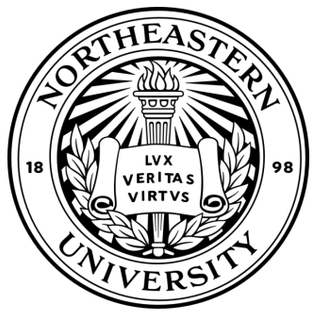
IoTLS: Understanding TLS Usage in Consumer IoT Devices

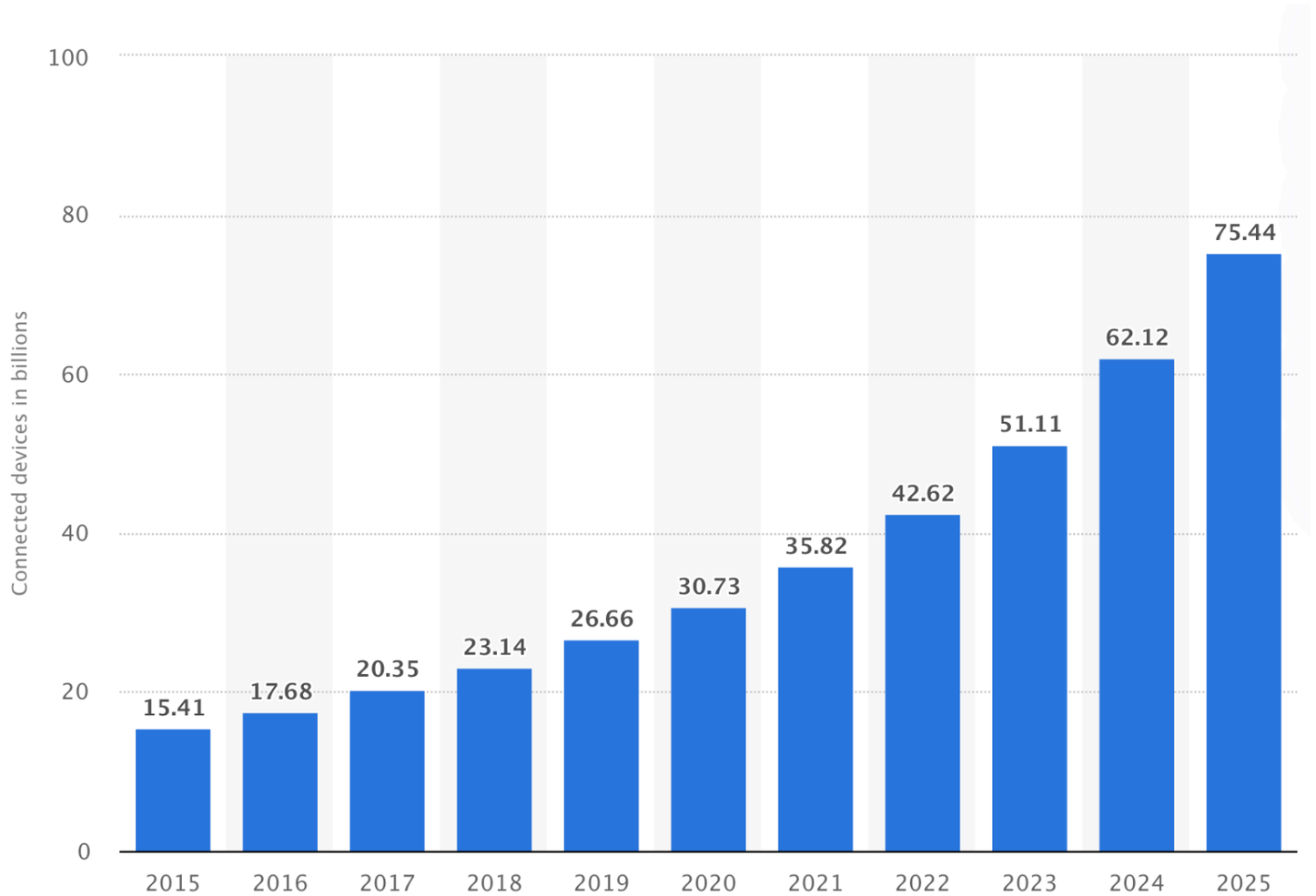
Muhammad Talha Paracha, Northeastern University
Daniel D. Dubois, Northeastern University
Narseo Vallina-Rodriguez, IMDEA Networks / ICSI / AppCensus Inc.
David Choffnes, Northeastern University



*Presented at **IETF 112 / MAPRG***
*Published at Proc. of Internet Measurement Conference (**IMC**) 2021*

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025



Projected Growth of IoT Devices
([Statista])

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025
- Invasive nature of these devices raises significant privacy implications

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025
- Invasive nature of these devices raises significant privacy implications

The Washington Post
Democracy Dies in Darkness

‘I’m in your baby’s room’: A hacker took over a baby monitor and broadcast threats, parents say

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025
- Invasive nature of these devices raises significant privacy implications

The Washington Post
Democracy Dies in Darkness

‘I’m in your baby’s room’: A hacker took over a baby monitor and broadcast threats, parents say

ars TECHNICA

Researchers hack Siri, Alexa, and Google Home by shining lasers at them

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025
- Invasive nature of these devices raises significant privacy implications

The Washington Post
Democracy Dies in Darkness

‘I’m in your baby’s room’: A hacker took over a baby monitor and broadcast threats, parents say

ars TECHNICA

Researchers hack Siri, Alexa, and Google Home by shining lasers at them

My Pacemaker Is Tracking Me From Inside My Body

The Atlantic

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025
- Invasive nature of these devices raises significant privacy implications
- Compromise in device security can lead to severe outcomes as well

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025
- Invasive nature of these devices raises significant privacy implications
- Compromise in device security can lead to severe outcomes as well

THE VERGE

Hacked webcams that helped shut down the internet last week are being recalled

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025
- Invasive nature of these devices raises significant privacy implications
- Compromise in device security can lead to severe outcomes as well

THE VERGE

Hacked webcams that helped shut down the internet last week are being recalled

Smart refrigerator hack exposes Gmail login credentials NETWORKWORLD

IoT privacy and security!

- IoT devices projected to be ~**75 billion** by 2025
- Invasive nature of these devices raises significant privacy implications
- Compromise in device security can lead to severe outcomes as well

THE VERGE

Hacked webcams that helped shut down the internet last week are being recalled

Smart refrigerator hack exposes Gmail login credentials NETWORKWORLD

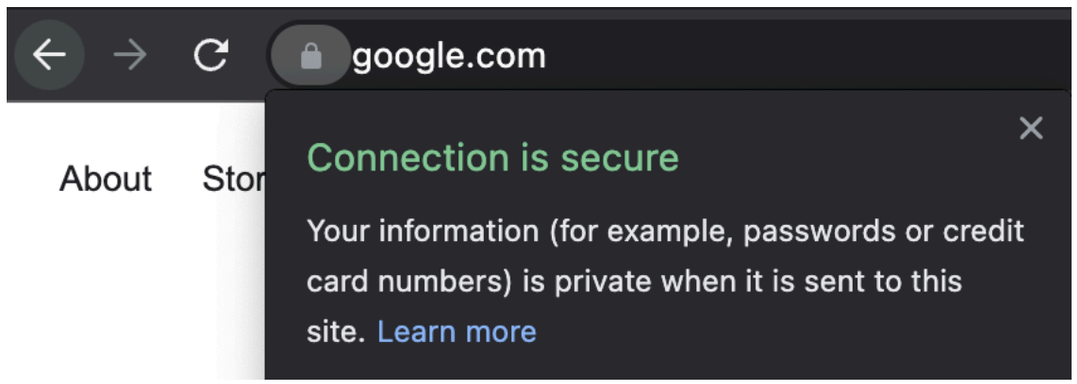
CNBC

Hackers remotely kill Jeep's engine on highway

TLS to the rescue!?

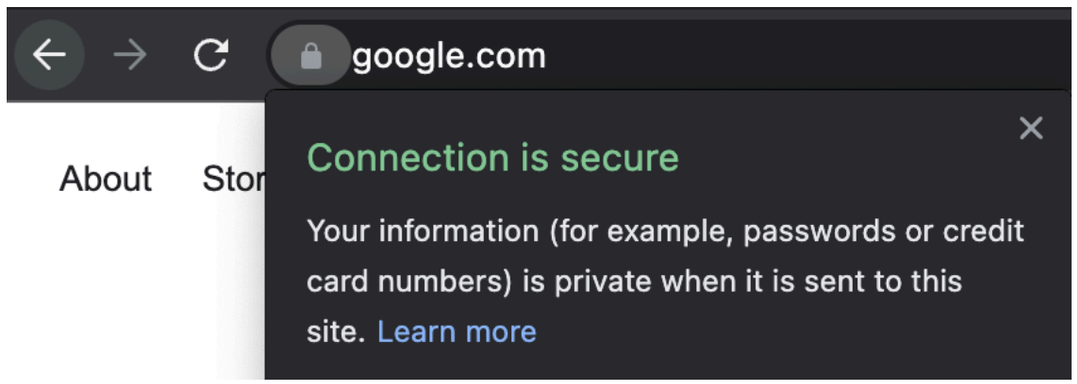
TLS to the rescue!?

- TLS de-facto web protocol to provide **confidentiality**, **authenticity**, and **data integrity**



TLS to the rescue!?

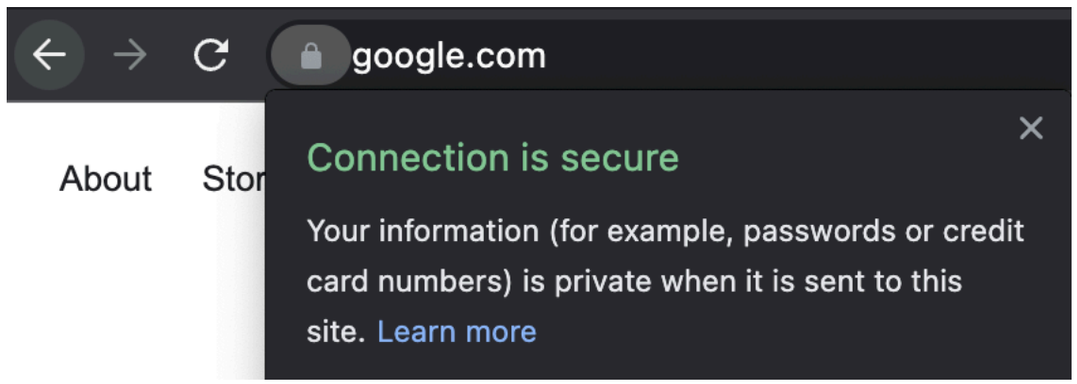
- TLS de-facto web protocol to provide **confidentiality**, **authenticity**, and **data integrity**



- Effective TLS usage means:

TLS to the rescue!?

- TLS de-facto web protocol to provide **confidentiality**, **authenticity**, and **data integrity**

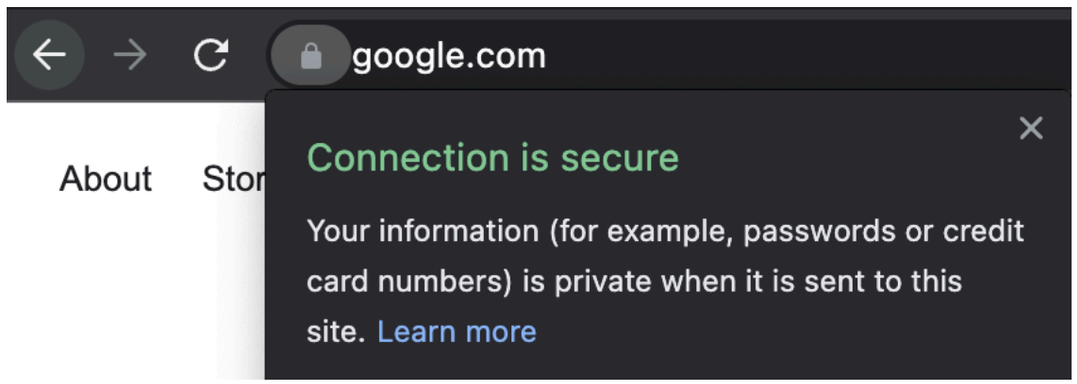


- Effective TLS usage means:

    1. Using secure protocol version and features (e.g., TLS 1.2)

TLS to the rescue!?

- TLS de-facto web protocol to provide **confidentiality**, **authenticity**, and **data integrity**



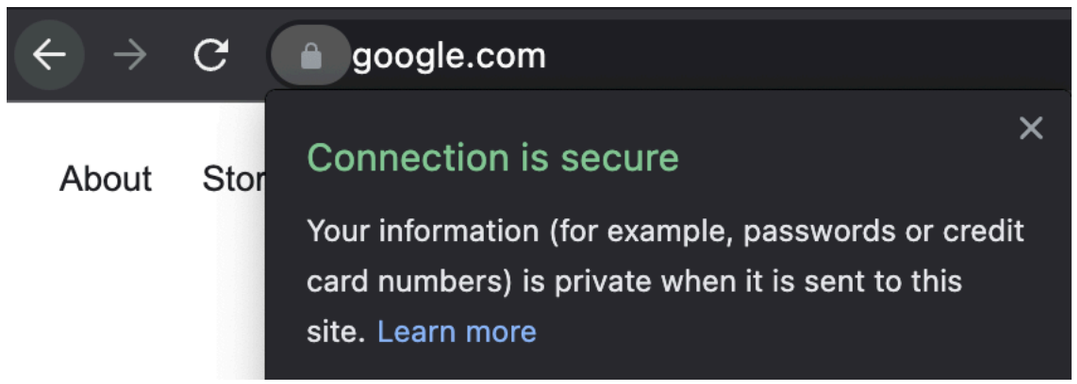
- Effective TLS usage means:

    1. Using secure protocol version and features (e.g., TLS 1.2)

    2. Properly validating certificate chains (e.g., trusted set of root certificates)

TLS to the rescue!?

- TLS de-facto web protocol to provide **confidentiality**, **authenticity**, and **data integrity**



- Effective TLS usage means:

1. Using secure protocol version and features (e.g., TLS 1.2)
2. Properly validating certificate chains (e.g., trusted set of root certificates)
3. Adopting new features as the protocol evolves over time
   (e.g., TLS 1.3, modern ciphersuites)

How effective is TLS in IoT?

How effective is TLS in IoT?

Studying TLS in IoT devices poses new challenges compared to other environments:

Challenge	***Our approach***

How effective is TLS in IoT?

Studying TLS in IoT devices poses new challenges compared to other environments:

Challenge	*Our approach*
1. Limited ways to trigger traffic	

How effective is TLS in IoT?

Studying TLS in IoT devices poses new challenges compared to other environments:

Challenge	*Our approach*
1. Limited ways to trigger traffic	
2. Limited vantage points	

How effective is TLS in IoT?

Studying TLS in IoT devices poses new challenges compared to other environments:

Challenge	***Our approach***
1. Limited ways to trigger traffic	1. Automate device reboots using smart plugs
2. Limited vantage points	

How effective is TLS in IoT?

Studying TLS in IoT devices poses new challenges compared to other environments:

Challenge	***Our approach***
1. Limited ways to trigger traffic	1. Automate device reboots using smart plugs
2. Limited vantage points	2. Uncontrolled experiments over a long period of time

Mon(IoT)r Lab at Northeastern University

Mon(IoT)r Lab at Northeastern University

- 40 TLS-supporting consumer IoT devices across 7 categories:
  Cameras, TVs, Home Automation, Audio, Smart Hubs & Appliances

Mon(IoT)r Lab at Northeastern University

- 40 TLS-supporting consumer IoT devices across 7 categories:
  Cameras, TVs, Home Automation, Audio, Smart Hubs & Appliances

- IRB-approved user-study with more than 30 participants

Mon(IoT)r Lab at Northeastern University

- 40 TLS-supporting consumer IoT devices across 7 categories:
  Cameras, TVs, Home Automation, Audio, Smart Hubs & Appliances
- IRB-approved user-study with more than 30 participants
- ~2 years of longitudinal data from January 2018 to March 2020

Key Results

Key Results

- Do devices ***securely establish*** TLS connections?

  ✓ Most devices use TLS 1.2

  ✓ No device uses insecure ciphersuites (ANON/NULL)

  ✗ Few devices upgrade to TLS 1.3 over time

  ✗ Few devices upgrade to modern ciphersuites (DH/ECDHE) over time

Key Results

- Do devices ***securely establish*** TLS connections?
- Do devices ***properly validate*** TLS certificates?

✗ 11 devices vulnerable to TLS interception attacks

✗ Devices do not appear to update their TLS root stores

Key Results

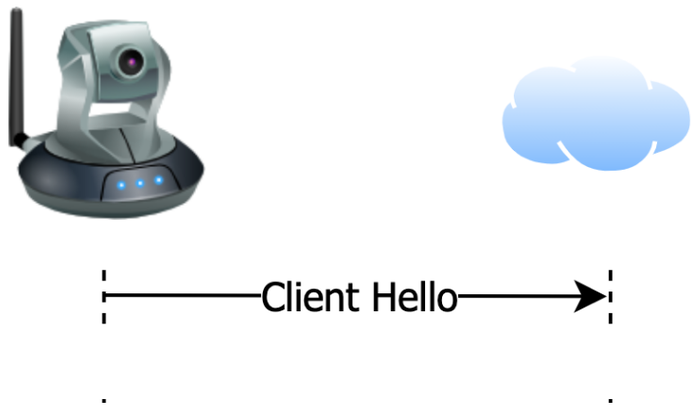
- Do devices ***securely establish*** TLS connections?
- Do devices ***properly validate*** TLS certificates?
- Do devices ***share TLS libraries*** with other clients?

  — Devices & applications from same vendor likely share TLS libraries.

