เครื่องยืนยันตัวตนด้วย NFC

ประภากร ศรีวรสาร
พีรดา แสงแป้
ศตคุณ อุตมะ

โครงงานนี้เป็นส่วนหนึ่งของ วิชาโครงงานรหัสวิชา 21909-2023
ตามหลักสูตรประกาศนียบัตรวิชาชีพ พุทธศักราช 2567
ประเภทวิชาอุตสาหกรรมดิจิทัลและเทคโนโลยีสารสนเทศ
สาขาวิชาช่างเทคนิคคอมพิวเตอร์ วิทยาลัยเทคนิคหนองคาย
สำนักงานคณะกรรมการการอาชีวศึกษา
ปีการศึกษา 2568

สารบัญ

สารบัญ ..... ก
สารบัญภาพ ..... ข
บทที่ 1 บทนำ 1
1.1 ที่มาและความสำคัญของปัญหา 1
1.2 วัตถุประสงค์ของโครงงาน 1
1.3 ประโยชน์ที่คาดว่าจะได้รับ 1
1.4 ขอบเขตของโครงงาน 1
1.5 นิยามศัพท์เฉพาะ 1
1.6 ผลที่คาดว่าจะได้รับ 2
บทที่ 2 ทฤษฎีและเอกสารที่เกี่ยวข้อง 3
2.1 ไมโครคอนโทรเลอร์ (Microcontroller) 3
2.4 เกณฑ์วิธีขนส่งข้อความหลายมิติแบบมั่นคง (Hypertext Transfer Protocol Secure; HTTPS) 4
2.5 เกณฑ์วิธีความมั่นคงของชั้นขนส่ง (Transport Layer Security; TLS) 9
2.6 การสื่อสารสนามใกล้ (Near-field communication; NFC) 15
2.7 เซ็นเซอร์อินฟราเรดแบบพาสซีฟ (PIR sensor) 15
2.8 ภาษาซี 23
2.9 Flutter 25
2.10 Git 28
ภาคผนวก 29
ลิขสิทธิ์เนื้อหาโครงงาน 29
ลิขสิทธิ์ซอร์สโคดโครงงาน 29
GNU GENERAL PUBLIC LICENSE 29
บรรณานุกรม 44
บรรณานุกรมภาพ 45

สารบัญภาพ

รูปที่ 2.7.0.1 เครื่องตรวจจับการเคลื่อนไหวแบบ PIR ทั่วไปสำหรับที่พักอาศัย/เชิงพาณิชย์ 15
รูปที่ 2.7.2.1 เครื่องตรวจจับความเคลื่อนไหว PIR ใช้สำหรับควบคุมไฟภายนอกอาคารแบบอัตโนมัติ. 16
รูปที่ 2.7.2.2 กล้องดักถ่ายพร้อมระบบตรวจจับความเคลื่อนไหวแบบ PIR 16
รูปที่ 2.7.2.3 สวิตช์ไฟภายในอาคารที่ติดตั้งเซนเซอรตรวจจับการครอบครองแบบ PIR 17
รูปที่ 2.7.6.1 การออกแบบเซ็นเซอร์ตรวจจับการเคลื่อนไหว PIR 18
รูปที่ 2.7.8.1 ตัวเรือนเครื่องตรวจจับความเคลื่อนไหว PIR พร้อมช่องหน้าต่างทรงกระบอกเหลี่ยม โดยแต่ละเหลี่ยมเป็นเลนส์เฟรสเนล โฟกัสแสงไปที่ชิ้นส่วนเซ็นเซอร์ไพโรอิเล็กทริกที่อยู่ด้านล่าง 19
รูปที่ 2.7.8.2 ฝาครอบด้านหน้า PIR เท่านั้น (ถอดอุปกรณ์อิเล็กทรอนิกส์ออก) โดยมีแหล่งกำเนิดแสงจุดอยู่ด้านหลัง เพื่อแสดงเลนส์แต่ละตัว 19
รูปที่ 2.7.8.3 PIR ที่ถอดฝาครอบด้านหน้าออก แสดงตำแหน่งของ เซ็นเซอร์ไพโรอิเล็กทริก (ลูกศรสีเขียว) 19
รูปที่ 2.7.9.1 PID ทั่วไปสำหรับที่พักอาศัย/เชิงพาณิชย์ที่ ใช้กระจกแบ่งส่วนภายในเพื่อการโฟกัส..... 20
รูปที่ 2.7.9.2 ถอดฝาครอบออกแล้ว กระจกแบ่งส่วน ด้านล่างมีแผงวงจรพิมพ์ (PC) อยู่ด้านบน . 20
รูปที่ 2.7.9.3 แผงวงจรพิมพ์ถูกถอดออกเพื่อแสดงกระจกแบบแบ่งส่วน 20
รูปที่ 2.7.9.4 กระจกพาราโบลาแบบแบ่งส่วนถอดออกจากตัวเครื่อง 21
รูปที่ 2.7.9.5 ด้านหลังของแผงวงจรที่หันเข้าหากระจกเมื่อติดตั้ง เซ็นเซอร์ไพโรอิเล็กทริกแสดงด้วยลูกศรสีเขียว 21
รูปที่ 2.7.10.1 เครื่องตรวจจับความเคลื่อนไหวที่มีรูปแบบลำแสงซ้อนทับ ความยาวของลำแสงเป็นตัวชี้วัดความไวของเครื่องตรวจจับในทิศทางนั้น 21

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ความปลอดภัยนั้นเป็นเรื่องสำคัญสำหรับทุกคนแต่องค์กรแต่ละองค์กรและคนแต่ละคนมักมีความต้องการด้านความปลอดภัยไม่เหมือนกัน แต่ในบางครั้ง เมื่อมีบุคคลหรือองค์กรที่ต้องการเทคโนโลยีด้านความปลอดภัยเหล่านี้ เทคโนโลยีความปลอดภัยนั้นอาจมีราคาสูงเกินกว่าจะเอื้อมถึงได้ ส่งผลให้อาจมีการลดระดับความปลอดภัยลงมา เพิ่มความเสี่ยงของชีวิต ทรัพย์สิน เอกสาร และข้อมูลต่าง ๆ ขององค์กรหรือบุคคลนั้น ๆ

ในโลกปัจจุบัน อินเทอร์เน็ตนั้นก็เป็นสิ่งที่สำคัญมากเช่นกัน และสถานที่ส่วนใหญ่มักจะมีอินเทอร์เน็ต จึงก่อให้เกิดการที่มีอุปกรณ์อินเทอร์เน็ตรอบตัวเพิ่มขึ้นทุกวัน และได้มีสิ่งที่เรียกว่า Internet of Things (IoT) เกิดขึ้น ซึ่งคืออุปกรณ์ที่ถูกปรับปรุงให้ใช้งานได้ดีขึ้นด้วยเทคโนโลยีไร้สายต่าง ๆ เช่น Wi-Fi, Bluetooth, Zigbee, และ Thread

โครงงานนี้จึงมีเป้าหมายที่จะแก้ไขปัญหาที่กล่าวไปข้างต้น พร้อมศึกษาและเรียนรู้เกี่ยวกับเทคโนโลยีไร้สาย Wi-Fi และ NFC เพื่อสร้างอุปกรณ์ยืนยันตัวตนที่ต้นทุนไม่สูงมากและให้ราคาเข้าถึงได้ง่ายขึ้น

1.2 วัตถุประสงค์ของโครงงาน

1.2.1 เพื่อเพิ่มความปลอดภัยของพื้นที่
1.2.2 เพื่อเพิ่มความไว้วางใจของบุคลากรในองค์กร
1.2.3 เพื่อป้องกันข้อมูลขององค์กรที่อาจรั่วไหล
1.2.4 เพื่อรับมือเหตุการณ์ผู้บุกรุกได้อย่างทันท่วงที

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 สามารถประยุกต์ความรู้ด้านอิเล็กทรอนิกส์และเทคโนโลยีมาใช้ในชีวิตประจำวันได้จริง
1.3.2 สามารถตรวจจับผู้บุกรุกได้ ช่วยเพื่อเพิ่มความไว้วางใจของบุคลากรในองค์กร

1.4 ขอบเขตของโครงงาน

1.4.1 สามารถแจ้งเตือนสัญญาณเสียงได้
1.4.2 สามารถแจ้งเตือนผ่านโทรศัพท์มือถือได้
1.4.3 สามารถตรวจจับบุคคลที่ไม่ได้รับอนุญาตได้

1.5 นิยามศัพท์เฉพาะ

เครื่องยืนยันตัวตนด้วย NFC คืออุปกรณ์ความปลอดภัยที่มีหน้าที่ในการยืนยันตัวตนบุคคลที่เข้าออกพื้นที่ โดยใช้เทคโนโลยี NFC เป็นระบบยืนยันตัวตนบุคคลและใช้เซนเซอร์ตรวจจับความเคลื่อนไหวในการตรวจสอบหากมีบุคคลเข้าไปโดยไม่ได้รับอนุญาต

1.6 ผลที่คาดว่าจะได้รับ

1.6.1 ได้รับความรู้ในด้านการรักษาความปลอดภัย

1.6.2 ได้รับประสบการณ์ในการทำงานกับเทคโนโลยีไร้สาย

1.6.3 ได้รับประสบการณ์ในการทำชิ้นงานด้วย ESP32

บทที่ 2
ทฤษฎีและเอกสารที่เกี่ยวข้อง

ผู้จัดทำโครงงาน “เครื่องยืนยันตัวตนด้วย NFC” ได้ศึกษาทฤษฎีที่เกี่ยวข้องต่าง ๆ และ รวบรวมแนวทางและหลักการต่าง ๆ จากเอกสารงานวิจัยที่เกี่ยวข้องดังต่อไปนี้

2.1 ไมโครคอนโทรเลอร์ (Microcontroller)
2.2 ลำโพงสัญญาณ (Buzzer)
2.3 เกณฑ์วิธีขนส่งข้อความหลายมิติ (HyperText Transfer Protocol; HTTP)
2.4 เกณฑ์วิธีขนส่งข้อความหลายมิติแบบมั่นคง (Hypertext Transfer Protocol Secure; HTTPS)
2.5 เกณฑ์วิธีความมั่นคงของชั้นขนส่ง (Transport Layer Security; TLS)
2.6 การสื่อสารสนามใกล้ (Near-field communication; NFC)
2.7 เซ็นเซอร์อินฟราเรดแบบพาสซีฟ (เซนเซอร์ PIR)
2.8 ภาษาซี
2.9 Flutter
2.10 Git

2.1 ไมโครคอนโทรเลอร์ (Microcontroller)

ความรู้เกี่ยวกับไมโครคอนโทรลเลอร์เบื้องต้น ไมโครคอนโทรลเลอร์ (มักย่อว่า uC หรือMCU) คือ อุปกรณ์ควบคุมขนาดเล็ก ซึ่งบรรจุความสามารถที่คล้ายคลึงกับระบบคอมพิวเตอร์ โดยใน ไมโครคอนโทรลเลอร์ได้รวม เอาซีพียูหน่วยความจำและพอร์ต ซึ่งเป็นส่วนประกอบหลักสำคัญของ ระบบคอมพิวเตอร์เข้าไว้ด้วยกัน โดยทำการบรรจุเข้าไว้ในตัวถังเดียวกัน ไมโครคอนโทรลเลอร์ถ้าแปล ความหมายแบบตรงตัวก็คือ ระบบคอนโทรลขนาดเล็กเรียกอีกอย่างหนึ่งคือเป็นระบบคอมพิวเตอร์ ขนาดเล็ก ที่สามารถนำมาประยุกต์ใช้งานได้หลากหลาย โดยผ่านการออกแบบวงจรให้เหมาะกับงาน ต่างๆ และยังสามารถเขียนโปรแกรมคำสั่งเพื่อควบคุมขา Input / Output เพื่อสั่งงานให้ไป ควบคุม อุปกรณ์ต่างๆ ได้อีกด้วย ซึ่งก็นับว่าเป็นระบบที่สามารถนำมาประยุกต์ใช้งานได้หลากหลาย ทั้ง ทางด้าน Digital และ Analog ยกตัวอย่างเช่น ระบบสัญญาณตอบรับอัตโนมัติ, ระบบบัตรคิว, ระบบ ตอกบัตรพนักงาน และอื่นๆ ยิ่งระบบไมโครคอนโทรลเลอร์ในยุคปัจจุบันนั้นสามารถทำการเชื่อต่อกับ ระบบ Network ของคอมพิวเตอร์ทั่วไปได้อีกด้วย ดังนั้นการสั่งงานจึงไม่ใช่แค่หน้าแผงวงจร แต่ อาจจะเป็นการสั่งงานอยู่คนละ ซีกโลกผ่านเครือข่ายอินเตอร์เน็ตก็ได้โครงสร้างโดยทั่วไปของไมโครคอนโทรลเลอร์นั้น สามารถแบ่งออกมาได้เป็น 5 ส่วนใหญ่ๆ ได้แก่ หน่วยประมวลผลกลาง หรือ ซีพียู, หน่วยความจ า, ส่วนติดต่อกับอุปกรณ์ภายนอก หรือพอร์ต, ช่องทางเดินของสัญญาณ หรือบัส และ วงจรกำเนิดสัญญาณนาฬิกา หน่วยความจำนั้น สามารถแบ่งออกเป็น 2 ส่วนคือ หน่วยความจำที่มีไว้สำหรับเก็บ โปรแกรมหลัก เปรียบเสมือนฮาร์ดดิสก์และหน่วยความจำข้อมูล ใช้เป็นเหมือนกับ กระดาษทดในการ คำนวณของซีพียู โดย ESP32 เป็นไมโครคอนโทรลเลอร์แบบ

System-on-a-Chip (SoC) ที่มีการรวมส่วนประกอบทั้งหมดที่จำเป็นสำหรับการประมวลผลและการสื่อสารไร้สายไว้ในชิปเดียว ที่มีคุณสมบัติเด่นด้านการเชื่อมต่อ Wi-Fi และ Bluetooth ในตัว

เป็นชิปไมโครคอนโทรลเลอร์แบบ 32 บิต ที่มีความสามารถสูง พัฒนาและผลิตโดย บริษัท Espressif Systems จากประเทศจีน ส่วนประกอบหลักของบอร์ด ESP32

2.1.1 ตารางพาร์ทิชัน (Partition Table)

Name	Type	SubType	Offset	Size	Flags
nvs	data	nvs	0x9000	0x5000	
otadata	data	ota	0xe000	0x2000	
app0	app	ota_0	0x10000	0x140000	
app1	app	ota_1	0x150000	0x140000	
spiffs	data	spiffs	0x290000	0x160000	
coredump	data	coredump	0x3F0000	0x10000	

2.1.2 LittleFS

2.4 เกณฑ์วิธีขนส่งข้อความหลายมิติแบบมั่นคง (Hypertext Transfer Protocol Secure; HTTPS)

เกณฑ์วิธีขนส่งข้อความหลายมิติแบบมั่นคง (Hypertext Transfer Protocol Secure; HTTPS) คือส่วนต่อขยายของโปรโตคอลเกณฑ์วิธีขนส่งข้อความหลายมิติ (Hypertext Transfer Protocol; HTTP) ซึ่งใช้การเข้ารหัสเพื่อการสื่อสารที่ปลอดภัยผ่านเครือข่ายคอมพิวเตอร์ และถูกใช้อย่างแพร่หลายบนอินเทอร์เน็ต โดยโปรโตคอลเครือข่าย HTTPS จะถูกเข้ารหัสด้วยเกณฑ์วิธีความมั่นคงของชั้นขนส่ง (Transport Layer Security; TLS) หรือก่อนหน้านี้คือเกณฑ์วิธีชั้นซ็อกเก็ตปลอดภัย (Secure Sockets Layer; SSL) ด้วยเหตุนั้น โปรโตคอลนี้สามารถเรียกด้วยชื่อ HTTP over TLS หรือ HTTP over SSL ได้เช่นกัน

