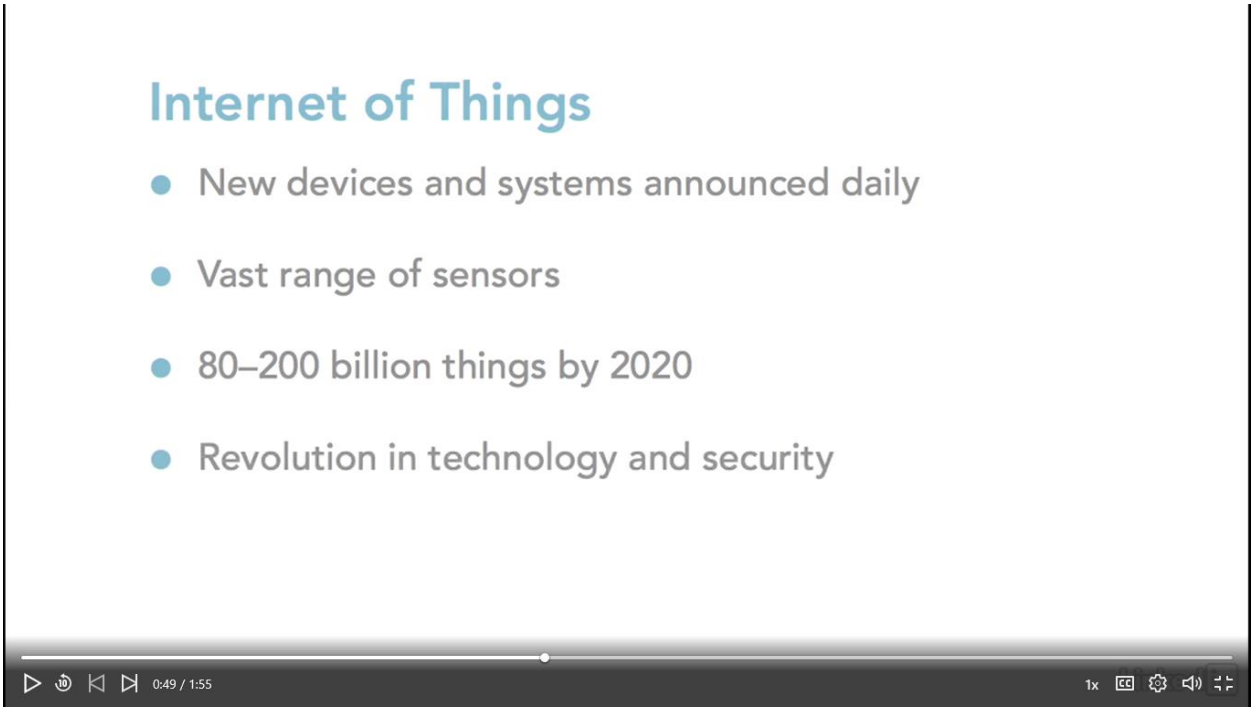
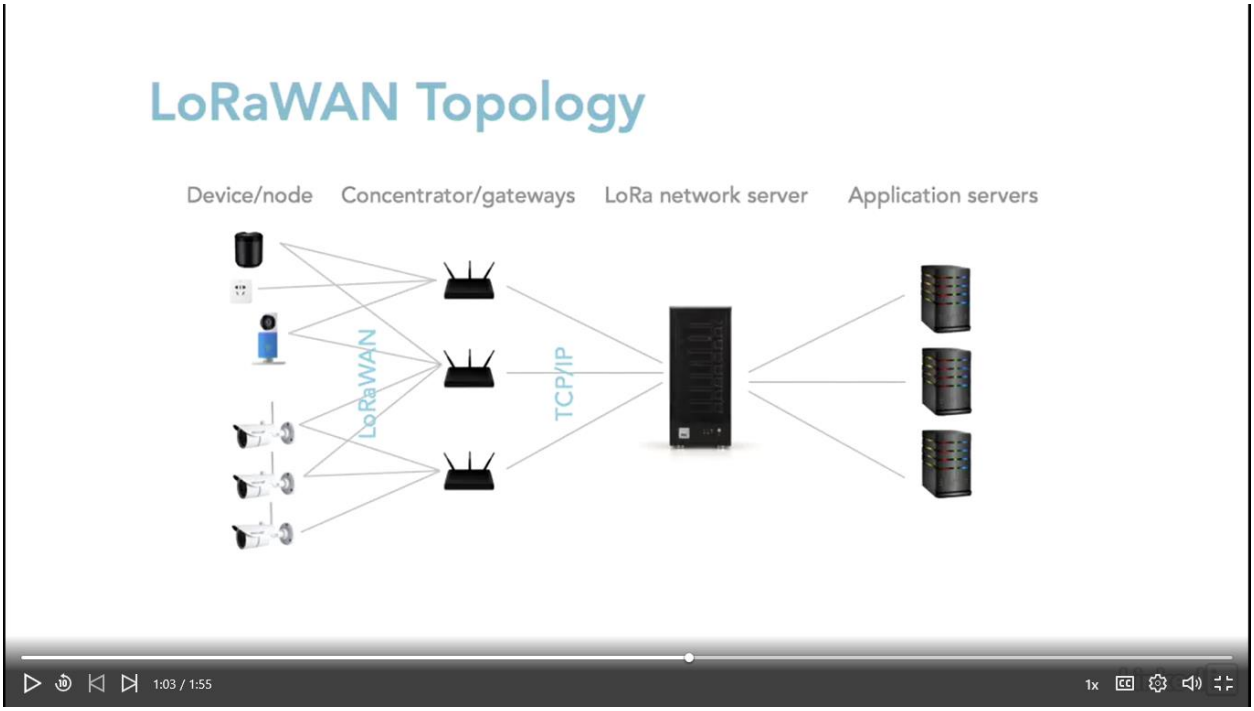
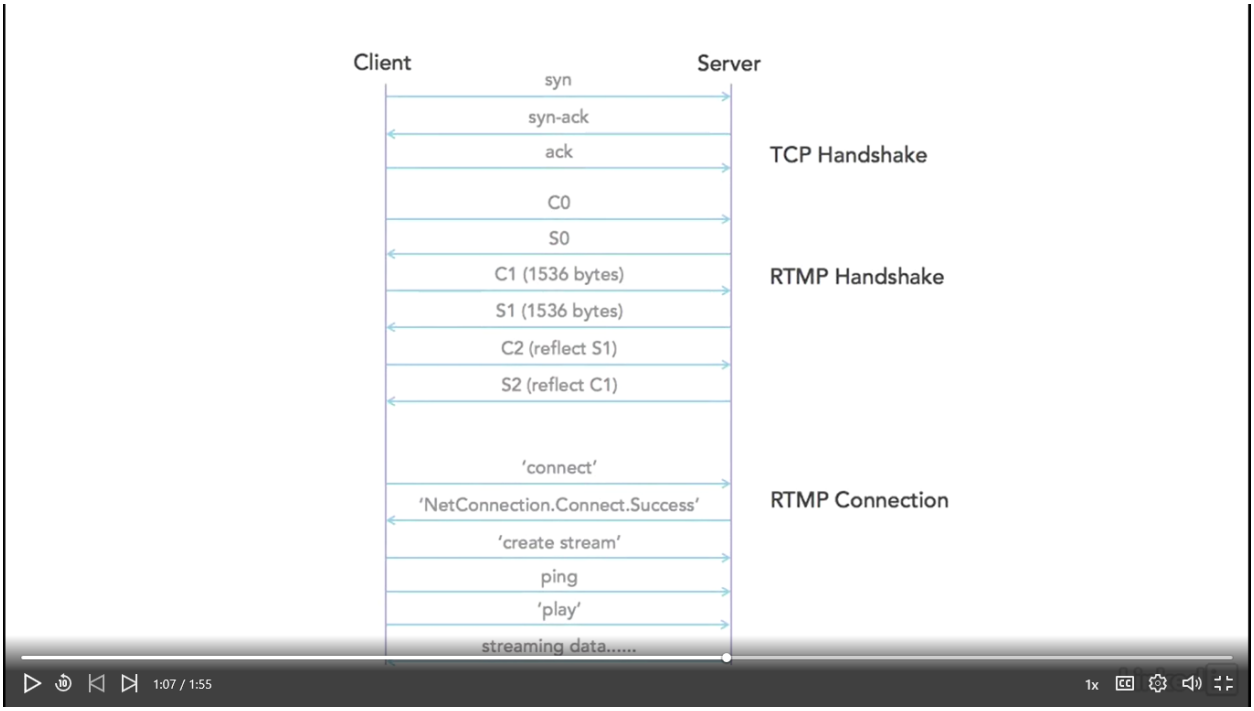
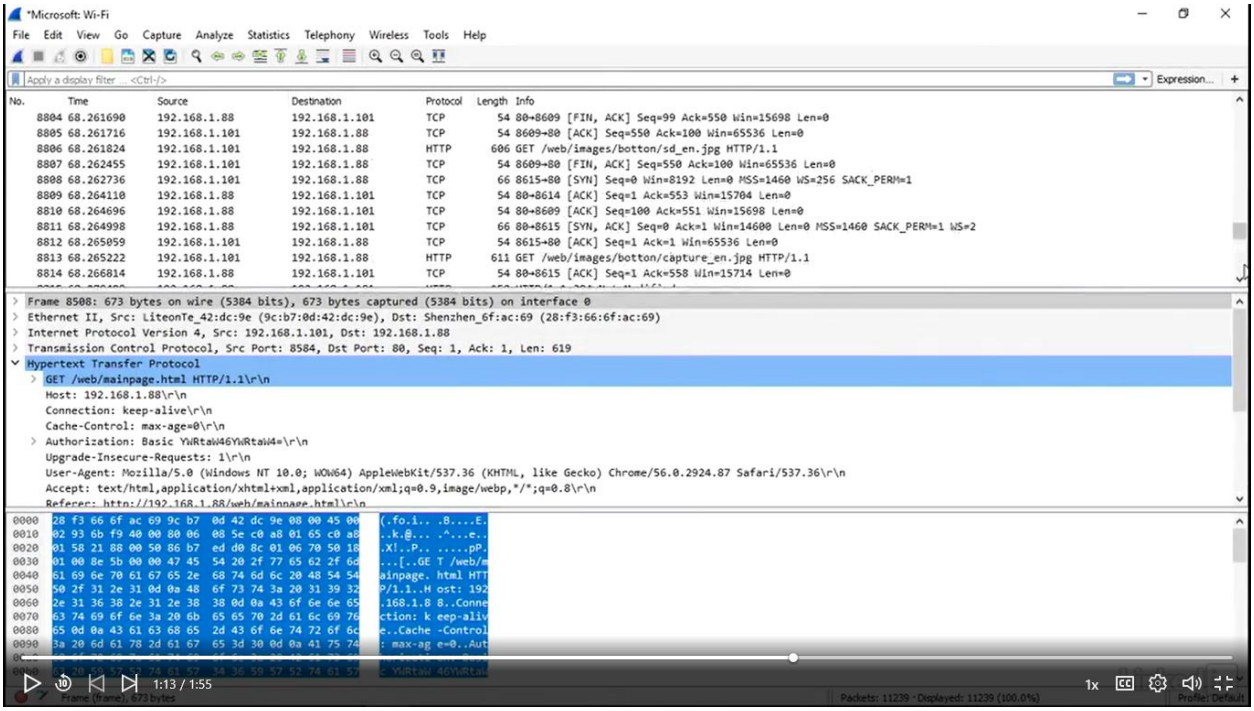
Internet of Things

- Cities and railways
- Cars and homes
- Wearables
- Implants

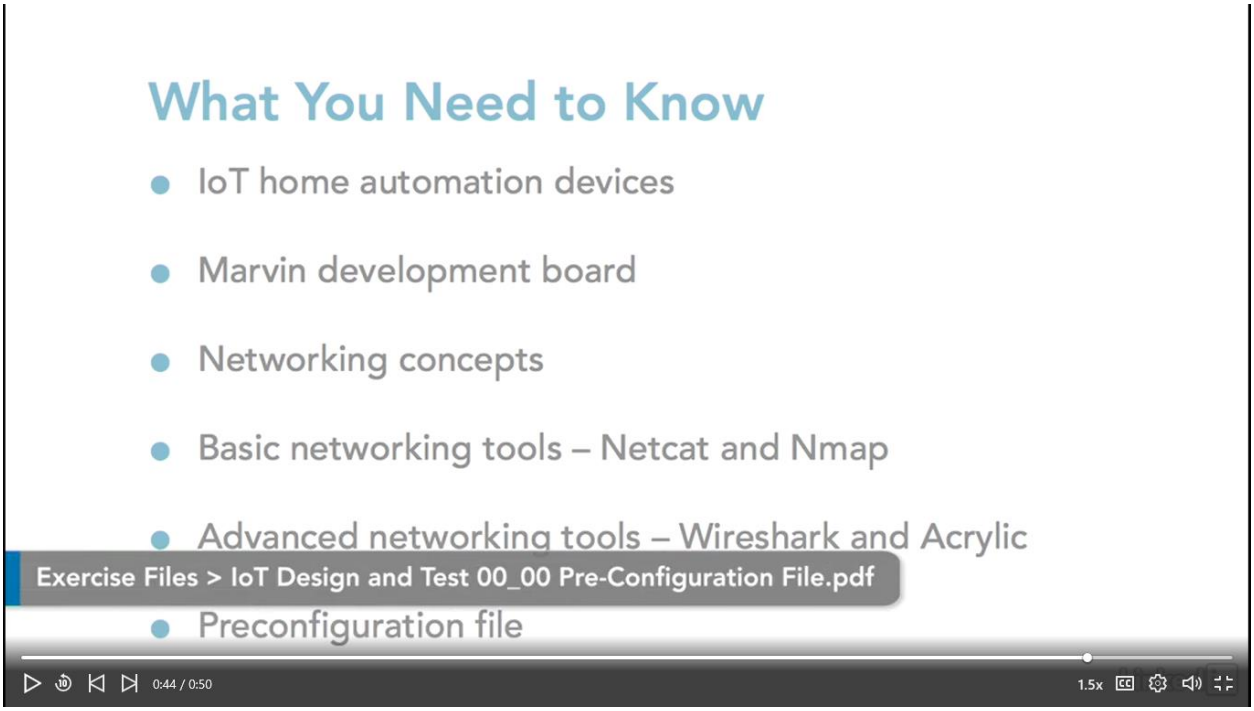

Internet of Things
New devices and systems announced daily
Vast range of sensors
80–200 billion things by 2020
Revolution in technology and security
0:49 / 1:55
1x

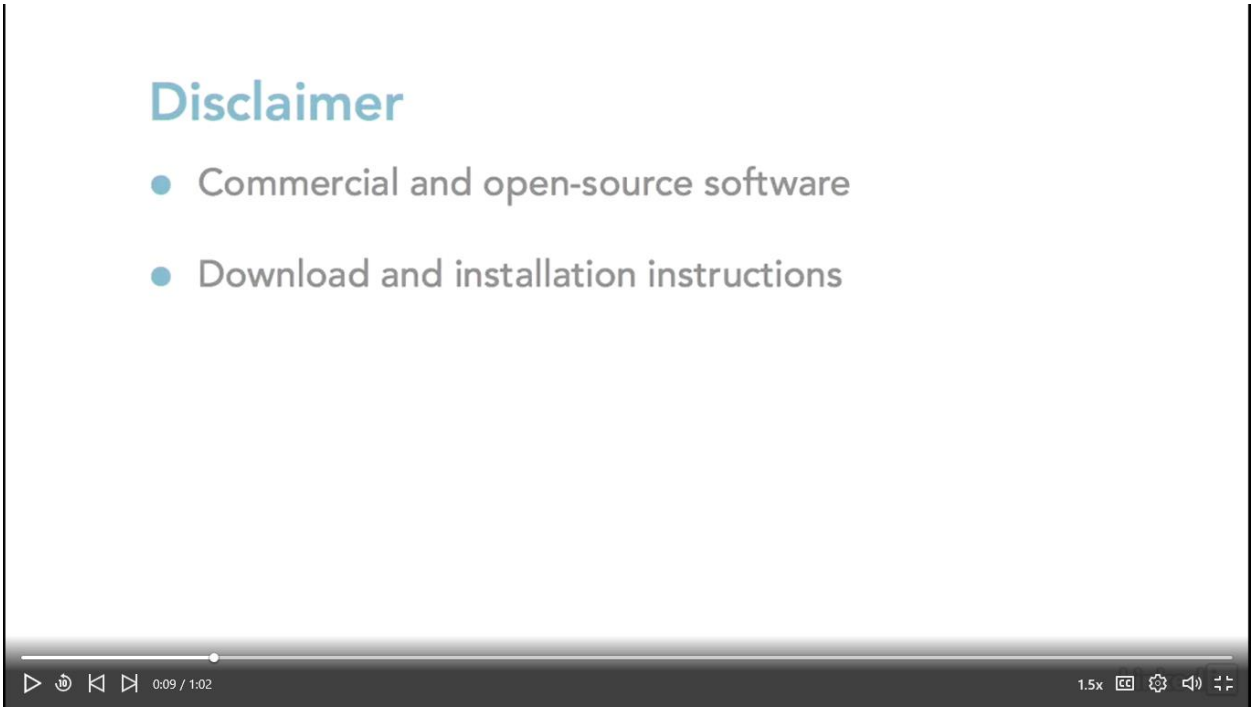

LoRaWAN Topology
Device/node
Concentrator/gateways
LoRa network server
Application servers
LoRaWAN
TCP/IP
1:03 / 1:55
1x


Client
Server
syn
syn-ack
ack
TCP Handshake
C0
S0
C1 (1536 bytes)
RTMP Handshake
S1 (1536 bytes)
C2 (reflect S1)
S2 (reflect C1)
'connect'
'NetConnection.Connect.Success'
RTMP Connection
'create stream'
ping
'play'
streaming data.....
1:07 / 1:55
1x


*Microsoft: Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
8804 68.261690 192.168.1.88 192.168.1.101 TCP 54 80→8609 [FIN, ACK] Seq=99 Ack=550 Win=15698 Len=0
8805 68.261716 192.168.1.101 192.168.1.88 TCP 54 8609→80 [ACK] Seq=550 Ack=100 Win=65536 Len=0
8806 68.261824 192.168.1.101 192.168.1.88 HTTP 606 GET /web/images/botton/sd_en.jpg HTTP/1.1
8807 68.262455 192.168.1.101 192.168.1.88 TCP 54 8609→80 [FIN, ACK] Seq=550 Ack=100 Win=65536 Len=0
8808 68.262736 192.168.1.101 192.168.1.88 TCP 66 8615→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8809 68.264110 192.168.1.88 192.168.1.101 TCP 54 80→8614 [ACK] Seq=1 Ack=553 Win=15704 Len=0
8810 68.264696 192.168.1.88 192.168.1.101 TCP 54 80→8609 [ACK] Seq=100 Ack=551 Win=15698 Len=0
8811 68.264998 192.168.1.88 192.168.1.101 TCP 66 80→8615 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=2
8812 68.265059 192.168.1.101 192.168.1.88 TCP 54 8615→80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
8813 68.265222 192.168.1.101 192.168.1.88 HTTP 611 GET /web/images/botton/capture_en.jpg HTTP/1.1
8814 68.266814 192.168.1.88 192.168.1.101 TCP 54 80→8615 [ACK] Seq=1 Ack=558 Win=15714 Len=0
Frame 8508: 673 bytes on wire (5384 bits), 673 bytes captured (5384 bits) on interface 0
Ethernet II, Src: LiteonTe_42:dc:9e (9c:b7:0d:42:dc:9e), Dst: Shenzhen_6f:ac:69 (28:f3:66:6f:ac:69)
Internet Protocol Version 4, Src: 192.168.1.101, Dst: 192.168.1.88
Transmission Control Protocol, Src Port: 8584, Dst Port: 80, Seq: 1, Ack: 1, Len: 619
Hypertext Transfer Protocol
GET /web/mainpage.html HTTP/1.1\r\n
Host: 192.168.1.88\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Authorization: Basic YWRtaW46YWRtaW4=\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Referer: http://192.168.1.88/web/mainpage.html\r\n
0000 28 f3 66 6f ac 69 9c b7 0d 42 dc 9e 08 00 45 00 (.fo.i.. .B....E.
0010 02 93 6b f9 40 00 80 06 08 5e c0 a8 01 65 c0 a8 ..k.@... .^...e..
0020 01 58 21 88 00 50 86 b7 ed d0 8c 01 06 70 50 18 .X!..P.. .....pP.
0030 01 00 8e 5b 00 00 47 45 54 20 2f 77 65 62 2f 6d ...[..GE T /web/m
0040 61 69 6e 70 61 67 65 2e 68 74 6d 6c 20 48 54 54 ainpage. html HTT
0050 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 31 39 32 P/1.1..H ost: 192
0060 2e 31 36 38 2e 31 2e 38 38 0d 0a 43 6f 6e 6e 65 .168.1.8 8..Conne
0070 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 ction: k eep-aliv
0080 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c e..Cache -Control
0090 3a 20 6d 61 78 2d 61 67 65 3d 30 0d 0a 41 75 74 : max-ag e=0..Aut
1:13 / 1:55
1x


IoT Course
Major security issues
Current thinking in IoT security
Marvin LoRa development
Testing
1:44 / 1:55
1.5x

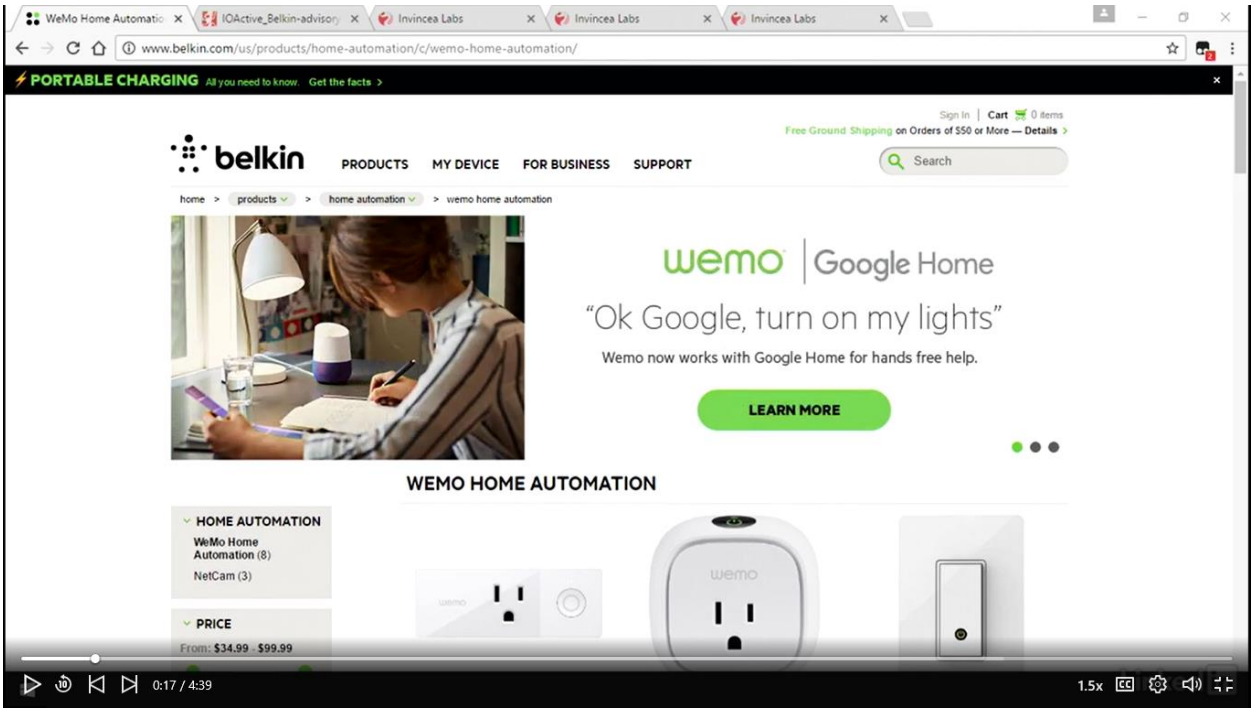

What You Need to Know
IoT home automation devices
Marvin development board
Networking concepts
Basic networking tools – Netcat and Nmap
Advanced networking tools – Wireshark and Acrylic
Exercise Files > IoT Design and Test 00_00 Pre-Configuration File.pdf
Preconfiguration file
0:44 / 0:50
1.5x

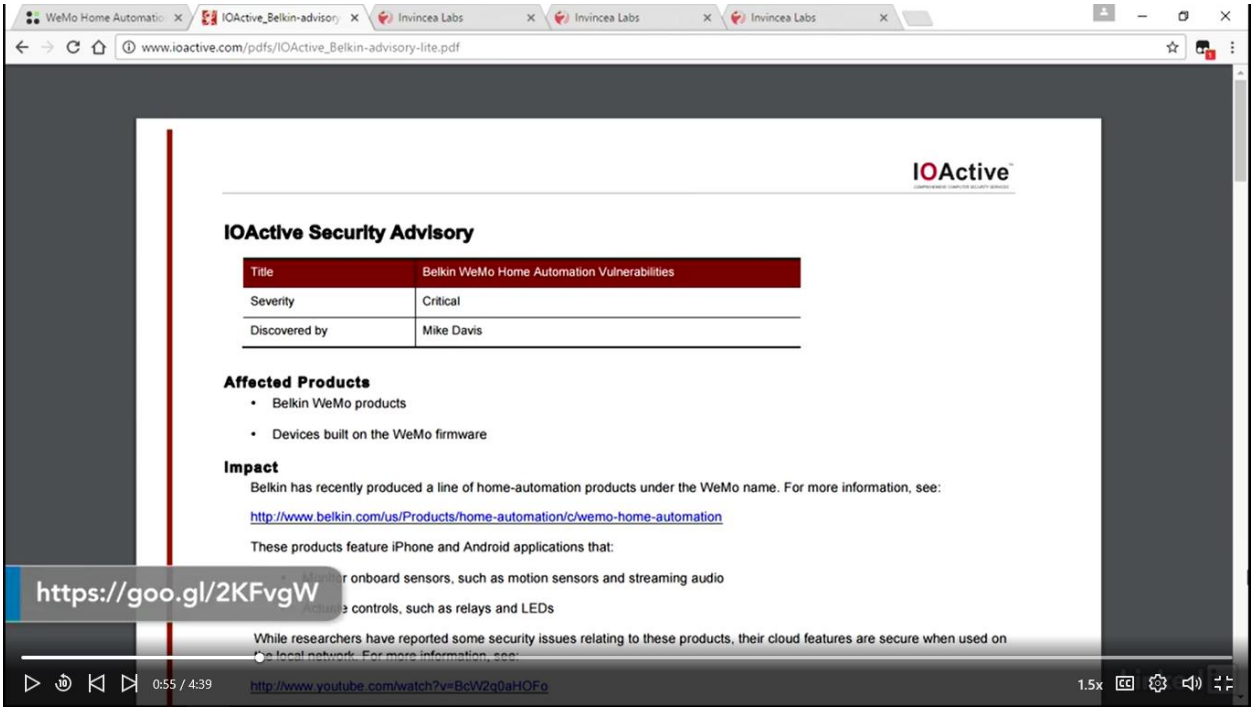

Disclaimer
Commercial and open-source software
Download and installation instructions
0:09 / 1:02
1.5x

