IoT-Enabled Smart City Security Considerations and Solutions

Rose Bellefleur and Danny Wang

Fall 2019 – MPTM 900-201

Georgetown University

Professor Trujillo

Contents

Abstract

The City of Lumpkinsville is growing quickly. To attract new residents and businesses as well as improve the quality of life of residents, manage available resources such as roads and water in an economically sustainable manner, and reduce environmental pollution the city has begun transforming to a smart city. The transition to a smart city has been beneficial to the city, its residents, visitors as well as business and private entities located in the city. However – this transition and the interconnectivity across IT (Information Technology) and OT (Operational Technology) infrastructures has made The City of Lumpkinsville susceptible to cybersecurity risks.

Internet of Things (IoT) technologies offers new ways for businesses and governments to create value, however, the increased connectivity and data sharing with intelligent machines and their software come with significant risk of IT security issues; security for emerging IoT technologies must not be a development afterthought, the future of humanity and society is going to depend on it. With each additional access point sensitive data exposure vulnerabilities expand. Smart cities can be susceptible to numerous cyber-attack techniques, such as remote execution and signal jamming, as well as traditional means, including malware, data manipulation and DDOS (PricewaterhouseCooper, n.d). In this paper we will present to The City of Lumpkinsville a multilayered defense approach to keeping their smart city infrastructure and its associated data secure.

Problem Understanding

Smart cities have begun emerging in urban areas to improve resident's life as well as make governance more efficient. Smart cities are a combination street lights, traffic signals and cameras, electric and gas meters and sewers that all feed into a city's digital infrastructure. You can think of smart cities as connected cities that work with everything from IoT sensors to open data collection and smart streetlights to provide better services and better communication (Maddox, 2016).

For residents, visitors and companies and business entities based in a smart city, there are a myriad of benefits including the following:

- Residents
    - Less congestion and a more walkable city
    - Services delivered to residents more efficiently
    - The city being more responsive to resident's needs
    - Improved living conditions and enhanced quality of life
- Companies and business entities based in city
    - More competitive talent pool due to influx of people choosing to live in the city
- Visitors
    - Less congestion, more walkable and safer city
    - Convenience and efficiency when using the city's services and resources
- Cities
    - More residents being attracted to the city will lead to an increase in tax dollars
    - Elimination of redundancies
    - Streamlining of workers responsibilities

However, with the interconnectivity required to bring the concept of a smart city to life comes massive amounts of data flowing from various endpoints. This data can be personally identifiable, sensitive or financial and could be a treasure trove for hackers and cyber criminals.

> […] tremendous communication among city systems means that huge amounts of data accrue to the agencies that provide municipal services, including private information about residents' finances and movements. Essentially, a smart city could be seen as one gigantic, city-sized Internet of Things (IoT) device, communicating with each other and with residents' smartphones or wearables, opening and closing virtual doors that would otherwise require locks and keys (PricewaterhouseCoopers, n.d).

By adding cybersecurity components to its smart city to make it safe, The City of Lumpkinsville will be impacting beneficiaries such as residents, visitors, companies and business entities based in the city as well as the city itself. If a cybersecurity event was to occur, hackers would gain access to service delivery grids and consumer hardware like meters and valves that could result in the denial of water, gas, or electricity to large population centers – with the attendant risks to health, crime, and civil unrest. Manipulation of traffic signaling, street lighting, or transportation scheduling could quickly escalate from delays and congestion to accidents and loss of life. Even a hack into the pickup and depositing routines for waste management systems or health care deliveries could have serious consequences.

Research

Smart cities are privy to data related to all forms of privacy. Additionally technology that powers smart cities has drastically expanded the range, granularity and volume of data being collected from everyday citizens. According to Ernst & Young's report titled Cyber Security: A necessary pillar of Smart Cities, it has been identified that privacy can be threatened and breached by a number of practices that are normally treated as unacceptable, however are part of operations in a smart city ecosystem.

- Surveillance: Watching, tracking, listening to or recording a person's activities
- Aggregation: Combination of various aspects of data about a person to identify a trend or pattern of activities.
- Data leakage: lack of data protection policies can lead to leakage or improper access of sensitive information.
- Extended usage: use of data collected for period longer than stated or for purposes other than the stated purpose without the subject's consent.

Some of the components of smart city infrastructure that cause concern are as followed:

- Insecure hardware: sensors in equipment, buildings and devices may not be secure and tested thoroughly. Currently there is no standardization of IoT devices so sensors are prone to hacking. Sensors can be hacked which would lead to signal failures and system shutdowns
- Larger attack surface: smart city operations utilize complex, networked assembly of information and communication technology (ICT) infrastructure to manage various services. There are multiple entry points, and if a single device is comprised it is possible to attack the entire system or network. This vulnerability is compounded by weak security and encryption: the use of insecure legacy systems and poor maintenance; cascade effects; and human error.

As the IoT moves toward the core of digital business for both private and public sector, the integration of security between IT and OT will likely introduce unexpected hazards. These potential risks include increased attack surface, impacts on business and city operations, theft of sensitive information, compromise of personal privacy information, and damage to critical infrastructure.

Data analysis

Gartner forecasts that 8.4 billion connected things will be in use worldwide in 2017, of 2.3 billion connected things will be used in smart cities this year, and 20 billion new IoT things will be available by

2020. Many issues surround IoT implementation, partially related to the collection, storage, and use of data acquired through the use of IoT devices, also because IoT security is a nascent practice. Most organizations and local governments lack the expertise and resources to design, deploy, and operate such an ecosystem on their own.

A recent survey by Gartner found that nearly 20% of organizations observed at least one IoT-based attack in the past three years. LOB devices from vertical markets, such as medical, manufacturing, and oil and gas, continue to use standard processors, memory and industry standard network connectivity as part of the 20 billion new IoT devices that will be available by 2020. However, many of these devices are "headless" due to the lack of memory and processing capacity create an ever-increasing attack surface for IT. Additionally, building automation (BA) and industrial OT devices are converging onto the bandwidth-rich enterprise and city's infrastructure, which only exasperates the problem (Zimmerman & Pace, 2018).

According to Kaspersky Labs, more than 40% of industrial control systems (ICS), which manage physical infrastructure, were infected with malware. For example, in 2016, hackers were able to infiltrate the Bowman Avenue Dam in Rye Brook, New York, enabling them to manipulate the dam's controls, a threat to flood hundreds of homes in the area. Evidence shows that transport systems are also vulnerable. It was revealed that nearly 25% of the networking used by the San Francisco Municipal Transportation Agency (SFMTA) had been infected with ransomware. The malware manipulated the barriers to open, giving free rides to passengers over the Thanksgiving weekend of 2016, and caused substantial financial losses for the city. Another incident is that the Dallas city warning system was hacked in 2016. All 156 emergency sirens started blaring, waking citizens up and overwhelming 911 operators. The attack beyond a nuisance as it could endanger lives by denying the city's emergency services in addition to taking up precious resources (ITOne, 2017).

FIGURE 1 - TEN MOST VULNERABLE IOT SECURITY TARGETS (SOURCE: HTTPS://WWW.IOTWORLDTODAY.COM/2016/07/27/10-MOST-VULNERABLE-IOT-SECURITY-TARGETS/)

Historically, industrial control environments were isolated from other networks physically using proprietary protocols. Operational technology security was mainly focused on physical security via “air gaps”. OT cybersecurity due to the isolated and proprietary environment, is almost a decade behind the maturity level of IT cybersecurity in many ways, such as development, funding, available tools, and skilled resources.

Firstly, ICS environments significantly differ from those of traditional IT networking. ICS suppliers often include remote access to devices as a contractual requirement for service level agreements (SLA). This communication channel enables ongoing performance data gathering as well as process

optimization to reduce downtimes and maintenance costs. It, however, also creates huge black holes for threat actors to enter the control system network. Additionally, vendor's contracts often prevent modification of devices on grounds of warranty violation even patch available to mitigate vulnerabilities to potential remote attacks.

Secondly, further complicating the cyber security countermeasures in ICS environment are safety regulations. Such regulations can be governed at multiple levels of government and industrial sector bodies, making the asset security steps a challenging one. Similar regulations may require operators to provide data to third parties, whether this is accomplished through a standing channel or by exporting that data via removable media, but either method could be a target for malicious actors who are seeking that proprietary information.