Trusted root stores

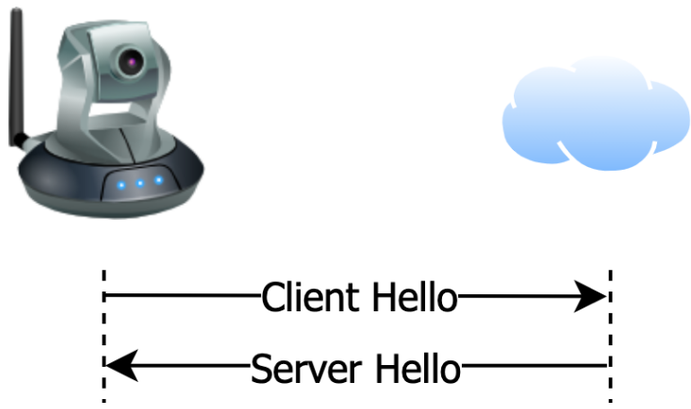
Example TLS Handshake

Trusted root stores



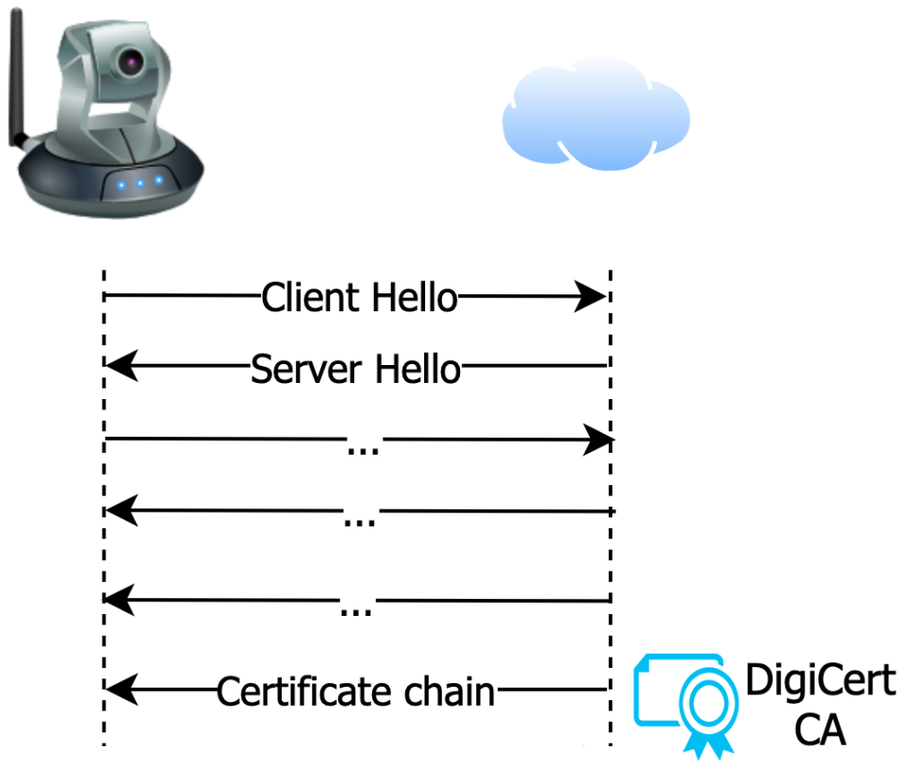
Example TLS Handshake

Trusted root stores



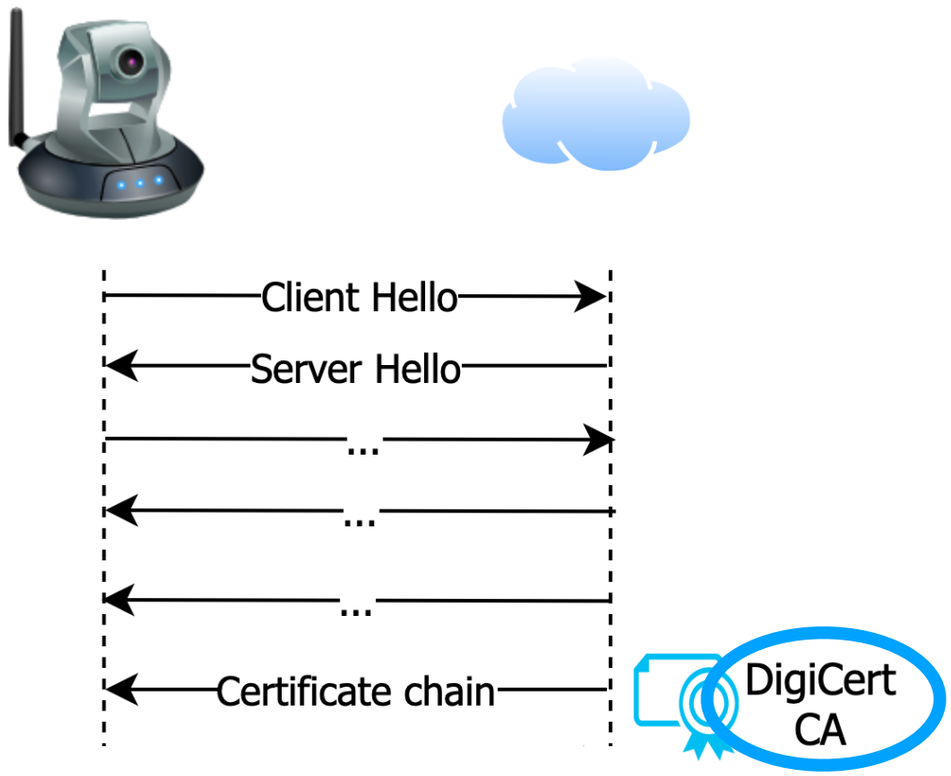
Example TLS Handshake

Trusted root stores



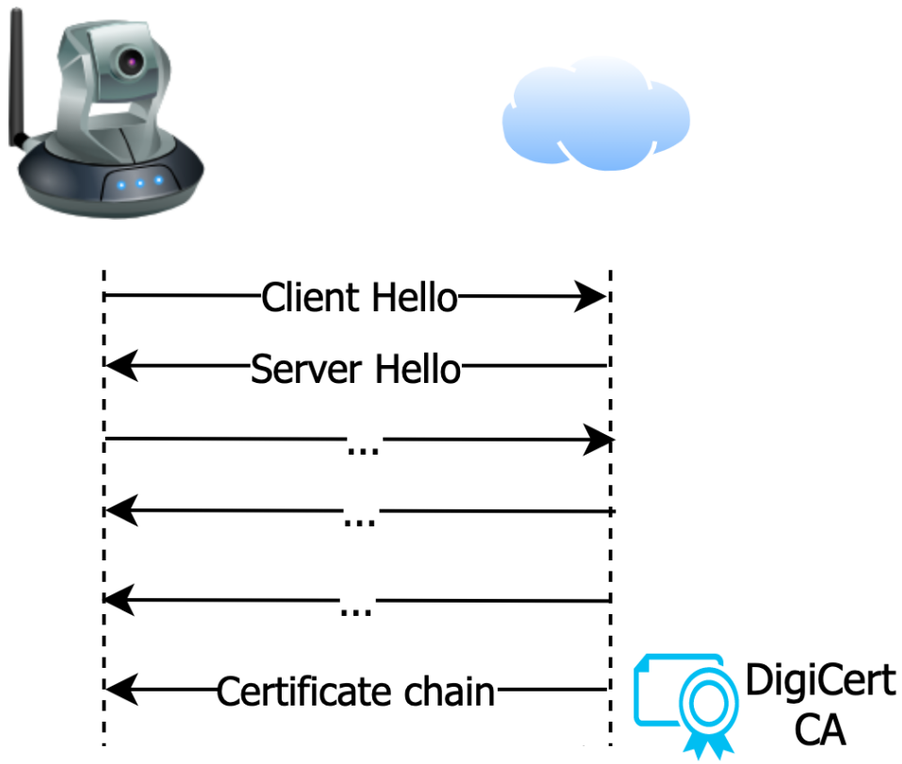
Example TLS Handshake

Trusted root stores



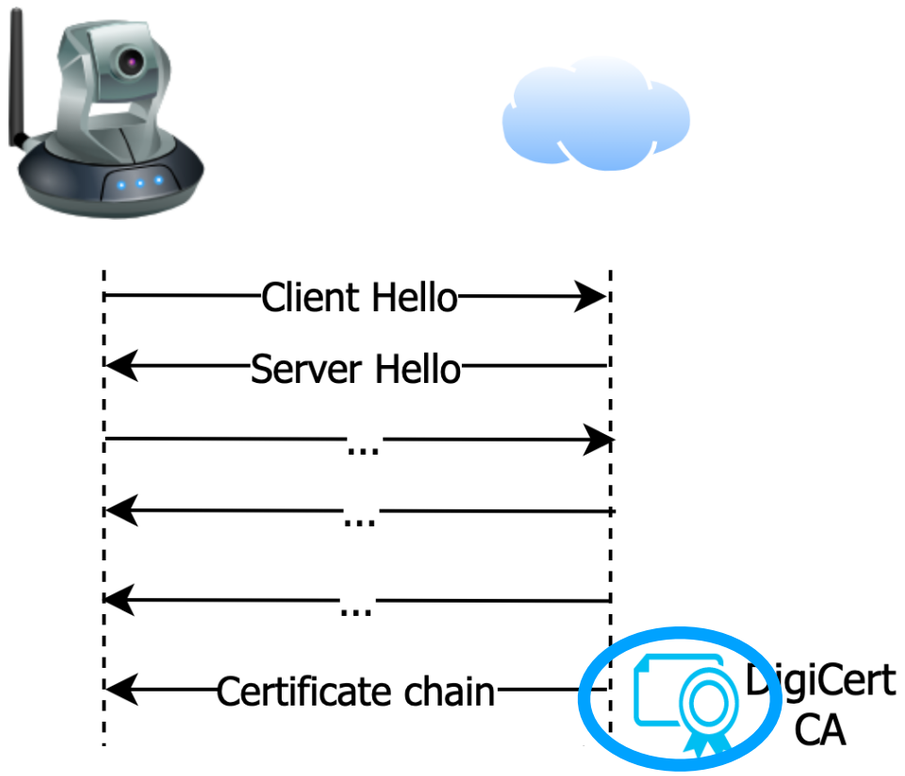
Example TLS Handshake

Trusted root stores



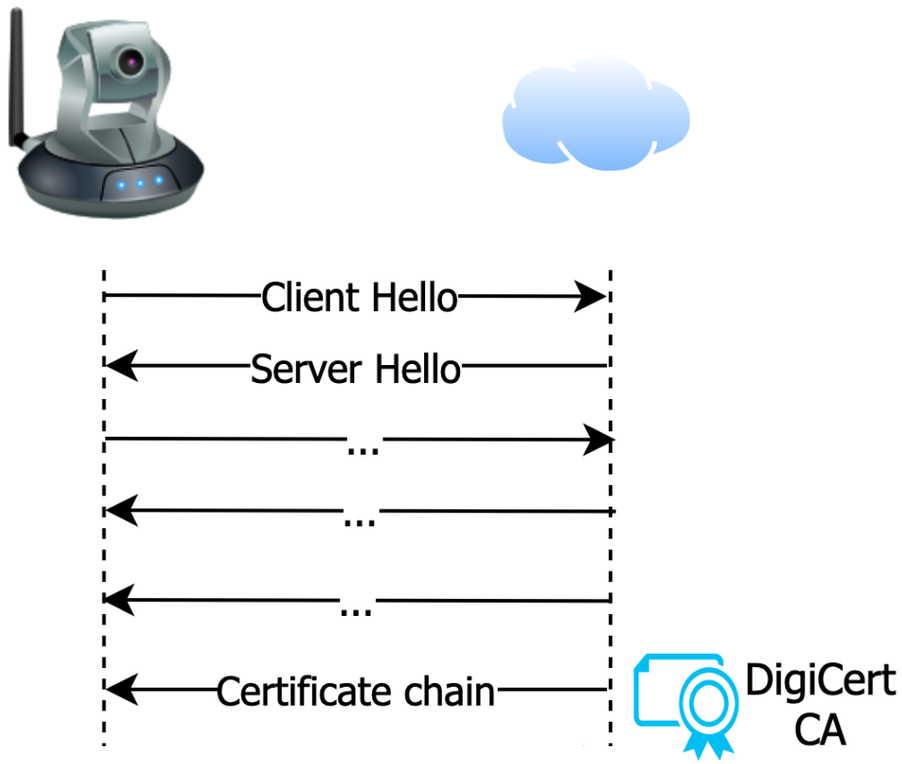
Example TLS Handshake

Trusted root stores



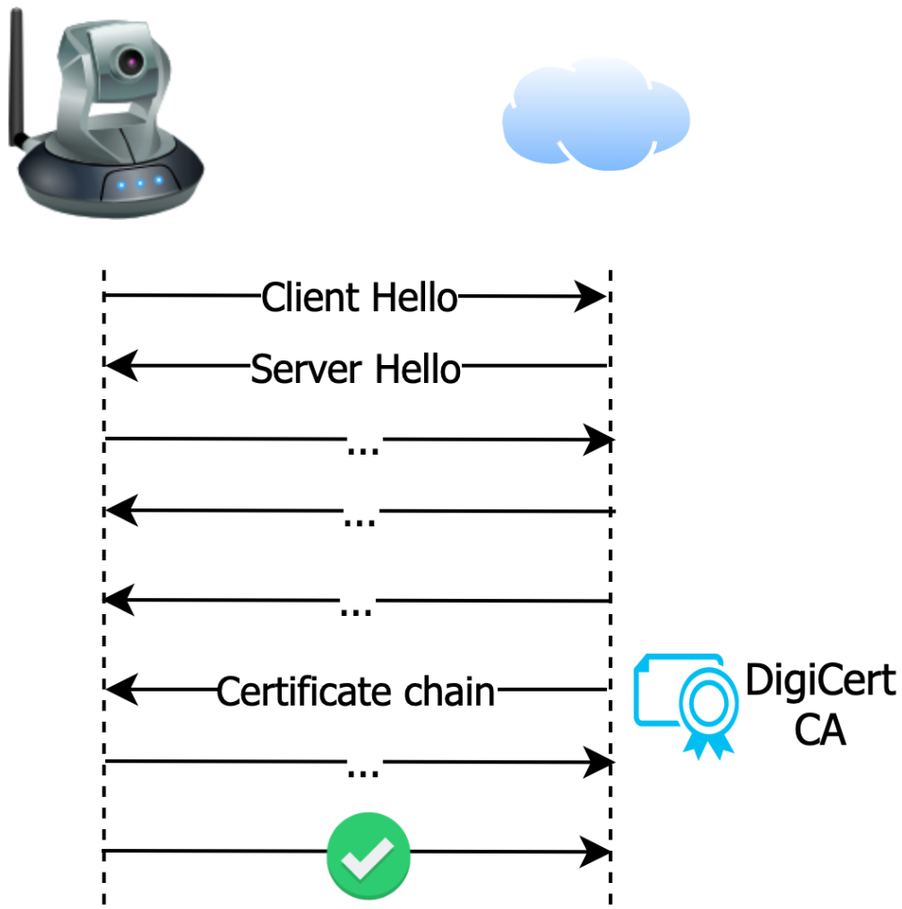
Example TLS Handshake

Trusted root stores



Example TLS Handshake

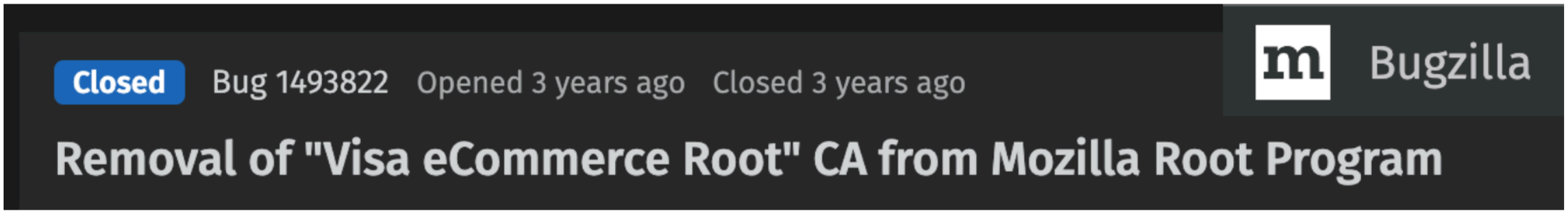
Trusted root stores



Example TLS Handshake

Why do root certificates matter?

Why do root certificates matter?

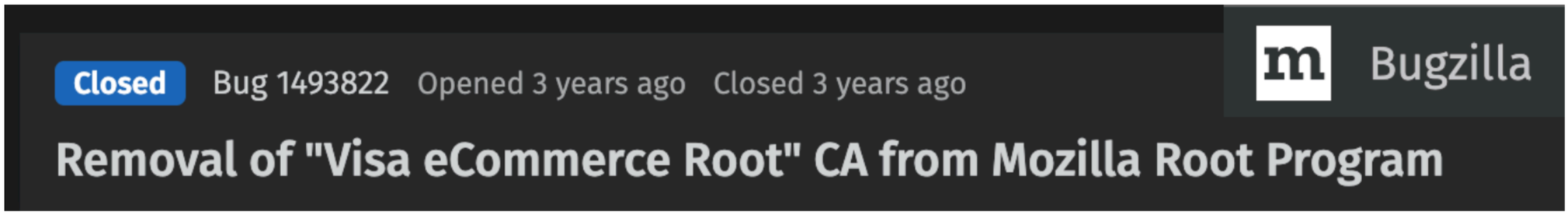


Why do root certificates matter?