Disclaimer

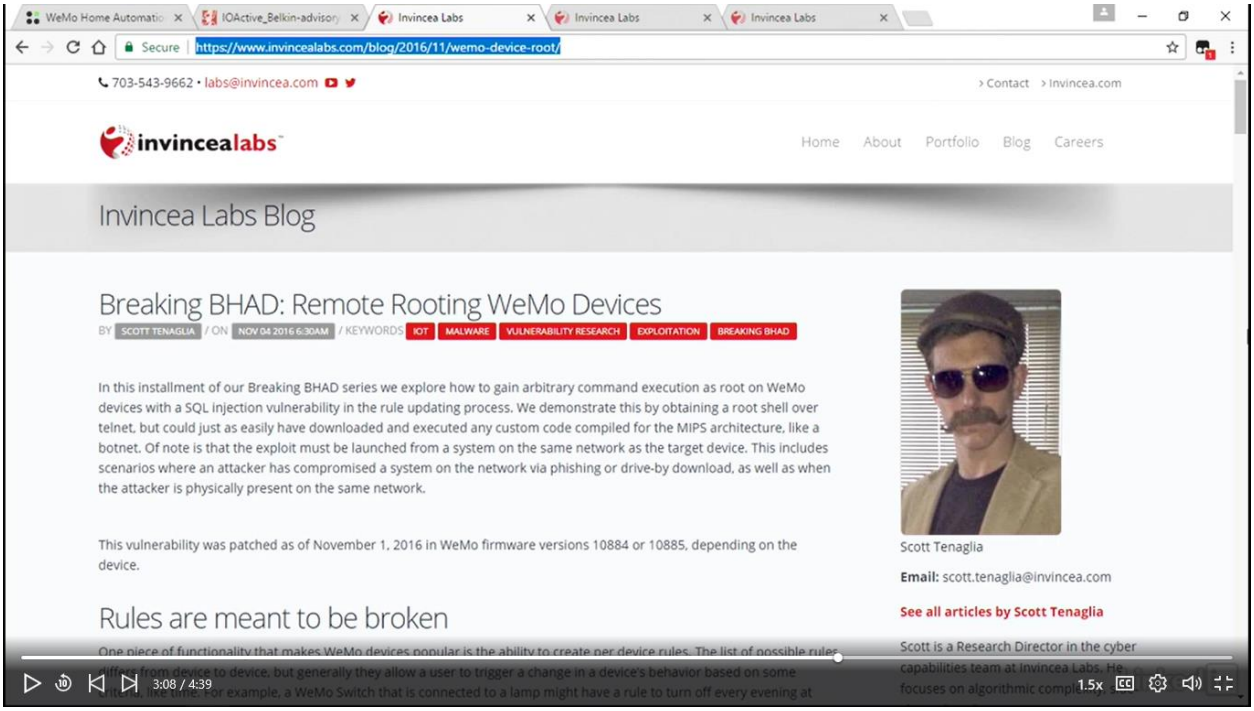
- Security testing sites can be targets for hackers.
- Sites may be flagged as dangerous.
- You must use due diligence when downloading software.

1:01 / 1:02 1.5x

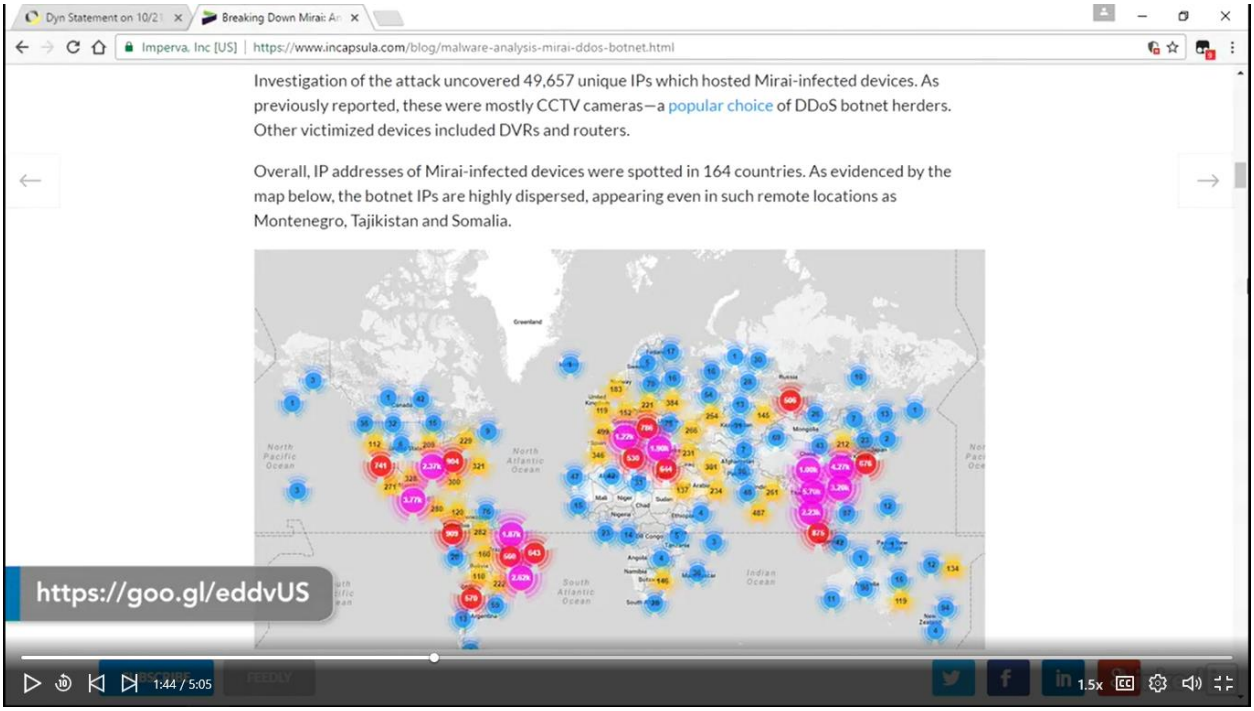



WeMo Home Automatio
IOActive_Belkin-advisory
Invincea Labs
Invincea Labs
Invincea Labs
www.ioactive.com/pdfs/IOActive_Belkin-advisory-lite.pdf
IOActive
IOActive Security Advisory
Title
Belkin WeMo Home Automation Vulnerabilities
Severity
Critical
Discovered by
Mike Davis
Affected Products
Belkin WeMo products
Devices built on the WeMo firmware
Impact
Belkin has recently produced a line of home-automation products under the WeMo name. For more information, see:
http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation
These products feature iPhone and Android applications that:
onboard sensors, such as motion sensors and streaming audio
controls, such as relays and LEDs
While researchers have reported some security issues relating to these products, their cloud features are secure when used on
https://goo.gl/2KFvgW
0:55 / 4:39
http://www.youtube.com/watch?v=BcW2q0aHOFo
1.5x


Wemo Light Switch
Remote control
Malicious signed firmware
Remote monitoring
Internal LAN access
1:48 / 4:39
1.5x


WeMo Home Automatio
IOActive_Belkin-advisory
Invincea Labs
Invincea Labs
Invincea Labs
Secure
https://www.invincealabs.com/blog/2016/11/wemo-device-root/
703-543-9662 • labs@invincea.com
› Contact › Invincea.com
invincealabs
Home About Portfolio Blog Careers
Invincea Labs Blog
Breaking BHAD: Remote Rooting WeMo Devices
BY SCOTT TENAGLIA / ON NOV 04 2016 6:30AM / KEYWORDS IOT MALWARE VULNERABILITY RESEARCH EXPLOITATION BREAKING BHAD
In this installment of our Breaking BHAD series we explore how to gain arbitrary command execution as root on WeMo devices with a SQL injection vulnerability in the rule updating process. We demonstrate this by obtaining a root shell over telnet, but could just as easily have downloaded and executed any custom code compiled for the MIPS architecture, like a botnet. Of note is that the exploit must be launched from a system on the same network as the target device. This includes scenarios where an attacker has compromised a system on the network via phishing or drive-by download, as well as when the attacker is physically present on the same network.
This vulnerability was patched as of November 1, 2016 in WeMo firmware versions 10884 or 10885, depending on the device.
Rules are meant to be broken
Scott Tenaglia
Email: scott.tenaglia@invincea.com
See all articles by Scott Tenaglia
Scott is a Research Director in the cyber
3:08 / 4:39
1.5x


Dyn Mirai Attack
Smart developers
Posted for script kiddies to use
1:34 / 5:05
1.5x



Dyn Mirai Technology

- Targets Linux, especially IoT devices
- SSH and telnet access vector
- Tries default and guessable credentials

  root/vizxv

  admin/1111111

Dyn Mirai Technology

- Targets such as home routers

  ZTE, using root/Zte521

  Ubiquiti airOS, using UBNT/UBNT

Dyn Mirai Sequence of Events

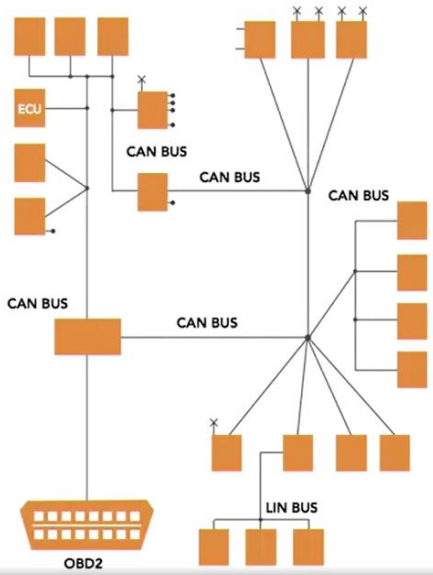
- TCP port 48101 process check
- Hides process name
- Detects debugging
- Closes ports 22, 23, and 80

Dyn Mirai Strength

- SYN scan network to propagate
- Real-time loading
- Attacks
  - HTTP flood
  - GRE IP and ethernet floods
  - SYN and ACK floods
  - STOMP, DNS, and UDP floods
  - DNS "water torture" attack

4:25 / 5:05 1.5x

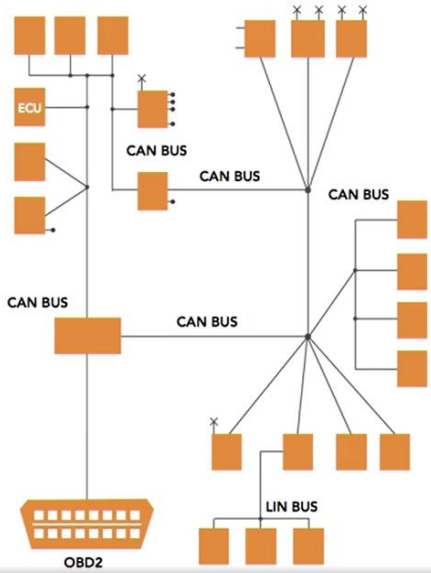
Hijacking the Physical World



0:22 / 7:40 1.5x

Hijacking the Physical World

- **Access also via**
  - Bluetooth
  - Wi-Fi
  - Internet



1:04 / 7:40

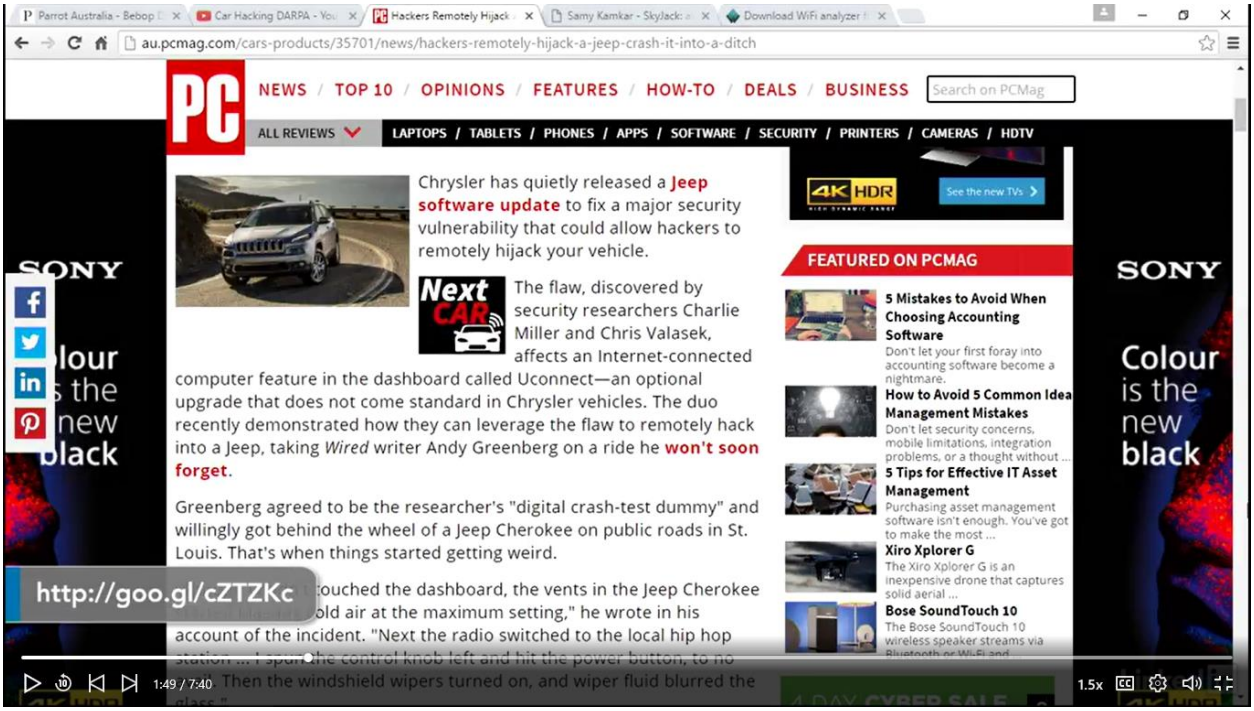
1.5x

Need for Remote Vehicle Access

- Crash alerts
- Pursuit
- Engine performance monitoring

https://goo.gl/r73wDb

1:34 / 7:40 1.5x

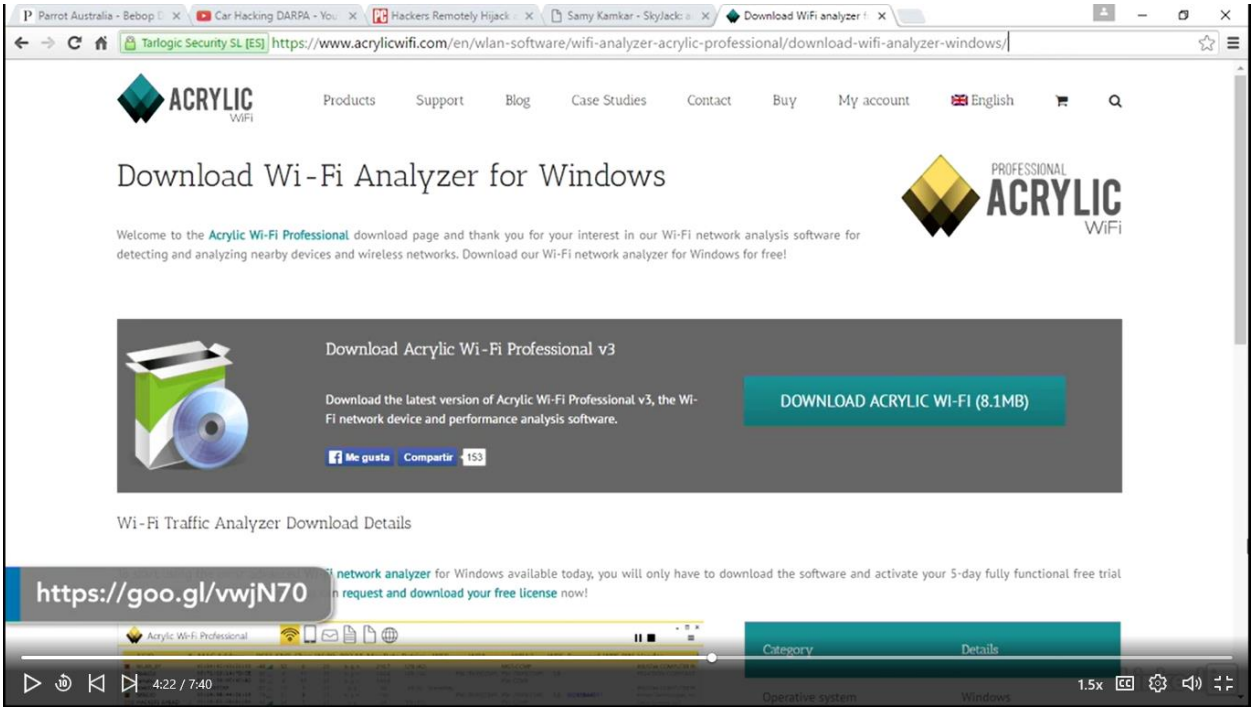


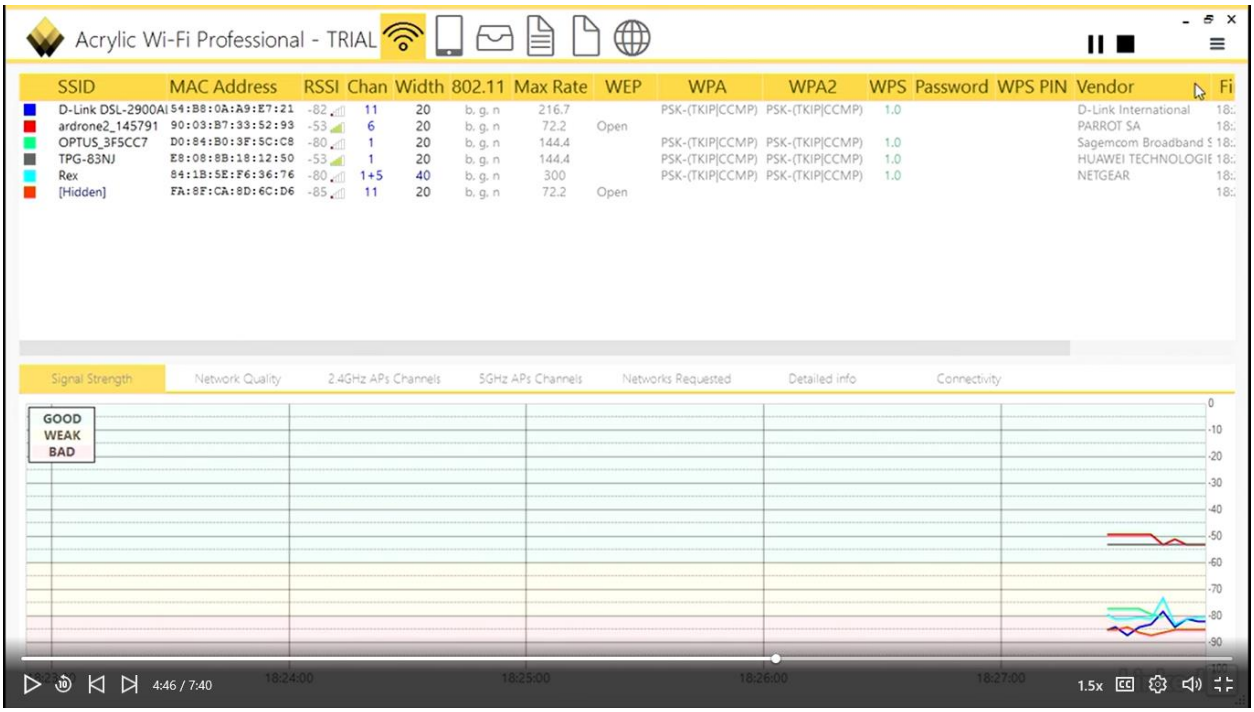
Parrot Drone

- UDP 5554—telemetry data
- TCP 5555—streaming video
- UDP 5556—flight commands
- UDP 5559—critical data

Kamkar SkyJack

- Client controlling flight
- Attacker sends deauthentication packets
- Drone drops connection
- Attacker connects

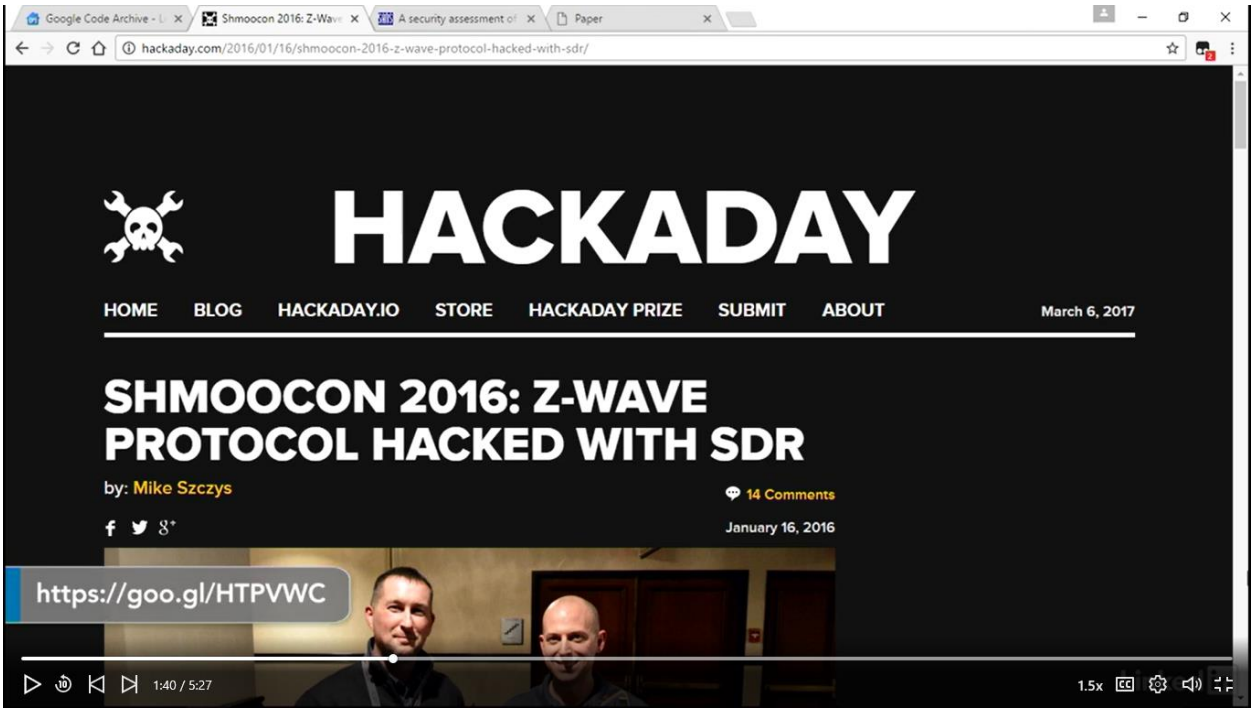

Parrot Australia - Bebop
Car Hacking DARPA - You
Hackers Remotely Hijack
Samy Kamkar - SkyJack
Download WiFi analyzer
Tarlogic Security SL [ES]
https://www.acrylicwifi.com/en/wlan-software/wifi-analyzer-acrylic-professional/download-wifi-analyzer-windows/
ACRYLIC WiFi
Products
Support
Blog
Case Studies
Contact
Buy
My account
English
Download Wi-Fi Analyzer for Windows
PROFESSIONAL ACRYLIC WiFi
Welcome to the Acrylic Wi-Fi Professional download page and thank you for your interest in our Wi-Fi network analysis software for detecting and analyzing nearby devices and wireless networks. Download our Wi-Fi network analyzer for Windows for free!
Download Acrylic Wi-Fi Professional v3
Download the latest version of Acrylic Wi-Fi Professional v3, the Wi-Fi network device and performance analysis software.
DOWNLOAD ACRYLIC WI-FI (8.1MB)
Me gusta
Compartir
153
Wi-Fi Traffic Analyzer Download Details
network analyzer for Windows available today, you will only have to download the software and activate your 5-day fully functional free trial
request and download your free license now!
https://goo.gl/vwjN70
Category
Details
Operative system
Windows
4:22 / 7:40
1.5x