Thirdly, lacking central visibility and control options and the high cost of industrial equipment further affect the ICS environment, making it nearly impossible to test changes except on the actual production devices during scheduled downtimes. Let it along, traditional tools developed for IT networking will not work in these environments. This forces IT departments to create complex policies for the data to traverse the networks.

Given all that ICS defenders have to successfully identify vulnerabilities to improve security posture of the systems and networks, but also keep up these changes that are even greater challenges in an OT environment. With hardware and software life cycles running into decades and schedule inflexibility, the complex of OT makes risk mitigation even harder.

Differences	IT Cybersecurity	OT Cybersecurity
Environments	Dynamic (from network to compute to storage to application to data, IT teams has responsibility for safeguarding every layer in a stack)	Deterministic (things only happen one way - either/or and there are no in-betweens)
Security priorities	Confidentiality (CIA model - confidentiality, integrity, availability)	Safety (AIC model - availability, integrity, and confidentiality)
Security focus	Data leaking	Process is king

Risk remediation	On regularly basis (vulnerabilities generally have effective patching available within days)	Often slow (not feasible to drop security countermeasures in and expect them to work right away)

TABLE 1 - VAST DIFFERENCES BETWEEN IT AND OT CYBER SECURITY (HTTPS://WWW.NOVOTEK.COM/EN/SOLUTIONS/CYBER-SECURITY-FOR-PRODUCTION-AND-PROCESS-NETWORKS/VAST-DIFFERENCES-BETWEEN-IT-AND-OT-CYBER-SECURITY)

Many practitioners suggest to employ a converged demilitarized zone (DMZ) between the IT and OT networking to mitigate the risk rising. DMZ, until now, is commonly deployed in enterprise's border with perimeter-based countermeasures. However, with increased sophistication of cyberattacks and as IoT becomes intelligent and connected, the traditional one line of defense is not working as the enterprise perimeter is quickly going away in this digital ear, which is based on social media, mobile, cloud, and analytics. In other words, "everything important is outside the enterprise perimeter but compliance models focus on the inside."

In their paper, Perkins and Contu state that for markets and enterprise strategies for security to succeed, a new approach to IoT security is required. Old or early views of a multifaceted, distinct IoT security market of products and services that is separate from the markets for IT security, OT security, and physical security is wrong. Both markets and security and risk management (SRM) leaders seeking to mature in the role of securing IoT should:

- Recognize and accept that current approaches and methods are not working.
- Reshape and refine organization communications and awareness regarding IoT security, paying particular attention to IoT strategy, desired business outcomes, and responsibilities.

Beyond security, digital ethics and privacy are becoming critical elements of smart city technology decision. Gartner says that organizations that bought compliance risk and are caught lacking in privacy protection will pay 100% more in compliance cost than competitors that adhere to security best practices. Best practices should focus not only on what organizations have to do, but also on what they should do ethically with regard to the rising issues around the smart city IoT technology.

Technical approach

Gartner argues that IoT solutions cannot be trusted and must be separated from the enterprise network to reduce risk. The approach recommends that infrastructure and operations leaders deploying IoT solutions on their infrastructure must:

- Establish the current risk of IoT breaches and associated liability by discovering, documenting, and classifying all devices connected to the network.
- Separate all IoT solutions from the device to the application and the rest of the network.
- Monitor full line rate wired and wireless traffic at the edge of the network to identify compromised devices, and implement a role-based policy enforcement to quarantine them.

However, the main challenge of separating all IoT solutions from the rest of the network in a digital infrastructure without a central policy platform or orchestration tools along with some sort of automated process in place is neither practical nor cost effective.

With the adoption of cloud services, the threat of network attacks against digital application infrastructure increases since resources cannot be protected with traditional perimeter defense techniques. To solve the problem on a digital application infrastructure, the Software Defined Perimeter (SDP) Workgroup, a research working group sponsored by the Cloud Security Appliance (CSA) that was established in 2013, developed a clean sheet approach that combines on device authentication, identity-based access and dynamically provisioned connectivity. More importantly, the SDP security model has shown to stop all forms of network attacks including DDoS, Man-in-the-Middle, SQL Injection, as well as Advanced Persistent Threat.

The SDP conceptual architecture is illustrated in Figure 2 below:

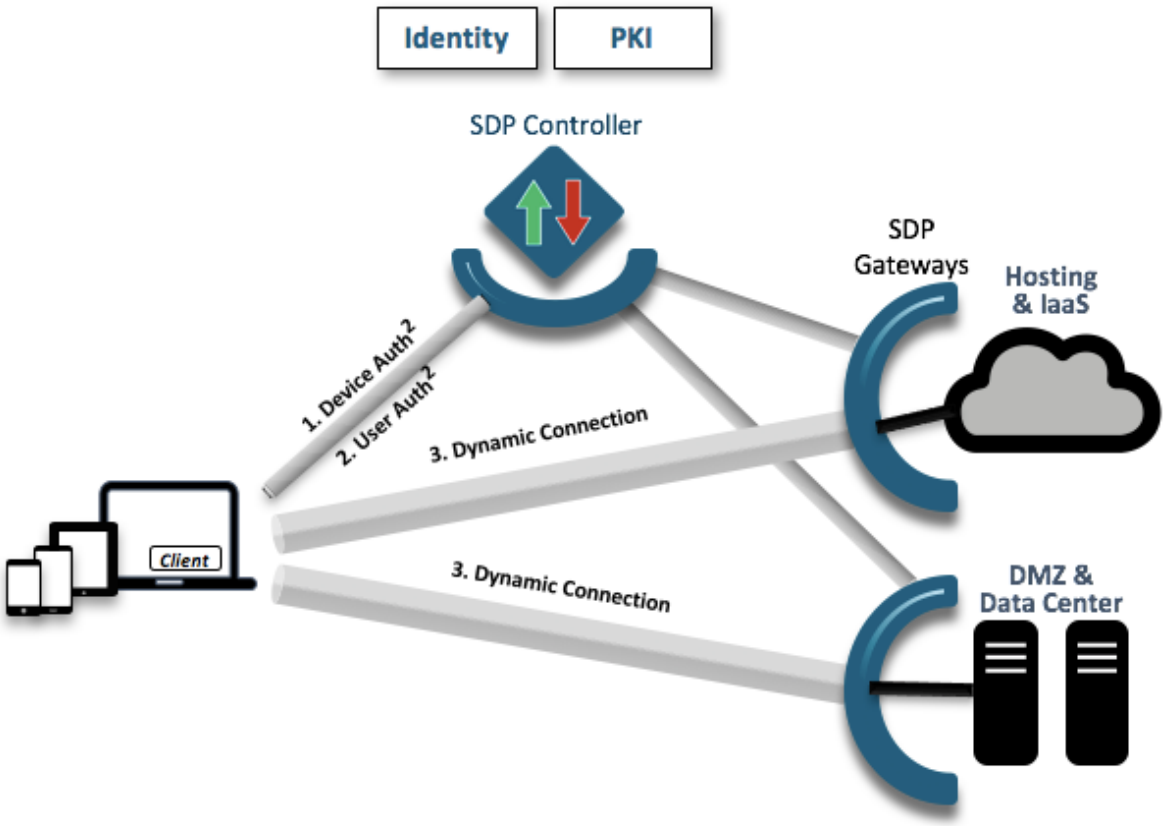

FIGURE 2 - SOFTWARE DEFINED PERIMETER CONCEPTUAL ARCHITECTURE (SOURCE: HTTPS://CLOUDSECURITYALLIANCE.ORG/WORKINGGROUPS/SOFTWAREDEFINEDPERIMETER/#_OVERVIEW)

- SDP Client handles a wide range of functions from verifying device's and user's identity to routing whitelisted applications to authorized protected applications. The SDP Client becomes the policy enforcement point for organizations as that is where access control is implemented.
- SDP Controller functions as a trust broker between the SDP Client and backend security controls, including issuing certificate authority and identity provider, and configuring both the SDP Client and Gateway in real time to provision a mutual encryption connection.
- SDP Gateway terminates the mutual encryption connection from the Client.