digicert®

Let's Encrypt

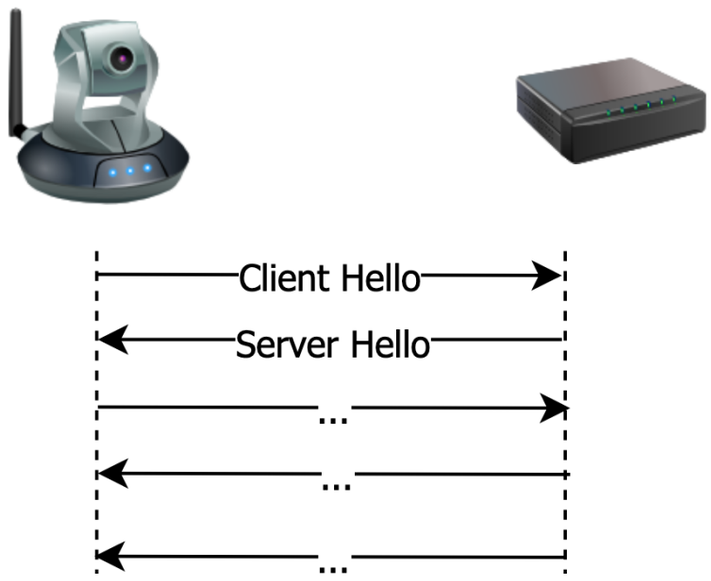
COMODO SSLCERTIFICATE



moz://a **Revoking Trust in Two TurkTrust Certificates**

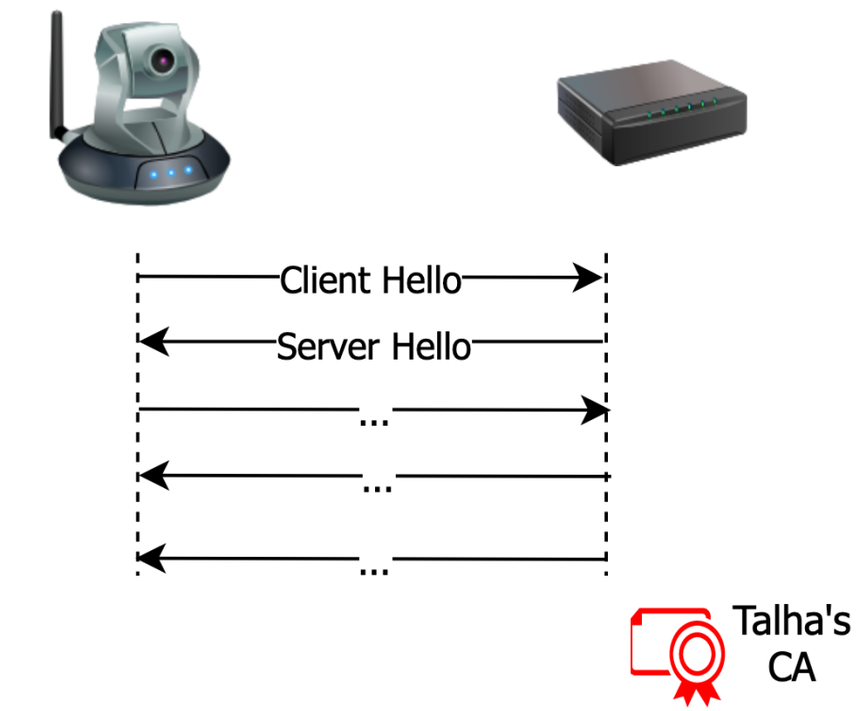
Root stores exploration in IoT devices

Root stores exploration in IoT devices



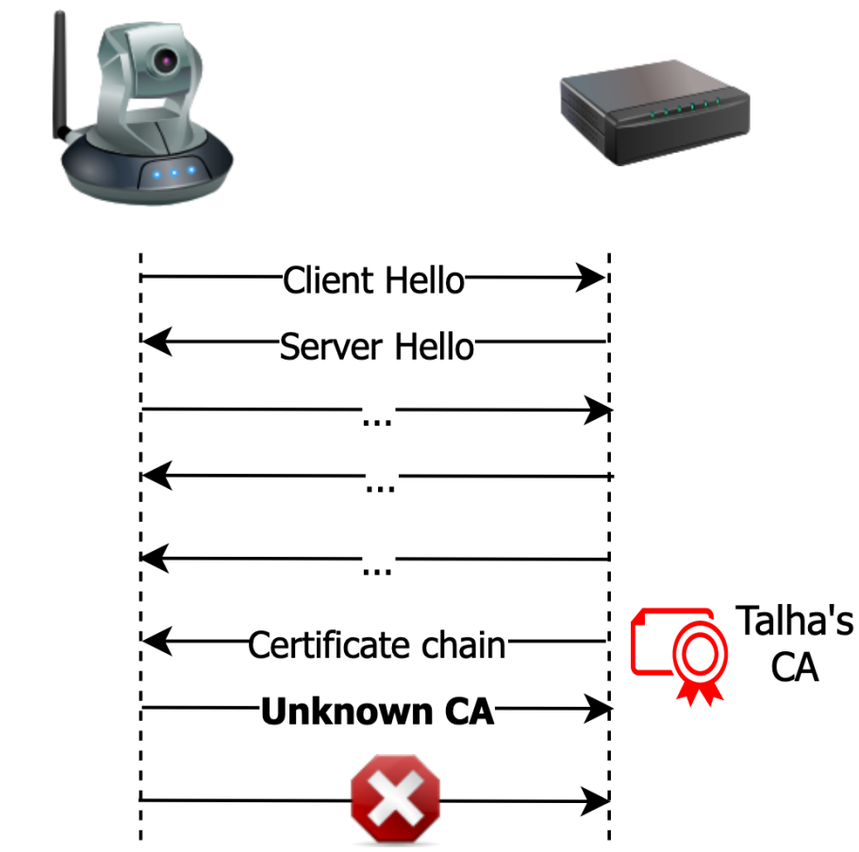
Intercepted TLS Handshake
with arbitrary CA

Root stores exploration in IoT devices



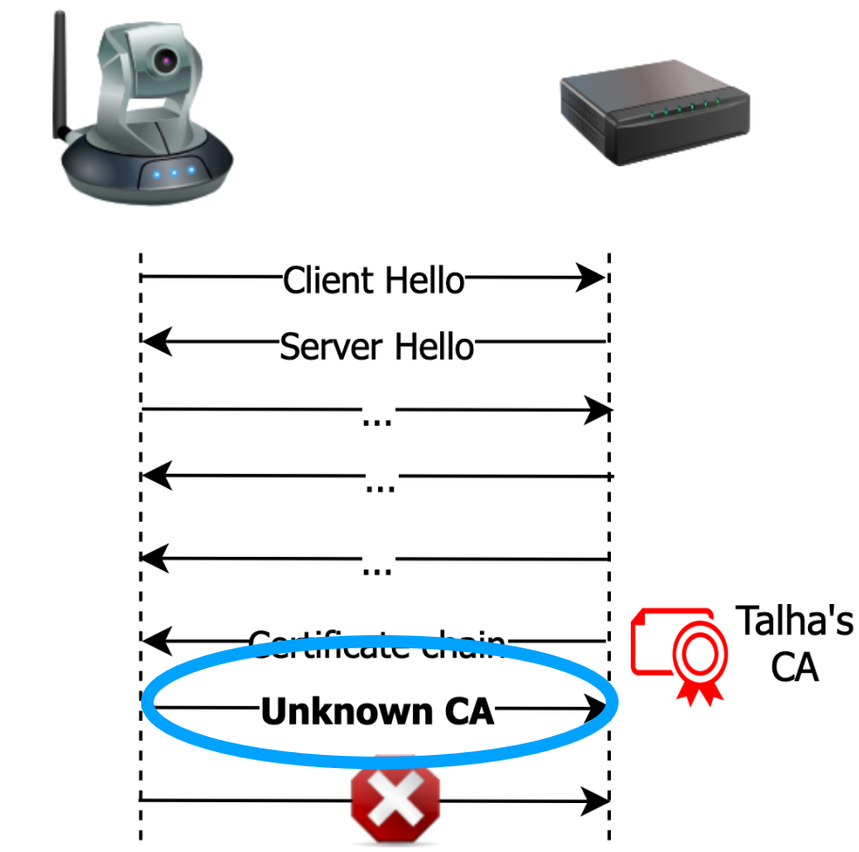
Intercepted TLS Handshake
with arbitrary CA

Root stores exploration in IoT devices



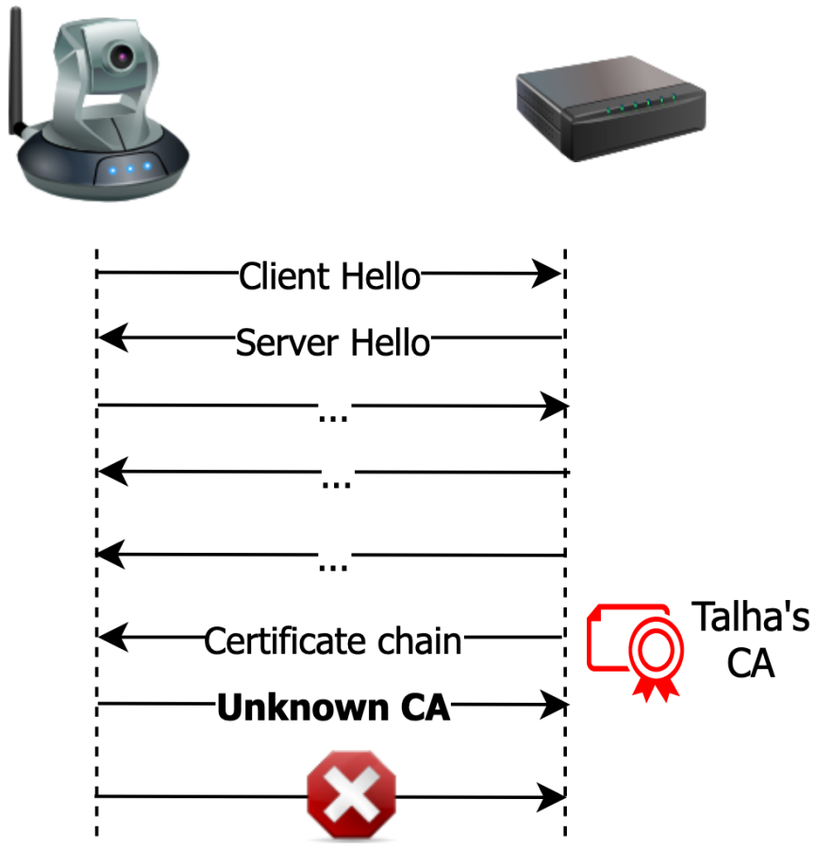
Intercepted TLS Handshake with arbitrary CA

