SECURITY AND PRIVACY IN SMART HOME ECOSYSTEMS

ANDREA SARACINO, GIACOMO GIORGI

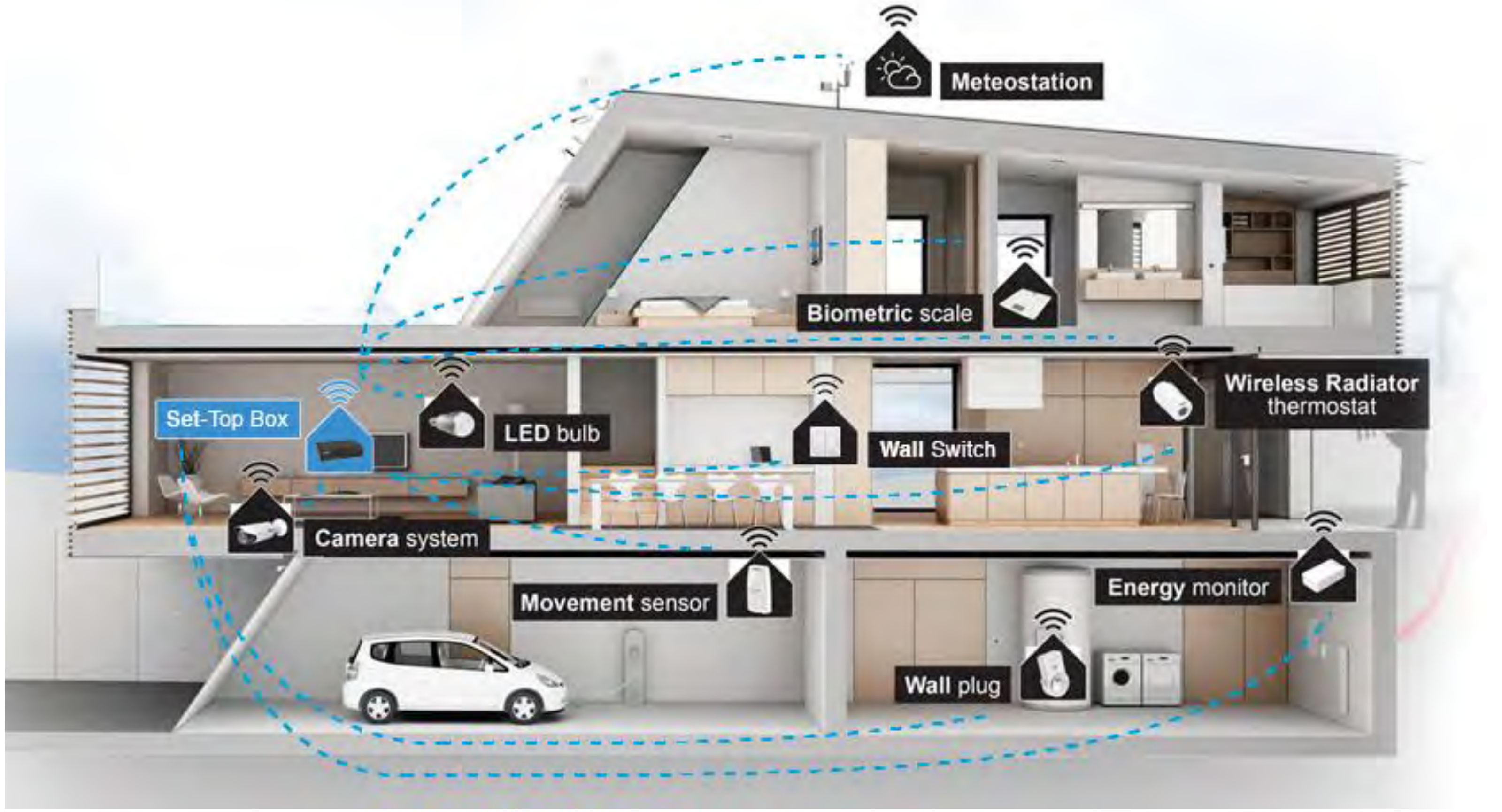
ANDREA.SARACINO@IIT.CNR.IT

Consiglio Nazionale delle Ricerche

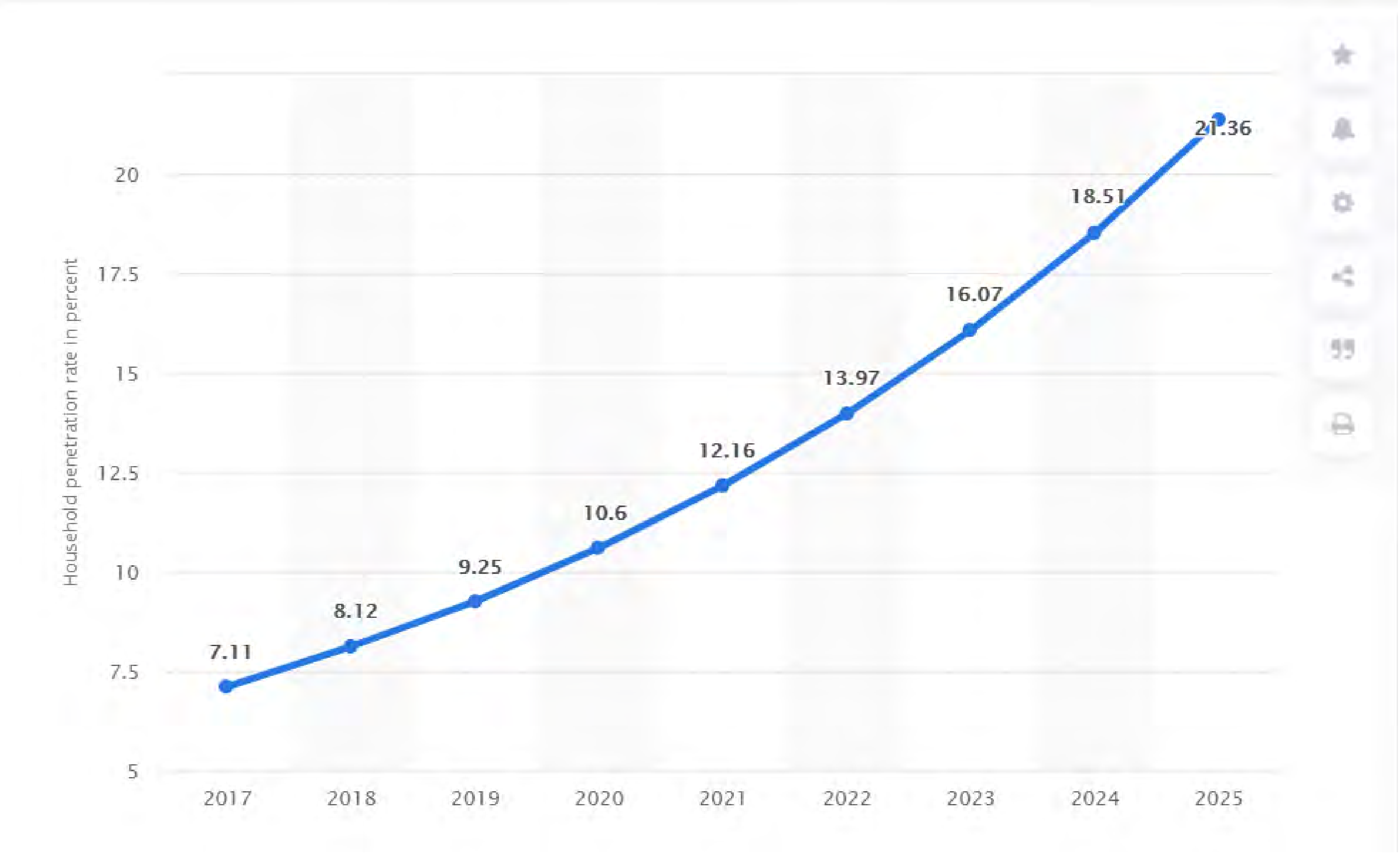
ISTITUTO DI INFORMATICA E TELEMATICA

1st Workshop on Trustworthy Software Ecosystems

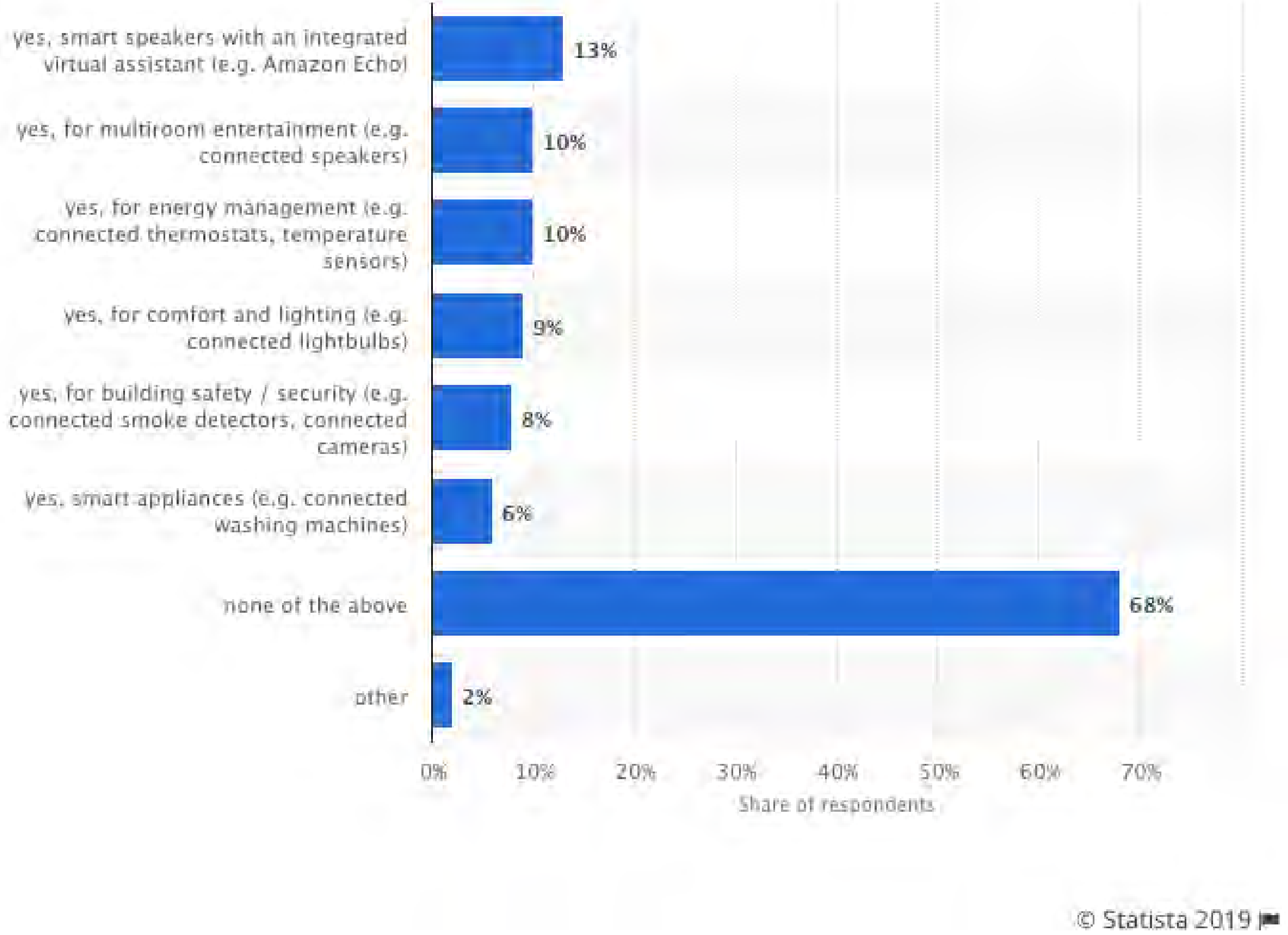
THE SMART HOME ECOSYSTEM



MARKET PENETRATION



MARKET PENETRATION



HOME AUTOMATION (DOMOTICS)

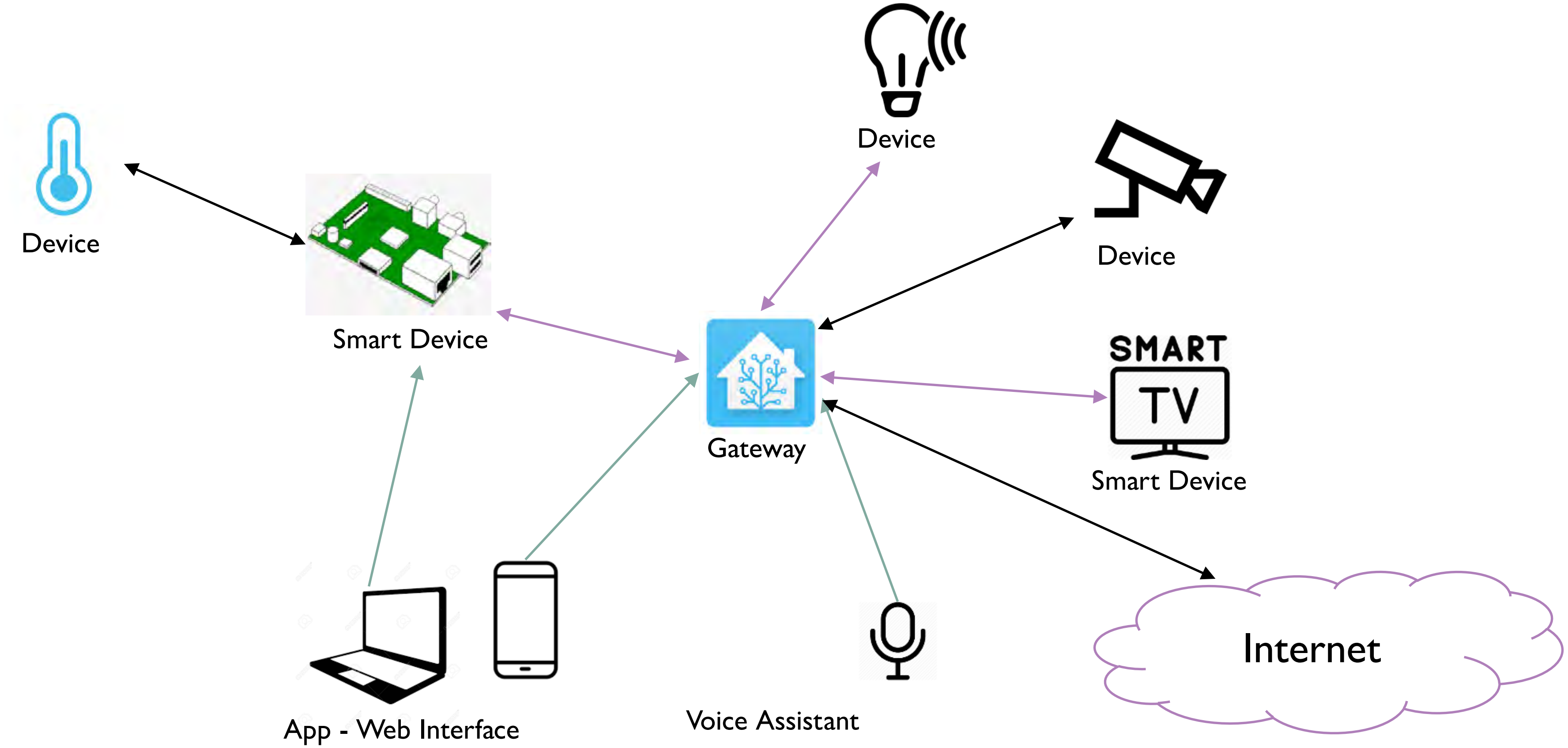
HOME AUTOMATION (DOMOTICS)

- Domotics
  - Hardcoded pre-configured routines for home management
  - Dedicated hardware and (mainly) wired connections.
  - Centralized control panel.
  - High costs for installation and maintanability
  - Requires dedicated personnel for reconfiguration.