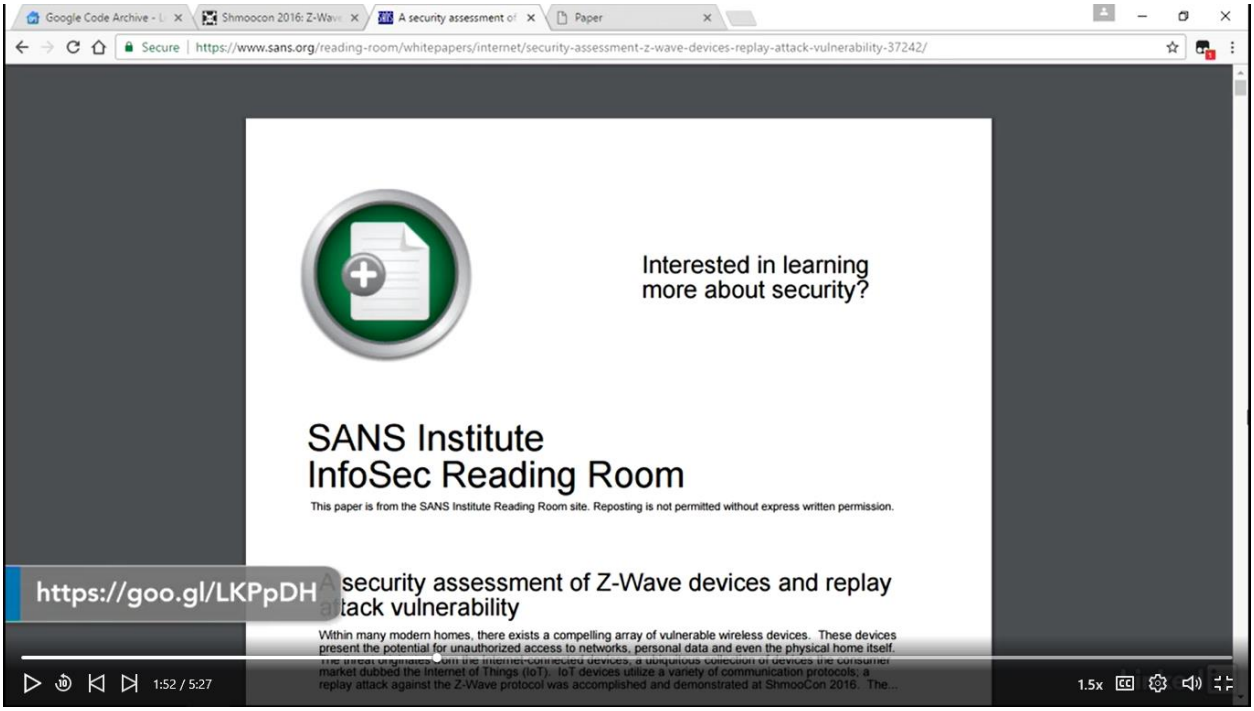

Acrylic Wi-Fi Professional - TRIAL
SSID
MAC Address
RSSI
Chan
Width
802.11
Max Rate
WEP
WPA
WPA2
WPS
Password
WPS PIN
Vendor
D-Link DSL-2900A
54:B8:0A:A9:E7:21
-82
11
20
b. g. n
216.7
PSK-(TKIP|CCMP)
PSK-(TKIP|CCMP)
1.0
D-Link International
ardrone2_145791
90:03:B7:33:52:93
-53
6
20
b. g. n
72.2
Open
PARROT SA
OPTUS_3F5CC7
D0:84:B0:3F:5C:C8
-80
1
20
b. g. n
144.4
PSK-(TKIP|CCMP)
PSK-(TKIP|CCMP)
1.0
Sagemcom Broadband S
TPG-83NJ
E8:08:8B:18:12:50
-53
1
20
b. g. n
144.4
PSK-(TKIP|CCMP)
PSK-(TKIP|CCMP)
1.0
HUAWEI TECHNOLOGIE
Rex
84:1B:5E:F6:36:76
-80
1+5
40
b. g. n
300
PSK-(TKIP|CCMP)
PSK-(TKIP|CCMP)
1.0
NETGEAR
[Hidden]
FA:8F:CA:8D:6C:D6
-85
11
20
b. g. n
72.2
Open
Signal Strength
Network Quality
2.4GHz APs Channels
5GHz APs Channels
Networks Requested
Detailed info
Connectivity
GOOD
WEAK
BAD
18:24:00
18:25:00
18:26:00
18:27:00
4:46 / 7:40
1.5x

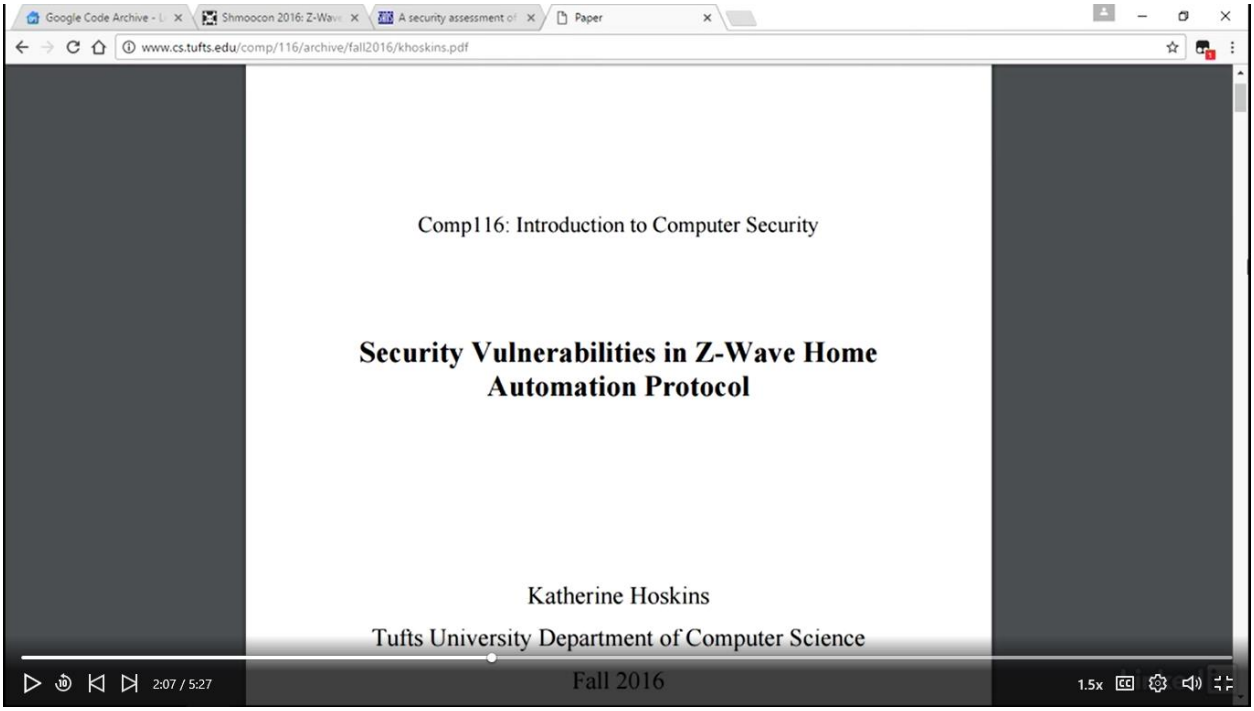
Z-Wave

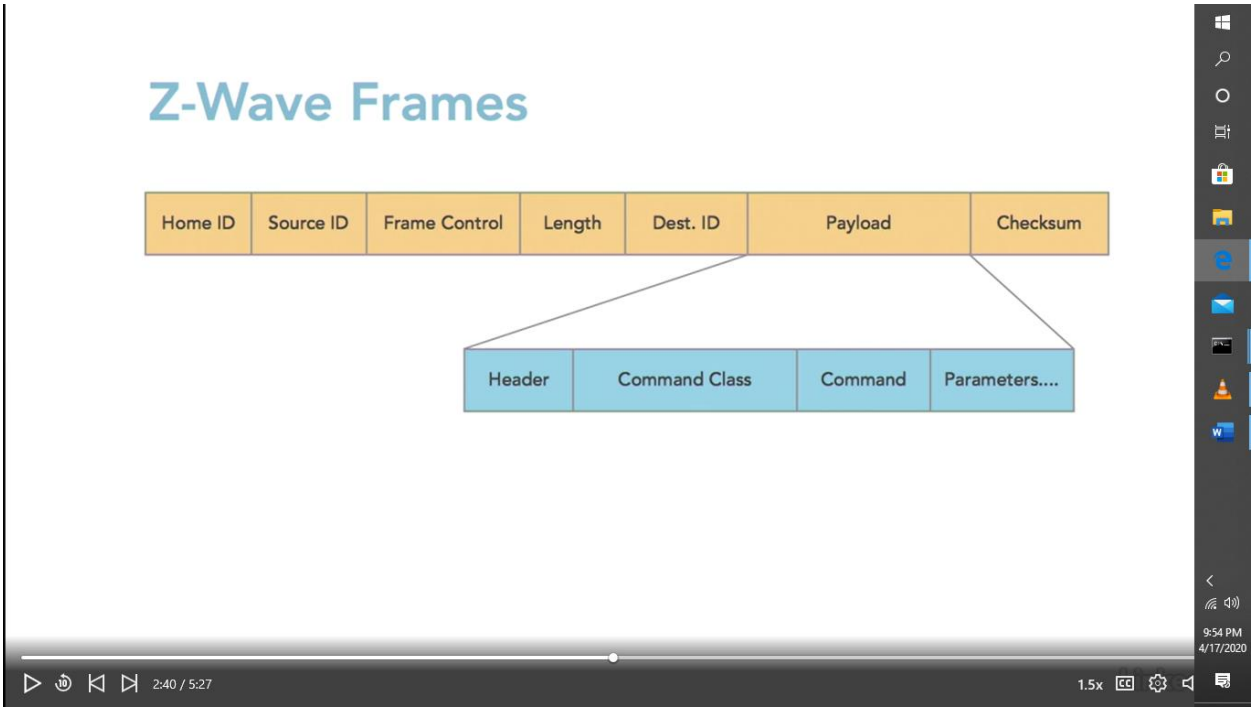
- Radio-based low-latency connections
- Controller and one or more devices
- Mesh network
- Device pairs to the controller

1:28 / 5:27 1.5x




Google Code Archive - L
Shmoocon 2016: Z-Wave
A security assessment of
Paper
Secure
https://www.sans.org/reading-room/whitepapers/internet/security-assessment-z-wave-devices-replay-attack-vulnerability-37242/
Interested in learning more about security?
SANS Institute
InfoSec Reading Room
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.
https://goo.gl/LKPpDH
security assessment of Z-Wave devices and replay
tack vulnerability
Within many modern homes, there exists a compelling array of vulnerable wireless devices. These devices present the potential for unauthorized access to networks, personal data and even the physical home itself.
market dubbed the Internet of Things (IoT). IoT devices utilize a variety of communication protocols; a replay attack against the Z-Wave protocol was accomplished and demonstrated at ShmooCon 2016. The...
1:52 / 5:27
1.5x


Google Code Archive - L
Shmoocon 2016: Z-Wave
A security assessment of
Paper
www.cs.tufts.edu/comp/116/archive/fall2016/khoskins.pdf
Comp116: Introduction to Computer Security
Security Vulnerabilities in Z-Wave Home Automation Protocol
Katherine Hoskins
Tufts University Department of Computer Science
Fall 2016
2:07 / 5:27
1.5x


Z-Wave Frames
Home ID
Source ID
Frame Control
Length
Dest. ID
Payload
Checksum
Header
Command Class
Command
Parameters....
2:40 / 5:27
1.5x
9:54 PM
4/17/2020

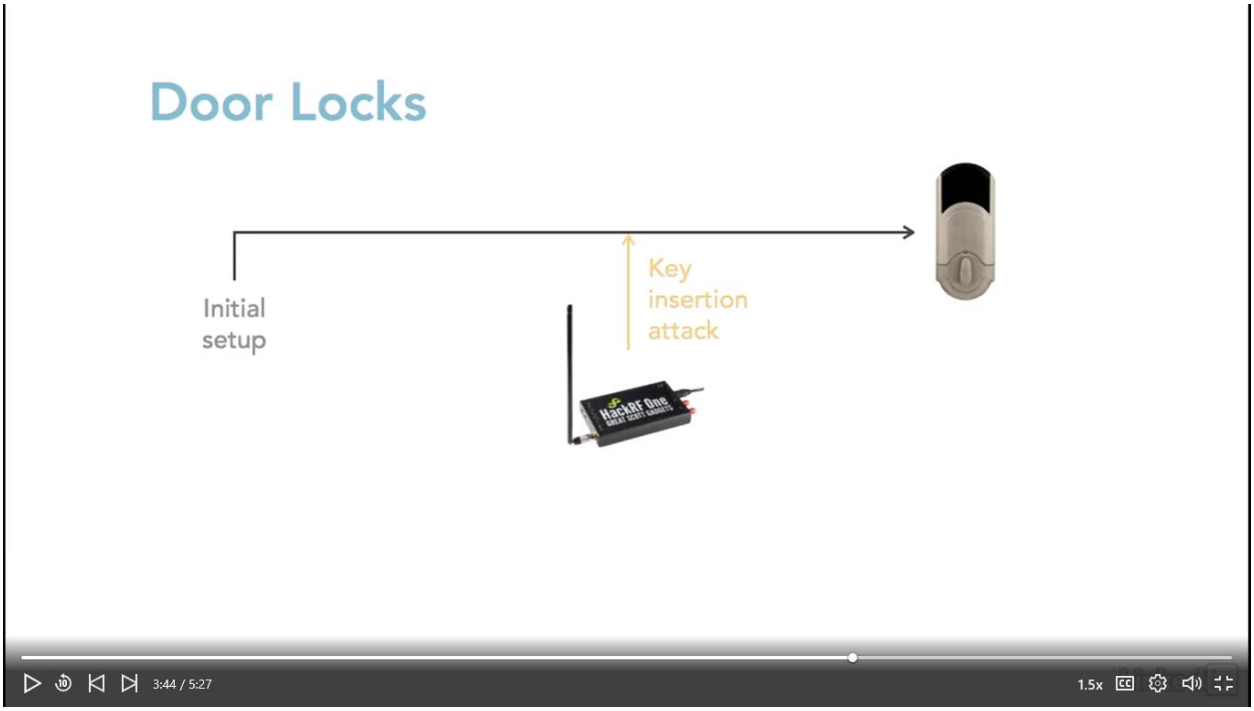
Z-Wave Command

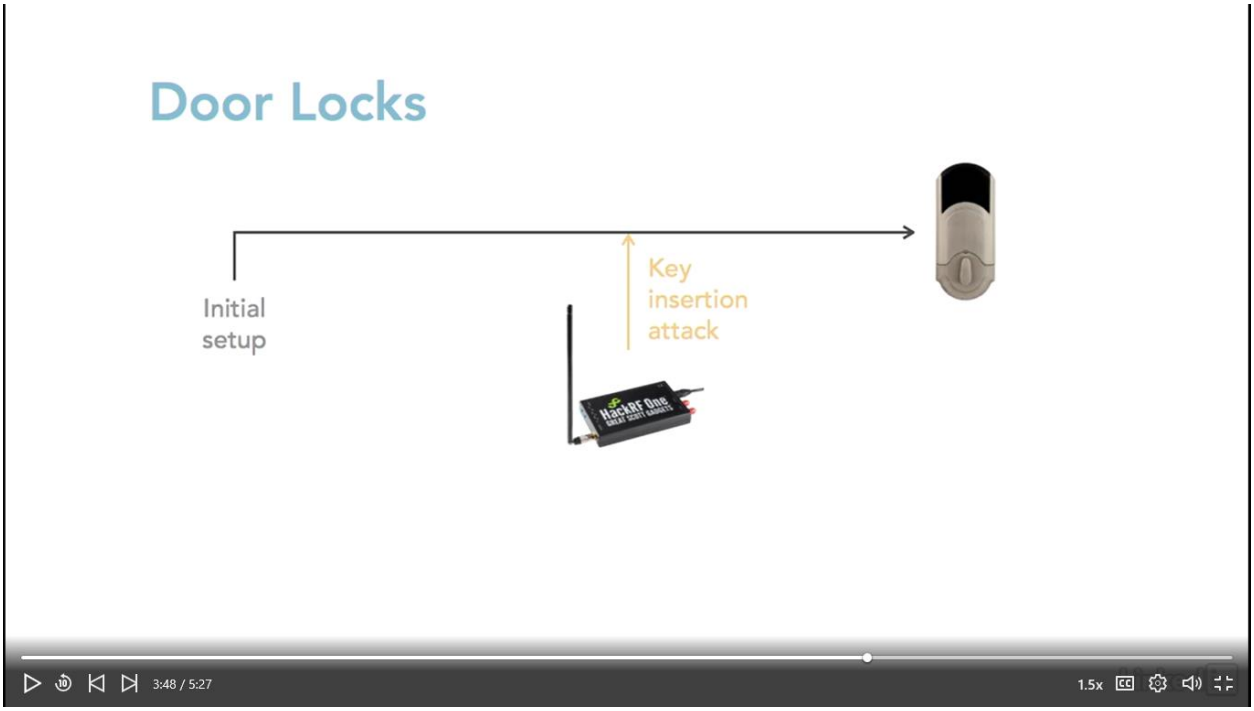
7	6	5	4	3	2	1	0
Command Class = COMMAND_CLASS_IRRIGATION							
Command = IRRIGATION_SYSTEM_INFO_REPORT							
Reserved			Reserved		Reserved		Master Valve
Total Number of Valves							
Total Number of Valve Tables							
Reserved				Valve Table Max Size			

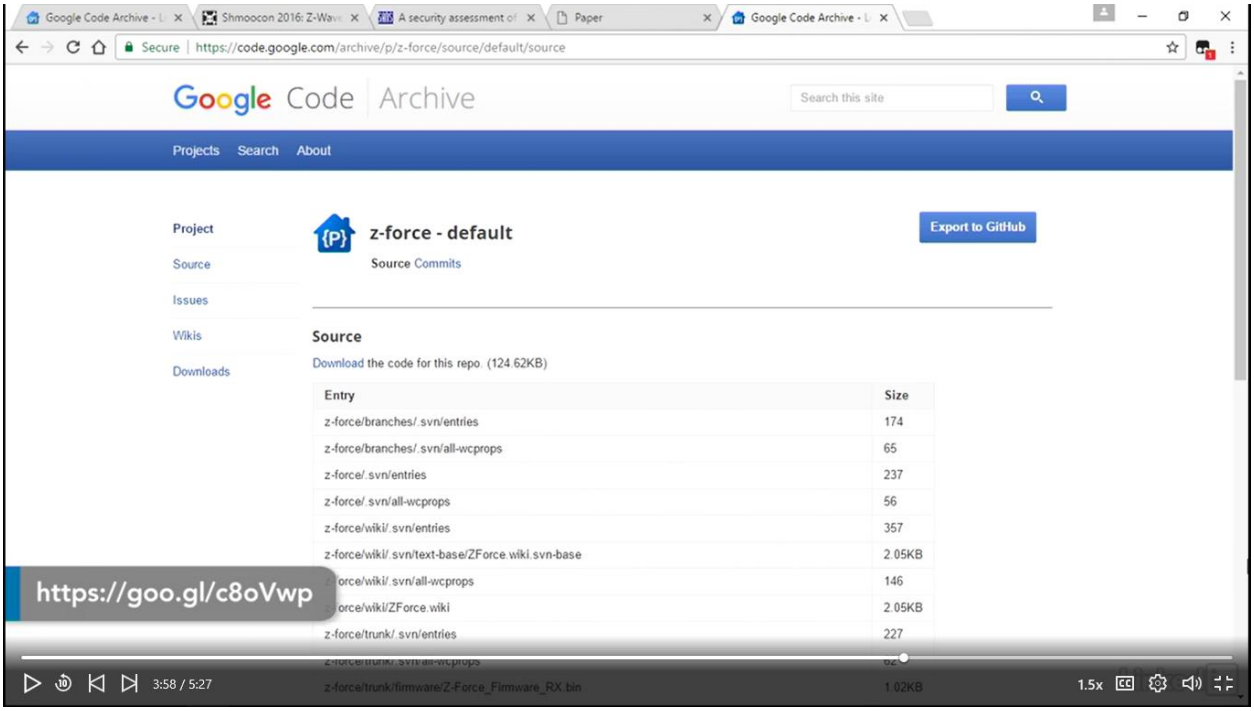
2:52 / 5:27 1.5x

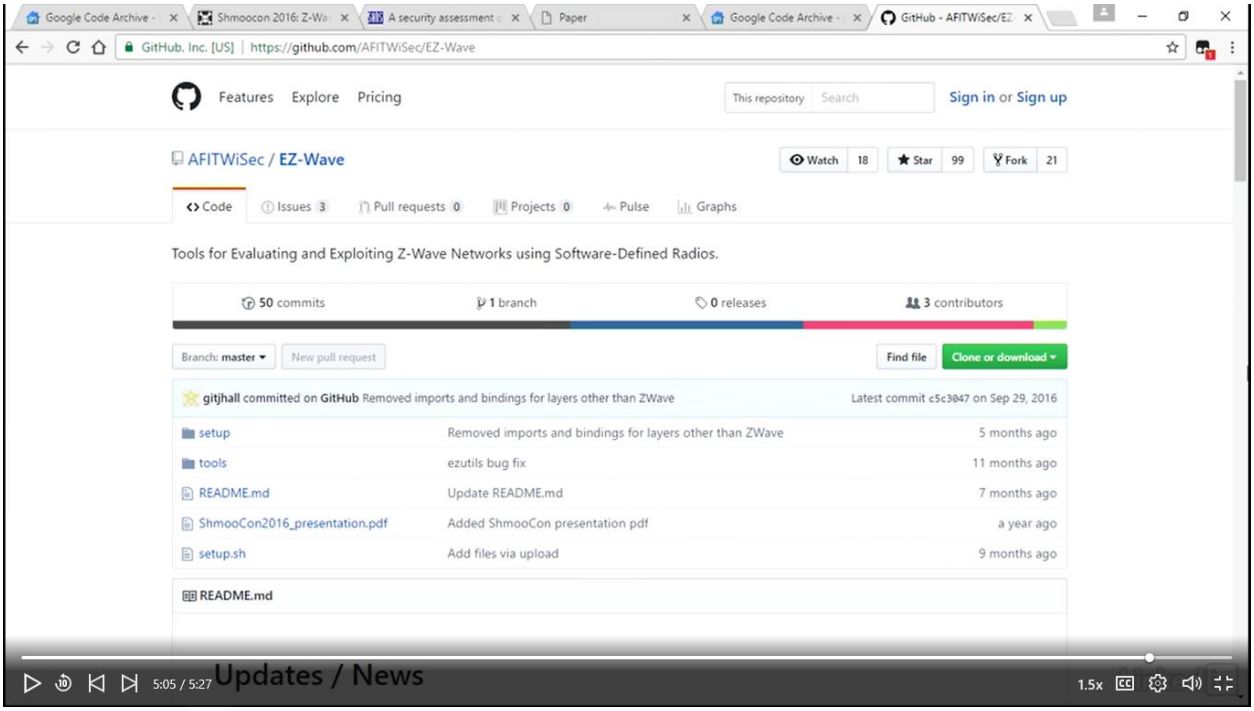
Door Locks

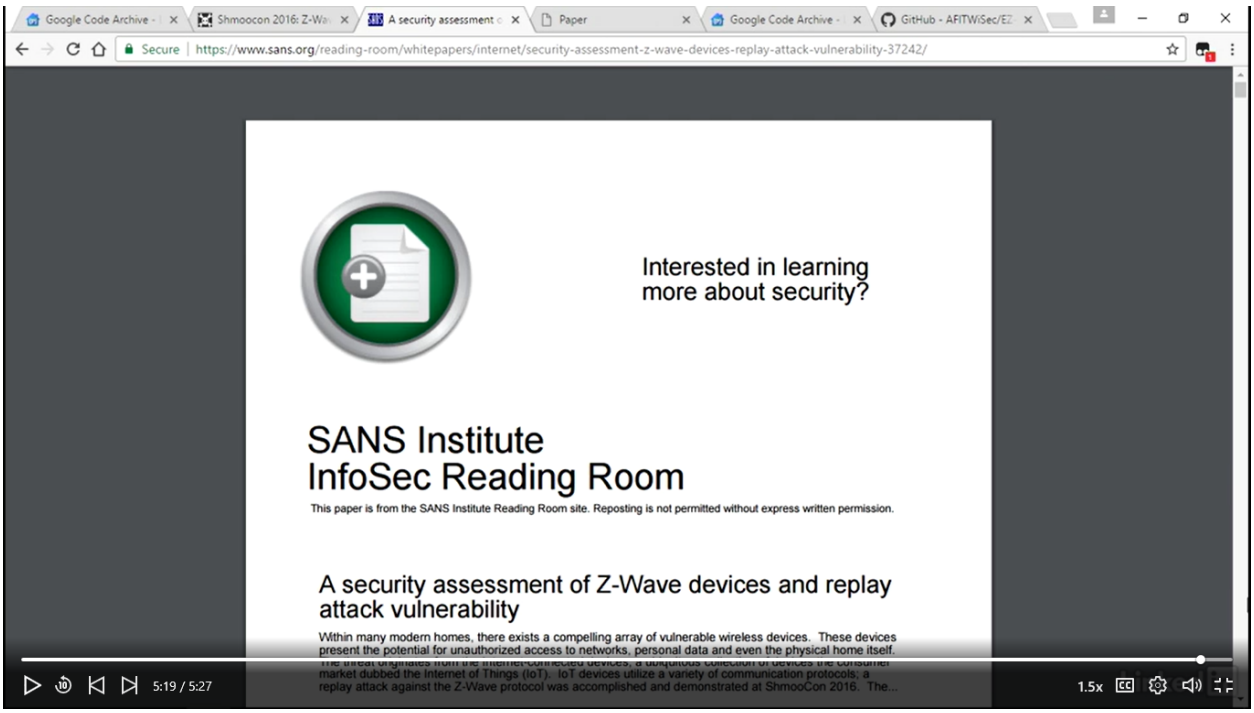
3:39 / 5:27 1.5x

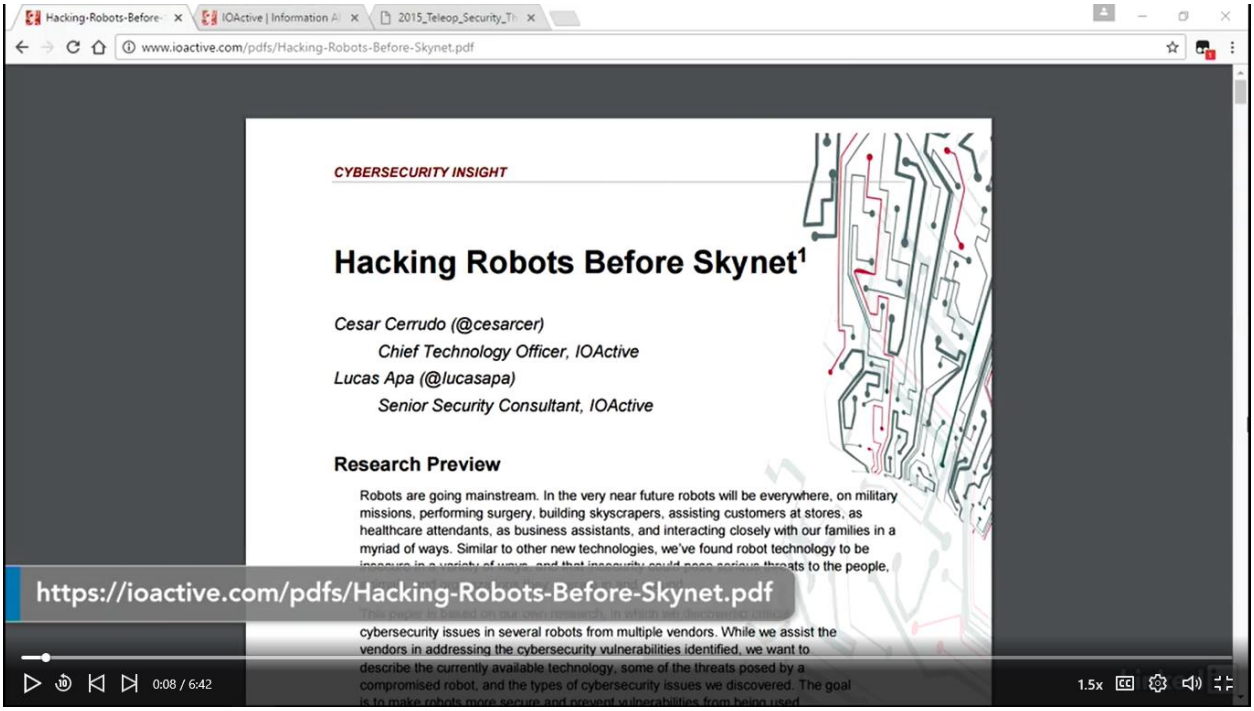

Door Locks
Initial setup
Key insertion attack
HackRF One
3:44 / 5:27
1.5x


Door Locks
Initial setup
Key insertion attack
HackRF One
3:48 / 5:27
1.5x


Google Code Archive - L
Shmoocon 2016: Z-Wave
A security assessment of
Paper
Google Code Archive - L
Secure | https://code.google.com/archive/p/z-force/source/default/source
Google Code Archive
Search this site
Projects Search About
Project
Source
Issues
Wikis
Downloads
z-force - default
Source Commits
Export to GitHub
Source
Download the code for this repo. (124.62KB)
Entry
Size
z-force/branches/.svn/entries
174
z-force/branches/.svn/all-wcprops
65
z-force/.svn/entries
237
z-force/.svn/all-wcprops
56
z-force/wiki/.svn/entries
357
z-force/wiki/.svn/text-base/ZForce.wiki.svn-base
2.05KB
z-force/wiki/.svn/all-wcprops
146
z-force/wiki/ZForce.wiki
2.05KB
z-force/trunk/.svn/entries
227
z-force/trunk/firmware/Z-Force_Firmware_RX.bin
1.02KB
https://goo.gl/c8oVwp
3:58 / 5:27
1.5x