In the IoT Frame Work, OWASP recommends evaluating the four distinct sections below when developing IoT security considerations. "These sections are representative of typical IoT system

archetypes. Each section has specific security related concerns that are outlined in the framework evaluation criteria for that section." These sections are:

- Edge - The edge code that runs on actual IoT devices. Often times edge components are resource constrained or operate in isolated environments.
- Gateway – A device is often used to aggregate and bridge communications from edge devices to data center or public cloud.
- Cloud Platform - This component could be deployed in a company data center or a public cloud computing environment to support complex user interfaces, analytics capabilities, and provide access to data aggregation back ends.
- Mobile - Many IoT ecosystems consist of mobile application components that allow users to interact with the ecosystem via smart phones or tablets.

In this dynamic and complex risk landscape, we second that IoT cybersecurity needs to take a holistic system approach to protect those critical infrastructures physically and digitally end to end. When designing IoT solutions, it is important to understand the potential threats to the IoT system and add appropriate defenses accordingly as the system is designed and architected from the get-go.

Additionally, we refer to Microsoft Threat Modeling for Azure IoT as the IoT defense reference architecture to evaluate our technical approach to address threats identified. The threat modelling illustrated in Figure 3 focus on four main areas:

- Devices and Data Sources
- Data Transport
- Device and Event Processing
- Presentation

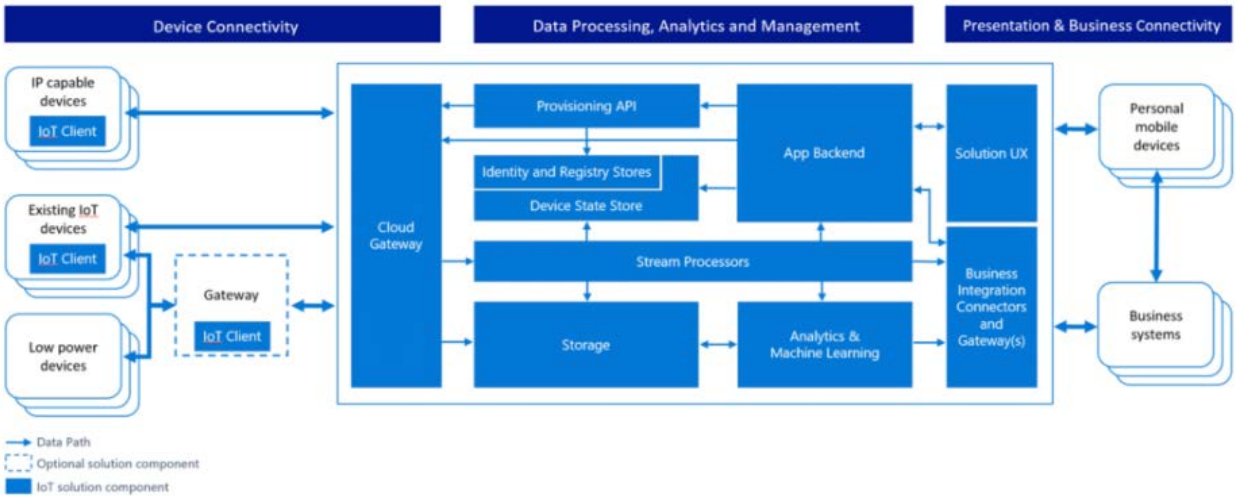

FIGURE 3 - THREAT MODELING FOR THE AZURE IOT REFERENCE ARCHITECTURE (SOURCE: MICROSOFT.COM)

Examples of threats identified by the Microsoft Threat Modeling:

- Spoofing: An attacker may extract cryptographic key material from a device, and subsequently access the system with a different physical or virtual device under the identity of the device the key material has been taken from.
- Information Disclosure: An attacker may leverage extracted key material to inject itself into the communication path between the device and a controller to siphon off information.
- Denial of Service: The device can be turned off or exhausted where communication is not possible.
- Tampering: The device can be reconfigured to operate in an unknown state to the control system and thus provide data that can be misinterpreted.
- Privilege Elevation: A device that does specific function can be forced to do something else. For example, a valve that is programmed to open half way can be tricked to open all the way.

Lastly, we take a close look at the network giant Cisco's IoT security approaches as Cisco is the leader in the IoT threat defense space according to the Gartner. In the Proposed Framework of Securing the Internet of Things, Cisco recommends addressing the highly diverse IoT environment and the related

security challenges with a flexible security framework. Figure 3 illustrates the security environment from an IoT perspective.

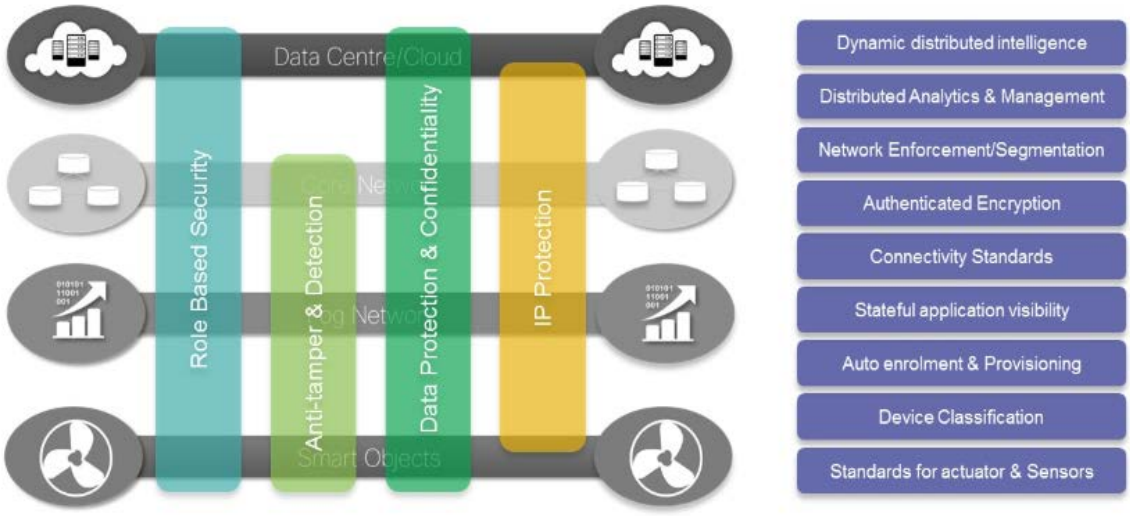

FIGURE 4 - IOT SECURITY ENVIRONMENT (SOURCE: HTTPS://WWW.CISCO.COM/C/EN/US/ABOUT/SECURITY-CENTER/SECURE-IOT-PROPOSED-FRAMEWORK.HTML)

The framework to secure the IoT environment is comprised of four layers:

- Authentication – the core layer of the framework is to provide and verify the identify information of an IoT entity. When connected IoT devices such as embedded sensors or actuators need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device.
- Authorization - the second layer of this framework is to control device's access throughout the network fabric. This layer builds upon the core authentication layer by leveraging the identity information of an entity.
- Network Enforced Policy - this layer encompasses all elements that route and transport endpoint traffic securely over the infrastructure.

- Visibility and Control - this layer defines the services by which all elements participated to provide telemetry for gaining visibility and eventually controlling the IoT ecosystem. For example, when telemetry big data injected into advanced analytics, organizations can conduct real statistical analysis on the security data to pick out anomalies, provide reconnaissance, and detect threats.

