HomeScan: Scrutinizing Implementations of Smart Home Integrations

ICECCS'18, 12 December 2018

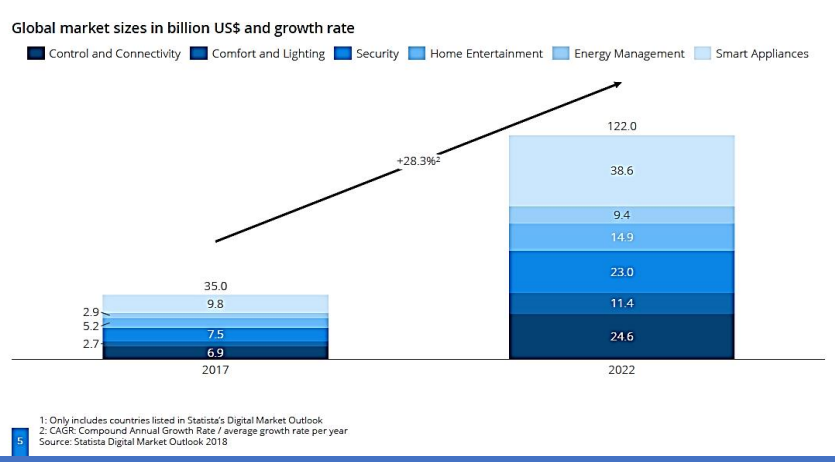
Kulani Mahadewa, Kailong Wang, Guangdong Bai, Ling Shi, Jin Song Dong and Zhenkai Liang

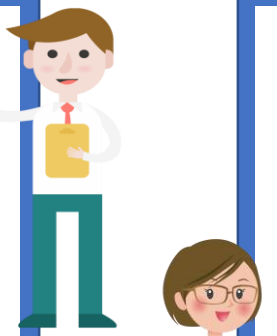
Background

IoT-enhanced smart home is getting popular

The global[1] Smart Home market is worth US$35.0 billion in 2017 and is expected to grow even bigger

Smart Home overview (3/4)





JUNIPER RESEARCH

HARVEST ACCESS

HOME · SUBSCRIPTIONS · RESEARCHSTORE · SERVICES · HARVEST · CONSULTANCY

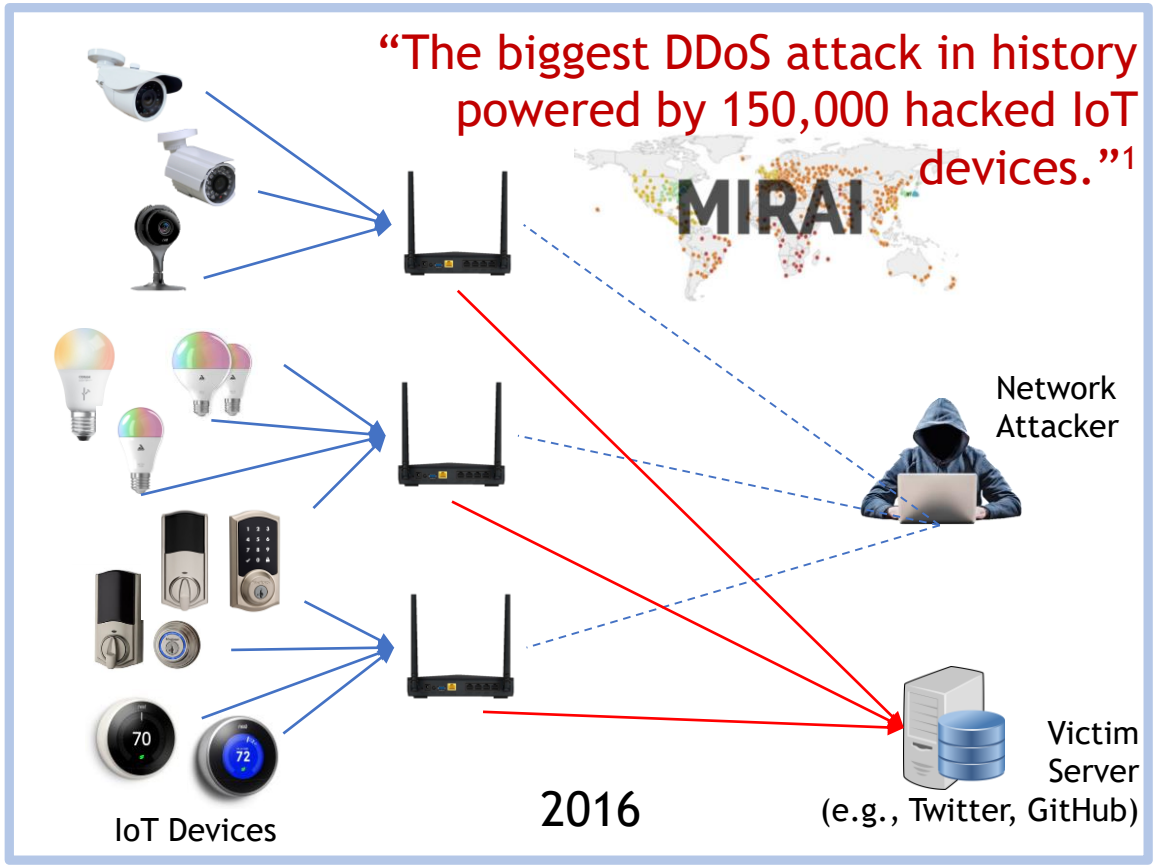
Home > Press > Press releases > Smart Home Revenues to Reach $100 Billion by 2020, Driven by Automation and En

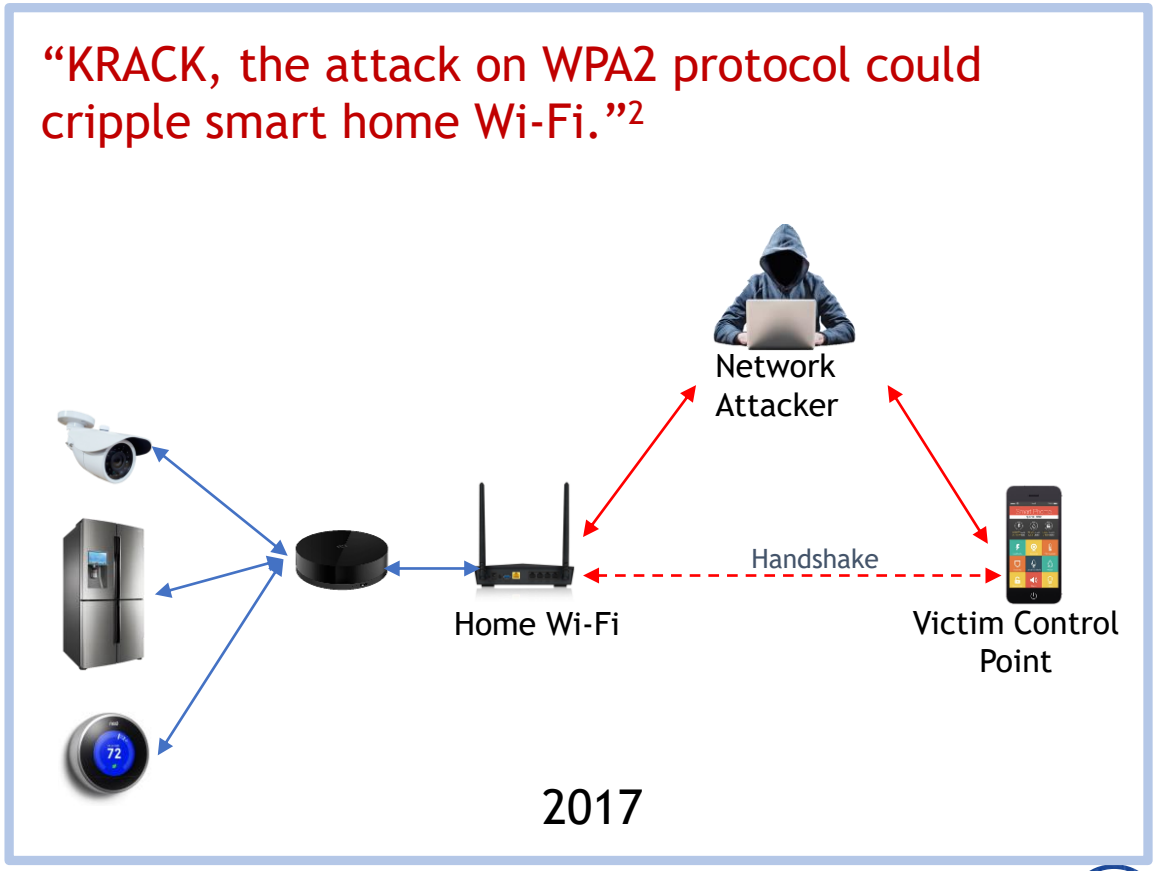
SMART HOME REVENUES TO REACH $100 BILLION BY 2020, DRIVEN BY AUTOMATION AND ENTERTAINMENT SERVICES

Connected Entertainment Leads, But the Gap is Closing

1 https://www.statista.com/study/42112/smart-home-report/
2 https://www.juniperresearch.com/press/press-releases/smart-home-revenues-to-reach-$100-billion-by-2020

