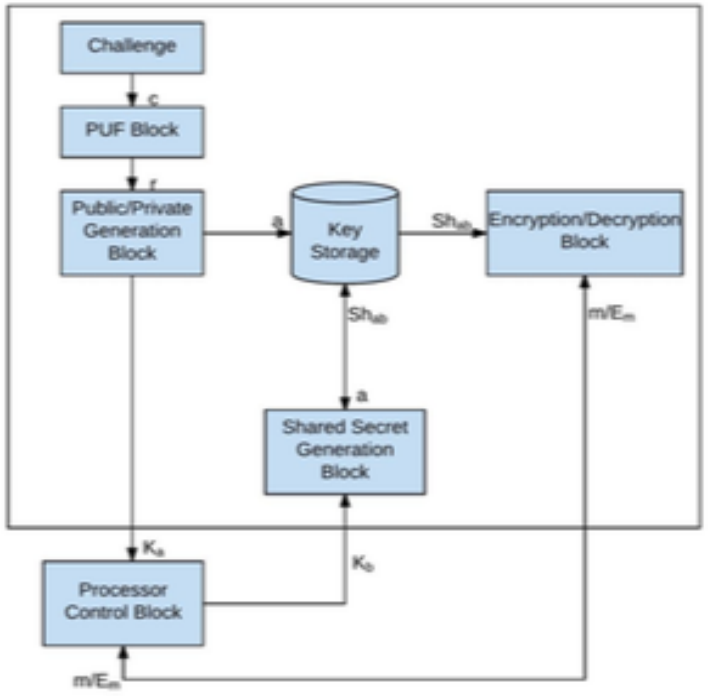
Techniques to mitigate malwares such as Rootkits and Bootkits



▪ Sponsored by NSF

Hardware Based Secure Communication over CAN bus

- ECUs are composed of a processing element connecting to an actuation and a telemetry interface of a component.
  - Hitting the brakes pedal should tell the braking system to actuate the brake disks.
  - The interactive dashboard system controlling the climate of the car.



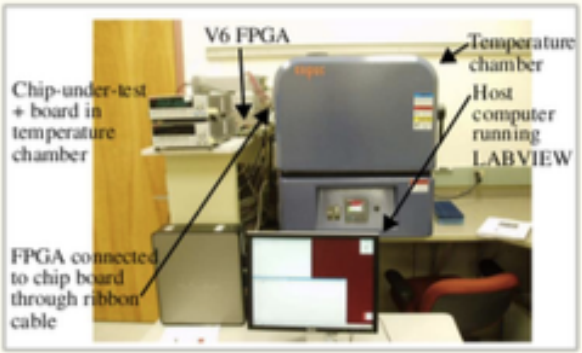
Hardware Security Curriculum Development

- This project address the need to train researchers, practitioners, and students to better understand hardware security and trust challenges as well as emergent solutions.
- ECE-5575 Hardware Oriented Security and Trust
  - **HACE Lab: An Online Hardware Security Attack and Countermeasure Evaluation Lab,.**

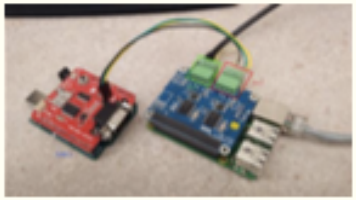
Sponsored by NSF

Hardware Platforms

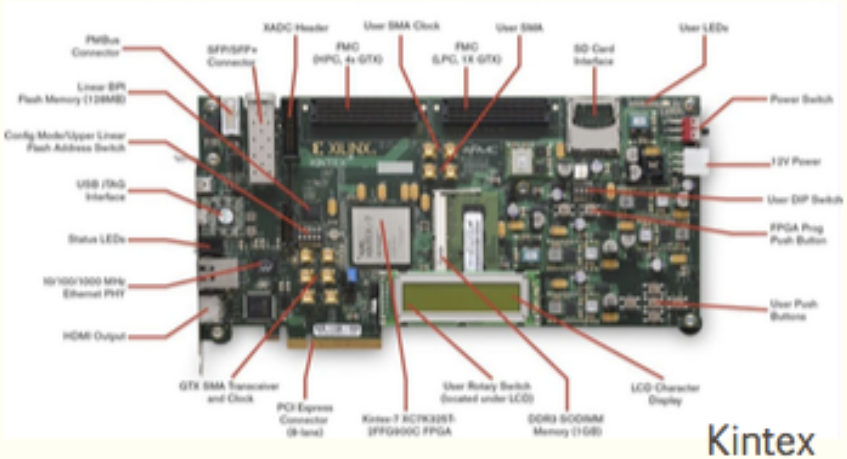
IHACS Board



Zynq



Can Shield



Kintex

Spartan3E

Questions?

