SECURING
SMART
CITIES

cloud
CSA security
alliance℠

Cyber Security Guidelines for Smart City Technology Adoption

AUTHORS:

Cesar Cerrudo

CTO, IOActive Labs

Amin Hasbini,

Senior Security Researcher, Kaspersky Lab

Brian Russell,

Chief Engineer, Leidos

CONTRIBUTORS:

Claudio Cracciolo, Giorgio Fedon, Ayoub Figuigui, David Jordan, Sabri Khemissa, Cédric Lévy-Bencheto, Ryan Naraine, Murray Rosenthal, Alan Seow, Ivan Shadrin, Shyam Sundaram, Arvind Tiwari

SECURING SMART CITIES

cloud security alliance SM

Table of contents

1 Introduction

Interest in the smart city concept has grown continuously over in the past few years, with top research being done in the Internet of Things (IoT) and urban domains to define, assess, and improve smart city services and offerings. In smart cities, information security plays a major role in protecting the higher levels of confidentiality, availability, and integrity as well as the stability that national services and organizations need to support sustainable and livable smart environments.

According to the Institute for Electrical and Electronics Engineers (IEEE), "a smart city brings together technology, government and society to enable the following characteristics: a smart economy, smart mobility, a smart environment, smart people, smart living and smart governance." This can be realized using a wide range of connected systems to process and exchange data between multiple stakeholders, including transportation, energy, and city services. As new points of connection are introduced throughout a city, having processes to methodically evaluate the security risks and appropriate mitigations for each connected system is critical to the success of the smart city.

The purpose of this document is to provide guidelines for public and private organizations when planning and organizing the selection and validation of smart city technologies. It describes the types of testing and assessments to consider in order to select the best and most secure vendors and technologies.

This guide is not a detailed information security testing or assessment program, but rather an overview of the key elements that organizations need to look for in order to implement the best technological solutions with a lower risk and exposure to cyber threats.

2 Cyber-security Guidelines

The following cyber-security guidelines provide practical recommendations for selecting, implementing, maintaining, and disposing of solutions both during and after the process of acquiring new smart technologies. It is important to note that a smart city solution is composed of many components and is typically designed to communicate with many other similar solutions. The building blocks of any particular solution can include the hardware components of the edge devices and gateways, the technology stacks deployed to each device (e.g. real-time operating system, application software, and messaging and communication protocols), the services that the devices communicate with, and the backend infrastructure that supports data analysis and storage. The complexities of these smart solutions drive new and unique threats, and while some vendors may try to package and sell turnkey solutions, city users will often have to integrate different solutions to meet their mission goals.

2.1 Technology Selection

Technology selection is when organizations want to find a solution that will be implemented on a city-wide scale. Examples include traffic management, street lighting, parking, sensors, utilities, public health, and transportation systems. The technology selection phase is the most important, as technology should be chosen with proper cyber security controls and protections in mind. If organization sonly consider the desired functionality, it could open city infrastructure up to possible cyber attacks.

2.1.1 Design and Planning Stage

Most business-oriented leaders look for solutions that provide maximum functionality and features for the organization and its client. This is not necessarily a bad thing, provided that the technology is really safe. While such a concern is not currently a game-changer, too many organizations are buying technology without requiring any security testing and with limited security requirements (if any). Organizations are blindly trusting vendors, and this must be addressed to stop vulnerable and insecure technologies from being deployed into production. In a smart city environment, weak services could cause large-scale damage, even affecting national stability and security. A smart city requires new levels of confidentiality, integrity, availability, and defense.

Municipalities and service providers implementing smart city solutions should take a methodical approach to evaluating the security posture of the products and services they procure for their city. Establishing proper security engineering practices, such as threat modeling, is an essential step in understanding the unique risks that apply to each particular smart city implementation. Organizations should perform a risk assessment, using an appropriate threat modeling, in order to define the minimum security requirements that meet their needs.

Smart city solutions should be expected to comply with basic security requirements such as:

- **Strong cryptography to protect data, both at rest and in transit:** All wired and wireless communications (data in transit) should be properly protected with strong encryption. Systems dealing with sensitive data should provide a mechanism to encrypt data at rest.
- **Authentication capabilities:** All systems should require a username and password to access functionality, at a minimum. To enhance authentication capabilities, the solution should support strong authentication mechanisms (one-time passwords, certificate- or biometric-based authentication, etc.).
- **Authorization capabilities:** All functionality should require and enforce proper permissions before performing any actions.
- **Automatic and secure update of software, firmware, etc.:** Software/firmware update mechanisms should be available, and updates should be delivered in an automatic and secure way.
- **Auditing, alerting, and logging capabilities:** All systems should provide mechanisms for auditing and logging security events. Logs must also be saved securely against tampering.
- **Anti-tampering capabilities:** Devices should have a mechanism to prevent tampering by unauthorized sources.
- **No backdoor/undocumented/hardcoded accounts:** Some vendors release systems with backdoor/undocumented/hardcoded accounts. Often, these accounts cannot be removed or disabled and have passwords that cannot be changed, allowing anyone to compromise the system using these accounts. Removing or disabling these accounts should be enforced in the service-level agreement (SLA) to ensure vendors will comply.
- **Non-basic functionality disabled by default:** Only basic functionality should be enabled by default, and the rest should be enabled depending on the organization's needs.

- **Fail safe/close:** In the case of a system malfunction or crash, the system should remain secure and security protections remain enforced.
- **Secure by default:** Solutions should come with a secure configuration by default.

There are numerous details to consider when discussing the implementation of cryptography within a smart city solution. Organizations should always consult relevant best-practices for guidance on how to use and manage the keys and certificates used by devices and services, and ensure that the vendors' solutions support state-of-the-art cipher suites and protocols. The organization should also discuss cryptographic provisioning options with the solution provider.

Another method to guarantee that smart solutions have appropriate security features is to have vendors commit to certain SLAs such as:

- An agreement about the specific security features of the product. There should be a clear understanding that the absence or malfunction of these features could have legal and/or financial consequences for the vendor.
- An agreement that the vendor will provide continuous (24/7/365) 'reliability tested' support for security incidents related to its products. There should be a defined and limited timeframe during which vendors must provide solutions when security flaws are found. There should be a clear understanding that non-compliance could have legal and/or financial consequences to the vendor.
- An agreement that vendors prove their compliance to security requirements through third-party testing, certifications, etc.

To provide enhanced security awareness, organizations should include physical security in their planning. Physical security includes safeguards that take into consideration where the devices are located during operation, what security controls the devices feature (e.g. tamper resistant or tamper evident), and the sensitivity of the data processed by devices.

Next, organizations should establish a baseline for auditing the smart city system's behavior. This includes identifying the audit capabilities of each device and system and determining if they need to be supplemented with other audit-capture devices such as gateways (to oversee traffic flowing to/from the edge). The organization should identify and document the normal

operating thresholds for each device and system type and determine what variance should trigger an alert and the criticality of that alert.

Organizations need to establish an authentication/authorization plan for their smart city solutions. The roles and services of each device type should be documented, and the roles that will service the devices (e.g. maintenance or security) need to be clearly differentiated. There should be an established access control matrix for each device and a plan for federated access to the devices. Also, organization need to develop an information sharing plan which specifically describes what data can be shared and with whom (persons, systems, other devices) as well as the required privacy controls for that data. This plan should strongly consider whether data in aggregate opens any additional privacy concerns.

2.1.2 Vulnerability History

A vendor's customer product deployment history (previous deployments) is a good indication of the maturity of its products, however, the vulnerability history (e.g. CVE data, vulnerability advisories, etc.) can tell a lot about its priorities. Vulnerability histories reveal:

- Security maturity (how long the vendor has been concerned about security exposure)
- The number of flaws, and if that number is trending up or down
- The type of flaws as well as their severity and impact (this could indicate the company's software development habits)
- The evolution of the product's security as compared to the competition
- The amount of time a vendor takes to patch security vulnerabilities and how easy it is to apply the patches

2.1.3 Vendor Security

Requesting details about how a vendor protects its own products, infrastructure, and operations can provide a certain amount of assurance regarding the safety of the vendor's products and their future.

- How does the vendor test its products and simulate large-scale environments to verify its product's usability?
- How does the vendor protect its own infrastructure from attacks and intellectual property leaks?
- Does the vendor adequately protect its development environment and intellectual property from spying or manipulation?
- Does the vendor implement policies and procedures that require independent entities to test its infrastructure for security flaws and backdoors?
- Does the vendor run regular independent code reviews and penetration tests on its products, networks, and systems?
- How does the vendor protect details about its clients, such as design details, product lists, and client contact information?
- Does the vendor have a Secure Development Life Cycle (SDLC) program? If so, how long has it been running?
- Does the vendor enforce supply-chain cyber security to prevent the delivery of products with malware, backdoors, etc.?
- Does the vendor have a public security vulnerability disclosure and reporting policy and proper contact channels to get the vulnerability reports?
- Does the vendor have support teams for security issues/incidents, such as a Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), online support, etc.?