แรงจูงใจหลักของ HTTPS คือการยืนยันตัวตนของเว็บไซต์ที่เข้าถึง และการปกป้องความเป็นส่วนตัวและความสมบูรณ์ของข้อมูลที่แลกเปลี่ยนระหว่างการรับส่งข้อมูล HTTPS ป้องกันการโจมตีแบบ man-in-the-middle และการเข้ารหัสบล็อกไซเฟอร์แบบสองทิศทางในการสื่อสารระหว่างไคลเอนต์และเซิร์ฟเวอร์ ช่วยป้องกันการสื่อสารจากการดักฟังและการปลอมแปลง ประเด็นการพิสูจน์ตัวตนของ HTTPS จำเป็นต้องมีบุคคลที่สามที่เชื่อถือได้ลงนามในใบรับรองดิจิทัลฝั่งเซิร์ฟเวอร์ เดิมทีการดำเนินการนี้มีค่าใช้จ่ายสูง ซึ่งหมายความว่าการเชื่อมต่อ HTTPS ที่ผ่านการรับรองความถูกต้องอย่างสมบูรณ์มักจะพบได้เฉพาะในบริการธุรกรรมการชำระเงินที่ปลอดภัยและระบบสารสนเทศขององค์กรที่ปลอดภัยอื่นๆ บนเวิลด์ไวด์เว็บเท่านั้น ในปี 2016 แคมเปญโดยมูลนิธิพรมแดนอิเล็กทรอนิกส์ (Electronic Frontier Foundation; EFF) ด้วยการสนับสนุนจากนักพัฒนาเว็บเบราว์เซอร์ ทำให้โปรโตคอลนี้แพร่หลายมากขึ้น นับตั้งแต่ปี 2018 เป็นต้นมา HTTPS ถูกใช้โดยผู้ใช้เว็บบ่อยกว่า HTTP ดั้งเดิมที่ไม่ปลอดภัย โดยส่วนใหญ่เพื่อปกป้องความถูกต้องของหน้าเว็บบนเว็บไซต์ทุกประเภท รักษาความปลอดภัยบัญชี และรักษาความเป็นส่วนตัวของการสื่อสาร การระบุตัวตน และการท่องเว็บของผู้ใช้

2.4.1 โดยรวม

รูปแบบ Uniform Resource Identifier (URI) ของ HTTPS มีรูปแบบการใช้งานที่เหมือนกันกับรูปแบบ HTTP อย่างไรก็ตาม HTTPS จะส่งสัญญาณให้เบราว์เซอร์ใช้ชั้นการเข้ารหัสเพิ่มเติมของ SSL/TLS เพื่อปกป้องการรับส่งข้อมูลซึ่ง SSL/TLS เหมาะอย่างยิ่งสำหรับ HTTP เนื่องจากสามารถให้การป้องกันได้แม้ว่าจะมีการตรวจสอบความถูกต้องเพียงด้านเดียวของการสื่อสาร ในกรณีนี้คือธุรกรรม HTTP บนอินเทอร์เน็ต ซึ่งโดยทั่วไปมีเพียงเซิร์ฟเวอร์เท่านั้นที่ได้รับการรับรองความถูกต้อง (โดยไคลเอนต์ตรวจสอบใบรับรองของเซิร์ฟเวอร์)

HTTPS สร้างช่องทางที่ปลอดภัยบนเครือข่ายที่ไม่ปลอดภัย วิธีนี้ช่วยให้มั่นใจได้ถึงการป้องกันที่เหมาะสมจากผู้ดักฟังและการโจมตีแบบ man-in-the-middle โดยมีเงื่อนไขว่ามีการใช้ชุดการเข้ารหัสที่เหมาะสม และใบรับรองเซิร์ฟเวอร์ได้รับการตรวจสอบและเชื่อถือได้

เนื่องจาก HTTPS เชื่อมโยง HTTP ทั้งหมดเข้ากับ TLS โดยตรงจึงสามารถเข้ารหัสโปรโตคอล HTTP พื้นฐานทั้งหมดได้ ซึ่งรวมถึง URL ของคำขอ พารามิเตอร์การค้นหา ส่วนหัว และคุกกี้ (ซึ่งมักจะมีข้อมูลระบุตัวตนของผู้ใช้) อย่างไรก็ตาม เนื่องจากที่อยู่เว็บไซต์และหมายเลขพอร์ตเป็นส่วนหนึ่งของโปรโตคอล TCP/IP พื้นฐาน HTTPS จึงไม่สามารถปกป้องการเปิดเผยข้อมูลเหล่านี้ได้ ในทางปฏิบัติ หมายความว่าแม้แต่บนเว็บเซิร์ฟเวอร์ที่กำหนดค่าอย่างถูกต้อง ผู้ดักฟังก็สามารถอนุมานที่อยู่ IP และหมายเลขพอร์ตของเว็บเซิร์ฟเวอร์ และบางครั้งอาจรวมถึงชื่อโดเมน (เช่น www.example.org แต่ไม่สามารถอนุมานส่วนที่เหลือของ URL) ที่ผู้ใช้กำลังสื่อสารด้วย รวมถึงปริมาณข้อมูลที่ถ่ายโอนและระยะเวลาของการสื่อสาร แต่อย่างไรก็ตามไม่รวมถึงเนื้อหาของการสื่อสาร

เว็บเบราว์เซอร์รู้วิธีเชื่อถือเว็บไซต์ HTTPS โดยอ้างอิงจากผู้ให้บริการออกใบรับรอง (Certificate Authority) ที่ติดตั้งไว้ล่วงหน้าในซอฟต์แวร์ ผู้สร้างเว็บเบราว์เซอร์จึงไว้วางใจผู้ให้บริการออกใบรับรองในการออกใบรับรองที่ถูกต้อง ดังนั้น ผู้ใช้ควรเชื่อถือการเชื่อมต่อ HTTPS ไปยังเว็บไซต์ก็ต่อเมื่อเป็นไปตามเงื่อนไขทั้งหมดต่อไปนี้:

- ผู้ใช้เชื่อมั่นว่าอุปกรณ์ของตน โฮสต์เบราว์เซอร์ และวิธีการเข้าถึงเบราว์เซอร์นั้นไม่ถูกบุกรุก (กล่าวคือ ไม่มีการโจมตีซัพพลายเชน)
- ผู้ใช้เชื่อมั่นว่าซอฟต์แวร์เบราว์เซอร์ใช้งาน HTTPS ได้อย่างถูกต้องพร้อมกับผู้ให้บริการออกใบรับรองที่ติดตั้งไว้ล่วงหน้าอย่างถูกต้อง
- ผู้ใช้เชื่อมั่นว่าผู้ให้บริการออกใบรับรองจะรับรองเฉพาะเว็บไซต์ที่ถูกต้องตามกฎหมายเท่านั้น (กล่าวคือ ผู้ให้บริการออกใบรับรองจะไม่ถูกบุกรุกและไม่มีการออกใบรับรองที่ผิดพลาด)
- เว็บไซต์มีใบรับรองที่ถูกต้อง ซึ่งหมายความว่าได้รับการลงนามโดยผู้ให้บริการที่เชื่อถือได้
- ใบรับรองระบุเว็บไซต์ได้อย่างถูกต้อง (เช่น เมื่อเบราว์เซอร์เข้าชม “https://example.com” ใบรับรองที่ได้รับนั้นถูกต้องสำหรับ “example.com” และไม่ใช่ของหน่วยงานอื่น)
- ผู้ใช้เชื่อมั่นว่าเลเยอร์การเข้ารหัสของโปรโตคอล (SSL/TLS) มีความปลอดภัยเพียงพอจากการดักฟัง

HTTPS มีความสำคัญอย่างยิ่งต่อเครือข่ายที่ไม่ปลอดภัยและเครือข่ายที่อาจถูกแทรกแซง เครือข่ายที่ไม่ปลอดภัย เช่น จุดเชื่อมต่อ Wi-Fi สาธารณะ ซึ่งเปิดโอกาสให้ทุกคนในเครือข่ายท้องถิ่นเดียวกันสามารถดักจับแพ็กเก็ตและค้นพบข้อมูลสำคัญที่ไม่ได้รับการป้องกันโดย HTTPS นอกจากนี้ ยัง

พบว่าเครือข่าย WLAN ทั้งแบบฟรีและแบบเสียเงินบางเครือข่ายได้แทรกแซงหน้าเว็บโดยการแทรกแพ็กเก็ตเพื่อแสดงโฆษณาของตนเองบนเว็บไซต์อื่น การกระทำเช่นนี้สามารถถูกนำไปใช้ในทางที่ผิดได้หลายวิธี เช่น การฉีดมัลแวร์ลงในหน้าเว็บและการขโมยข้อมูลส่วนบุคคลของผู้ใช้

เมื่อมีข้อมูลมากขึ้นเกี่ยวกับการเฝ้าระวังมวลชนทั่วโลกและการขโมยข้อมูลส่วนบุคคลของอาชญากร การใช้ระบบรักษาความปลอดภัย HTTPS บนเว็บไซต์ทั้งหมดจึงมีความสำคัญเพิ่มมากขึ้นเรื่อยๆ โดยไม่คำนึงถึงประเภทของการเชื่อมต่ออินเทอร์เน็ตที่ใช้งาน แม้ว่าข้อมูลเมตาเกี่ยวกับหน้าเว็บแต่ละหน้าที่ผู้ใช้เข้าชมอาจไม่ถือว่ามีความละเอียดอ่อน แต่เมื่อนำมารวมกันแล้ว ข้อมูลเมตาเหล่านี้อาจเปิดเผยข้อมูลเกี่ยวกับผู้ใช้ได้มาก และกระทบต่อความเป็นส่วนตัวของผู้ใช้

การปรับใช้ HTTPS ยังอนุญาตให้ใช้ HTTP/2 และ HTTP/3 (และรุ่นก่อนหน้าอย่าง SPDY และ QUIC) ซึ่งเป็น HTTP เวอร์ชันใหม่ที่ออกแบบมาเพื่อลดเวลา ขนาด และความหน่วงในการโหลดหน้าเว็บ

และมีการแนะนำให้ใช้ HTTP Strict Transport Security (HSTS) ร่วมกับ HTTPS เพื่อป้องกันผู้ใช้จากการโจมตีแบบ man-in-the-middle โดยเฉพาะอย่างยิ่ง SSL stripping

2.4.2 ความปลอดภัย

ความปลอดภัยของ HTTPS อยู่ที่ TLS พื้นฐาน ซึ่งโดยทั่วไปจะใช้คีย์สาธารณะและคีย์ส่วนตัวระยะยาวเพื่อสร้างคีย์เซสชันระยะสั้น ซึ่งจะถูกนำไปใช้ในการเข้ารหัสการไหลของข้อมูลระหว่างไคลเอนต์และเซิร์ฟเวอร์ ใบรับรอง X.509 ถูกใช้เพื่อยืนยันตัวตนของเซิร์ฟเวอร์ (และบางครั้งรวมถึงไคลเอนต์ด้วย) ด้วยเหตุนี้ ผู้ให้บริการออกใบรับรองและใบรับรองคีย์สาธารณะจึงจำเป็นต่อการตรวจสอบความสัมพันธ์ระหว่างใบรับรองและเจ้าของ รวมถึงการสร้าง ลงนาม และดูแลความถูกต้องของใบรับรอง แม้ว่าวิธีนี้อาจมีประโยชน์มากกว่าการตรวจสอบตัวตนผ่านเครือข่ายที่เชื่อถือได้ แต่การเปิดเผยข้อมูลการเฝ้าระวังข้อมูลจำนวนมากในปี 2013 ได้ชี้ให้เห็นถึงผู้ให้บริการออกใบรับรองว่าเป็นจุดอ่อนที่อาจนำไปสู่การโจมตีแบบ man-in-the-middle คุณสมบัติที่สำคัญในบริบทนี้คือความลับแบบส่งต่อ (Forward Secrecy) ซึ่งรับประกันว่าการสื่อสารที่เข้ารหัสที่บันทึกไว้ในอดีตจะไม่สามารถดึงข้อมูลและถอดรหัสได้ หากคีย์ลับหรือรหัสผ่านระยะยาวถูกบุกรุกในอนาคต ไม่ใช่ทุกเว็บเซิร์ฟเวอร์ที่จะมีระบบความลับแบบส่งต่อ

เพื่อให้ HTTPS มีประสิทธิภาพ เว็บไซต์จะต้องโฮสต์ผ่าน HTTPS ทั้งหมด หากเนื้อหาบางส่วนของเว็บไซต์ถูกโหลดผ่าน HTTP (เช่น สคริปต์หรือรูปภาพ) หรือหากโหลดเฉพาะหน้าที่มีข้อมูลละเอียดอ่อน เช่น หน้าเข้าสู่ระบบ ผ่าน HTTPS ขณะที่ส่วนอื่นๆ ของเว็บไซต์ผ่าน HTTP ธรรมดา ผู้ใช้จะเสี่ยงต่อการถูกโจมตีและการเฝ้าระวัง นอกจากนี้ คุกกี้บนเว็บไซต์ที่รันผ่าน HTTPS จะต้องเปิดใช้งานแอตทริบิวต์ secure ในเว็บไซต์ที่มีข้อมูลละเอียดอ่อน ผู้ใช้และเซสชันจะถูกเปิดเผยทุกครั้งที่เข้าถึงเว็บไซต์นั้นด้วย HTTP แทนที่จะเป็น HTTPS

2.4.3 รายละเอียดทางเทคนิค

2.4.3.1 ความแตกต่างจาก HTTP

URL แบบ HTTPS เริ่มต้นด้วย “https://” และใช้พอร์ต 443 ตามค่าเริ่มต้น ในขณะที่ URL แบบ HTTP เริ่มต้นด้วย “http://” และใช้พอร์ต 80 ตามค่าเริ่มต้น

HTTP ไม่ได้เข้ารหัส จึงมีความเสี่ยงต่อการโจมตีแบบ man-in-the-middle และการดักฟังซึ่งอาจทำให้ผู้โจมตีสามารถเข้าถึงบัญชีเว็บไซต์และข้อมูลสำคัญ และแก้ไขหน้าเว็บเพื่อแทรกมัลแวร์หรือโฆษณาได้ HTTPS ได้รับการออกแบบมาให้ทนทานต่อการโจมตีประเภทนี้ และถือว่าปลอดภัย (ยกเว้นการใช้งาน HTTPS ที่ใช้ SSL เวอร์ชันที่ล้าสมัย)

2.4.3.2 ชั้นเครือข่าย

HTTP ทำงานที่เลเยอร์สูงสุดของโมเดล TCP/IP นั่นคือเลเยอร์แอปพลิเคชัน เช่นเดียวกับโปรโตคอลความปลอดภัย TLS (ซึ่งทำงานเป็นเลเยอร์ย่อยที่ต่ำกว่าของเลเยอร์เดียวกัน) ซึ่งเข้ารหัสข้อความ HTTP ก่อนส่ง และถอดรหัสเมื่อข้อความมาถึง โดยเคร่งครัดแล้ว HTTPS ไม่ใช่โปรโตคอลใหม่ที่แยกจากกัน แต่หมายถึงการใช้ HTTP ทั่วไปบนการเชื่อมต่อ SSL/TLS ที่เข้ารหัส (เป็นส่วนต่อขยายจาก HTTP อย่างที่กล่าวไปข้างต้น)

HTTPS เข้ารหัสเนื้อหาข้อความทั้งหมด รวมถึงส่วนหัว HTTP และข้อมูลคำขอ/การตอบกลับ ยกเว้นการโจมตีด้วยการเข้ารหัส CCA ที่อาจเกิดขึ้นตามที่อธิบายไว้ในส่วนข้อจำกัดด้านล่าง ผู้โจมตีควรจะสามารถตรวจพบการเชื่อมต่อระหว่างสองฝ่ายได้มากที่สุด รวมถึงชื่อโดเมนและที่อยู่ IP ของฝ่ายนั้นด้วย

2.4.3.3 การตั้งค่าเซิร์ฟเวอร์

เพื่อเตรียมเว็บเซิร์ฟเวอร์ให้ยอมรับการเชื่อมต่อ HTTPS ผู้ดูแลระบบต้องสร้างใบรับรองคีย์สาธารณะสำหรับเว็บเซิร์ฟเวอร์ ใบรับรองนี้ต้องได้รับการลงนามโดยผู้ออกใบรับรองที่เชื่อถือได้เพื่อให้เว็บเบราว์เซอร์ยอมรับโดยไม่มีการแจ้งเตือน ผู้ออกใบรับรองจะรับรองว่าผู้ถือใบรับรองคือผู้ดำเนินการของเว็บเซิร์ฟเวอร์ที่นำเสนอใบรับรองนั้น โดยทั่วไปเว็บเบราว์เซอร์จะเผยแพร่รายชื่อใบรับรองการลงนามของผู้ออกใบรับรองหลักๆ เพื่อให้สามารถตรวจสอบใบรับรองที่ลงนามโดยผู้ออกใบรับรองเหล่านั้นได้

2.4.3.3.1 การขอใบรับรอง

มีผู้ให้บริการออกใบรับรองเชิงพาณิชย์จำนวนหนึ่งที่เสนอใบรับรอง SSL/TLS แบบชำระเงินหลายประเภท รวมถึงใบรับรองการตรวจสอบขยาย