Google Code Archive -
Shmoocon 2016: Z-Wa
A security assessment
Paper
Google Code Archive -
GitHub - AFITWiSec/EZ
GitHub, Inc. [US] | https://github.com/AFITWiSec/EZ-Wave
Features Explore Pricing
This repository Search
Sign in or Sign up
AFITWiSec / EZ-Wave
Watch 18 Star 99 Fork 21
Code Issues 3 Pull requests 0 Projects 0 Pulse Graphs
Tools for Evaluating and Exploiting Z-Wave Networks using Software-Defined Radios.
50 commits 1 branch 0 releases 3 contributors
Branch: master New pull request
Find file Clone or download
gitjhall committed on GitHub Removed imports and bindings for layers other than ZWave
Latest commit c5c3047 on Sep 29, 2016
setup Removed imports and bindings for layers other than ZWave 5 months ago
tools ezutils bug fix 11 months ago
README.md Update README.md 7 months ago
ShmooCon2016_presentation.pdf Added ShmooCon presentation pdf a year ago
setup.sh Add files via upload 9 months ago
README.md
5:05 / 5:27
Updates / News
1.5x


Google Code Archive -
Shmoocon 2016: Z-Wa
A security assessment
Paper
Google Code Archive -
GitHub - AFITWiSec/EZ
Secure | https://www.sans.org/reading-room/whitepapers/internet/security-assessment-z-wave-devices-replay-attack-vulnerability-37242/
Interested in learning more about security?
SANS Institute
InfoSec Reading Room
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.
A security assessment of Z-Wave devices and replay attack vulnerability
Within many modern homes, there exists a compelling array of vulnerable wireless devices. These devices present the potential for unauthorized access to networks, personal data and even the physical home itself.
market dubbed the Internet of Things (IoT). IoT devices utilize a variety of communication protocols; a replay attack against the Z-Wave protocol was accomplished and demonstrated at ShmooCon 2016. The...
5:19 / 5:27
1.5x


Hacking-Robots-Before-
IOActive | Information Al
2015_Teleop_Security_Th
www.ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf
CYBERSECURITY INSIGHT
Hacking Robots Before Skynet[1]
Cesar Cerrudo (@cesarcer)
Chief Technology Officer, IOActive
Lucas Apa (@lucasapa)
Senior Security Consultant, IOActive
Research Preview
Robots are going mainstream. In the very near future robots will be everywhere, on military missions, performing surgery, building skyscrapers, assisting customers at stores, as healthcare attendants, as business assistants, and interacting closely with our families in a myriad of ways. Similar to other new technologies, we've found robot technology to be
https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf
cybersecurity issues in several robots from multiple vendors. While we assist the vendors in addressing the cybersecurity vulnerabilities identified, we want to describe the currently available technology, some of the threats posed by a compromised robot, and the types of cybersecurity issues we discovered. The goal
0:08 / 6:42
1.5x

Home and Industrial Robots

- IOActive Research
  - UBTech, SoftBank, and ROBOTIS
  - Universal Robots and Rethink Robotics
  - Asratec control software

0:35 / 6:42 1.5x

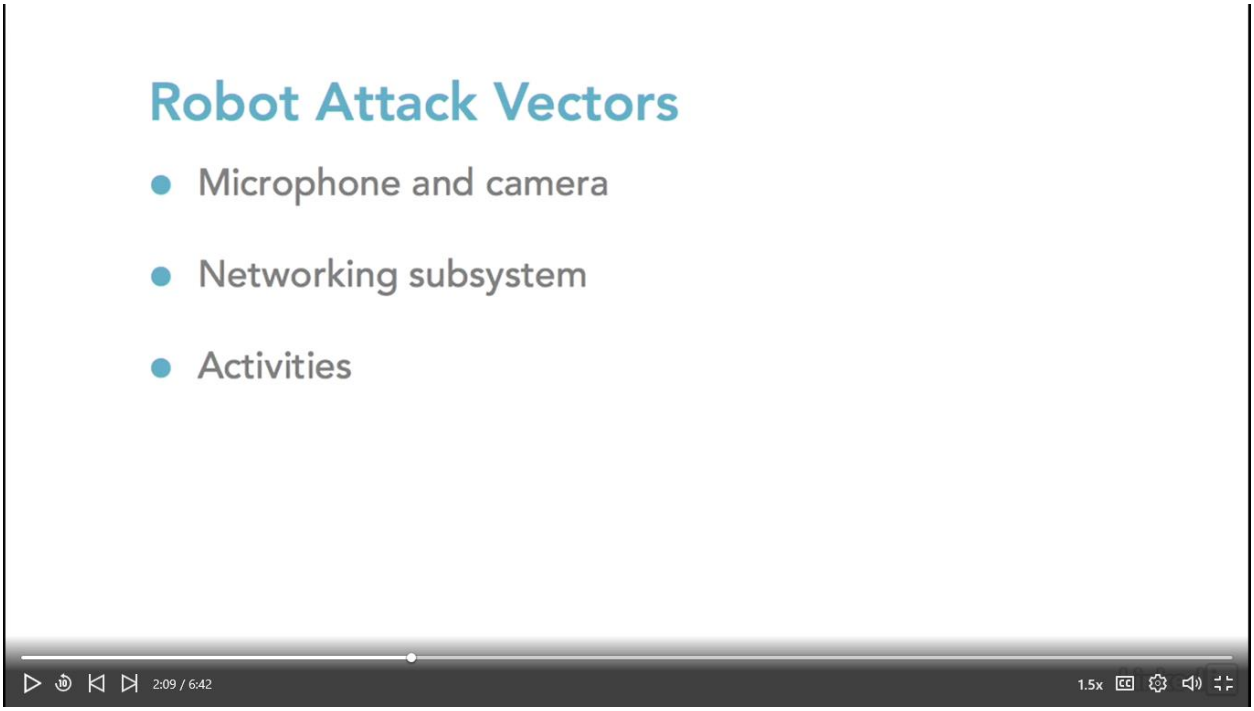
Robot Security Issues

- Insecure communications
- Authentication issues
- Missing authorization
- Weak cryptography
- Privacy issues
- Weak default configuration

0:56 / 6:42 1.5x


Hacking-Robots-Before-
IOActive | Information Al
2015_Teleop_Security_Th
www.ioactive.com/alerts/robotics-hacking-research2.html
IOActive
SERVICES
INDUSTRIES
IOACTIVE LABS
NEWS
ABOUT
CONTACT
IOActive
HACKING ROBOTS
BEFORE SKYNET
ROBOTICS HACKING RESEARCH
https://www.ioactive.com/alerts/robotics-hacking-research.html
1:01 / 6:42
1.5x


Robot Software Vulnerabilities
Robot operating system
Cleartext communication
Authentication issues
Weak authorization
1:29 / 6:42
1.5x

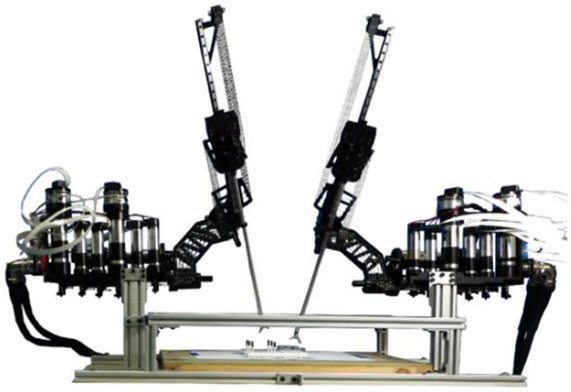

Robot Attack Vectors
Microphone and camera
Networking subsystem
Activities
2:09 / 6:42
1.5x

Industrial Robots

- Larger and more powerful
- 2014 – worker killed in Japan
- 2015 – worker killed in Germany

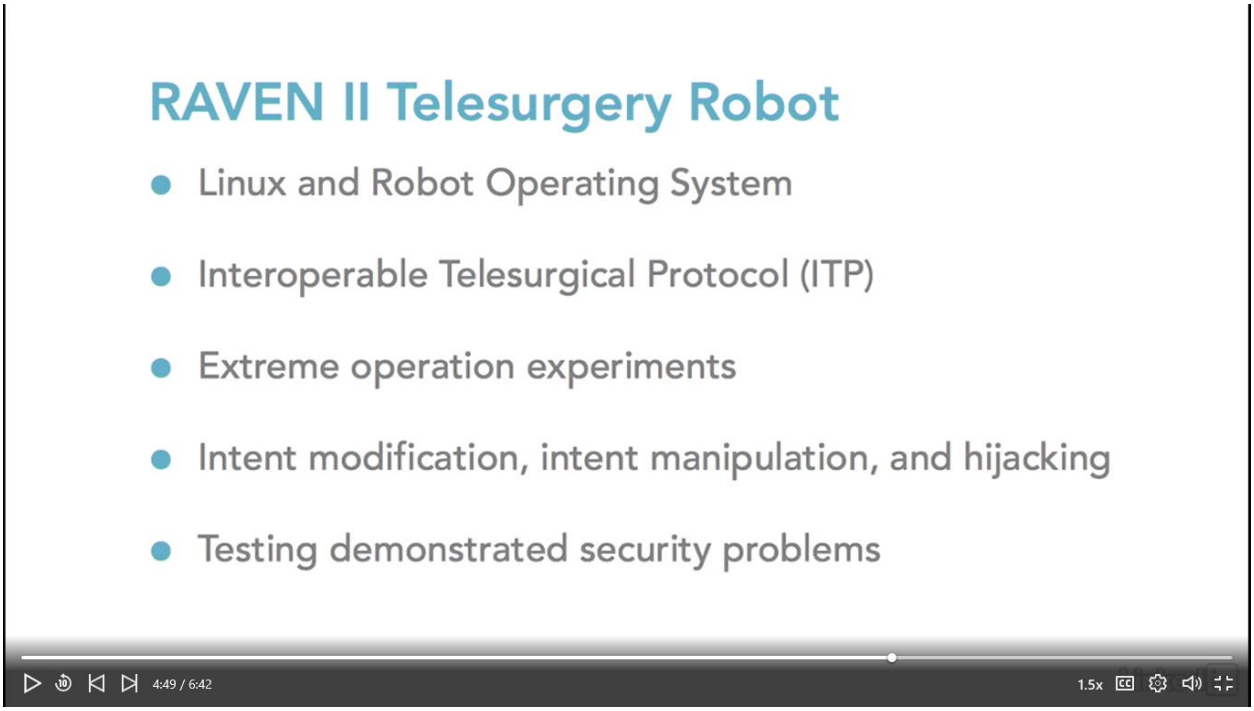
2:58 / 6:42 1.5x

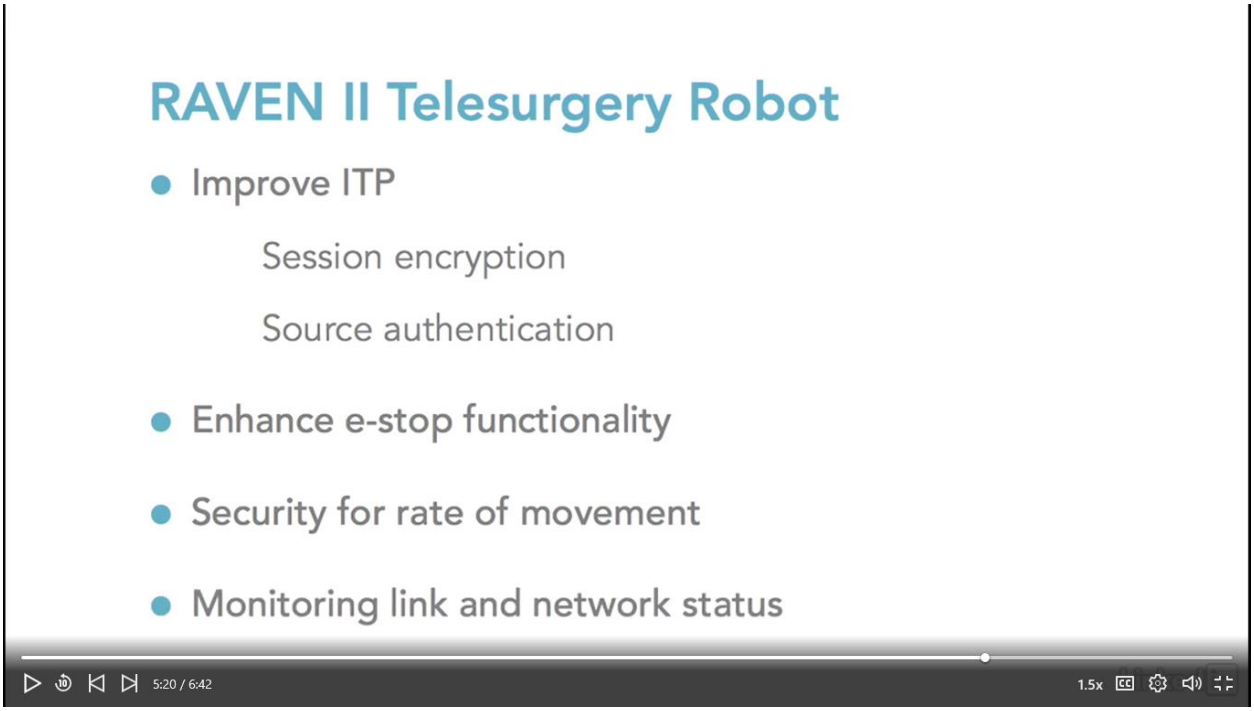
Teleoperated Surgical Robots



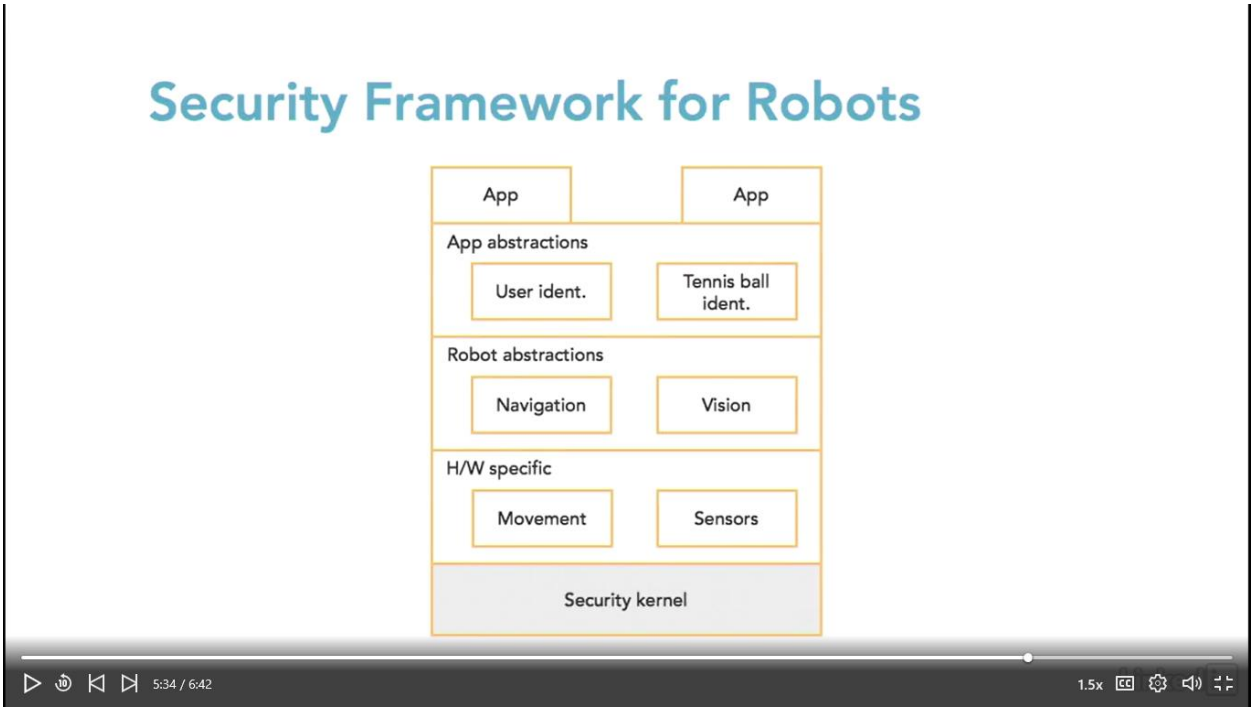
RAVEN II

3:38 / 6:42 1.5x


RAVEN II Telesurgery Robot
Linux and Robot Operating System
Interoperable Telesurgical Protocol (ITP)
Extreme operation experiments
Intent modification, intent manipulation, and hijacking
Testing demonstrated security problems
4:49 / 6:42
1.5x


RAVEN II Telesurgery Robot
Improve ITP
Session encryption
Source authentication
Enhance e-stop functionality
Security for rate of movement
Monitoring link and network status
5:20 / 6:42
1.5x


Hacking-Robots-Before-
IOActive | Information Al
2015_Teleop_Security_Th
brl.ee.washington.edu/eprints/6/1/2015_Teleop_Security_Threats.pdf
To Make a Robot Secure:
An Experimental Analysis of Cyber Security Threats Against
Teleoperated Surgical Robotics*
Tamara Bonaci†, Jeffrey Herron †, Tariq Yusuf‡, Junjie Yan†, Tadayoshi Kohno‡, Howard Jay Chizeck†‡
May 12, 2015
Abstract
Teleoperated robots are playing an increasingly important role in military actions and medical services. In the future, remotely operated surgical robots will likely be used in more scenarios such as battlefields and emergency response. But rapidly growing applications of teleoperated surgery raise the question; what if the computer systems for these robots are attacked, taken over and even turned into weapons?
Our work seeks to answer this question by systematically analyzing possible cyber security attacks against Raven II®, an advanced teleoperated robotic surgery system. We identify a slew of possible cyber security threats, and experimentally evaluate their scopes and impacts. We demonstrate the ability to maliciously control a wide range of robots functions, and even to completely ignore or override command inputs from the surgeon. We further find that it is possible to abuse the robot's existing emergency stop (E-stop) mechanism to execute efficient (single packet) attacks.
We then consider steps to mitigate these identified attacks, and experimentally evaluate the feasibility of applying the existing security solutions against these threats. The broader goal of our paper, however, is to raise awareness and increase understanding of these emerging threats. We anticipate that the majority of attacks against telerobotic surgery will also be relevant to other teleoperated robotic and co-robotic systems.
1 Introduction
https://goo.gl/xQnnUh
5:26 / 6:42
1.5x


Security Framework for Robots
App
App
App abstractions
User ident.
Tennis ball ident.
Robot abstractions
Navigation
Vision
H/W specific
Movement
Sensors
Security kernel
5:34 / 6:42
1.5x


www.ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf
CYBERSECURITY INSIGHT
Hacking Robots Before Skynet[1]
Cesar Cerrudo (@cesarcer)
Chief Technology Officer, IOActive
Lucas Apa (@lucasapa)
Senior Security Consultant, IOActive
Research Preview
Robots are going mainstream. In the very near future robots will be everywhere, on military missions, performing surgery, building skyscrapers, assisting customers at stores, as healthcare attendants, as business assistants, and interacting closely with our families in a myriad of ways. Similar to other new technologies, we've found robot technology to be insecure in a variety of ways, and that insecurity could pose serious threats to the people, animals, and organizations they operate in and around.
This paper is based on our own research, in which we discovered critical cybersecurity issues in several robots from multiple vendors. While we assist the vendors in addressing the cybersecurity vulnerabilities identified, we want to describe the currently available technology, some of the threats posed by a compromised robot, and the types of cybersecurity issues we discovered. The goal
0:19 / 6:42
1.5x

Home and Industrial Robots

- IOActive Research
  - UBTech, SoftBank, and ROBOTIS
  - Universal Robots and Rethink Robotics
  - Asratec control software


Robot Security Issues
Insecure communications
Authentication issues
Missing authorization
Weak cryptography
Privacy issues
Weak default configuration
0:56 / 6:42
1.5x


www.ioactive.com/alerts/robotics-hacking-research2.html
IOActive
SERVICES
INDUSTRIES
IOACTIVE LABS
NEWS
ABOUT
CONTACT
IOActive
HACKING ROBOTS
BEFORE SKYNET
ROBOTICS HACKING RESEARCH
As electronic devices become smarter and the cost of cutting-edge technology decreases, machines can be used to actively help meet human needs, save lives, entertain, teach, and cure, amongst other things.
1:05 / 6:42
1.5x

Robot Software Vulnerabilities

- Robot operating system
  - Cleartext communication
  - Authentication issues
  - Weak authorization

Robot Attack Vectors

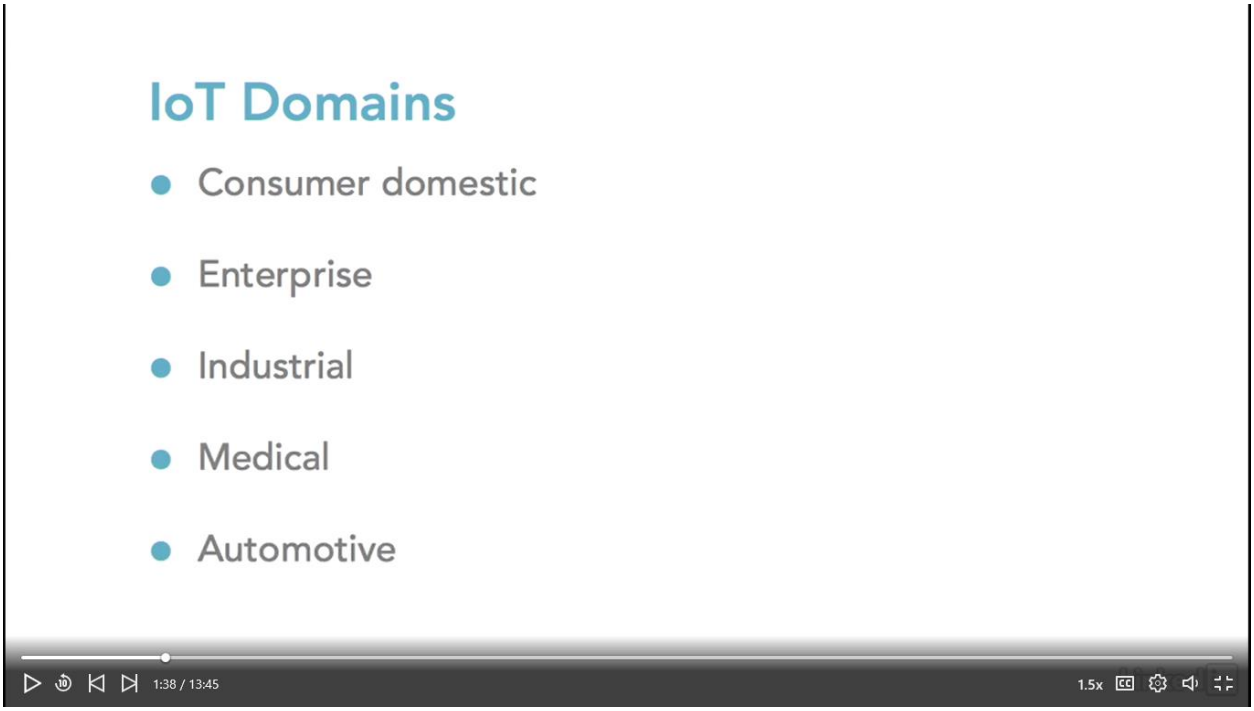
- Microphone and camera
- Networking subsystem
- Activities