Root stores exploration in IoT devices

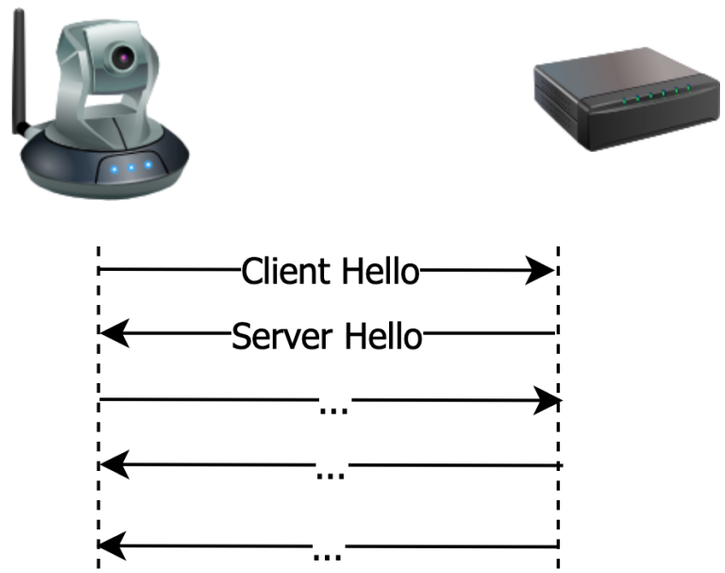


Intercepted TLS Handshake with arbitrary CA

Root stores exploration in IoT devices

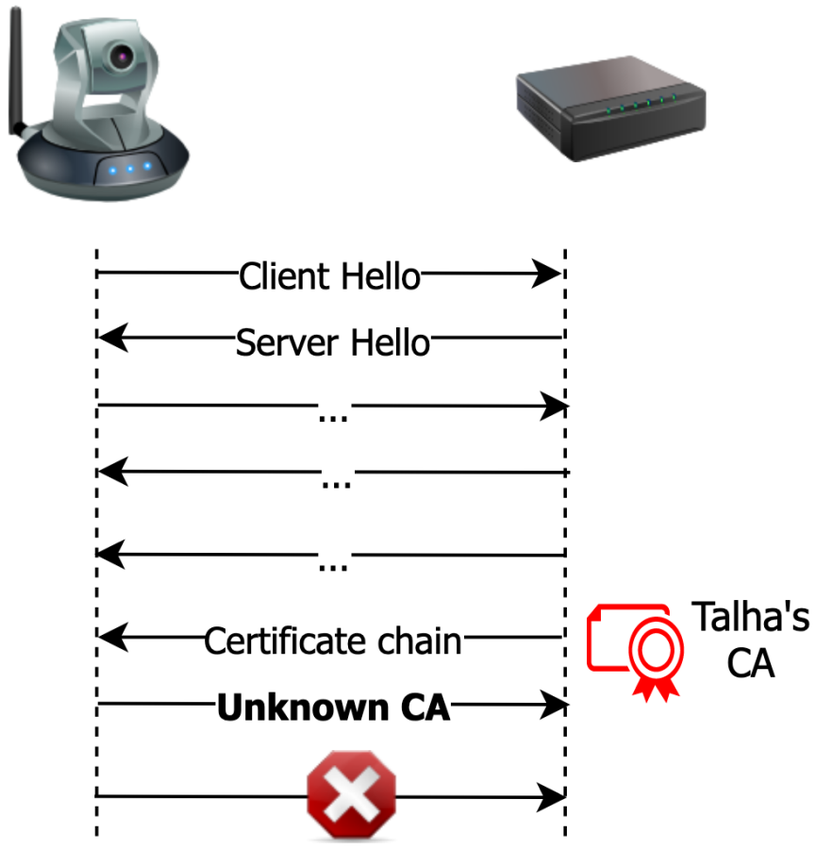


Intercepted TLS Handshake with arbitrary CA

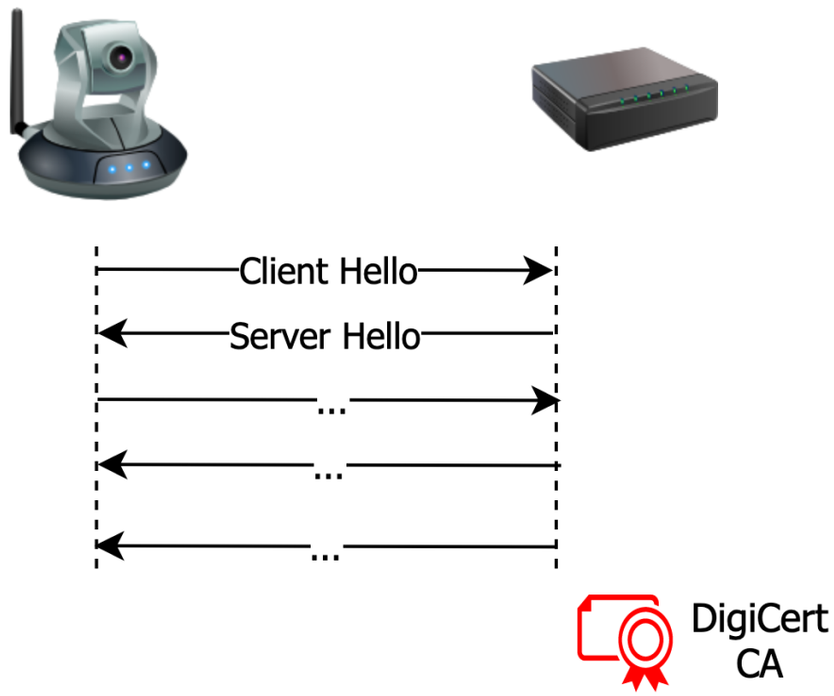


Intercepted TLS Handshake with known CA

Root stores exploration in IoT devices

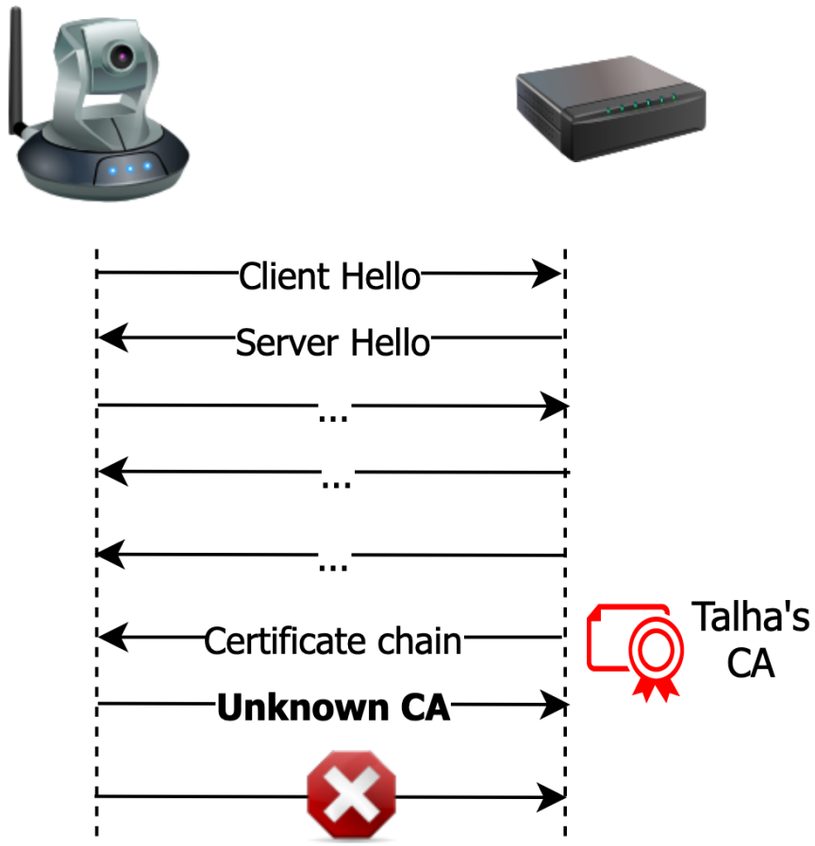


Intercepted TLS Handshake with arbitrary CA

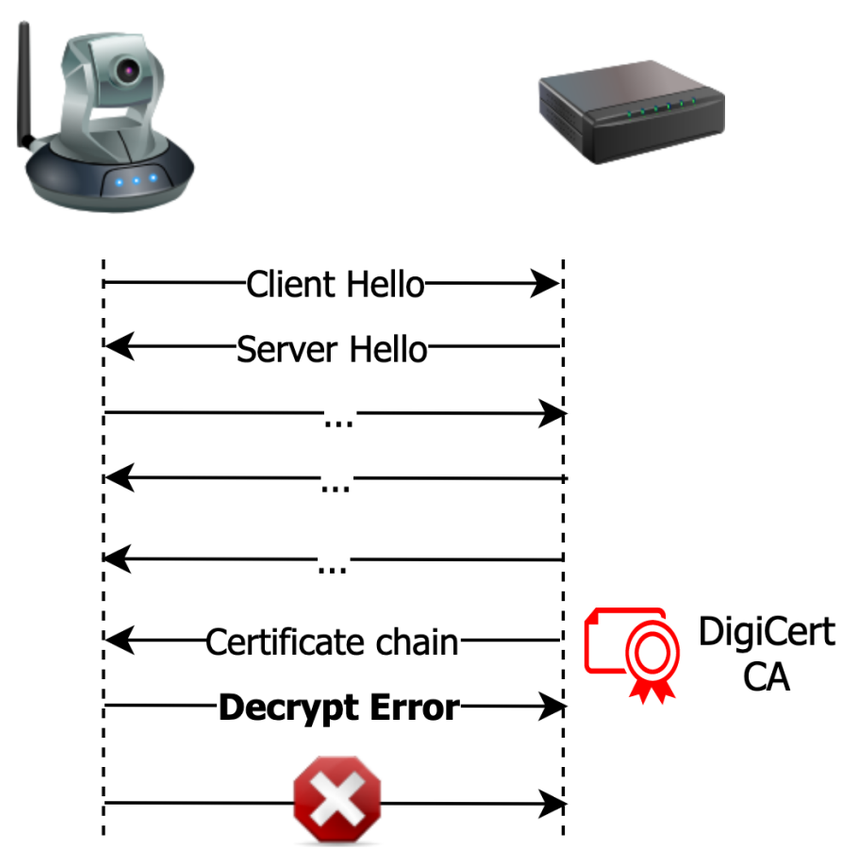


Intercepted TLS Handshake with known CA

Root stores exploration in IoT devices

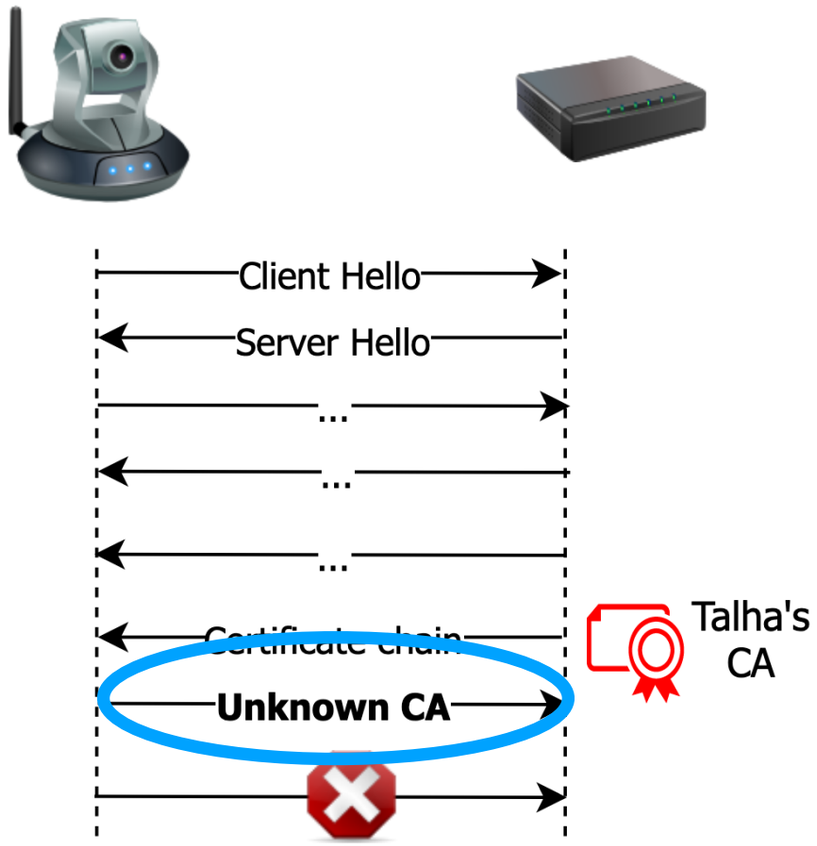


Intercepted TLS Handshake with arbitrary CA

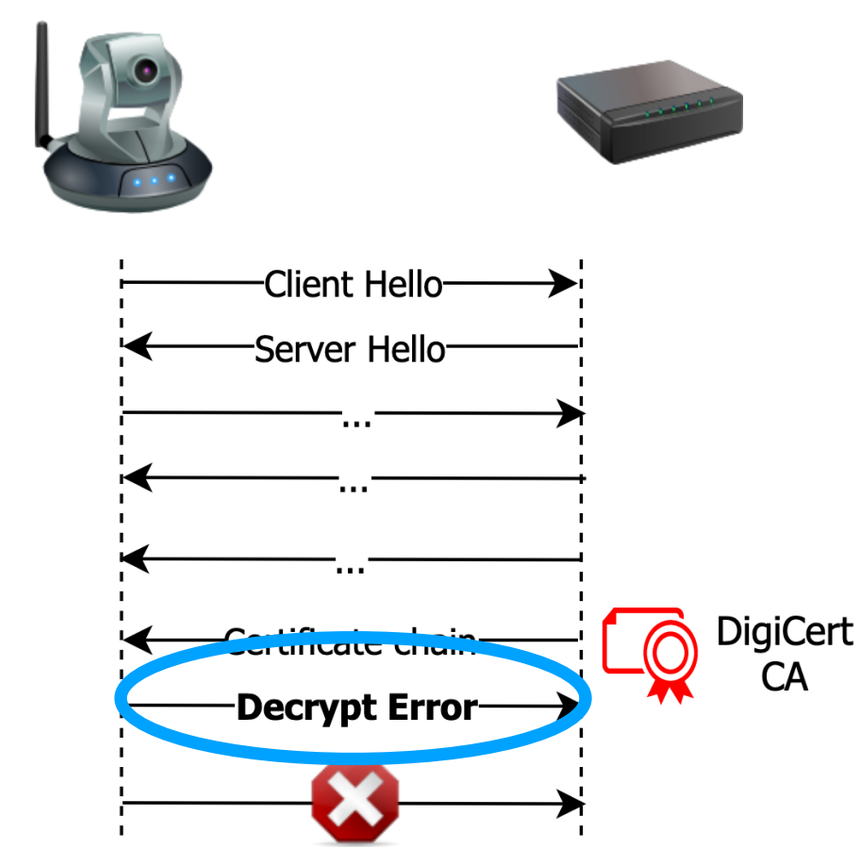


Intercepted TLS Handshake with known CA

Root stores exploration in IoT devices



Intercepted TLS Handshake with arbitrary CA



Intercepted TLS Handshake with known CA

Root stores exploration in IoT devices

Root stores exploration in IoT devices

- Technique works for **8/24** IoT devices tested

Root stores exploration in IoT devices

- Technique works for **8/24** IoT devices tested
- Extracted historical root stores from 4 major root stores (Ubuntu, Android, Mozilla, and Microsoft)

Root stores exploration in IoT devices

- Technique works for **8/24** IoT devices tested
- Extracted historical root stores from 4 major root stores (Ubuntu, Android, Mozilla, and Microsoft)
- Generated two sets of CA certificates:

Root stores exploration in IoT devices

- Technique works for **8/24** IoT devices tested
- Extracted historical root stores from 4 major root stores (Ubuntu, Android, Mozilla, and Microsoft)
- Generated two sets of CA certificates:
  - *Commonly-trusted certificates* — certs available in latest versions of all platforms

Root stores exploration in IoT devices

- Technique works for **8/24** IoT devices tested
- Extracted historical root stores from 4 major root stores (Ubuntu, Android, Mozilla, and Microsoft)
- Generated two sets of CA certificates:
  - *Commonly-trusted certificates* — certs available in latest versions of all platforms
  - *Deprecated certificates* — certs that were removed from one or more stores over time

Do IoT devices use *commonly-trusted* root certificates?

Device	Commonly-trusted certs (total = 122)
Google Home Mini	
Amazon Echo Plus	
Amazon Echo Dot	
Amazon Echo Dot 3	
Wink Hub 2	
Roku TV	
LG TV	
Harman Invoke	

Do IoT devices use *commonly-trusted* root certificates?

Device	Commonly-trusted certs (total = 122)
Google Home Mini	100%
Amazon Echo Plus	98%
Amazon Echo Dot	98%
Amazon Echo Dot 3	90%
Wink Hub 2	92%
Roku TV	91%
LG TV	93%
Harman Invoke	82%

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	
Amazon Echo Plus	
Amazon Echo Dot	
Amazon Echo Dot 3	
Wink Hub 2	
Roku TV	
LG TV	
Harman Invoke	

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	6%
Amazon Echo Plus	18%
Amazon Echo Dot	19%
Amazon Echo Dot 3	27%
Wink Hub 2	38%
Roku TV	41%
LG TV	59%
Harman Invoke	59%

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	6%
Amazon Echo Plus	18%
Amazon Echo Dot	19%
Amazon Echo Dot 3	27%
Wink Hub 2	38%
Roku TV	41%
LG TV	59%
Harman Invoke	59%

- All devices trust some *deprecated* root certificates

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	6%
Amazon Echo Plus	18%
Amazon Echo Dot	19%
Amazon Echo Dot 3	27%
Wink Hub 2	38%
Roku TV	41%
LG TV	59%
Harman Invoke	59%

- All devices trust some *deprecated* root certificates

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	6%
Amazon Echo Plus	18%
Amazon Echo Dot	19%
Amazon Echo Dot 3	27%
Wink Hub 2	38%
Roku TV	41%
LG TV	59%
Harman Invoke	59%

- All devices trust some *deprecated* root certificates

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	6%
Amazon Echo Plus	18%
Amazon Echo Dot	19%
Amazon Echo Dot 3	27%
Wink Hub 2	38%
Roku TV	41%
LG TV	59%
Harman Invoke	59%

- All devices trust some *deprecated* root certificates
- Devices likely do not update their root stores

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	6%
Amazon Echo Plus	18%
Amazon Echo Dot	19%
Amazon Echo Dot 3	27%
Wink Hub 2	38%
Roku TV	41%
LG TV	59%
Harman Invoke	59%

- All devices trust some *deprecated* root certificates
- Devices likely do not update their root stores

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	6%
Amazon Echo Plus	18%
Amazon Echo Dot	19%
Amazon Echo Dot 3	27%
Wink Hub 2	38%
Roku TV	41%
LG TV	59%
Harman Invoke	59%

- All devices trust some *deprecated* root certificates
- Devices likely do not update their root stores

Do IoT devices use *deprecated* root certificates?

Device	Deprecated certs (total = 87)
Google Home Mini	6%
Amazon Echo Plus	18%
Amazon Echo Dot	19%
Amazon Echo Dot 3	27%
Wink Hub 2	38%
Roku TV	41%
LG TV	59%
Harman Invoke	59%

- All devices trust some *deprecated* root certificates
- Devices likely do not update their root stores
- All 8 devices trust at least one CA certificate that is **explicitly distrusted** by Firefox or Chrome (e.g, *TurkTrust, WoSign*)

Conclusion!

Conclusion!

- Mix of good and bad news about TLS usage in IoT devices

Conclusion!

- Mix of good and bad news about TLS usage in IoT devices

IoTLS: Understanding TLS Usage in Consumer IoT Devices

Muhammad Talha Paracha
Northeastern University

Daniel J. Dubois
Northeastern University

Narseo Vallina-Rodriguez
IMDEA Networks / ICSI / AppCensus Inc.

David Choffnes
Northeastern University

ABSTRACT

Consumer IoT devices are becoming increasingly popular, with most leveraging TLS to provide connection security. In this work, we study a large number of TLS-enabled consumer IoT devices to shed light on how effectively they use TLS, in terms of establishing secure connections and correctly validating certificates, and how observed behavior changes over time. To this end, we gather more than two years of TLS network traffic from IoT devices, conduct active probing to test for vulnerabilities, and develop a novel black-box technique for exploring the trusted root stores in IoT devices by exploiting a side-channel through TLS *Alert Messages*. We find a wide range of behaviors across devices, with some adopting best security practices but most being vulnerable in one or more of the following ways: use of old/insecure protocol versions and/or ciphersuites, lack of certificate validation, and poor maintenance of root stores. Specifically, we find that *at least* 8 IoT devices still include distrusted certificates in their root stores, 11/32 devices are vulnerable to TLS interception attacks, and that many devices fail to adopt modern protocol features over time. Our findings motivate the need for IoT manufacturers to audit, upgrade, and maintain their devices' TLS implementations in a consistent and uniform way that safeguards all of their network traffic.

CCS CONCEPTS

• **Security and privacy** → **Network security**; **Embedded systems security**; • **Networks** → *Network measurement*; **Network security**;

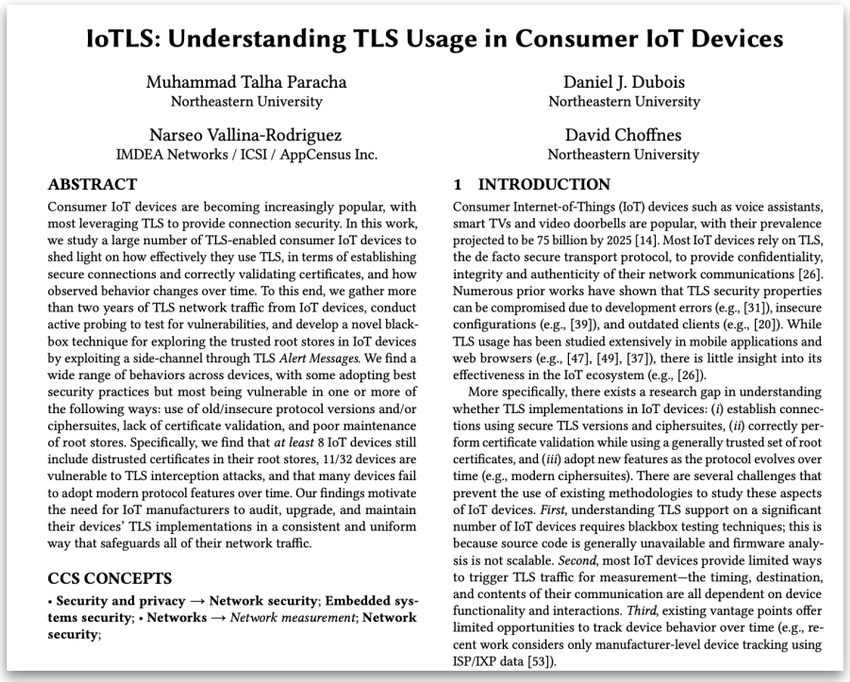
1 INTRODUCTION

Consumer Internet-of-Things (IoT) devices such as voice assistants, smart TVs and video doorbells are popular, with their prevalence projected to be 75 billion by 2025 [14]. Most IoT devices rely on TLS, the de facto secure transport protocol, to provide confidentiality, integrity and authenticity of their network communications [26]. Numerous prior works have shown that TLS security properties can be compromised due to development errors (e.g., [31]), insecure configurations (e.g., [39]), and outdated clients (e.g., [20]). While TLS usage has been studied extensively in mobile applications and web browsers (e.g., [47], [49], [37]), there is little insight into its effectiveness in the IoT ecosystem (e.g., [26]).

More specifically, there exists a research gap in understanding whether TLS implementations in IoT devices: (*i*) establish connections using secure TLS versions and ciphersuites, (*ii*) correctly perform certificate validation while using a generally trusted set of root certificates, and (*iii*) adopt new features as the protocol evolves over time (e.g., modern ciphersuites). There are several challenges that prevent the use of existing methodologies to study these aspects of IoT devices. *First*, understanding TLS support on a significant number of IoT devices requires blackbox testing techniques; this is because source code is generally unavailable and firmware analysis is not scalable. *Second*, most IoT devices provide limited ways to trigger TLS traffic for measurement—the timing, destination, and contents of their communication are all dependent on device functionality and interactions. *Third*, existing vantage points offer limited opportunities to track device behavior over time (e.g., recent work considers only manufacturer-level device tracking using ISP/IXP data [53]).

Conclusion!

- Mix of good and bad news about TLS usage in IoT devices
- Longitudinal TLS handshake data + controlled experimentation data + analysis software **publicly available**



IoTLS: Understanding TLS Usage in Consumer IoT Devices

Muhammad Talha Paracha
Northeastern University

Daniel J. Dubois
Northeastern University

Narseo Vallina-Rodriguez
IMDEA Networks / ICSI / AppCensus Inc.

David Choffnes
Northeastern University

ABSTRACT

Consumer IoT devices are becoming increasingly popular, with most leveraging TLS to provide connection security. In this work, we study a large number of TLS-enabled consumer IoT devices to shed light on how effectively they use TLS, in terms of establishing secure connections and correctly validating certificates, and how observed behavior changes over time. To this end, we gather more than two years of TLS network traffic from IoT devices, conduct active probing to test for vulnerabilities, and develop a novel black-box technique for exploring the trusted root stores in IoT devices by exploiting a side-channel through TLS *Alert Messages*. We find a wide range of behaviors across devices, with some adopting best security practices but most being vulnerable in one or more of the following ways: use of old/insecure protocol versions and/or ciphersuites, lack of certificate validation, and poor maintenance of root stores. Specifically, we find that *at least* 8 IoT devices still include distrusted certificates in their root stores, 11/32 devices are vulnerable to TLS interception attacks, and that many devices fail to adopt modern protocol features over time. Our findings motivate the need for IoT manufacturers to audit, upgrade, and maintain their devices' TLS implementations in a consistent and uniform way that safeguards all of their network traffic.

CCS CONCEPTS

• **Security and privacy** → **Network security**; **Embedded systems security**; • **Networks** → *Network measurement*; **Network security**;

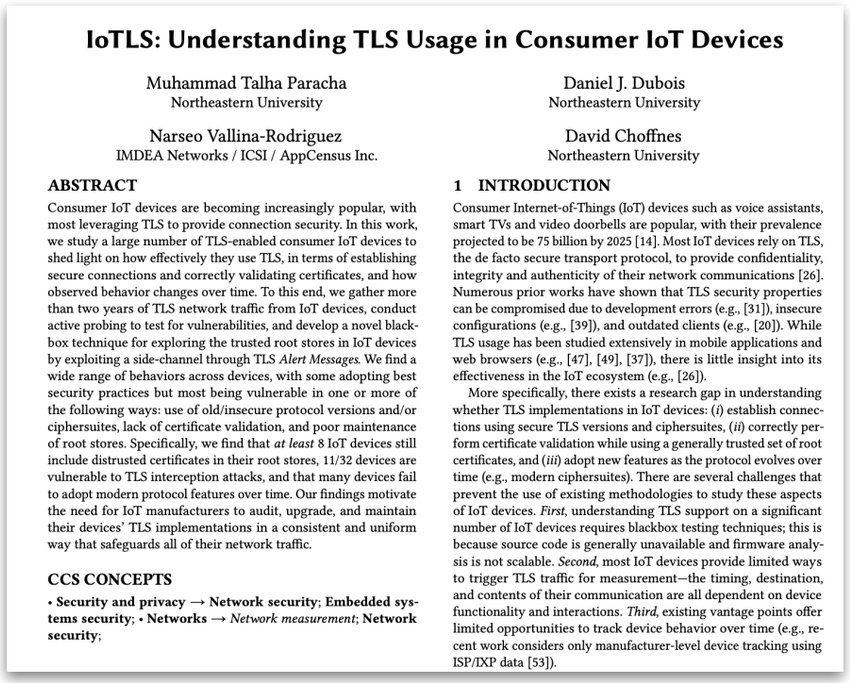
1 INTRODUCTION

Consumer Internet-of-Things (IoT) devices such as voice assistants, smart TVs and video doorbells are popular, with their prevalence projected to be 75 billion by 2025 [14]. Most IoT devices rely on TLS, the de facto secure transport protocol, to provide confidentiality, integrity and authenticity of their network communications [26]. Numerous prior works have shown that TLS security properties can be compromised due to development errors (e.g., [31]), insecure configurations (e.g., [39]), and outdated clients (e.g., [20]). While TLS usage has been studied extensively in mobile applications and web browsers (e.g., [47], [49], [37]), there is little insight into its effectiveness in the IoT ecosystem (e.g., [26]).

More specifically, there exists a research gap in understanding whether TLS implementations in IoT devices: (*i*) establish connections using secure TLS versions and ciphersuites, (*ii*) correctly perform certificate validation while using a generally trusted set of root certificates, and (*iii*) adopt new features as the protocol evolves over time (e.g., modern ciphersuites). There are several challenges that prevent the use of existing methodologies to study these aspects of IoT devices. *First*, understanding TLS support on a significant number of IoT devices requires blackbox testing techniques; this is because source code is generally unavailable and firmware analysis is not scalable. *Second*, most IoT devices provide limited ways to trigger TLS traffic for measurement—the timing, destination, and contents of their communication are all dependent on device functionality and interactions. *Third*, existing vantage points offer limited opportunities to track device behavior over time (e.g., recent work considers only manufacturer-level device tracking using ISP/IXP data [53]).

Conclusion!

- Mix of good and bad news about TLS usage in IoT devices
- Longitudinal TLS handshake data + controlled experimentation data + analysis software **publicly available**



IoTLS: Understanding TLS Usage in Consumer IoT Devices

Muhammad Talha Paracha
Northeastern University

Daniel J. Dubois
Northeastern University

Narseo Vallina-Rodriguez
IMDEA Networks / ICSI / AppCensus Inc.