Let’s Encrypt เปิดตัวในเดือนเมษายน 2559 ให้บริการใบรับรอง SSL/TLS พื้นฐานแบบอัตโนมัติฟรีแก่เว็บไซต์ มูลนิธิ Electronic Frontier Foundation ระบุว่า Let’s Encrypt จะทำให้การเปลี่ยนจาก HTTP เป็น HTTPS “ง่ายดายเพียงแค่ออกคำสั่งหรือคลิกปุ่ม” ปัจจุบันผู้ให้บริการเว็บโฮสต์และผู้ให้บริการคลาวด์ส่วนใหญ่ใช้ประโยชน์จาก Let’s Encrypt เพื่อมอบใบรับรองฟรีให้กับลูกค้า

2.4.3.3.2 ใช้เป็นการควบคุมการเข้าถึง

ระบบนี้ยังสามารถใช้สำหรับการตรวจสอบสิทธิ์ไคลเอ็นต์เพื่อจำกัดการเข้าถึงเว็บเซิร์ฟเวอร์เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้น ในการดำเนินการนี้ ผู้ดูแลระบบเว็บไซต์มักจะสร้างใบรับรองสำหรับผู้ใช้แต่ละราย ซึ่งผู้ใช้จะโหลดใบรับรองลงในเบราว์เซอร์ โดยปกติใบรับรองจะมีชื่อและที่อยู่อีเมลของผู้ใช้ที่ได้รับอนุญาต และจะถูกตรวจสอบโดยเซิร์ฟเวอร์โดยอัตโนมัติในแต่ละการเชื่อมต่อเพื่อยืนยันตัวตนของผู้ใช้ ซึ่งอาจไม่จำเป็นต้องใช้รหัสผ่านด้วยซ้ำ

2.4.3.3.3 ในกรณีที่คีย์ลับถูกบุกรุก

คุณสมบัติที่สำคัญในบริบทนี้คือการเข้ารหัสแบบส่งต่อที่สมบูรณ์แบบ (PFS) การมีคีย์ลับแบบอสมมาตรระยะยาวตัวใดตัวหนึ่งที่ใช้สร้างเซสชัน HTTPS ไม่น่าจะทำให้การได้มาซึ่งคีย์เซสชันระยะสั้นเพื่อถอดรหัสการสนทนาทำได้ง่ายขึ้น แม้ในภายหลังก็ตาม ในปี 2013 มีเพียงการแลกเปลี่ยนคีย์ Diffie–Hellman (DHE) และการแลกเปลี่ยนคีย์ Diffie–Hellman แบบเส้นโค้งวงรี (ECDHE) เท่านั้นที่ทราบว่ามีคุณสมบัตินี้ ในปี 2013 มีเพียง 30% ของเซสชัน Firefox, Opera และ Chromium Browser เท่านั้นที่ใช้คุณสมบัตินี้ และเกือบ 0% ของเซสชัน Safari และ Microsoft Internet Explorer ของ Apple ที่ใช้คุณสมบัตินี้ TLS 1.3 ซึ่งเผยแพร่ในเดือนสิงหาคม 2018 ได้ยกเลิกการสนับสนุนการเข้ารหัสแบบไม่มีการเข้ารหัสแบบส่งต่อ ณ เดือนกุมภาพันธ์ พ.ศ. 2562 เว็บเซิร์ฟเวอร์ที่สำรวจ 96.6% รองรับการรักษาความลับแบบ Forward ในรูปแบบใดรูปแบบหนึ่ง และ 52.1% จะใช้การรักษาความลับแบบ Forward กับเบราว์เซอร์ส่วนใหญ่ ณ เดือนกรกฎาคม พ.ศ. 2566 เว็บเซิร์ฟเวอร์ที่สำรวจ 99.6% รองรับการรักษาความลับแบบ Forward ในรูปแบบใดรูปแบบหนึ่ง และ 75.2% จะใช้การรักษาความลับแบบ Forward กับเบราว์เซอร์ส่วนใหญ่

2.4.3.3.3.1 การเพิกถอนใบรับรอง

ใบรับรองอาจถูกเพิกถอนก่อนหมดอายุได้ เช่น เนื่องจากความลับของคีย์ส่วนตัวถูกละเมิด เบราว์เซอร์ยอดนิยมเวอร์ชันที่ใหม่พอเช่น Firefox Opera และ Internet Explorer บน Windows Vista จะใช้ Online Certificate Status Protocol (OCSP) เพื่อตรวจสอบว่าไม่เป็นเช่นนั้น เบราว์เซอร์จะส่งหมายเลขซีเรียลของใบรับรองไปยังผู้ออกใบรับรองหรือผู้แทนผ่าน OCSP และผู้ออกใบรับรองจะตอบกลับ โดยแจ้งให้เบราว์เซอร์ทราบว่าใบรับรองยังคงใช้ได้อยู่หรือไม่ นอกจากนี้ CA อาจออกรายการเพิกถอนใบรับรอง (Certificate Revocation List; CRL) เพื่อแจ้งให้ผู้ใช้ทราบว่าใบรับรองเหล่านี้ถูกเพิกถอนแล้ว อย่างไรก็ตาม CRL ไม่จำเป็นสำหรับฟอรัม CA/Browser (“ฟอรัม CA/Browser” ดังกล่าวคือองค์กร) อีกต่อไป อย่างไรก็ตาม CA ยังคงใช้ CRL กันอย่างแพร่หลาย สถานะการเพิกถอนส่วนใหญ่บนอินเทอร์เน็ตจะหายไปในไม่ช้าหลังจากใบรับรองหมดอายุ

2.4.3.4 ข้อจำกัด

การเข้ารหัส SSL (Secure Sockets Layer) และ TLS (Transport Layer Security) สามารถกำหนดค่าได้สองโหมด ได้แก่ โหมดธรรมดาและโหมด Mutual ในโหมดธรรมดา การตรวจสอบสิทธิ์จะดำเนินการโดยเซิร์ฟเวอร์เท่านั้น โหมด Mutual กำหนดให้ผู้ใช้ต้องติดตั้งใบรับรองไคลเอ็นต์ส่วนบุคคลในเว็บเบราว์เซอร์เพื่อการตรวจสอบสิทธิ์ผู้ใช้ ไม่ว่าในกรณีใด ระดับการป้องกันจะขึ้นอยู่กับความถูกต้องของการใช้งานซอฟต์แวร์และอัลกอริทึมการเข้ารหัสที่ใช้

SSL/TLS ไม่ป้องกันการจัดทำดัชนีของเว็บไซต์โดยเว็บครอว์เลอร์ และในบางกรณี URI ของทรัพยากรที่เข้ารหัสสามารถอนุมานได้โดยการทราบขนาดคำขอ/การตอบสนองที่ถูกสกัดกั้นเท่านั้น วิธีนี้ช่วยให้ผู้โจมตีสามารถเข้าถึงข้อความธรรมดา (เนื้อหาคงที่ที่เปิดเผยต่อสาธารณะ) และข้อความที่เข้ารหัส (เนื้อหาคงที่เวอร์ชันเข้ารหัส) ทำให้สามารถโจมตีด้วยการเข้ารหัสได้

เนื่องจาก TLS ทำงานที่ระดับโปรโตคอลที่ต่ำกว่า HTTP และไม่มีความรู้เกี่ยวกับโปรโตคอลระดับสูงกว่า เซิร์ฟเวอร์ TLS จึงสามารถแสดงใบรับรองได้เพียงใบเดียวสำหรับที่อยู่และพอร์ตที่กำหนดเท่านั้น ในอดีต นั่นหมายความว่าไม่สามารถใช้การโฮสต์เสมือนแบบอิงชื่อกับ HTTPS ได้ มีโซลูชันที่

เรียกว่า Server Name Indication (SNI) ซึ่งส่งชื่อโฮสต์ไปยังเซิร์ฟเวอร์ก่อนเข้ารหัสการเชื่อมต่อ แม้ว่าเบราว์เซอร์รุ่นเก่าจะไม่รองรับส่วนขยายนี้ก็ตาม การรองรับ SNI มีให้ใช้งานตั้งแต่ Firefox 2, Opera 8, Apple Safari 2.1, Google Chrome 6 และ Internet Explorer 7 บน Windows Vista

การโจมตีแบบ man-in-the-middle ที่ซับซ้อนประเภทหนึ่งที่เรียกว่า SSL stripping ถูกนำเสนอในงานประชุม Blackhat Conference ปี 2009 การโจมตีประเภทนี้ทำลายความปลอดภัยของ HTTPS โดยการเปลี่ยนลิงก์ https: ให้เป็นลิงก์ http: โดยใช้ประโยชน์จากข้อเท็จจริงที่ว่าผู้ใช้อินเทอร์เน็ตเพียงไม่กี่คนเท่านั้นที่พิมพ์ “https” ลงในอินเทอร์เฟซเบราว์เซอร์ พวกเขาจึงเข้าสู่เว็บไซต์ที่ปลอดภัยได้โดยการคลิกลิงก์ และถูกหลอกให้คิดว่ากำลังใช้ HTTPS ในขณะที่จริงๆ แล้วกำลังใช้ HTTP ผู้โจมตีจึงสื่อสารกับไคลเอ็นต์อย่างชัดเจน สิ่งนี้กระตุ้นให้เกิดการพัฒนามาตรการรับมือใน HTTP ที่เรียกว่า HTTP Strict Transport Security

HTTPS ได้รับการพิสูจน์แล้วว่ามีความเสี่ยงต่อการโจมตีวิเคราะห์ทราฟฟิกหลากหลายรูปแบบ การโจมตีวิเคราะห์ทราฟฟิกเป็นการโจมตีแบบ Side-Channel ประเภทหนึ่งที่อาศัยการเปลี่ยนแปลงเวลาและขนาดของทราฟฟิกเพื่ออนุมานคุณสมบัติของทราฟฟิกที่เข้ารหัส การวิเคราะห์ทราฟฟิกเป็นไปได้เนื่องจากการเข้ารหัส SSL/TLS เปลี่ยนแปลงเนื้อหาของทราฟฟิก แต่มีผลกระทบน้อยมากต่อขนาดและระยะเวลาของทราฟฟิก ในเดือนพฤษภาคม 2553 งานวิจัยโดยนักวิจัยจาก Microsoft Research และ Indiana University ค้นพบว่าข้อมูลผู้ใช้ที่ละเอียดอ่อนโดยละเอียดสามารถอนุมานได้จากช่องทางด้านข้าง เช่น ขนาดแพ็กเก็ต นักวิจัยพบว่าแม้จะมีการป้องกัน HTTPS ในแอปพลิเคชันเว็บชั้นนำที่มีชื่อเสียงหลายตัวในด้านการดูแลสุขภาพ ภาษี การลงทุน และการค้นหาเว็บ แต่ผู้แอบฟังสามารถอนุมานโรค/ยา/การผ่าตัดของผู้ใช้ รายได้ของครอบครัว และความลับในการลงทุนได้

ความจริงที่ว่าเว็บไซต์สมัยใหม่ส่วนใหญ่ รวมถึง Google, Yahoo! และ Amazon ใช้ HTTPS ทำให้เกิดปัญหาสำหรับผู้ใช้จำนวนมากที่พยายามเข้าถึงจุดเชื่อมต่อ Wi-Fi สาธารณะ เนื่องจากหน้าเข้าสู่ระบบจุดเชื่อมต่อ Wi-Fi ของพอร์ทัลแบบแคปทีฟไม่สามารถโหลดได้หากผู้ใช้พยายามเปิดทรัพยากร HTTPS และเว็บไซต์หลายแห่ง เช่น NeverSSL รับประกันว่าเว็บไซต์เหล่านั้นจะสามารถเข้าถึงได้ผ่าน HTTP เสมอ

2.5 เกณฑ์วิธีความมั่นคงของชั้นขนส่ง (Transport Layer Security; TLS)

เกณฑ์วิธีความมั่นคงของชั้นขนส่ง (Transport Layer Security; TLS) เป็นโปรโตคอลการเข้ารหัสที่ออกแบบมาเพื่อรักษาความปลอดภัยการสื่อสารบนเครือข่ายคอมพิวเตอร์เช่นอินเทอร์เน็ต โปรโตคอลนี้ถูกใช้อย่างแพร่หลายในแอปพลิเคชันต่างๆเช่นอีเมลการส่งข้อความโต้ตอบแบบทันทีและบริการเสียงผ่าน IP แต่การใช้งานเพื่อรักษาความปลอดภัย HTTPS ยังคงเป็นที่เปิดเผยต่อสาธารณะมากที่สุด

โปรโตคอล TLS มีวัตถุประสงค์หลักเพื่อรักษาความปลอดภัย รวมถึงความเป็นส่วนตัว (ความลับ) ความสมบูรณ์ และความถูกต้อง ผ่านการใช้การเข้ารหัสเช่น การใช้ใบรับรองระหว่างแอปพลิเคชันคอมพิวเตอร์ที่สื่อสารกันตั้งแต่สองแอปพลิเคชันขึ้นไป โปรโตคอลนี้ทำงานในเลเยอร์การนำเสนอและประกอบด้วยสองชั้น ได้แก่ ระเบียน TLS และโปรโตคอล TLS handshake

Datagram Transport Layer Security (DTLS) ซึ่งเป็นโปรโตคอลการสื่อสารที่เกี่ยวข้องอย่างใกล้ชิดมอบความปลอดภัยให้กับ แอปพลิเคชันที่ใช้ ดาต้าแกรมในงานเขียนทางเทคนิค มักพบการอ้างอิงถึง “(D)TLS” เมื่อใช้กับทั้งสองเวอร์ชัน

TLS เป็นมาตรฐานที่ได้รับการเสนอโดย Internet Engineering Task Force (IETF) ซึ่งกำหนดขึ้นครั้งแรกในปี 1999 และเวอร์ชันปัจจุบันคือ TLS 1.3 ซึ่งกำหนดขึ้นในเดือนสิงหาคม 2018 TLS สร้างขึ้นจาก ข้อกำหนด SSL (Secure Sockets Layer) ที่ไม่รองรับอีกต่อไป (1994, 1995, 1996) ซึ่งพัฒนาโดย Netscape Communications เพื่อเพิ่มโปรโตคอล HTTPS ลงในเว็บเบราว์เซอร์ Netscape Navigator

2.5.1 คำอธิบาย

เนื่องจากแอปพลิเคชันสามารถสื่อสารได้ทั้งแบบมีหรือไม่มี TLS (หรือ SSL) จึงจำเป็นที่ไคลเอนต์จะต้องร้องขอให้เซิร์ฟเวอร์ตั้งค่าการเชื่อมต่อ TLS หนึ่งในวิธีหลักในการทำเช่นนี้คือการใช้หมายเลขพอร์ต อื่น สำหรับการเชื่อมต่อ TLS โดยทั่วไปแล้ว พอร์ต 80 จะใช้สำหรับ การรับส่งข้อมูล HTTP ที่ไม่ได้เข้ารหัส ในขณะที่พอร์ต 443 เป็นพอร์ตทั่วไปที่ใช้สำหรับ การรับส่งข้อมูล HTTPS ที่เข้ารหัส อีกกลไกหนึ่งคือการสร้างคำขอ STARTTLS เฉพาะโปรโตคอลไปยังเซิร์ฟเวอร์เพื่อสลับการเชื่อมต่อกับ TLS ตัวอย่างเช่น เมื่อใช้โปรโตคอลอีเมลและข่าวสารบางอย่าง

เมื่อไคลเอนต์และเซิร์ฟเวอร์ตกลงที่จะใช้ TLS แล้ว พวกเขาจะเจรจา การเชื่อมต่อ แบบมีสถานะโดยใช้ขั้นตอนการจับมือ (ดูการจับมือ TLS) โปรโตคอลใช้การจับมือกับรหัสแบบอสมมาตรเพื่อกำหนดค่าการเข้ารหัสไม่เพียงเท่านั้น แต่ยังรวมถึงคีย์ที่ใช้ร่วมกันเฉพาะเซสชัน ซึ่งการสื่อสารต่อไปจะถูกเข้ารหัสโดยใช้รหัสแบบสมมาตรในระหว่างการจับมือนี้ ไคลเอนต์และเซิร์ฟเวอร์จะตกลงกันเกี่ยวกับพารามิเตอร์ต่างๆ ที่ใช้สร้างความปลอดภัยของการเชื่อมต่อ:

- การจับมือเริ่มต้นเมื่อไคลเอนต์เชื่อมต่อกับเซิร์ฟเวอร์ที่เปิดใช้งาน TLS เพื่อขอการเชื่อมต่อที่ปลอดภัยและไคลเอนต์แสดงรายการชุดรหัสที่รองรับ (รหัสและฟังก์ชันแฮช)
- จากรายการนี้ เซิร์ฟเวอร์จะเลือกฟังก์ชันรหัสและแฮชที่รองรับ และแจ้งให้ไคลเอนต์ทราบถึงการตัดสินใจ
- โดยปกติแล้วเซิร์ฟเวอร์จะระบุตัวตนในรูปแบบของใบรับรองดิจิทัลใบรับรองประกอบด้วยชื่อเซิร์ฟเวอร์ผู้ให้บริการออกใบรับรอง (CA) ที่เชื่อถือได้ซึ่งรับรองความถูกต้องของใบรับรอง และคีย์การเข้ารหัสสาธารณะของเซิร์ฟเวอร์
- ลูกค้าต้องยืนยันความถูกต้องของใบรับรองก่อนดำเนินการต่อ
- ในการสร้างคีย์เซสชันที่ใช้สำหรับการเชื่อมต่อที่ปลอดภัย ไคลเอนต์จะต้องทำดังนี้:
    - เข้ารหัสตัวเลขสุ่ม (PreMasterSecret) ด้วยคีย์สาธารณะของเซิร์ฟเวอร์และส่งผลลัพธ์ไปยังเซิร์ฟเวอร์ (ซึ่งเฉพาะเซิร์ฟเวอร์เท่านั้นที่จะสามารถถอดรหัสด้วยคีย์ส่วนตัว) จากนั้นทั้งสองฝ่ายใช้ตัวเลขสุ่มเพื่อสร้างคีย์เซสชันเฉพาะสำหรับการเข้ารหัสและถอดรหัสข้อมูลในระหว่างเซสชันในภายหลังหรือ
    - ใช้การแลกเปลี่ยนคีย์ Diffie–Hellman (หรือรูปแบบ DH ที่เป็นเส้นโค้งวงรี) เพื่อสร้างคีย์เซสชันแบบสุ่มและไม่ซ้ำกันอย่างปลอดภัยสำหรับการเข้ารหัสและถอดรหัส ซึ่งมีคุณสมบัติเพิ่มเติมของการปกปิดแบบส่งต่อ : หากคีย์ส่วนตัวของเซิร์ฟเวอร์ถูกเปิดเผยในอนาคต จะไม่

สามารถใช้คีย์นั้นเพื่อถอดรหัสเซสชันปัจจุบันได้ แม้ว่าเซสชันนั้นจะถูกดักจับและบันทึกโดยบุคคลที่สามก็ตาม

การดำเนินการนี้จะสิ้นสุดการจับมือและเริ่มการเชื่อมต่อที่ปลอดภัยซึ่งจะถูกเข้ารหัสและถอดรหัสด้วยคีย์เซสชันจนกว่าการเชื่อมต่อจะสิ้นสุดลงหากขั้นตอนใดขั้นตอนหนึ่งข้างต้นล้มเหลวการจับมือ TLS จะล้มเหลวและการเชื่อมต่อจะไม่ถูกสร้างขึ้น

TLS และ SSL ไม่สามารถจัดวางได้อย่างลงตัวในเลเยอร์ใดเลเยอร์หนึ่งของแบบจำลอง OSI หรือแบบจำลอง TCP/IP TLS ทำงาน “บนโปรโตคอลการขนส่งที่เชื่อถือได้ (เช่น TCP)”ซึ่งหมายความว่ามันอยู่เหนือเลเยอร์การขนส่งมันทำหน้าที่เข้ารหัสให้กับเลเยอร์ที่สูงกว่า ซึ่งโดยปกติแล้วเป็นหน้าที่ของเลเยอร์การนำเสนออย่างไรก็ตาม โดยทั่วไปแอปพลิเคชันจะใช้ TLS เหมือนกับเป็นเลเยอร์การขนส่งแม้ว่าแอปพลิเคชันที่ใช้ TLS จะต้องควบคุมการเริ่มต้นการจับมือ TLS และการจัดการใบรับรองการตรวจสอบสิทธิ์ที่แลกเปลี่ยนกัน

เมื่อได้รับการรักษาความปลอดภัยโดย TLS การเชื่อมต่อระหว่างไคลเอนต์ (เช่น เว็บเบราว์เซอร์) และเซิร์ฟเวอร์ (เช่น wikipedia.org) จะมีคุณสมบัติทั้งหมดดังต่อไปนี้

- การเชื่อมต่อเป็นแบบส่วนตัว (หรือมีความลับ) เนื่องจาก มีการใช้ อัลกอริทึมคีย์แบบสมมาตรในการเข้ารหัสข้อมูลที่ส่ง คีย์สำหรับการเข้ารหัสแบบสมมาตรนี้จะถูกสร้างขึ้นอย่างเฉพาะเจาะจงสำหรับแต่ละการเชื่อมต่อ และอิงจากความลับร่วมที่เจรจากันไว้เมื่อเริ่มต้นเซสชัน เซิร์ฟเวอร์และไคลเอ็นต์จะเจรจารายละเอียดเกี่ยวกับอัลกอริทึมการเข้ารหัสและคีย์การเข้ารหัสที่จะใช้ก่อนที่จะส่งข้อมูลไบต์แรก (ดูด้านล่าง) การเจรจาความลับร่วมนั้นทั้งปลอดภัย (ความลับที่เจรจากันไว้จะไม่สามารถเข้าถึงได้โดยผู้ดักฟังและไม่สามารถได้รับ แม้แต่โดยผู้โจมตีที่วางตัวเองอยู่ตรงกลางการเชื่อมต่อ) และเชื่อถือได้ (ไม่มีผู้โจมตีคนใดสามารถแก้ไขการสื่อสารระหว่างการเจรจาโดยไม่ถูกตรวจพบ)
- การยืนยันตัวตนของฝ่ายที่สื่อสารสามารถยืนยันได้โดยใช้การเข้ารหัสด้วยคีย์สาธารณะการยืนยันตัวตนนี้จำเป็นสำหรับเซิร์ฟเวอร์และเป็นทางเลือกสำหรับไคลเอนต์
- การเชื่อมต่อมีความน่าเชื่อถือ (หรือมีความสมบูรณ์) เนื่องจากข้อความแต่ละข้อความที่ส่งออกจะมีการตรวจสอบความสมบูรณ์ของข้อความโดยใช้รหัสยืนยันข้อความเพื่อป้องกันการสูญหายหรือการเปลี่ยนแปลงข้อมูลที่ไม่ถูกตรวจพบระหว่างการส่งข้อมูล

TLS รองรับวิธีการที่หลากหลายสำหรับการแลกเปลี่ยนคีย์ การเข้ารหัสข้อมูล และการตรวจสอบความถูกต้องของข้อความ ดังนั้น การกำหนดค่า TLS อย่างปลอดภัยจึงเกี่ยวข้องกับพารามิเตอร์ที่กำหนดค่าได้มากมาย และตัวเลือกทั้งหมดไม่ได้มีคุณสมบัติที่เกี่ยวข้องกับความเป็นส่วนตัวทั้งหมดที่อธิบายไว้ในรายการด้านบน (ดูตารางด้านล่าง การแลกเปลี่ยนคีย์ ความปลอดภัยของการเข้ารหัสและความสมบูรณ์ของข้อมูล)

มีการพยายามบ่อนทำลายแง่มุมด้านความปลอดภัยในการสื่อสารที่ TLS มุ่งหวังจะมอบให้ และโปรโตคอลนี้ได้รับการแก้ไขหลายครั้งเพื่อจัดการกับภัยคุกคามด้านความปลอดภัยเหล่านี้ นักพัฒนาเว็บเบราว์เซอร์ได้ปรับปรุงผลิตภัณฑ์ของตนซ้ำแล้วซ้ำเล่าเพื่อป้องกันจุดอ่อนด้านความปลอดภัยที่อาจเกิดขึ้นหลังจากค้นพบจุดอ่อนเหล่านี้ (ดูประวัติการสนับสนุน TLS/SSL ของเว็บเบราว์เซอร์) ความปลอดภัยของเลเยอร์การขนส่งดาต้าแกรม

Datagram Transport Layer Security หรือเรียกย่อๆ ว่า DTLS เป็นโปรโตคอลการสื่อสาร ที่เกี่ยวข้องซึ่งให้ความปลอดภัยแก่ แอปพลิเคชันที่ใช้ Datagram โดยอนุญาตให้แอปพลิเคชันสื่อสารในลักษณะที่ออกแบบมาเพื่อป้องกันการดักฟัง การปลอมแปลงหรือการปลอมแปลงข้อความโปรโตคอล DTLS ใช้ โปรโตคอล Transport Layer Security (TLS) ที่เน้น การสตรีมและมีจุดประสงค์เพื่อให้การรับประกันความปลอดภัยที่คล้ายคลึงกัน อย่างไรก็ตาม โปรโตคอลนี้แตกต่างจาก TLS ตรงที่สามารถใช้งานร่วมกับโปรโตคอลที่เน้น Datagram ส่วนใหญ่ ได้แก่User Datagram Protocol (UDP), Datagram Congestion Control Protocol (DCCP), Control And Provisioning of Wireless Access Points (CAPWAP), Stream Control Transmission Protocol (SCTP) encapsulation และSecure Real-time Transport Protocol (SRTP)

เนื่องจากเดตาแกรมของโปรโตคอล DTLS รักษาความหมายของการขนส่งพื้นฐานไว้ แอปพลิเคชันจึงไม่ประสบปัญหาความล่าช้าที่เกี่ยวข้องกับโปรโตคอลสตรีม อย่างไรก็ตาม แอปพลิเคชันต้องจัดการกับการเรียงลำดับแพ็กเก็ตใหม่ การสูญหายของเดตาแกรม และข้อมูลที่มีขนาดใหญ่กว่าขนาดของแพ็กเก็ตเครือข่าย เดตาแกรม เนื่องจาก DTLS ใช้ UDP หรือ SCTP แทน TCP จึงหลีกเลี่ยงปัญหา TCP ล่มเมื่อนำไปใช้สร้างอุโมงค์ VPN

DTLS เวอร์ชัน 1.0 ฉบับดั้งเดิมในปี 2006 ไม่ใช่เอกสารแบบสแตนด์อโลน แต่ได้รับการกำหนดให้เป็นชุดเดลต้าของ TLS 1.1 ทำนองเดียวกัน DTLS เวอร์ชัน 2012 ที่ตามมาก็ถูกกำหนดให้เป็นเดลต้าของ TLS 1.2 โดยได้รับหมายเลขเวอร์ชันของ DTLS 1.2 เพื่อให้ตรงกับเวอร์ชัน TLS สุดท้าย DTLS 1.3 ปี 2022 ก็ถูกกำหนดให้เป็นเดลต้าของ TLS 1.3 เช่นเดียวกับสองเวอร์ชันก่อนหน้า DTLS 1.3 มีวัตถุประสงค์เพื่อให้ “การรับประกันความปลอดภัยที่เทียบเท่า [กับ TLS 1.3] ยกเว้นการป้องกันคำสั่ง/การไม่สามารถเล่นซ้ำได้”

ไคลเอนต์ VPN จำนวนมากรวมถึง Cisco AnyConnect & InterCloud Fabric, OpenConnect, อุโมงค์ ZScaler, F5 Networks Edge VPN Client และ Citrix Systems NetScaler ใช้ DTLS เพื่อรักษาความปลอดภัยการรับส่งข้อมูล UDP นอกจากนี้ เว็บเบราว์เซอร์สมัยใหม่ทั้งหมดยังรองรับ DTLS-SRTP สำหรับ WebRTC

2.5.2 X.509 (รูปแบบใบรับรอง TLS/SSL)

ในการเข้ารหัส X.509 เป็นมาตรฐานของสหภาพโทรคมนาคมระหว่างประเทศ (ITU) ที่กำหนดรูปแบบของใบรับรองคีย์สาธารณะใบรับรอง X.509 ถูกใช้ในโปรโตคอลอินเทอร์เน็ตมากมายรวมถึง TLS/SSL ซึ่งเป็นพื้นฐานของ HTTPS โปรโตคอลที่ปลอดภัยสำหรับการท่องเว็บ นอกจากนี้ยังใช้ในแอปพลิเคชันออฟไลน์เช่น ลาย เซ็นอิเล็กทรอนิกส์ ใบรับรอง X.509 เชื่อมโยงข้อมูลประจำตัวกับคีย์สาธารณะโดยใช้ลายเซ็นดิจิทัล ใบรับรองประกอบด้วยข้อมูลประจำตัว (ชื่อโฮสต์องค์กร หรือบุคคล) และคีย์สาธารณะ (RSA, DSA, ECDSA, ed25519 เป็นต้น) ซึ่งลงนามโดยผู้ออกใบรับรองหรือลงนามด้วยตนเอง เมื่อใบรับรองได้รับการลงนามโดยผู้ออกใบรับรองที่เชื่อถือได้หรือผ่านการตรวจสอบความถูกต้องด้วยวิธีอื่น ผู้ถือใบรับรองนั้นสามารถใช้คีย์สาธารณะที่มีอยู่เพื่อสร้างการสื่อสารที่ปลอดภัยกับบุคคลอื่น หรือตรวจสอบความถูกต้องของเอกสารที่ลงนามดิจิทัลด้วย คีย์ส่วนตัวที่เกี่ยวข้องได้

X.509 ยังกำหนดรายการเพิกถอนใบรับรองซึ่งเป็นวิธีการแจกจ่ายข้อมูลเกี่ยวกับใบรับรองที่ถือว่าไม่ถูกต้องโดยผู้มีอำนาจลงนาม ตลอดจนอัลกอริทึมการตรวจสอบเส้นทางการรับรองซึ่งช่วยให้ใบ

รับรองได้รับการลงนามโดยใบรับรอง CA ตัวกลาง ซึ่งใบรับรองเหล่านี้จะได้รับการลงนามโดยใบรับรองอื่นๆ ต่อไปจนไปถึงจุดยึดที่เชื่อถือได้ในที่สุด

X.509 ถูกกำหนดโดย “Standardization Sector” ของ ITU (SG17 ของ ITU-T) ใน ITU-T Study Group 17 และมีพื้นฐานมาจาก Abstract Syntax Notation One (ASN.1) ซึ่งเป็นมาตรฐานอีกประการหนึ่งของ ITU-T

2.5.2.1 โครงสร้างของใบรับรอง

โครงสร้างที่กำหนดไว้โดยมาตรฐานจะแสดงอยู่ในภาษาทางการที่เรียกว่า Abstract Syntax Notation One (ASN.1)

โครงสร้างของใบรับรองดิจิทัล X.509 v3 มีดังนี้:

- ใบรับรอง
  - หมายเลขเวอร์ชัน
  - หมายเลขซีเรียล
  - รหัสอัลกอริทึมลายเซ็น
  - ชื่อผู้ออก
  - ระยะเวลาใช้งาน
    - ไม่ก่อน
    - ไม่หลังจากนั้น
  - ชื่อเรื่อง
  - ข้อมูลคีย์สาธารณะของเรื่อง
    - อัลกอริทึมคีย์สาธารณะ
    - คีย์สาธารณะของเรื่อง รหัสประจำตัวผู้ออก (ทางเลือก) รหัสประจำตัวเฉพาะเรื่อง (ทางเลือก) ส่วนขยาย (ทางเลือก)
  - อัลกอริทึมลายเซ็นใบรับรอง
  - ลายเซ็นใบรับรอง

ฟิลด์ส่วนขยาย (ถ้ามี) จะเป็นลำดับของส่วนขยายใบรับรองอย่างน้อยหนึ่งรายการ แต่ละส่วนขยายมีรหัสประจำตัวเฉพาะของตัวเอง ซึ่งแสดงเป็นตัวระบุวัตถุ (OID) ซึ่งเป็นชุดค่าพร้อมกับข้อบ่งชี้ที่สำคัญหรือไม่สำคัญ ระบบที่ใช้ใบรับรองต้องปฏิเสธใบรับรองหากพบส่วนขยายที่สำคัญที่ไม่รู้จักหรือส่วนขยายที่สำคัญซึ่งมีข้อมูลที่ไม่สามารถประมวลผลได้ ส่วนขยายที่ไม่สำคัญอาจถูกละเว้นหากไม่รู้จัก แต่จะต้องได้รับการประมวลผลหากรู้จักส่วนขยายใบรับรอง

โครงสร้างของเวอร์ชัน 1 มีอยู่ ใน RFC 1422

รูปแบบภายในของตัวระบุเฉพาะของผู้เผยแพร่และเรื่องที่ระบุไว้ใน X.520 ไดเร็กทอรี:คำแนะนำ ประเภทแอตทริบิวต์ที่เลือก

ITU-T ได้นำตัวระบุเฉพาะของผู้ออกหลักทรัพย์และบุคคลมาใช้ในเวอร์ชัน 2 เพื่ออนุญาตให้นำชื่อผู้ออกหลักทรัพย์หรือบุคคลมาใช้ซ้ำได้หลังจากระยะเวลาหนึ่ง ตัวอย่างหนึ่งของการนำกลับมาใช้ซ้ำคือเมื่อ CA ล้มละลายและชื่อถูกลบออกจากรายชื่อสาธารณะของประเทศ หลังจากนั้น CA อื่นที่มีชื่อ

