UNIVERSIDAD D CÓRDOBA

Instituto de

Estudios de Posgrado

Máster en Inteligencia Computacional e Internet de las Cosas

Curso: Ciberseguridad

Proyecto

Ciberseguridad y Smart city

Autor. Artem Mozhegov

FEBRERO - 2023

Índice general

Capítulo 1

Introducción

La urbanización y el desarrollo de las tecnologías de la información han hecho inevitable la aparición de un fenómeno como la Smart City. Al mismo tiempo, la informatización de la sociedad abre no solo nuevos horizontes para el desarrollo de la sociedad, sino que crea aquellos peligros que antes no existían. La ciberseguridad está diseñada para combatir los efectos secundarios negativos del desarrollo de la sociedad digital.

En este trabajo se estudia como ya se ha mencionado, la influencia de las tecnologías de la información y los riesgos que conllevan. En otras palabras, el aprovechamiento de la simbiosis de la ciberseguridad y el concepto Smart City para el pleno desarrollo de la sociedad. Para ello, se darán definiciones de los principales conceptos, se estudiarán las últimas tecnologías del concepto Smart City y los riesgos asociados. Luego se describirán métodos para la resolución de problemas en el campo de la ciberseguridad. Para una mejor comprensión de la trayectoria de desarrollo de los procesos, se describirá el desarrollo previo tanto de Smart City como de Ciberseguridad. En conclusión, se realizarán previsiones sobre las perspectivas de desarrollo de ambos conceptos y el posible impacto en el desarrollo posterior de la sociedad.

Capítulo 2

Objetivos

2.1 Objetivo principal

El objetivo principal de este proyecto, como ya se ha mencionado anteriormente, es el de estudiar qué es la simbiosis de Ciberseguridad y Smart City y cómo afecta el desarrollo de la sociedad.

2.2 Objetivos específicos

Los objetivos teóricos de este trabajo son los siguientes:

- Estudio del desarrollo antecedente de los conceptos de Ciberseguridad y Smart City.
- Estudio de los riesgos asociados al desarrollo de Smart City.
- Estudio de la necesidad de implantar la Ciberseguridad en Smart City.
- Estudio de las perspectivas de desarrollo de Ciberseguridad y Smart City y su impacto en la sociedad.

Capítulo 3

Desarrollo antecedente

La idea y la existencia de ciudades inteligentes es relativamente nueva. Está estrechamente relacionado con el rápido desarrollo reciente de la tecnología de la información. El concepto de ciudad inteligente se centra en el uso de computadoras por parte de una ciudad para resolver problemas urbanos. El uso del análisis estadístico computacional por parte de la Oficina de Análisis de la Comunidad (Community Analysis Bureau) en Los Ángeles a fines de la década de 1960 y el establecimiento por parte de Singapur de la Junta Nacional de Computación (National Computer Board) en 1981 se citan como algunas de las primeras intervenciones cibernéticas en la planificación urbana.

El concepto de ciudad inteligente (Smart City) implica la integración profunda de las tecnologías digitales con un paisaje nuevo o existente de un ecosistema complejo de servicios municipales metropolitanos, empresas públicas y privadas, personas, procesos, dispositivos, sensores e infraestructura urbana que interactúan constantemente.

La necesidad de implementación de la ciberseguridad se estudiará en el Capítulo La necesidad de implementar la Ciberseguridad en Smart City. Ahora es el momento de aprender qué es la ciberseguridad.

De acuerdo con la Ley de seguridad cibernética de 2018 de la República de Singapur,

"**ciberseguridad**" significa el estado en el que una computadora o sistema informático está protegido contra accesos o ataques no autorizados, y debido a ese estado:

A. la computadora o sistema informático continúa siendo disponible y operativo;
B. se mantiene la integridad de la computadora o del sistema informático;

C. se mantenga la integridad y confidencialidad de la información almacenada, procesada o transmitida a través de la computadora o sistema informático;

Asimismo,

"**incidente de ciberseguridad**" significa un acto o actividad llevado a cabo sin autorización legal en o a través de una computadora o sistema informático que pone en peligro o afecta negativamente su ciberseguridad o la ciberseguridad de otra computadora o sistema informático.