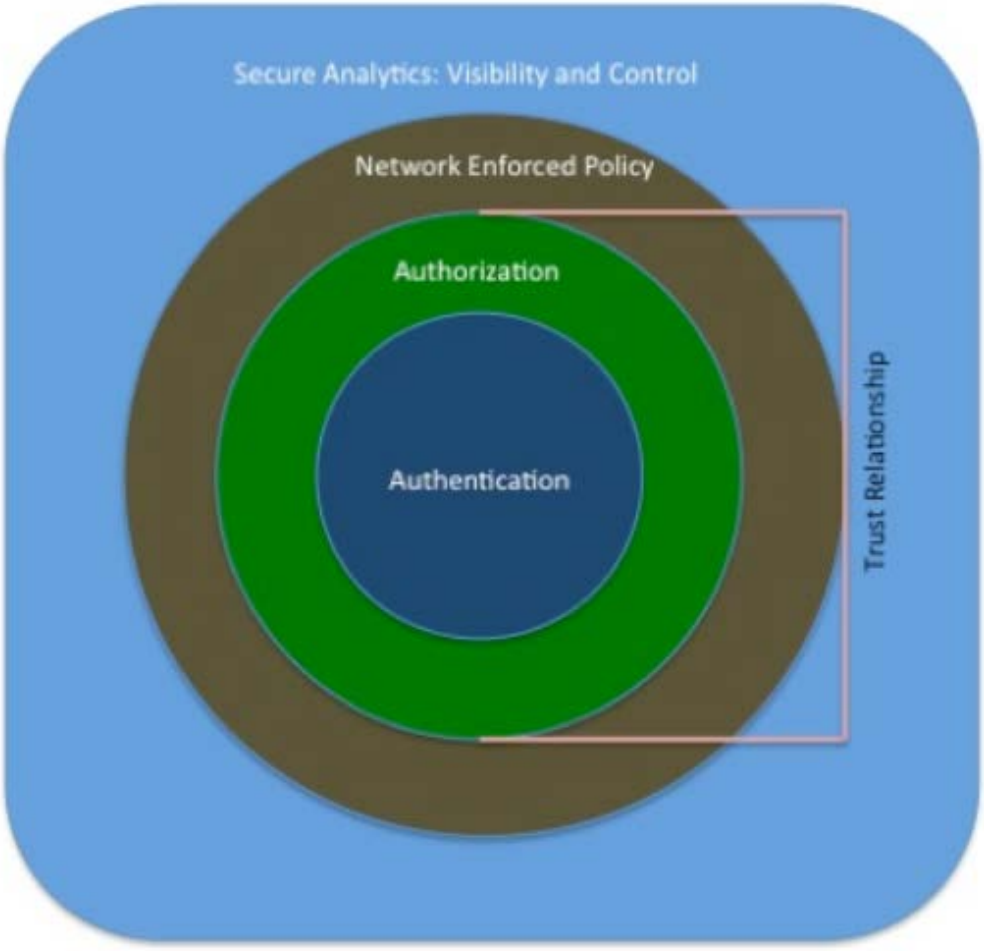

FIGURE 5 - SECURE IOT FRAMEWORK (SOURCE: HTTPS://WWW.CISCO.COM/C/EN/US/ABOUT/SECURITY-CENTER/SECUREIOT-PROPOSED-FRAMEWORK.HTML)

Solution development

As we explore the interaction areas or layers in the IoT reference architecture examples above, IoT security solutions must address each layer individually as each has its own data and access control requirements.

Layered defense model to reduce attack surface and isolate the business impact

The first step in developing a defense-in-depth solution is to take all of the capabilities that can thwart threats and match them up with the real-world business functions and flows enabled in IoT smart cities such as one below:

Layers	Smart City Security Considerations
Web Application & Interfaces	• Ensure no weak passwords and default username & password used • Ensure account lockout mechanism enabled • Ensure any web-based interface has XSS, SQL Injection, and CSRF vulnerabilities thoroughly tested • Implement two-factor authentication for cloud-based web interfaces • Use HTTPS to protect transmitted information • Include a WAF (Web Application Firewalls) to protect any web interfaces
Mobile Apps & Interface	• Ensure no weak passwords and default username & password used • Ensure account lockout mechanism enabled • Implement two-factor authentication for mobile applications (e.g Apple's Touch ID) • Ensure any mobile application uses transport encryption
	• Ensure no weak passwords and default username & password used • Ensure account lockout mechanism enabled

Cloud Apps & Interface	• Ensure any cloud-based interface has XSS, SQL Injection, and CSRF vulnerabilities thoroughly tested • Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) • Implement two-factor authentication for cloud-based web interfaces • Ensure all cloud interfaces use transport encryption
Device Security	• Ensure all system devices have update capability and can be patched quickly when vulnerabilities detected • Ensure update files are signed and validated • Ensure update files are encrypted and using encryption when transmitted • Ensure update servers are secure
Network Access Control	• Start with Zero-trust • Ensure authentication with strong passwords • Ensure roles can be properly segregated in multi-user environments • Enable two-factor authentication where possible • Ensure authorization
Data at Rest	• Ensure password security options are in place, such as enabling strong passwords with two-factor authentication • Ensure encryption options available to meet confidential requirements • Ensure data accounting and secure logging • Ensure alerts and notifications for security events
Data in Transit	• Ensure all communication is encrypted between the device and the internet • Ensure SSL/TLS implementations are up to date like TLS 1.2

	• Use recommended and accepted encryption practices and avoid proprietary protocols
Privacy Concerns	• Ensure personal data collected is properly protected using encryption at rest and in transit • Ensure only authorized individuals have access to collected personal private information • Ensure data is de-identified or anonymized • Ensure a data retention policy is in place • Ensure end-users are given a choice for data collected beyond what is needed for proper operation of the device
Physical Security	• Ensure the device is locked down • Ensure the firmware of OS (Operating System) is locked down • Ensure the product is tamper resistant • Ensure the system has the ability to limit administrative capabilities • Disable unused physical ports

TABLE 2 - IOT SECURITY CONSIDERATIONS (HTTPS://WWW.OWASP.ORG/INDEX.PHP/IOT_SECURITY_GUIDANCE)

Improving visibility and control

Threats evolve as quickly as the new technologies that attackers strive to exploit. This means that there is limited time between threat detection and response. Smart cities need to know when new devices connected to their networks, including application program interfaces (API), protocols, applications, and users as they attempt to get on the networks. The smart cities also need to detect and block threats before they can affect the city's infrastructure remotely. An automated and behavior-

based detections will ferret out the latest known threats; protocol analysis helps prevent human error; anomaly detection uncovers new threats such as zero-day threats.

Device discovery and access management

One of the security weaknesses inherent in IoT devices is that they usually have minimal, if not at all, built-in security. When a device cannot be uniquely identified, it can be easily spoofed or imitated, enabling threat actors to penetrate the network. Having strong device authentication mitigates this risk, and helps ensure data integrity and effective threat prevention.

Intelligence software-defined network segmentation

Given all that risks of future IoT compromises will increase as connected devices proliferate. Software defined perimeter/segmentation (SDP/SDS) allows smart cities integrating security into their network such as provisioning and decommissioning micro-segmentation on-demanding. With some orchestration tools, security policies can be pulled or pushed centrally. Moreover, SDS combined with predictive cybersecurity analytics can make API calls to automate adaptive responses to the increasingly complex network to prevent future unknown attack such as zero-day attack. Additionally, SDS enhances IoT security by reducing the attack surface. It quarantines potential threats and limits their ability to propagate across a wider infrastructure. With proper network segmentation, a threat infiltrates a smart city's camera systems, for example, would unlikely be able to spread to the city's traffic management systems. It makes security incident response more quickly and more manageable as the affected network segment is isolated from its noise neighbors.