INTERNET2 2017 global SUMMIT Washington DC April 23-26

IOT PEDAGOGY

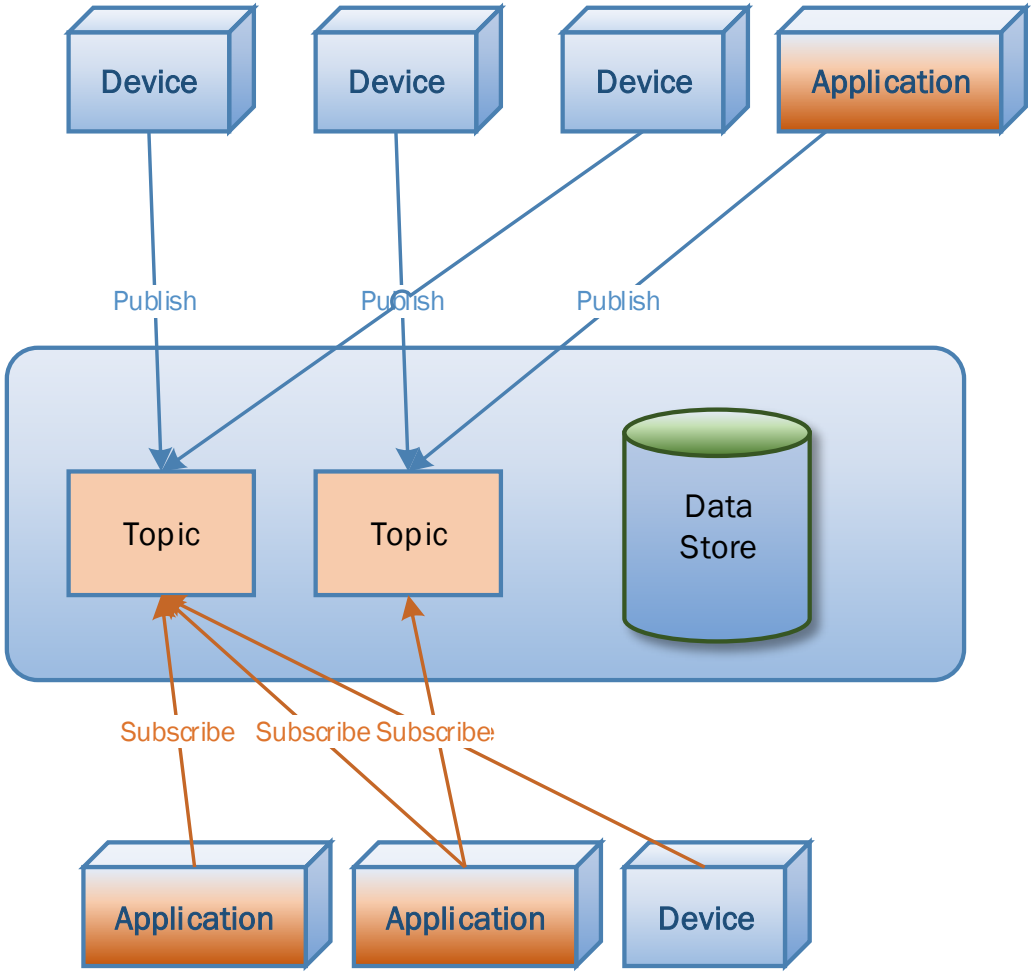
ED ARACTINGI
Marshall University

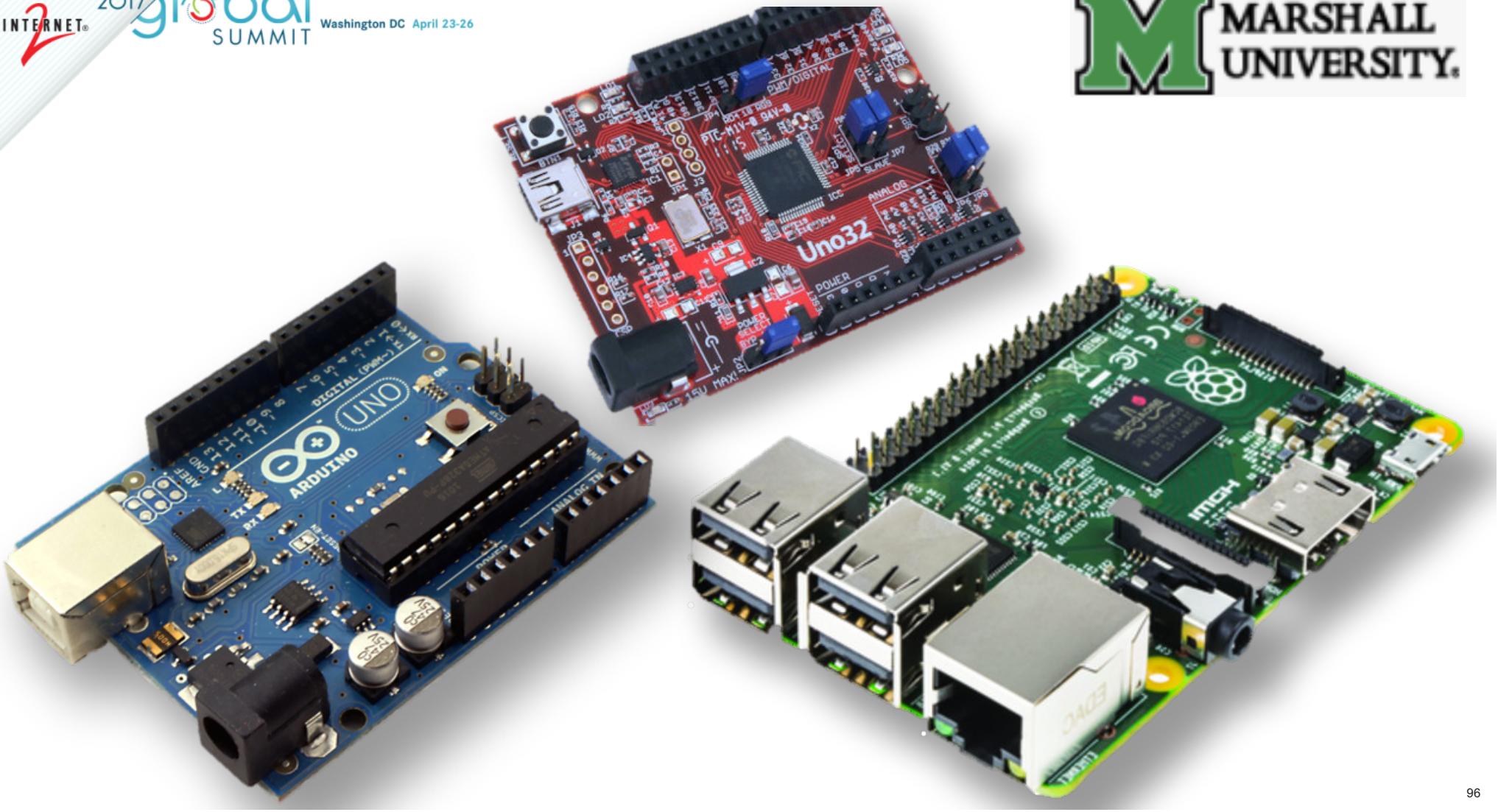
The introduction of the course

- The course was offered as a Special Topic in Computer Science at the College of Information Technology and Engineering
- Offered in Fall 2015, Spring 2016, Fall 2016, Spring 2017 and scheduled for Fall 2017
- Average of 30 graduate students mostly from Computer Science

Class Areas of Focus

- IoT Use Cases and domains
- Architecture (Subscribe/Publish, Gateways, etc.)
- Technologies (z-wave, zigbee, Bluetooth) and concepts (iBeacan, Geofencing, security, etc.)
- Cloud Services (Azure, Bluemix, AWS and others)
- Devices and sensors (Raspberry Pi, Arduino …etc.)
- Lab work for course project


Device
Device
Device
Application
Publish
Publish
Publish
Topic
Topic
Data Store
Subscribe
Subscribe
Subscribe
Application
Application
Device