Internet of Things

- 2002 – one billion mobile phones
- 2020 – up to 100 billion things (devices and sensors)
- Recognized security issue
- Emerging security frameworks and architectures

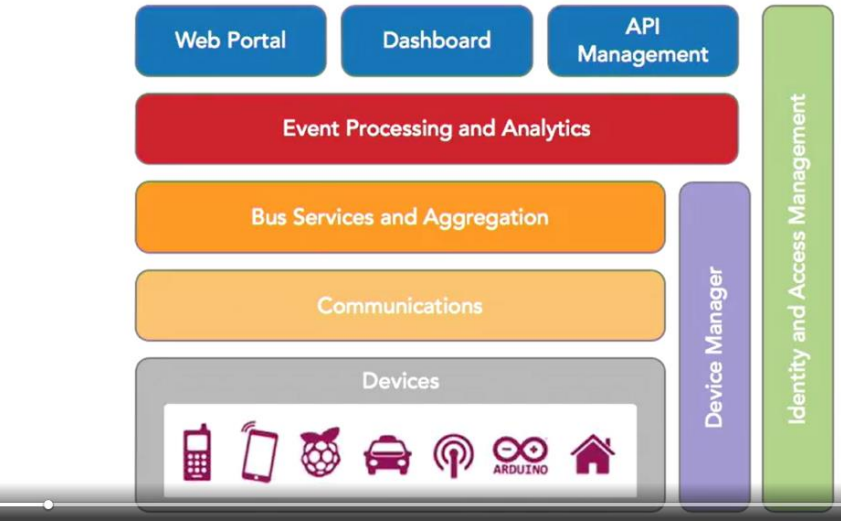
IoT Reference Architecture

- Supports many things
- Is modular and scalable


IoT Domains
Consumer domestic
Enterprise
Industrial
Medical
Automotive
1:38 / 13:45
1.5x


IoT Domains
Public agency
Critical infrastructure
1:45 / 13:45
1.5x

IoT Reference Architecture



1:55 / 13:45 1.5x

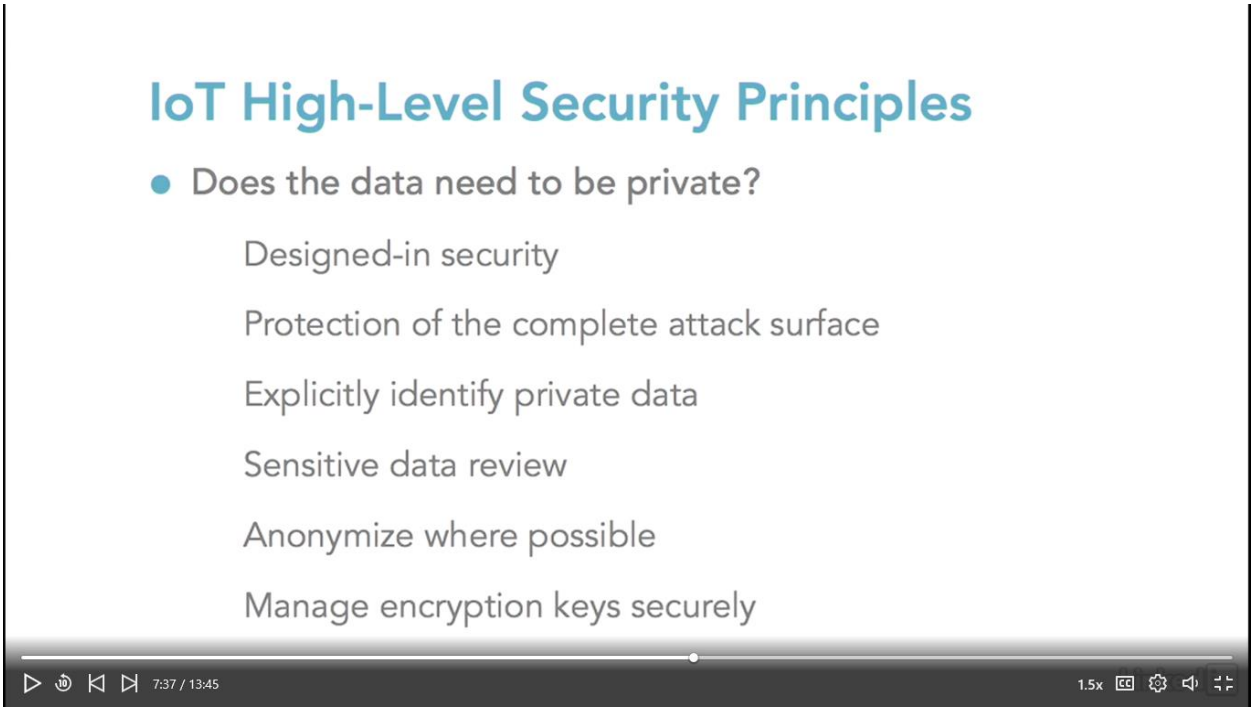
IoT Reference Architecture

- Sensors and devices
- Narrowband network
- Gateway and wideband network
- Server-side systems

4:11 / 13:45 1.5x


IoT Security and Privacy Requirements
Available on demand
Trusted to protect privacy
Not able to be compromised
Designed using robust trust and assurance frameworks
May be subject to privacy laws
5:02 / 13:45
1.5x


IoT Security and Privacy Requirements
Unsuitable to use traditional security controls
Agile and adaptable
Global ecosystem
High-level principles and sector-specific implementation
6:21 / 13:45
1.5x


IoT High-Level Security Principles
Does the data need to be private?
Designed-in security
Protection of the complete attack surface
Explicitly identify private data
Sensitive data review
Anonymize where possible
Manage encryption keys securely
7:37 / 13:45
1.5x


IoT High-Level Security Principles
Does the data need to be trusted?
Software integrity
Hardware root of trust
Data authentication and integrity
Malfunctioning devices revoked
Isolated data
Skip back
8:26 / 13:45
1.5x


IoT High-Level Security Principles
Does the data need to be trusted?
Testing and calibration
Trusted and verified metadata
Reuse
8:57 / 13:45
1.5x

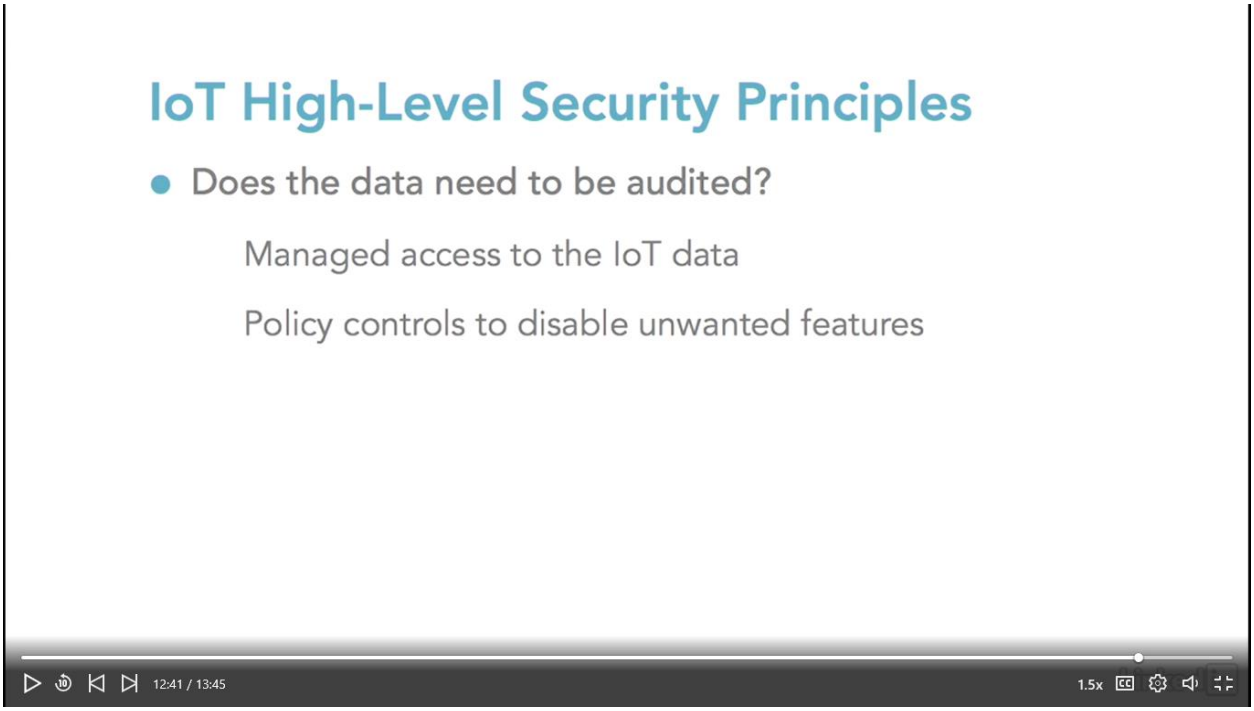

IoT High-Level Security Principles
Is the safe and timely arrival of data important?
Accurate timestamps
Designed-in integrity
Availability management
Safety and timeliness
Identified dependencies
9:41 / 13:45
1.5x


IoT High-Level Security Principles
Is the safe and timely arrival of data important?
Secure device identifier
Explicit functionality
10:20 / 13:45
1.5x


IoT High-Level Security Principles
Restrict access to or control of the device?
Designed-in defense against hacking
Secure and penetration tested code
Authenticated channel for service management
10:47 / 13:45
1.5x


IoT High-Level Security Principles
Update software on the device?
Best security practices
Authenticated source for updates and patches
Show device patching status
11:28 / 13:45
1.5x


IoT High-Level Security Principles
Secure transfer of device ownership?
Secure method of transfer
Clear status of ownership scope
Transfer – does not compromise security updates
12:14 / 13:45
1.5x


IoT High-Level Security Principles
Does the data need to be audited?
Managed access to the IoT data
Policy controls to disable unwanted features
12:41 / 13:45
1.5x


IoT Device Active Security Management
Updating the device software
Remotely enabling or disabling certain hardware capabilities
Remotely reconfiguring devices
Disconnecting a rogue or stolen device
13:23 / 13:45
1.5x

IoT Device Active Security Management

- Locating a lost device
- Remote wiping of data

Compliance Framework

- Release 1 – December 2016
- Supply chain approach
- Compliance process:
  - Product domain
  - Compliance class

Compliance Class

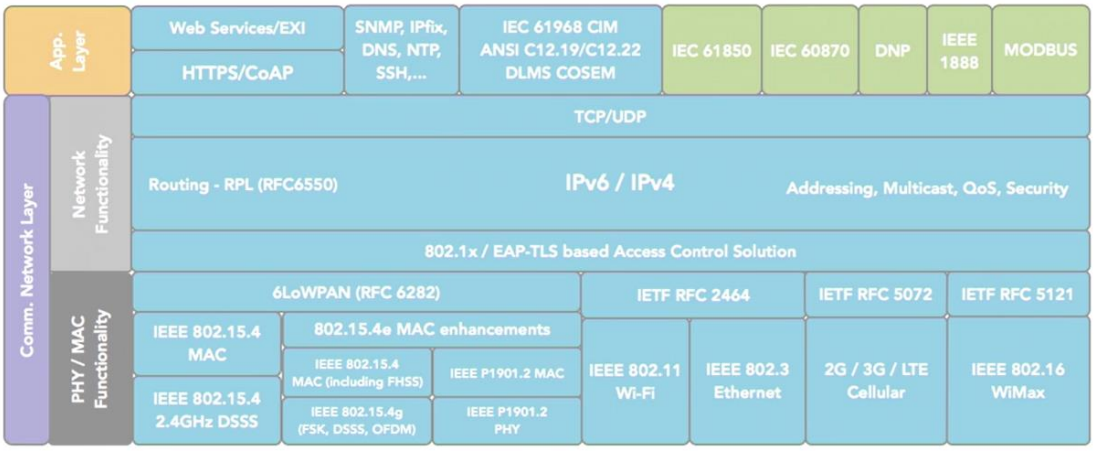
Compliance Class	Security Objective		
	Integrity	Availability	Confidentiality
Class 0	Basic	Basic	Basic
Class 1	Medium	Medium	Basic
Class 2	Medium	High	Medium
Class 3	Medium	High	High
Class 4	High	High	High

Compliance Framework

Compliance Checklist			
1	Business security processes	7	Web user interface
2	Device hardware and physical security	8	Mobile application
3	Device software and OS	9	Privacy
4	Device wired and wireless interfaces	10	Cloud and network elements
5	Authentication and authorization	11	Secure supply chain and production
6	Encryption and key management	12	Configuration

IoTSF Compliant

Open Standards Reference Model



0:10 / 5:04 1.5x

Other Physical Layer Protocols

- ZigBee, Sigfox, WirelessHART, and DigiMesh
- LoRa
- Narrowband IoT (NB-IoT) in trials

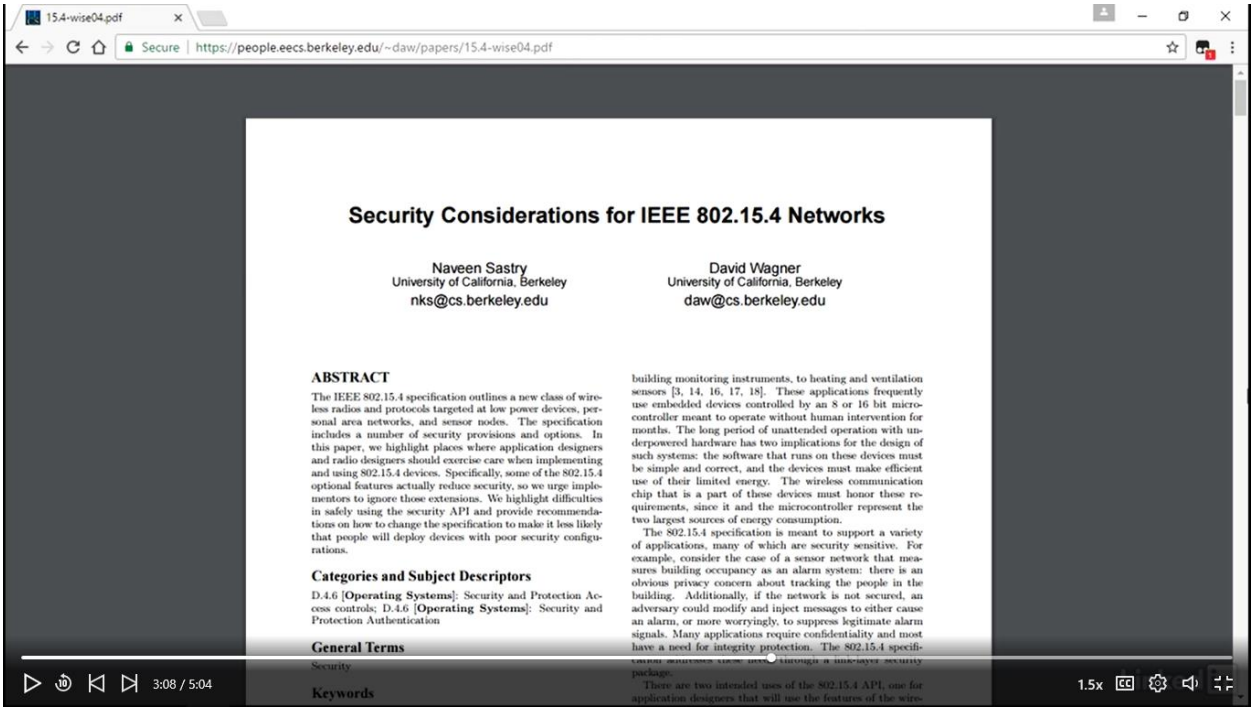
1:00 / 5:04 1.5x

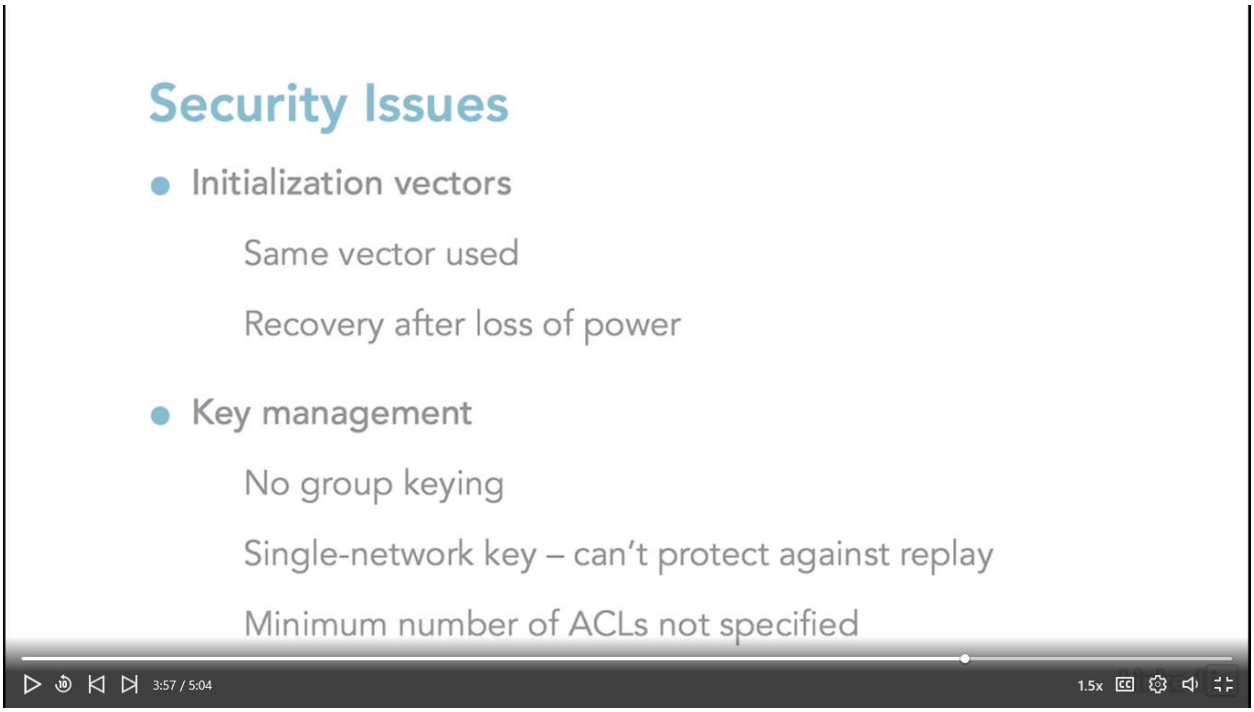
IEEE 802.15.4

- Physical layer and media access control for LR-WPAN
- Low cost and low speed
- ~10 meters
- ZigBee and 6LoWPAN

Cryptographic Modes

Mode	Description
No security	-
AES-CBC-MAC-32	Data is not encrypted; uses a 32-bit integrity code.
AES-CBC-MAC-64	Data is not encrypted; uses a 64-bit integrity code.
AES-CBC-MAC-128	Data is not encrypted; uses a 128-bit integrity code.
AES-CTR	Data is encrypted; uses no integrity code.
AES-CCM-32	Data is encrypted; uses a 32-bit integrity code.
AES-CCM-64	Data is encrypted; uses a 64-bit integrity code.
AES-CCM-128	Data is encrypted; uses a 128-bit integrity code.


15.4-wise04.pdf
Secure | https://people.eecs.berkeley.edu/~daw/papers/15.4-wise04.pdf
Security Considerations for IEEE 802.15.4 Networks
Naveen Sastry
University of California, Berkeley
nks@cs.berkeley.edu
David Wagner
University of California, Berkeley
daw@cs.berkeley.edu
ABSTRACT
The IEEE 802.15.4 specification outlines a new class of wireless radios and protocols targeted at low power devices, personal area networks, and sensor nodes. The specification includes a number of security provisions and options. In this paper, we highlight places where application designers and radio designers should exercise care when implementing and using 802.15.4 devices. Specifically, some of the 802.15.4 optional features actually reduce security, so we urge implementors to ignore those extensions. We highlight difficulties in safely using the security API and provide recommendations on how to change the specification to make it less likely that people will deploy devices with poor security configurations.
Categories and Subject Descriptors
D.4.6 [Operating Systems]: Security and Protection Access controls; D.4.6 [Operating Systems]: Security and Protection Authentication
General Terms
Security
Keywords
building monitoring instruments, to heating and ventilation sensors [3, 14, 16, 17, 18]. These applications frequently use embedded devices controlled by an 8 or 16 bit microcontroller meant to operate without human intervention for months. The long period of unattended operation with underpowered hardware has two implications for the design of such systems: the software that runs on these devices must be simple and correct, and the devices must make efficient use of their limited energy. The wireless communication chip that is a part of these devices must honor these requirements, since it and the microcontroller represent the two largest sources of energy consumption.
The 802.15.4 specification is meant to support a variety of applications, many of which are security sensitive. For example, consider the case of a sensor network that measures building occupancy as an alarm system: there is an obvious privacy concern about tracking the people in the building. Additionally, if the network is not secured, an adversary could modify and inject messages to either cause an alarm, or more worryingly, to suppress legitimate alarm signals. Many applications require confidentiality and most have a need for integrity protection. The 802.15.4 specifi-
package.
There are two intended uses of the 802.15.4 API, one for application designers that will use the features of the wire-
3:08 / 5:04
1.5x


Security Issues
Initialization vectors
Same vector used
Recovery after loss of power
Key management
No group keying
Single-network key – can't protect against replay
Minimum number of ACLs not specified
3:57 / 5:04
1.5x

Security Issues

- Integrity

  AES Counter mode messages are vulnerable to modification.

  AES Counter mode is vulnerable to denial of service.

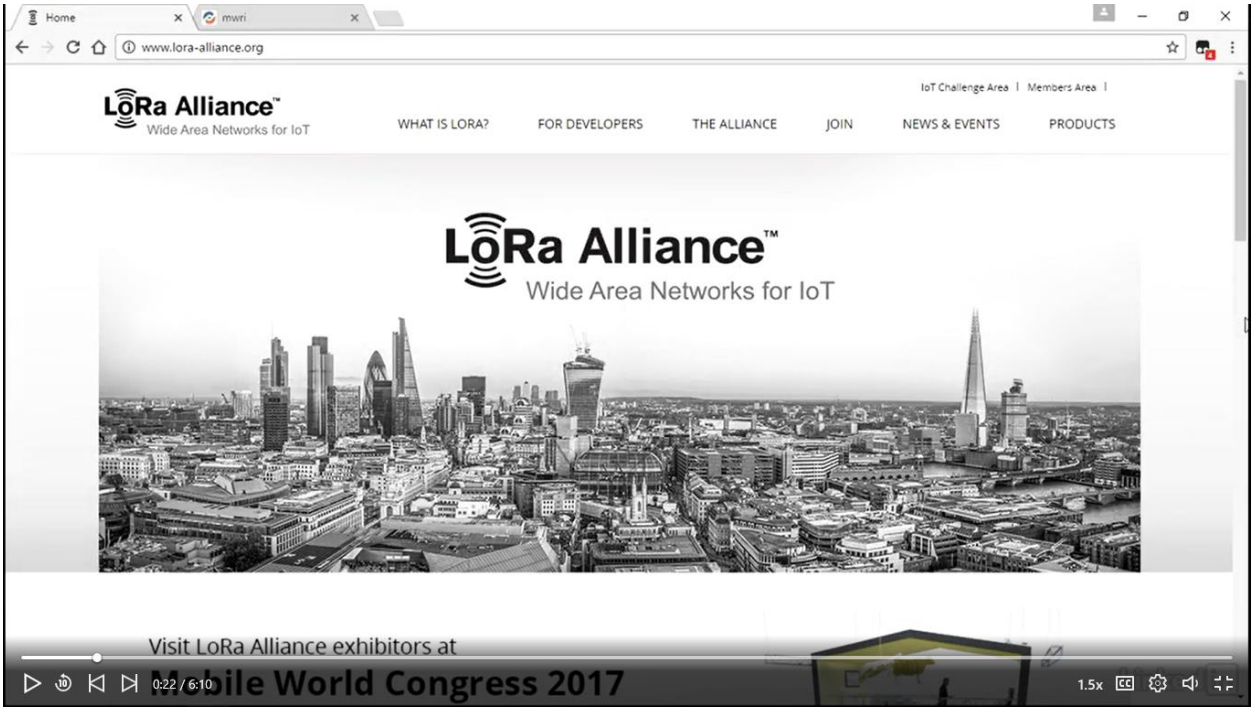
  There is no integrity of acknowledgment packets.