เดียวกันอาจลงทะเบียนตัวเองได้ แม้ว่าจะไม่เกี่ยวข้องกับ CA แรกก็ตาม อย่างไรก็ตาม IETF แนะนำว่าไม่ควรนำชื่อผู้ออกหลักทรัพย์และบุคคลมาใช้ซ้ำ ดังนั้นเวอร์ชัน 2 จึงยังไม่แพร่หลายในอินเทอร์เน็ต

ส่วนขยายได้รับการแนะนำในเวอร์ชัน 3 CA สามารถใช้ส่วนขยายเพื่อออกใบรับรองได้เฉพาะสำหรับจุดประสงค์เฉพาะ (เช่น สำหรับการลงนามในวัตถุดิจิทัล เท่านั้น)

ในทุกเวอร์ชันหมายเลขซีเรียลจะต้องไม่ซ้ำกันสำหรับใบรับรองแต่ละใบที่ออกโดย CA เฉพาะ (ดังที่กล่าวถึงใน RFC 5280)

2.5.2.2 นามสกุลไฟล์ใบรับรอง

นามสกุลไฟล์ที่ใช้กันทั่วไปสำหรับใบรับรอง X.509 มีหลายประเภทนามสกุลไฟล์เหล่านี้ยังใช้สำหรับข้อมูลอื่นๆ เช่น คีย์ส่วนตัวด้วย

- **.pem** – (อีเมลอิเล็กทรอนิกส์ที่เพิ่มความเป็นส่วนตัว) ใบรับรอง DER ที่เข้ารหัส Base64 แนบระหว่าง **———BEGIN CERTIFICATE———** และ **———END CERTIFICATE———**
- **.cer**, **.crt**, **.der** – โดยปกติจะอยู่ในรูปแบบไบนารี DER แต่ใบรับรองที่เข้ารหัส Base64 ก็เป็นเรื่องปกติเช่นกัน (ดู **.pem** ด้านบน)
- **.p8**, **.p8e**, **.pk8** – คีย์ส่วนตัวที่ส่งออกตามที่ระบุไว้ใน PKCS#8 อาจอยู่ในรูปแบบ DER หรือ PEM ที่ขึ้นต้นด้วย **———BEGIN PRIVATE KEY———** คีย์ที่เข้ารหัสจะขึ้นต้นด้วย **———BEGIN ENCRYPTED PRIVATE KEY———** และอาจมี **.p8e** เป็นนามสกุลไฟล์
- **.p10**, **.csr** – PKCS#10 เป็นคำขอลงนามใบรับรอง (CSR) ในรูปแบบ PEM ขึ้นต้นด้วย **———BEGIN CERTIFICATE REQUEST———** แบบฟอร์มเหล่านี้สร้างขึ้นเพื่อส่งไปยังผู้ออกใบรับรอง (CA) แบบฟอร์มประกอบด้วยรายละเอียดสำคัญของใบรับรองที่ร้องขอ เช่น ชื่อสามัญ (/CN), หัวเรื่อง, องค์กร, รัฐ, ประเทศ รวมถึงคีย์สาธารณะของใบรับรองที่ต้องการให้ลงนาม คีย์เหล่านี้จะได้รับการลงนามโดย CA และใบรับรองจะถูกส่งกลับคืน ใบรับรองที่ส่งคืนคือใบรับรอง สาธารณะ (ซึ่งมีคีย์สาธารณะแต่ไม่มีคีย์ส่วนตัว) ซึ่งตัวใบรับรองเองสามารถอยู่ในรูปแบบต่างๆ ได้หลายรูปแบบ แต่โดยปกติจะเป็น **.p7r**
- **.p7r** – คำตอบ ของ PKCS#7 ต่อ CSR ประกอบด้วยใบรับรองที่เพิ่งลงนาม และใบรับรองของ CA เอง
- **.p7s** – ลายเซ็นดิจิทัล PKCS#7 อาจมีไฟล์หรือข้อความที่ลงนามต้นฉบับ ใช้ใน S/MIME สำหรับการลงนามในอีเมลกำหนดไว้ใน RFC 2311
- **.p7m** – PKCS#7 (SignedData, EnvelopedData) ข้อความ เช่น ไฟล์ที่เข้ารหัส (“enveloped”) ข้อความ หรือจดหมายอีเมล MIME กำหนดไว้ใน RFC 2311
- **.p7c** – โครงสร้าง SignedData แบบ “certs-only” ของ PKCS#7 ที่เสื่อมลง โดยไม่มีข้อมูลใดๆ ให้ลงนาม กำหนดไว้ใน RFC 2311
- **.p7b** – โครงสร้าง SignedData ของ PKCS#7 ที่ไม่มีข้อมูล มีเพียงใบรับรองแบบบันเดิลและ/หรือ CRL (ไม่ค่อยเกิดขึ้น) แต่ไม่มีคีย์ส่วนตัว ใช้รูปแบบ DER หรือ BER หรือ PEM ที่ขึ้นต้นด้วย **———BEGIN PKCS7———** รูปแบบที่ Windows ใช้สำหรับการแลกเปลี่ยนใบรับรอง รองรับโดย Java แต่มักใช้นามสกุล **.keystore** แทน ซึ่งแตกต่างจากใบรับรองแบบ **.pem** รูปแบบนี้มีวิธีที่กำหนดไว้สำหรับการรวมใบรับรองเส้นทางการรับรอง

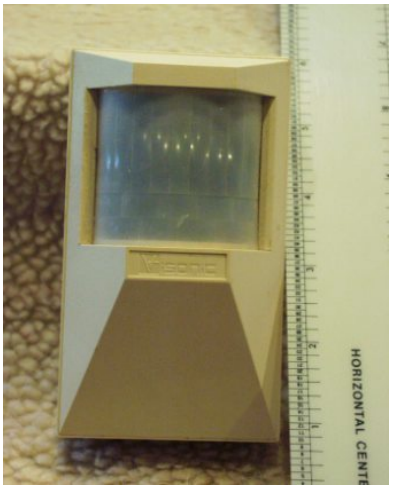
- **.p12**, **.pfx**, **.pkcs12** – PKCS#12 อาจมีใบรับรอง (สาธารณะ) และคีย์ส่วนตัว (ป้องกันด้วยรหัสผ่าน) ในไฟล์เดียว **.pfx** - *Personal Information eXchange* PFX ซึ่งเป็นรุ่นก่อนของ PKCS#12 (โดยปกติจะมีข้อมูลในรูปแบบ PKCS#12 เช่น ไฟล์ PFX ที่สร้างใน IIS)
- **.crl** – รายการเพิกถอนใบรับรอง (CRL) หน่วยงานที่ออกใบรับรองจะจัดทำรายการเหล่านี้ขึ้นเพื่อใช้ในการเพิกถอนใบรับรองก่อนหมดอายุ

PKCS#7 เป็นมาตรฐานสำหรับการลงนามหรือเข้ารหัสข้อมูล (เรียกอย่างเป็นทางการว่า "enveloping") เนื่องจากจำเป็นต้องใช้ใบรับรองเพื่อตรวจสอบข้อมูลที่ลงนามแล้วจึงสามารถรวมใบรับรองไว้ในโครงสร้าง SignedData ได้

2.6 การสื่อสารสนามใกล้ (Near-field communication; NFC)

2.7 เซ็นเซอร์อินฟราเรดแบบพาสซีฟ (PIR sensor)

เซ็นเซอร์อินฟราเรดแบบพาสซีฟ (PIR sensor) คือ เซ็นเซอร์อิเล็กทรอนิกส์ที่วัด แสงอินฟราเรด (IR) ที่แผ่ออกมาจากวัตถุในระยะการมองเห็น เซ็นเซอร์ชนิดนี้มักใช้ในเครื่องตรวจจับความเคลื่อนไหว แบบ PIR เซ็นเซอร์ PIR มักใช้ในสัญญาณเตือนภัยและระบบไฟส่องสว่างอัตโนมัติ



รูปที่ 2.7.0.1: เครื่องตรวจจับการเคลื่อนไหวแบบ PIR ทั่วไปสำหรับที่พักอาศัย/เชิงพาณิชย์

เซ็นเซอร์ PIR ตรวจจับการเคลื่อนไหวทั่วไป แต่ไม่ได้ให้ข้อมูลว่าใครหรือสิ่งใดเคลื่อนไหว ดังนั้น จึงจำเป็นต้องใช้ เซ็นเซอร์ IR แบบสร้างภาพ เซ็นเซอร์ PIR มักเรียกสั้นๆ ว่า "PIR" หรือบางครั้งเรียกว่า "PID" ซึ่งย่อมาจาก "เครื่องตรวจจับอินฟราเรดแบบพาสเซ็นเซอร์ PIR ตรวจจับการเคลื่อนไหวทั่วไป แต่ไม่ได้ให้ข้อมูลว่าใครหรือสิ่งใดเคลื่อนไหว ดังนั้น จึงจำเป็นต้องใช้ เซ็นเซอร์ IR แบบสร้างภาพ เซ็นเซอร์ PIR มักเรียกสั้นๆ ว่า "PIR" หรือบางครั้งเรียกว่า "PID" ซึ่งย่อมาจาก "เครื่องตรวจจับอินฟราเรดแบบพาสซีฟ" คำว่าพาสซีฟหมายถึงข้อเท็จจริงที่ว่าอุปกรณ์ PIR ไม่ได้แผ่พลังงานเพื่อจุดประสงค์ในการตรวจจับ แต่ทำงานโดยการตรวจจับรังสีอินฟราเรด (ความร้อนจากการแผ่รังสี) ที่แผ่ออกมาจากหรือสะท้อนจากวัตถุ เท่านั้นซีฟ" คำว่าพาสซีฟหมายถึงข้อเท็จจริงที่ว่าอุปกรณ์ PIR ไม่ได้แผ่พลังงานเพื่อจุดประสงค์ในการตรวจจับ แต่ทำงานโดยการตรวจจับรังสีอินฟราเรด (ความร้อนจากการแผ่รังสี) ที่แผ่ออกมาจากหรือสะท้อนจากวัตถุ เท่านั้น

2.7.1 หลักการทำงาน

วัตถุทุกชนิดที่มีอุณหภูมิสูงกว่าศูนย์องศาสัมบูรณ์จะปล่อย พลังงาน ความร้อน ออก มาในรูปของรังสีแม่เหล็กไฟฟ้า โดยปกติแล้วรังสีนี้มองไม่เห็นด้วยตาเปล่าเนื่องจากแผ่รังสีในช่วงความยาวคลื่นอินฟราเรด แต่อุปกรณ์อิเล็กทรอนิกส์ที่ออกแบบมาเพื่อจุดประสงค์นี้ สามารถตรวจจับได้

2.7.2 เครื่องตรวจจับการเคลื่อนไหวแบบ PIR

รูปที่ 2.7.2.1: เครื่องตรวจจับความเคลื่อนไหว PIR ใช้สำหรับควบคุมไฟภายนอกอาคารแบบอัตโนมัติ

รูปที่ 2.7.2.2: กล้องดักถ่ายพร้อมระบบตรวจจับความเคลื่อนไหวแบบ PIR

รูปที่ 2.7.2.3: สวิตช์ไฟภายในอาคารที่ติดตั้งเซนเซอรตรวจจับการครอบครองแบบ PIR

เครื่องตรวจจับความเคลื่อนไหวแบบ PIR ใช้เพื่อตรวจจับการเคลื่อนไหวของคน สัตว์ หรือวัตถุอื่นๆ มักใช้กับสัญญาณกันขโมยและระบบไฟส่องสว่างแบบอัตโนมัติ

2.7.3 การดำเนินการ

เซ็นเซอร์ PIR สามารถตรวจจับการเปลี่ยนแปลงของปริมาณรังสีอินฟราเรดที่กระทบกับวัตถุ ซึ่งจะแตกต่างกันไปขึ้นอยู่กับอุณหภูมิและลักษณะพื้นผิวของวัตถุที่อยู่ด้านหน้าเซ็นเซอร์เมื่อวัตถุ เช่น บุคคล ผ่านด้านหน้าพื้นหลัง เช่น กำแพง อุณหภูมิ ณ จุดนั้นในมุมมองของเซ็นเซอร์จะเพิ่มขึ้นจากอุณหภูมิห้องเป็นอุณหภูมิร่างกายแล้วกลับมาอีกครั้ง เซ็นเซอร์จะแปลงการเปลี่ยนแปลงที่เกิดขึ้นของรังสีอินฟราเรดที่เข้ามาเป็นการเปลี่ยนแปลงของแรงดันไฟฟ้าขาออก และสิ่งนี้จะกระตุ้นการตรวจจับวัตถุที่มีอุณหภูมิใกล้เคียงกันแต่มีลักษณะพื้นผิวต่างกันอาจมีรูปแบบการปล่อยรังสีอินฟราเรดที่แตกต่างกัน ดังนั้นการเคลื่อนย้ายวัตถุเทียบกับพื้นหลังอาจกระตุ้นเครื่องตรวจจับได้เช่นกัน

PIR มีหลายรูปแบบการใช้งานที่หลากหลาย รุ่นที่นิยมใช้กันมากที่สุดมีเลนส์เฟรสเนลหรือส่วนกระจกจำนวนมาก ระยะการทำงานประมาณ 10 เมตร (30 ฟุต) และมุมมองภาพน้อยกว่า 180° มีรุ่นที่มีมุมมองภาพกว้างกว่า รวมถึง 360° ซึ่งโดยทั่วไปออกแบบมาเพื่อติดตั้งบนเพดาน PIR ขนาดใหญ่บางรุ่นผลิตด้วยกระจกส่วนเดียวและสามารถตรวจจับการเปลี่ยนแปลงของพลังงานอินฟราเรดได้ในระยะ 30 เมตร (100 ฟุต) จาก PIR นอกจากนี้ยังมี PIR ที่ออกแบบด้วยกระจกแบบปรับทิศทางได้ ซึ่งสามารถครอบคลุมพื้นที่ได้กว้าง (110°) หรือครอบคลุมพื้นที่แคบมากแบบ “ม่าน” หรือสามารถเลือกส่วนกระจกแยกแต่ละส่วนเพื่อ “ปรับแต่ง” พื้นที่ครอบคลุมได้

2.7.4 การตรวจจับความแตกต่าง

เซ็นเซอร์หลายตัวอาจเชื่อมต่อเป็นอินพุตตรงข้ามกับเครื่องขยายสัญญาณดิฟเฟอเรนเชียล ในรูปแบบนี้ การวัดค่า PIR จะหักล้างกันเอง ทำให้อุณหภูมิเฉลี่ยของระยะการมองเห็นถูกตัดออกจากสัญญาณไฟฟ้า การเพิ่มขึ้นของพลังงานอินฟราเรดทั่วทั้งเซ็นเซอร์จะหักล้างตัวเองและจะไม่กระตุ้นอุปกรณ์ วิธีนี้ช่วยให้อุปกรณ์ต้านทานการเปลี่ยนแปลงที่ผิดพลาดในกรณีที่ได้รับแสงแฟลชสั้นๆ หรือแสงที่ส่องสว่างทั่วทั้งสนาม (การได้รับพลังงานสูงอย่างต่อเนื่องอาจทำให้วัสดุเซ็นเซอร์อิ่มตัวและทำให้เซ็นเซอร์ไม่สามารถบันทึกข้อมูลเพิ่มเติมได้) ในขณะเดียวกัน การจัดเรียงแบบดิฟเฟอเรนเชียลนี้ยังช่วยลดสัญญาณรบกวนโหมดทั่วไปทำให้อุปกรณ์ต้านทานการกระตุ้นเนื่องจากสนามไฟฟ้าใกล้เคียง อย่างไร

ก็ตาม เซ็นเซอร์แบบดิฟเฟอเรนเชียลคู่ไม่สามารถวัดอุณหภูมิได้ในรูปแบบนี้ ดังนั้นจึงมีประโยชน์เฉพาะสำหรับการตรวจจับการเคลื่อนไหวเท่านั้น