David Choffnes
Northeastern University

ABSTRACT

Consumer IoT devices are becoming increasingly popular, with most leveraging TLS to provide connection security. In this work, we study a large number of TLS-enabled consumer IoT devices to shed light on how effectively they use TLS, in terms of establishing secure connections and correctly validating certificates, and how observed behavior changes over time. To this end, we gather more than two years of TLS network traffic from IoT devices, conduct active probing to test for vulnerabilities, and develop a novel black-box technique for exploring the trusted root stores in IoT devices by exploiting a side-channel through TLS *Alert Messages*. We find a wide range of behaviors across devices, with some adopting best security practices but most being vulnerable in one or more of the following ways: use of old/insecure protocol versions and/or ciphersuites, lack of certificate validation, and poor maintenance of root stores. Specifically, we find that *at least* 8 IoT devices still include distrusted certificates in their root stores, 11/32 devices are vulnerable to TLS interception attacks, and that many devices fail to adopt modern protocol features over time. Our findings motivate the need for IoT manufacturers to audit, upgrade, and maintain their devices' TLS implementations in a consistent and uniform way that safeguards all of their network traffic.

CCS CONCEPTS

• **Security and privacy** → **Network security**; **Embedded systems security**; • **Networks** → *Network measurement*; **Network security**;

1 INTRODUCTION

Consumer Internet-of-Things (IoT) devices such as voice assistants, smart TVs and video doorbells are popular, with their prevalence projected to be 75 billion by 2025 [14]. Most IoT devices rely on TLS, the de facto secure transport protocol, to provide confidentiality, integrity and authenticity of their network communications [26]. Numerous prior works have shown that TLS security properties can be compromised due to development errors (e.g., [31]), insecure configurations (e.g., [39]), and outdated clients (e.g., [20]). While TLS usage has been studied extensively in mobile applications and web browsers (e.g., [47], [49], [37]), there is little insight into its effectiveness in the IoT ecosystem (e.g., [26]).

More specifically, there exists a research gap in understanding whether TLS implementations in IoT devices: (*i*) establish connections using secure TLS versions and ciphersuites, (*ii*) correctly perform certificate validation while using a generally trusted set of root certificates, and (*iii*) adopt new features as the protocol evolves over time (e.g., modern ciphersuites). There are several challenges that prevent the use of existing methodologies to study these aspects of IoT devices. *First*, understanding TLS support on a significant number of IoT devices requires blackbox testing techniques; this is because source code is generally unavailable and firmware analysis is not scalable. *Second*, most IoT devices provide limited ways to trigger TLS traffic for measurement—the timing, destination, and contents of their communication are all dependent on device functionality and interactions. *Third*, existing vantage points offer limited opportunities to track device behavior over time (e.g., recent work considers only manufacturer-level device tracking using ISP/IXP data [53]).

moniotrlab.ccis.neu.edu

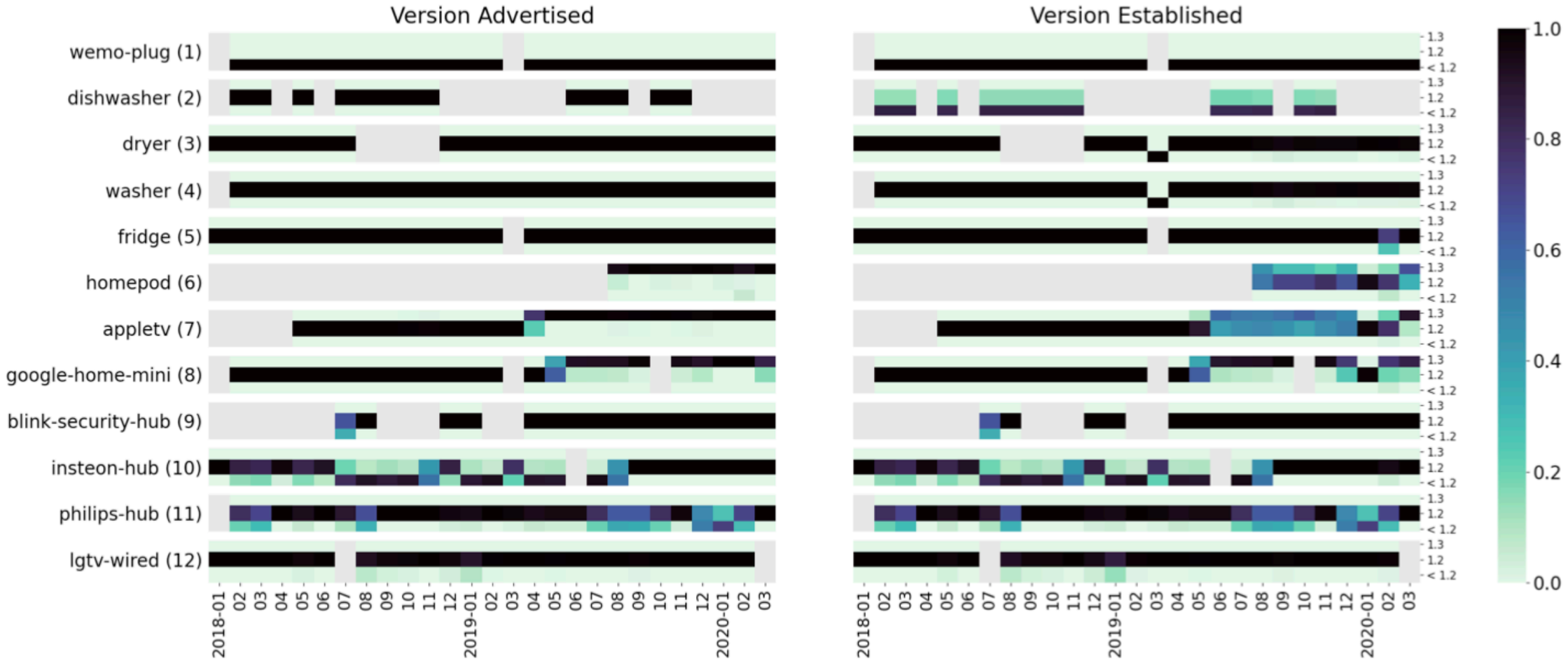
END

Mon(IoT)r Lab at Northeastern University

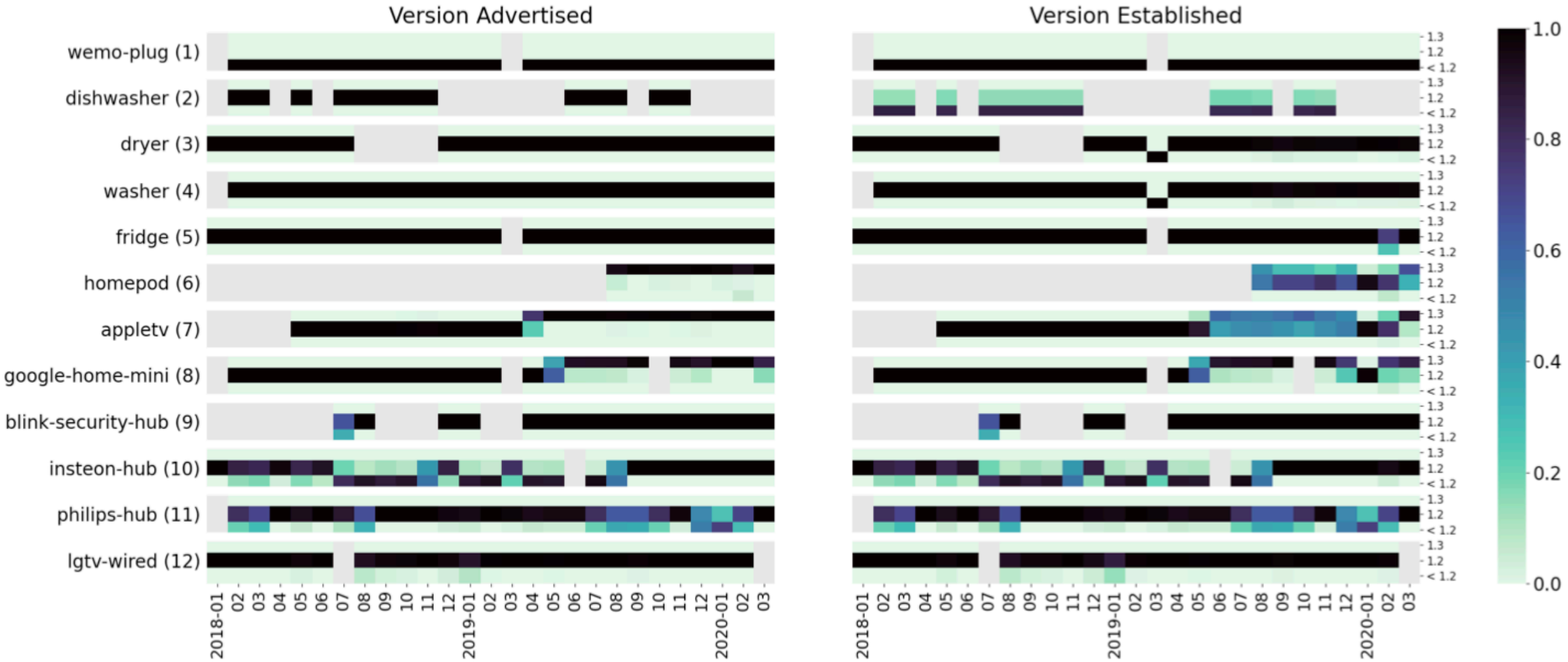
Table 1: List of the 40 TLS-supporting devices in our study. (*) denotes devices used only in *passive* experiments.

Cameras (n = 7)	Smart Hubs (n = 7)	Home Automation (n = 7)	TV (n = 5)	Audio (n = 7)	Appliances (n = 7)
Blink Camera*	Blink Hub	Smartlife Bulb	Fire TV	Google Home Mini	GE Microwave
Amazon Cloudcam*	Smartthings Hub	Smartlife Remote	Samsung TV*	Amazon Echo Plus	Samsung Washer*
Zmodo Doorbell	Philips Hub	Meross Dooropener	LG TV	Amazon Echo Dot	Samsung Dryer
Yi Camera	Wink Hub 2	TP-Link Bulb	Roku TV	Amazon Echo Dot 3	Samsung Fridge
D-Link Camera	Sengled Hub*	Nest Thermostat	Apple TV	Amazon Echo Spot	Smarter iKettle
Amcrest Camera	Switchbot Hub	TP-Link Plug		Harman Invoke	Behmor Brewer
Ring Doorbell*	Insteon Hub*	Wemo Plug		Apple HomePod	LG Dishwasher*

RQ1: TLS Connection Security (Passive)

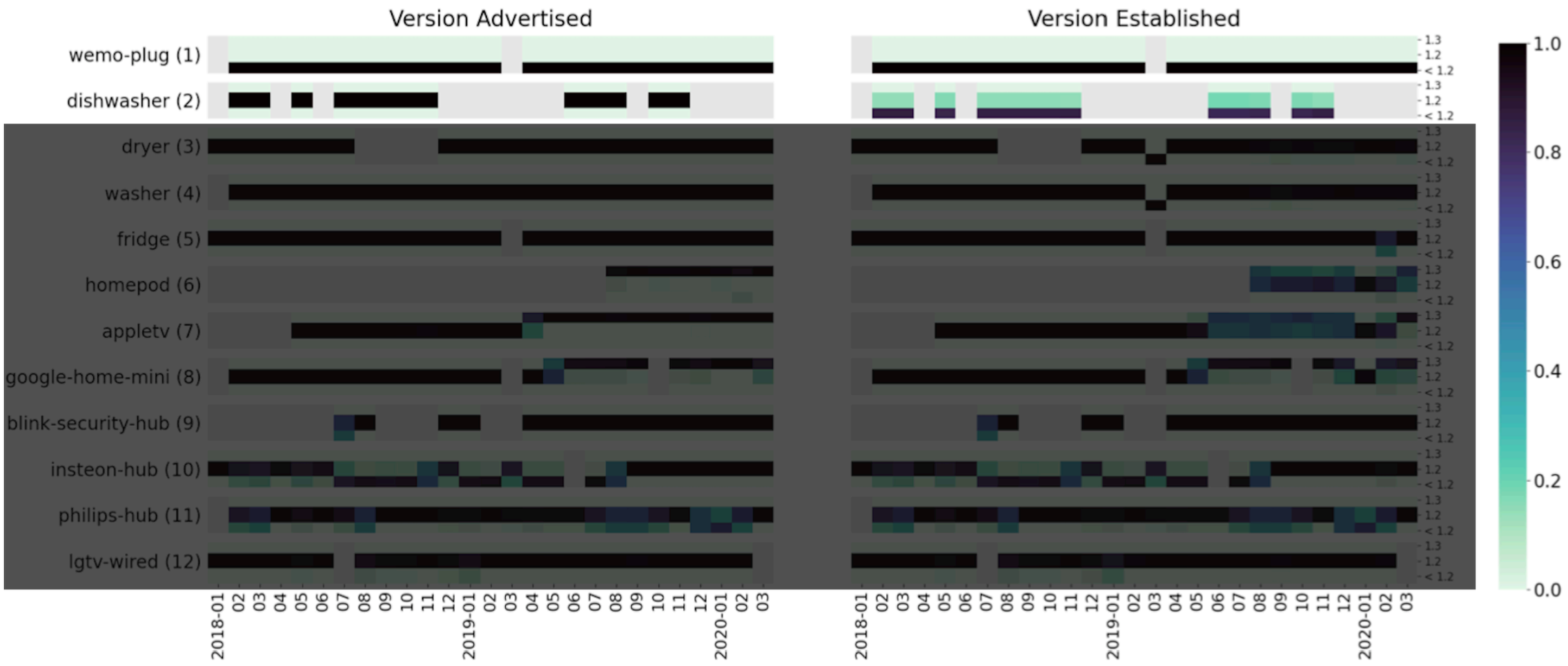


RQ1: TLS Connection Security (Passive)

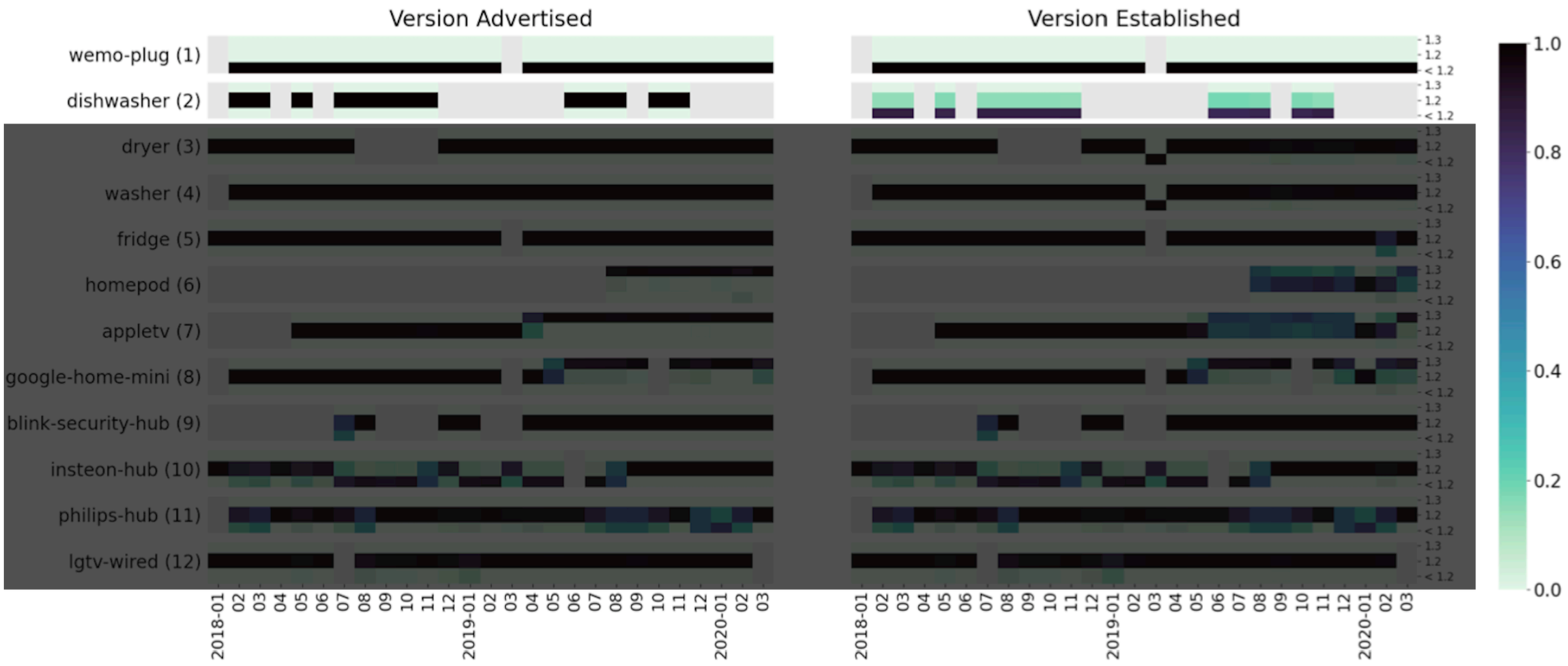


TLS version supported in IoT devices.