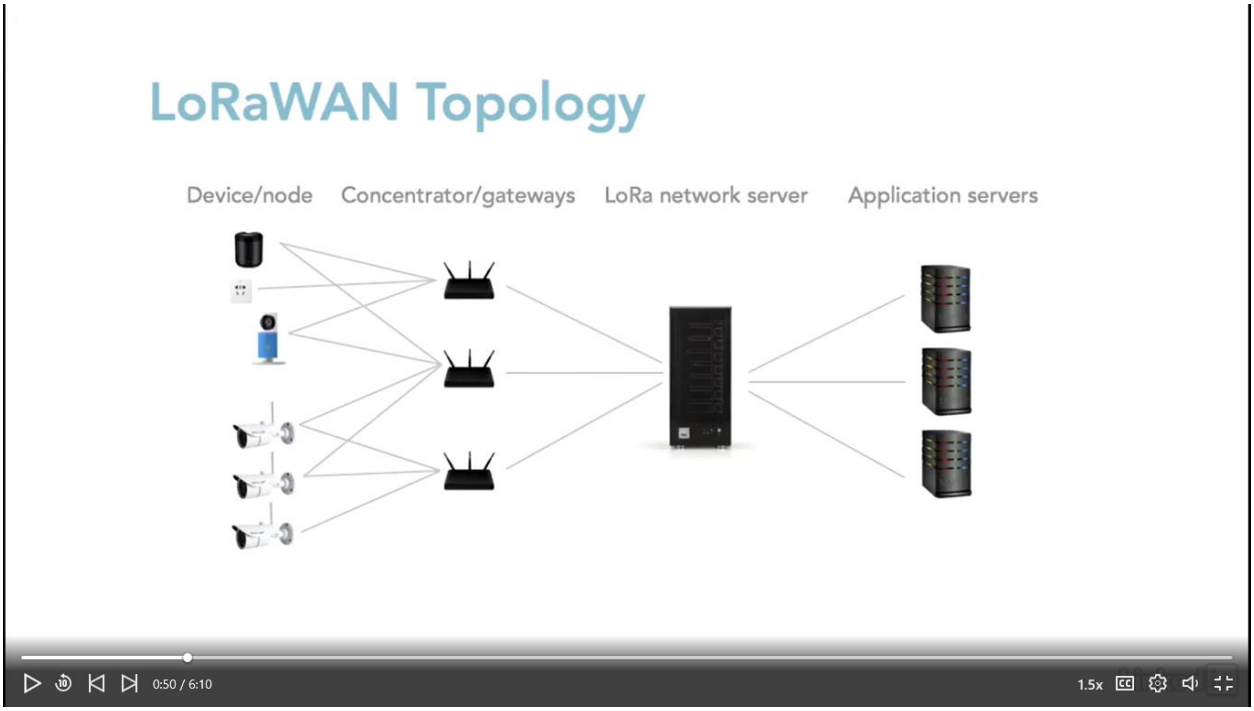
4:39 / 5:04 1.5x

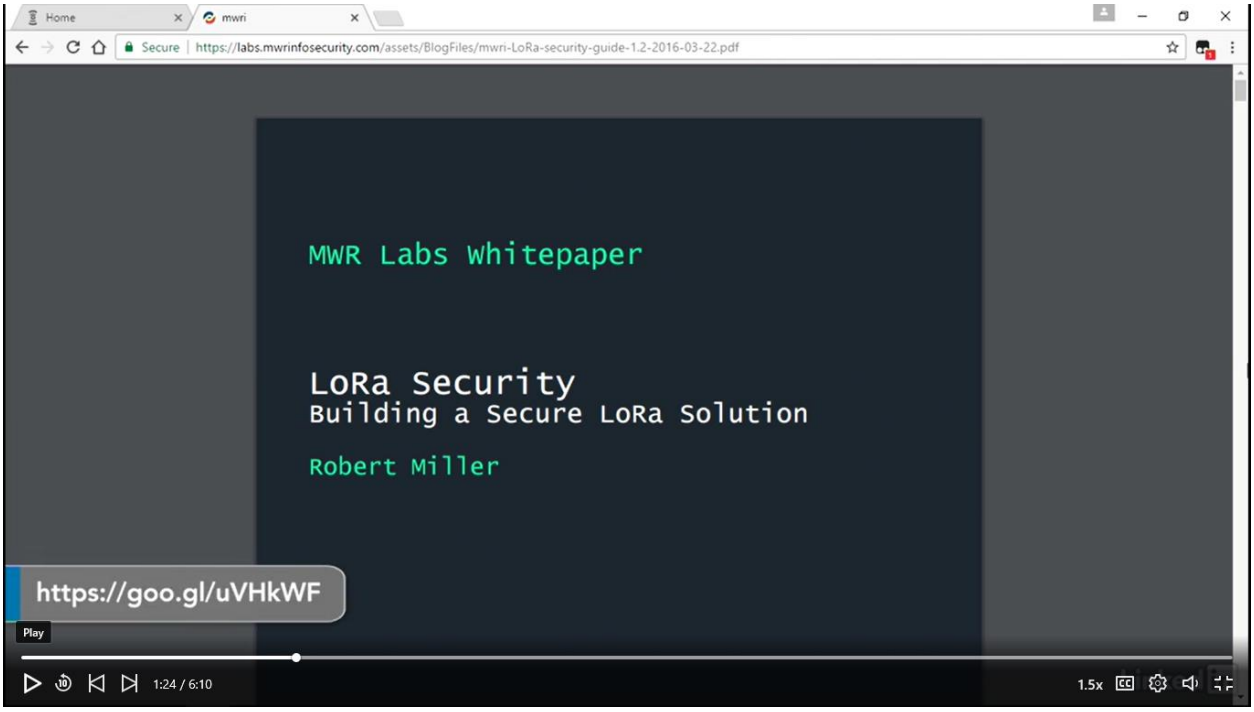
IEEE 802.15.4

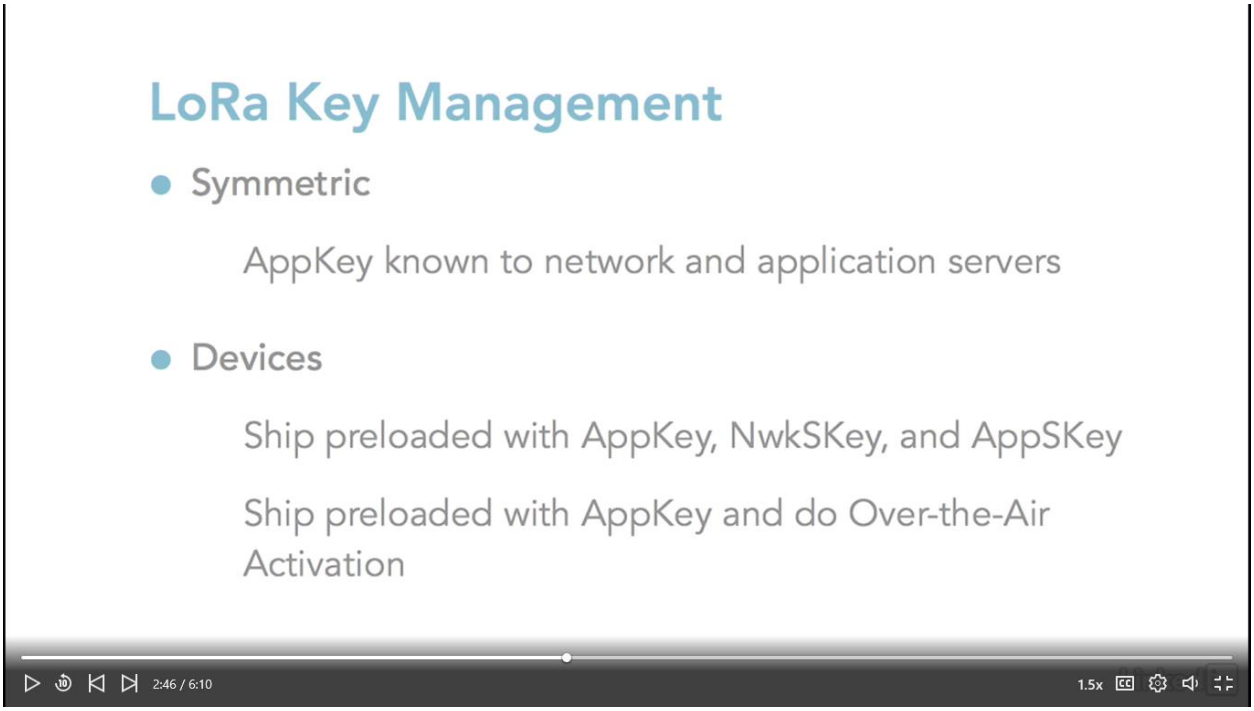
4:49 / linkedin.com switched to full screen (Esc to exit). Okay Exit now 1.5x


LoRa®
Internet of Things
0:04 / 6:10
1.5x


Home
mwri
www.lora-alliance.org
LoRa Alliance™
Wide Area Networks for IoT
IoT Challenge Area | Members Area |
WHAT IS LORA?
FOR DEVELOPERS
THE ALLIANCE
JOIN
NEWS & EVENTS
PRODUCTS
LoRa Alliance™
Wide Area Networks for IoT
Visit LoRa Alliance exhibitors at
Mobile World Congress 2017
0:22 / 6:10
1.5x


LoRaWAN Topology
Device/node
Concentrator/gateways
LoRa network server
Application servers
0:50 / 6:10
1.5x


Home
mwri
Secure
https://labs.mwrinfosecurity.com/assets/BlogFiles/mwri-LoRa-security-guide-1.2-2016-03-22.pdf
MWR Labs Whitepaper
LoRa Security
Building a Secure LoRa Solution
Robert Miller
https://goo.gl/uVHkWF
Play
1:24 / 6:10
1.5x


LoRa Key Management
Symmetric
AppKey known to network and application servers
Devices
Ship preloaded with AppKey, NwkSKey, and AppSKey
Ship preloaded with AppKey and do Over-the-Air Activation
2:46 / 6:10
1.5x

LoRa Threats

- Testing design and implementation
- FIPS 140-2 accreditation for level 3 and level 4 devices
- Unique AppKeys
- Protection of network server key stores
- Random AppKey

LoRa Threats

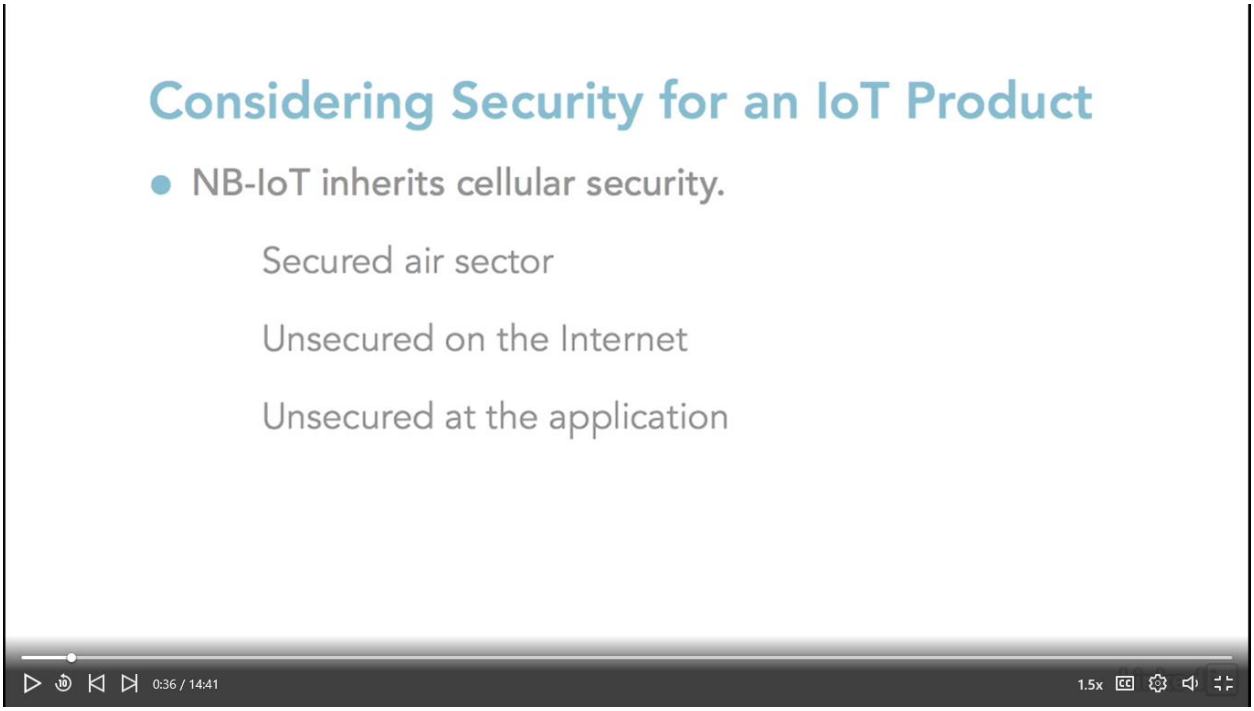
- Testing design and implementation
- FIPS 140-2 accreditation for level 3 and level 4 devices
- Unique AppKeys
- Protection of network server key stores
- Random AppKey

LoRa Threats

- Data validation
- Hardening

Considering Security for an IoT Product

- Internet is security agnostic.
- Wi-Fi may or may not be secure.
- IEEE 802.15.4 security is optional.


Considering Security for an IoT Product
NB-IoT inherits cellular security.
Secured air sector
Unsecured on the Internet
Unsecured at the application
0:36 / 14:41
1.5x


Elements of Product Security
Protect data
Protect activities
Secure network interfaces
Secure communications
Additional security relevant to use case
1:05 / 14:41
1.5x

Elements of Product Security

- Secured against inadvertent use cases
- Checkmark requirements

Secure Design Process

- Generic controls checklist of limited use
- Establish use cases
- Consider threats and opportunities
- Assess risks to the product's use
- Select controls to mitigate risk
- Implement using design patterns

Example Design

Unpaired → Paired Learning → Paired Operating

2:52 / 14:41 1.5x

Unpaired Mode Design Decisions

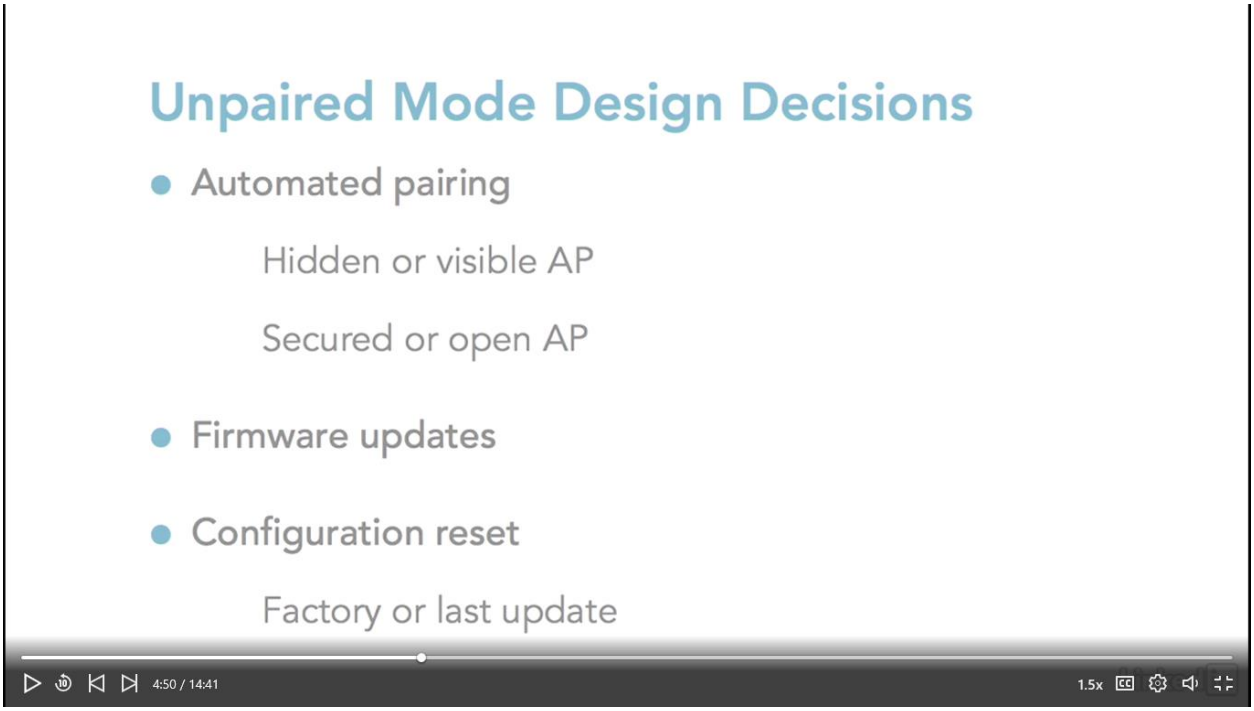
- Connect simply and securely
- Communicate to establish connectivity

  Wireless AP

- Pairing to the local network

  Limited or full operation

3:46 / 14:41 1.5x

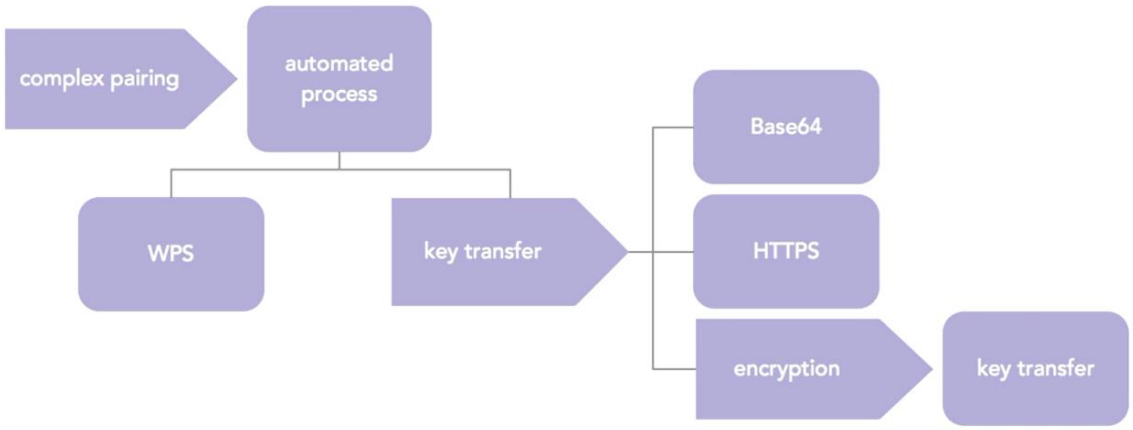

Unpaired Mode Design Decisions
Automated pairing
Hidden or visible AP
Secured or open AP
Firmware updates
Configuration reset
Factory or last update
4:50 / 14:41
1.5x

Unpaired Mode Design Decisions

- Call home
- DHCP and DNS ports

5:20 / 14:41 1.5x

Threat Risk Assessment



8:00 / 14:41 1.5x

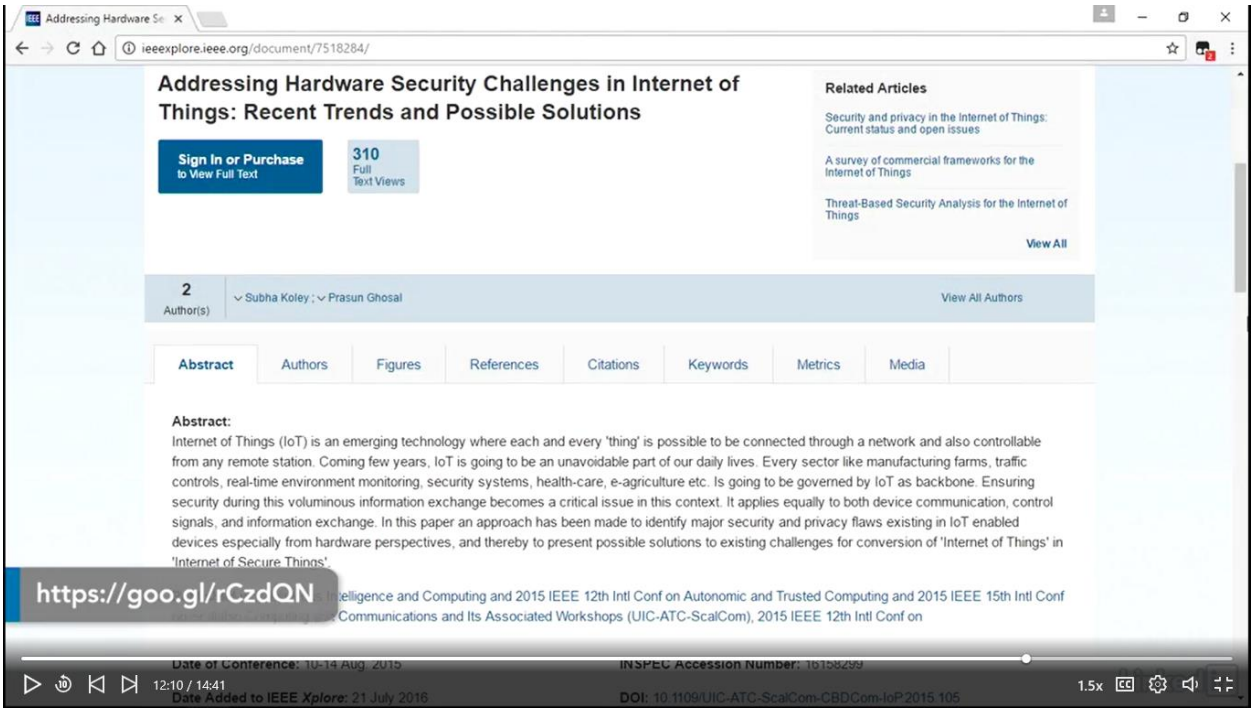

Threat Risk Assessment
malicious setup
unauthorized access
malicious misuse
back doors
design pattern
10:06 / 14:41
1.5x


Hardware Security Benefits
Firmware crypto functions
Hardware trusted root certificate
10:33 / 14:41
1.5x

Hardware Threats

- Hardware ports
- Anti-tamper
- Reflashing firmware
  - Code lock bit
  - Secure firmware image
- Random number generators

11:54 / 14:41 1.5x



IoT Security Foundation Controls

Does the data need to be private?	
Designed-in security	Yes
Protection of the complete attack surface	Device
Explicitly identify private data	-
Sensitive data review	-
Anonymize where possible	-
Manage encryption keys securely	Yes

IoT Security Foundation Controls

Does the data need to be trusted?	
Software integrity	Yes
Hardware root of trust	Yes
Data authentication and integrity	Yes
Malfunctioning devices revoked	-
Isolated data	-
Testing and calibration	Yes
Trusted and verified metadata	-
Reuse	Yes

IoT Security Foundation Controls

Is the safe and timely arrival of data important?	
Accurate timestamps	-
Integrity is designed-in	-
Availability management	-
Safety and timeliness	-
Identified dependencies	-
Secure device identifier	-
Explicit functionality	-

IoT Security Foundation Controls

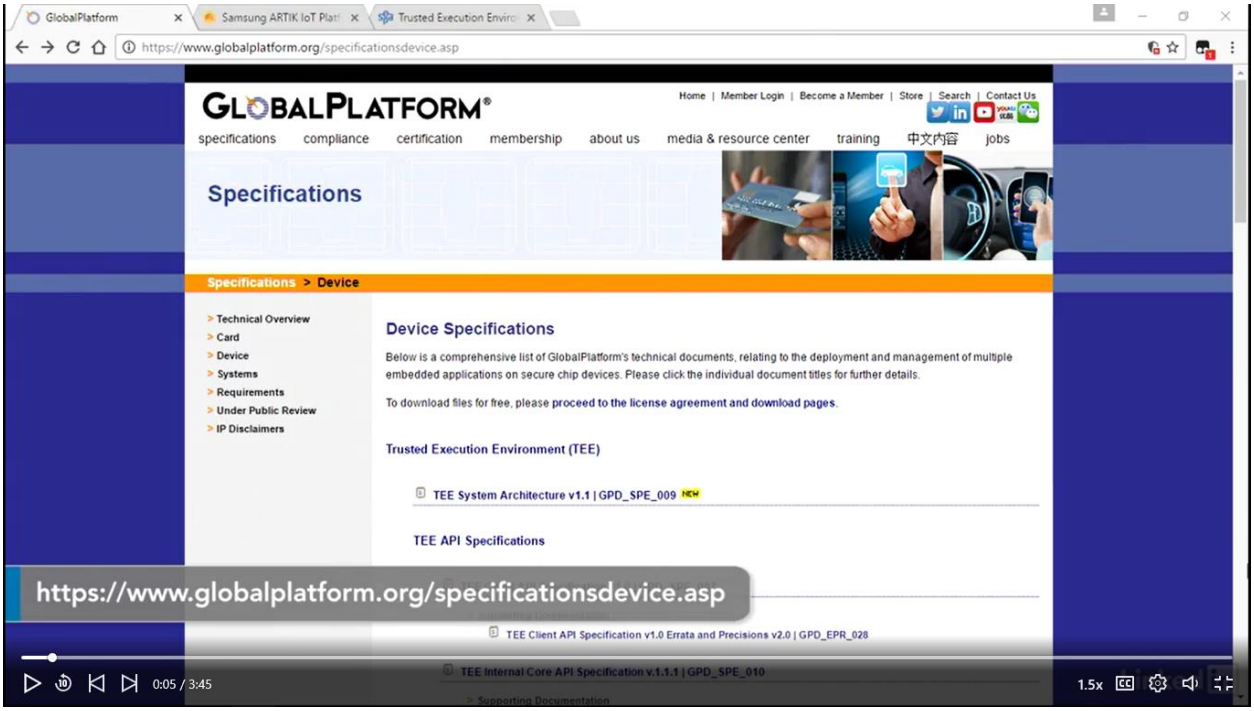
Restrict access to or control of the device?	
Designed-in defense against hacking	Yes
Secure and penetration tested code	Yes
Authenticated channel for service management	Yes