  - Fully automated – few to none user interaction

SMART HOME

- Set of stand-alone smart devices
- Controlled through an home assistant or smartphone
- No architecture costs (only device cost)
- Requires constant user interaction for providing smart service
- Commands issued through the home assistant
    - Need Internet connection
    - Single point of failure

SMART HOME ARCHITECTURE



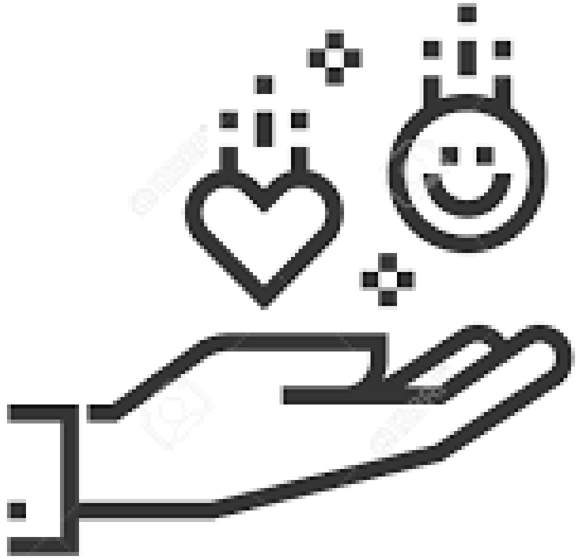
NEW GENERATION SMART HOMES

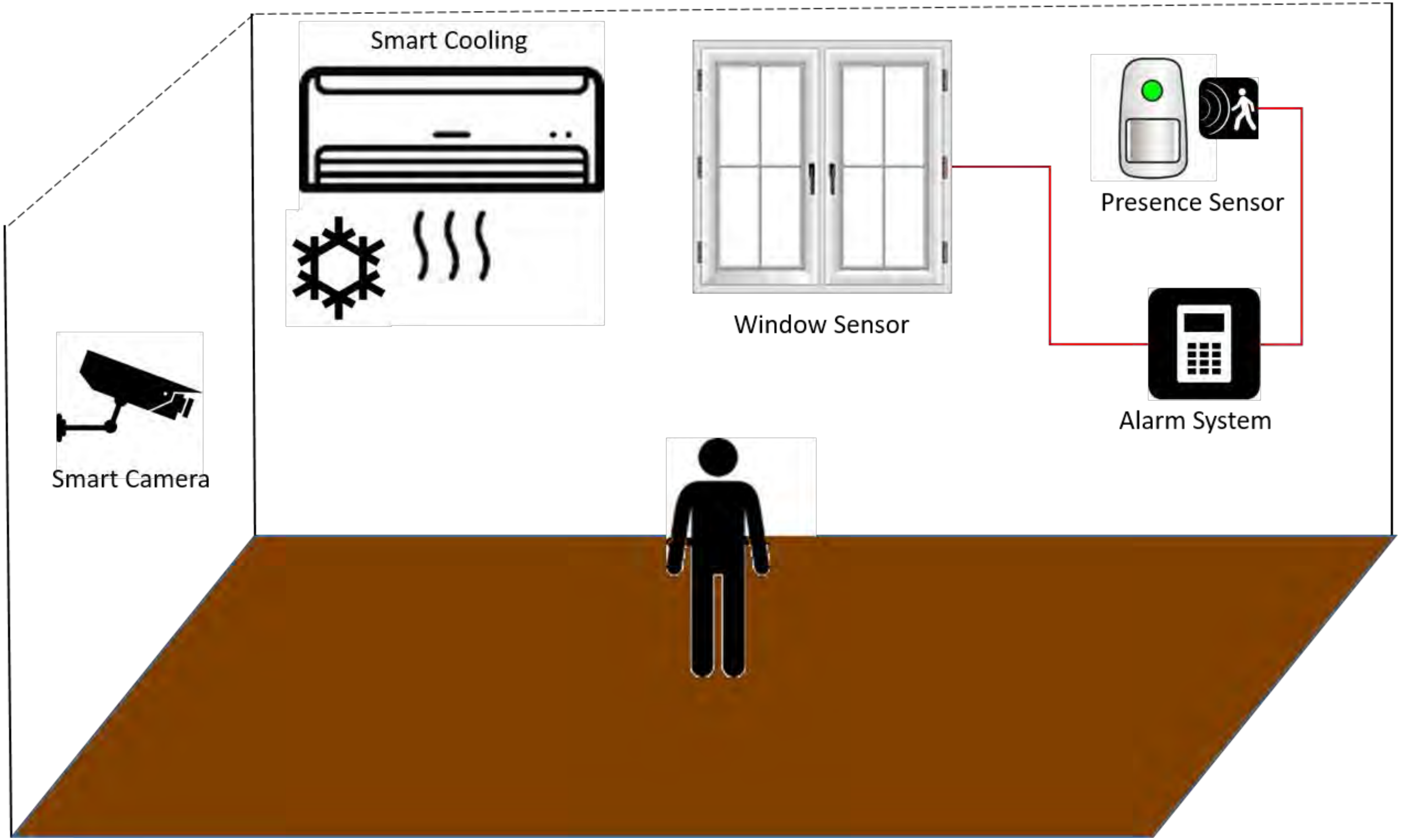
NEW GENERATION SMART HOME

- Autonomous device interaction (Machine-to-Machine)
- Smart – custom services
- Autonomous inter-device communication
- Requires limited user interaction
  - Anticipating User Needs
  - Reacting to context changes
- Heavy usage of Artificial Intelligence