Uno32
UNO
ARDUINO

Cloud services

MARSHALL UNIVERSITY

Internet Of Things
IBM

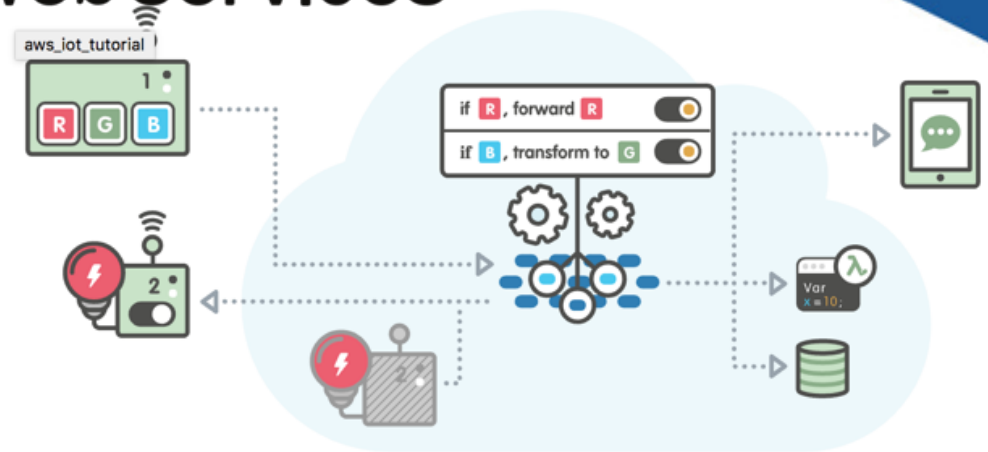
AWS IoT

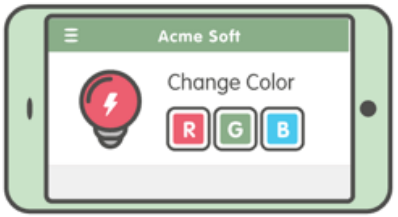
INTERNET2 2017 global SUMMIT Washington DC April 23-26

MARSHALL UNIVERSITY

amazon web services

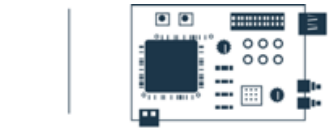
AWS IoT





MARSHALL UNIVERSITY

IBM Bluemix™



Your device or gateway

We start with your device, be it a sensor, a gateway or something else. To find out how to get it connected, search our recipes.

Internet Of Things

IBM

MQTT

Your device data is sent securely up to the cloud using the open, lightweight MQTT messaging protocol.

api

REST & Real-time APIs

Use our secure APIs to connect your apps with the data coming from your devices.

IBM Internet of Things Foundation

This is the hub of all things IBM IoT. This is where you can setup and manage your connected devices so that your apps can access their live and historical data.