2.7.5 การปฏิบัติจริง

เมื่อเซ็นเซอร์ PIR ถูกกำหนดค่าในโหมดดิฟเฟอเรนเชียล เซ็นเซอร์จะสามารถใช้งานได้เฉพาะในฐานะอุปกรณ์ตรวจจับการเคลื่อนไหว ในโหมดนี้ เมื่อตรวจจับการเคลื่อนไหวภายใน “แนวสายตา” ของเซ็นเซอร์ พัลส์เสริมคู่หนึ่งจะถูกประมวลผลที่ขาเอาต์พุตของเซ็นเซอร์ เพื่อนำสัญญาณเอาต์พุตนี้ไปใช้งานจริงในการกระตุ้นโหลด เช่น รีเลย์หรือเครื่องบันทึกข้อมูลหรือสัญญาณเตือนสัญญาณดิฟเฟอเรนเชียลจะถูกแก้ไขโดยใช้วงจรเรียงกระแสแบบบริดจ์และป้อนเข้าสู่วงจรขับรีเลย์แบบทรานซิสเตอร์ หน้าสัมผัสของรีเลย์นี้จะปิดและเปิดเพื่อตอบสนองต่อสัญญาณจาก PIR โดยกระตุ้นโหลดที่เชื่อมต่ออยู่ผ่านหน้าสัมผัสของมัน รับรู้ถึงการตรวจจับบุคคลภายในพื้นที่จำกัดที่กำหนดไว้ล่วงหน้า

2.7.6 การออกแบบผลิตภัณฑ์

รูปที่ 2.7.6.1: การออกแบบเซ็นเซอร์ตรวจจับการเคลื่อนไหว PIR

โดยทั่วไปเซ็นเซอร์ PIR จะติดตั้งอยู่บนแผงวงจรพิมพ์ซึ่งมีอุปกรณ์อิเล็กทรอนิกส์ที่จำเป็นสำหรับการตีความสัญญาณจากตัวเซ็นเซอร์เอง โดยทั่วไปแล้วชุดประกอบทั้งหมดจะบรรจุอยู่ภายในตัวเรือน ซึ่งติดตั้งในตำแหน่งที่เซ็นเซอร์สามารถครอบคลุมพื้นที่ที่ต้องการตรวจสอบได้ ตัวเรือนมักจะมี “หน้าต่าง” พลาสติกที่พลังงานอินฟราเรดสามารถผ่านเข้ามาได้ แม้ว่ามักจะโปร่งแสงต่อแสงที่มองเห็นแต่พลังงานอินฟราเรดสามารถผ่านเข้ามายังเซ็นเซอร์ได้ผ่านหน้าต่าง เนื่องจากพลาสติกที่ใช้นั้นโปร่งใสต่อรังสีอินฟราเรด หน้าต่างพลาสติกช่วยลดโอกาสที่วัตถุแปลกปลอม (ฝุ่น แมลง ฝน ฯลฯ) จะบดบังมุมมองของเซ็นเซอร์ ทำให้กลไกเสียหาย และ/หรือทำให้เกิดสัญญาณเตือนที่ผิดพลาดหน้าต่างนี้สามารถใช้เป็นตัวกรองเพื่อจำกัดความยาวคลื่นให้อยู่ที่ 8-14 ไมโครเมตร ซึ่งใกล้เคียงกับรังสีอินฟราเรดที่มนุษย์ปล่อยออกมามากที่สุด นอกจากนี้ยังสามารถใช้เป็นกลไกโฟกัสได้อีกด้วย (ดูด้านล่าง)

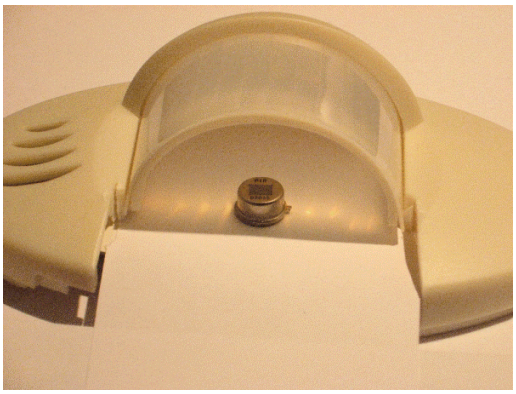
2.7.7 การโฟกัส

สามารถใช้กลไกที่แตกต่างกันเพื่อโฟกัสพลังงานอินฟราเรดระยะไกลลงบนพื้นผิวเซ็นเซอร์ได้

2.7.8 เลนส์

ม่านพลาสติกอาจหล่อขึ้นรูปหลายเหลี่ยมเพื่อรวมพลังงานอินฟราเรดไปยังเซ็นเซอร์ แต่ละเหลี่ยมคือเลนส์เฟรสเนล

2.7.8.1 เลนส์มัลติเฟรสเนลของ PIR



รูปที่ 2.7.8.1: ตัวเรือนเครื่องตรวจจับความเคลื่อนไหว PIR พร้อมช่องหน้าต่างทรงกระบอกเหลี่ยมโดยแต่ละเหลี่ยมเป็นเลนส์เฟรสเนล โฟกัสแสงไปที่ชิ้นส่วนเซ็นเซอร์ไพโรอิเล็กทริกที่อยู่ด้านล่าง

รูปที่ 2.7.8.2: ฝาครอบด้านหน้า PIR เท่านั้น (ถอดอุปกรณ์อิเล็กทรอนิกส์ออก) โดยมีแหล่งกำเนิดแสงจุดอยู่ด้านหลัง เพื่อแสดงเลนส์แต่ละตัว

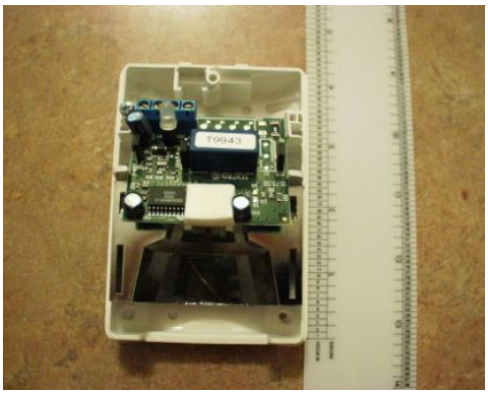
รูปที่ 2.7.8.3: PIR ที่ถอดฝาครอบด้านหน้าออก แสดงตำแหน่งของ เซ็นเซอร์ไพโรอิเล็กทริก (ลูกศรสีเขียว)

2.7.9 กระจก PIR

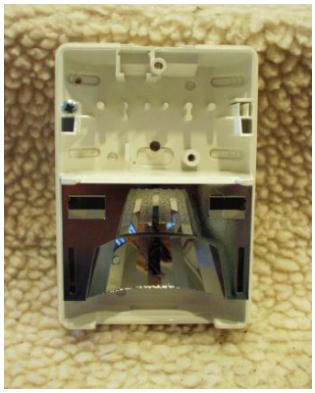
บางรุ่นผลิตขึ้นโดยใช้กระจกพาราโบลา แบบแบ่งส่วนภายใน เพื่อรวมพลังงานอินฟราเรด ในกรณีที่ใช้กระจก ฝาครอบกระจกพลาสติกโดยทั่วไปจะไม่มีเลนส์เฟรสเนลหล่อขึ้นรูป

2.7.9.1 PIR ชนิดกระจกแบ่งส่วน

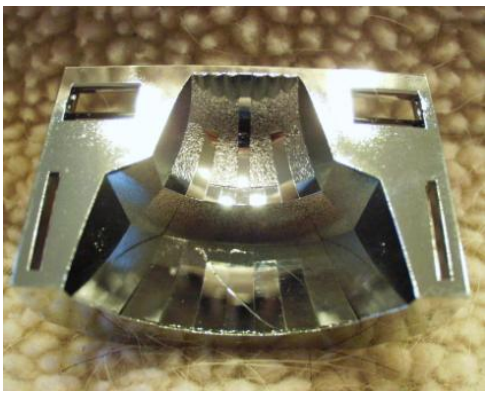
รูปที่ 2.7.9.1: PID ทั่วไปสำหรับที่พักอาศัย/เชิงพาณิชย์ที่ ใช้กระจกแบ่งส่วนภายในเพื่อการโฟกัส



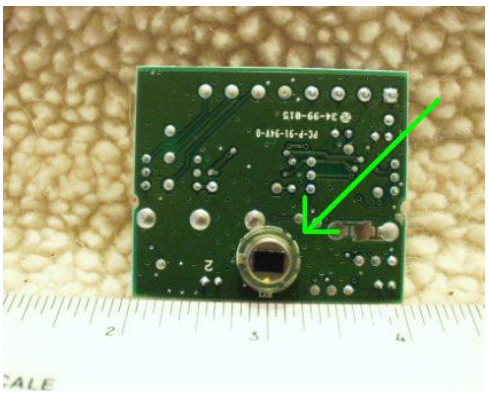
รูปที่ 2.7.9.2: ถอดฝาครอบออกแล้ว กระจกแบ่งส่วน ด้านล่างมีแผงวงจรพิมพ์ (PC) อยู่ด้านบน



รูปที่ 2.7.9.3: แผงวงจรพิมพ์ถูกถอดออกเพื่อแสดงกระจกแบบแบ่งส่วน

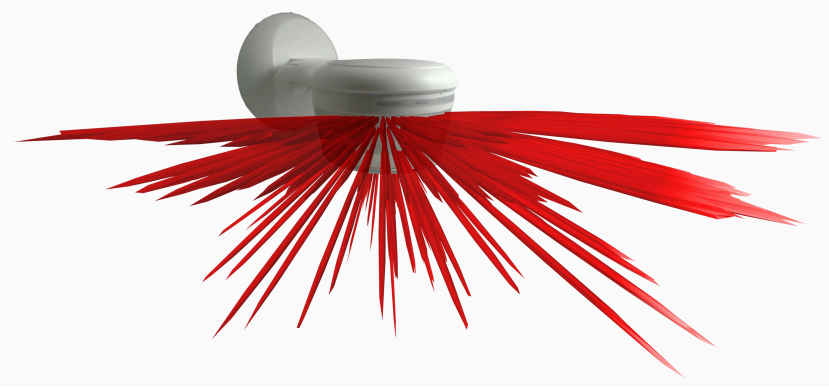


รูปที่ 2.7.9.4: กระจกพาราโบลาแบบแบ่งส่วนถอดออกจากตัวเครื่อง



รูปที่ 2.7.9.5: ด้านหลังของแผงวงจรที่หันเข้าหากระจกเมื่อติดตั้ง เซ็นเซอร์ไพโรอิเล็กทริกแสดงด้วยลูกศรสีเขียว

2.7.10 รูปแบบลำแสง



รูปที่ 2.7.10.1: เครื่องตรวจจับความเคลื่อนไหวที่มีรูปแบบลำแสงซ้อนทับ ความยาวของลำแสงเป็นตัวชี้วัดความไวของเครื่องตรวจจับในทิศทางนั้น

จากการโฟกัส ทำให้มุมมองของเครื่องตรวจจับกลายเป็นรูปแบบลำแสง ภายใต้มุมบางมุม (โซน) เซ็นเซอร์ PIR แทบจะไม่ได้รับพลังงานรังสีใดๆ และภายใต้มุมอื่นๆ PIR จะได้รับพลังงานอินฟราเรดในปริมาณที่เข้มข้น การแยกนี้ช่วยให้เครื่องตรวจจับความเคลื่อนไหวสามารถแยกแยะระหว่างแสงสว่างที่กว้างและวัตถุที่กำลังเคลื่อนที่ได้

เมื่อบุคคลเดินจากมุมหนึ่ง (ลำแสง) ไปยังอีกมุมหนึ่ง เครื่องตรวจจับจะมองเห็นบุคคลที่กำลังเคลื่อนไหวเป็นระยะ ๆ เท่านั้น ส่งผลให้สัญญาณเซ็นเซอร์เปลี่ยนแปลงอย่างรวดเร็ว ซึ่งระบบอิเล็กทรอนิกส์จะใช้เพื่อส่งสัญญาณเตือนภัยหรือเปิดไฟ ระบบอิเล็กทรอนิกส์จะไม่สนใจสัญญาณที่เปลี่ยนแปลงช้า ๆ

จำนวน รูปร่าง การกระจาย และความไวของโซนเหล่านี้ถูกกำหนดโดยเลนส์และ/หรือกระจก ผู้ผลิตพยายามอย่างเต็มที่เพื่อสร้างรูปแบบลำแสงความไวที่เหมาะสมที่สุดสำหรับการใช้งานแต่ละประเภท

2.7.11 การใช้งานระบบไฟอัตโนมัติ

เมื่อใช้เป็นส่วนหนึ่งของระบบไฟส่องสว่าง ระบบอิเล็กทรอนิกส์ใน PIR มักจะควบคุมรีเลย์ในตัวที่สามารถสลับแรงดันไฟฟ้าหลักได้ ซึ่งหมายความว่า PIR สามารถตั้งค่าให้เปิดไฟที่เชื่อมต่อกับ PIR เมื่อตรวจพบการเคลื่อนไหวได้ วิธีนี้มักใช้ในสถานการณ์กลางแจ้ง ทั้งเพื่อป้องกันอาชญากร (ไฟรักษาความปลอดภัย) หรือเพื่อการใช้งานจริง เช่น การเปิดไฟประตูหน้าบ้านเพื่อให้คุณหากุญแจเจอในความมืด การใช้งานเพิ่มเติมสามารถทำได้ในห้องน้ำสาธารณะ ห้องเตรียมอาหารแบบวอล์กอิน ทางเดิน หรือบริเวณใดก็ตามที่สามารถควบคุมไฟอัตโนมัติได้ วิธีนี้ช่วยประหยัดพลังงานได้ เพราะไฟจะเปิดเฉพาะเมื่อจำเป็นเท่านั้น และผู้ใช้ไม่จำเป็นต้องปิดไฟเมื่อออกจากพื้นที่

2.7.12 แอปพลิเคชั่นด้านความปลอดภัย

เมื่อใช้เป็นส่วนหนึ่งของระบบรักษาความปลอดภัย วงจรอิเล็กทรอนิกส์ใน PIR มักจะควบคุมรีเลย์ ขนาดเล็ก รีเลย์นี้จะทำหน้าที่เชื่อมต่อวงจรไฟฟ้าผ่านหน้า สัมผัสไฟฟ้าคู่หนึ่งที่เชื่อมต่อกับโซนอินพุตตรวจจับของแผงควบคุมสัญญาณกันขโมยโดยทั่วไประบบจะออกแบบให้หากไม่มีการเคลื่อนไหว หน้าสัมผัสรีเลย์จะปิดอยู่ ซึ่งเรียกว่ารีเลย์แบบ ‘ปกติปิด’ (NC) หากตรวจพบการเคลื่อนไหว รีเลย์จะเปิดวงจรเพื่อส่งสัญญาณเตือนภัย หรือหากสายไฟถูกตัดการเชื่อมต่อ สัญญาณเตือนภัยก็จะทำงานเช่นกัน

2.7.13 การจัดวาง

ผู้ผลิตแนะนำให้วางผลิตภัณฑ์อย่างระมัดระวังเพื่อป้องกันการแจ้งเตือนที่ผิดพลาด (เช่น การตรวจจับใดๆ ที่ไม่ได้เกิดจากผู้บุกรุก)

พวกเขาแนะนำให้ติดตั้ง PIR ในลักษณะที่ PIR ไม่สามารถ “มองเห็น” ออกจากหน้าต่างได้ แม้ว่าความยาวคลื่นของรังสีอินฟราเรดที่ชิปมีความไวต่อแสงจะทะลุผ่านกระจกได้ไม่ดีนัก แต่แหล่งกำเนิดแสงอินฟราเรดที่แรง (เช่น จากไฟหน้ารถยนต์หรือแสงแดด) อาจทำให้เซ็นเซอร์รับภาพเกินพิกัดและทำให้เกิดสัญญาณเตือนภัยผิดพลาดได้ บุคคลที่เคลื่อนไหวอยู่อีกฝั่งของกระจกจะไม่ถูก PID “มองเห็น” ซึ่งอาจเป็นผลดีสำหรับหน้าต่างที่หันหน้าไปทางทางเท้าสาธารณะ หรือเป็นผลเสียสำหรับหน้าต่างในฉากกั้นภายใน

ขอแนะนำว่าไม่ควรติดตั้ง PIR ในตำแหน่งที่ ช่องระบายอากาศ HVACจะเป่าลมร้อนหรือเย็นลงบนพื้นผิวพลาสติกที่ปิดหน้าต่างของตัวบ้าน แม้ว่าอากาศจะมีค่าการแผ่รังสี ต่ำมาก (ปล่อยพลังงานอินฟราเรดในปริมาณน้อยมาก) แต่ลมที่พัดผ่านฝาครอบหน้าต่างพลาสติกอาจทำให้อุณหภูมิของพลาสติกเปลี่ยนแปลงจนทำให้เกิดสัญญาณเตือนที่ผิดพลาดได้

เซ็นเซอร์มักได้รับการออกแบบมาให้ “เพิกเฉย” สัตว์เลี้ยงในบ้าน เช่น สุนัขหรือแมว โดยการตั้งค่าความไวให้สูงขึ้น หรือทำให้แน่ใจว่าพื้นห้องจะไม่อยู่ในโฟกัส