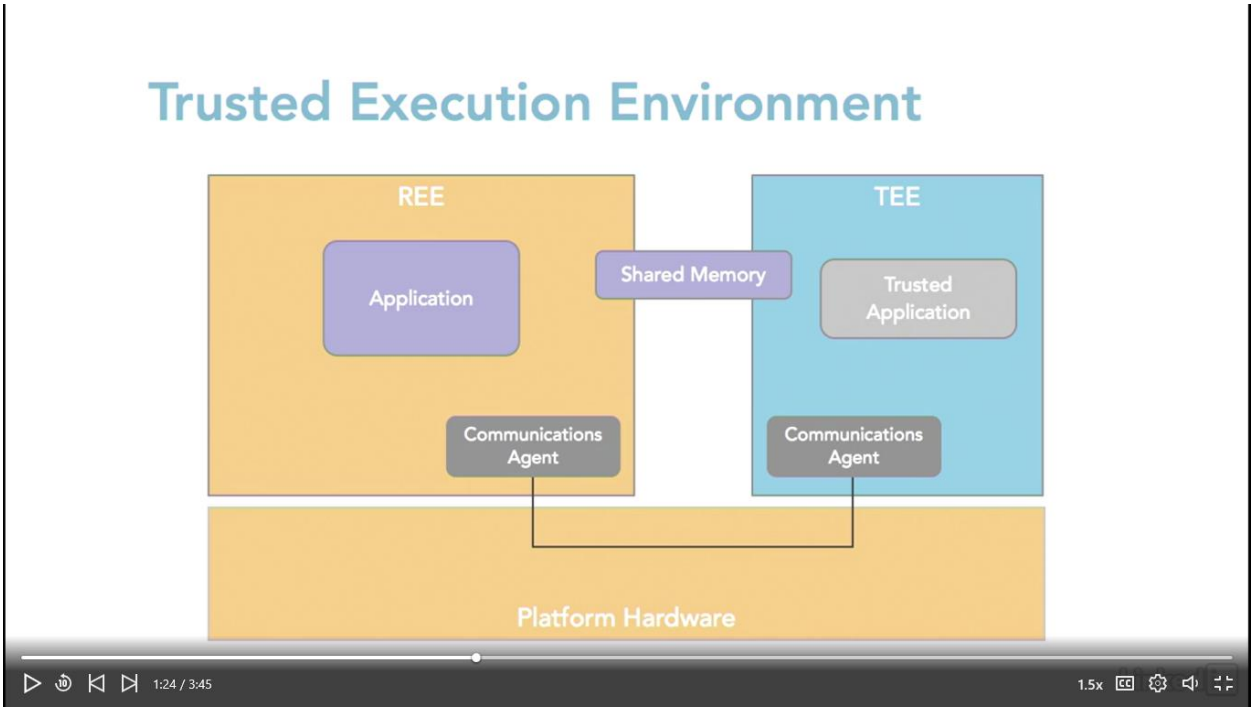
IoT Security Foundation Controls

Update software on the device?	
Best security practices	Yes
Authenticated source for updates and patches	Yes
Show device patching status	Yes

IoT Security Foundation Controls

Does the data need to be audited?	
Managed access to IoT data	-
Policy controls to disable unwanted features	-


GlobalPlatform
Samsung ARTIK IoT Platf
Trusted Execution Enviro
https://www.globalplatform.org/specificationsdevice.asp
GLOBALPLATFORM®
Home | Member Login | Become a Member | Store | Search | Contact Us
specifications compliance certification membership about us media & resource center training 中文内容 jobs
Specifications
Specifications > Device
> Technical Overview
> Card
> Device
> Systems
> Requirements
> Under Public Review
> IP Disclaimers
Device Specifications
Below is a comprehensive list of GlobalPlatform's technical documents, relating to the deployment and management of multiple embedded applications on secure chip devices. Please click the individual document titles for further details.
To download files for free, please proceed to the license agreement and download pages.
Trusted Execution Environment (TEE)
TEE System Architecture v1.1 | GPD_SPE_009 NEW
TEE API Specifications
https://www.globalplatform.org/specificationsdevice.asp
TEE Client API Specification v1.0 Errata and Precisions v2.0 | GPD_EPR_028
TEE Internal Core API Specification v.1.1.1 | GPD_SPE_010
Supporting Documentation
0:05 / 3:45
1.5x

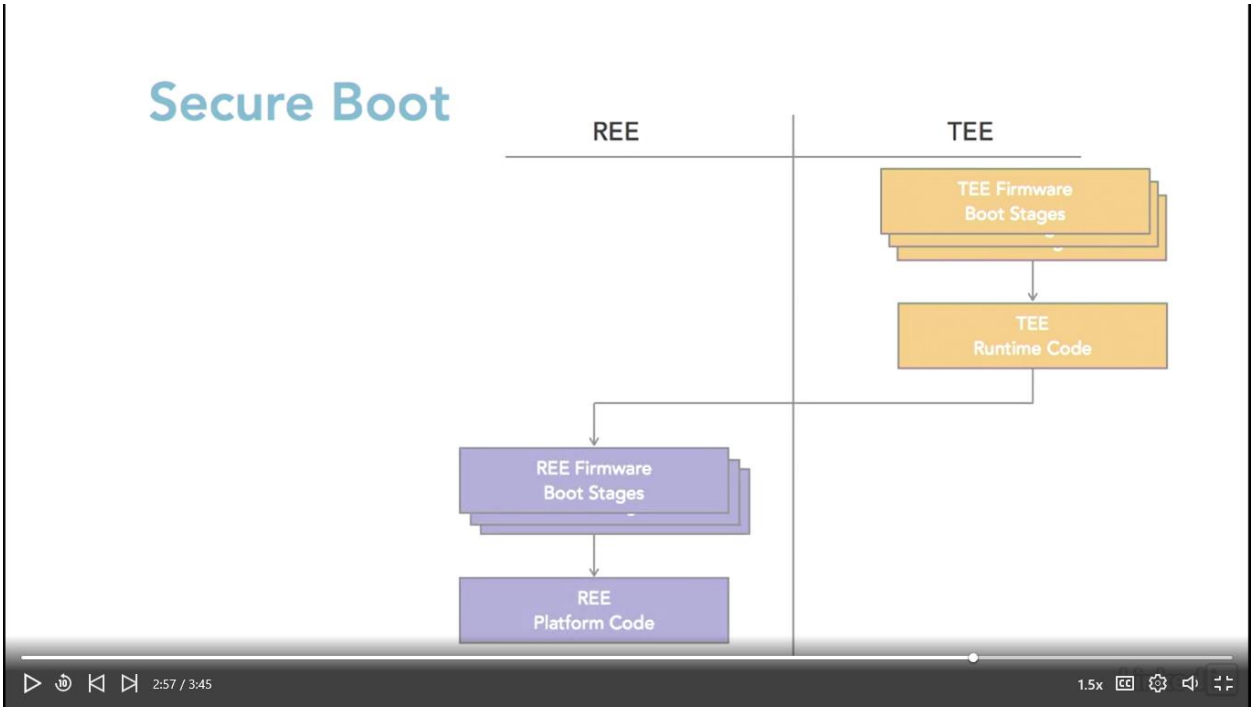

Trusted Execution Environment
REE
Application
Communications Agent
Shared Memory
TEE
Trusted Application
Communications Agent
Platform Hardware
1:24 / 3:45
1.5x

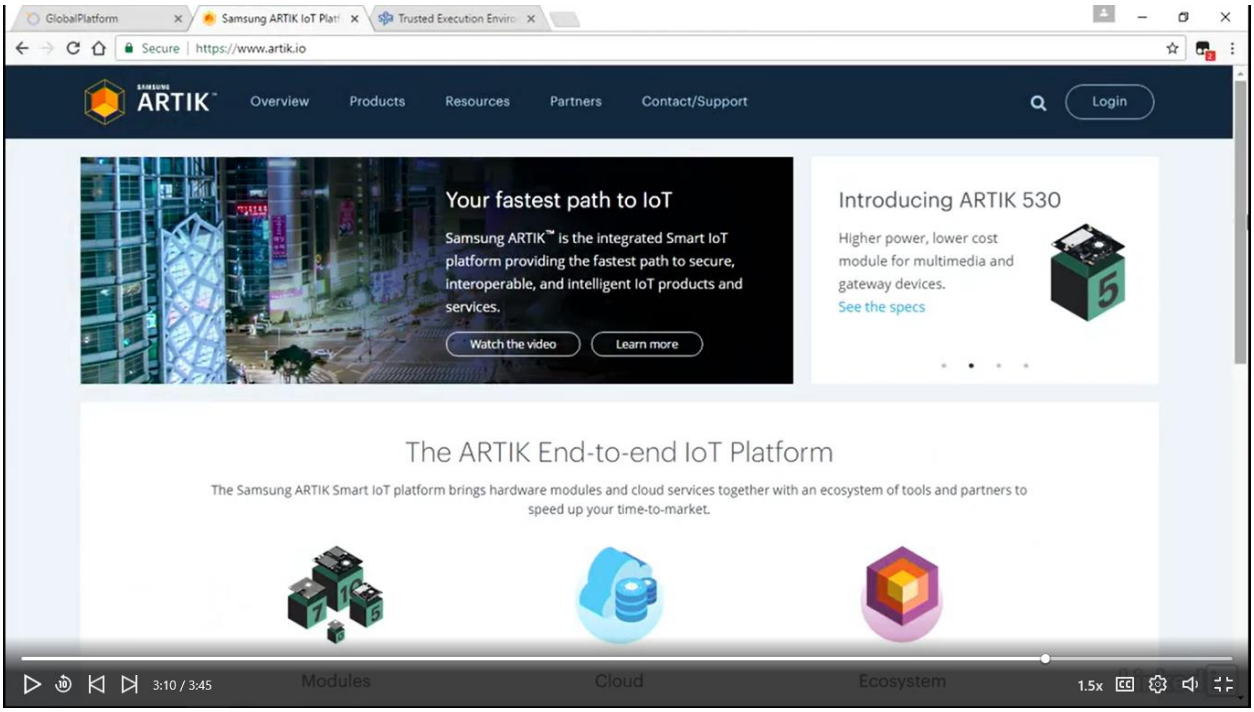
TEE Core Internal API

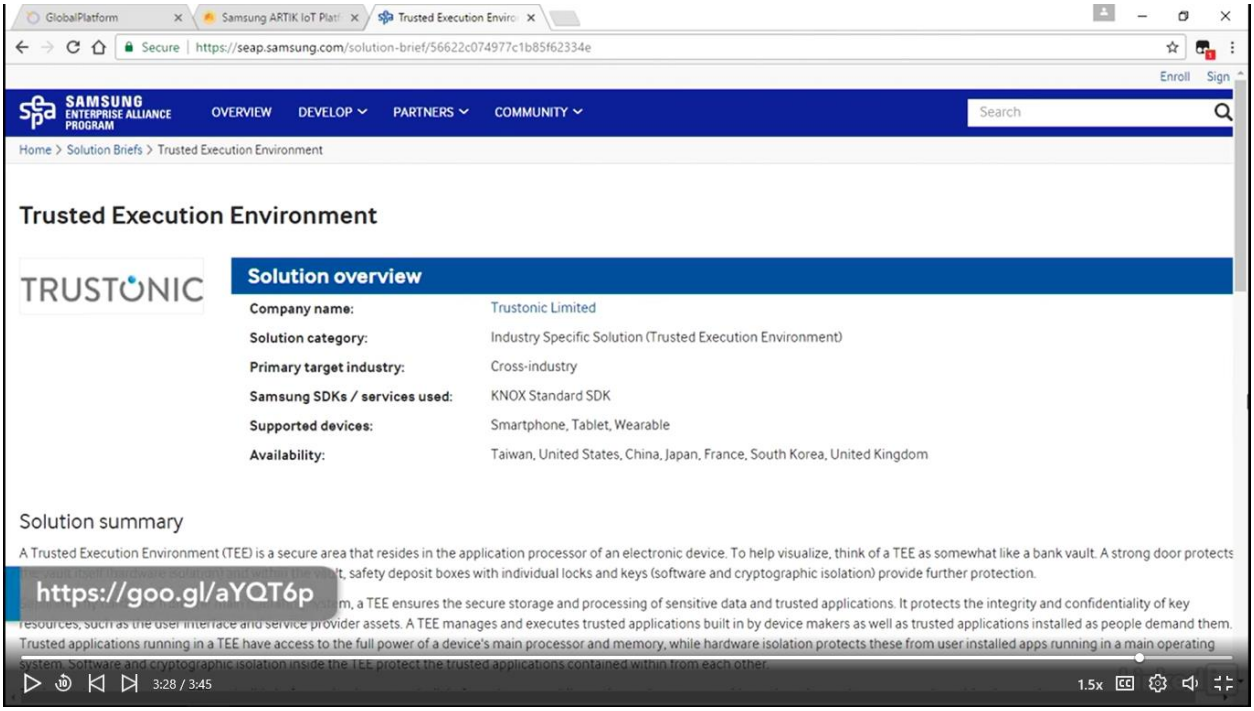
- Core functions
- Cryptography
- Maths
- Secure data stores
- Secure time

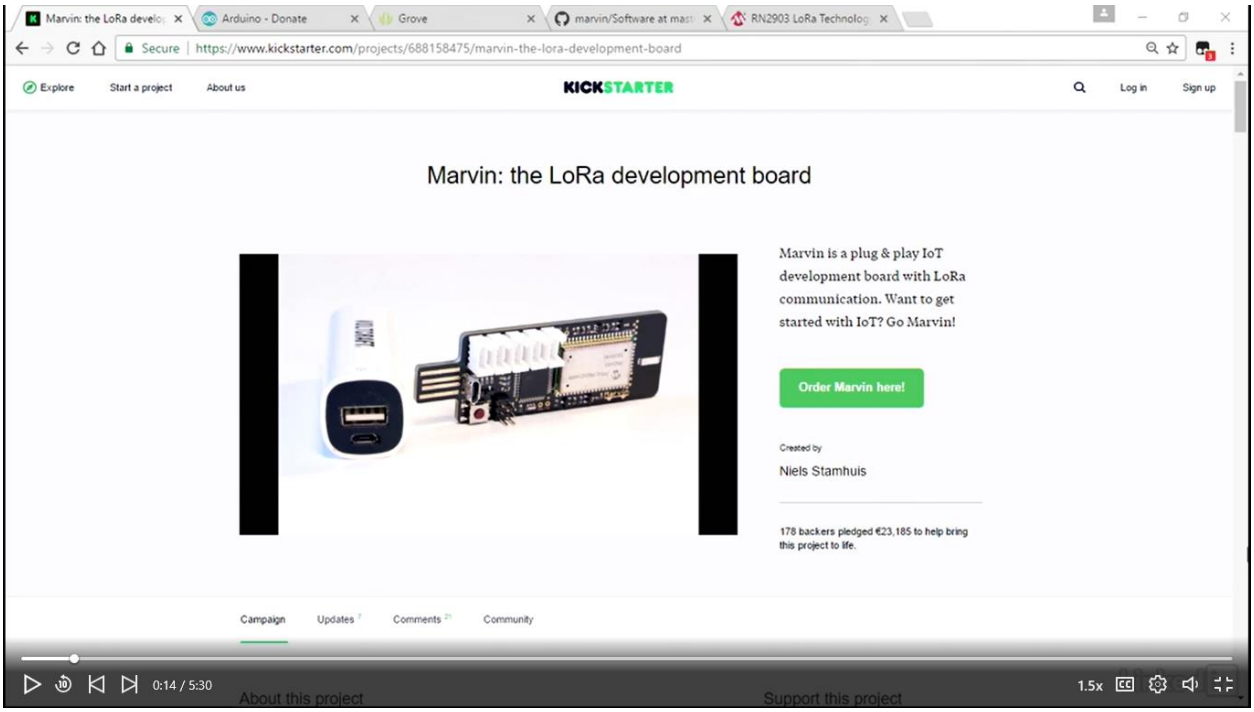
Other TEE APIs

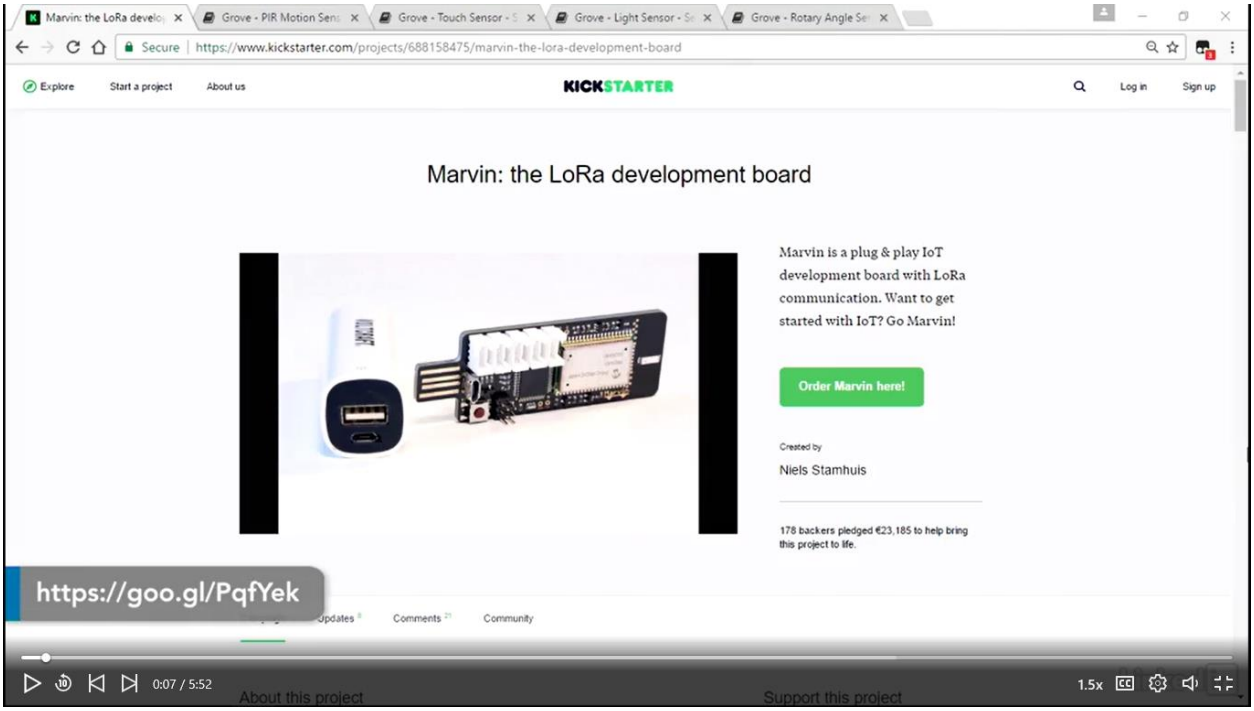
- Sockets API
- Debug API
- Secure Element API
- Trusted User Interface API

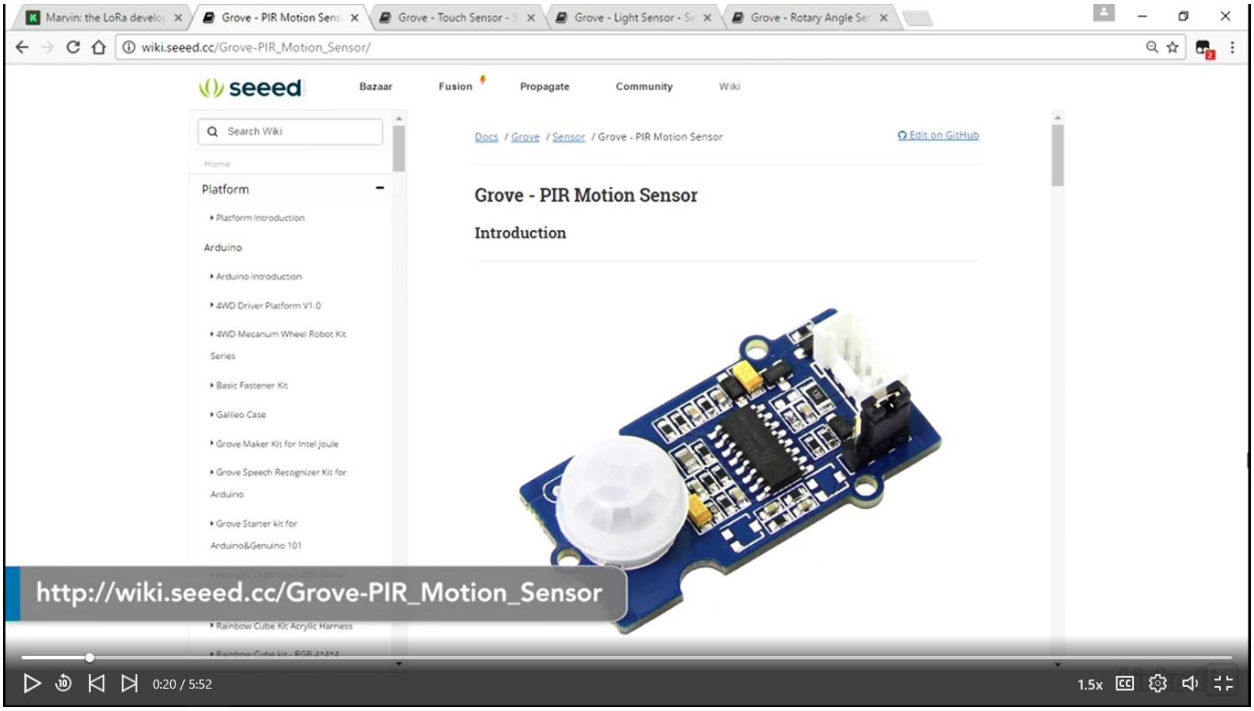

Secure Boot
REE
TEE
TEE Firmware
Boot Stages
TEE
Runtime Code
REE Firmware
Boot Stages
REE
Platform Code
2:57 / 3:45
1.5x

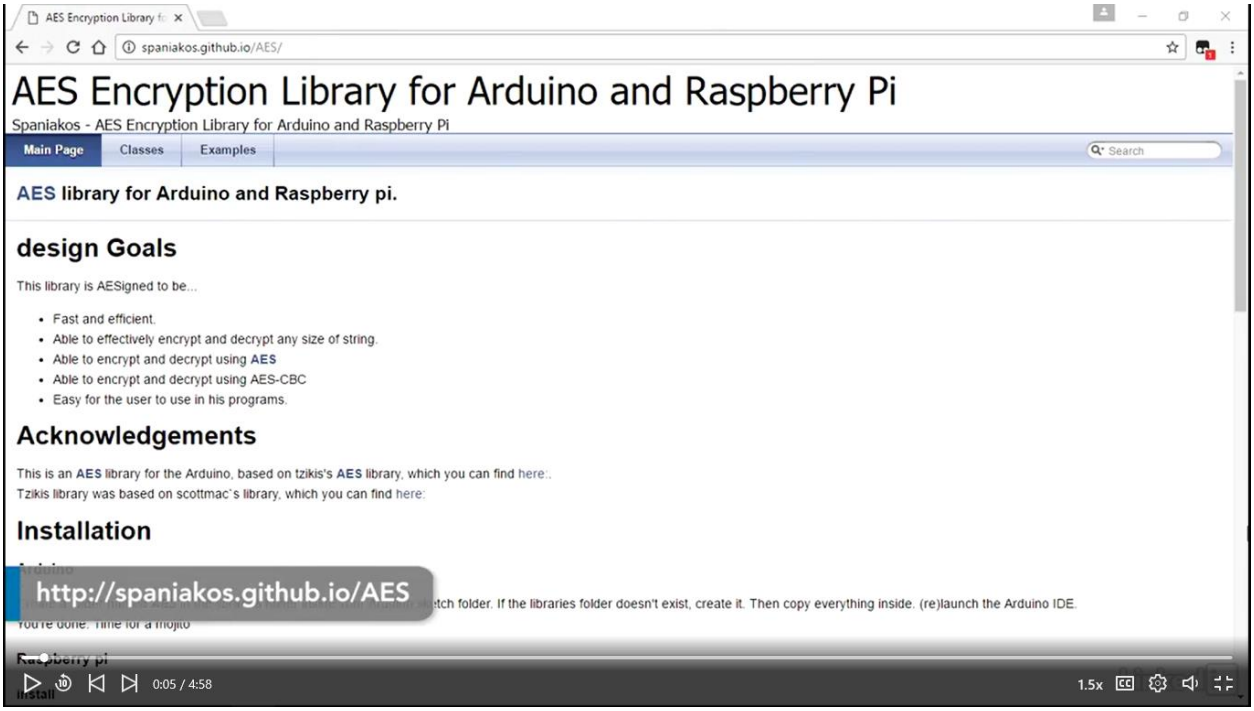

GlobalPlatform
Samsung ARTIK IoT Platf
Trusted Execution Enviro
Secure
https://www.artik.io
ARTIK
Overview
Products
Resources
Partners
Contact/Support
Login
Your fastest path to IoT
Samsung ARTIK™ is the integrated Smart IoT platform providing the fastest path to secure, interoperable, and intelligent IoT products and services.
Watch the video
Learn more
Introducing ARTIK 530
Higher power, lower cost module for multimedia and gateway devices.
See the specs
The ARTIK End-to-end IoT Platform
The Samsung ARTIK Smart IoT platform brings hardware modules and cloud services together with an ecosystem of tools and partners to speed up your time-to-market.
Modules
Cloud
Ecosystem
3:10 / 3:45
1.5x