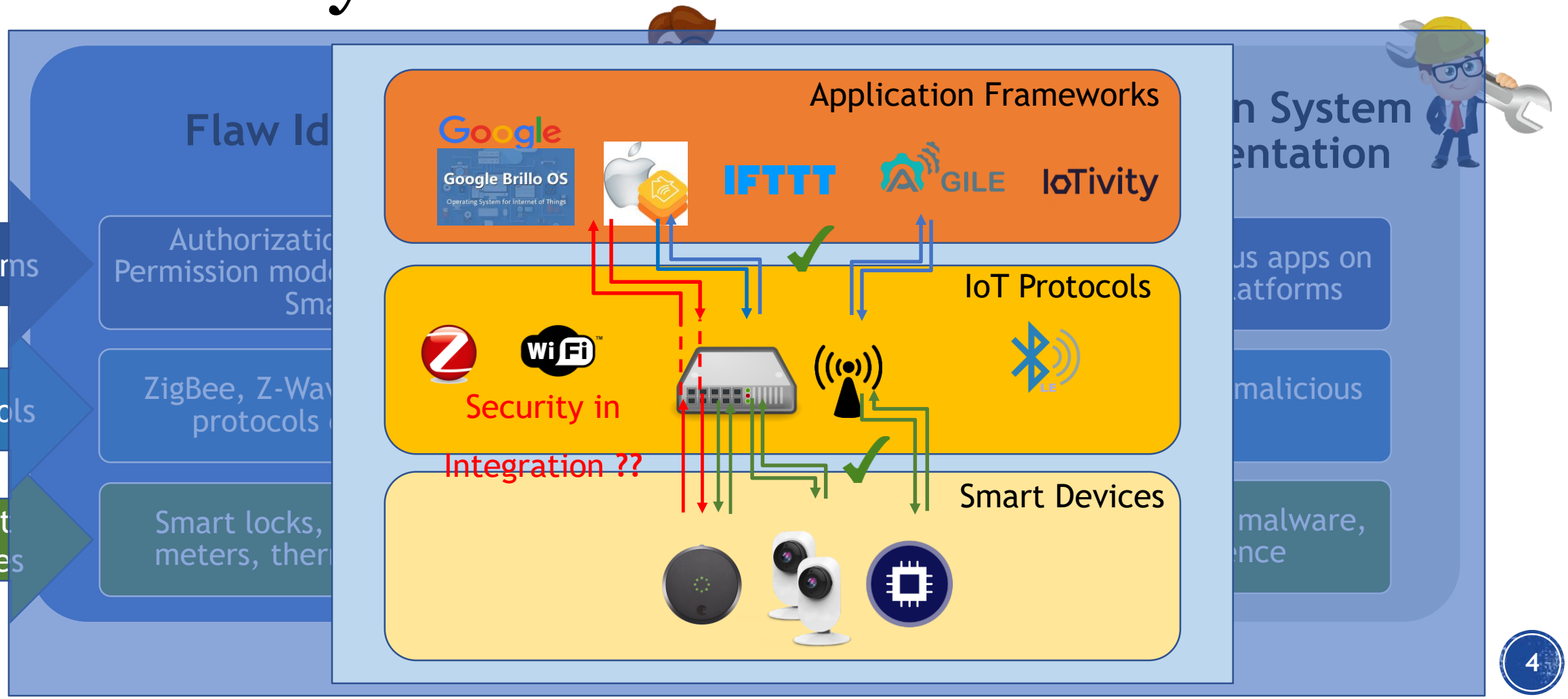
Smart Home Vulnerable to Attacks !



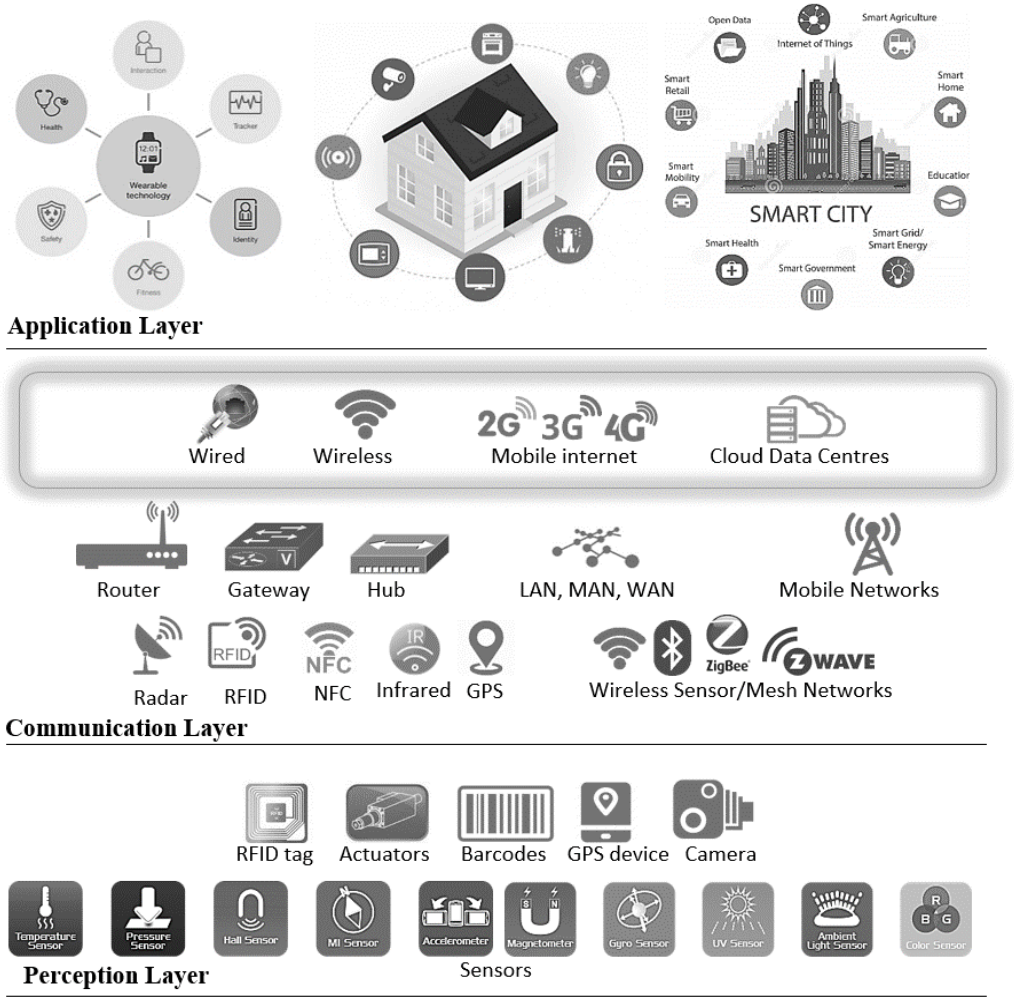


1 http://www.bbc.com/news/technology-37738823
2 http://www.bbc.com/news/av/technology-41641814/krack-wi-fi-security-flaw-explained

Existing Work on Smart Home Security



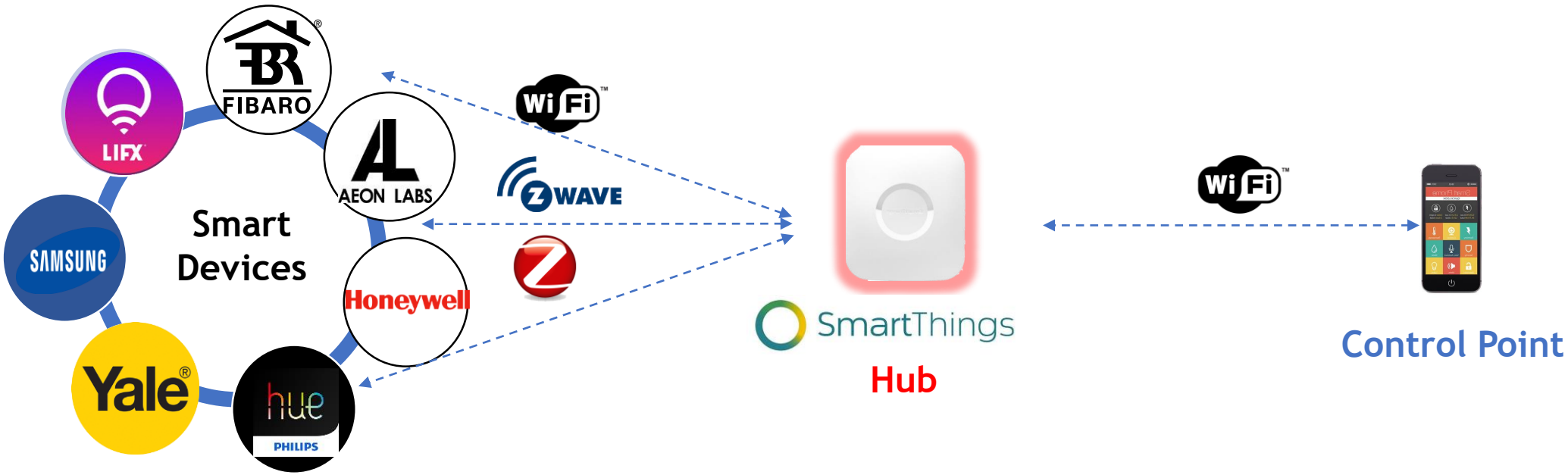
Security of Smart Home Integration



- Causes of insecurity when integrating a smart home system.
  1) Incompatibilities
  2) Invalidated assumptions