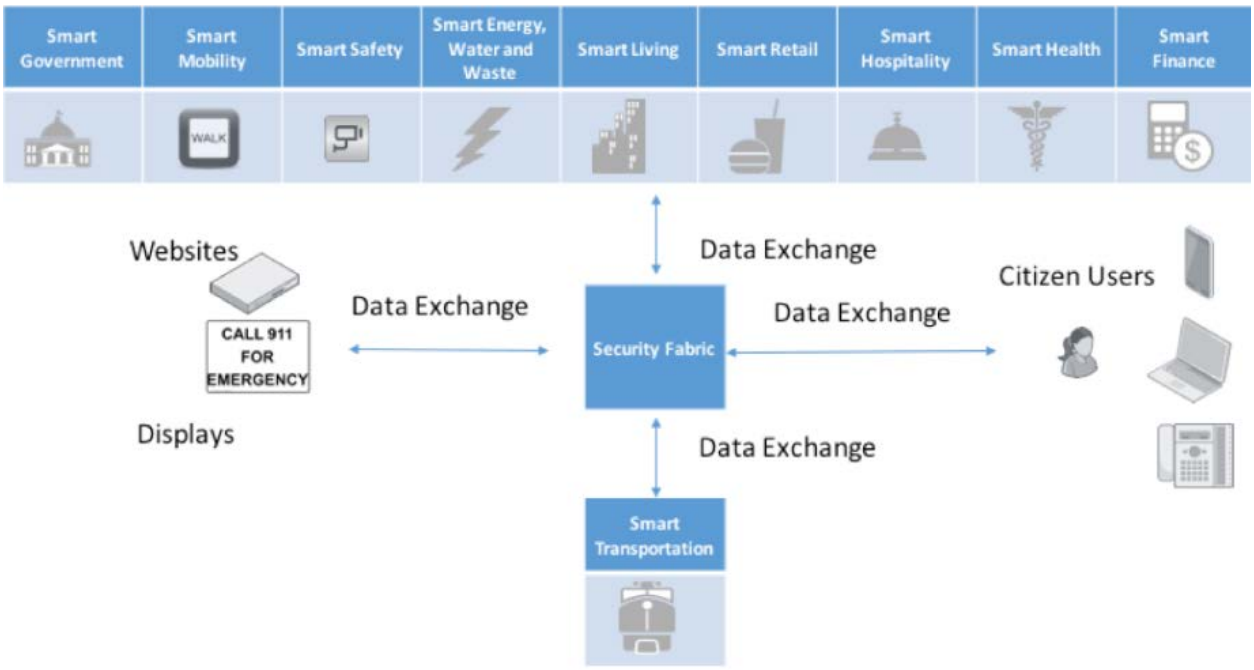

FIGURE 6 – SMART CITY NETWORK SEGMENTATION BASED ON ATTACK SURFACE (HTTPS://WWW.FORTINET.COM/BLOG/INDUSTRY-TRENDS/POST-MIRAI-MANAGING-THE-ATTACK-SURFACE-OF-A-SMART-CITY.HTML)

This strategy will be a more viable approach to IoT security. Instead of having firewalls at the edge of every network, SDS can create software defined network segmentations or virtual overlay network as needed to limit which devices can access to the overlay, and route the traffic based on the identity instead of the IP address, to protect endpoints from Man in the middle (MITM) and DDoS attack.

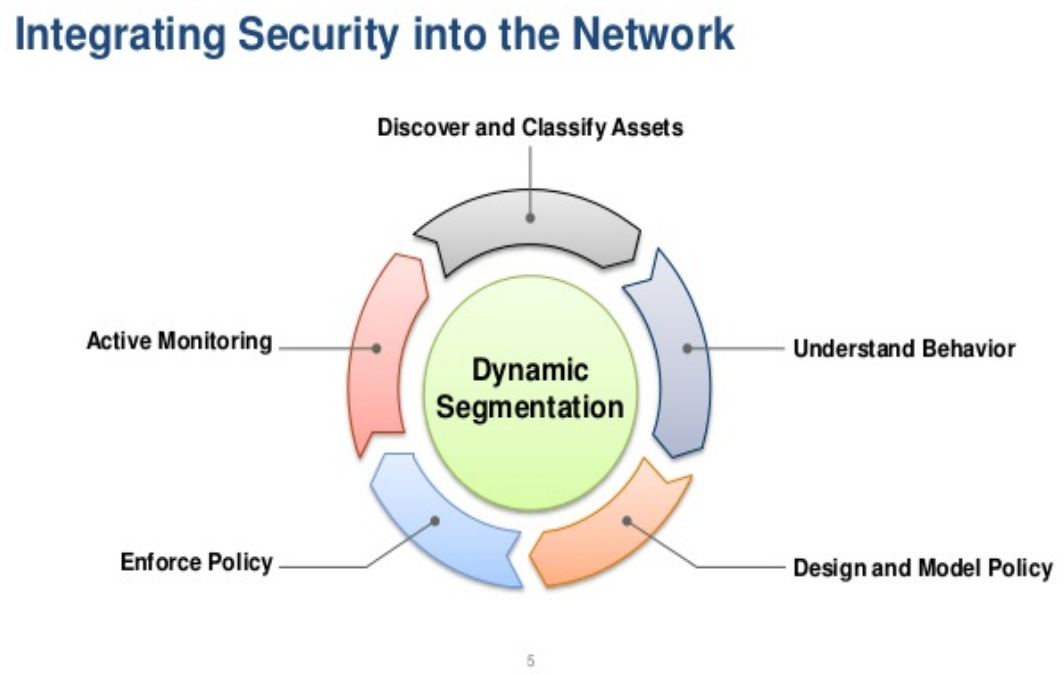

FIGURE 7 - ENFORCE SECURITY POLICY VIA SOFTWARE DEFINED SEGMENTATION (SOURCE: CISCO.COM)

Admittedly, SDS alone is hardly an elixir for IoT security. However, the techniques described in our researches are excellent fits, and they represent a substantial improvement over what is typically implemented in city and ICS networks today. The most considerable advantage these technologies offer is that the industrial end devices do not need to be upgraded to support the new cyber-secure network capabilities. Instead of updating the entire installed complement of end devices, if it is impossible at all, the network infrastructure can be segmented without change the underplaying network infrastructure to deliver higher levels of security.

Business case and financial analysis

City of Lumpkinsville profile

Lumpkinsville is located 20-25 minutes east of Atlanta, a developed suburb and is part of the metro Atlanta area. Over 2,000 businesses operate in the Lumpkinsville area and bring over $1.5 billion in revenue annually. Forbes ranked Lumpkinsville 27th in “America’s Best Places to move in 2010”, while BusinessWeek named it the “Best Suburb in Georgia” in 2011.

The key goal of the town was to propose the transformation of Lumpkinsville to a smart city. The IoT-enabled smart city promises benefits for Lumpkinsville, including rich supplies of data that can help them more effectively serve their residents, businesses, and visitors in addition to improving efficiency of all systems and infrastructure.

City IoT strategic objectives

- Investing IoT technology to improve urban operations such as lighting, parking, and safety and security systems. Reduce cost and increase government transparency by collecting, managing, and analyzing data where it lives. The IoT-enabled network infrastructure allows the city to integrate, visualize, transform, and analyze IoT data across the ecosystem, from edge devices, data centers, or the cloud.
- Improving the overall IoT-enabled smart city security posture and reduce the IoT security risk. Monitoring the IoT digital infrastructure and assets for operations and maintenance, such as malware and attack detection, central IoT security policy enforcement, and fast security incidence response.

Problem statement

As the highly-lauded IoT continues to grow at a stunning pace, IoT-based attacks are already a reality. “The toll continues to rise in the aftermath of a ransomware attack on Atlanta’s computer systems. Since March this year, the city has asked for nearly $15 million to restore its corrupted systems. More than a third of the programs it uses were thrown offline or at least partially disabled. Years of police dashcam footage simply vanished, leaving experts to wonder if the data breach will jeopardize some criminal cases.” (PWC, 2018)

The city of Lumpkinsville main concerns about their IoT-enabled network infrastructure as followed:

- Line of business (LOB), operational technology, and building automation networks that were historically air-gapped are converging onto the city's infrastructure, adding more IoT devices meaning more attack opportunities.
- New IoT devices connected are weak or nonexistent authentication leading to unauthorized accessing the city networks and, thus, exposing citizen data and information and causing city and taxpayer's financial loss.
- No network visibility about who, when, where the IoT devices connected to, and to what network access they are granted into City's network infrastructure.
- For managed devices, the proxy model works well. But they are out of control when those managed devices are not connected to City's corporate network or off-line. Further, for non-managed devices such as BYOD, lacking of malware detection and threat prevention mechanism.

Proposed Solutions

Solution Architecture and Overview

IoT threat defense solutions we proposed for the City of Lumpkinsville tackles the challenge these threats pose to the IoT-enabled digital infrastructure on four critical fronts below.

FIGURE 8 - SOLUTIONS FOCAL POINTS (SOURCE: CISCO.COM)

The first step in developing a defense-in-depth architecture for Lumpkinsville is to take all of the capabilities that can thwart threats and match them up with the city's operational functions, process, and service offering. The IoT security solutions we proposed starts with software-defined segmentation, then visibility and analysis, remote access control, and IoT network service management and automation:

Segmentation using Cisco Identity Service Engine (ISE) and TrustSec

Security typically starts with visibility. However, for the IoT systems segmentation comes first. Intelligence segmentation not only builds a software-defined perimeter to protect what the City has from the known and unknown risks on the existing network, but also keeps these devices out of the reach from attackers for new deployments. Hence, it prevents these devices from being used as pivot points to move through the network if they get compromised.

