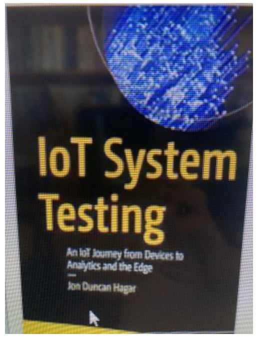


IoT System Testing

An IoT Journey from Devices to Analytics and the Edge

Jon Duncan Hagar

PNSQC

OCTOBER 10-12 2022

Jon Duncan Hagar

Testing IoT Systems using V&V, Security Hacks, & Data Analytics

40TH ANNUAL
PACIFIC NW SOFTWARE QUALITY CONFERENCE
OCT. 10–12, 2022

Introduction

- The Internet of Things (IoT) systems is a hot growth area in tech
- Problem: at what level/system to stop testing
  - Many IoT managers and stakeholders may wish to limit the testing to just their device
  - May leave IoT fielded systems with severe problems—especially with regard to security

- Presentation considers important IoT system-level test activities and the technical skills
  - IoT device, software, edge interfaces, and finally, the cloud elements
- Simplistic, manual testing of IoT needs to evolve into complete Verification and Validation (V&V) of systems
- Traditionnel pure manual testing will have important but limited application in the IoT domain compared to test automation, V&V, security testing, AI and data analytics

  - Test practitioners that can master advanced testing skills will be in demand

Taken From

IoT System Testing

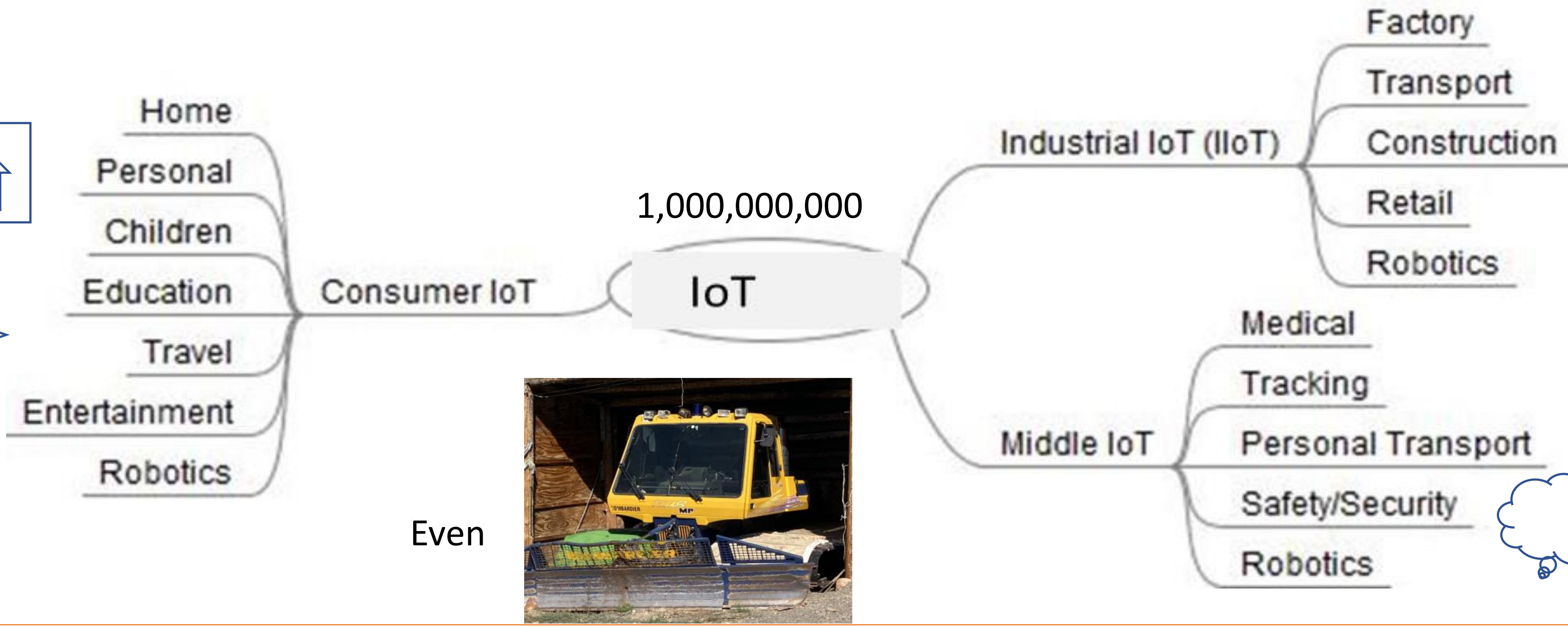
An IoT Journey from Devices to Analytics and the Edge