SMART HOME SERVICES

- Video surveillance
- Energy management
    - Temperature (heating/cooling)
    - Lights
- Comfort management
- Parental Control
- Custom services based on standard device functionalities

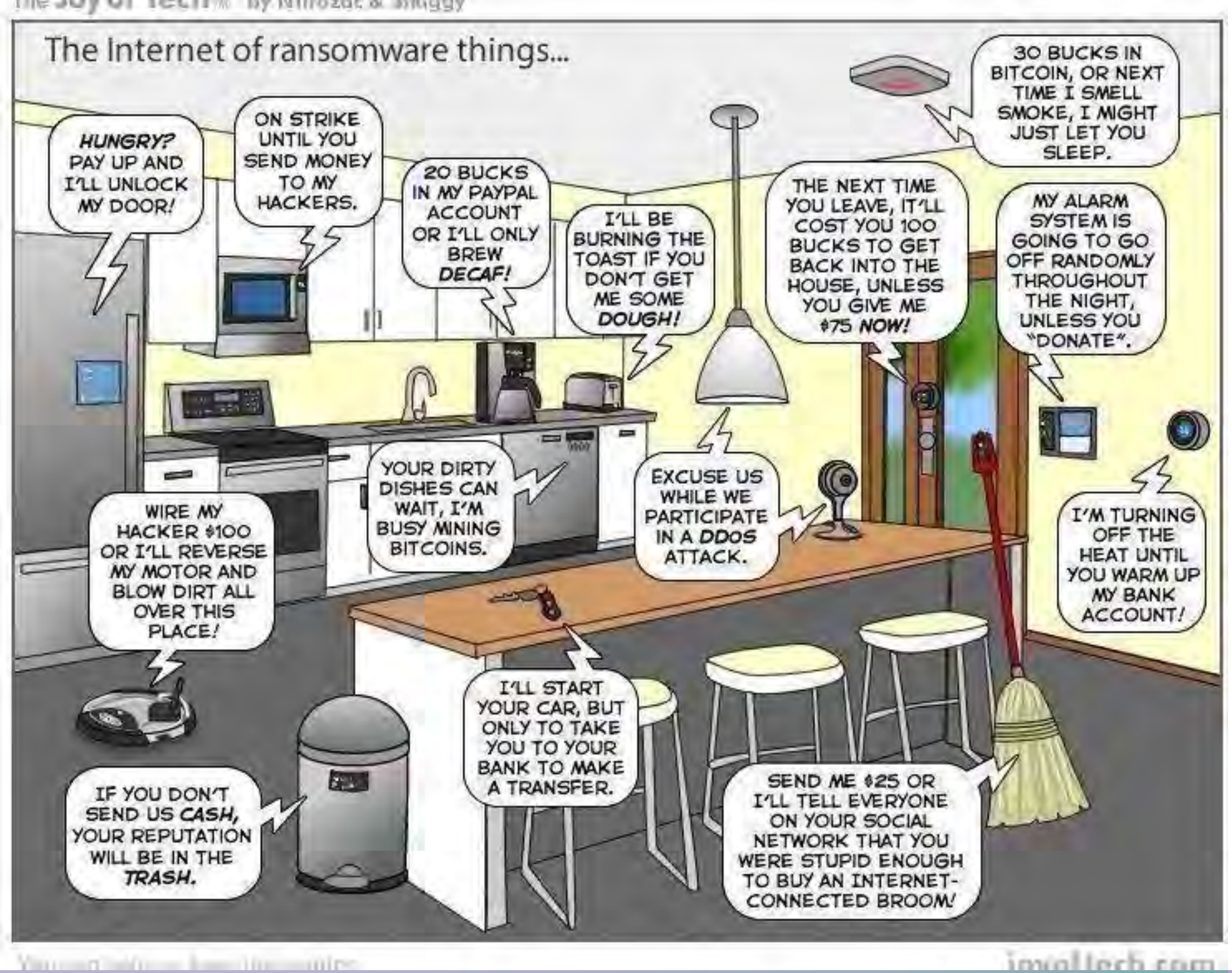



Smart Cooling
Window Sensor
Presence Sensor
Alarm System
Smart Camera

THIRD PARTY APPLICATIONS

- Devices can be customized by installing 3rd party apps
  - Main difference with previous models
  - Smarter services to fully exploit device functionalities
  - Accessible through general or dedicated marketplaces
  - Trust assumptions are not straightforward
    - Vulnerabilities and weaknesses
    - Malicious code