Capacity Needed	Solution Functions	Solution Components
Identity	Context-based identity of devices and users for access control, including context items such as time of day, location, and security posture.	Cisco ISE
Profile	Profile devices when connected to the network, profiling defines the contextual elements necessary for device classification and categorization.	Cisco ISE
TrustSec	Identity-based software-defined segmentation. Separates IoT systems and users based on role and policy, and stops unknown IoT devices from connecting to the network	ISE, switches, routers, wireless access points and controllers, and firewalls

TABLE 3 - SOLUTION COMPONENTS (SOURCE: CISCO.COM)

Visibility and Analysis using Cisco StealthWatch and OpenDNS

Once the initial level of segmentation is in place for known IoT devices and users, adding layered defense for visibility enables identification of undocumented devices on the network. City gets control for detecting and remediating those threats as all devices become identified and known.

Capacity Needed	Solution Functions	Solution Components
Identity	Context-based identity of devices and users for access control, including context items such as time of day, location, and security posture.	Cisco ISE
DNS Security	Identifies Internet communications from every device on the network based on name resolution, blocks malicious domains, and breaks command & control callbacks.	Cisco OpenDNS
Network Monitoring	Uses infrastructure communication flow information to better pinpoint nuisances in the network, identifies and alerts on abnormal device traffic flows.	Cisco StealthWatch
Analysis and Detection	Analyzes normal IoT network behaviors, creating a baseline for city operations and known devices connected to the network. Generates alerts when abnormal activities start.	Cisco StealthWatch
Intrusion Prevention	Provides IoT visibility with deep packet inspection; blocks attacks, exploitation, and intelligence gathering.	Next generation firewalls
Threat Intelligence	Provides knowledge of existing malware and communication vectors, and learned knowledge of emerging behavioral threats.	Cisco StealthWatch

TABLE 4 - SOLUTION COMPONENTS (SOURCE: CISCO.COM)

Remote Access Control using Cisco AnyConnect and Advanced Malware Protection (AMP)

To maintain City's expensive and sophisticated IoT investments, vendors need to access to their devices remotely for operation and maintenance. Secure remote access replaces the legacy modems and other connectivity methods like physical presence vendors used in the past, eliminating the back doors to the digitally connected network.

Capacity Needed	Solution Functions	Solution Components
Identity	Context-based identity of devices and users for access control, including context items such as time of day, location, and security posture.	Cisco ISE
Virtual Private Network	Provides secure encrypted access for remote operators, vendors, and providers based on role and policies.	Cisco AnyConnect
Anti-Malware	Inspects files for malware and viruses, quarantines and removes any threat quickly before it can spread and contaminate vulnerable IoT systems.	Cisco AMP

TABLE 5 - SOLUTION COMPONENTS (SOURCE: CISCO.COM)

Services Management

All of the capabilities described above help to create a secure IoT network. In preparation for deploying these, it is necessary to fully assess and evaluate the city's environment. We recommend including deployment and incident response services early in the City's IoT projects to ensure the best results possible from the investment. Many of these solutions as followed, such as ISE and StealthWatch design and deployment, are difficult, for the City to accomplish themselves:

- Security penetration assessment
- Automation and control system risk assessment
- Privacy impact assessment
- Incident response services
- Software defined segmentation service

Solution Cost and Benefits

Solutions Cost	
Hardware total	$ 69,180
Support service total	$ 9,284
Subscription total (5 years term)	$ 603,589
Planning and consulting total	$ 66,813
Training	$ 42,761
Total Capital Cost	**$791,627**

TABLE 6 - CAPITAL COST OF THE IOT SOLUTIONS

We recommended the City to consume subscription-based model for the end-to-end solutions proposed for threefold: 1) up-front capital expenditure saving; 2) flexible payment plan for scale up and down as they go; 3) better cash flow management. For example, the total capital cost calculated above is composed of:

Product	Description	Service Duration (Month)	Quantity
ISE-10K	10K endpoint subscription license	60	1
StealthWatch-5K	5K threat intelligence subscription license	60	1
OpenDNS-1K	1K user subscription license	60	1

WLAN 50	50 WiFi access points license for guest		
AnyConnect/AMP 1K	1K user subscription license	60	1

TABLE 7 - CAPITAL COST BREAKDOWN PER PRODUCT

Key Benefits of Solutions:

Simplify access management

- Control access to critical assets by line of business role, device type, and location
- Easily manage access control and segmentation across the city's digital infrastructure

Gain consistent policy across the whole network infrastructure

- Consistently enforce policies across the IoT-enabled network and scale from mobile users to the data center and public cloud
- Centrally apply and enforce consistent policies across wired, wireless, and remote-access users and devices

Reduce operational expenses

- Limit the impact of data breaches and prevent the lateral movement of threats and compromises across city's network with software-defined segmentation
- Reduce the need for costly and time-consuming moves, adds, and change management by automating firewall rules and access control list (ACL) administration
- Easily comply with audits and avoid a costly network redesign to meet compliance requirements

Gain visibility across whole IoT infrastructure

- Gain visibility across all network conversations to detect internal and external threats
- Conduct advanced security analytics and obtain in-depth context to detect a wide range of anomalous behaviors
- Accelerate and improve threat detection, incident response, and forensics across the entire network to reduce security risk

- Enable deeper forensic investigations with audit histories of network activity
- Simplify compliance, network segmentation, performance monitoring, and capacity planning by extending visibility across the network

Financial Analysis and Business as Usual

The City of Lumpkinsville intended for smart city deployment to serve as a catalyst for transforming her capabilities to operate more efficiently and effectively. Therefore, it necessitates for the city to embrace the software-defined perimeter solutions proposed as a way to simplify its IoT digital infrastructure, unify control of things, end-points, edges, and data center & cloud environments, and reduce capital expenses and operating expenses. We recommend implementing the proposed solutions in order to maximize its operational efficiencies, financial return, and city growth while reducing attack surfaces and lowering IoT cybersecurity risk and privacy concerns.