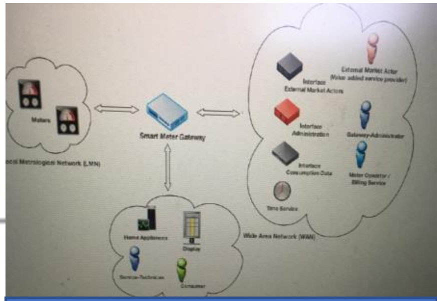
Jon Duncan Hagar

Released

IoT will be in Everything and Everywhere

- Electronic devices will be IoT
- Non-electronic things may become IoT
- Testing will be everywhere, and this presentation goes beyond device only testing



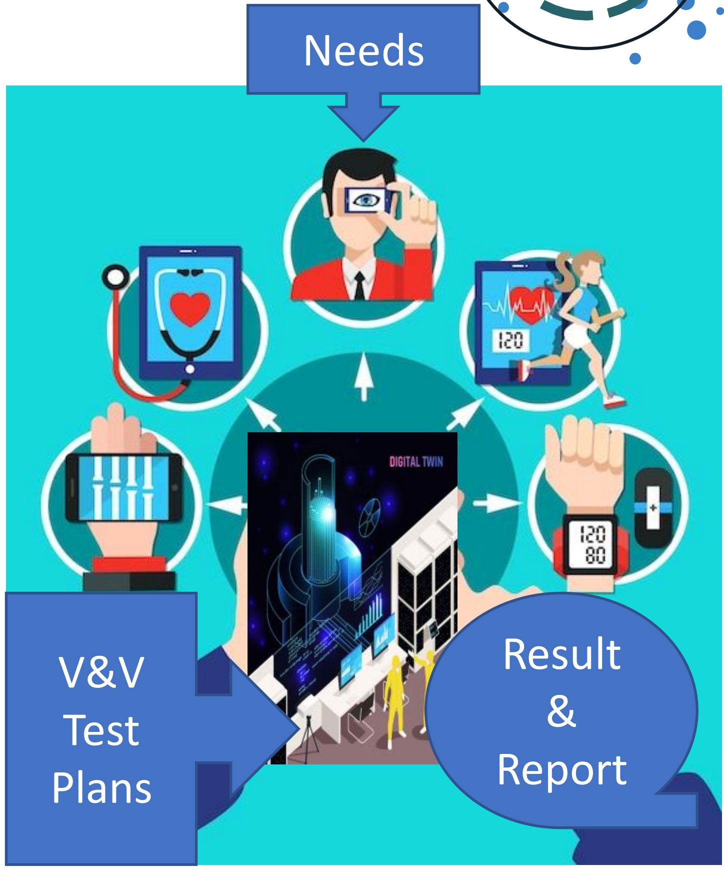

Smart Meters

Test, Verification, and Validation Concepts

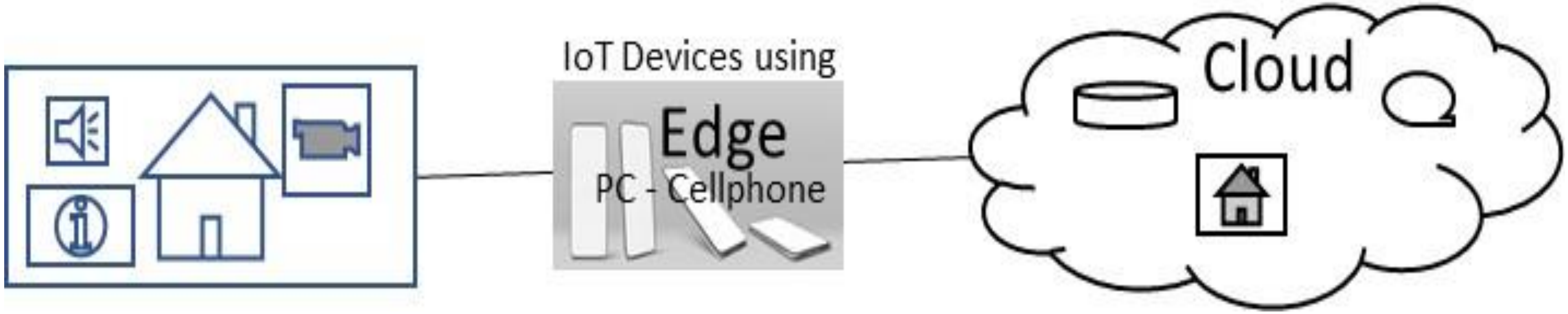
In IoT System Testing

- *Verification is assessing a system to ensure it meets requirements and design specifications*
- *Validation assesses a system to assure it meets stakeholder needs beyond the published specification*

