INTERNET OF THINGS AND SMART CITIES[1]


Vincent W. S. Chan

IoT and Smart-City, broadly defined, encompasses current sensors, networking infrastructure, computing and storage elements as well as 5th generation cellular and fiber architectures, new services and cognitive networking paradigms for heterogeneous networks and data analytics. The vast amount of potential data from sensors and mobile devices, the increased traffic demand from end-users, and the ever-increasing number of end-users (up to 50 billion worldwide) will require smarter approaches to sensor, network and computing resources deployment, interconnection, usage and management.

Researchers and technologists have envisioned a wide range of Internet of Things applications; the most prominent of these falls into the general areas of public safety, healthcare, "smart grid" power infrastructure, vehicular telematics including autonomous vehicles, manufacturing and logistics, and of course, advertising and entertainment. A significant portion of IoT research and development is application-focused, either identifying new use cases for the integration of sensor networks and mobile devices with the greater Internet and computing/storage elements connected by the network, or describing the infrastructure and protocols required for the more complex of these use cases. Additionally, research and development in big data analytics continues with an eye toward processing the vast expected quantities of generated IoT data. One critical issue is the security aspect of IoT/Smart-City. This includes end-devices, networks, computing and storage elements.

The general consensus seems to be that machine learning will be the basis of a lot of IoT data processing. One issue to be addressed is the value of historic data in handling extreme "Black Swan" events (such as a "zero-day" attack on the network or the end devices), especially for time-critical applications. Black Swans by definition have not occurred before and would not be in any data base or historic data. Thus, pure learning algorithms are likely not to be adequate in dealing with Black Swans. A class of different techniques must also be brought into the solution space of the problem.

On the software side, a considerable amount of research and development has been done to develop IoT "middleware" solutions to enable easy integration of heterogeneous devices with different purposes, data formats, and probably different manufacturers. This is especially relevant for what is sometimes known as the "Web of Things": the interconnection of web-enabled devices. A common software platform, e.g., semantic web, ideally would enable rapid deployment of composable applications that utilize available IoT nodes in new ways. However, multiple standards continue to be developed and the question is: "what should be the role of the governments of nations in standards setting?"

The utility of composable IoT could be vast, and indeed the benefit of composability is that we need not know today what we may need tomorrow, but the political issues will be as complex if not more as the technical issues. A critical point is that there would need to be some method of defining "available" information so as to take privacy and user permissions into account. Privacy and human rights are clear examples where the technical and political interact, but there are others as well. Different standards bodies will have competing priorities; where the U.S. Government will prioritize security, the IEEE may prioritize fairness while commercial companies put profit as their priorities. In any case, the global marketplace may reject the options put forth. The adoption of middleware could have unintended consequences, e.g., an artificial monopoly and the resultant stifling of innovation. Thus, even the technical aspects of the IoT architecture will be dependent on the resolutions of political questions.

Much research has to be done on this subject. There are at least four general objectives:

1. Identify what the Smart City of the future will look like.
2. Identify what the security challenges will be.
3. Identify steps or processes on how to make Smart Cities more resilient.
4. Recommend research and development directions; provide advice and recommendations on key issues that should be considered when the service sector composes new applications on top of the richness of the IOT/Smart-City and guide what additional research and development is necessary.

Objectives 3 and 4 are related and here we will expound around this theme.

CHALLENGES

There are several near-term challenges between now and seven years from now:

1. Control systems (especially the network control plane) and applications must be secure but also provide easy access to IoT.
2. Most sensors and actuators are not likely to be secure due to power/computation constraints, therefore creating the challenge to accommodate unsecure endpoints and secure the system.
3. Autonomous vehicle hardware and software security.
4. Secure patching of software and updating infrastructure for endpoints in IoT.
5. IoT security requires cooperation of multiple entities and organizations but can be impeded by IP and business profit issues.

[1] Some of the ideas in this piece have contributed to the report on IoT/Smart-City https://www.dhs.gov/sites/default/files/publications/IoT%20Smart%20Cities%20ReportMay2017_508%20FINAL.PDF. Special thanks to CDS for her contributions to many of the ideas captured here.

6. Separation of security and authentication requirements for monitoring and action-based channels.
   a. Action-based channels require significantly more authentication and verification and often with time delivery time guarantees for the execution of control functions.
   b. Any IoT system which can potentially impact life safety should be considered a supervisory control and data acquisition (SCADA) system and subject to certification.
7. IoT security or lack-of can affect the following:
   a. theft of intellectual property or strategic plans
   b. increase of physical criminal activity
   c. financial fraud
   d. reputational damage
   e. business disruption
   f. destruction of critical infrastructure, and threats to health and safety.
8. IoT systems are likely to use cloud technologies for cost effectiveness, which means organizations will have data related to their physical presence and activities potentially stored in locations outside of their control unless they plan for trusted, integrated solutions providers.
9. Different vendors may use separate and non-interoperable cloud providers, leading to a loss of interoperability.
10. IoT is really a SCADA/ICS at large and poses the same risks and challenges such as:
    a. Patching and upgrading (we have a chance to design in now as opposed to legacy SCADA systems). Security of codebases and development channels at vendors, verification of patch veracity before implementation on the IoT device, reboot challenges, and vulnerability management.
    b. The supply chain challenge for trusted systems will expand for consumer and commercial vendors to develop code in less trusted locations.
    c. It is extremely likely that sensitive government entities will end up in commercial facilities that have untrusted IoT systems for efficiency purposes.
    d. Very hardware-oriented IoT implementations will likely face similar End of Life, legacy and maintenance challenges that ICS and other embedded systems currently face. Modularity is the solution to allow for an easy upgrade of relevant hardware components.