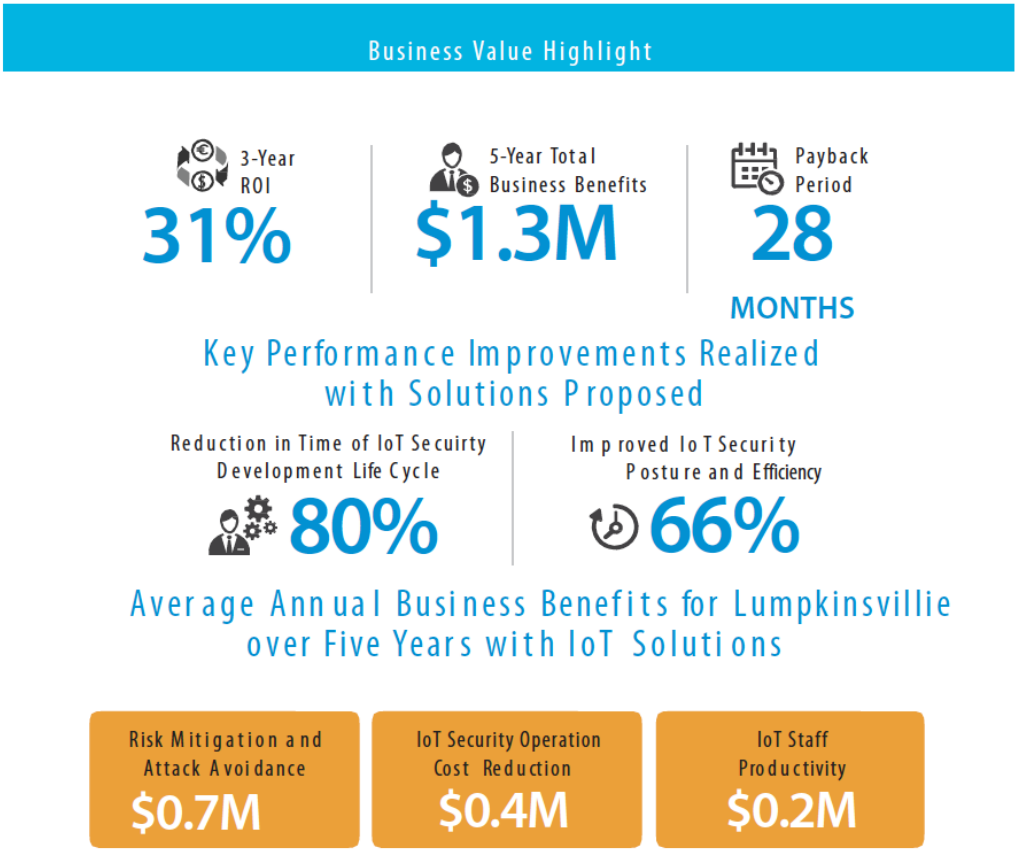

FIGURE 9 - KEY PERFORMANCE IMPROVEMENT REALIZED WITH THE RECOMMENDED SOLUTIONS

Statistics shows that a security breach costs about $ 6 million in average. Atlanta smart city network was lacked down in March this year. Attackers encrypted files, locking employees out of the smart city network completely, while the rest were forced to shut down to prevent the virus from spreading. It is believed that the cyberattack destroyed 'years' worth of police dash cam video footage. The cyber-attack that struck the City of Atlanta in March 2018 could cost taxpayers as much as $17 million, according to The Atlanta Journal-Constitution and Channel 2 Action News.

The IoT industry is still evolving, and there is large potential for zero-day attacks. This offers an opportunity to drive the security at the appropriate layer. The embedded endpoint layer is comprised of highly constrained devices, and so far, has limited the growth of malware to this layer. The growth of IP-based sensors corresponds to attack surface growth. This highlights the fact that new security protocols and identification techniques are required, and IoT endpoint security needs to correlate to its enhanced capabilities. Clearly, IoT presents new challenges to smart city deployments. We have provided a comparative matrix of solutions proposed versus business as usual, let alone the rising issues around privacy & its implications and regulatory compliance.

Comparative Matrix of Solutions			
		Business as Usual	**Propose Solutions**
Functional	Support city growth and smart city deployments	Slow/Siloed	Fast/Central
	Operational risk (low visibility & control)	High	Low
	Operation efficiency and cost	High	Low
	Time to incident response	Length	Fast
	IoT-enabled digital infrastructure	Complexity	Simple
Technical	IoT security service orchestration and automation	Manual/Siloed	Auto/Central
	IoT network visibility and analysis	Low/Siloed	High/Central
	IoT network segmentation	Manual/Perimeter-based	Auto/Software-defined
	IoT security policy and enforcement	Slow/Manual	Fast/Auto
	IoT security monitoring and alerting	Complexity	Simple

TABLE 8 – COMPARISON OF PROPOSED SOLUTIONS VS. BUSINESS AS USUAL

Ethics

There are several ethical concerns associated with smart cities. First and foremost, the data collected from the smart city's infrastructure can be inputted into algorithms and used to flag problems and make decisions based on resident behavior. This introduces the problem of algorithmic fairness that is stemmed from the algorithmic bias associated with that data coming from smart cities. Unfortunately – we are biased beings so data collected from the city's residents and visitors can lead to biased outcomes.

Secondly, data derived from a smart city can be used to make decisions that positively affect one group of residents while compromising the day to day activities and lifestyle of another group. An outcome of a smart city transformation is a reduction in congestion due to the capture of traffic flows and its data being used as insight to effective traffic routing. The changes suggested by such a system to the paths that drivers take through the city could help them get to their destinations faster by using lesser known routes, including bypass lanes, residential areas, etc. That's where we might experience some friction (Gupta, 2018). The increased traffic in "quiet" residential areas might conflict with the current residents in said area. There would need to be balance in how traffic congestion is reduced and the negative impact that may be brought upon to certain communities due to this rerouting. For The City of Lumpkinsville to be a successful smart city with satisfied residents there will need to be a balance between the potential for social good of connected devices that share data with one another and how they affect various demographics.

There is also the question of who will be held responsible if a cyber-attack occurs in a smart city. For the concept of a smart city to come to life there are numerous solution providers involved. Will it be The City of Lumpkinsville or the providers who make the smart city platform and solution possible that are held responsible if a cyber-attack were to occur? Additionally, if the smart city has infrastructure that experiences an outage and issues occur – in the case of a stop light that is improperly programmed

and leads to an accident – will it be the driver of the vehicle who is held responsible or will the responsibility lie on The City of Lumpkinsville?

Smart cities are an emerging technology. We are at the tip of the iceberg and as the technology becomes more prevalent laws and regulations will need to be put in effect to minimize harm, ensure public good as well as establish how various parties and entities will be held responsible and accountable.

Conclusion

With smart cities come a myriad of benefits such as efficiency, cost reduction and environmental sustainability. These benefits are evident in facilities like energy, lighting, transport and water management. These benefits impact residents living in smart cities, business located in these cities and also trickle to visitors.

Despite these benefits there are trepidations associated with this burgeoning technology. Smart cities are privy to tons of data that if put in the wrong hands could cripple the City of Lumpkinsville. With data stolen from a smart city a cybercriminal could not only have access to resident's personal and private information but also gain access to service delivery grids and consumer hardware like meters and valves that could result in the denial of water, gas, or electricity to large population centers. The outcome of a cybersecurity attack would affect the current optimistic outlook associated with this technology, cripple the city's infrastructure and cost the city millions of dollars.

In this proposal we examined the technology behind smart cities, and the cybersecurity ramifications on stakeholders such as residents, businesses, visitors and also examined the ethics associated with them. We provided the City of Lumpkinsville with a layered defense approach to reduce the attack surface and isolate business impacts, enact threat prevention for improving visibility and controls, and set up software defined perimeter/network segmentation with a central security policy

platform for policy enforcement and real-time responses when and if a cyber incident were to occur. Cyber security is a necessary pillar of smart cities as cyber threats are magnified due to the infinite supply of sensitive and private data they are privy to and in order for cities of the future to be smart – they must be safe and resilient.

Annotated Bibliography

Adams, R. (2016, March 25). Is Artificial Intelligence Dangerous? Forbes. Retrieved from, http://www.forbes.com/sites/robertadams/2016/03/25/is-artificial-intelligence-dangerous/#630b4a171d01

Adams explores the current state of artificial intelligence, its future and examines whether or not the technology behind the concept is dangerous.

Cybersecurity of the Internet of Things. (n.d.). Retrieved from https://oversight.house.gov/hearing/cybersecurity-internet-things/

Hearing held on October 3, 2017 that examines the use of devices that comprise the Internet of Things (IoT) and their current and potential uses in federal government, explores potential cyber threats posed by the use of IoT devices and reviews private sector recommendations for securing the IoT, and explore potential legislative solutions.

Cisco IoT Security. (2018, September 26). Retrieved from https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-security.html

Cisco IoT Security allows users to defend against IoT threats, gain visibility and control as well as simplify compliance.

Cisco TrustSec Accelerates and Simplifies Network Security Solution Overview. (2017, June 23). Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution-overview-c22-737173.html

Cisco TrustSec solution overview. Cisco TrustSec helps organizations protect their most critical assets from malware and bad intent by controlling access to your applications, equipment, and users.

Etherington, D., & Conger, K. (2016, October 21). Large DDoS attacks cause outages at Twitter, Spotify, and other sites. Retrieved from https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

Etherington and Conger explore distributed denial of service (DDOS) attack on the DNS provider Dyn that affected websites such as Twitter, SoundCloud, Spotify, Shopify and left websites inaccessible to users. The attack came from the Mirai botnet, a network of infected Internet of Things devices used in other recent large-scale DDoS attacks

Forbes, H. (n.d.). Software-defined Industrial Networks Deliver Cybersecurity Breakthroughs. Retrieved from https://www.arcweb.com/blog/software-defined-industrial-networks-deliver-cybersecurity-breakthroughs

Forbes explores SDN protocol and OpenFlow - two promising software-defined networking (SDN) technologies recently applied in industrial control systems that may deliver substantial improvements in the cybersecurity of both new and existing industrial control systems.