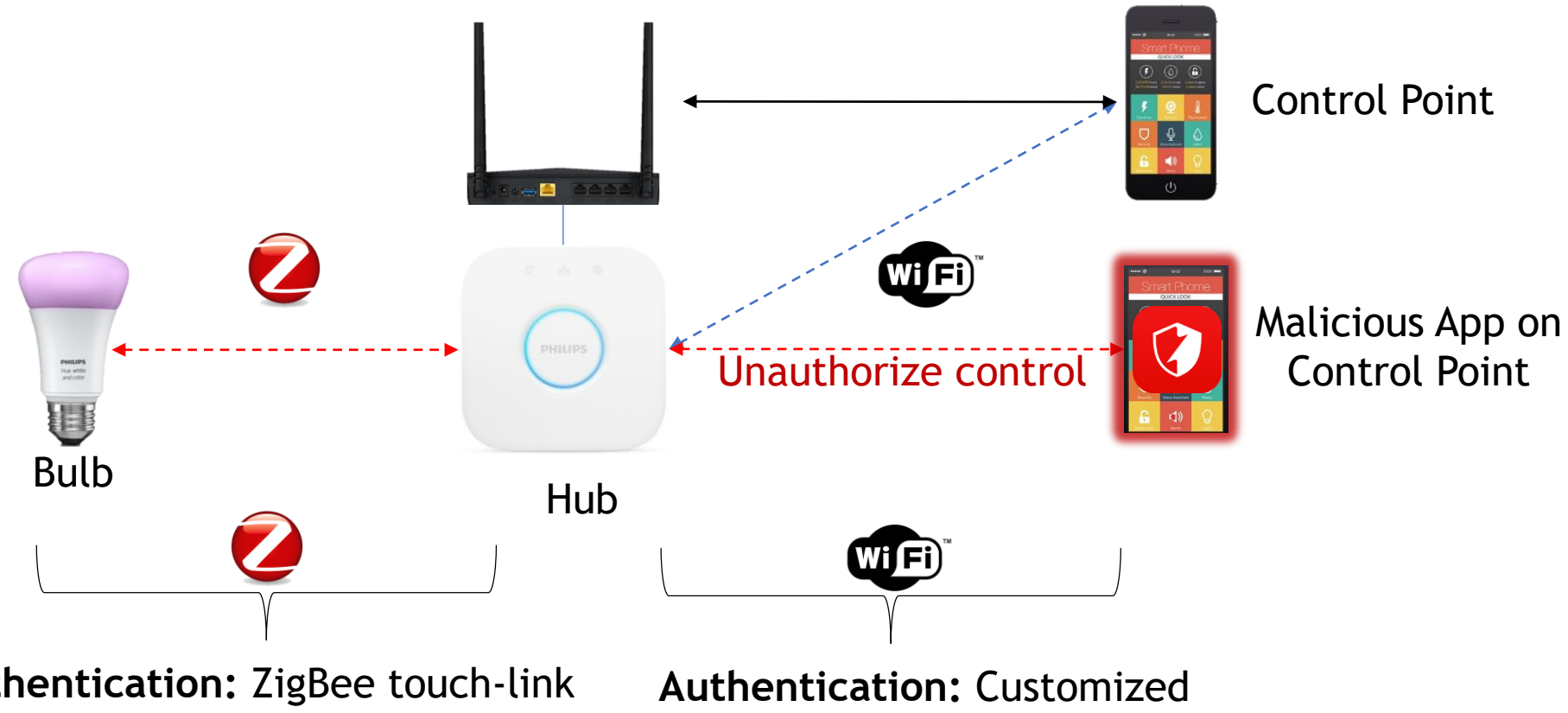
Incompatibilities in Integration (1)

Wide assortments of technologies and devices manufactured by diverse vendors.



Incompatibilities in Integration (2)

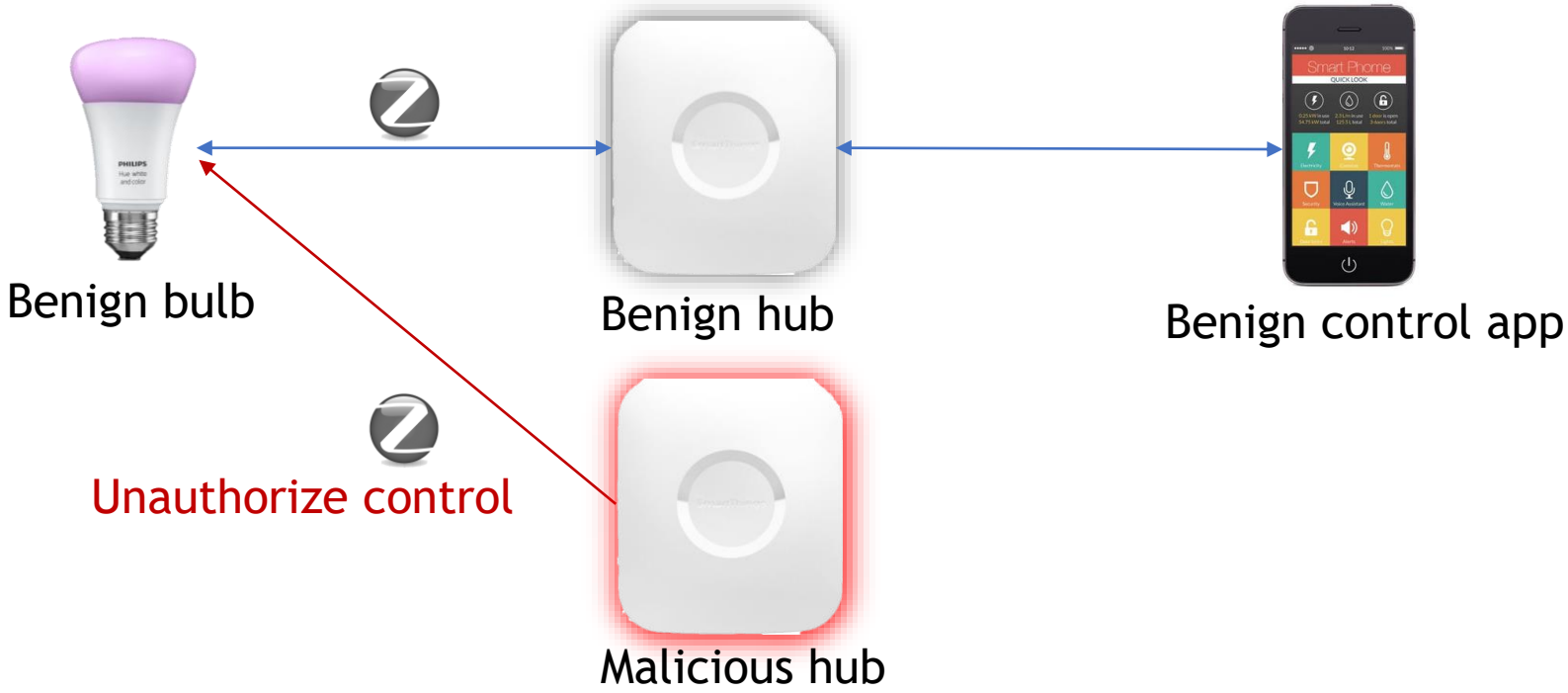
E.g. Smart bulb cannot verify the identity of the control point.



Invalidated Assumptions

Manufactures make assumptions to reduce complexity and cost in building smart home systems.

- Home Wi-Fi is secure. ✗
- Implicit trust on other components in the integrated system. ✗



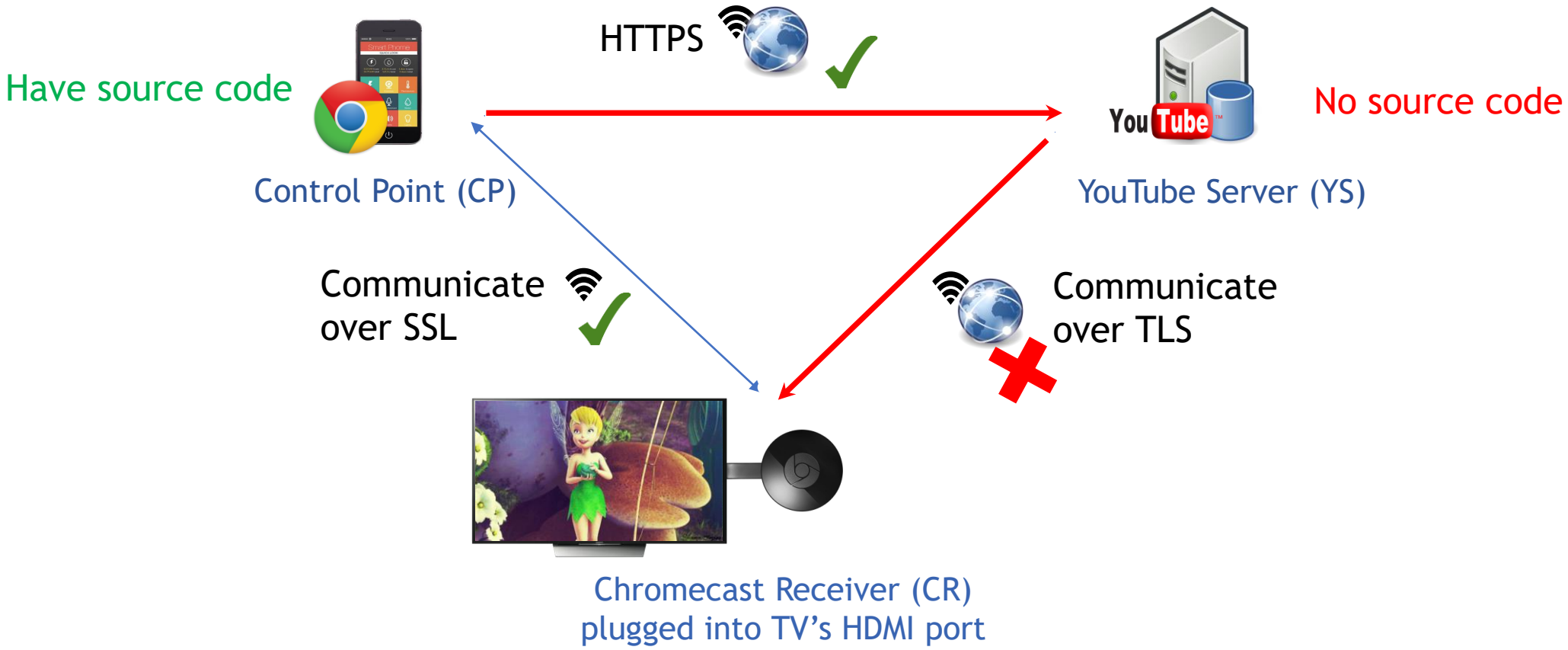
Our Solution: HomeScan

Extract the abstract specification of application-layer protocols and security-relevant internal behaviours from the implementation, and analysing security of the specification.