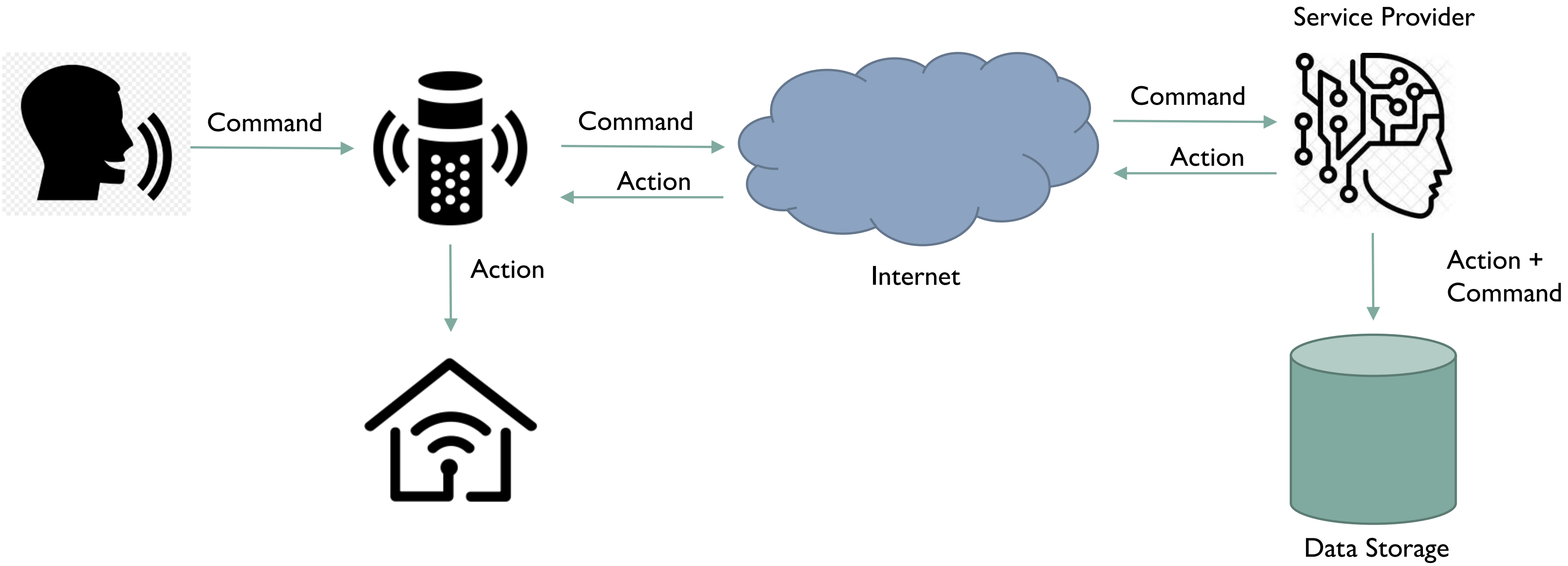
THREATS AND VULNERABILITIES

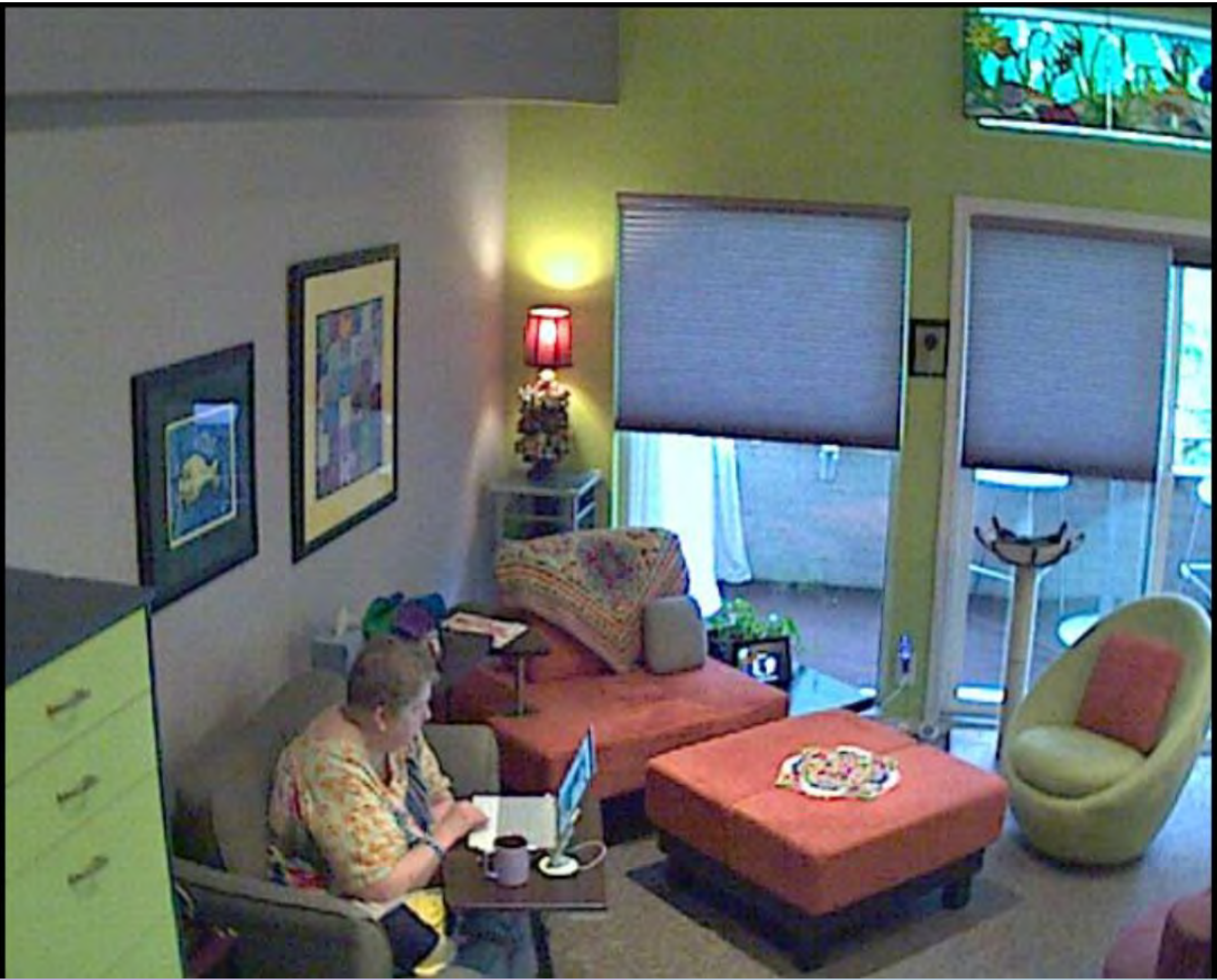

The Joy of Tech by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDoS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
joyoftech.com

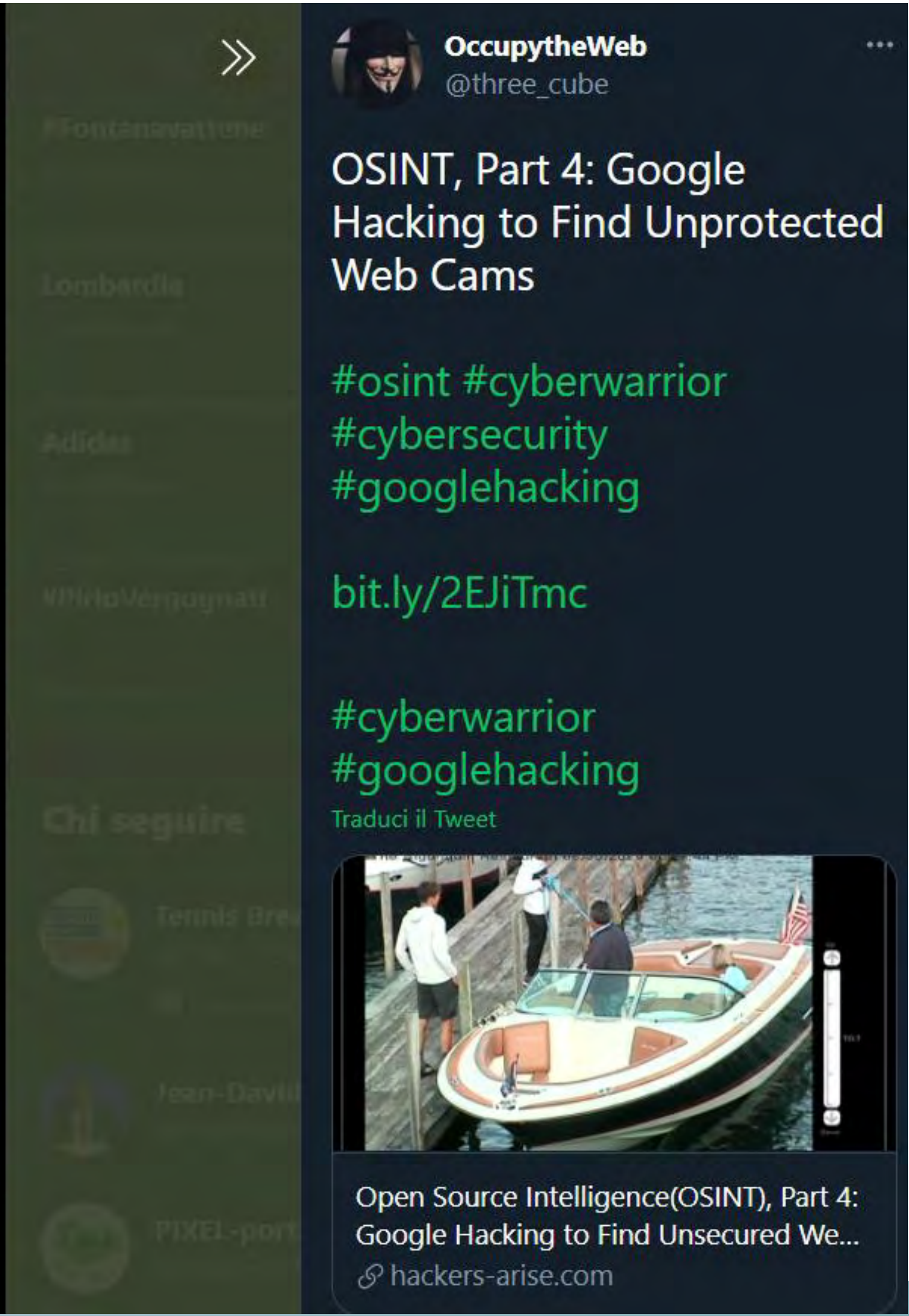
DEVICE VULNERABILITIES

- Connection vulnerabilities
- Hardware vulnerabilities
- Usage of deprecated APIs
- Malicious usage of genuine functionalities
- Weak passwords

DATA PRIVACY







OccupytheWeb
@three_cube

OSINT, Part 4: Google Hacking to Find Unprotected Web Cams

#osint #cyberwarrior #cybersecurity #googlehacking

bit.ly/2EJiTmc

#cyberwarrior #googlehacking

Traduci il Tweet

Open Source Intelligence(OSINT), Part 4: Google Hacking to Find Unsecured We...
hackers-arise.com

LARGE ATTACK SURFACE

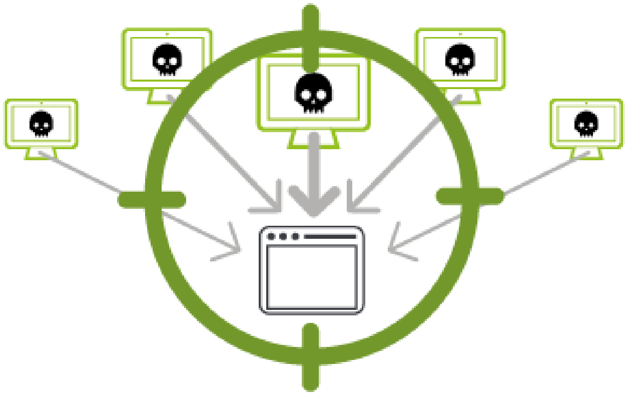
- Network
  - Internet-connected devices
- Roaming devices
  - Smartphones
  - Tablets/Laptops
- App marketplaces
- Physical compromission

INCREASING ATTACKER MOTIVATION

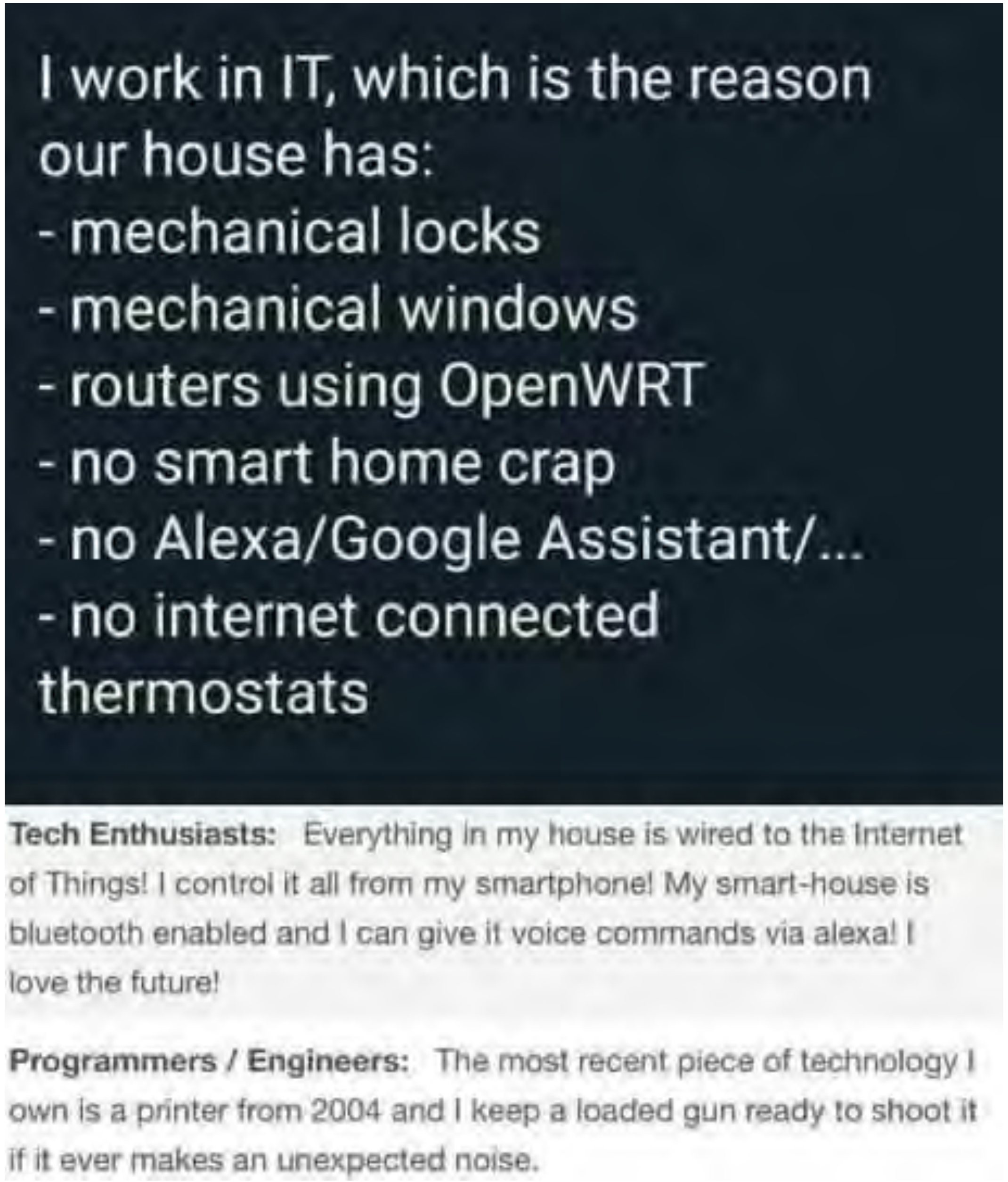
- Access to physical resources with direct impact on real life.
- Compromission might be a first step for physical intrusion detection.
- Huge amount of extremely private data constantly produced
- Smart Working
- Reputation tampering

ATTACK TYPES

- Denial of Service (DoS)
  - Network level
  - Application level
- Botnet
- Spyware
- Ransomware



SOLUTION?