Las ciudades deben desarrollar una estrategia detallada de ciberseguridad que sea consistente con su estrategia general de desarrollo, lo que ayudará a mitigar los problemas que surgen de la convergencia e interacción de los sistemas y procesos de la ciudad. Por ejemplo, una visión holística de los riesgos asociados a los procesos tecnológicos y el conocimiento de la interdependencia de los activos críticos permitió a Singapur, como parte de la estrategia de "nación inteligente", lanzar un Plan Maestro de Seguridad Cibernética en 2013, en 2016 para desarrollar una de las mejores estrategias nacionales en esta materia en la actualidad, y en 2018 aprobar la Ley de Ciberseguridad, la cual es considerada un estándar de nueva generación para la protección de infraestructuras de información clave, lo que la convierte en objeto de estrecha atención de profesionales de diversas áreas.

Los componentes tecnológicos básicos de una ciudad inteligente constan de 3 capas:

- Capa de sensores y actuadores,
- Capa de red,
- Capa de gestión.

La capa de sensores y actuadores incluye miles de millones de sensores, cámaras conectadas a dispositivos de Internet de las cosas (IoT), dispersos por toda la ciudad (contadores inteligentes de gas, agua y electricidad, dispositivos médicos inteligentes y dispositivos de seguridad contra incendios, sensores meteorológicos, etc).

La capa de red es una red que conecta dispositivos entre sí. Entre tales dispositivos se encuentran sensores y teléfonos móviles y computadoras personales de los usuarios. Esta capa usando tecnologías como Bluetooth, 5g, Wi-Fi, etc proporciona un intercambio de datos en tiempo real constante, casi instantáneo, entre varios componentes del ecosistema de la ciudad inteligente.

En la tercera capa se procesan los datos recibidos de los sensores y de los usuarios. El procesamiento de datos se puede llevar a cabo tanto automáticamente como por especialistas. Los datos recibidos se almacenan en los servidores.

Así, en las Smart Cities, las TI penetran en todos los ámbitos de la vida humana. Las personas y los dispositivos se integran entre sí mediante la tecnología de la información.

Capítulo 4

Riesgos de Smart city

La introducción masiva de sistemas de información en la gestión de los recursos urbanos aumenta la eficiencia de los servicios municipales, brinda a los ciudadanos beneficios económicos, sociales y culturales sin precedentes que afectan significativamente su calidad de vida. Al mismo tiempo, la digitalización de la ciudad genera una gran cantidad de desafíos, riesgos y amenazas que, si son implementados por ciberdelincuentes, pueden traer un caos irresistible al soporte vital de las aglomeraciones urbanas.

Clasificación	Ejemplos de incidentes	Descripción / Ejemplos
Contenido abusivo	Spam	Correo no deseado
	Habla dañina	Acoso cibernético, racismo o amenazas
	Contenido sexual/violento	Exaltación de la violencia
Código malicioso	Sistema infectado	Sistema infectado con malware
	Servidor C2	Servidor de comando y control contactado por malware en el sistema infectado
	Distribución de malware	URI utilizado para la distribución de malware

	Configuración de malware	URI que aloja un archivo de configuración de malware
Recopilación de información	Scanning	Ataques que envían solicitudes a un sistema para descubrir debilidades
	Sniffing	Observación y registro del tráfico de red
	Ingeniería social	Recopilación de información de un ser humano de una manera no técnica
Intentos de intrusión	Explotación de vulnerabilidades conocidas	Un intento de comprometer un sistema o interrumpir cualquier servicio mediante la explotación de vulnerabilidades
	Intentos de acceso	Múltiples intentos de inicio de sesión de fuerza bruta
	Nueva firma de ataque	Un ataque usando un exploit desconocido
Intrusiones	Compromiso de cuenta privilegiada	El atacante obtiene privilegios administrativos
	Compromiso de cuenta sin privilegios	Usar una cuenta sin privilegios
	Compromiso de la aplicación	Explotar vulnerabilidades de software (des)conocidas
	Compromiso del sistema	Inicios de sesión o comandos no autorizados
	Robo	Intrusión física

Disponibilidad	Negación de servicio	Ataque de denegación de servicio que hace que la aplicación se bloquee o se ralentice
	Denegación de servicio distribuida	Ataque de denegación de servicio distribuido
	Configuración incorrecta	Configuración incorrecta del software que genera problemas de disponibilidad del servicio
	Sabotaje	Sabotaje físico
	Corte	Un apagón causado por una falla
Seguridad del contenido de la información	Acceso no autorizado a la información	Abusar de credenciales de inicio de sesión robadas para un sistema o aplicación
	Modificación no autorizada de la información	Abusar de credenciales de inicio de sesión robadas para un sistema o aplicación
	Pérdida de datos	Pérdida de datos causada por falla o robo
	Fuga de Información Confidencial	Credenciales o datos personales filtrados
Fraude	Uso no autorizado de recursos	Uso de recursos para fines no autorizados
	Copyright	Instalación de copias de software comercial sin licencia