เนื่องจากเซ็นเซอร์ PIR มีระยะการทำงานสูงสุด 10 เมตร (30 ฟุต) ดังนั้นการติดตั้งเครื่องตรวจจับเพียงตัวเดียวใกล้ทางเข้าจึงเพียงพอสำหรับห้องที่มีทางเข้าเพียงทางเดียว ระบบรักษาความปลอดภัยที่ใช้ PIR ยังใช้งานได้ดีกับระบบรักษาความปลอดภัยภายนอกอาคารและระบบไฟที่ไวต่อการเคลื่อนไหว ข้อดีอย่างหนึ่งคือใช้พลังงานต่ำ ซึ่งทำให้สามารถใช้พลังงานแสงอาทิตย์ได้

2.7.14 เทอร์โมมิเตอร์แบบควบคุมระยะไกลด้วย PIR

มีการออกแบบวงจร PIR ที่ใช้วัดอุณหภูมิของวัตถุที่อยู่ห่างไกลในวงจรดังกล่าว จะใช้เอาต์พุต PIR แบบไม่มีค่าความแตกต่าง สัญญาณเอาต์พุตจะถูกประเมินตามการสอบเทียบสเปกตรัม IR ของสสารชนิดเฉพาะที่ต้องการตรวจวัด ด้วยวิธีนี้ การวัดอุณหภูมิจากระยะไกลจึงค่อนข้างแม่นยำและแม่นยำ หากไม่มีการสอบเทียบกับชนิดของวัสดุที่ตรวจวัด อุปกรณ์เทอร์โมมิเตอร์ PIR จะสามารถวัดการเปลี่ยนแปลงของการแผ่รังสี IR ซึ่งสอดคล้องกับการเปลี่ยนแปลงของอุณหภูมิโดยตรง แต่ไม่สามารถคำนวณค่าอุณหภูมิที่แท้จริงได้

2.8 ภาษาซี

ภาษาซีเป็นภาษาโปรแกรมสำหรับวัตถุประสงค์ทั่วไปสร้างขึ้นในช่วงทศวรรษ 1970 โดยเดนนิสริตชีและยังคงได้รับความนิยมและใช้งานอย่างกว้างขวางด้วยการออกแบบภาษาซีทำให้โปรแกรมเมอร์สามารถเข้าถึงคุณลักษณะต่างๆของสถาปัตยกรรมซีพียูทั่วไปได้โดยตรง ซึ่งปรับแต่งให้เหมาะกับชุดคำสั่ง เป้าหมาย ภาษาซี ถูกนำมาใช้และยังคงนำมาใช้ในการพัฒนาระบบปฏิบัติการไดรเวอร์อุปกรณ์และสแต็กโปรโตคอลแต่การใช้งานในซอฟต์แวร์แอปพลิเคชั่นกำลังลดลงภาษาซีถูกนำมาใช้ในคอมพิวเตอร์ตั้งแต่ซูเปอร์คอมพิวเตอร์ขนาดใหญ่ที่สุดไปจนถึงไมโครคอนโทรลเลอร์ขนาดเล็กที่สุดและระบบฝังตัว

ภาษาซีเป็นภาษาเชิงกระบวนการที่จำเป็นรองรับการเขียนโปรแกรมแบบมีโครงสร้างขอบเขตตัวแปรเชิงศัพท์และการเรียกซ้ำด้วยระบบชนิดข้อมูลแบบคงที่ภาษาซีถูกออกแบบมาเพื่อการคอมไพล์เพื่อให้สามารถเข้าถึงหน่วยความจำ และโครงสร้างภาษา ในระดับต่ำซึ่งแมปกับคำสั่งเครื่องได้อย่างมีประสิทธิภาพ โดยทั้งหมดนี้รองรับรันไทม์ขั้นต่ำ แม้จะมีความสามารถในระดับต่ำ แต่ภาษาซีก็ถูกออกแบบมาเพื่อสนับสนุนการเขียนโปรแกรมข้ามแพลตฟอร์ม โปรแกรมซี ที่สอดคล้องกับมาตรฐานที่เขียนขึ้นโดยคำนึงถึงความสามารถในการพกพาสามารถคอมไพล์สำหรับแพลตฟอร์มคอมพิวเตอร์และระบบปฏิบัติการที่หลากหลาย โดยมีการเปลี่ยนแปลงซอร์สโคดเพียงเล็กน้อย

แม้ว่าทั้งภาษาซีและไลบรารีมาตรฐานของภาษา ซีจะไม่ได้มีคุณสมบัติยอดนิยมบางอย่างที่พบในภาษาอื่น แต่ก็มีความยืดหยุ่นเพียงพอที่จะรองรับคุณสมบัติเหล่านั้นได้ ตัวอย่างเช่นการวางแนววัตถุและการเก็บขยะนั้นจัดทำโดยไลบรารีภายนอก GLib Object SystemและBoehm garbage collector ตามลำดับ

ตั้งแต่ปี 2000 เป็นต้นมาภาษาซี ได้รับการจัดอันดับอย่างต่อเนื่องให้อยู่ในอันดับสี่ภาษาสูงสุดในดัชนี TIOBEซึ่งเป็นการวัดความนิยมของภาษาการเขียนโปรแกรม

2.8.1 ตัวอย่าง “Hello, world”

ตัวอย่างโปรแกรม “Hello, World!” ที่ปรากฏใน K&R ฉบับพิมพ์ครั้งแรกได้กลายเป็นต้นแบบของโปรแกรมเบื้องต้นในตำราเรียนการเขียนโปรแกรมส่วนใหญ่ โปรแกรมจะพิมพ์ “hello, world” ออกทางเอาต์พุตมาตรฐาน

เวอร์ชันดั้งเดิมคือ

```
main()
{
    printf("hello, world\n");
}
```

เวอร์ชันที่ทันสมัยกว่าคือ

```
#include <stdio.h>

int main(void)
{
    printf("hello, world\n");
}
```

บรรทัดแรกเป็นคำสั่งพรีโพรเซสเซอร์ ซึ่งระบุด้วย **#include** ซึ่งทำให้พรีโพรเซสเซอร์แทนที่บรรทัดโคดนั้นด้วยข้อความของไฟล์ส่วนหัว **stdio.h** ซึ่งประกอบด้วยการประกาศสำหรับฟังก์ชันอินพุตและเอาต์พุต รวมถึง **printf** โดยวงเล็บเหลี่ยมที่อยู่รอบ ๆ **stdio.h** ระบุว่าสามารถค้นหาไฟล์ส่วนหัวได้โดยใช้กลยุทธ์การค้นหาที่เลือกไฟล์ส่วนหัวที่มาพร้อมกับคอมไพเลอร์ แทนที่จะเป็นไฟล์ที่มีชื่อเดียวกันซึ่งอาจพบได้ในไดเรกทอรีเฉพาะโครงการ

บรรทัดโคดถัดไปประกาศฟังก์ชันจุดเข้าสภาพแวดล้อมรันไทม์ **main** เรียกใช้ฟังก์ชันนี้เพื่อเริ่มการทำงานของโปรแกรม ตัวระบุชนิด **int** ระบุว่าฟังก์ชันส่งคืนค่าจำนวนเต็ม รายการพารามิเตอร์ **void** ระบุว่าฟังก์ชันไม่ได้ใช้อาร์กิวเมนต์ใด ๆ สภาพแวดล้อมรันไทม์ส่งอาร์กิวเมนต์สองรายการ (**int** และ **char*[]**) แต่การใช้งานนี้จะละเว้นอาร์กิวเมนต์เหล่านี้ มาตรฐาน ISO C (หัวข้อ 5.1.2.2.1) กำหนดให้ใช้ไวยากรณ์ที่เป็นโมฆะหรืออาร์กิวเมนต์สองรายการนี้ ซึ่งเป็นการปฏิบัติพิเศษที่ฟังก์ชันอื่น ๆ ไม่ได้ให้

วงเล็บปีกกาเปิดระบุจุดเริ่มต้นของโคดที่กำหนดฟังก์ชัน

บรรทัดถัดไปของโคดจะเรียกใช้ (เปลี่ยนเส้นทางการทำงานไปยัง) ฟังก์ชันไลบรารีมาตรฐานของ C **printf** พร้อมระบุตำแหน่งอักขระตัวแรกของสตริงที่สิ้นสุดด้วยค่า **null** ที่ระบุเป็นสตริงลิเทอรัล ข้อความนี้ **\n** เป็นลำดับ escape ที่แสดง อักขระขึ้นบรรทัด ใหม่ซึ่งเมื่อส่งออกในเทอร์มินัลจะส่งผลให้เคอร์เซอร์เลื่อนไปที่จุดเริ่มต้นของบรรทัดถัดไป แม้ว่า **printf** จะคืนค่า **int** แต่ค่านั้นจะถูกละทิ้งไปอย่างเงียบๆ เครื่องหมายเซมิโคลอน **;** จะสิ้นสุดคำสั่งเรียก

วงเล็บปีกกาปิดหมายถึงจุดสิ้นสุดของฟังก์ชัน **main** โดยก่อน C99 จำเป็นต้องมีคำสั่ง **return 0;** ที่ชัดเจนเมื่อสิ้นสุดฟังก์ชัน **main** แต่ตั้งแต่ C99 ฟังก์ชัน **main** (ซึ่งเป็นการเรียกใช้ฟังก์ชันเริ่มต้น) จะคืนค่าโดยปริยาย 0 เมื่อถึงวงเล็บปีกกาปิดสุดท้าย

2.8.2 ชุดแปลโปรแกรมของกนู (GNU Compiler Collection; GCC)

ในกระบวนการการพัฒนาโครงงานนี้ ชุดแปลโปรแกรมของกนูนั้นถูกใช้เป็นหลักเนื่องจากเป็นชุดแปลโปรแกรม (คอมไพเลอร์; Compiler) ที่ใช้เป็นหลักในการพัฒนาโคดที่สร้างบนพื้นฐาน Arduino และบอร์ดต่าง ๆ รวมถึงบอร์ด ESP32

ชุดคอมไพเลอร์ GNU (GNU Compiler Collection; GCC) (เดิมชื่อ GNU C Compiler) คือชุดคอมไพเลอร์จากโครงการ GNU ที่รองรับภาษาโปรแกรม สถาปัตยกรรมฮาร์ดแวร์ และระบบปฏิบัติการต่าง ๆ มูลนิธิซอฟต์แวร์เสรี (FSF) เผยแพร่ GCC ในฐานะซอฟต์แวร์เสรีภายใต้สัญญาอนุญาตสาธารณะทั่วไปของ GNU (GNU GPL) GCC เป็นองค์ประกอบสำคัญของชุดเครื่องมือ GNU ซึ่งใช้สำหรับโครงการส่วนใหญ่ที่เกี่ยวข้องกับ GNU และเคอร์เนล Linux ด้วยโคดประมาณ 15 ล้านบรรทัดในปี 2019 GCC จึงเป็นหนึ่งในโปรแกรมฟรีที่ใหญ่ที่สุดเท่าที่เคยมีมา GCC มีบทบาทสำคัญในการเติบโตของซอฟต์แวร์เสรี ทั้งในฐานะเครื่องมือและตัวอย่าง

นอกจากจะเป็นคอมไพเลอร์อย่างเป็นทางการของระบบปฏิบัติการ GNU แล้ว GCC ยังได้รับการยอมรับให้เป็นคอมไพเลอร์มาตรฐานโดยระบบปฏิบัติการคอมพิวเตอร์สมัยใหม่ที่คล้ายกับ Unix อื่นๆ อีกมากมาย รวมถึงระบบปฏิบัติการ Linux ส่วนใหญ่ ระบบปฏิบัติการตระกูล BSD ส่วนใหญ่ก็เปลี่ยนมาใช้ GCC ไม่นานหลังจากเปิดตัว แม้ว่าหลังจากนั้น FreeBSD และ Apple macOS ได้เปลี่ยนมาใช้คอมไพเลอร์ Clang ส่วนใหญ่เป็นเพราะเหตุผลด้านลิขสิทธิ์ GCC ยังสามารถคอมไพเลอร์โคดสำหรับระบบปฏิบัติการ Windows, Android, iOS, Solaris, HP-UX, AIX และ MS-DOS ได้อีกด้วย

GCC ได้รับการพอร์ตไปยังแพลตฟอร์มและสถาปัตยกรรมชุดคำสั่งต่าง ๆ มากกว่าคอมไพเลอร์อื่น ๆ และถูกนำไปใช้งานอย่างกว้างขวางในฐานะเครื่องมือในการพัฒนาซอฟต์แวร์ทั้งแบบฟรีและแบบที่เป็นกรรมสิทธิ์ นอกจากนี้ GCC ยังพร้อมใช้งานสำหรับระบบฝังตัวมากมาย รวมถึงชิปที่ใช้ ARM และ Power ISA

2.9 Flutter

Flutter เป็นชุดพัฒนาซอฟต์แวร์ UI แบบโอเพนซอร์สที่สร้างโดย Google สามารถใช้พัฒนาแอปพลิเคชันข้ามแพลตฟอร์มจากฐานโคดเดียวสำหรับเว็บ Fuchsia, Android, iOS, Linux, macOS และ Windows โดย Flutter ได้รับการพูดถึงครั้งแรกในปี 2015 และเปิดตัวในเดือนพฤษภาคม 2017 และ Flutter ถูกใช้งานภายในโดย Google ในแอปพลิเคชันต่างๆ เช่น Google Pay และ Google Earth รวมถึงโดยนักพัฒนาซอฟต์แวร์รายอื่นๆ เช่น ByteDance และ Alibaba

Flutter จะสร้างแอปพลิเคชันที่มีเอ็นจิ้นการเรนเดอร์ของตัวเอง ซึ่งส่งข้อมูลพิกเซลไปยังหน้าจอโดยตรง ซึ่งแตกต่างจากเฟรมเวิร์ก UI อื่น ๆ อีกมากมายที่อาศัยแพลตฟอร์มเป้าหมายเพื่อจัดหาเอ็นจิ้นการเรนเดอร์ เช่น แอป Android พื้นฐานที่ใช้ Android SDK ระดับอุปกรณ์ หรือ iOS SDK ที่ใช้ UI stack ในตัวของแพลตฟอร์มเป้าหมาย การควบคุมขั้นตอนการแสดงผลของ Flutter ช่วยลดความยุ่งยากในการรองรับหลายแพลตฟอร์ม เนื่องจากสามารถใช้โคด UI ที่เหมือนกันได้กับทุกแพลตฟอร์มเป้าหมาย

2.9.1 โครงสร้างโปรเจกต์ Flutter

ในโครงงานนี้ โปรเจกต์ Flutter มีโครงสร้างคร่าว ๆ ดังกล่าว

```
├─ android
│  ├─ app
│  │  └─ src
│  │     └─ main
│  │        ├─ java: โคด Java
│  │        ├─ kotlin: โคด Kotlin
│  │        ├─ res: โฟลเดอร์ทรัพยากร เช่น ไอคอนแอพลิเคชัน
│  │        └─ AndroidManifest.xml
│  ├─ build.gradle.kts
│  └─ settings.gradle.kts
├─ assets
│  └─ certificates
│     └─ rootCA.crt: ใบรับรอง Root (ดูหัวข้อ 2.5.2 สำหรับรายละเอียด)
├─ build: โฟลเดอร์สำหรับเก็บไฟล์ไบนารี
├─ ios
├─ lib: ซอร์สโคดของแอพลิเคชัน
├─ linux
├─ macos
├─ test
├─ windows
├─ l10n.yaml: ไฟล์ตั้งค่าฟีเจอร์แปลภาษา
└─ pubspec.yaml: ไฟล์ข้อมูลโปรเจกต์ Flutter
```

(รายการข้างต้นรวมถึงแค่ไฟล์ที่สำคัญที่จะถูกกล่าวถึงในหัวข้อ 2.9 นี้)

2.9.2 Android

ในการพัฒนาแอพลิเคชัน Android โดยใช้เฟรมเวิร์ก Flutter จำเป็นต้องใช้ส่วนประกอบเครื่องมือพัฒนา Android ดังนี้

- Android SDK (API Level 36 ณ เวลาที่พิมพ์)
- Android SDK Build-Tools
- Android SDK Command-line Tools
- Android SDK Platform-Tools
- Android Emulator (ไม่บังคับ)

และแนะนำให้จัดการและติดตั้งเครื่องมือเหล่านี้ผ่าน Android Studio

ในการติดตั้ง Android SDK ควรติดตั้ง Android SDK ล่าสุดถึงแม้ว่าอุปกรณ์ของคุณจะใช้เวอร์ชันที่เก่ากว่านั้น เพื่อความมั่นใจว่าแอพลิเคชันจะสามารถใช้กับอุปกรณ์ที่ใหม่ล่าสุดได้