I work in IT, which is the reason our house has:
- mechanical locks
- mechanical windows
- routers using OpenWRT
- no smart home crap
- no Alexa/Google Assistant/...
- no internet connected thermostats

Tech Enthusiasts: Everything in my house is wired to the Internet of Things! I control it all from my smartphone! My smart-house is bluetooth enabled and I can give it voice commands via alexa! I love the future!

Programmers / Engineers: The most recent piece of technology I own is a printer from 2004 and I keep a loaded gun ready to shoot it if it ever makes an unexpected noise.

HANDLING SECURITY AND PRIVACY

SECURITY DIRECTIONS

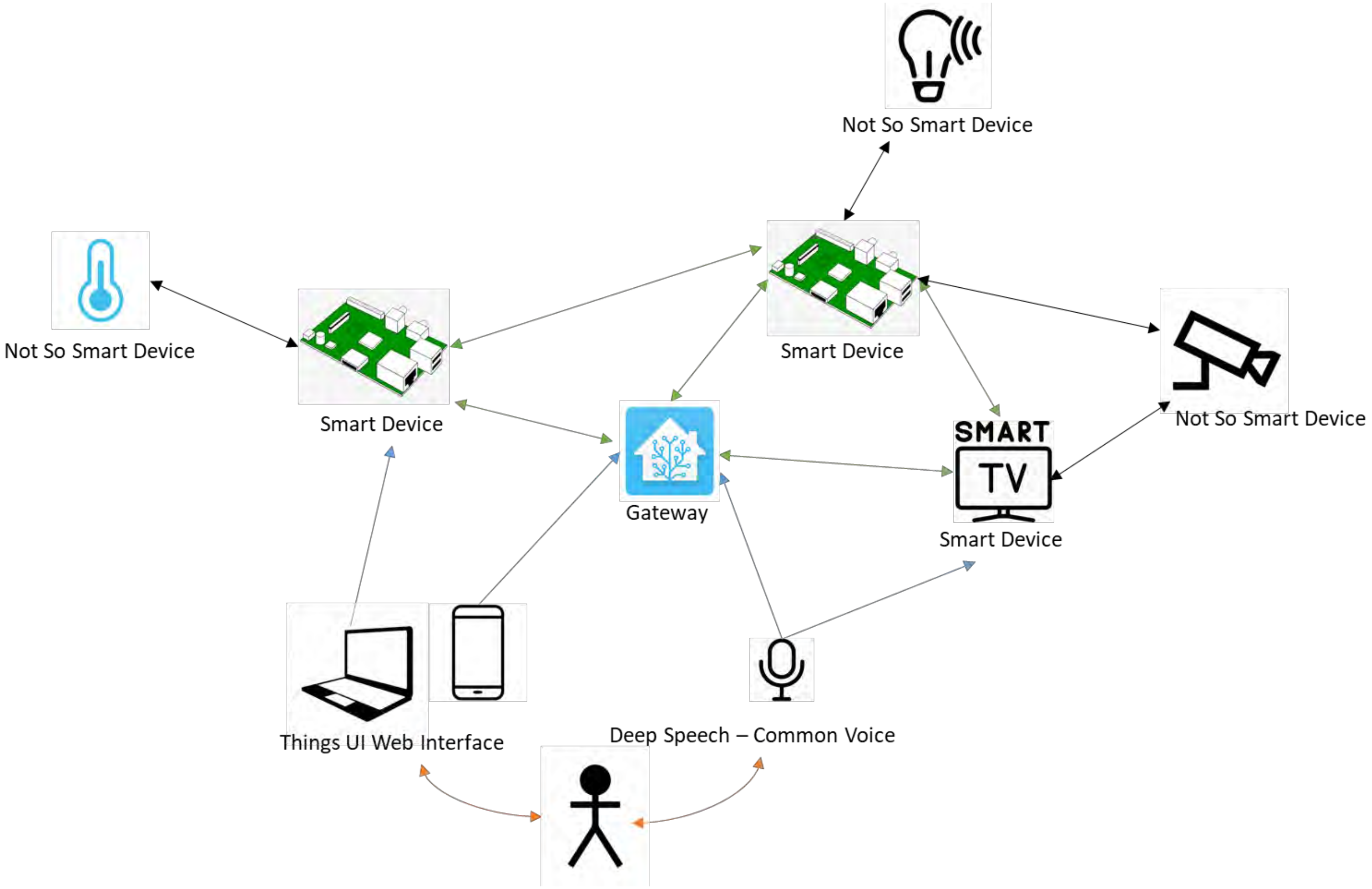
- Protecting data privacy
  - Data Flow Control
  - Privacy preserving analysis
- Enforcing Access Control on critical resources and operations
- Avoiding Single Point of Failure
- Proactively detecting intrusion attempts

LOCALIZED STORAGE AND ANALYSIS

- Store data locally
- Controlling data flows
  - Managing the house cyber-perimeter
  - Tainting data and identifying data sinks
- Exploiting anonymization when data are sent out of the perimeter

AVOIDING SINGLE POINT OF FAILURE

- P2P Architecture
- Decentralization
- Functionality replication
- Fault Tolerance

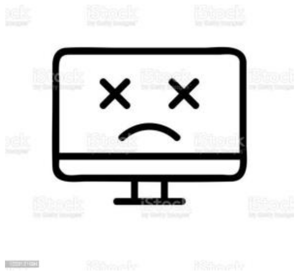


PRIVACY PRESERVING ANALYSIS

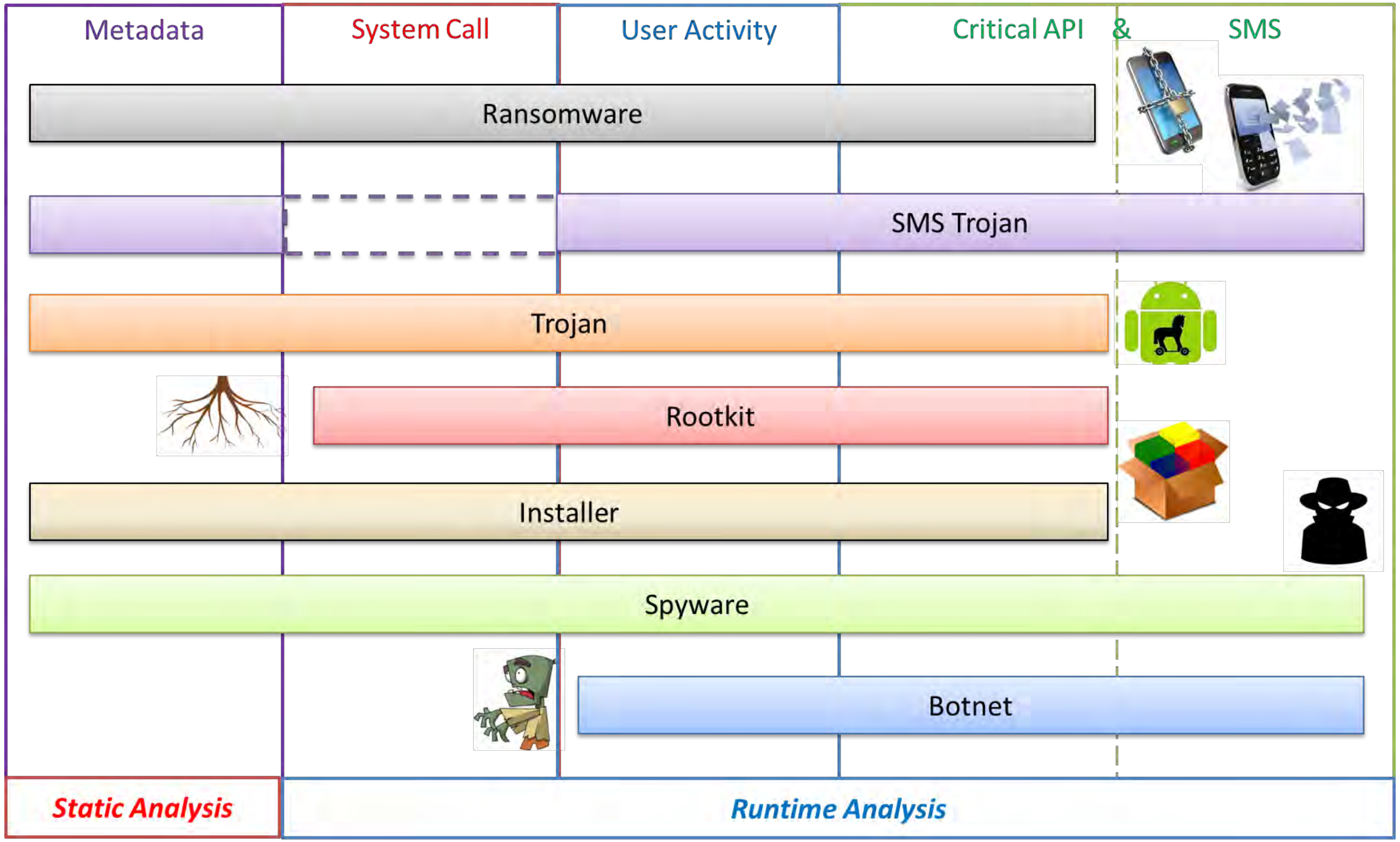
- Performing analysis without disclosing sensitive information
- Minimum needed privilege
- Usage of anonymization, data suppression and other Privacy Enhancing technologies