Your application and analytics

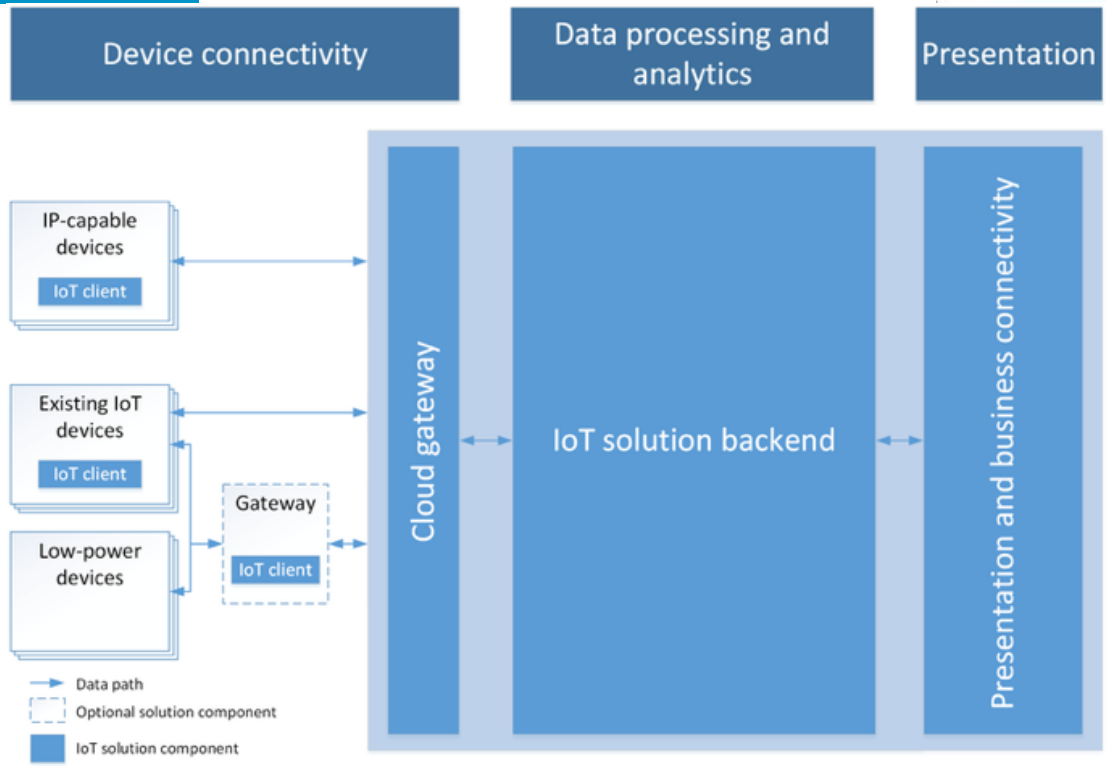
Create applications within IBM Bluemix, another cloud, or your own servers to interpret the data you now have access to!