RQ1: TLS Connection Security (Passive)

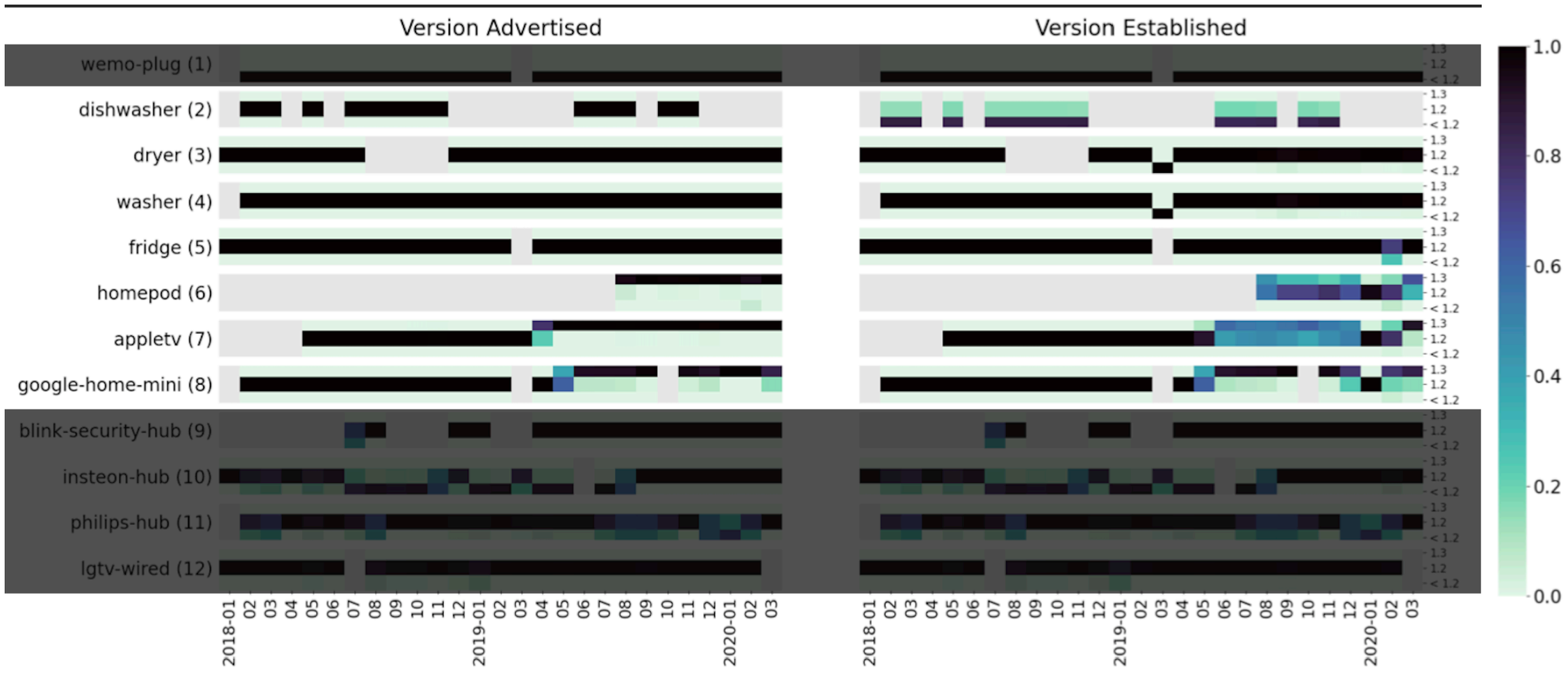


RQ1: TLS Connection Security (Passive)

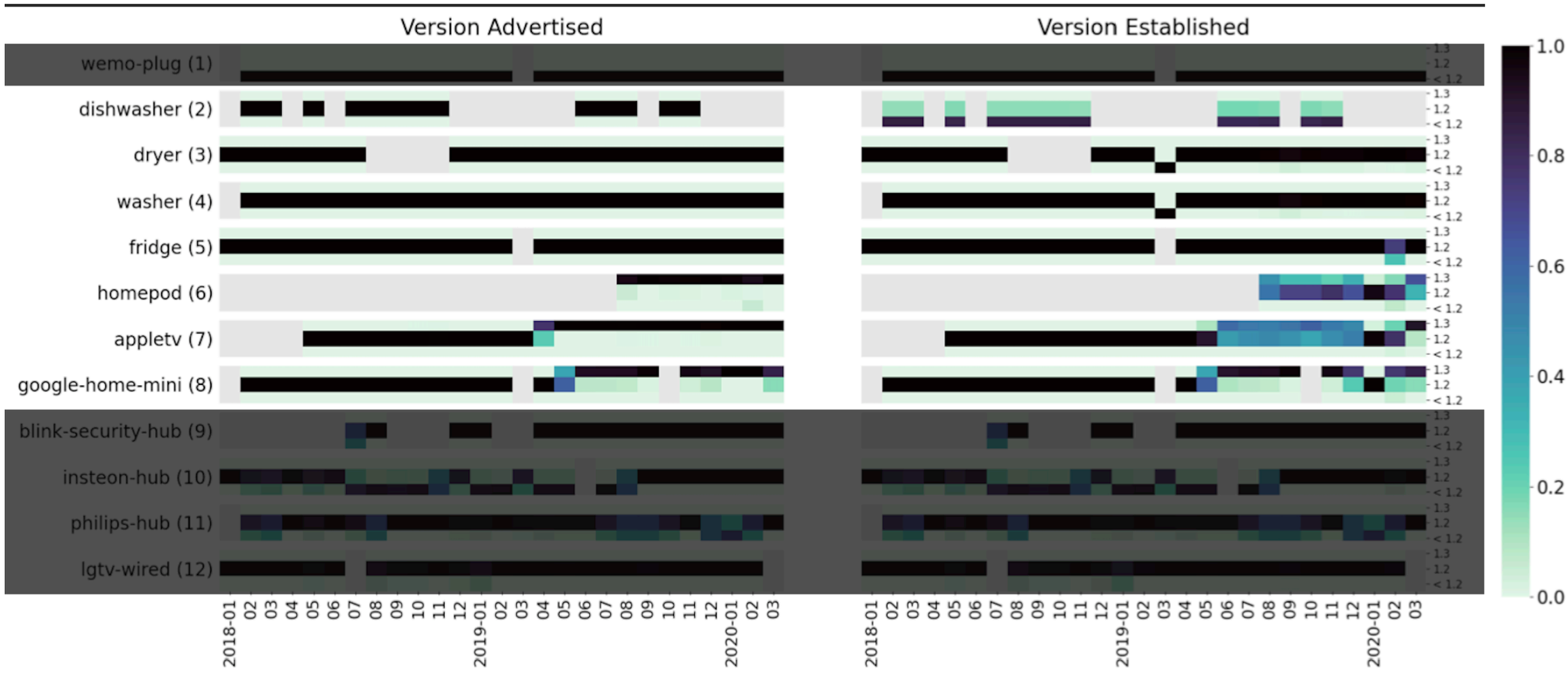


TLS version supported in IoT devices.

RQ1: TLS Connection Security (Passive)

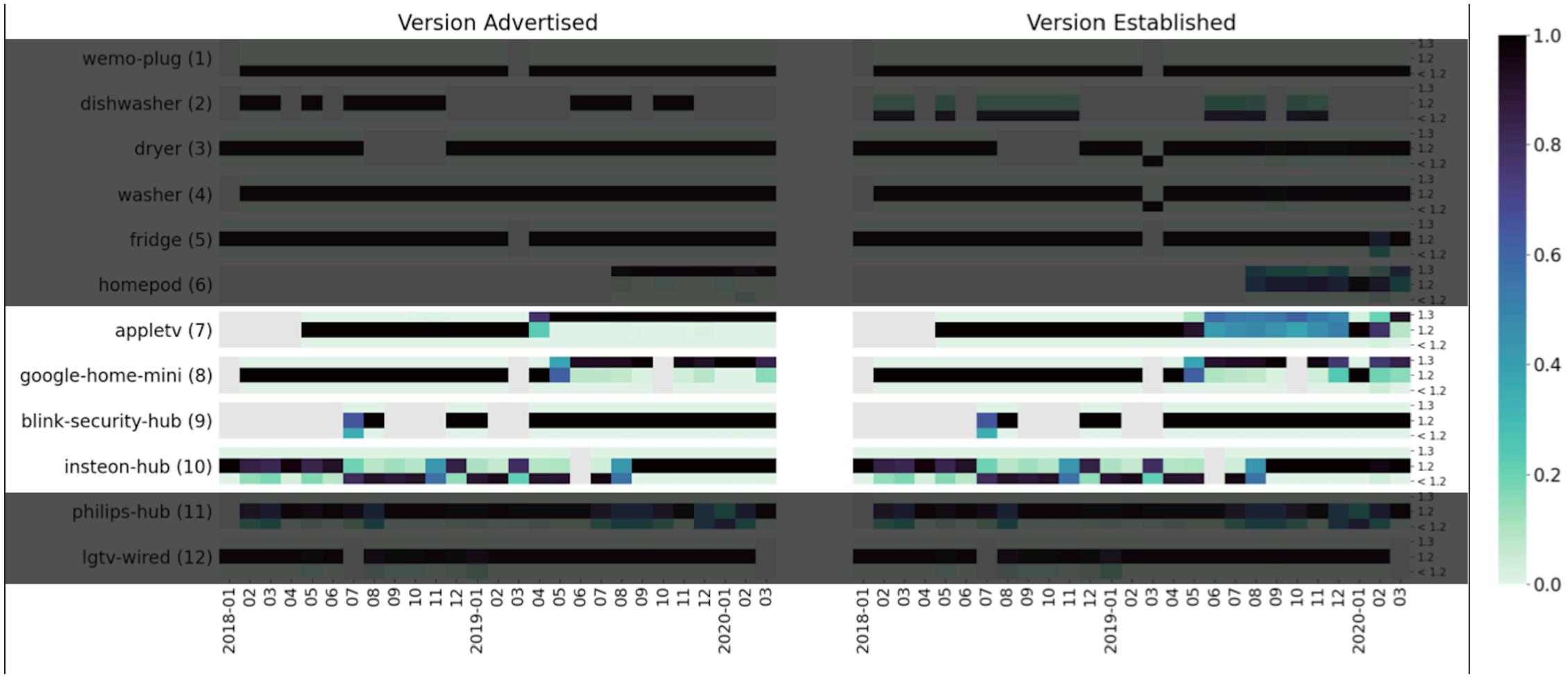


RQ1: TLS Connection Security (Passive)

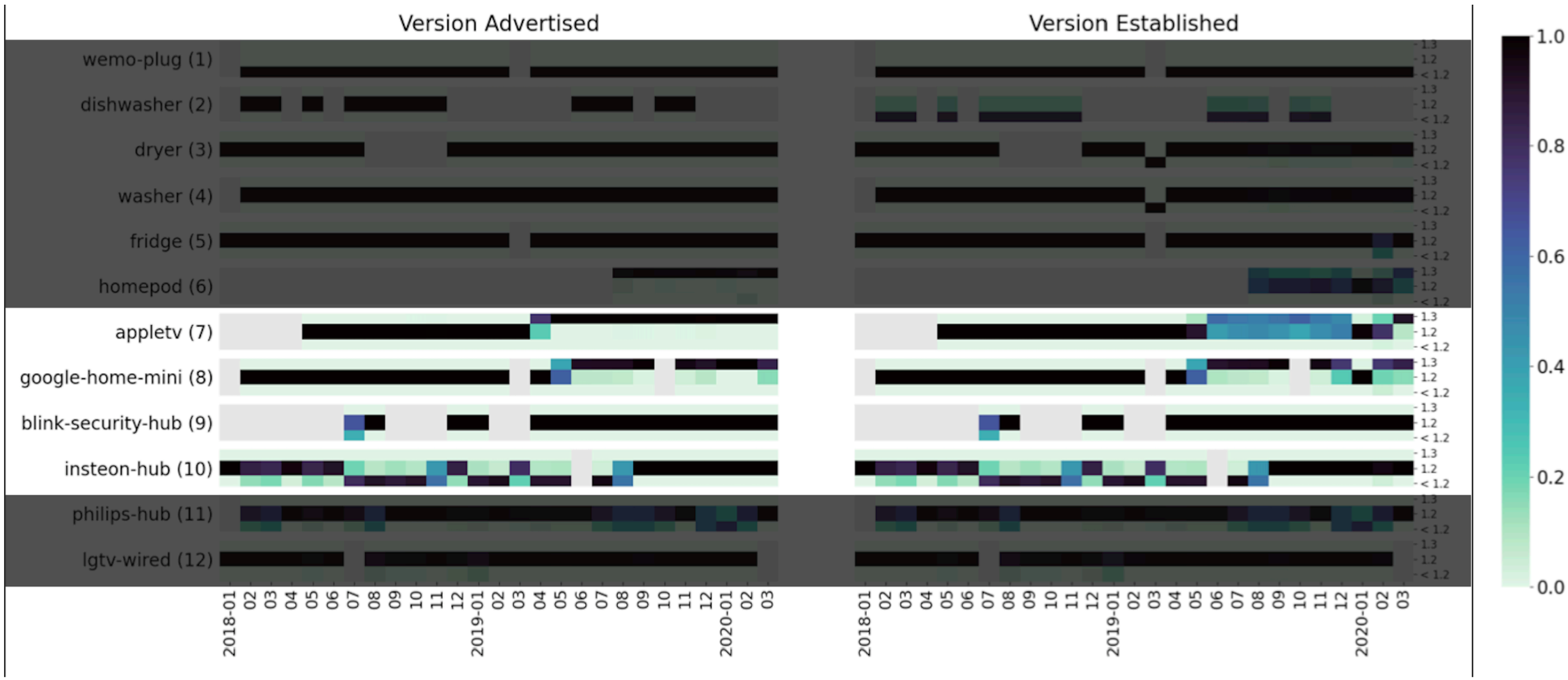


TLS version supported in IoT devices.

RQ1: TLS Connection Security (Passive)



RQ1: TLS Connection Security (Passive)



TLS version supported in IoT devices.

RQ1: TLS Connection Security (Active)

Device	TLS 1.0 Available?	TLS 1.1 Available?
Zmodo Doorbell	✓	✓
Wink Hub 2	✓	✓
Yi Camera	✓	✓
Philips Hub	✓	✓
Smarter Brewer	✓	✓
TP-Link Bulb	✓	✓
Roku TV	✓	✓
Meross Dooropener	✓	✓
LG TV	✓	✓
Google Home Mini	✓	✓
Amazon Fire TV	✓	✓
Amazon Echo Spot	✓	✓
Amazon Echo Plus	✓	✓
Amazon Echo Dot	✓	✓
Amcrest Camera	✓	✓
Samsung Fridge	✗	✓
Samsung Dryer	✗	✓
Wemo Plug	✓	✗

Device	Failed Handshake	Incomplete Handshake	Behavior	Downgraded / Total Destinations
Amazon Echo Dot	✗	✓	Falls back to using SSL 3.0	7 / 9
Amazon Echo Plus	✗	✓	Falls back to using SSL 3.0	6 / 7
Amazon Echo Spot	✗	✓	Falls back to using SSL 3.0	11 / 15
Amazon Fire TV	✗	✓	Falls back to using SSL 3.0	13 / 21
Apple Homepod	✗	✓	Falls back to using TLS 1.0	7 / 9
Google Home Mini	✗	✓	Falls back to supporting a weaker ciphersuite and signature algorithm (TLS_RSA_WITH_3DES_EDE_CBC_SHA and RSA_PKCS1_SHA1)	5 / 5
Roku TV	✓	✓	Falls back from offering 73 ciphersuites to just 1 (TLS_RSA_WITH_RC4_128_SHA)	8 / 15

RQ1: TLS Connection Security (Active)

Device	TLS 1.0 Available?	TLS 1.1 Available?
Zmodo Doorbell	✓	✓
Wink Hub 2	✓	✓
Yi Camera	✓	✓
Philips Hub	✓	✓
Smarter Brewer	✓	✓
TP-Link Bulb	✓	✓
Roku TV	✓	✓
Meross Dooropener	✓	✓
LG TV	✓	✓
Google Home Mini	✓	✓
Amazon Fire TV	✓	✓
Amazon Echo Spot	✓	✓
Amazon Echo Plus	✓	✓
Amazon Echo Dot	✓	✓
Amcrest Camera	✓	✓
Samsung Fridge	✗	✓
Samsung Dryer	✗	✓
Wemo Plug	✓	✗

Device	Failed Handshake	Incomplete Handshake	Behavior	Downgraded / Total Destinations
Amazon Echo Dot	✗	✓	Falls back to using SSL 3.0	7 / 9
Amazon Echo Plus	✗	✓	Falls back to using SSL 3.0	6 / 7
Amazon Echo Spot	✗	✓	Falls back to using SSL 3.0	11 / 15
Amazon Fire TV	✗	✓	Falls back to using SSL 3.0	13 / 21
Apple Homepod	✗	✓	Falls back to using TLS 1.0	7 / 9
Google Home Mini	✗	✓	Falls back to supporting a weaker ciphersuite and signature algorithm (TLS_RSA_WITH_3DES_EDE_CBC_SHA and RSA_PKCS1_SHA1)	5 / 5
Roku TV	✓	✓	Falls back from offering 73 ciphersuites to just 1 (TLS_RSA_WITH_RC4_128_SHA)	8 / 15

7 IoT devices that downgrade security upon connection failures.

RQ1: TLS Connection Security (Active)

Device	TLS 1.0 Available?	TLS 1.1 Available?
Zmodo Doorbell	✓	✓
Wink Hub 2	✓	✓
Yi Camera	✓	✓
Philips Hub	✓	✓
Smarter Brewer	✓	✓
TP-Link Bulb	✓	✓
Roku TV	✓	✓
Meross Dooropener	✓	✓
LG TV	✓	✓
Google Home Mini	✓	✓
Amazon Fire TV	✓	✓
Amazon Echo Spot	✓	✓
Amazon Echo Plus	✓	✓
Amazon Echo Dot	✓	✓
Amcrest Camera	✓	✓
Samsung Fridge	✗	✓
Samsung Dryer	✗	✓
Wemo Plug	✓	✗

18 IoT devices that support older TLS versions.

Device	Failed Handshake	Incomplete Handshake	Behavior	Downgraded / Total Destinations
Amazon Echo Dot	✗	✓	Falls back to using SSL 3.0	7 / 9
Amazon Echo Plus	✗	✓	Falls back to using SSL 3.0	6 / 7
Amazon Echo Spot	✗	✓	Falls back to using SSL 3.0	11 / 15
Amazon Fire TV	✗	✓	Falls back to using SSL 3.0	13 / 21
Apple Homepod	✗	✓	Falls back to using TLS 1.0	7 / 9
Google Home Mini	✗	✓	Falls back to supporting a weaker ciphersuite and signature algorithm (TLS_RSA_WITH_3DES_EDE_CBC_SHA and RSA_PKCS1_SHA1)	5 / 5
Roku TV	✓	✓	Falls back from offering 73 ciphersuites to just 1 (TLS_RSA_WITH_RC4_128_SHA)	8 / 15

7 IoT devices that downgrade security upon connection failures.

RQ2: TLS Certificate Validation

Device	No-Validation	InvalidBasic-Constraints	Wrong-Hostname	Vulnerable/Total Destinations
Zmodo Doorbell	✓	✓	✓	6 / 6
Amcrest Camera	✓	✓	✓	2 / 2
Smarter Brewer	✓	✓	✓	1 / 1
Yi Camera	✓	✓	✓	1 / 1
Wink Hub 2	✓	✓	✓	1 / 2
LG TV	✓	✓	✓	1 / 2
Smartthings Hub	✓	✓	✓	1 / 3
Amazon Echo Plus	✗	✗	✓	1 / 8
Amazon Echo Dot	✗	✗	✓	1 / 9
Amazon Echo Spot	✗	✗	✓	1 / 17
Amazon Fire TV	✗	✗	✓	1 / 21

RQ2: TLS Certificate Validation

- 11 devices are vulnerable to TLS interception attacks.