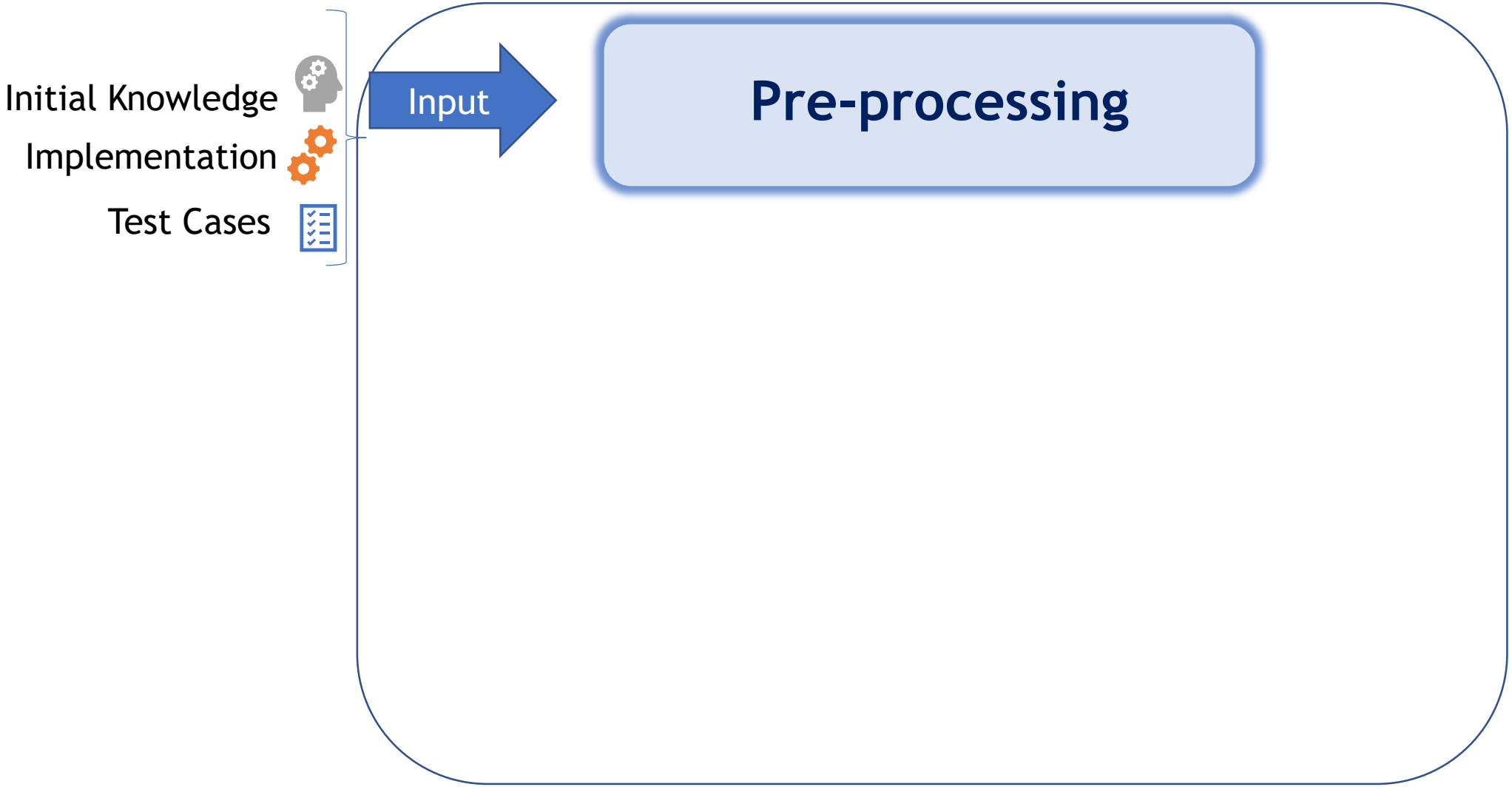
Challenges: Partial availability of the implementations.

- Unavailability of source code, and only executables/libraries provided by the vendors available.
- Communication is not clear due to use of cryptographic protocols.