- Testing just the device in a standalone mode is necessary but not sufficient
  - Users may be disappointed in an IoT device, stop using it (so much for product viability), or worse many users will publicly complain in social media
- Recommend concepts of Verification and Validation (V&V) and independent (IV&V)
  - IV&V and independent testing have a long history in critical systems
- The present economic society of Technology-Capitalism will drive us to IoT V&V/IV&V
  - Hard to envision the whole nature, scope and expanse of IoT systems but quality is essential
- Test environment architectures will be needed with hardware, software, test, ops, and system elements



IoT System from the Device -> the Edge -> Cloud



- IoT System-Software Architecture goes beyond the device, beyond the local (home) to edge, cloud, infinity and beyond

IV&V/V&V Example Assessments of IoT Systems

Failure example, I have a smart IoT based house that generates much of its own power, heat, and while remote is “connected” to the world

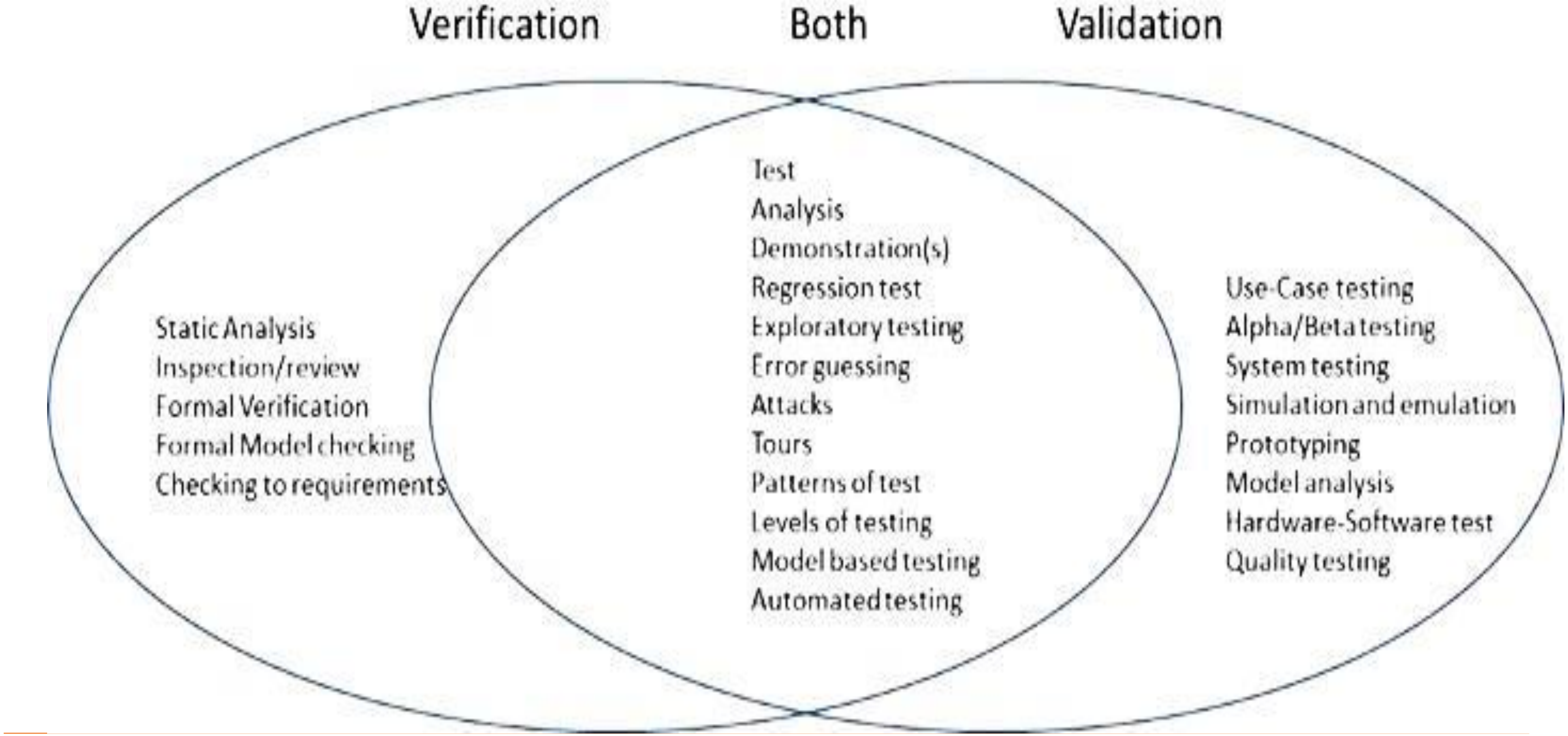
- We see problems with the connections between the solar panels, house devices, and the outside power grid with IoT systems
- The testing of a full system was limited and did not include our “unique” architecture
- As the house systems expand, we do the integration testing/fix of the architecture (we are techies, but is that our job?) __________