	Mascarada/Phishing	Suplantación de identidad de otra persona para beneficiarse de ella
Vulnerable	Criptografía débil	Servicios de acceso público que ofrecen criptografía débil
	Amplificador DDoS	Servicios de los que se puede abusar para realizar ataques DDoS de reflexión/amplificación
	Servicios accesibles potencialmente no deseados	Servicios de acceso público potencialmente no deseados
	Divulgación de información	Servicios de acceso público que pueden revelar información confidencial
	Sistema Vulnerable	Un sistema que es vulnerable a ciertos ataques

Tabla 4.1: Ejemplos de incidentes peligrosos

Capítulo 5

La necesidad de implantar la Ciberseguridad en Smart City

Los objetivos de seguridad de la ciudad inteligente de confidencialidad, integridad, disponibilidad, seguridad y resiliencia deben basarse tanto en datos seguros como en sistemas resistentes. Su aplicación integrada ayudará a mantener un entorno urbano más seguro y sostenible.

A menudo, los servicios de la ciudad comprometidos con la digitalización se ven obligados a integrar nuevas tecnologías de la información con sistemas de TI que tienen poca o ninguna protección contra las ciberamenazas. Según estudios del Congreso, alrededor de 3/4 de los $80 mil millones que gasta anualmente el gobierno federal en tecnología de la información se destinan al mantenimiento de los llamados sistemas obsoletos. La combinación de sistemas nuevos y heredados crea serios problemas y conduce a vulnerabilidades ocultas en todo el ecosistema de la ciudad inteligente.

De particular preocupación y peligro son los llamados "ciberactivistas" asociados con individuos radicales, grupos criminales, organizaciones extremistas y terroristas. En una ciudad inteligente, los ataques cibernéticos pueden desestabilizar la situación sociopolítica, inspirar y apoyar la actividad de protesta de los ciudadanos, provocar acciones callejeras espontáneas, como mítines y manifestaciones, provocar una escalada de tensión y también fortalecer las posiciones de los propios ciberdelincuentes. en presionar a autoridades y administraciones, organizaciones para obligarlas a cumplir con sus demandas.

A medida que los grupos de ciberdelincuentes se equipen con herramientas técnicas avanzadas, las ciudades inteligentes estarán

sujetas a ataques cada vez más sofisticados y destructivos, que van desde el robo de identidad hasta la interrupción de servicios vitales completos.

Como una de las opciones para solucionar el problema de la ciberseguridad utilizando las tecnologías del Internet de las Cosas está la introducción de una gran cantidad de sensores y sensores diversos para una mejor identificación del usuario. Dichas autorizaciones fisiológicas reducirán los riesgos de posesión no autorizada de datos personales, robo de finanzas y otros daños en el ámbito de la ciberdelincuencia.

Necesidad de red amplificadora de sensores IoT para identificación fisiológica

- Criterio: Aplicación Urbanismo (Los sistemas IoT son capaces de automatizar muchas acciones)
- Criterio: Personalizar servicios a cliente (En medicina, cada cliente tiene su propia historia única e IoT podría hacer que la atención médica sea más personalizada)
- Criterio: Seguridad (Los datos personales son un tema delicado e IoT podría ayudar a asegurar esos datos)

Capítulo 6

Perspectivas de desarrollo de Ciberseguridad y Smart city

En el artículo científico "An approach to develop the smart health using Internet of Things and authentication based on biometric technology" escrito por Hodjat Hamidi, presenta un nuevo estándar para aplicar la biometría para desarrollar un cuidado de la salud inteligente usando IoT que incluye alta capacidad para acceder a datos además de ser fácil de usar. Como resultado de su investigación, el autor llegó a una forma más segura de acceder a IoT basada en la biometría y el estándar de identidad rápido por el cual cree que se utilizará en dispositivos inteligentes y sistemas de salud. En este artículo, el autor investigó el estado actual de la salud inteligente y el IoT. Concluye que el desarrollo de IoT resultó en la aparición de un nuevo estándar en las aplicaciones de datos biométricos.

Hodjat Hamidi sugiere usar tecnologías IoT para fusionar tecnología biométrica e identidad rápida en línea. El estudio se basa en dos fundamentos:

1. biometría fisiológica
    a. huella dactilar
    b. rostro
    c. geometría de la mano
    d. reconocimiento de huellas de palma
    e. pulsación de tecla
2. biometría conductual
    a. reconocimiento de voz,
    b. reconocimiento de firma
    c. perfil de comportamiento, dinámica táctil

Este tipo de métodos son ampliamente utilizados para el acceso de personas a grandes sistemas de organizaciones o acceso a sistemas de

atención médica para la información de los pacientes, y también para el uso de cosas relacionadas con el Internet de las Cosas.