The contract with the vendor must include an audit clause for one security assessment per year at a minimum. The goals are to:

- Verify the answers to the previous questions when the vendor is selected.
- Maintain a high-level of security for the solution being delivered throughout the contract period.

2.1.4 Product Management

For security to be applied and verified, visibility is crucial. Powerful solutions need powerful management interfaces that monitor operation status and stability, correlate logging

activities, and are compatible with multiple devices and sources. Centralized management of smart solutions simplifies the process of safely operating smart services and enables the engineers to focus on important tasks without being overwhelmed with information.

- Evaluate the security impact when integrating a new product to the current system.
- Deploy specific measures to ensure security requirements for the integration of new products (i.e. network segregation, monitoring of specific KPI, etc.).

2.1.5 Testing

Organizations adopting smart technologies should verify vendors' claims about the security features of their products. Solutions should be audited for security vulnerabilities, weak security protections, and compliance with the basic security requirements detailed in section

2.1.6. Organizations should develop a complete security test bench for verification:

- **Basic security requirements compliance:** Organizations should verify that products comply with the basic security requirements detailed in section 2.1.1.
- **Penetration testing:** Penetration testing is a recommended method for verifying the security of smart city products. When faced with real-world attacks, services could misbehave, leak data, or even crash.
- **Hardening:** System hardening needs to be verified. Non-production services are not expected to be reachable from a network perspective and solutions processes should be running in isolated sandboxes that are available only to restricted users (blocking permission escalation attacks if successful).
- **Certification:** In smart cities, certification authorities could be available to evaluate products and solutions on behalf of organizations. These certifications could be used to support decision-making, but the testing scope and procedures should be verified. They should not be used exclusively, as the results could be wrong or misleading.
- **Operational security verification and validation:** Validate security processes are running correctly and that the right audit data is being captured.

If organizations want to outsource security testing, the safety requirements of their suppliers should be as high as those applicable to technology vendors.

2.2 Technology Implementation, Operation, and Maintenance

2.2.1 Implementation

When an organization's professionals or third parties implement technology, it is important to deploy systems in a secure way. Organizations should ensure:

- **Technology passed selection phase security tests (2.1.5):** Before implementing specific technology, the same model, version, etc. must have passed security testing.
- **Technology was securely delivered:** It should have not tampered with, modified, etc. from the time it was shipped from the solution provider. Binaries should be cryptographically signed, and devices should have not been tampered with.
- **Enable strong encryption:** All communications should be properly protected against unauthorized eavesdropping, interception, and modification. Encryption keys must be well protected and kept in a safe place.
- **Secure system administration:** Avoid using a single administrator system user to perform all actions on all systems. Use different administrator users and passwords and grant granular permissions.
- **Set strong passwords**: All access to administration interfaces, functionality, etc. should require a user account with a strong password. Passwords policy must be defined for password strength and duration validity. To enhance authentication capabilities, use strong authentication mechanisms (one-time password, certificate- or biometric-based authentication, multifactor authentication, etc.) especially any technology that can impact public safety.
- **Remove unnecessary user accounts:** Some solutions come with test/default accounts and passwords that could be used by unauthorized parties to access the systems, if these accounts are not removed. Specific accounts can be created for the implementation process, but these accounts must be removed after the solution is installed and not used for operation purposes. These accounts should be identified in the product and implementation documentations for easy identification and removal.
- **Disable unused functionality and services:** Some solutions have all functionality and services enabled by default. Disabling unused functionality and

services reduces the attack surface and prevents possible attacks that abuse weaknesses in those functions and services.

- **Enable auditing of security events:** Constantly monitoring audit logs will help to identify ongoing attacks and breaches.
- **Add anti-tampering, anti-vandalism mechanisms:** Devices should be protected against unauthorized physical access for modification, vandalism, or device stealing.

2.2.2 Operation and Maintenance

Once a solution has been implemented in a smart city, continuous support, tracking, and monitoring is a must. The following list of requirements support safe operation:

- **Monitoring:** Organizations are expected to monitor the stability of the services, tracking any suspicious activity, abnormal behavior, performance hooks, or any other service-threatening events by regularly reviewing system audit logs and/or other available mechanisms.
- **Patching:** Organizations and vendors are expected to collaborate on deploying the latest security patches. Patches should be deployed per the company's patch management policies, taking into account the urgency of the patches. Patches are expected to be tested in the lab environment first. There are challenges associated with patching IoT devices when compared to traditional enterprise IT systems. Often it is the device firmware that must be updated. When doing so, make sure that the firmware update mechanisms deliver the updates in a secure manner—that is with encryption and a digital signature.
- **Regular assessment and auditing:** Testing smart services is also expected to run continuously to verify service compliance with the applicable standards and security policies (i.e. make sure encryption remains turned on, authentication enabled, strong passwords set, security settings not changed, etc.). Every day, vulnerabilities and exploits are announced and published; being ready to respond is imperative to protecting infrastructure. Testing services is especially relevant after applying new changes to the systems, where simulating a large-scale live environment might not be possible, and testing changes might only be possible in the production environment.
- **Protection of logging environment:** All logs should be safely transmitted and stored. The integrity and protection of evidence is critical to investigating misbehavior, tracking incidents, and legal liability. Logging should occur as close to the end-device as possible, although it may not be possible to collect or routinely forward data at