Another example, I run heavy equipment for snow removal

- Once my snow cat froze under engine full power. The IoT remote reboot from my phone did not work. So what did I do? ___________

- Aerospace has connection and test challenges thus V&V/IV&V were common

Major IoT System Activities of V&V/IV&V



Verification

- Static Analysis
- Inspection/review
- Formal Verification
- Formal Model checking
- Checking to requirements

Both

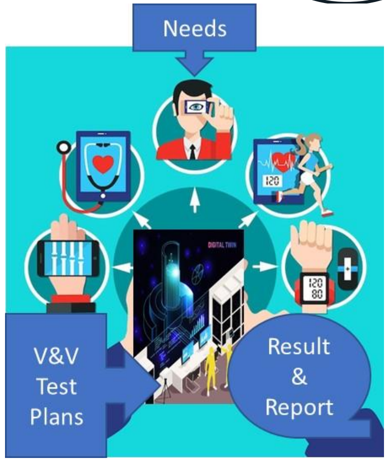
- Test
- Analysis
- Demonstration(s)
- Regression test
- Exploratory testing
- Error guessing
- Attacks
- Tours
- Patterns of test
- Levels of testing
- Model based testing
- Automated testing

Validation

- Use-Case testing
- Alpha/Beta testing
- System testing
- Simulation and emulation
- Prototyping
- Model analysis
- Hardware-Software test
- Quality testing

IoT V&V Tester Skills

- A skills list for V&V activities includes all levels of test knowledge and :