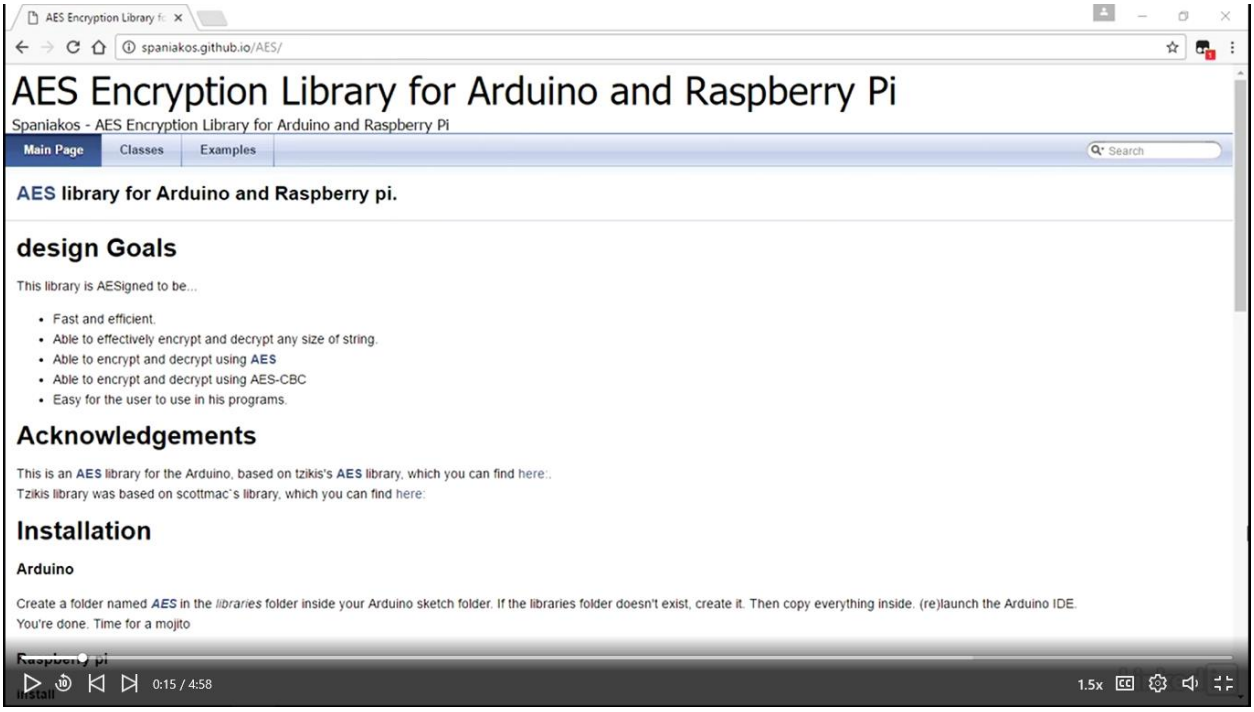

GlobalPlatform
Samsung ARTIK IoT Platf
Trusted Execution Enviro
Secure | https://seap.samsung.com/solution-brief/56622c074977c1b85f62334e
Enroll Sign
SAMSUNG ENTERPRISE ALLIANCE PROGRAM
OVERVIEW DEVELOP PARTNERS COMMUNITY
Search
Home > Solution Briefs > Trusted Execution Environment
Trusted Execution Environment
TRUSTONIC
Solution overview
Company name: Trustonic Limited
Solution category: Industry Specific Solution (Trusted Execution Environment)
Primary target industry: Cross-industry
Samsung SDKs / services used: KNOX Standard SDK
Supported devices: Smartphone, Tablet, Wearable
Availability: Taiwan, United States, China, Japan, France, South Korea, United Kingdom
Solution summary
A Trusted Execution Environment (TEE) is a secure area that resides in the application processor of an electronic device. To help visualize, think of a TEE as somewhat like a bank vault. A strong door protects
safety deposit boxes with individual locks and keys (software and cryptographic isolation) provide further protection.
https://goo.gl/aYQT6p
m, a TEE ensures the secure storage and processing of sensitive data and trusted applications. It protects the integrity and confidentiality of key
resources, such as the user interface and service provider assets. A TEE manages and executes trusted applications built in by device makers as well as trusted applications installed as people demand them.
Trusted applications running in a TEE have access to the full power of a device's main processor and memory, while hardware isolation protects these from user installed apps running in a main operating
system. Software and cryptographic isolation inside the TEE protect the trusted applications contained within from each other.
3:28 / 3:45
1.5x


Marvin: the LoRa develop
Arduino - Donate
Grove
marvin/Software at mast
RN2903 LoRa Technolog
Secure | https://www.kickstarter.com/projects/688158475/marvin-the-lora-development-board
Explore Start a project About us
KICKSTARTER
Log in Sign up
Marvin: the LoRa development board
Marvin is a plug & play IoT development board with LoRa communication. Want to get started with IoT? Go Marvin!
Order Marvin here!
Created by
Niels Stamhuis
178 backers pledged €23,185 to help bring this project to life.
Campaign Updates 7 Comments 21 Community
0:14 / 5:30
1.5x
About this project
Support this project

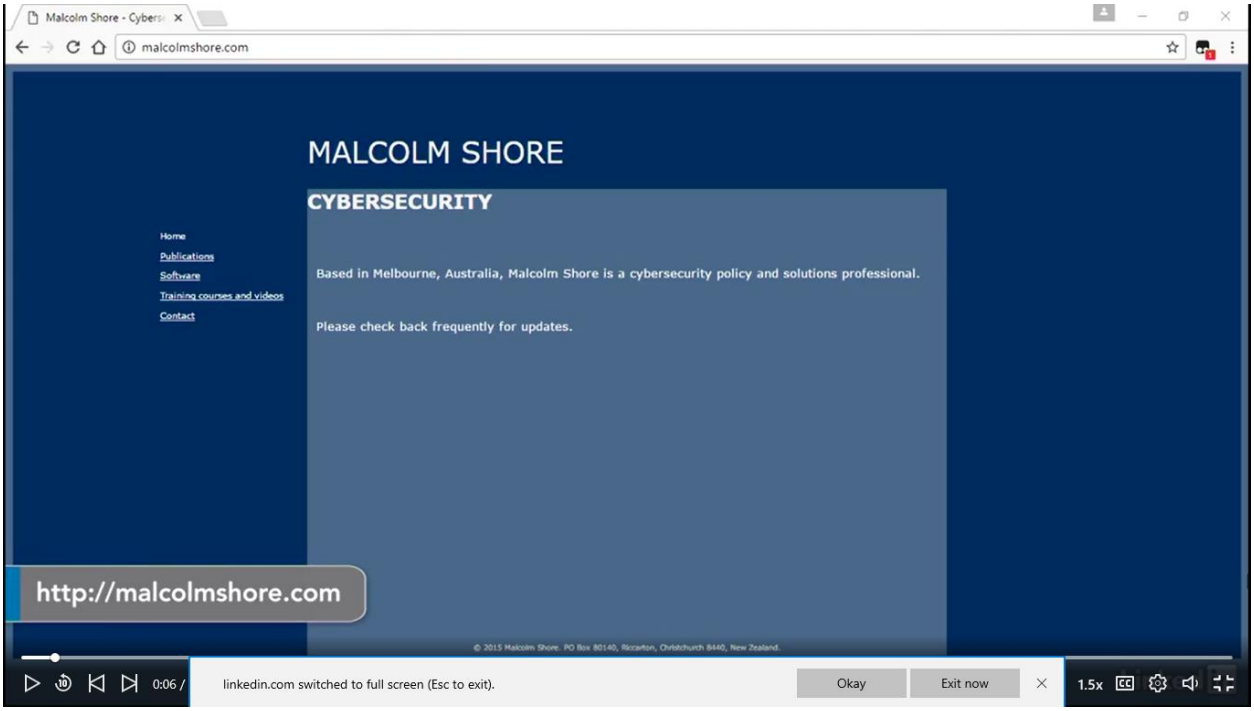

Marvin: the LoRa development board
Marvin is a plug & play IoT development board with LoRa communication. Want to get started with IoT? Go Marvin!
Order Marvin here!
Created by
Niels Stamhuis
178 backers pledged €23,185 to help bring this project to life.
https://goo.gl/PqfYek
0:07 / 5:52
1.5x

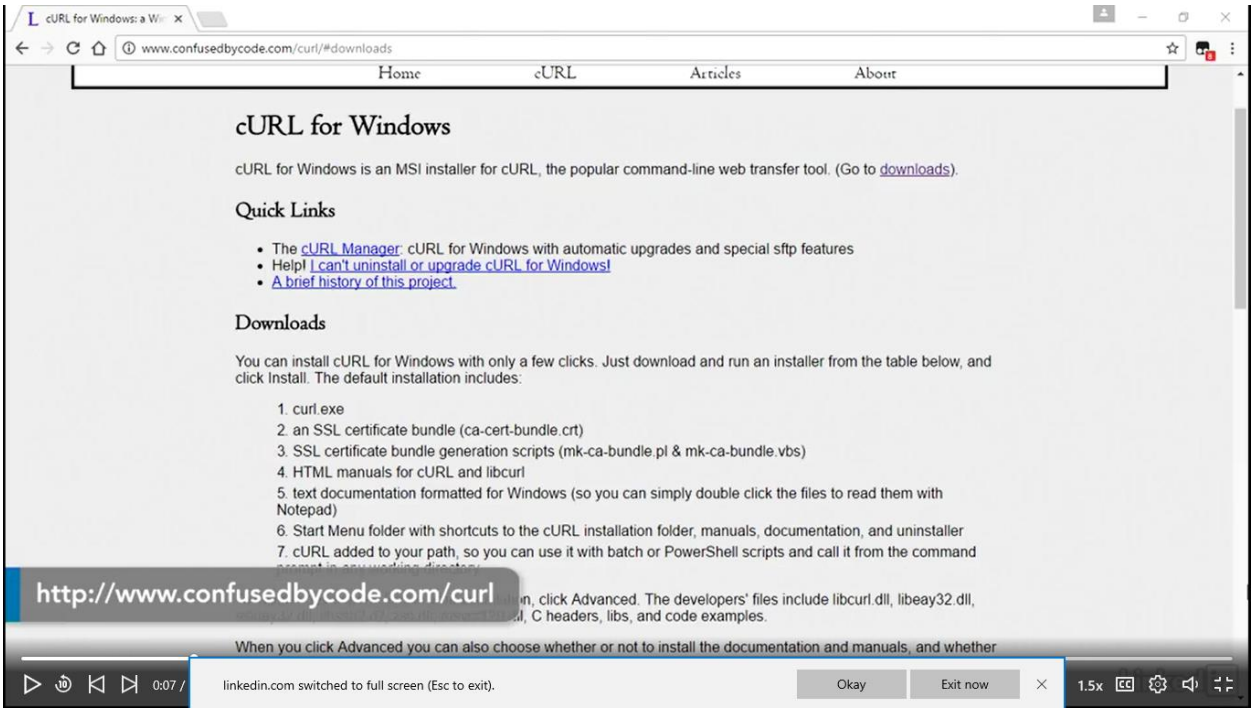

Grove - PIR Motion Sensor
Introduction
http://wiki.seeed.cc/Grove-PIR_Motion_Sensor
0:20 / 5:52
1.5x

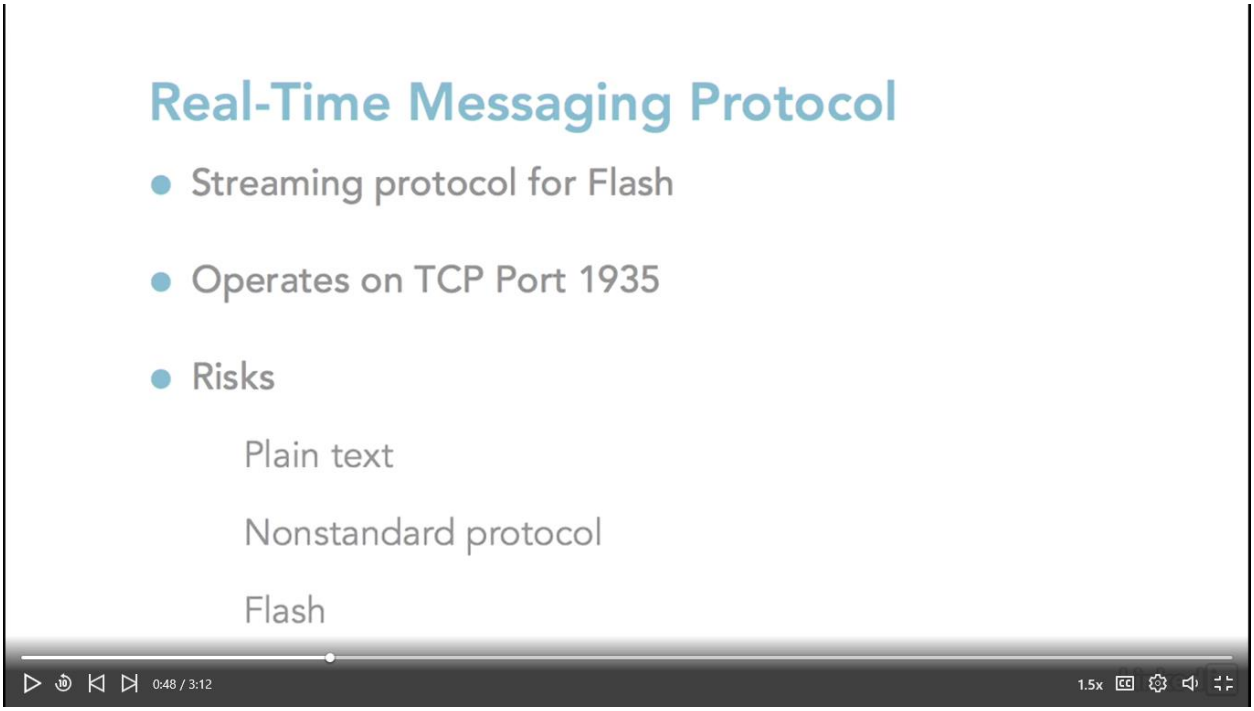

AES Encryption Library fc
spaniakos.github.io/AES/
AES Encryption Library for Arduino and Raspberry Pi
Spaniakos - AES Encryption Library for Arduino and Raspberry Pi
Main Page
Classes
Examples
Search
AES library for Arduino and Raspberry pi.
design Goals
This library is AESigned to be...
Fast and efficient.
Able to effectively encrypt and decrypt any size of string.
Able to encrypt and decrypt using AES
Able to encrypt and decrypt using AES-CBC
Easy for the user to use in his programs.
Acknowledgements
This is an AES library for the Arduino, based on tzikis's AES library, which you can find here:.
Tzikis library was based on scottmac's library, which you can find here:
Installation
http://spaniakos.github.io/AES
0:05 / 4:58
1.5x

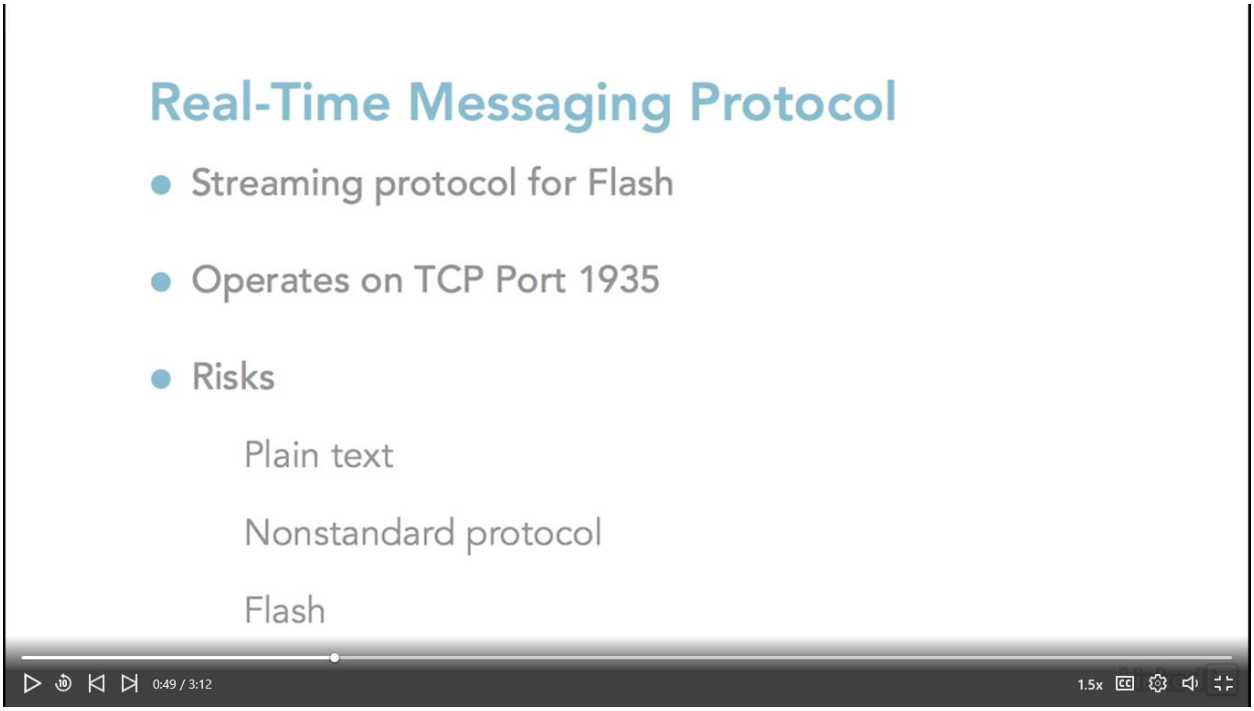

AES Encryption Library fc
spaniakos.github.io/AES/
AES Encryption Library for Arduino and Raspberry Pi
Spaniakos - AES Encryption Library for Arduino and Raspberry Pi
Main Page
Classes
Examples
Search
AES library for Arduino and Raspberry pi.
design Goals
This library is AESigned to be...
Fast and efficient.
Able to effectively encrypt and decrypt any size of string.
Able to encrypt and decrypt using AES
Able to encrypt and decrypt using AES-CBC
Easy for the user to use in his programs.
Acknowledgements
This is an AES library for the Arduino, based on tzikis's AES library, which you can find here:.
Tzikis library was based on scottmac's library, which you can find here:
Installation
Arduino
Create a folder named AES in the libraries folder inside your Arduino sketch folder. If the libraries folder doesn't exist, create it. Then copy everything inside. (re)launch the Arduino IDE.
You're done. Time for a mojito
0:15 / 4:58
1.5x

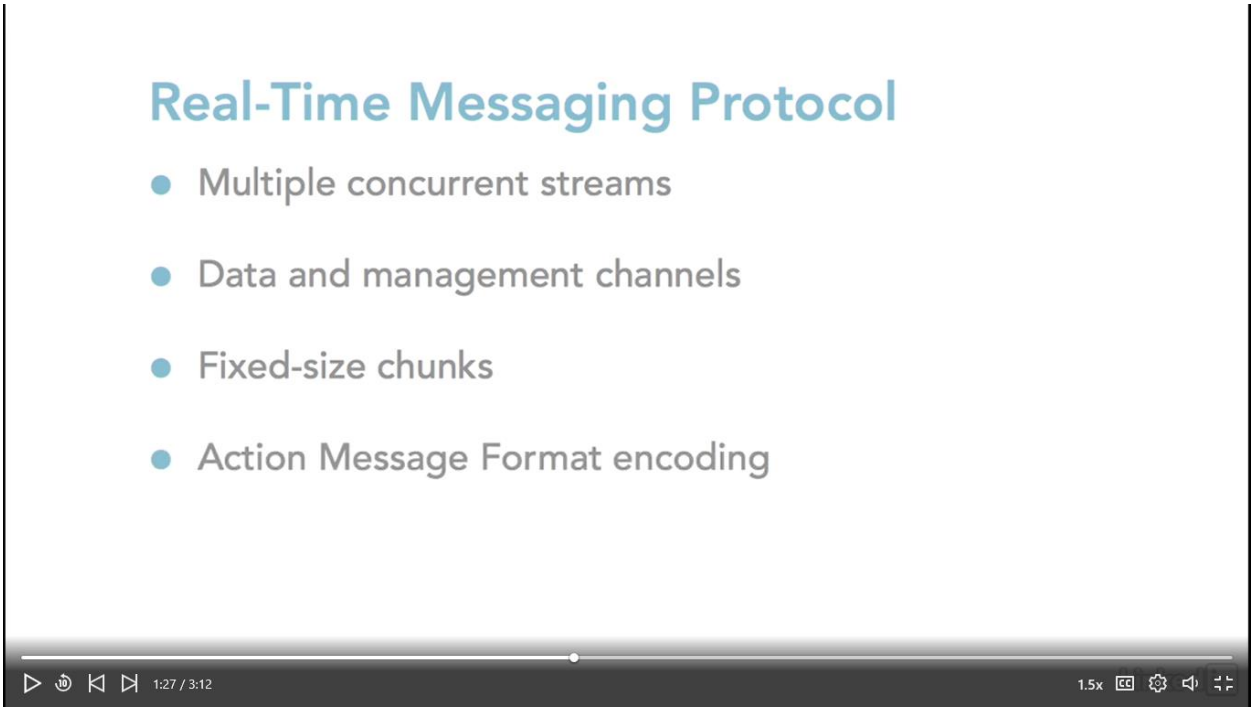
Chapter 4

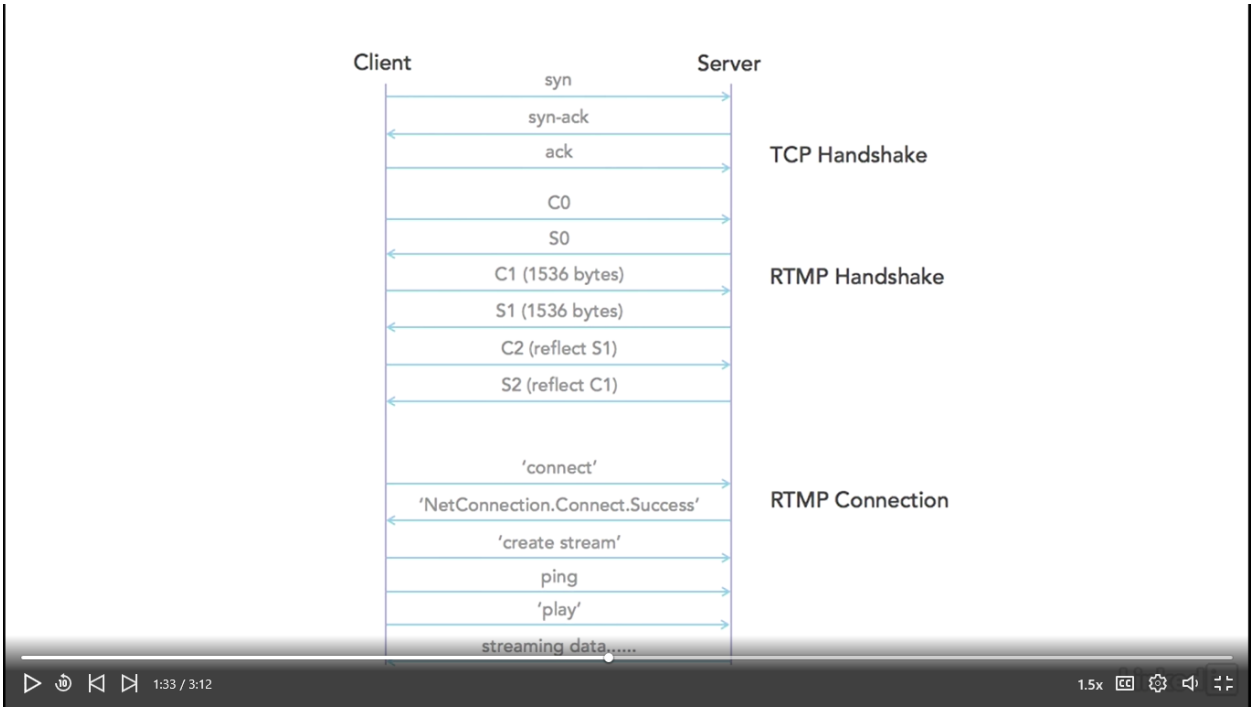

Malcolm Shore - Cyberse
malcolmshore.com
MALCOLM SHORE
CYBERSECURITY
Home
Publications
Software
Training courses and videos
Contact
Based in Melbourne, Australia, Malcolm Shore is a cybersecurity policy and solutions professional.
Please check back frequently for updates.
http://malcolmshore.com
© 2015 Malcolm Shore. PO Box 80140, Riccarton, Christchurch 8440, New Zealand.
0:06 /
linkedin.com switched to full screen (Esc to exit).
Okay
Exit now
1.5x


cURL for Windows: a Wi
www.confusedbycode.com/curl/#downloads
Home
cURL
Articles
About
cURL for Windows
cURL for Windows is an MSI installer for cURL, the popular command-line web transfer tool. (Go to downloads).
Quick Links
The cURL Manager: cURL for Windows with automatic upgrades and special sftp features
Help! I can't uninstall or upgrade cURL for Windows!
A brief history of this project
Downloads
You can install cURL for Windows with only a few clicks. Just download and run an installer from the table below, and click Install. The default installation includes:
1. curl.exe
2. an SSL certificate bundle (ca-cert-bundle.crt)
3. SSL certificate bundle generation scripts (mk-ca-bundle.pl & mk-ca-bundle.vbs)
4. HTML manuals for cURL and libcurl
5. text documentation formatted for Windows (so you can simply double click the files to read them with Notepad)
6. Start Menu folder with shortcuts to the cURL installation folder, manuals, documentation, and uninstaller
7. cURL added to your path, so you can use it with batch or PowerShell scripts and call it from the command
http://www.confusedbycode.com/curl
n, click Advanced. The developers' files include libcurl.dll, libeay32.dll,
l, C headers, libs, and code examples.
When you click Advanced you can also choose whether or not to install the documentation and manuals, and whether
0:07 /
linkedin.com switched to full screen (Esc to exit).
Okay
Exit now
1.5x


Real-Time Messaging Protocol
Streaming protocol for Flash
Operates on TCP Port 1935
Risks
Plain text
Nonstandard protocol
Flash
0:48 / 3:12
1.5x


Real-Time Messaging Protocol
Streaming protocol for Flash
Operates on TCP Port 1935
Risks
Plain text
Nonstandard protocol
Flash
0:49 / 3:12
1.5x


Real-Time Messaging Protocol
Multiple concurrent streams
Data and management channels
Fixed-size chunks
Action Message Format encoding
1:27 / 3:12
1.5x


Client
Server
syn
syn-ack
ack
TCP Handshake
C0
S0
C1 (1536 bytes)
RTMP Handshake
S1 (1536 bytes)
C2 (reflect S1)
S2 (reflect C1)
'connect'
'NetConnection.Connect.Success'
RTMP Connection
'create stream'
ping
'play'
streaming data.....
1:33 / 3:12
1.5x