INTRUSION DETECTION

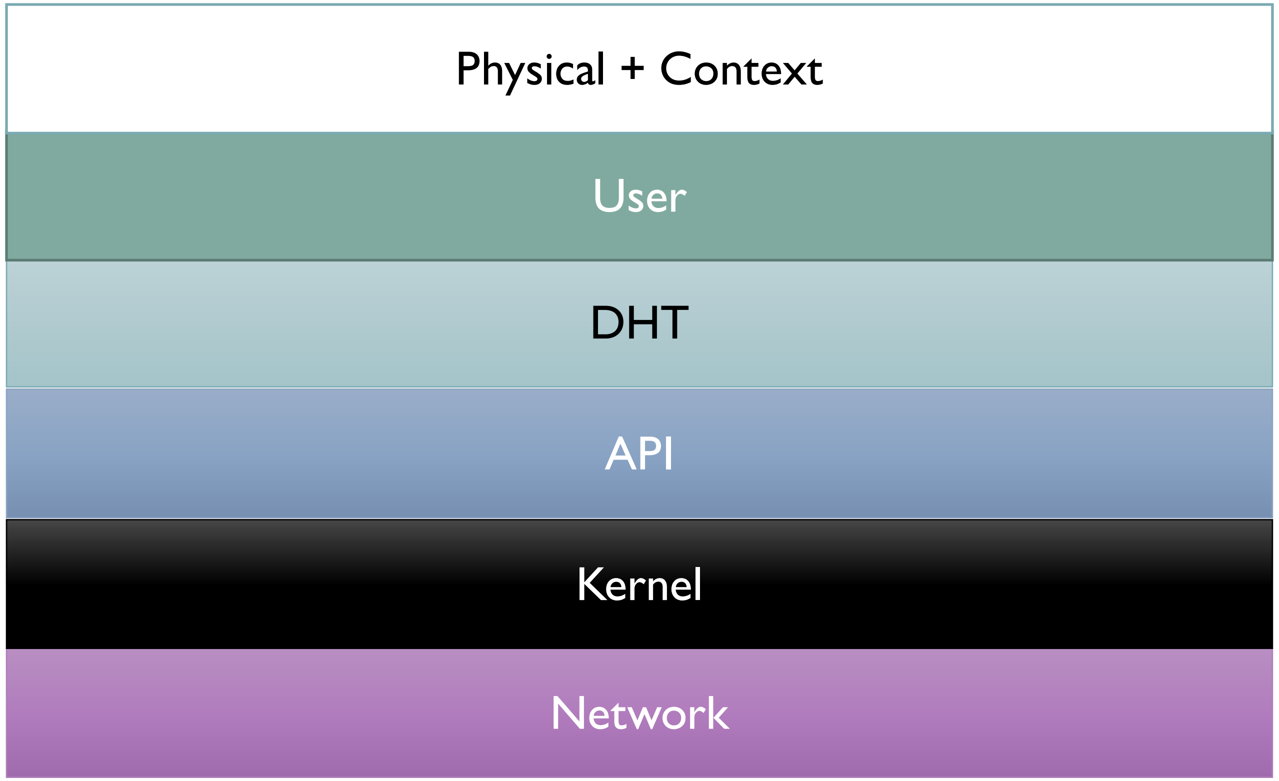
- Physical Intrusion
  - Intruder
  - Physical misbehavior
- Software Intrusion
  - Malware
  - Compromised device
- Device Fault
  - Broken sensor/actuator



MULTI LEVEL IDS



MULTI LEVEL IDS



Physical + Context

User

DHT

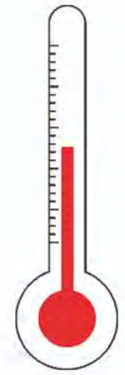
API

Kernel

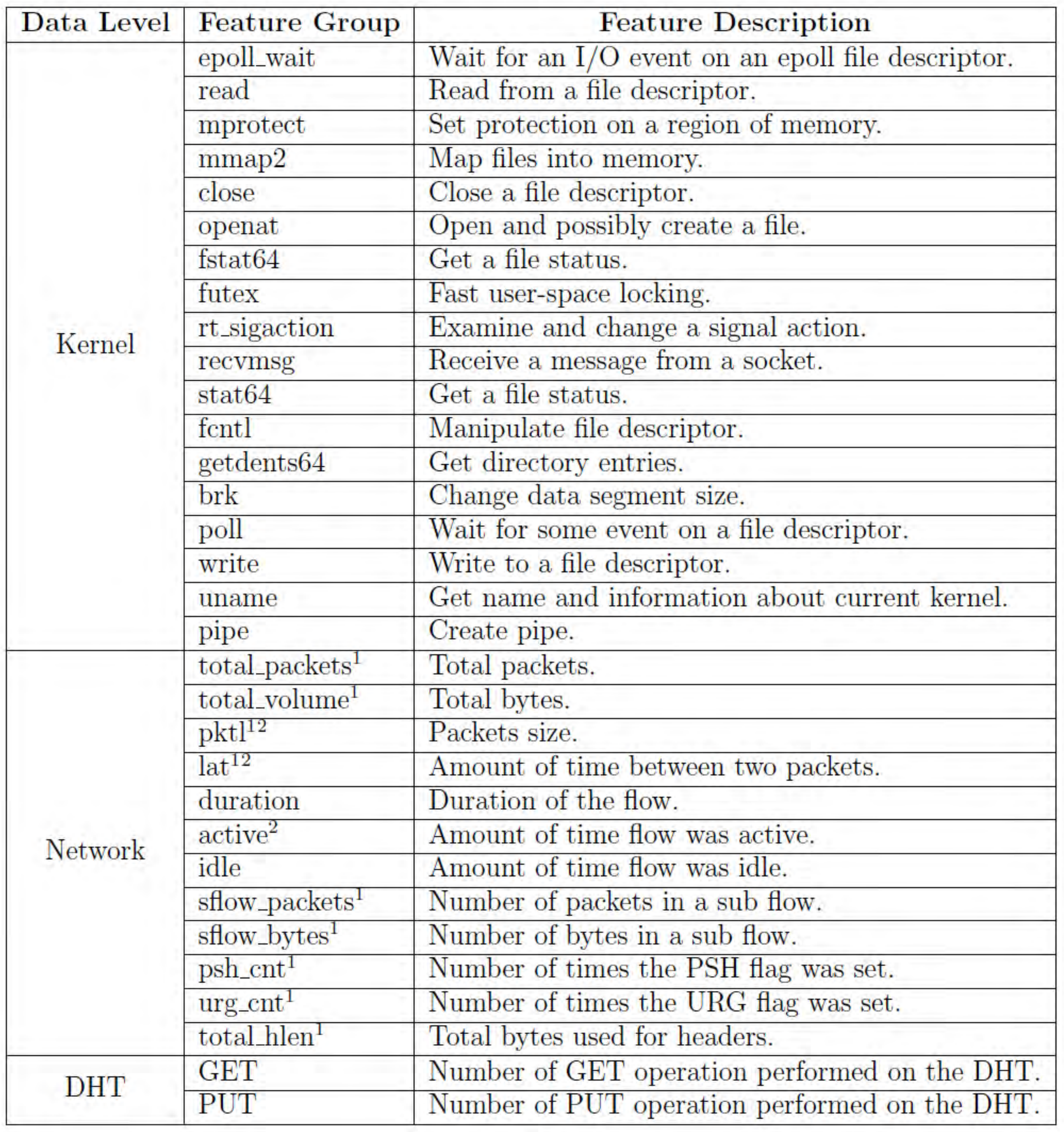
Network

PRELIMINARY IDS FOR SMART HOME ENVIRONMENTS

- Simulated testbed representing a smart home system
- Using Kademlia as a DHT
  - Replicated database
  - Handling communication
- Standard machine learning classifier
- Tested against the MIRAI botnet attack