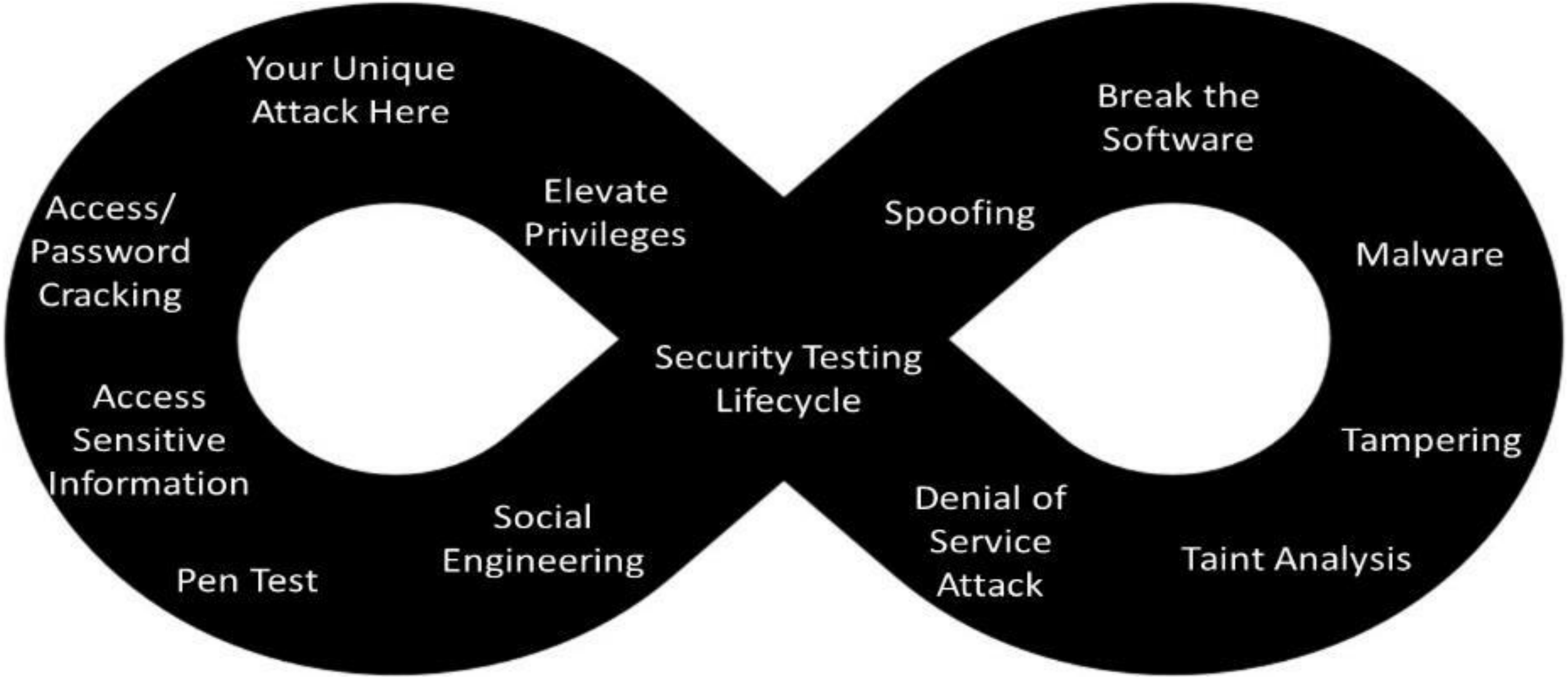


- Hardware engineering and testing/assessment
- Software engineering and testing/assessment
- Systems engineering and testing/assessment

- Operations and deployment particularly with AI and data analytics
- Identification of potential project/test management, planning, risks and impacts
- Documentation and technical communication of testing/assessment
- Working knowledge of programming/models as related to test automation and analysis
- V&V processes and standards (love/hate relationship) => IEEE 1012, ISO, IEC, FDA,

How many books/subjects are in your engineering library and do you use them? _________

Next IoT Top Task: Security Testing and Assessment

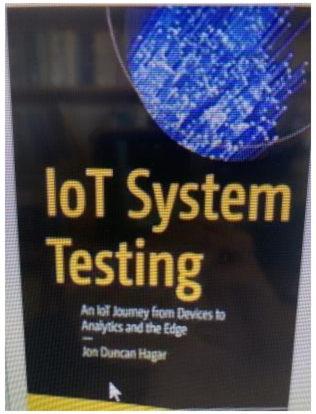


- **You are never done with a security testing life cycle**
- **IoT Software Security testing definitely goes beyond a single IoT device**

Jon Duncan Hagar

Software Security Testing (white hat thinking like a black hat)

- ***Social Engineering*** - Testers need to think and act like the "bad guys" by using social engineering
- ***Penetration (Pen) testing*** - Pen testing is where the security tester attempts to penetrate the IoT system's security measures
- ***Access Sensitive information*** - This activity is a continuation of social engineering and is part of gathering information to support security risk assessment, Pen, and later testing
- ***Access control and password cracking*** - process that is a productive subset of Pen testing that goes after password cracking or gaining system control access (what bad guys like to do)
- ***Elevate access privileges*** - After the Pen or cracking testing works and the tester-hacker is within the IoT system, they try to gain elevated access privileges to get at really "fun" critical data
- ***Denial of Service (DoS) Attack*** - IoT systems are very attractive to bad guys because many deployed IoT devices become a large attack surface, and in many of them security features of devices are lacking
  - Bad guy, black hat hackers will attack all IoT systems to later use them in DOS
- ***Security Taint Analysis*** - Security taint analysis is associated with malware, code faults, and a DoS
  - See book for details