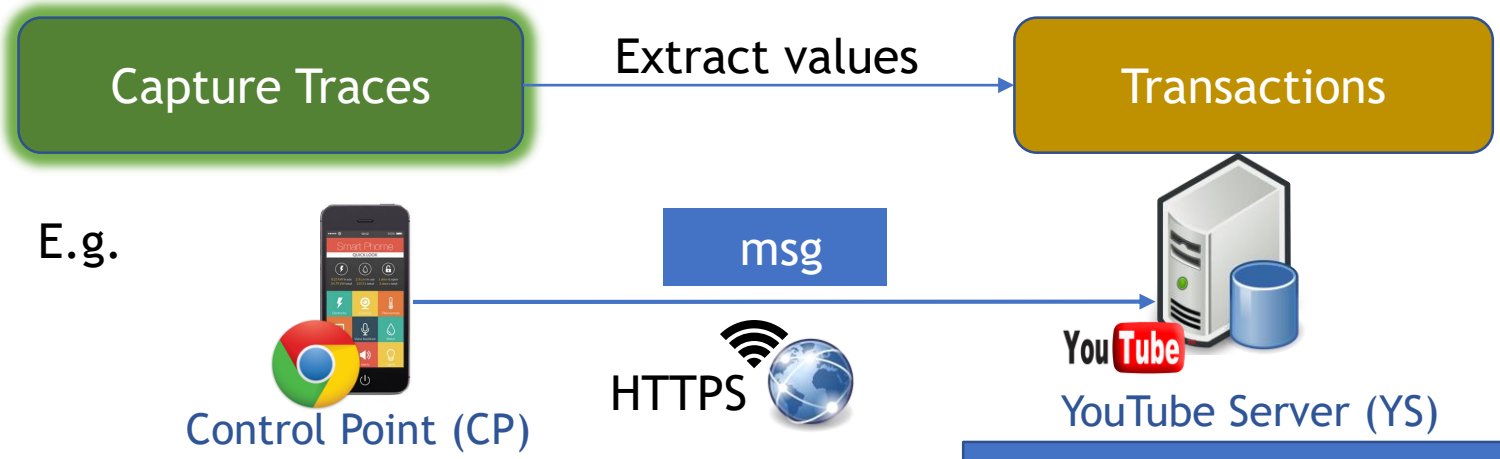
Running Example – Chromecast



Our Approach



Pre-processing

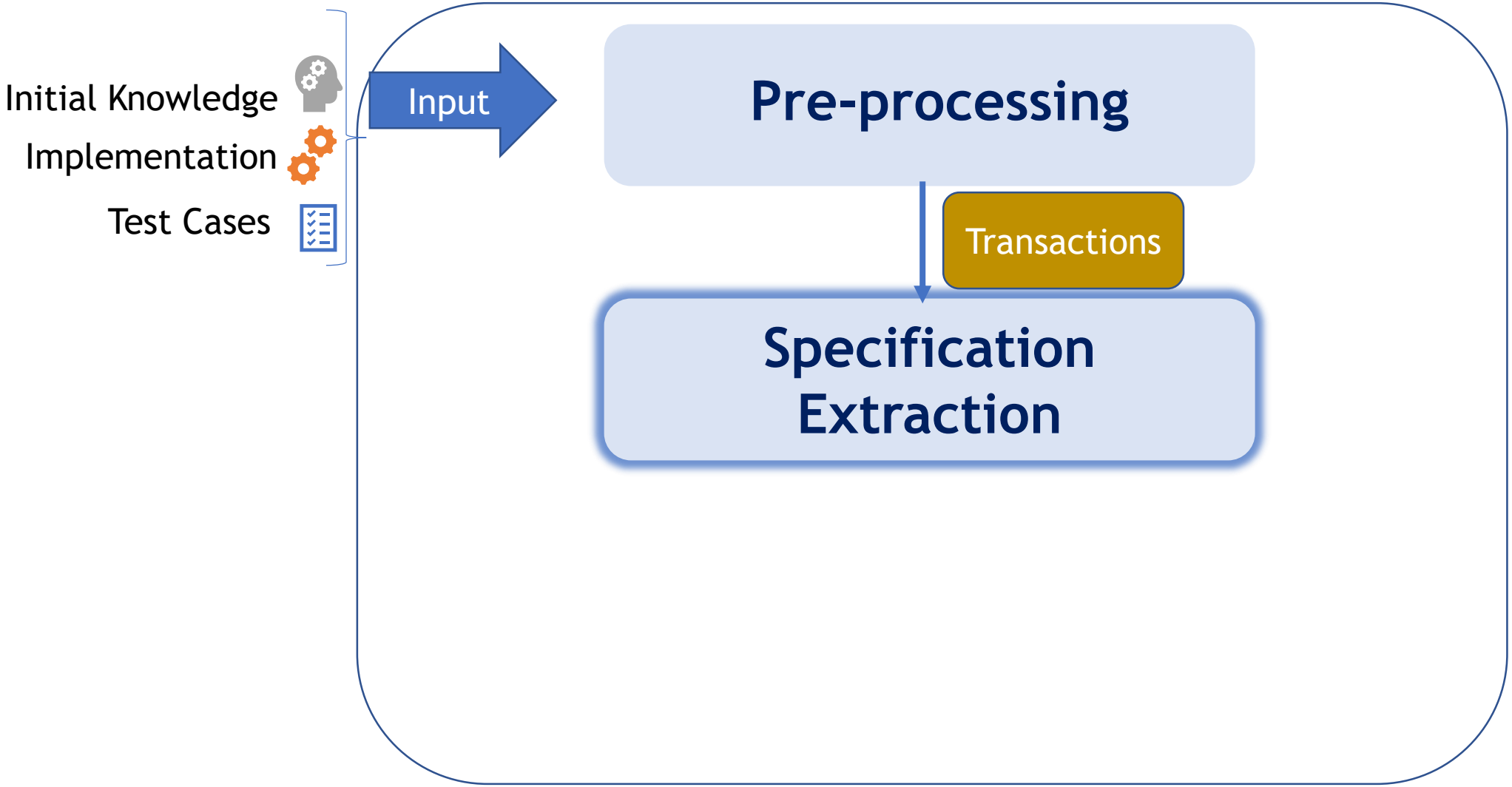


F

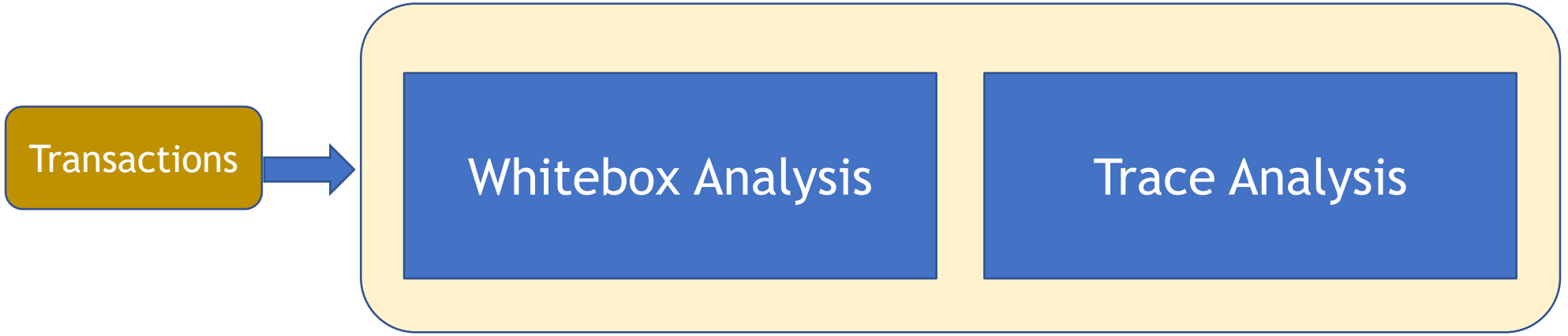
POST https://www.youtube.com/api/lounge/pairing/get_lounge_token_batch HTTP/1.1
Host: www.youtube.com
Chrome/63.0.3239.132 Safari/537.36
screen_ids=fsti0e72vuamj9p8b26h5j08ug

Transaction = (sender: CP, receiver: YS, channel: Wi-Fi, Message: {"fsti0e72vuamj9p8b26h5j08ug"}

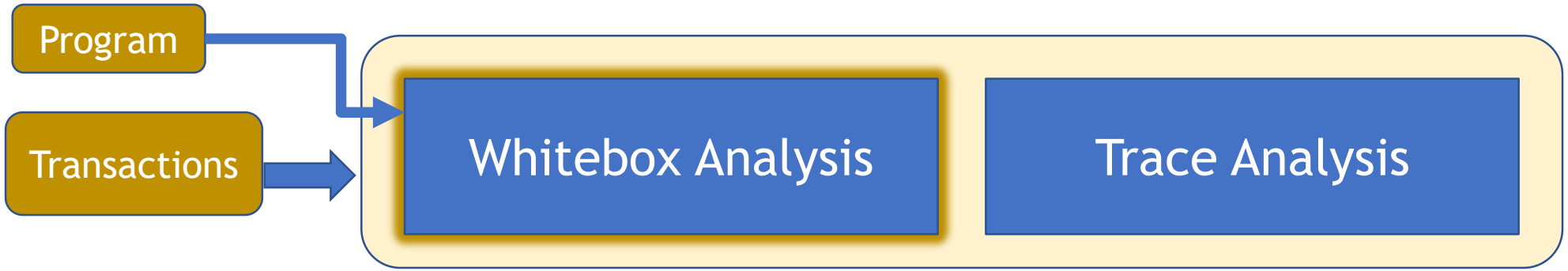
Our Approach



Specification Extraction



Specification Extraction



E.g.

Control Point (CP)

Have source code

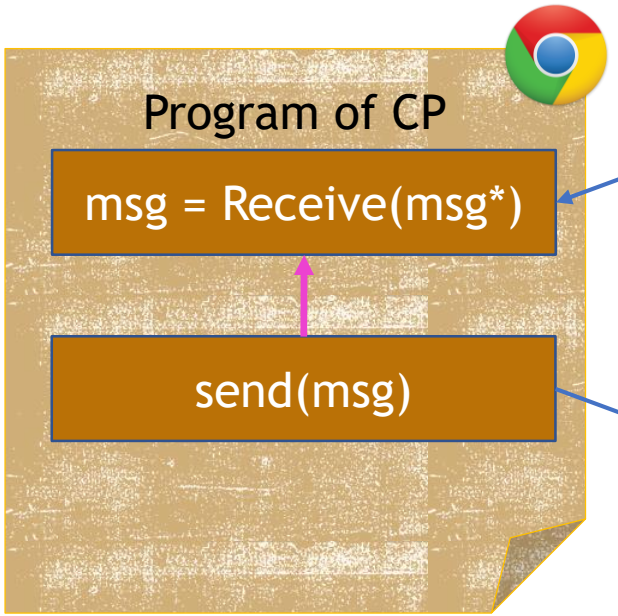
msg

HTTPS

YouTube Server (YS)

No source code

Transaction = (
sender: CP, receiver: YS, channel: Wi-Fi,
Message: {"fsti0e72vuamj9p8b26h5j08ug"}



msg*

over SSL

Chromecast Receiver

No source code

HTTPS

msg

YouTube Server (YS)

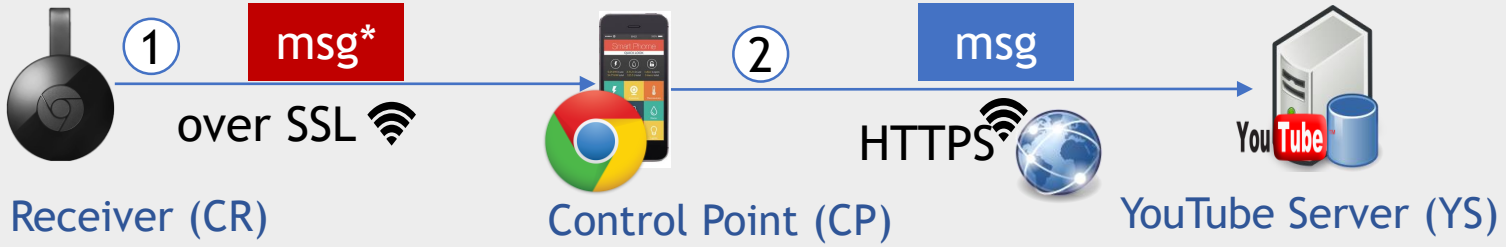
Specification Extraction

Transactions

Whitebox Analysis

Trace Analysis

1. Known Configuration - (1)



Before reset of CR — Trace 1

After reset of CR — Trace 2

Analyse the difference in the values in msg before and after the reset of CR.

Semantics of the msg = CR's session identity

Specification Extraction

Transactions

Whitebox Analysis

Trace Analysis

1. Known Configuration - (2)

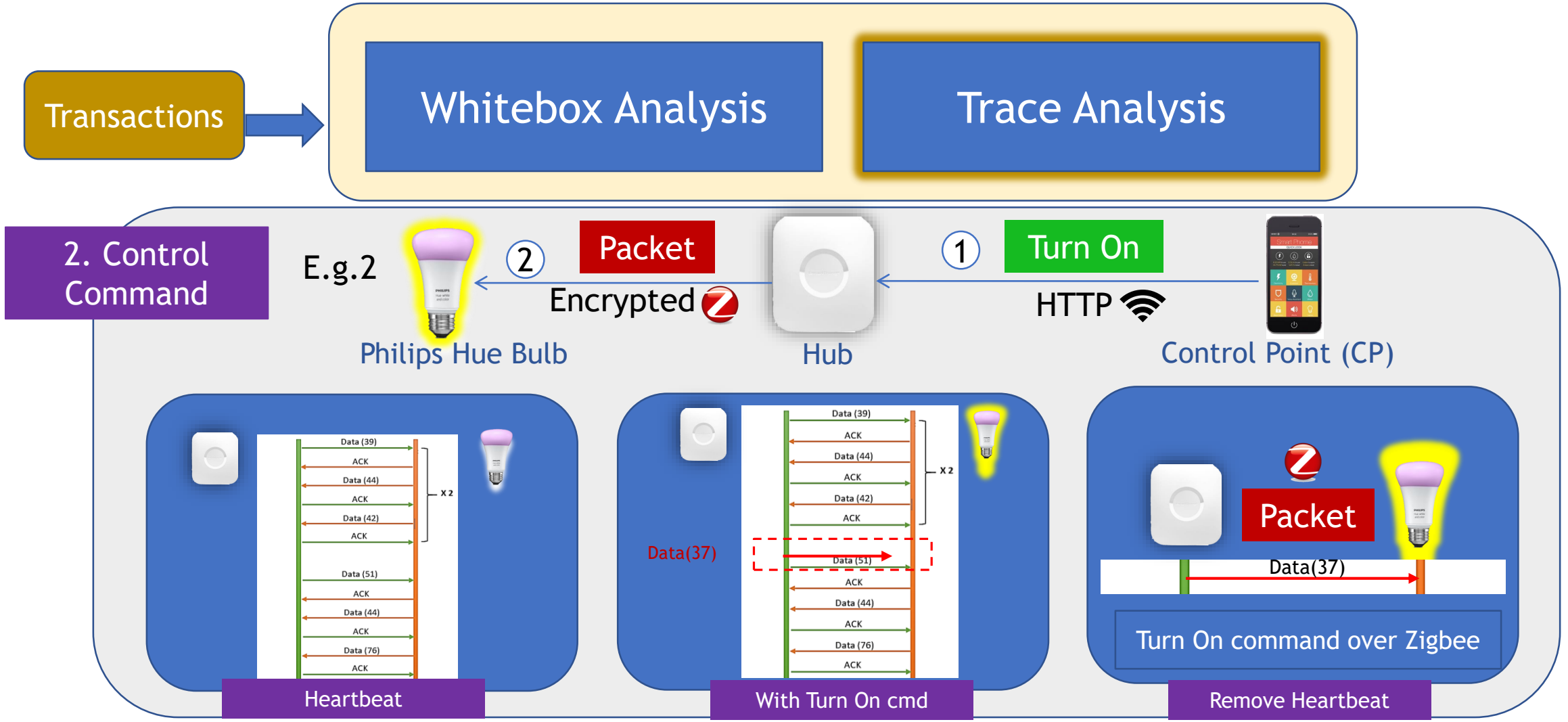
Before replace of Hub — Trace 1

After replace of Hub — Trace 2

Analyse the difference in “s” before and after the reset of CR.