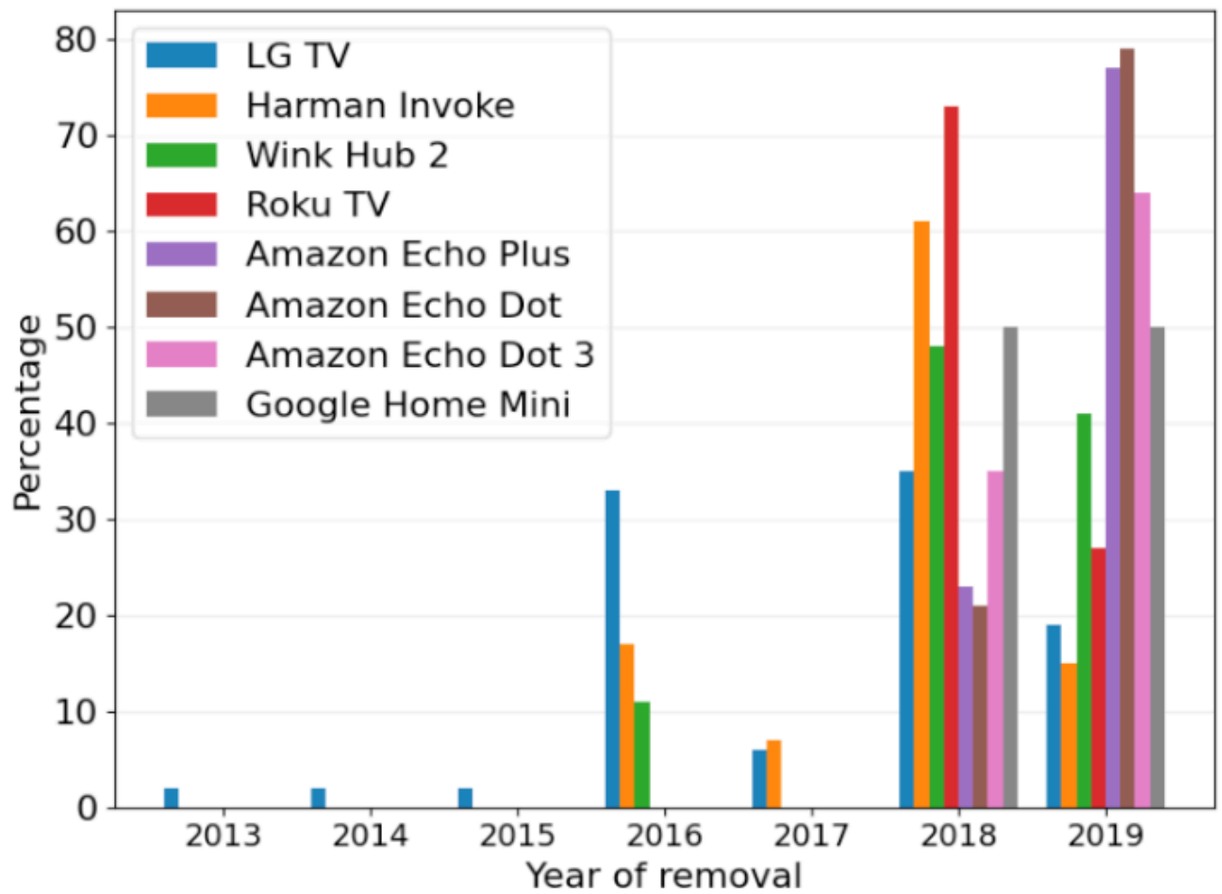
Device	No-Validation	InvalidBasic-Constraints	Wrong-Hostname	Vulnerable/Total Destinations
Zmodo Doorbell	✓	✓	✓	6 / 6
Amcrest Camera	✓	✓	✓	2 / 2
Smarter Brewer	✓	✓	✓	1 / 1
Yi Camera	✓	✓	✓	1 / 1
Wink Hub 2	✓	✓	✓	1 / 2
LG TV	✓	✓	✓	1 / 2
Smartthings Hub	✓	✓	✓	1 / 3
Amazon Echo Plus	✗	✗	✓	1 / 8
Amazon Echo Dot	✗	✗	✓	1 / 9
Amazon Echo Spot	✗	✗	✓	1 / 17
Amazon Fire TV	✗	✗	✓	1 / 21

RQ2: TLS Certificate Validation

- 11 devices are vulnerable to TLS interception attacks.
- 7 vulnerable devices contained sensitive data that can be exposed to attackers.

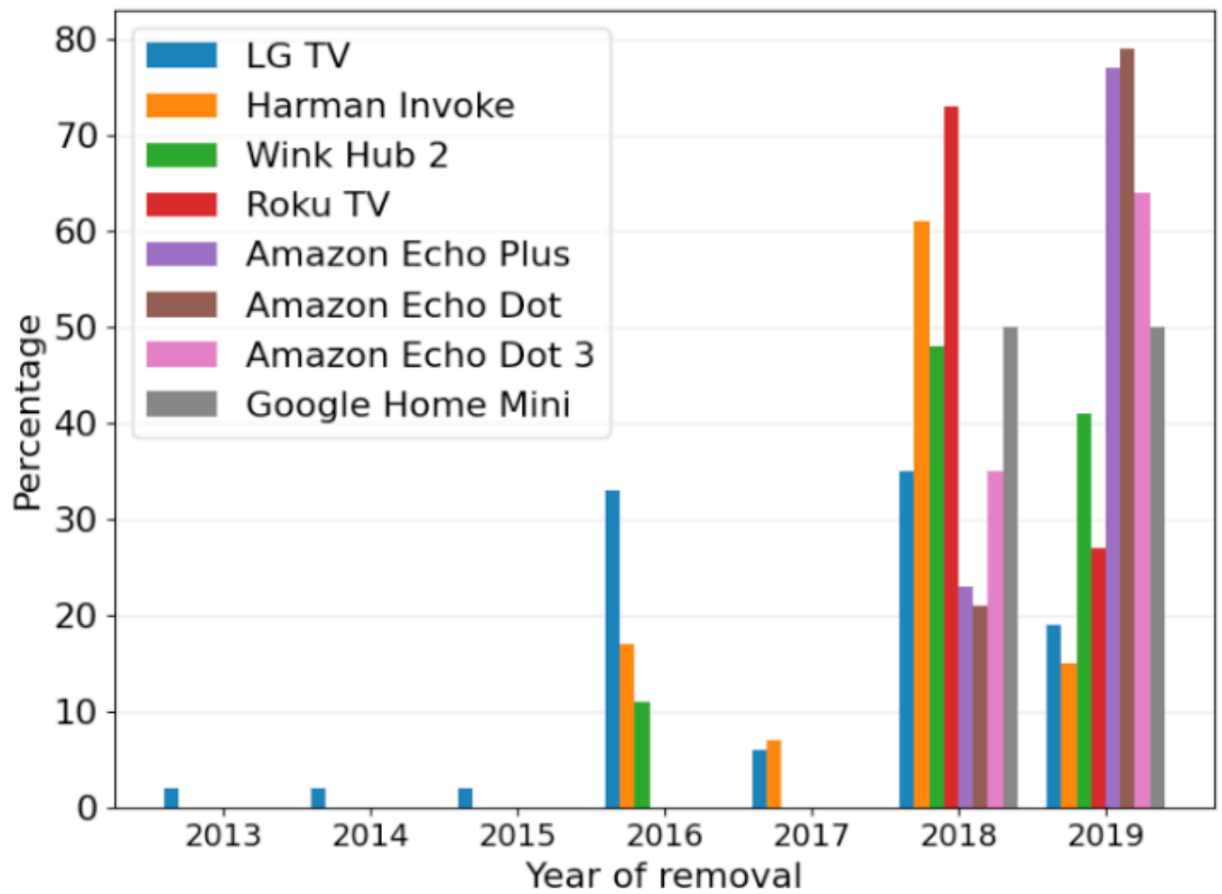
Device	No-Validation	InvalidBasic-Constraints	Wrong-Hostname	Vulnerable/Total Destinations
Zmodo Doorbell	✓	✓	✓	6 / 6
Amcrest Camera	✓	✓	✓	2 / 2
Smarter Brewer	✓	✓	✓	1 / 1
Yi Camera	✓	✓	✓	1 / 1
Wink Hub 2	✓	✓	✓	1 / 2
LG TV	✓	✓	✓	1 / 2
Smartthings Hub	✓	✓	✓	1 / 3
Amazon Echo Plus	✗	✗	✓	1 / 8
Amazon Echo Dot	✗	✗	✓	1 / 9
Amazon Echo Spot	✗	✗	✓	1 / 17
Amazon Fire TV	✗	✗	✓	1 / 21

RQ2: TLS Certificate Validation



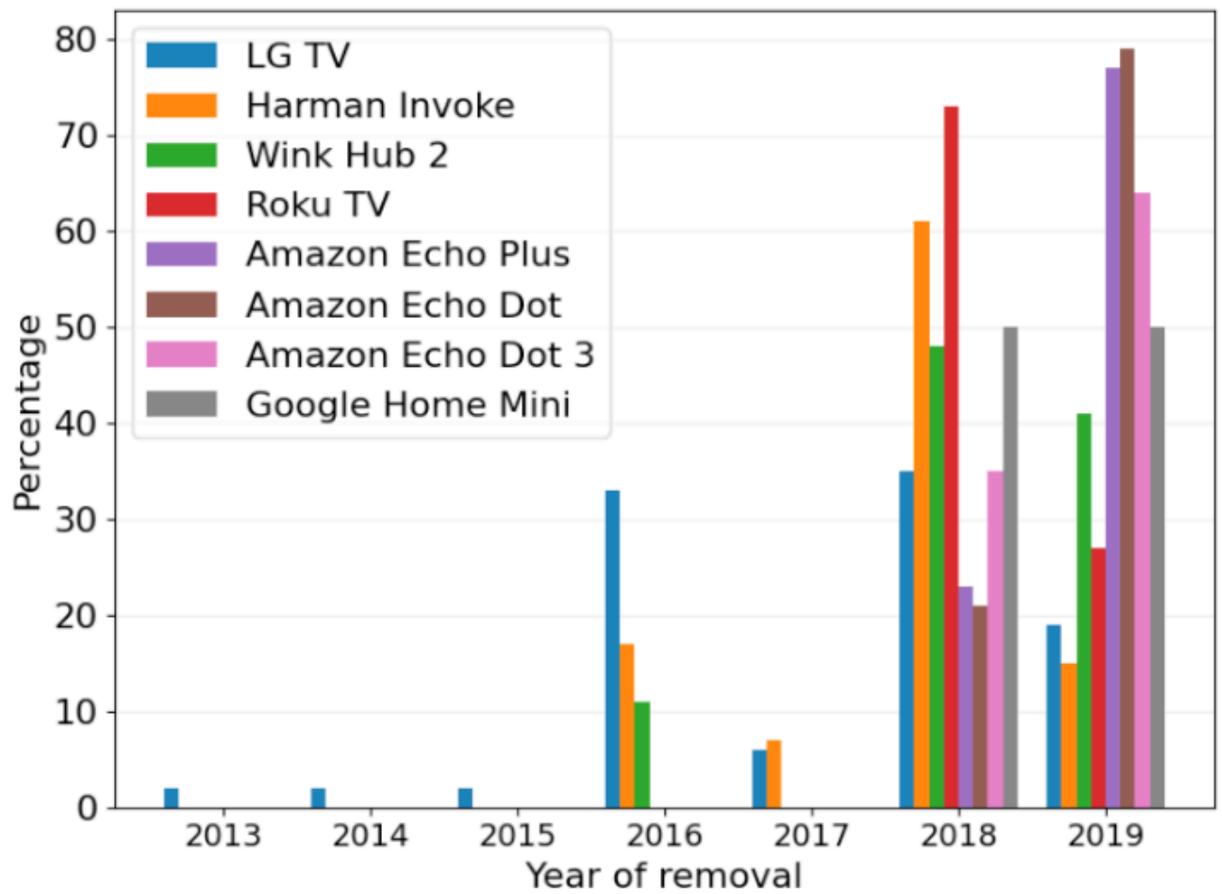
RQ2: TLS Certificate Validation

- All 8 devices trust at-least-one CA certificate that is ***explicitly distrusted*** by one of the major platforms (i.e., Chrome, Firefox, Ubuntu, Microsoft).

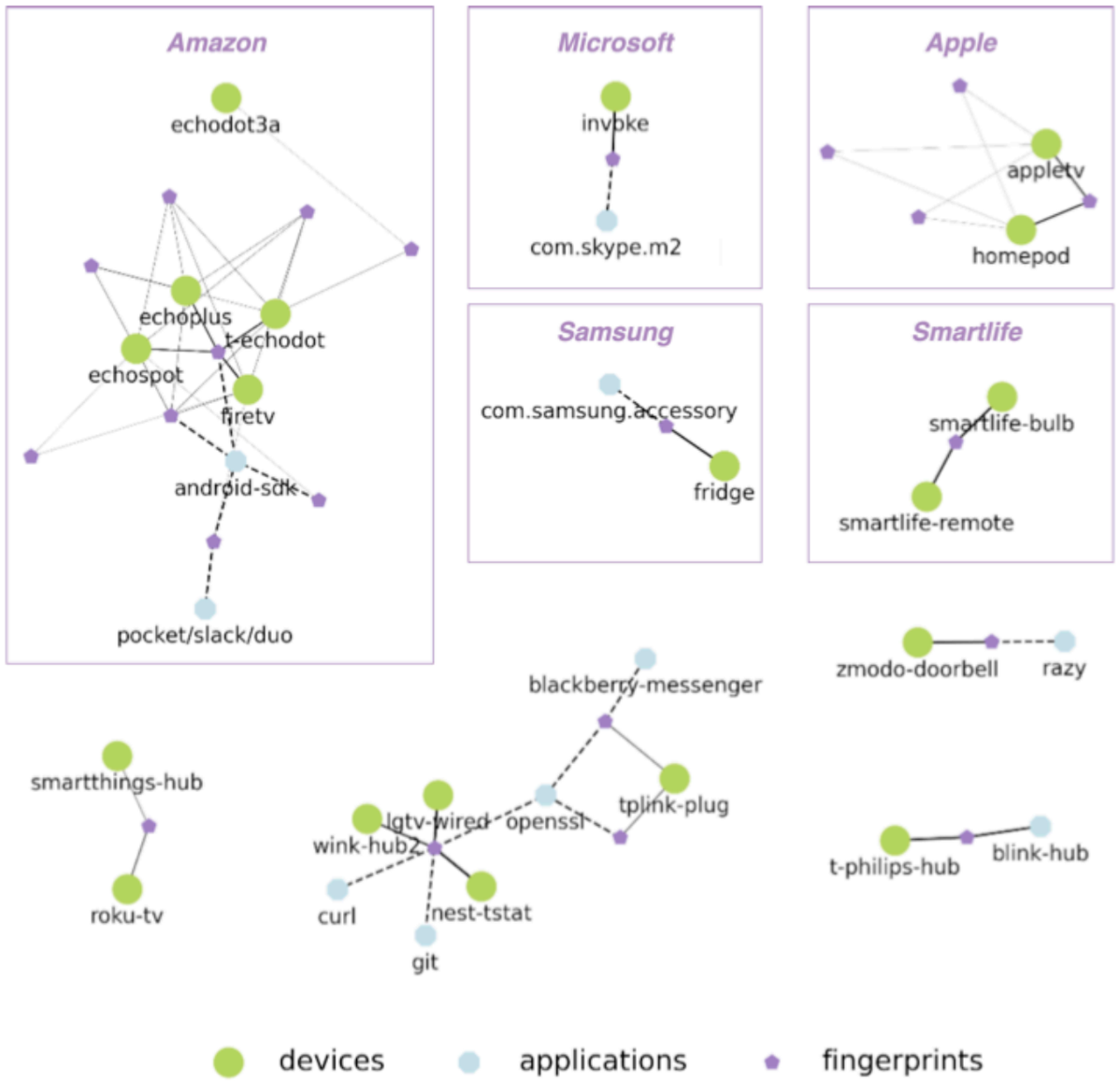


RQ2: TLS Certificate Validation

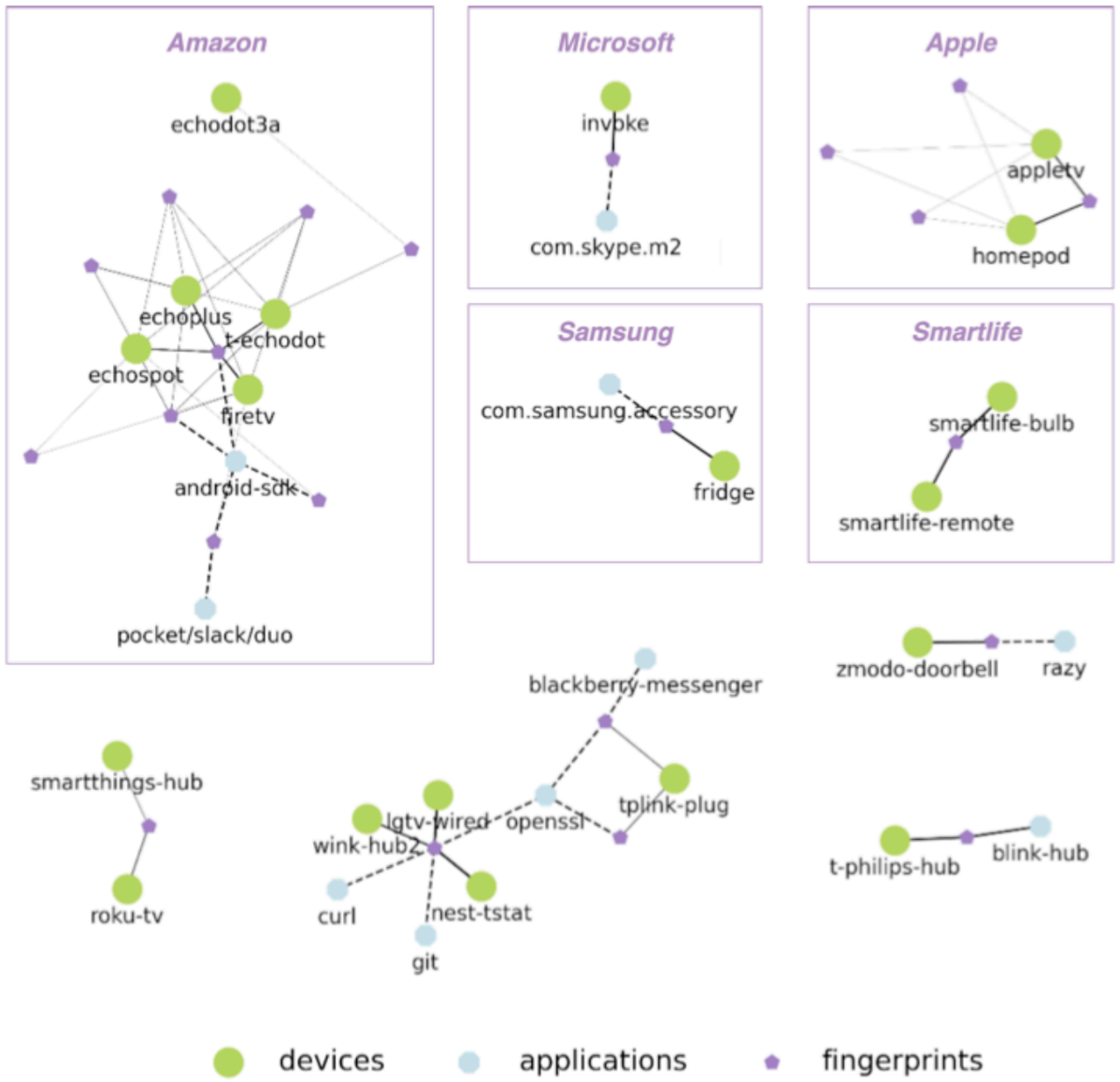
- All 8 devices trust at-least-one CA certificate that is ***explicitly distrusted*** by one of the major platforms (i.e., Chrome, Firefox, Ubuntu, Microsoft).
- Some devices trust CA certificates as old as 2013.