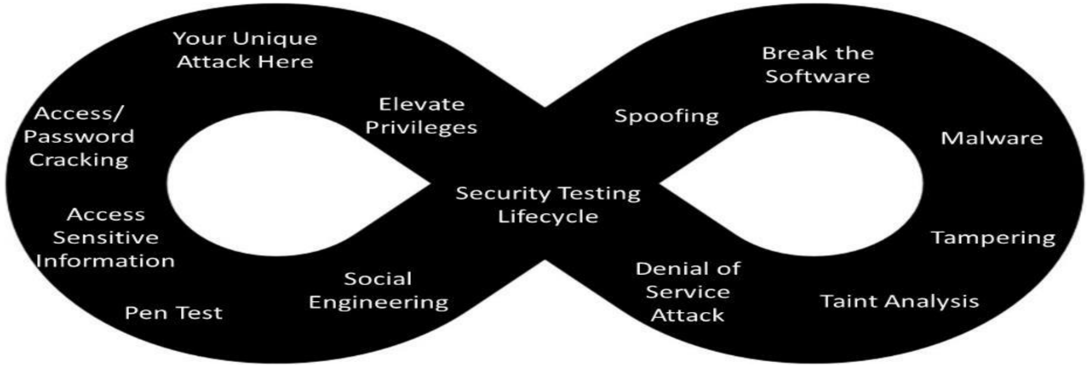
IoT System Testing

An IoT Journey from Devices to Analytics and the Edge

Jon Duncan Hagar

More Security Testing (namely a few more of my favorites but not everyone possible)

- ***Tampering Attack* -** In tampering, testers try to “break” into the hardware and/or software to gain access and understand the following:
  - Does the external checking of CM/SCM system or internal versioning detect the tampering?
  - Does the IoT system itself notice and inform stakeholders or provide notification of this attack to Ops?
  - Can bad data be input, output or used without IoT Ops knowing?
  - OWASP ZAP (if you don’t know OWASP, you should)
- ***Malware and Security Attacking the Off-the-Shelf (OTS) Software for Malware* -** Most IoT systems will include OTS software from open sources or procured from third parities that may have security flaws (or back doors) that hackers leverage
- ***Spoofing* -** A spoofing attack uses the information to impersonate an authorized device or user including:
  - Website or Domain name for IoT edge, fog or cloud services
  - IP addresses
  - Address Resolution Protocol
  - GPS spoofing of the location
  - User (man, system, hardware)-in-the-middle
  - Identity of user or login



- **Finally Break the Software - Test Attacks from security** “breaking the software” books by Whittaker, Thomson, Hagar ital.

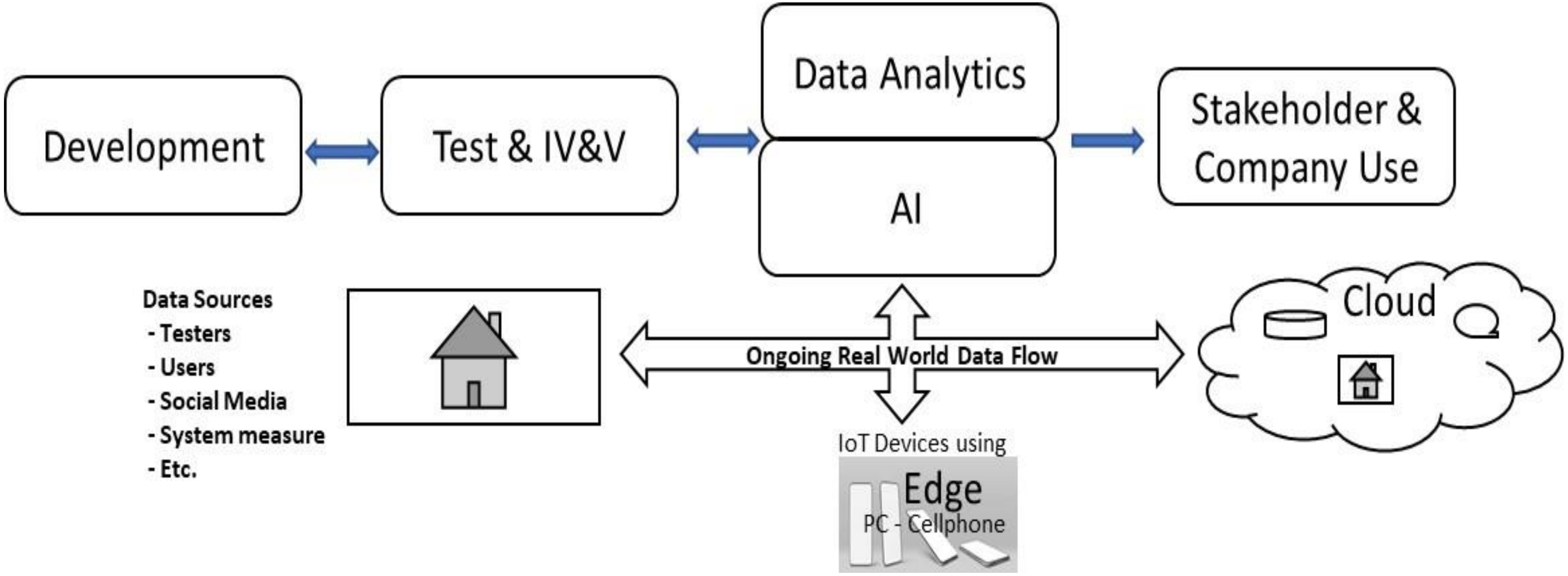
Security Tester Skills for your IoT Future