some disadvantaged devices. In these instances, maintaining situational awareness through data collection at IP propagators such as WiFi or other protocol routers, gateways, and standard network security devices should be evaluated.

- **Access control:** Appropriately monitoring who, when, and how someone has access to smart service systems is critical to prevent unplanned changes, tampering, or downtime, which are not acceptable in smart city environments.

- **Cyber-threat intelligence:** Threat intelligence enables an organization to identify regional and worldwide occurrences, such as new, trending, common, and regional attacks. Armed with such information, an organization can update its security posture and parameters as needed to block attacks before they happen. Many examples have proven that the same attacks are replicated and the same vulnerabilities are reused. Cyber-threat intelligence could also be used on a country-level by the government, where certain traffic patterns and source locations could be blocked upon need on the regional Internet gateways, protecting all organizations within.

- **Compromise reaction and recovery:** It is important to create detailed procedure manuals or checklists that define what must be done if a smart city system is compromised. This includes things like certificate revocation, key zeroization, and systems isolation and clean up, as well as how to follow up on the incident in order to understand how the system was compromised and develop plans so that it will not happen again.

2.3 Technology Disposal

Smart city technologies are complex. Organizations plan for them, implement them, and then on a certain day in the future, they need to dispose of them. Multiple factors need to be considered when performing technology disposal. It is important for organizations to develop specific policies for securely disposing of technology, keeping the following in mind:

- **Avoid repurposing technology** by the same organization or third parties. It could leak sensitive design, client, password, or cryptographic information, which could create a threat to production services.

- **Securely erase data** on systems storage. This is a good measure to apply, but destruction of storage may be required to assure the safe, quick disposal of critical data.

- **Vendor replacement is also important.** While many organizations think about the disposal of data correctly, a vendor's maintenance and support personnel could easily access smart service systems to perform regular maintenance activities. If they

replace hardware, the vendor could repurpose it at other clients or dispose of it without appropriate security measures. Hardware that is removed from live environments by support personnel is not usually protected. Vendors are expected to provide secure technology disposal as part of their services and maintenance contract with the client organization.

2.4 Conclusion

In this paper, we have highlighted important security guidelines for the selection and operation of smart city technologies. We hope that this expert guidance will be followed by organizations migrating their operations and services to a smart city scale. In the future, numerous cyber threats are expected to plague smart cities. At the same time, tolerance to cyber damage is minimal, in a smart city "one is too many." This document provides guidelines that support a certain level of assurance and bring trust to operations and services. Our goal is to help organizations minimize problems and downtime in the hope of encouraging smart services to be deployed with high reliability and availability.

About Securing Smart Cities

Securing Smart Cities is a not-for-profit global initiative that aims to solve the existing and future cybersecurity problems of smart cities through collaboration between companies, governments, media outlets, other not-for-profit initiatives and individuals across the world.

Learn more at **securingsmartcities.org**

contact@securingsmartcities.org

Twitter: @SecuringCities

LinkedIn

About Cloud Security Alliance (CSA)

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud – from providers and customers, to governments, entrepreneurs and the assurance industry – and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA operates the most popular cloud security provider certification program, the CSA Security, Trust & Assurance Registry (STAR), a three-tiered provider assurance program of self assessment, 3rd party audit and continuous monitoring.

CSA launched the industry's first cloud security user certification in 2010, the Certificate of Cloud Security Knowledge (CCSK), the benchmark for professional competency in cloud computing security.

CSA's comprehensive research program works in collaboration with industry, higher education and government on a global basis. CSA research prides itself on vendor neutrality, agility and integrity of results.

CSA has a presence in every continent except Antarctica. With our own offices, partnerships, member organizations and chapters, there are always CSA experts near you. CSA holds dozens of high quality educational events around the world and online. Please check out our events page for more information.

Contact Info

General inquiries: info@cloudsecurityalliance.org
Membership information: membership@cloudsecurityalliance.org
Media inquiries: pr@cloudsecurityalliance.org
Website: webmaster@cloudsecurityalliance.org