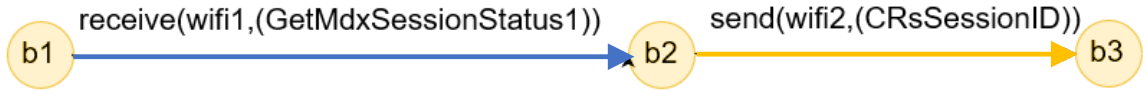
Semantics of the String “s” = Hub specific value

Specification Extraction

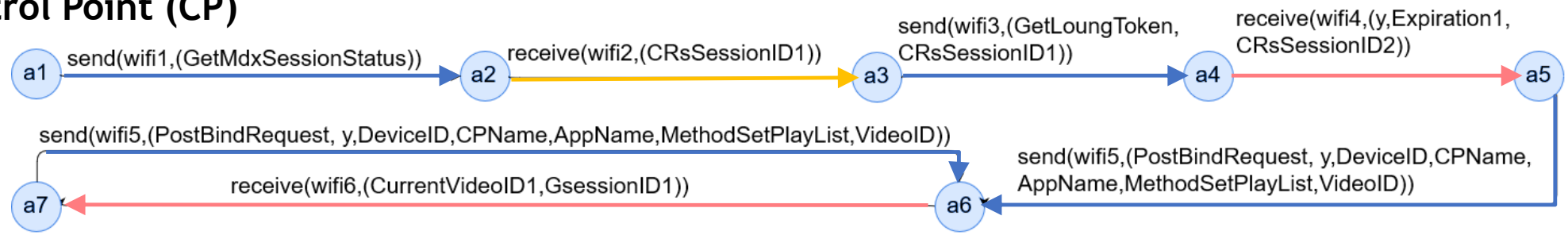


Specification: LTS Representation

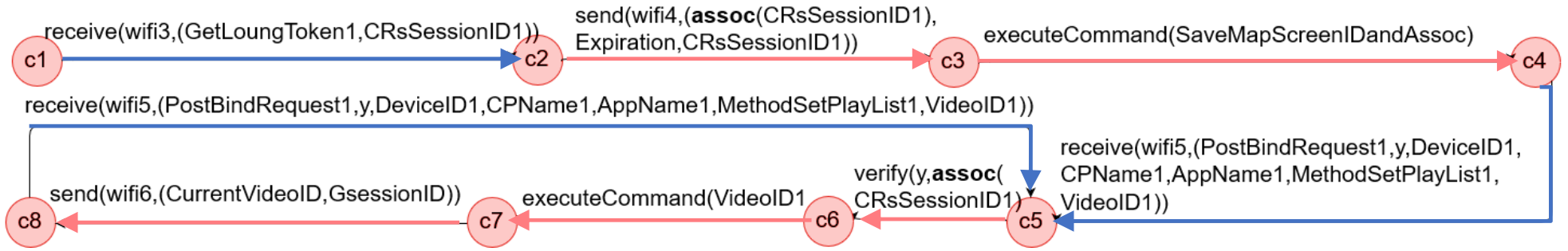
Chromecast Receiver (CR)



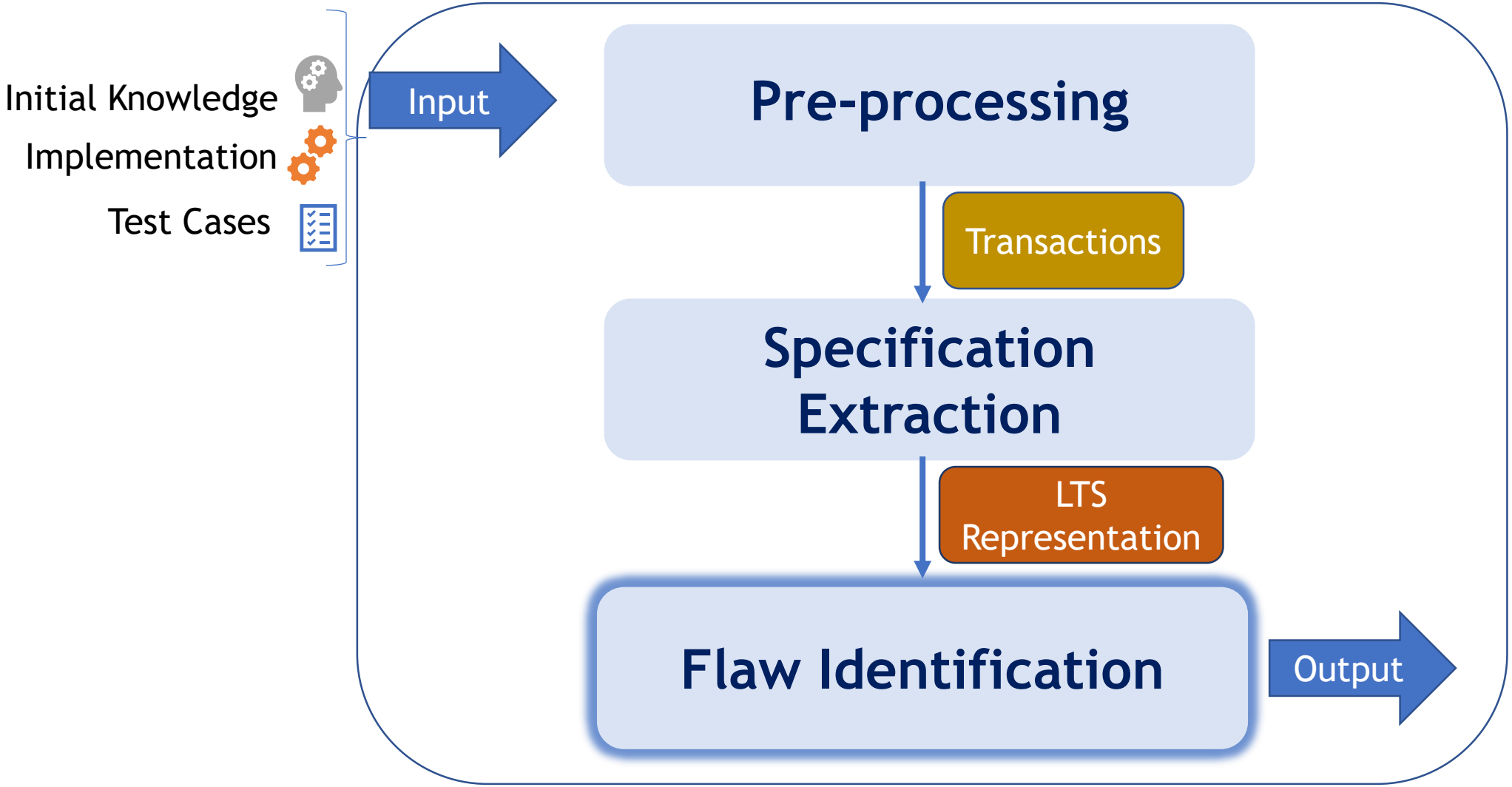
Control Point (CP)



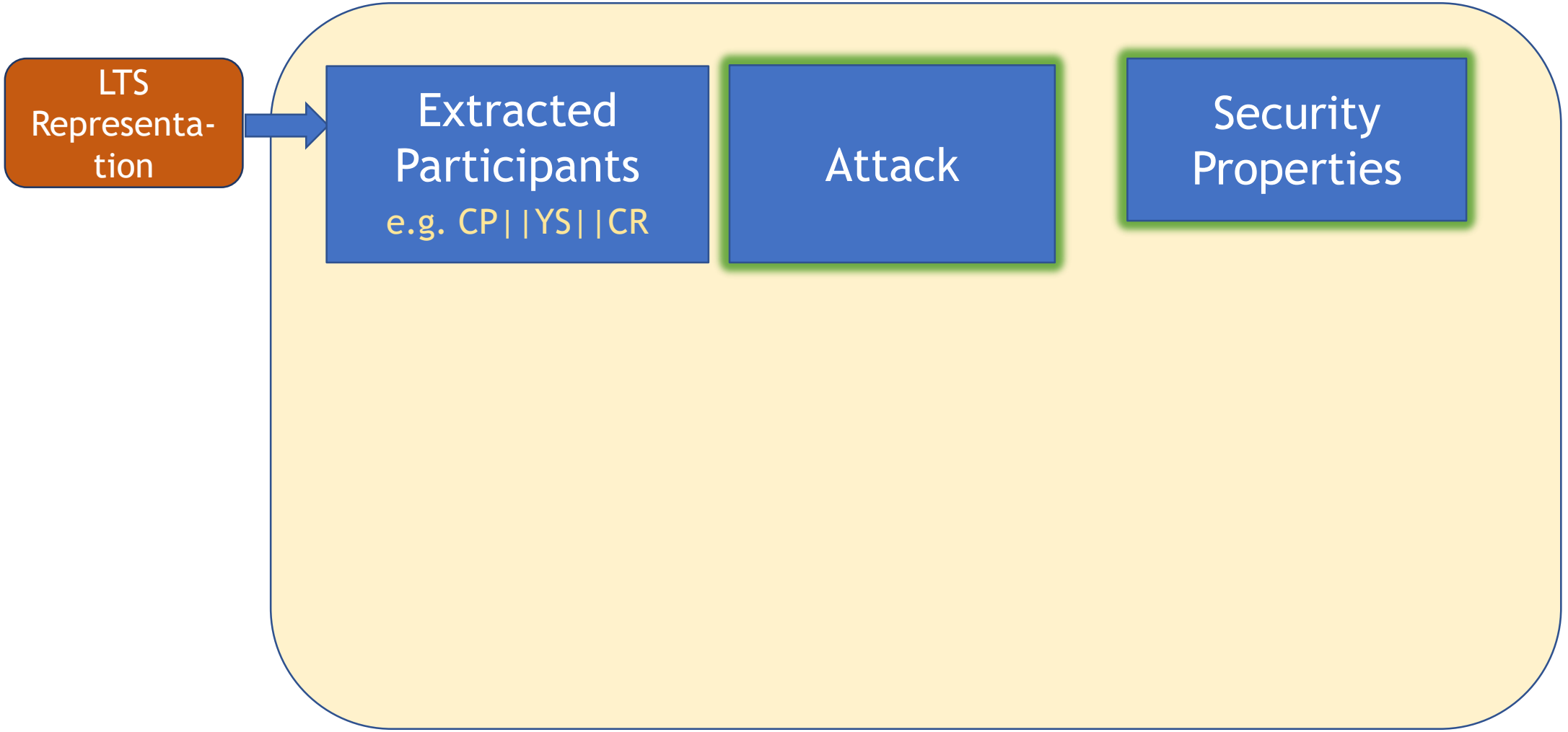
YouTube Server (YS)