- Sample skills list for security assessments ** on the following:
  - Software engineering
  - Systems engineering
  - Partners and suppliers of support products from a security risk viewpoint
  - Test governance, standards, certification, and guidance
  - Testing of quality characteristics, which are essential to the security of IoT systems

** Dependability V&V (and IEEE 982.1…….)

○ Performance
○ Interoperability and integration
○ Reliability
○ Security attacks
○ Maintainability

An AI and Data-driven IoT Future



- Data Analytics (DA) and AI are keys in the IoT future even for testers

AI and Analytics for Testers

- DevTestSecOps improvement must use information coming from AI and DA
- The massive data millions of IoT devices and systems can generate exceeds human capabilities (it must not just be used by Ops, Sales, and Management)
  - The data that flows from the real world of local IoT devices (a home), the edge, and the cloud requires analysis
- While based on statistical tools and concepts, DA will need AI support also
- Many IoT teams may forget to include development and testers in the information coming from the AI and DA by choosing not to update or improve products and testing => a mistake, big, huge. So, great testers must know the “math”

AI and Analytics on IoT Data -> Testing

Skills list for these AI and DA activities include general test knowledge and

- Systems engineering
- Creating software test architectures (STAs)
- Knowledge and familiarity with test framework tool sets (e.g., unit test; automation; AI, data analytics, STAs with continuous integration, test, and deployment frameworks)
- Statistics, AI, and data analytics math concepts as applied to IoT testing
- Understanding and using AI processing, tools and analysis

Summary

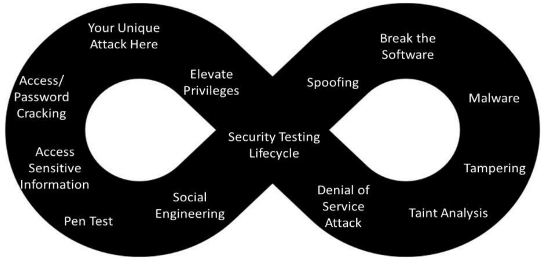
Future work

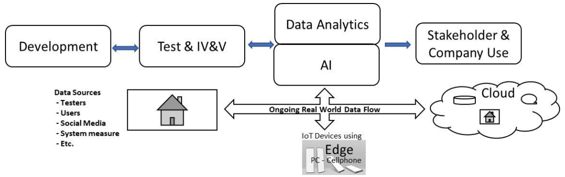
- The nature of IoT will unfold and evolve the way general IT and the web did - my prediction

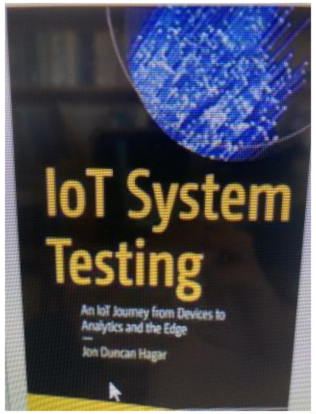
Conclusion

- This paper advocates the need for IoT software system-level testing including and beyond the IoT device software

- Focus
  - V&V/IV&V at system level as well as traditional testing
  - Security assessment
  - AI and data analytics to drive DevTestSecOps







IoT System Testing

An IoT Journey from Devices to Analytics and the Edge

Jon Duncan Hagar

PNSQC

OCTOBER 10-12 2022

IoT System Testing

An IoT Journey from Devices to Analytics and the Edge

Jon Duncan Hagar

https://link.springer.com/book/10.1007/978-1-4842-8276-2?sap-outbound-id=196819AEC565DF8EE670D48A57E6080126F9C1D8

THANK YOU