Los dispositivos biométricos siempre están bajo varios ataques. Los piratas generalmente utilizan diferentes métodos para engañar a los sistemas de identificación. El proceso de identificación puede basarse tanto en software como en hardware. Aunque esto puede aumentar los costos, es altamente efectivo. Según la investigación, la biometría de huella dactilar es la máxima prioridad y luego la pulsación de teclas, por lo que la combinación de estas dos debe ser altamente eficiente.

Hodjat Hamidi discutió sobre el principal desafío al que nos enfrentaremos para desarrollar el Internet de las Cosas y el método propuesto basado en la biometría para el uso de sistemas de salud inteligentes. El uso creciente de sistemas de salud inteligentes, los servicios electrónicos proporcionados por instituciones económicas y comerciales, y la expansión de medios y herramientas para ingresar al ciberespacio, resaltan la creciente importancia de la seguridad en el intercambio de información. Dada la importancia de las conexiones seguras de las cosas a Internet y el acceso a las mismas, las características biométricas se utilizan como identificadores; porque no pueden ser prestados, comprados, olvidados y son muy difíciles de falsificar o copiar

Implementación de IoT en medicina y sistema de salud para aumentar la ciberseguridad

- Criterio: Aplicación Salud (IoT podría mejorar drásticamente el seguridad de sistema de salud)
- Criterio: Optimizar costes de negocio (Los sensores podrían hacer que las empresas sean más seguras y permitir que ahorren más en ciberseguridad)
- Criterio: Seguridad (Los datos personales son un tema delicado e IoT podría ayudar a asegurar esos datos)

Capítulo 7

Conclusiones

El Internet de las Cosas tiene un futuro prometedor que influenciará todos los aspectos de la vida tal y como se conocemos, entre otros. Dicho futuro se podrá apreciar en la industria, transporte, agricultura, y en el que se centra este trabajo, la ciudad inteligente. Por lo tanto, una ciudad inteligente es un ecosistema complejo para el funcionamiento de las instituciones de la ciudad individual.

Aunque el uso de tecnologías digitales modernas ayuda a mejorar la calidad de su trabajo, también hay una desventaja en este proceso. Surgen nuevos tipos de vulnerabilidades que requieren constante monitoreo y eliminación. El gran volumen de intercambio de datos, la integración entre dispositivos IoT dispares y los procesos que cambian dinámicamente crean amenazas cibernéticas que se ven exacerbadas por las complejidades en otros componentes del ecosistema que abarcan la infraestructura tecnológica de las ciudades inteligentes. El problema de su seguridad aún no se ha resuelto suficientemente, ni en términos jurídicos ni prácticos, y requiere una mayor atención y un análisis exhaustivo.

Bibliografía

[1]J. Montes, “A Historical View of Smart Cities: Definitions, Features and Tipping Points,” SSRN Electronic Journal, 2020, doi: 10.2139/ssrn.3637617.

[2]K. P. Miller, “Review: THE NEXT LOS ANGELES: The Struggle for a Livable City, by Robert Gottlieb, Mark Vallianatos, Regina Freer, and Peter Dreier,” Southern California Quarterly, vol. 87, no. 3, pp. 328–331, 2005, doi: 10.2307/41172278.

[3]H. Hamidi, “An approach to develop the smart health using Internet of Things and authentication based on biometric technology,” Future Generation Computer Systems, vol. 91, pp. 434–449, Feb. 2019, doi: 10.1016/j.future.2018.09.024.

[4]B. Ang, “Singapore, ASEAN, and international cybersecurity,” Routledge Handbook of International Cybersecurity, pp. 218–226, Jan. 2020, doi: 10.4324/9781351038904-21.

[5]M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, “Long-range communications in unlicensed bands: the rising stars in the IoT and smart city scenarios,” IEEE Wireless Communications, vol. 23, no. 5, pp. 60–67, Oct. 2016, doi: 10.1109/mwc.2016.7721743.

[6]I. Lee and K. Lee, “The Internet of Things (IoT): Applications, investments, and challenges for enterprises,” Business Horizons, vol. 58, no. 4, pp. 431–440, Jul. 2015, doi: 10.1016/j.bushor.2015.03.008.