The long-term challenges of IoT security are even more daunting with the wide spread globally of cyber-attack technologies. The following is a set of critical areas to consider:

1. Compromised nodes and fraction of network infrastructure will be routine. A system must be planned for operation in the presence of compromised assets.
2. "Insider" attacks are a distinct possibility. There should be in place automated systems to sense, isolate, mitigate and operate through such attacks at speeds.
3. Preventing "normal accidents" and deliberate sabotage in complex composed IoT systems is a must.
4. Security in the dynamic changing IoT system must be maintained.
5. Cyber and physical security are increasingly interlinked. IoT can be used as an overlay for cyber-physical security applications, but also can be used as a point of entry for attacks.
6. Data volumes and criticality of network connectivity are going to skyrocket with IoT. This poses questions for how devices function when connectivity is not available, and increase of device susceptibility to exploitation in this state. There needs to be a "fail safe" standard for operating these devices in the event of impaired network connectivity.
7. IoT has massive vulnerability for electromagnetic disruption, either man-made (EMP, electromagnetic pulse, HERF, high energy radiation field etc.) or natural. Similar to the fail-safe situation, IoT devices should have minimal essential functionality that is not dependent on connectivity, etc.
8. Plans for disaster recovery and critical systems restoration must take into account distributed sensor networks and loss of communications with responders and devices.

Resilient Architecture Construct

Almost surely, the IoT/Smart-City infrastructure will be attacked in the future either from forces outside the infrastructure or from insider attacks. Isolated cases have already occurred in the U.S. and other nations. This system should not be so fragile that it becomes dysfunctional under a limited scope attack. A properly designed architecture should ride through these attacks albeit with degraded performance. Graceful degradation to failures is a necessary property of that part of the system that is depended on for critical services such as first responder support, power and water infrastructure integrity, and medical and financial systems. Resiliency to benign failure and attacks requires a planned architecture, hopefully before the infrastructure deployment. The retrofitting of security overlay features on systems is both costly and often ineffective.

Resiliency is a different issue from security. One must be resigned to the fact that somehow, somewhere, sometime a part of the system is going to break down, either naturally, because of a natural disaster, or due to adversarial attacks. The question is how will the architecture perform when such events occur? Some architectures might just collapse. Some might heal themselves. What are the necessary attributes of those architectures that make it self-healing and at least have some part of the system survives? How does one reconstitute whatever is left and retain some form of infrastructure capability, no matter how thin, to perform the most critical tasks?

The following items should be addressed immediately to make smart cities more resilient:

1. There needs to be a comprehensive security architecture and plan in place.
2. Critical assets need to be protected against known and emerging threats across the ecosystem, including: perimeter defenses, vulnerability management, asset management, identity management, and data protection.
3. Gaining detective visibility and preemptive threat insights to detect both known and unknown adversarial activities including threat intelligence, security monitoring, behavioral analytics, and risk analytics.
4. There should be a substantial increase in strength and ability to recover when incidents occur through inci-

dence responses, fast adaptive and automated responses to contain damages, analyzing and inferring from forensics, crisis management and reconstitution of thin-line capabilities post-attack.
5. Information sharing and collaboration among agencies and governments is a must.
6. Red Team exercises and certifications are vital for preparation.
7. There will need to be constant monitoring of IoT control systems and improvement in responses to faults.
8. Create a new security paradigm and architecture construct that assumes compromised resources and insider proliferations, but IoT still provides useable services.
9. Create an architecture for time-critical applications to react to and function through Black Swan events, e.g., zero-day attacks. Architectural resilience for disaster recovery is key.
10. Create an architecture for management and control plane security, especially with ubiquitous deployment of "orchestration."
11. Consider the use of satellites as an alternate thin-line heart-beat network, e.g., for emergency command and control and reconstitution.
12. Security research is needed to be focused on dynamic (but bounded by M2M machine to machine, devices) environments.
13. New standards should be created to support interoperability at different timing and data volume scales.
14. New algorithms to support data fusion and validation/cross-checking of a large number of measurements with unknown certainties, including machine learning interfaced with a corrective control system.
15. Create new applications to improve cyber-physical systems security.
16. Develop control system theory where the internal states and feedback mechanisms of networks are intimately affected by inputs (traffic) and network algorithms used.
17. Develop cognitive networking where the "network" senses current network conditions to improve resource management based on observables.
18. Proactively investigate the vulnerability of machine learning as specifically applied to the IoT/Smart-City system.

Even with the best of current technologies there will not be any provably secure systems. There will always be unknown and unexplored attack surfaces. Of particular vulnerability is intrusion with software updates and new application software installations. To improve security these software and hardware additions should be first verified before insertion into operating systems. These new additions can be tested in a simulated environment such as a digital twin of the system. Note in this case the digital twin cannot be only software in a cloud; hardware interfaces and internals may have unknown vulnerabilities that cannot be truthfully modeled in a software simulation. Thus, some hardware replicating the actual operating system should be integrated in the simulation which is a nontrivial task.

A final important frontier is the development of legislation that enables the implementation of network security and resiliency. Currently in many countries, privacy and human rights protection laws prevent massive-scale monitoring of traffic and analysis of possible malicious intents. These laws often prevent human in the loop on data analytics. However, there is no clear legislation addressing automated data analysis done via algorithms and not by humans. There is a big hurdle to be overcome to pass legislation on letting machines do analytics and when enough evidence is present to flag the incidence to a judge for approval for human intervention. This is technically feasible but legislators, scientists/engineers, and human rights scholars must work together to understand what technology can do and pass the right legislation securing our infrastructure without sacrificing human rights or privacy.