RQ3: Diversity of Behaviors

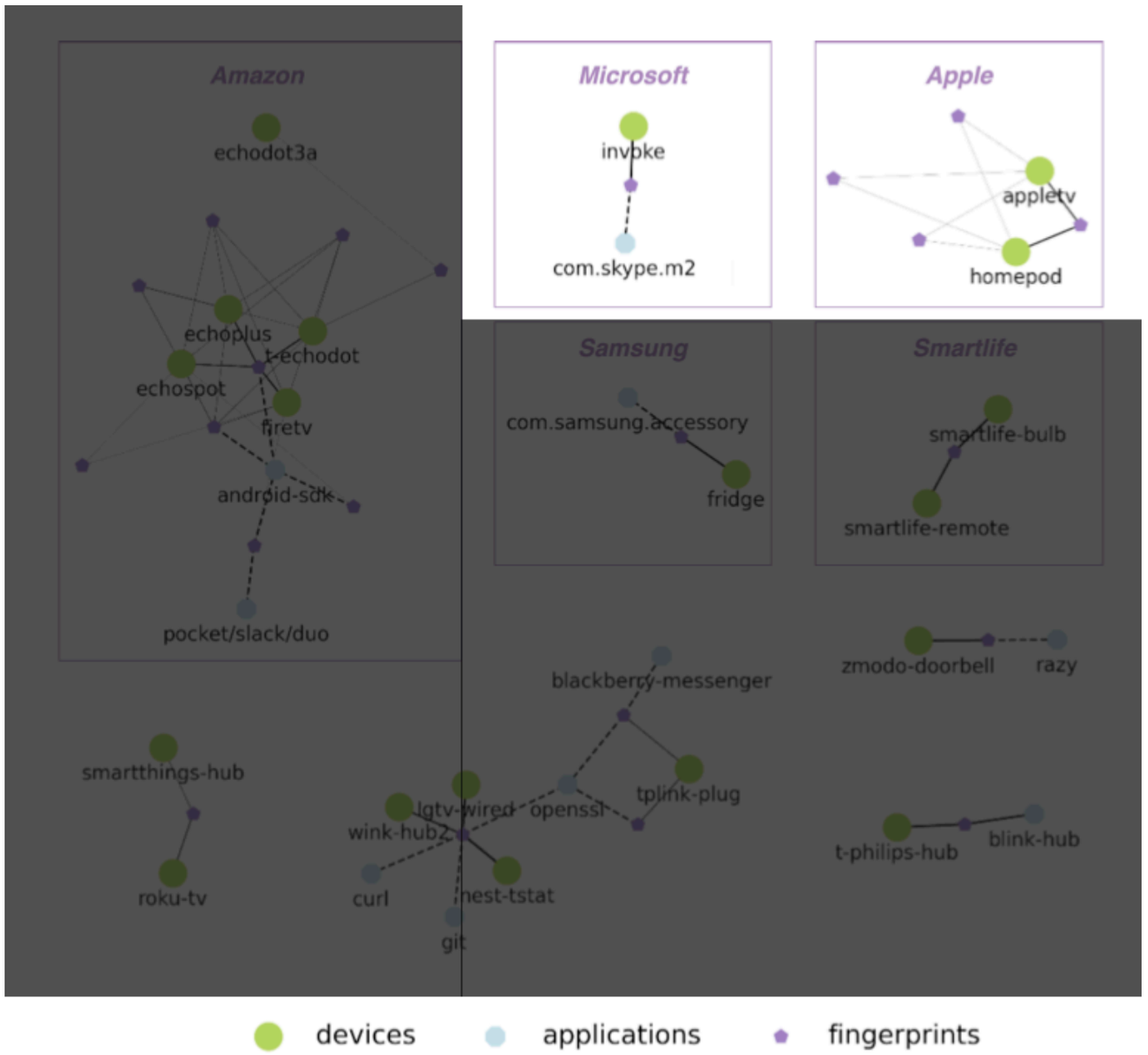


RQ3: Diversity of Behaviors

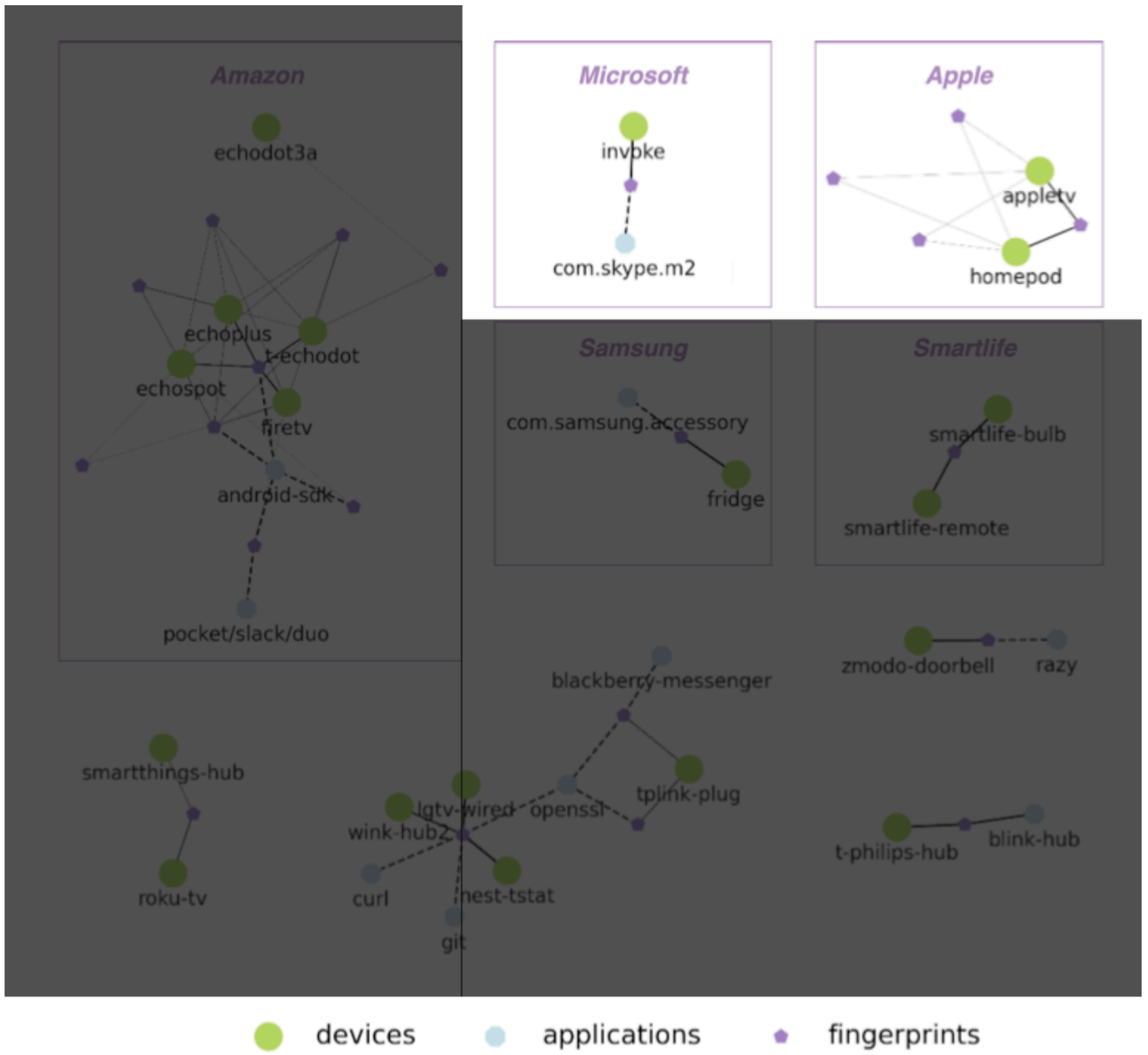


IoT devices that share TLS fingerprints with other devices and applications.

RQ3: Diversity of Behaviors

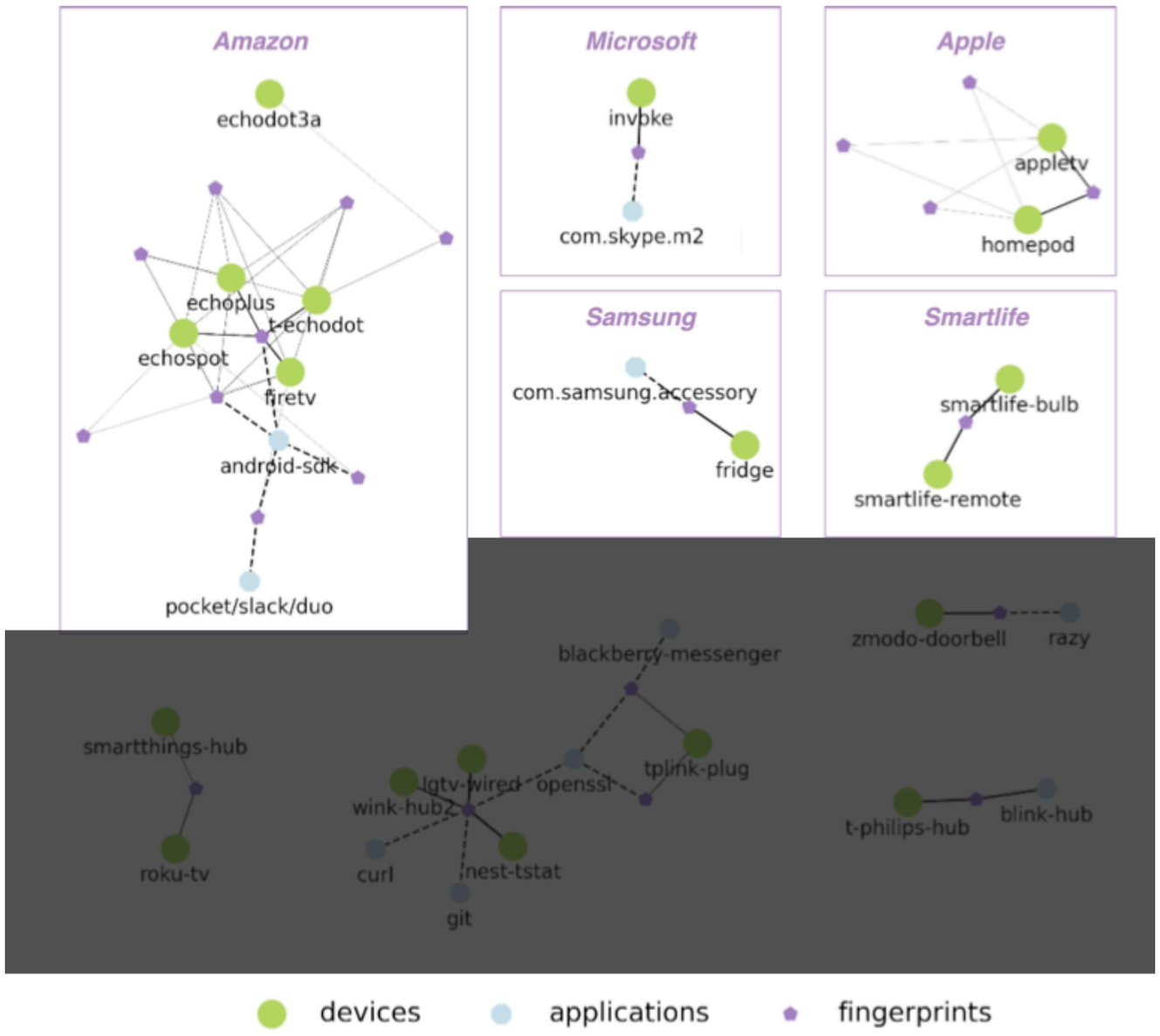


RQ3: Diversity of Behaviors



IoT devices that share TLS fingerprints with other devices and applications.

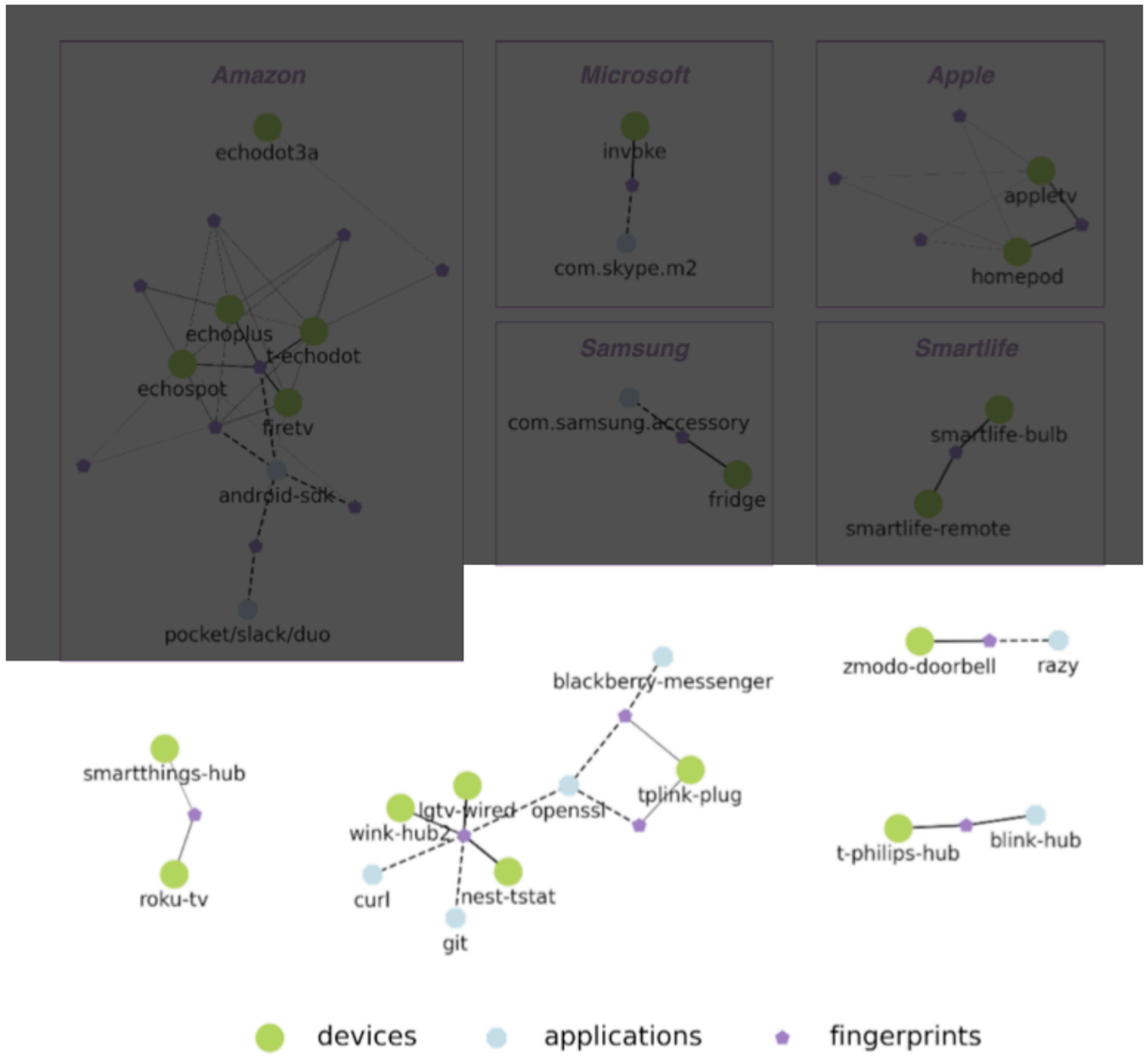
RQ3: Diversity of Behaviors



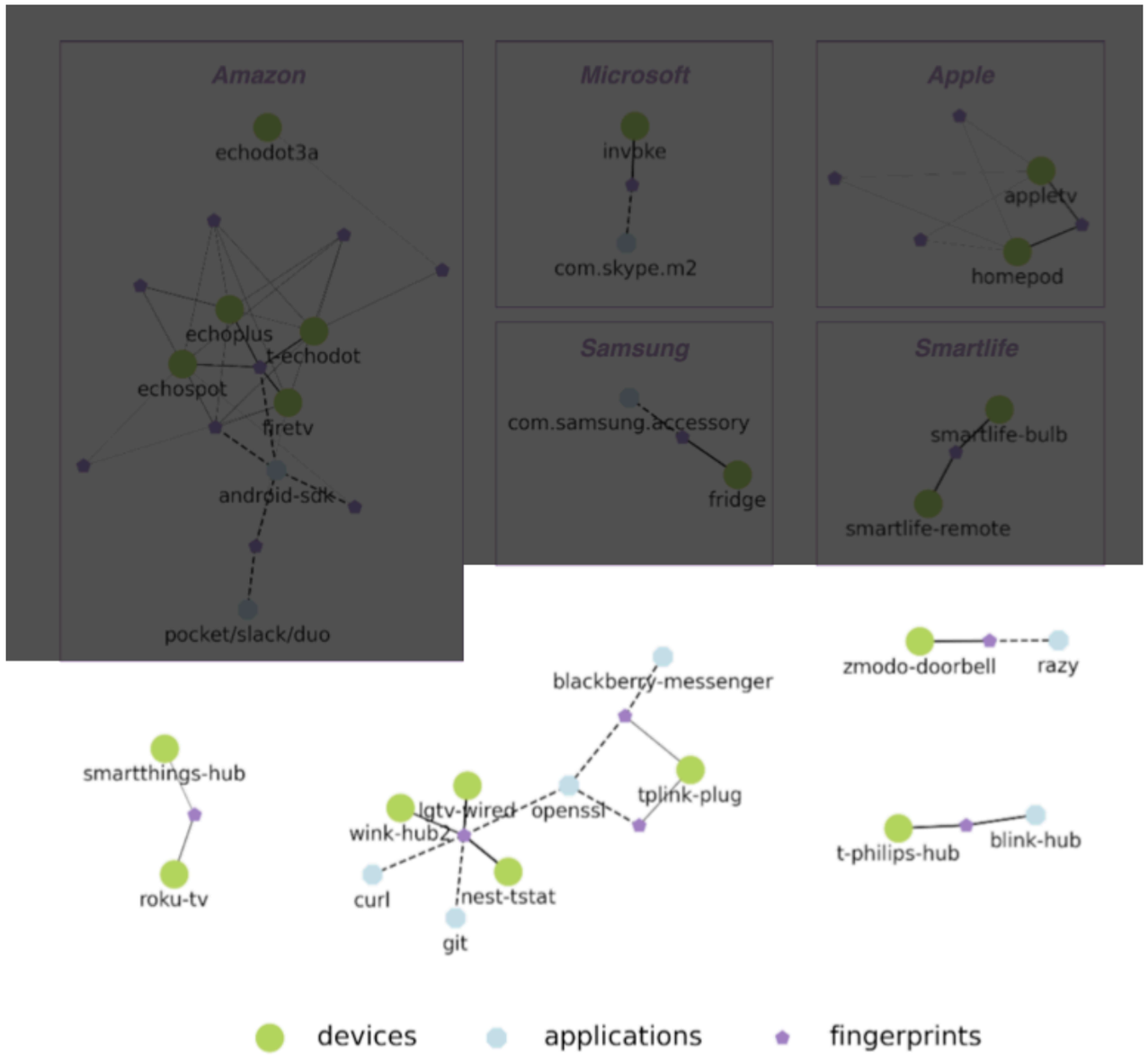
RQ3: Diversity of Behaviors

IoT devices that share TLS fingerprints with other devices and applications.

RQ3: Diversity of Behaviors



RQ3: Diversity of Behaviors



IoT devices that share TLS fingerprints with other devices and applications.