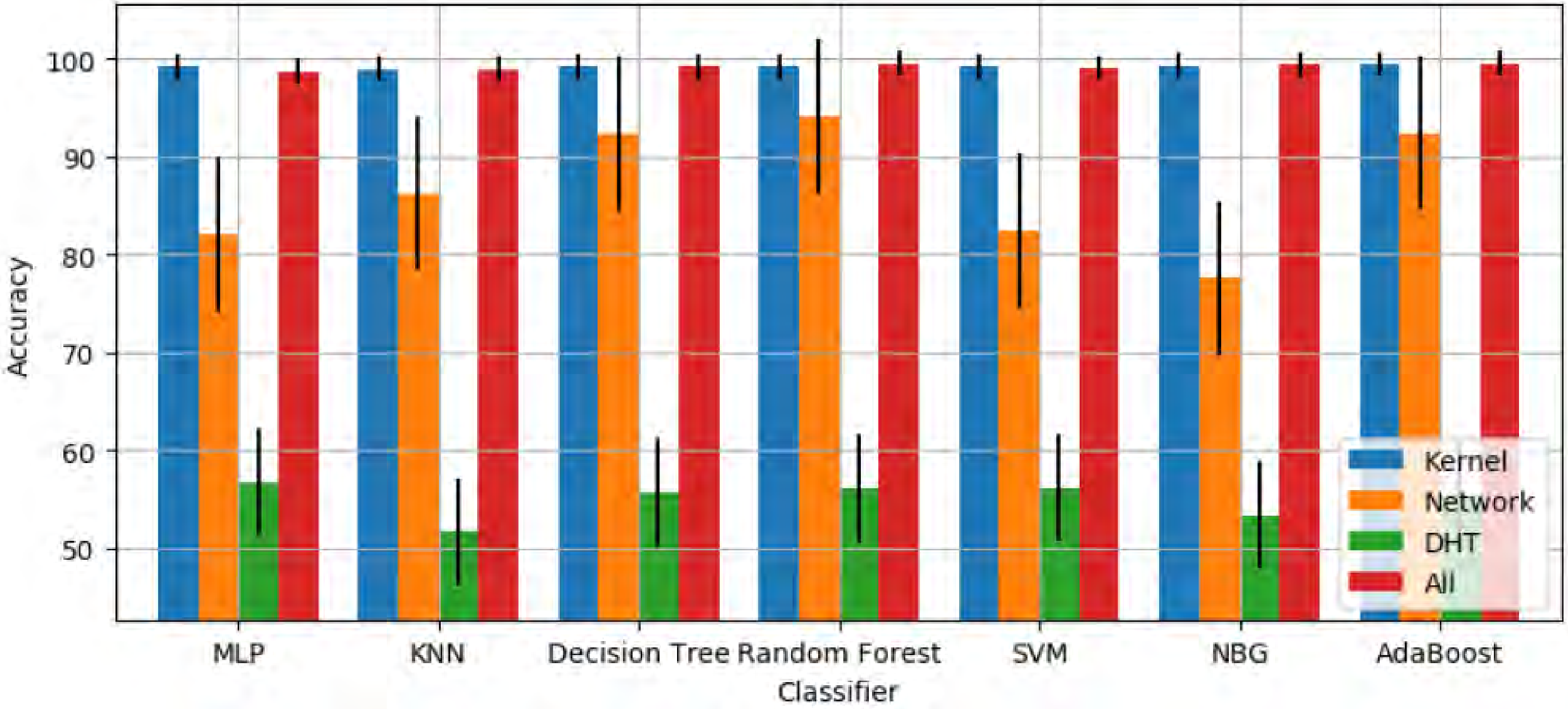


ANALYZED FEATURES

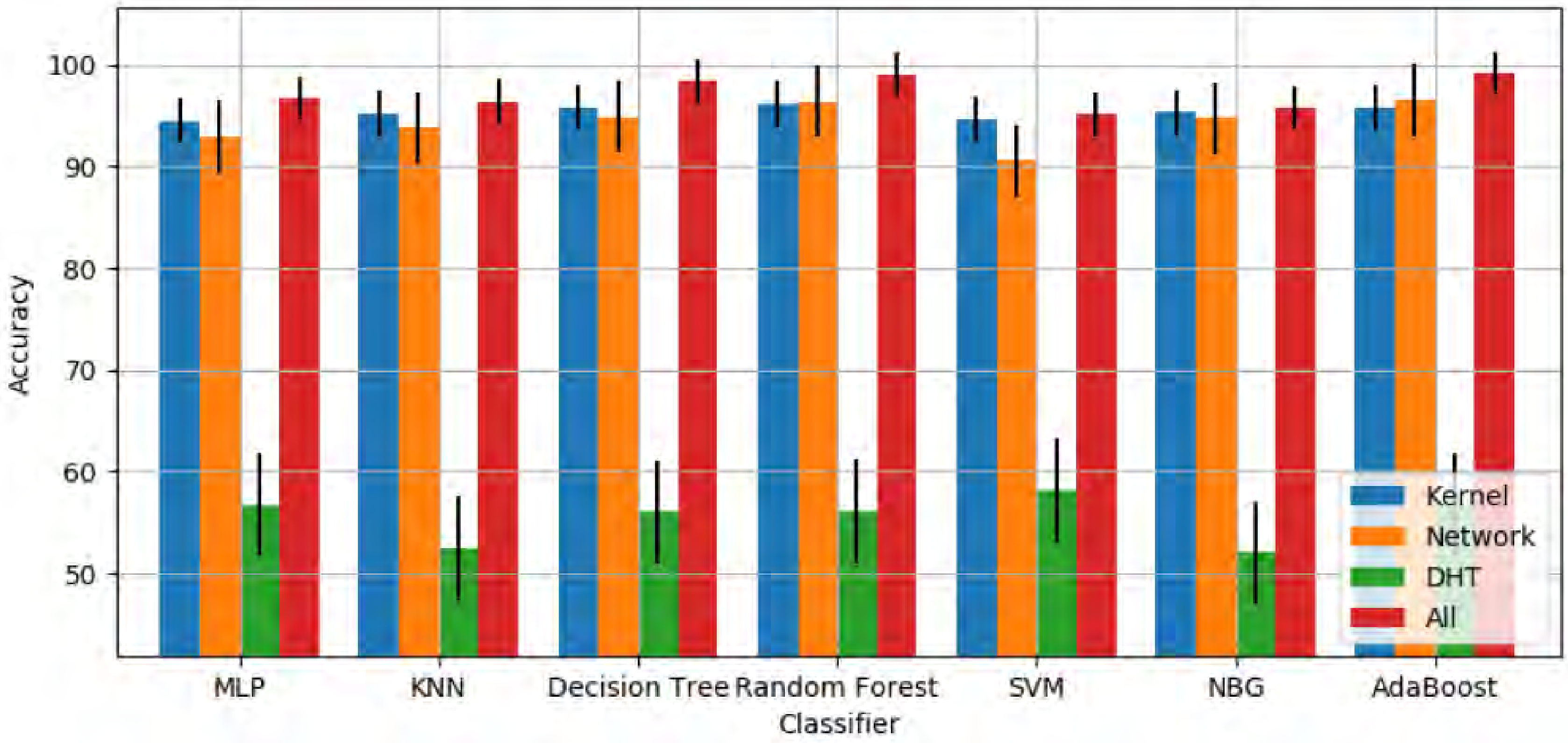


Data Level	Feature Group	Feature Description
Kernel	epoll_wait	Wait for an I/O event on an epoll file descriptor.
	read	Read from a file descriptor.
	mprotect	Set protection on a region of memory.
	mmap2	Map files into memory.
	close	Close a file descriptor.
	openat	Open and possibly create a file.
	fstat64	Get a file status.
	futex	Fast user-space locking.
	rt_sigaction	Examine and change a signal action.
	recvmsg	Receive a message from a socket.
	stat64	Get a file status.
	fcntl	Manipulate file descriptor.
	getdents64	Get directory entries.
	brk	Change data segment size.
	poll	Wait for some event on a file descriptor.
	write	Write to a file descriptor.
	uname	Get name and information about current kernel.
	pipe	Create pipe.
Network	total_packets[1]	Total packets.
	total_volume[1]	Total bytes.
	pktl[1,2]	Packets size.
	lat[1,2]	Amount of time between two packets.
	duration	Duration of the flow.
	active[2]	Amount of time flow was active.
	idle	Amount of time flow was idle.
	sflow_packets[1]	Number of packets in a sub flow.
	sflow_bytes[1]	Number of bytes in a sub flow.
	psh_cnt[1]	Number of times the PSH flag was set.
	urg_cnt[1]	Number of times the URG flag was set.
	total_hlen[1]	Total bytes used for headers.
DHT	GET	Number of GET operation performed on the DHT.
	PUT	Number of PUT operation performed on the DHT.

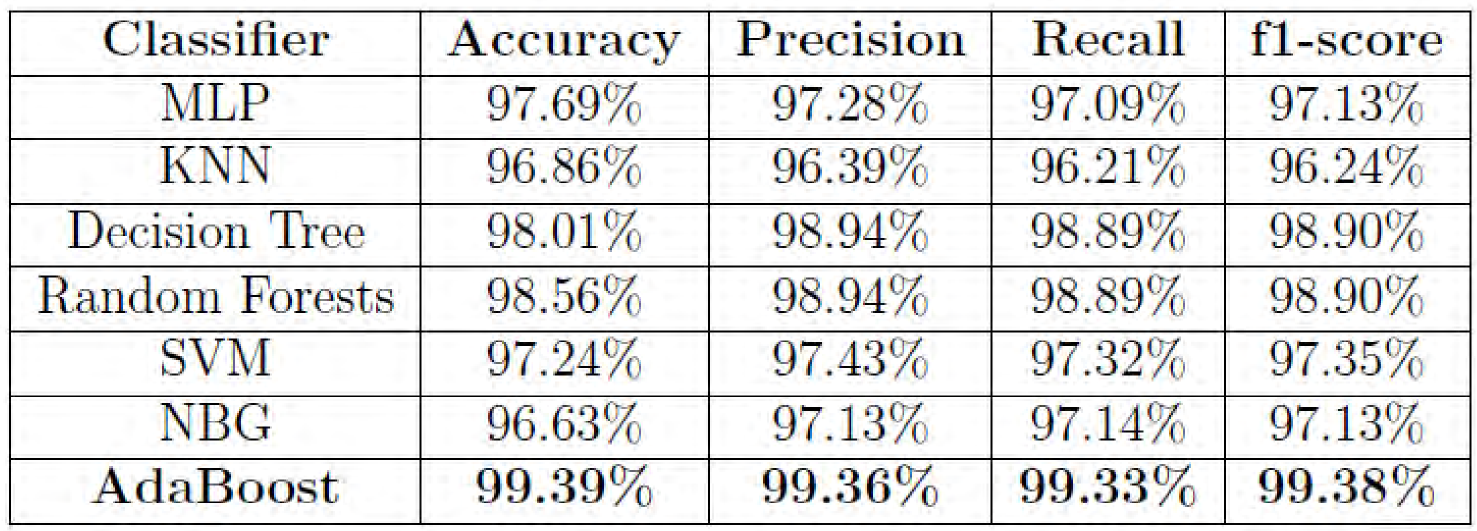
CLASSIFICATION RESULTS (SCANNER)



CLASSIFICATION RESULTS (DDOS)