Our Approach



Flaw Identification



Attack Models and Security Properties

Malicious Participant

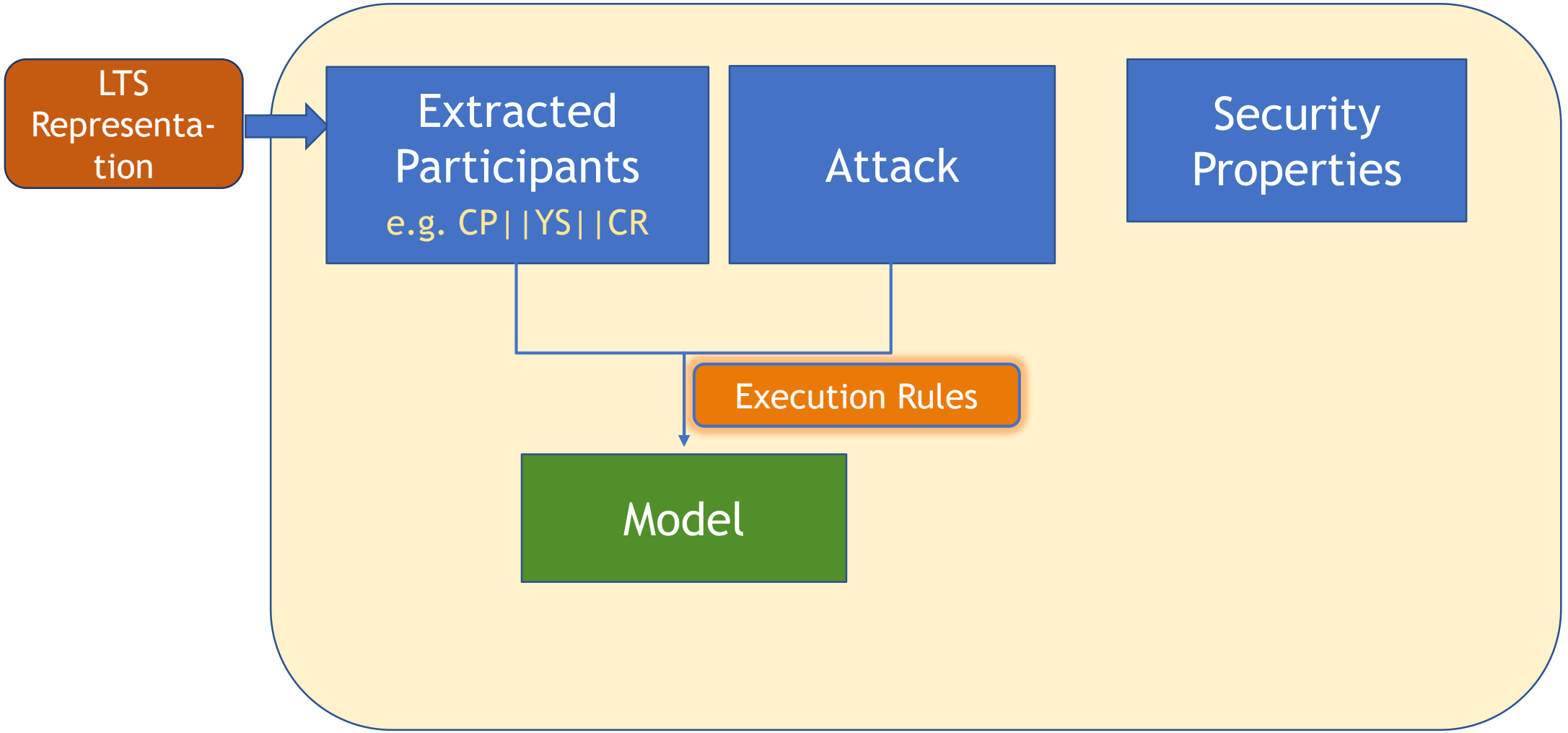
- Collect information illegally
- Send unauthorized commands

Network Attacker

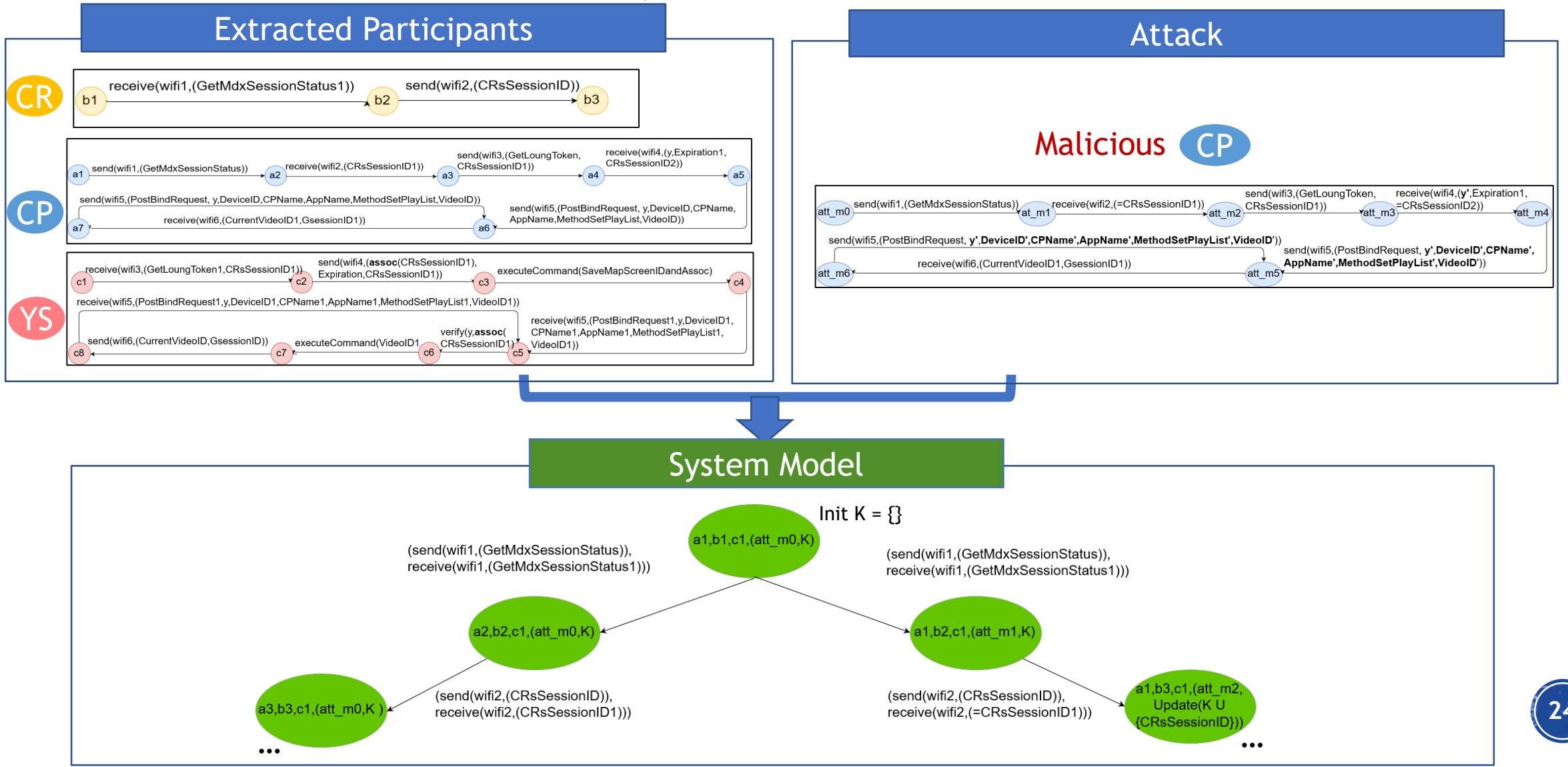
- Eavesdropping
- Intercept and modify

Security Properties	Data Level	Association Level	Access Level
Confidentiality	✓	✓	
Integrity	✓		
Authentication			✓
Authorization			✓