INTERNET2 2017 global SUMMIT Washington DC April 23-26

MARSHALL UNIVERSITY

Microsoft Azure

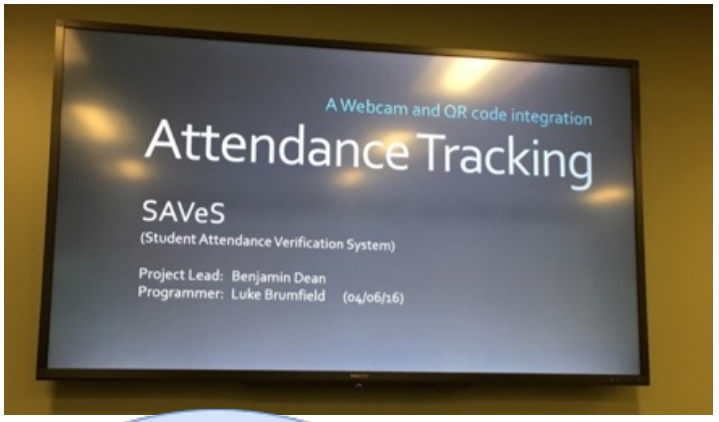
Azure IoT Suite

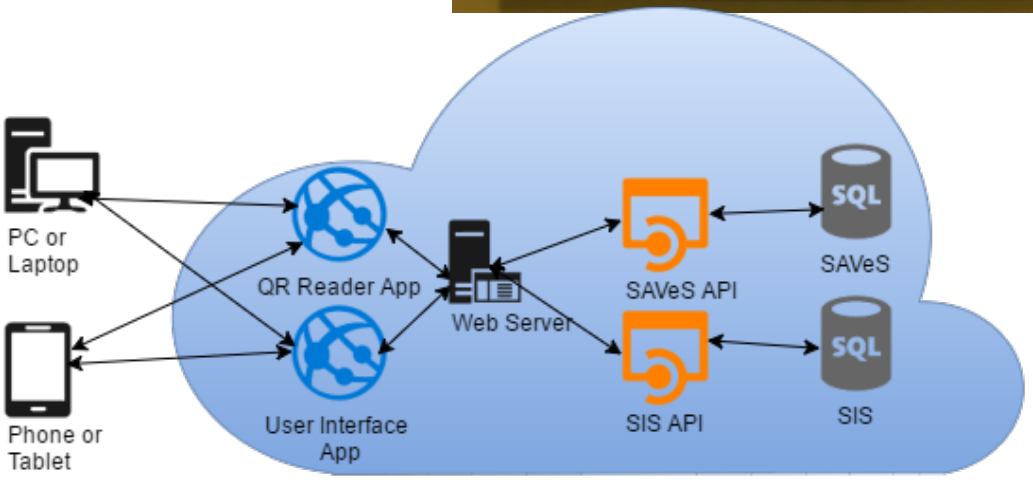


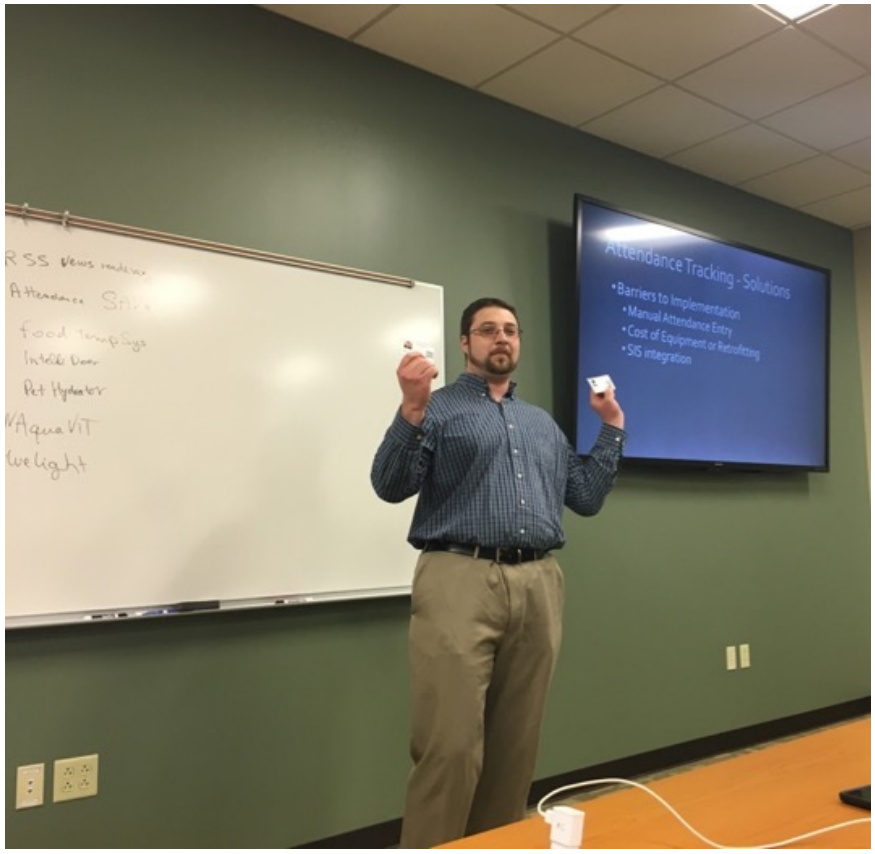
INTERNET2 2017 global SUMMIT Washington DC April 23-26