Gupta, A. (2017, August 06). What Cyber Threats Are Smart Cities Facing? An in-depth look . . . Retrieved November 23, 2018, from https://newcities.org/the-big-picture-ai-smart-cities-privacy-trust-ethics

Gupta explores privacy, trust and the ethics surrounding smart cities and how technical experts, urban planners, residents, city officials represented from all parts and demographics of cities is going to be crucial in the safe and inclusive push towards turning our cities into smart cities.

IoT Framework Assessment. (2016, May 14). Retrieved from https://www.owasp.org/index.php/IoT_Framework_Assessment

Explores specific security related concerns of typical IoT system archetypes – gates, gateway, cloud platform and mobile.

IoT Threat Defense for Manufacturing SAFE Design Guide. (2018, May). Retrieved from https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/iot-threat-defense-mfg-design-implementation-guide.pdf

Solution overview of Cisco's IoT Threat Defense solution takes an architectural approach to protecting IoT using the SAFE model for security. Design guide details components and configurations that can be used to valid architecture.

Jain, H. (2016, November 24). Managing the Attack Surface of a Smart City. Retrieved from https://www.fortinet.com/blog/industry-trends/post-mirai-managing-the-attack-surface-of-a-smart-city.html

For a smart city to work cities will need to deploy plenty of IoT devices and services for metering, sensing, and controlling. The increase in the size of a smart city's IoT device footprint corresponds to an increase in the size of its attack surface. In this article Jain explores how to manage the attack surface of a smart city.

JustinGopinath, N. Y. (n.d.). DDoS Mitigation using Software Defined Network. Retrieved from http://www.ijettjournal.org/2015/volume-24/number-5/IJETT-V24P246.pdf

JustinGopinath explores software defined networks and configurations that resist DDOS attacks, balance throughput, minimizes response time and avoid overload.

Kiertzner, H. (2018, June 14). The first step in ensuring cybersecurity: Understanding what's normal. Retrieved from https://na.smartcitiescouncil.com/article/first-step-ensuring-cybersecurity-understanding-whats-normal

Kiertzner explores how cities can address the security of their systems through analytics which will assist with maintaining service delivery and public safety in the face of cyberattacks while reducing mean time to detect and mean time to respond.

Maddox, T. (2016, August 1). Smart Cities: 6 Essential Technologies. Retrieved November 23, 2018, from https://www.techrepublic.com/article/smart-cities-6-essential-technologies/

Maddox explores the key technologies that comprise a smart city – 1) Smart Engergy 2) Smart Transportation 3) Smart Data 4) Smart Infrastructure 5) Smart Mobility 6) Smart IoT Devices and how these technologies work together to make a smart city even smarter

National Institute of Standards and Technology. Cyber-Physical Systems (CPS) Framework Release 1.0 (n.d.). Retrieved from https://pages.nist.gov/cpspwg/

The CPS Framework Release 1.0 has been prepared by the Cyber-Physical Systems Public Working Group (CPS PWG), an open public forum established by the National Institute of Standards and Technology (NIST) to support stakeholder discussions and development of a framework for cyber-physical systems.

National Institute of Standards and Technology. Building Security into Cyber-Physical Systems (n.d.). Retrieved from https://www.nist.gov/news-events/news/2016/05/building-security-cyber-physical-systems-nist-researchers-suggest-approach

NIST researchers suggest approach for trustworthy modern infrastructure and explore how to build security into cyber-physical systems. Ways to incorporate time-tested security design principles and concepts into these systems at every step, from concept to implementation are examined.

Raza, K. (2016, December 01). How to architect the network so IoT devices are secure. Retrieved from https://www.networkworld.com/article/3146090/internet-of-things/how-to-architect-the-network-so-iot-devices-are-secure.html

Raza explores the networks behind smart cities and examines the changes that will need to be made in branch and site location architectures to mitigate the threat of large-scale attacks that hijack IoT devices.

Perkins, E., Contu, R., & Alabeyi, S. (2017, November 14). The Death of IoT Security as You Know It. Retrieved from https://www.gartner.com/doc/reprints?id=1-4KQ5GVY&ct=171117&st=sb

Perkins, Contu & Alabeyi explore the death of IoT security which has resulted in major changes to skills development, organizational structure, service selection, risk management and other decision processes.

PricewaterhouseCoopers. (n.d.). Smart cities: Five smart steps to cybersecurity. Retrieved November 23, 2018, from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/smart-cities.html

Price Waterhouse Coopers investigates the steps needed to make smart cities fortified for cybersecurity attacks as well as describes the burgeoning vulnerabilities associated with smart cities.

Securing the Internet of Things: A Proposed Framework. (2016, December 16). Retrieved from https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

Cisco explores challenges in traditional IoT frameworks and proposes a flexible security framework that is comprised of four components: authentication, authorization, network enforced policy and secure analytics.

Securing industrial IoT: Spotlight on DMZ and segmentation. (n.d.). Retrieved from http://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/Securing-industrial-IoT-Spotlight-on-DMZ-and-segmentation

Bhattacharjee describes breakdown of critical infrastructure and human safety that could occur if a cybersecurity attack targeted a smart city. Bhattacharjee also explores how to secure IoT backed smart cities with segmentation and DMZ (also known as perimeter network) for plausible rescue.

Security in a Converging IT/OT World. (2016, November). Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/security-converging-it-ot-world-37382

This paper looks at the challenges in securing ICS environments and recommendations for effective ICS security. Explores fundamentals such as controlling access to devices and applications; monitoring networks to identify potential issues and direct appropriate responsive action; oversight and periodic reviews of controls and their effectiveness; securing the supply chain; and securing the human factor through awareness training.

Shahan, R., & Lamos, B. (2018, October 8). IoT Security Architecture. Retrieved from https://docs.microsoft.com/en-us/azure/iot-fundamentals/iot-security-architecture

Shahan and Lamos explore how to identify potential threats when designing a system and when to add appropriate defenses accordingly, as the system is designed and architected.

Smart Cities Need Smart Security. (n.d.). Retrieved from http://www.itone.lu/actualites/smart-cities-need-smart-security

Explores the risks associated with smart cities, the infrastructures that power them and makes recommendations on what can be done to minimize cybersecurity risks associated with the networks that power smart cities and the volumes of data they produce.

Software Defined Perimeter. (n.d.). Retrieved from https://cloudsecurityalliance.org/working-groups/software-defined-perimeter/#_overview

To solve the problem of stopping network attacks on application infrastructure the SDP Workgroup developed a clean sheet approach that combines device authentication, identity-based access and dynamically provisioned connectivity.

Solution Overview: Cisco Stealthwatch Improves Threat Defense with Network Visibility and Security Analytics. (2018, September 19). Retrieved from https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/solution-overview-c22-736505.html

Solution overview of Cisco Stealthwatch which collects and analyzes data to give dynamic networks comprehensive internal visibility and protection. Allows teams ability to gain real-time situational awareness of all users, devices, and traffic on the extended network so they can quickly and effectively respond to threats.

The 10 Most Vulnerable IoT Security Targets. (2017, May 31). Retrieved from http://www.ioti.com/security/10-most-vulnerable-iot-security-targets

Internet of Things is exponentially increasing the number of potential targets for cyber-criminals. In this article Buntz goes into detail on the potential targets in a smart city environment with an accompanying poll.

Uncovering the potential of the Internet of Things. (n.d.). Retrieved from https://www.pwc.ru/ru/assets/pdf/gsiss-the-internet-of-things-eng.pdf

Describes how IoT is poised to transform business models of Russian companies. Examines how establishing an integrated cybersecurity and privacy program is key to businesses realizing the potential advantages of IoT as it evolves.

Zimmerman, T., & Pace, B. (2018, May 14). IoT Solutions Can't Be Trusted and Must Be Separated From the Enterprise Network to Reduce Risk. Retrieved from https://www.gartner.com/document/3874933?ref=solrAll&refval=212170019&qid=

Scholars from Gartner argue that IoT solutions can't be trusted and must be separated from the enterprise network to reduce risk. The approach suggests the infrastructure and operations (I&O) leaders deploying IoT on their infrastructure should consider.