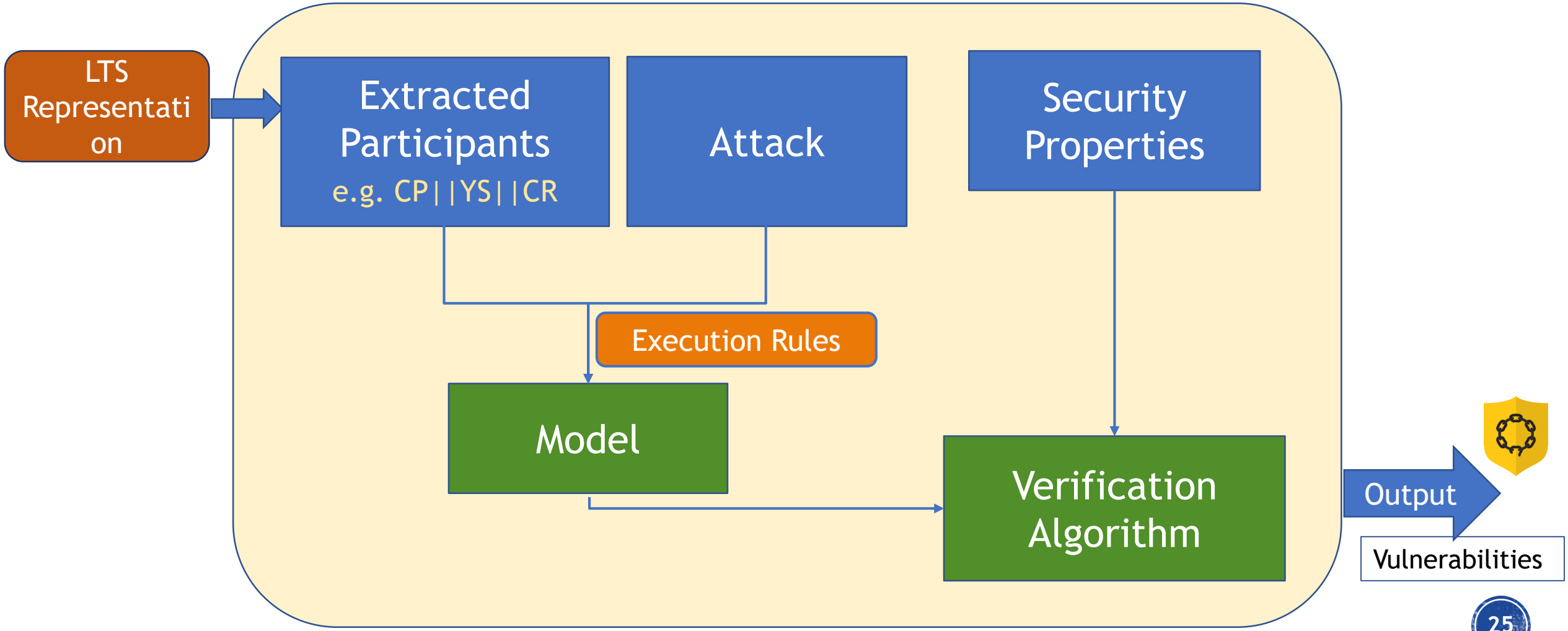
Approach


LTS Representa-tion
Extracted Participants
e.g. CP||YS||CR
Attack
Security Properties
Execution Rules
Model

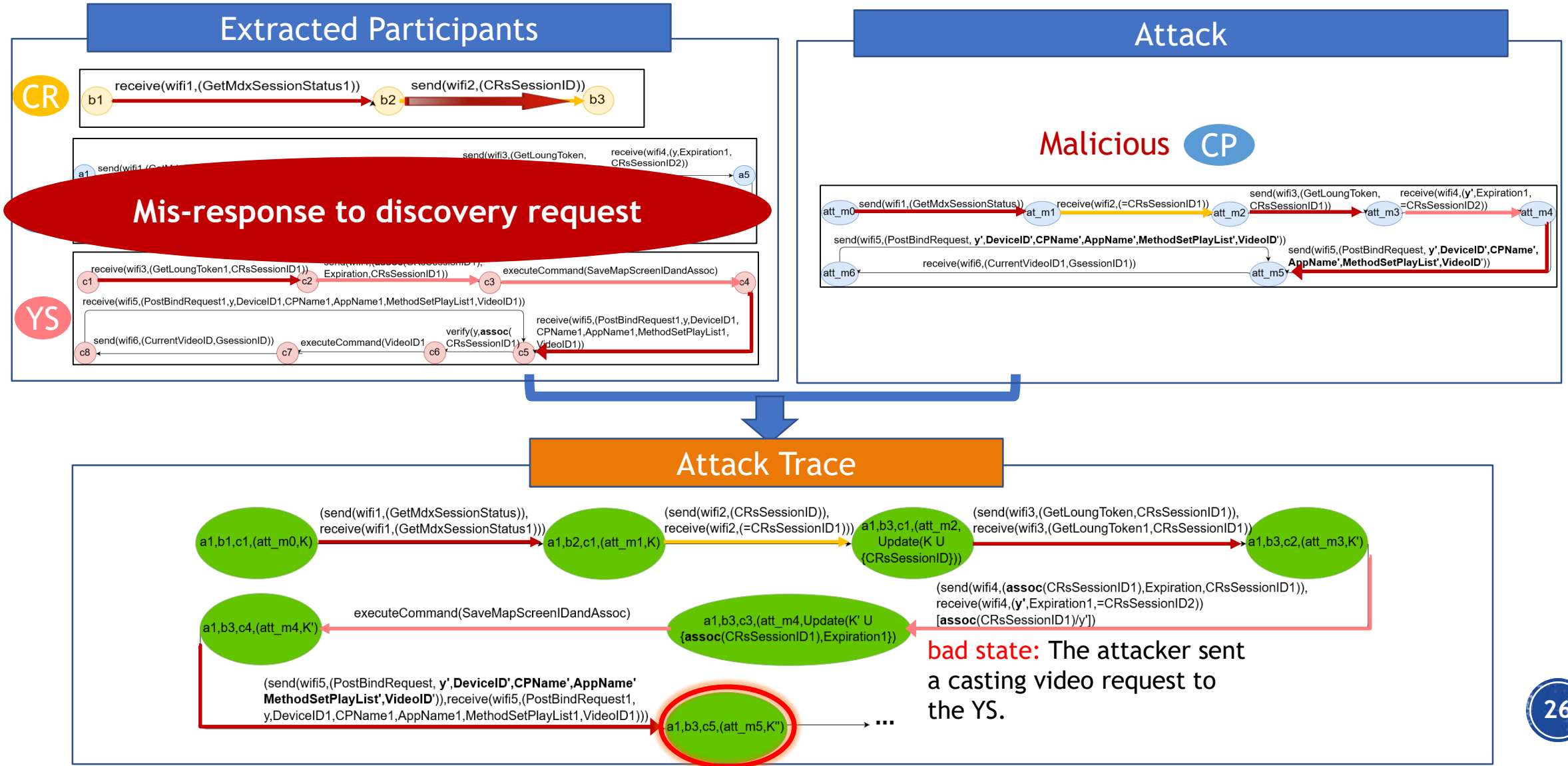
Generate the System Model



Approach

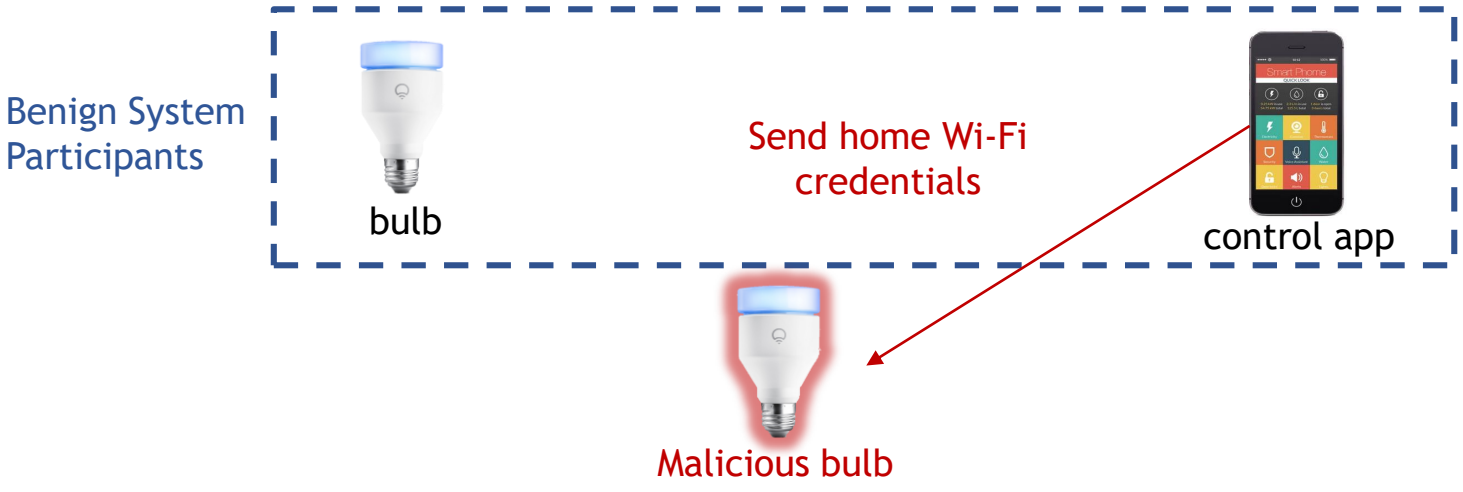

LTS Representation
Extracted Participants
e.g. CP||YS||CR
Attack
Security Properties
Execution Rules
Model
Verification Algorithm
Output
Vulnerabilities

Flaw Identification



Evaluation: Vulnerabilities

Chromecast	Philips Hue	LIFX
Mis-response to discovery request: allows a malicious control point to obtain the identity of the TV screen and casting a video to the TV.	**Misuse of ZigBee Light Link protocol:** allows a malicious hub to hijack the bulb.	**Unprotected Wi-Fi hotspot on the bulb:** allows a malicious bulb with a fake hotspot to steal the password of the victim's home Wi-Fi.
Lack of device or user authentication: allows a malicious control point to obtain the identity of a private YouTube video of the victim.	**Lack of control to administration commands:** results in uncontrolled authentication.	



Conclusion and Future Work

Conclusion

- Propose hybrid techniques to extract the specification of the smart home integration.
- Analyse the security of the extracted specification using formal verification techniques.
- Applied the approach for three existing smart home systems.
- Found twelve vulnerabilities in them.

Future Work

- Plan to propose new attack models to find vulnerabilities in similar IoT systems.

Thank You ☺

Questions?

Reference

1. Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets. https://arxiv.org/abs/1702.03681.
2. M. Vanhoef and F. Piessens. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In CCS, 2017.
3. N.Apthorpe, D.Reisman, S.Sundaresan, A.Narayanan, and N.Feamster, 2017. Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic. *arXiv preprint arXiv:1708.05044*.
4. https://hometheaterreview.com/attack-of-the-smart-home-devices/
5. S. Majumder, E. Aghayi, M. Noferesti, H. Memarzadeh-Tehran, T. Mondal, Z. Pang, & M. J. Deen (2017). Smart Homes for Elderly Healthcare—Recent Advances and Research Challenges. *Sensors*, *17*(11), 2496.