แอพลิเคชัน Android จะมี SDK/API level เป้าหมาย (Target SDK/API level) และ SDK/API level ขั้นต่ำ (Minimum SDK/API level) โครงงานนี้ ณ เวลาที่พิมพ์ ใช้ API level เป้าหมาย 36 (Android 16) และ API level ขั้นต่ำ 24 (Android 7) ซึ่งรวมกันแล้ว แอพลิเคชัน Android จะสามารถติดตั้งได้บนระบบตั้งแต่ API level ขั้นต่ำจนถึง API level เป้าหมาย หรือก็คือ แอพลิเคชันในโครงงานนี้สามารถติดตั้งได้ตั้งแต่บนระบบ Android 7 ถึง Android 16 นั่นเอง

2.9.2.1 Java

Java เป็นภาษาสำคัญสำหรับการพัฒนาแอพลิเคชัน Android ถึงอย่างไรก็ตาม แอพลิเคชัน Flutter นั้นถูกเขียนด้วยภาษา Dart แต่ยังจำเป็นต้องมีโคด Java เล็กน้อยเพื่อเริ่มต้นแอพลิเคชัน Flutter

โครงการนี้ใช้ Java 21 (JetBrains Runtime/Azul Zulu OpenJDK) เป็นหลักในการทำงานกับ Gradle แต่แอพลิเคชัน Android ที่ผลิตออกมานั้น เพื่อให้เข้ากับเวอร์ชันที่เก่ากว่าของระบบปฏิบัติการได้ ใช้ Java 11

2.9.2.2 Gradle

Gradle เป็นเครื่องมือสร้างระบบอัตโนมัติสำหรับการพัฒนาซอฟต์แวร์หลายภาษา จัดการงานต่าง ๆ เช่น การคอมไพล์ การแพ็คเกจ การทดสอบ การปรับใช้ และการเผยแพร่ ภาษาที่รองรับ ได้แก่ Java (รวมถึงภาษา Kotlin, Groovy, Scala ที่ใช้ JDK), C/C++ และ JavaScript Gradle พัฒนาต่อยอดจากแนวคิดของ Apache Ant และ Apache Maven และนำเสนอภาษาเฉพาะโดเมนที่ใช้ Groovy และ Kotlin ซึ่งต่างจากการกำหนดค่าโครงการที่ใช้ XML ที่ Maven ใช้ Gradle ใช้กราฟแบบอะไซคลิกกำกับทิศทางเพื่อจัดการการอ้างอิง กราฟนี้ใช้เพื่อกำหนดลำดับของงานที่ควรดำเนินการ Gradle ทำงานบน Java Virtual Machine

Gradle คือเครื่องมือหลักที่ใช้ในการจัดการโปรเจกต์ Java ส่วนใหญ่ รวมถึงโปรเจกต์ Android โดยในโครงการนี้ จะใช้ Gradle เวอร์ชัน 8.14.3 เป็นหลัก

2.9.3 Linux

Flutter ใช้ไลบรารีดังต่อไปนี้ในขั้นตอนการพัฒนาแอพลิเคชันบน Linux (development dependencies)

- curl
- git
- unzip
- xz
- zip
- glu

การติดตั้งไลบรารีและโปรแกรมที่กล่าวไปข้างต้นจะแตกต่างกันไปแต่ละการแจกจ่าย Linux และ Flutter ใช้ไลบรารีพื้นฐานดังกล่าวในการทำงานของแอพลิเคชัน (runtime dependencies)

- GTK 3
- blkid

- LZMA

แต่โดยทั่วไปแล้ว ไลบรารีเหล่านี้ควรถูกติดตั้งมาอยู่แล้วหากคุณใช้ graphical desktop ทั่วไป

2.9.3.1 Debian

```
# Development dependencies:
sudo apt install -y curl git unzip xz-utils zip libglu1-mesa
# Runtime dependencies:
sudo apt install libgtk-3-0 libblkid1 liblzma5
```

2.9.3.2 Fedora Linux

```
# Development dependencies:
sudo dnf install curl git unzip xz zip mesa-libglu
# Runtime dependencies:
sudo dnf install gtk3 libblkid xz
```

2.9.3.3 Arch Linux

```
# Development dependencies:
sudo pacman -S --needed curl git unzip xz zip glu
# Runtime dependencies:
sudo pacman -S --needed util-linux-libs xz gtk
```

2.9.4 Windows

ในการพัฒนาซอฟต์แวร์บน Windows ด้วย Flutter คุณจำเป็นต้องติดตั้ง Git สำหรับ Windows ซึ่งคุณสามารถดูขั้นตอนการติดตั้งได้โดยการสแกน QR code ด้านข้าง หรือที่ https://git-scm.com/install/windows หรือเพียงแค่ใช้ WinGet ในการติดตั้งโดยการใช้คำสั่งด้านล่าง

```
winget install --id Git.Git -e --source winget
```

2.10 Git

Git เป็นระบบซอฟต์แวร์ควบคุมเวอร์ชันแบบกระจาย ที่สามารถจัดการเวอร์ชันของซอร์สโคดหรือข้อมูลได้ มักใช้เพื่อควบคุมซอร์สโคดโดยโปรแกรมเมอร์ที่พัฒนาซอฟต์แวร์ร่วมกัน

2.10.1 Gitea

Gitea เป็นชุดซอฟต์แวร์ forge สำหรับการโฮสต์ระบบควบคุมเวอร์ชันการพัฒนาซอฟต์แวร์โดยใช้ Git รวมถึงฟีเจอร์การทำงานร่วมกันอื่น ๆ เช่น การติดตามบั๊ก การตรวจสอบโคด การผสานรวมอย่างต่อเนื่อง (Continuous Integration; CI) กระดาน Kanban ระบบรายงานปัญหา และวิกิ รองรับการโฮสต์ด้วยตนเอง และยังมีอินสแตนซ์สาธารณะของบุคคลที่หนึ่งให้ใช้งานฟรีอีกด้วย Gitea เป็นส่วนหนึ่งของ Gogs และเขียนด้วยภาษา Go Gitea สามารถโฮสต์ได้บนทุกแพลตฟอร์มที่รองรับ Go รวมถึง FreeBSD, Linux, macOS และ Windows โครงการนี้ได้รับทุนสนับสนุนจาก Open Collective

โครงงานนี้ใช้ Gitea (self-hosted) ในการโฮสต์โคดของโครงงาน

ภาคผนวก

ลิขสิทธิ์เนื้อหาโครงงาน

© พ.ศ. 2568 งานนี้อยู่ภายใต้สัญญาอนุญาต Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0) หากต้องการดูรายละเอียดเพิ่มเติมเกี่ยวกับสัญญาอนุญาตนี้ โปรดไปที่ https://creativecommons.org/licenses/by-sa/4.0/

ลิขสิทธิ์ซอร์สโคดโครงงาน

เนื่องจากโคดในโครงการนี้เป็นสาธารณะและถูกปกป้องด้วยกฎหมายลิขสิทธิ์ โคดนี้จึงมาพร้อมกับสัญญาอนุญาตในการใช้งานโคดสาธารณะทั่วไปของ GNU (GNU Public License) เวอร์ชัน 3

โดยสรุปแล้ว สัญญาอนุญาตนี้มีคุณสมบัติดังนี้ (ไม่ใช่คำแนะนำทางกฎหมาย โปรดอ่านเนื้อหาสัญญาเต็มเพื่อรายละเอียดที่ชัดเจน)

การอนุญาต:

- อนุญาตการใช้เนื้อหาที่ติดลิขสิทธิ์ในเชิงพาณิชย์
- อนุญาตให้สามารถเผยแพร่เนื้อหาที่ติดลิขสิทธ์ได้
- อนุญาตให้ดัดแปลงเนื้อหาที่ติดลิขสิทธิ์ได้
- ใบอนุญาตนี้ให้สิทธิ์ในการจดสิทธิบัตรจากผู้สนับสนุน
- อนุญาตให้ใช้และดัดแปลงเนื้อหาที่ติดลิขสิทธิ์อย่างเป็นส่วนตัวได้

โดยมีเงื่อนไขว่า:

- โคดต้องถูกเปิดเผยหากเนื้อหาที่ติดลิขสิทธิ์ถูกแจกจ่าย
- สัญญาอนุญาตต้องถูกรวมกับเนื้อหาที่ติดลิขสิทธิ์ที่ถูกเผยแพร่
- การแก้ไขเนื้อหาที่ติดลิขสิทธิ์จะต้องอยู่ภายใต้สัญญาอนุญาตเดียวกัน
- หากมีการแก้ไขเนื้อหาที่ติดลิขสัทธิ์ ต้องมีหมายเหตุชัดเจนว่างานนั้นถูกแก้ไขจากงานต้นฉบับ

และมีข้อจำกัดว่า:

- ผู้ที่เป็นเจ้าของงานไม่มีความรับผิดชอบใด ๆ ทั้งสิ้นหากเกิดความเสียหายต่อการใช้หรือใช้ไม่ได้ของโปรแกรม
- โปรแกรมไม่มีการรับประกันใด ๆ ทั้งสิ้น

สัญญาอนุญาตแบบเต็มที่ถูกบังคับใช้กับโคดในโครงงานนี้มีดังนี้

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. https://fsf.org/

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program–to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work’s System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.
c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation’s users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing

this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued

functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright

holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party’s predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent

claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you

grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others’ Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively state the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
    <one line to give the program's name and a brief idea of what it
does.>
    Copyright (C) <year>  <name of author>

    This program is free software: you can redistribute it and/or
modify
    it under the terms of the GNU General Public License as published
by
    the Free Software Foundation, either version 3 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program.  If not, see <https://www.gnu.org/
licenses/>.
```

Also add information on how to contact you by electronic and paper mail.

If the program does terminal interaction, make it output a short notice like this when it starts in an interactive mode:

```
    <program>  Copyright (C) <year>  <name of author>
    This program comes with ABSOLUTELY NO WARRANTY; for details type
`show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, your program's commands might be different; for a GUI interface, you would use an "about box".

You should also get your employer (if you work as a programmer) or school, if any, to sign a "copyright disclaimer" for the program, if necessary. For more information on this, and how to apply and follow the GNU GPL, see https://www.gnu.org/licenses/.

The GNU General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License. But first, please read https://www.gnu.org/licenses/why-not-lgpl.html.

บรรณานุกรม

“Arch Linux - Package Search”. 2025. พฤศจิกายน 30. https://archlinux.org/packages/.

“Build Linux Apps with Flutter”. 2025. Flutter (ภายใต้ CC BY 3.0 และ BSD License), กันยายน 5. https://docs.flutter.dev/platform-integration/linux/building.

“C (Programming Language)”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), พฤศจิกายน 26. https://en.wikipedia.org/w/index.php?title=C_(programming_language)&oldid=1324211766.

“Debian -- Packages”. 2025. พฤศจิกายน 30. https://www.debian.org/distrib/packages.

“Esp32”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), พฤศจิกายน 2. https://en.wikipedia.org/w/index.php?title=ESP32&oldid=1320113248.

“Espressif Systems”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), ตุลาคม 6. https://en.wikipedia.org/w/index.php?title=Espressif_Systems&oldid=1315427960.

“Fedora Packages”. 2025. พฤศจิกายน 30. https://packages.fedoraproject.org/.

“Flutter”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), พฤศจิกายน 12. https://en.wikipedia.org/w/index.php?title=Flutter_(software)&oldid=1321794260.

“Git - Install for Windows”. 2025. พฤศจิกายน 30. https://git-scm.com/install/windows.

“Gitea”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), พฤศจิกายน 17. https://en.wikipedia.org/w/index.php?title=Gitea&oldid=1322631603.

“Git”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), พฤศจิกายน 1. https://en.wikipedia.org/w/index.php?title=Git&oldid=1319901866.

“GNU Compiler Collection”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), พฤศจิกายน 30. https://en.wikipedia.org/w/index.php?title=GNU_Compiler_Collection&oldid=1324929423.

“Https”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), พฤศจิกายน 30. https://en.wikipedia.org/w/index.php?title=HTTPS&oldid=1324964055.

“Install Flutter Manually”. 2025. Flutter (ภายใต้ CC BY 3.0 และ BSD License), ตุลาคม 28. https://docs.flutter.dev/install/manual.

“Java Versions in Android Builds”. 2025. Android Developers (ภายใต้สัญญาอนุญาต Apache License 2.0), พฤศจิกายน 21. https://developer.android.com/build/jdks.

“Nodemcu”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), สิงหาคม 15. https://en.wikipedia.org/w/index.php?title=NodeMCU&oldid=1306030712.

“Transport Layer Security”. 2025. มูลนิธิวิกิมีเดีย (ภายใต้ CC BY-SA 4.0), พฤศจิกายน 24. https://en.wikipedia.org/w/index.php?title=Transport_Layer_Security&oldid=1323879251.

“Where Is the Value of "Flutter.minsdkversion" in Flutter Project Initialized?”. 2025. Stackoverflow (ภายใต้ CC BY-SA 4.0), สิงหาคม 26. https://stackoverflow.com/a/79746636.

บรรณานุกรมภาพ

รูปที่ 2.7.1.1 เครื่องตรวจจับการเคลื่อนไหวแบบ PIR ทั่วไปสำหรับที่พักอาศัย/เชิงพาณิชย์

โดย Jack LaRosa, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4479143

รูปที่ 2.7.3.1 เครื่องตรวจจับความเคลื่อนไหว PIR ใช้สำหรับควบคุมไฟภายนอกอาคารแบบอัตโนมัติ

โดย CHG, Public Domain, https://commons.wikimedia.org/w/index.php?curid=6087132

รูปที่ 2.7.3.2 กล้องดักถ่ายพร้อมระบบตรวจจับความเคลื่อนไหวแบบ PIR

โดย Dariusz Kowalczyk, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=96211951

รูปที่ 2.7.3.3 สวิตช์ไฟภายในอาคารที่ติดตั้งเซนเซอรตรวจจับการครอบครองแบบ PIR

โดย Z22, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=35183184

รูปที่ 2.7.7.1 การออกแบบเซ็นเซอร์ตรวจจับการเคลื่อนไหว PIR

โดย Versatile Techno - http://www.sensinova.in/pir-motion-sensor/SNPR11.php, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=48377787

รูปที่ 2.7.9.1 ตัวเรือนเครื่องตรวจจับความเคลื่อนไหว PIR พร้อมช่องหน้าต่างทรงกระบอกเหลี่ยมโดยแต่ละเหลี่ยมเป็นเลนส์เฟรสเนล โฟกัสแสงไปที่ชิ้นส่วนเซ็นเซอร์ไพโรอิเล็กทริกที่อยู่ด้านล่าง

CC BY-SA 3.0, https://en.wikipedia.org/w/index.php?curid=14193664

รูปที่ 2.7.9.2 ฝาครอบด้านหน้า PIR เท่านั้น (ถอดอุปกรณ์อิเล็กทรอนิกส์ออก) โดยมีแหล่งกำเนิดแสงจุดอยู่ด้านหลัง เพื่อแสดงเลนส์แต่ละตัว

โดย Jack LaRosa, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4463018

รูปที่ 2.7.9.3 PIR ที่ถอดฝาครอบด้านหน้าออก แสดงตำแหน่งของ เซ็นเซอร์ ไพโรอิเล็กทริก (ลูกศรสีเขียว)

โดย Jack LaRosa, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4478366

รูปที่ 2.7.10.1 PID ทั่วไปสำหรับที่พักอาศัย/เชิงพาณิชย์ที่ ใช้กระจกแบ่งส่วนภายในเพื่อการโฟกัส

โดย Jack LaRosa, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4501665

รูปที่ 2.7.10.2 ถอดฝาครอบออกแล้ว กระจกแบ่งส่วน ด้านล่างมีแผงวงจรพิมพ์ (PC) อยู่ด้านบน

โดย Deuxdad, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4501724

รูปที่ 2.7.10.3 แผงวงจรพิมพ์ถูกถอดออกเพื่อแสดงกระจกแบบแบ่งส่วน

โดย Jack LaRosa, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4502198

รูปที่ 2.7.10.4 กระจกพาราโบลาแบบแบ่งส่วนถอดออกจากตัวเครื่อง

โดย Deuxdad, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4502224

รูปที่ 2.7.10.5 ด้านหลังของแผงวงจรที่หันเข้าหากระจกเมื่อติดตั้ง เซ็นเซอร์ไพโรอิเล็กทริกแสดงด้วยลูกศรสีเขียว

โดย Jack LaRosa, Public Domain, https://commons.wikimedia.org/w/index.php?curid=4508036

รูปที่ 2.7.11.1 เครื่องตรวจจับความเคลื่อนไหวที่มีรูปแบบลำแสงซ้อนทับ ความยาวของลำแสงเป็ นตัวชี้วัดความไวของเครื่องตรวจจับในทิศทางนั้น

โดย AndreasCT, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=84066723