Attendance tracking system

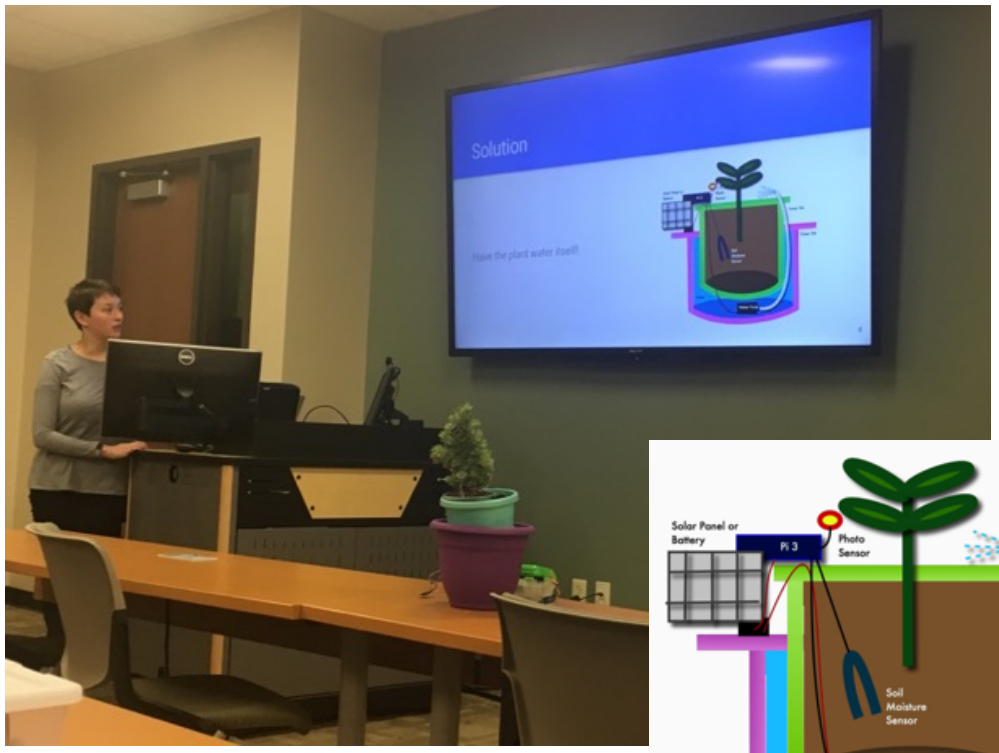
MARSHALL UNIVERSITY

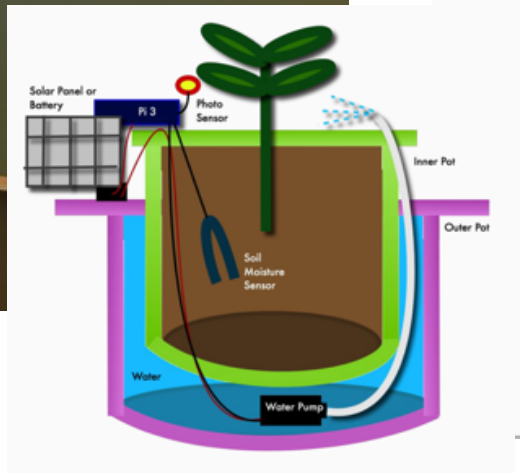


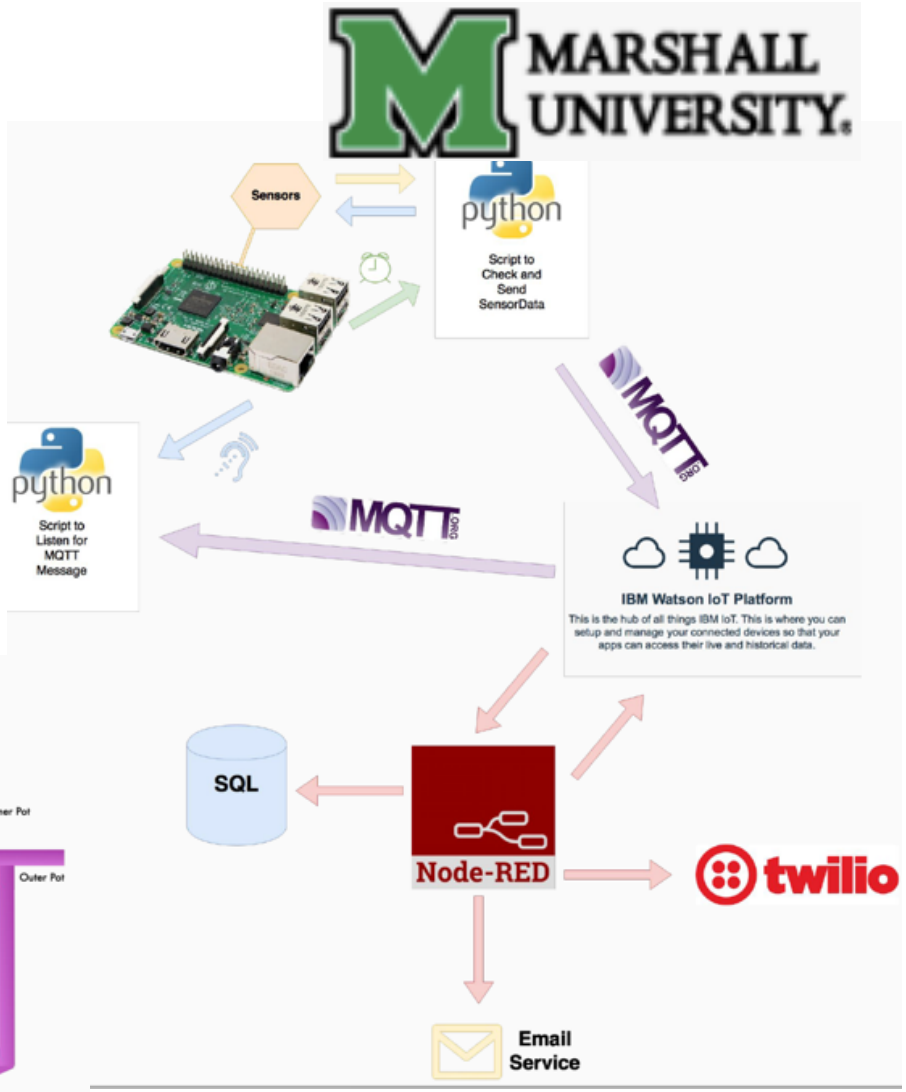




Self Watering Plant

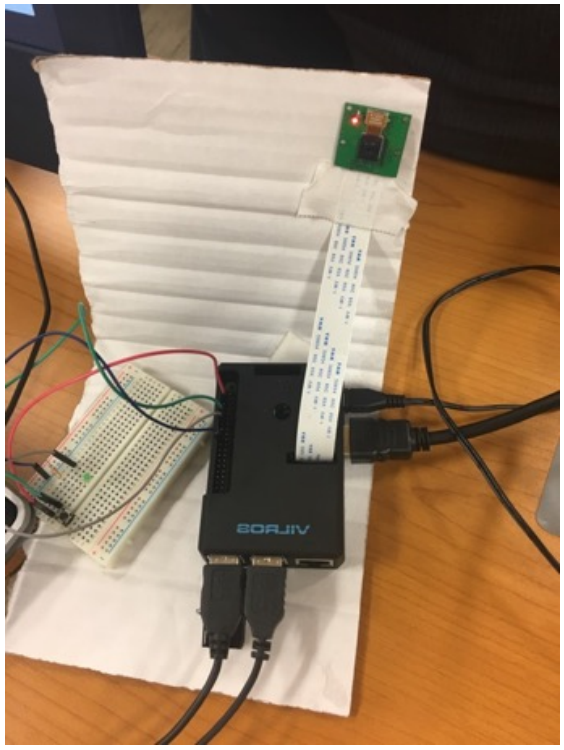






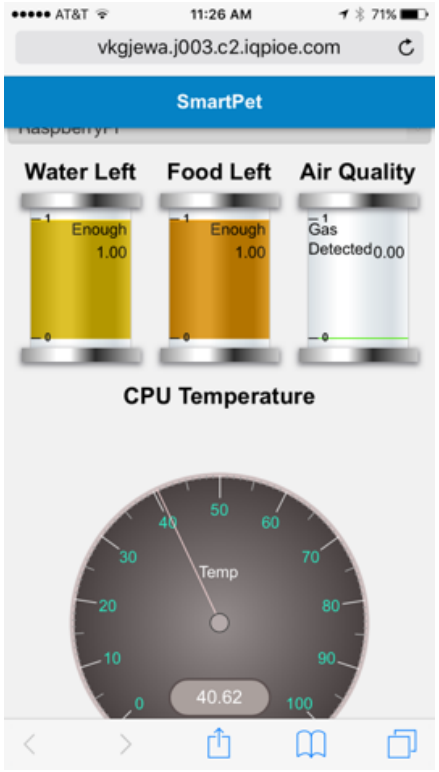
Home Automation

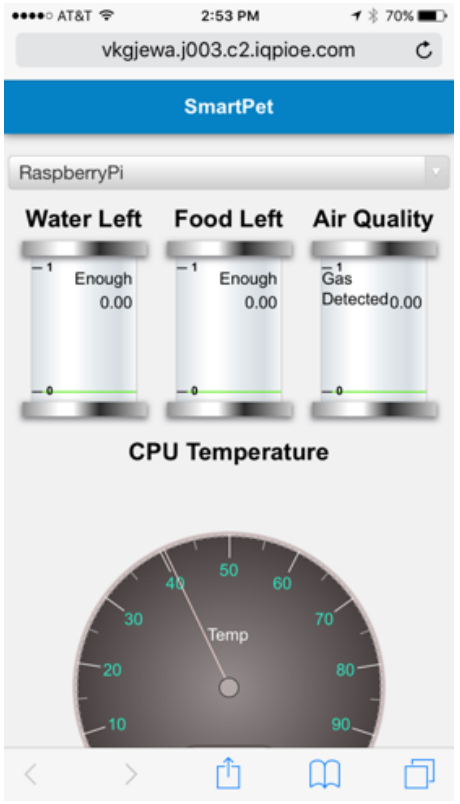
Smart Doorbell



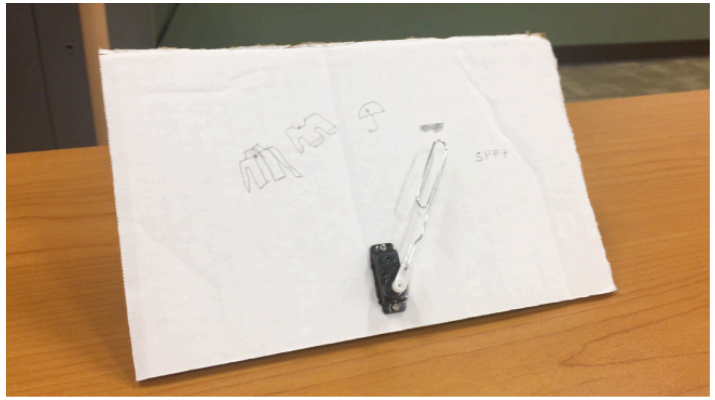
Pet care system

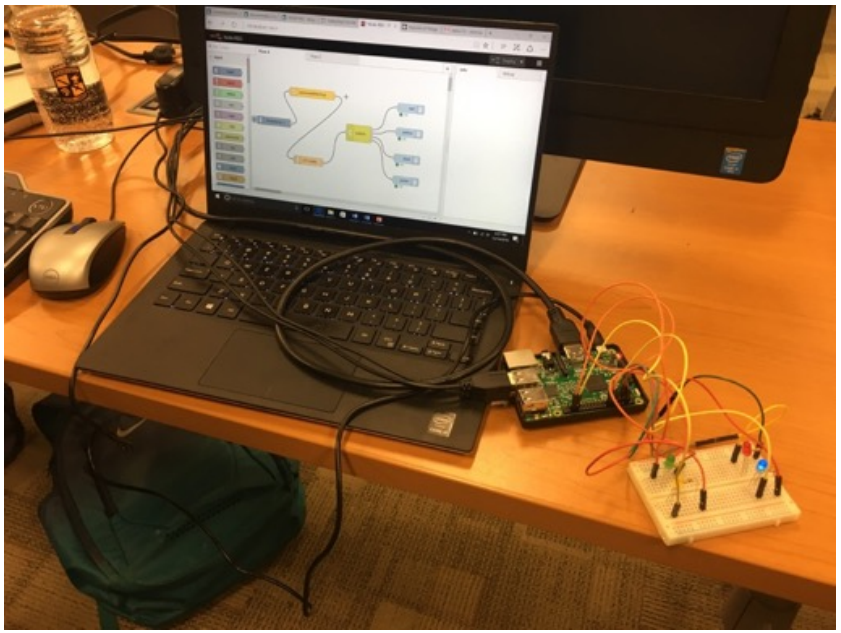
MARSHALL UNIVERSITY



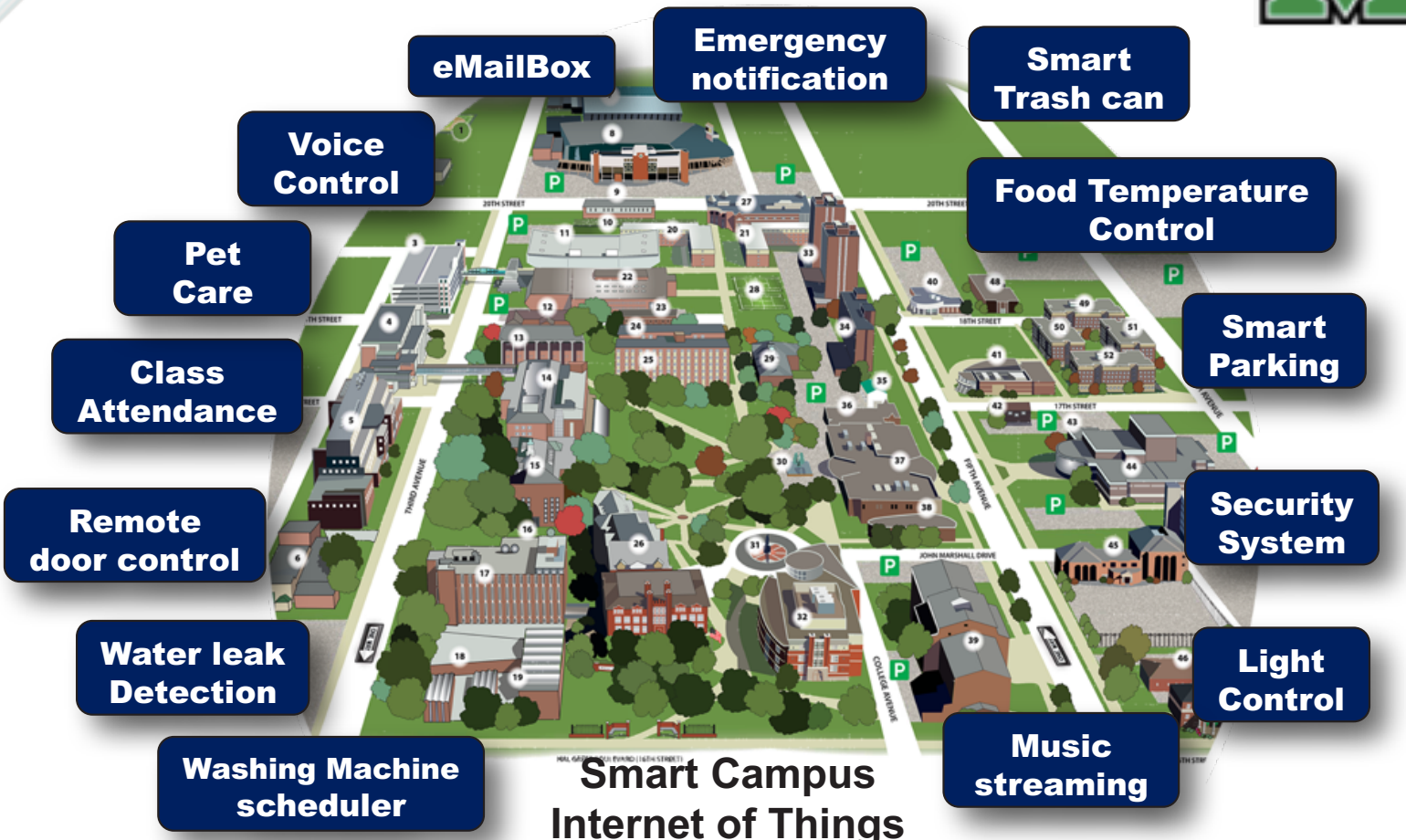


Weasley Family Clock





MARSHALL UNIVERSITY



Smart Campus Internet of Things Class Projects

NEXT STEPS

EMILY NICHOLS
INTERNET2

Internet2 Smart Campus Initiative Next Steps.

- **Increase** IoT systems risk awareness leveraging Shodan and Censys.io, demos at GS17
- **Share** IoT Systems Vendor Requirements Document at GS17
- **Planning Workshop** with Princeton University Center for Information Technology Policy (CITP) on TIPPSS and Ethics in Campus IoT Networks, 2017
- **Create** thought leadership on TIPPSS for IoT for smart & connected campus/communities
  - **White paper collaborations:** Enterprise IoT ITANA Collaboration and Internet2 CINO PAG-led White Paper
- **Participate** in new initiatives and collaborations toward a Smart Campus
- **Identify** additional smart campus best practices across the community and enable sharing

INTERNET2 2017 global SUMMIT Washington DC April 23-26

CINO Sponsored Schedule of Events at GS17

- **Sunday, April 23, 4:15-5:30pm: CINC UP: CINO Program Advisory Group Meeting (Open), Meeting Room 15**
- **Tuesday, April 25, 8-10am: CINC UP: Collaborative Innovation Community Meeting: IoT, E2ET&S, Smart Campus, Renaissance Ballroom West B**
  - Collaborative Innovation Community & Innovation Working Groups Update: IoT, E2ET&S, DBDA
    - Smart Campus Initiatives Update and invitation to participate
    - Smart Campus: IoT Systems Risk Management Task Force Update. Shodan & Censys.io demonstrations 4/24 & 4/25
    - TIPPSS for IoT: ITANA Collaboration and White Paper
  - Smart Campus-themed Cybersecurity Transition to Practice Researcher Presentations
  - IoT Pedagogy
- **Wednesday, April 26, 7:30-8:30am: CINC UP: NSF Big Data Innovation Hubs, Meeting Room 10/11**
  - NSF Big Data Hubs and Spokes Overview by Fen Zhao, NSF, and René Bastón Northeast Big Data Innovation Hub ED
  - How to get involved, connections for researchers, regional networks, and IT
- **Wednesday, April 26, 12:30-5:30pm: CINC UP: Cybersecurity Research Acceleration Transition To Practice (TTP) Workshop and Showcase (NSF #1650445), Meeting Room 8/9**
  - Join us for an interactive discussion to determine how – working together – we can accelerate Transition To Practice (TTP) of cybersecurity research into operational environments. Regional networks, IT, industry, labs, students: everyone is invited.
  - University CIO Perspective on Leveraging Cybersecurity Research
  - 12 Researcher Presentations on Identity & Access Management, Network Security, Smart Grid, Cloud Security & Storage, Data Analytics & Security, and IoT
  - Discussion, Pilot Opportunities, and Feedback, tell us what cybersecurity assets you need
  - Poster Session & Networking at breaks. Additional poster sessions on Monday and Tuesday: breakfast, lunch, breaks.

INTERNET 2

2017 global SUMMIT

CINC UP: COLLABORATIVE INNOVATION COMMUNITY MEETING: IOT, E2ET&S, SMART CAMPUS

April 25, 2017