CLASSIFICATION RESULTS



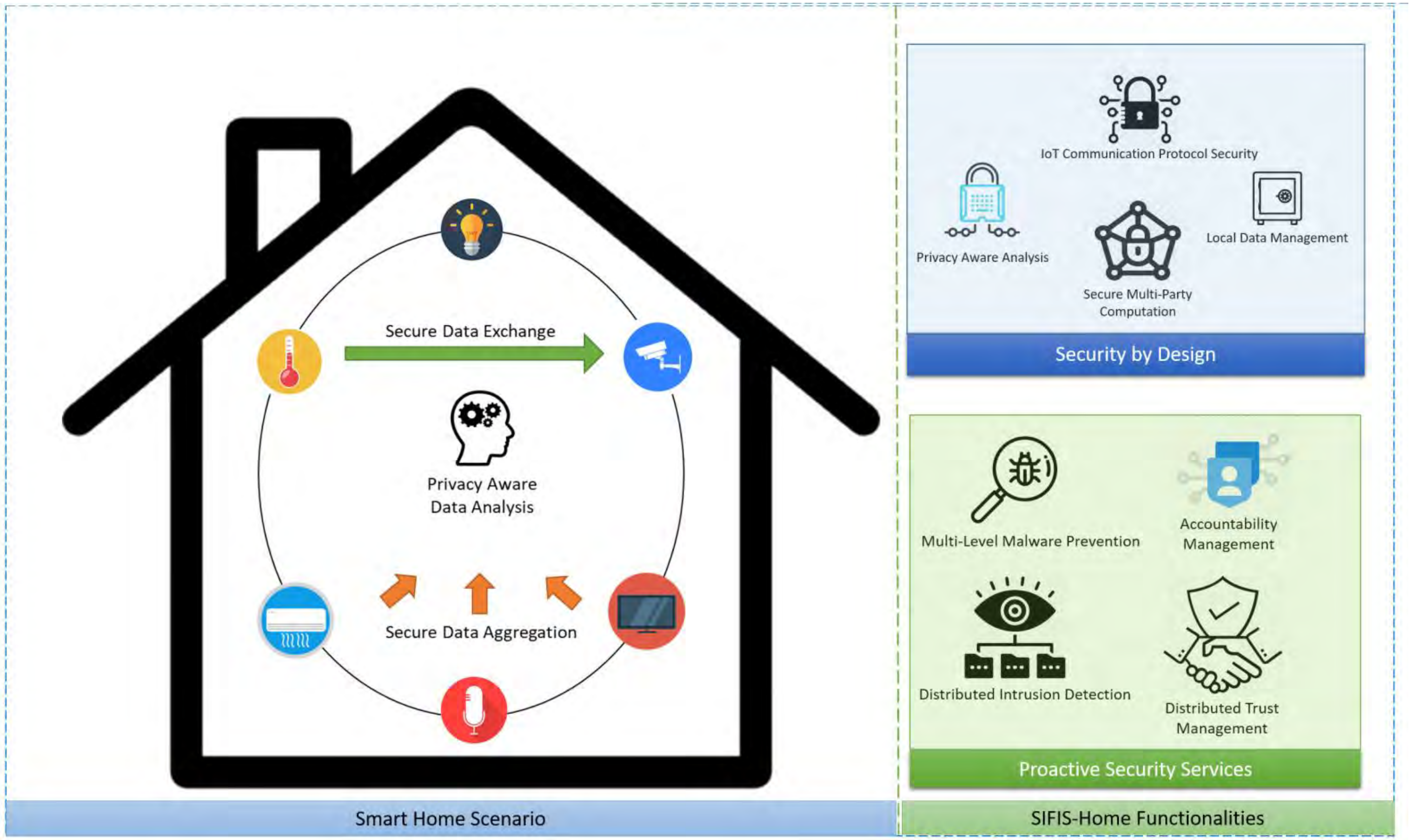
Classifier	Accuracy	Precision	Recall	f1-score
MLP	97.69%	97.28%	97.09%	97.13%
KNN	96.86%	96.39%	96.21%	96.24%
Decision Tree	98.01%	98.94%	98.89%	98.90%
Random Forests	98.56%	98.94%	98.89%	98.90%
SVM	97.24%	97.43%	97.32%	97.35%
NBG	96.63%	97.13%	97.14%	97.13%
AdaBoost	**99.39%**	**99.36%**	**99.33%**	**99.38%**

THE SIFIS-HOME PROJECT

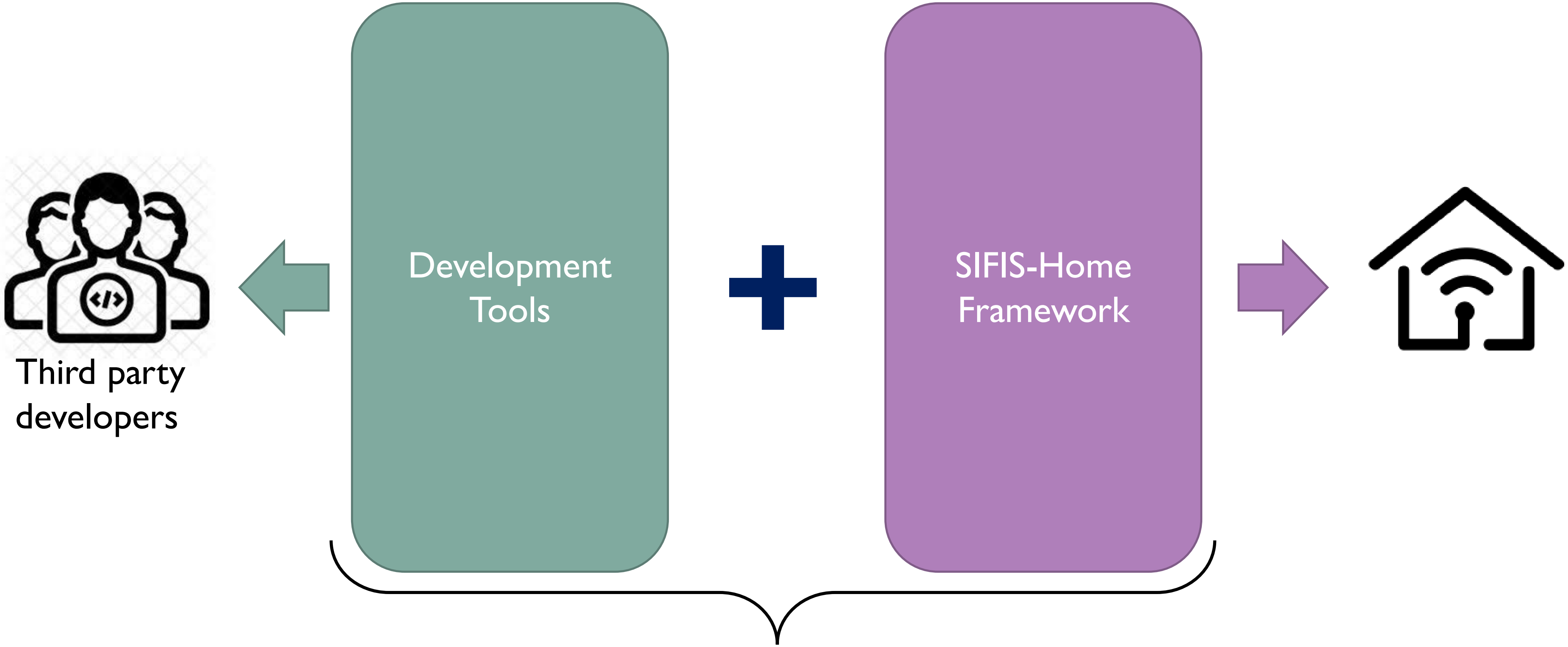
SIFIS-Home

EU project Funded by H2020 under
GA #952652

THE SIFIS-HOME CONCEPT



THE SIFIS-HOME SOLUTION



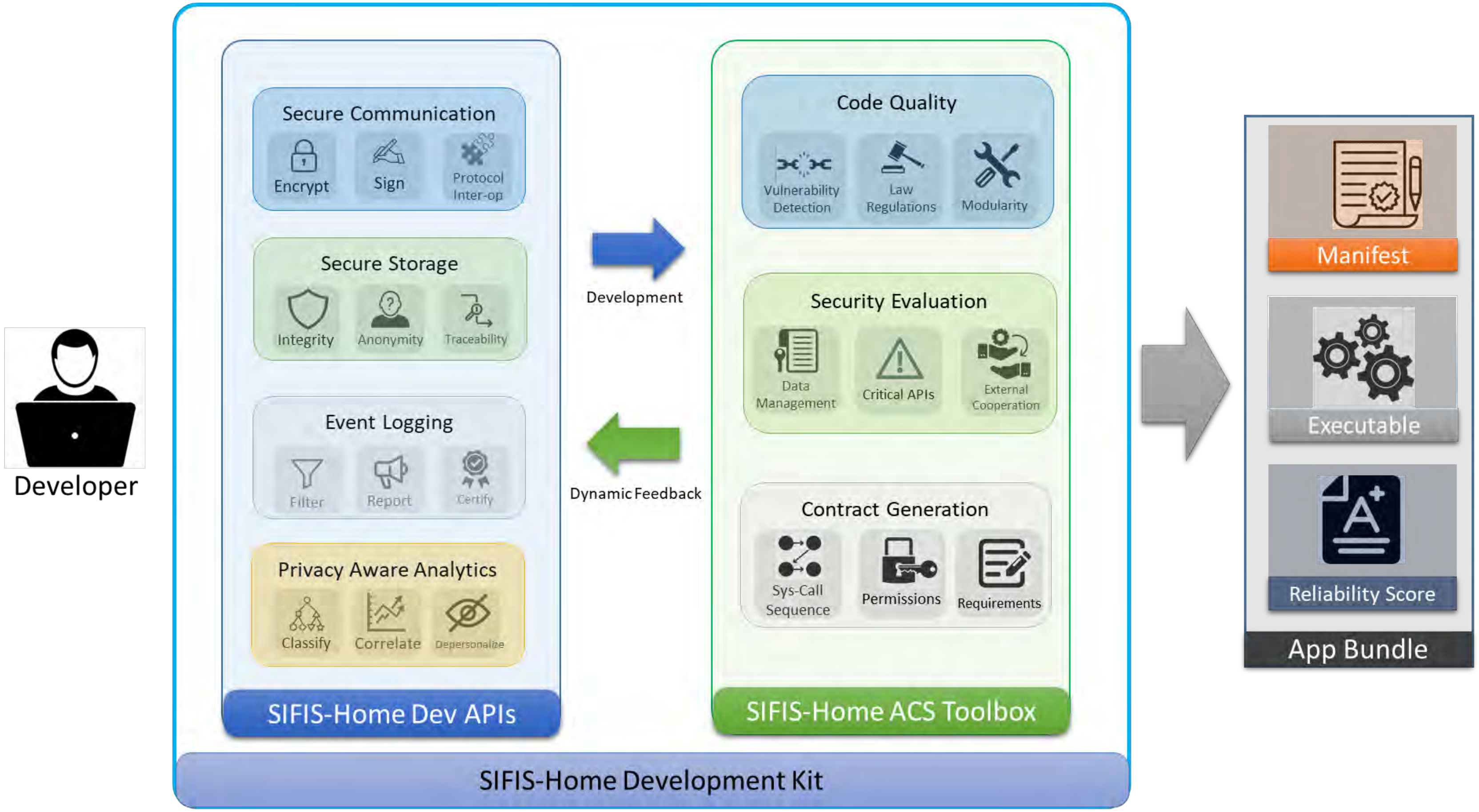
Third party developers

Development Tools

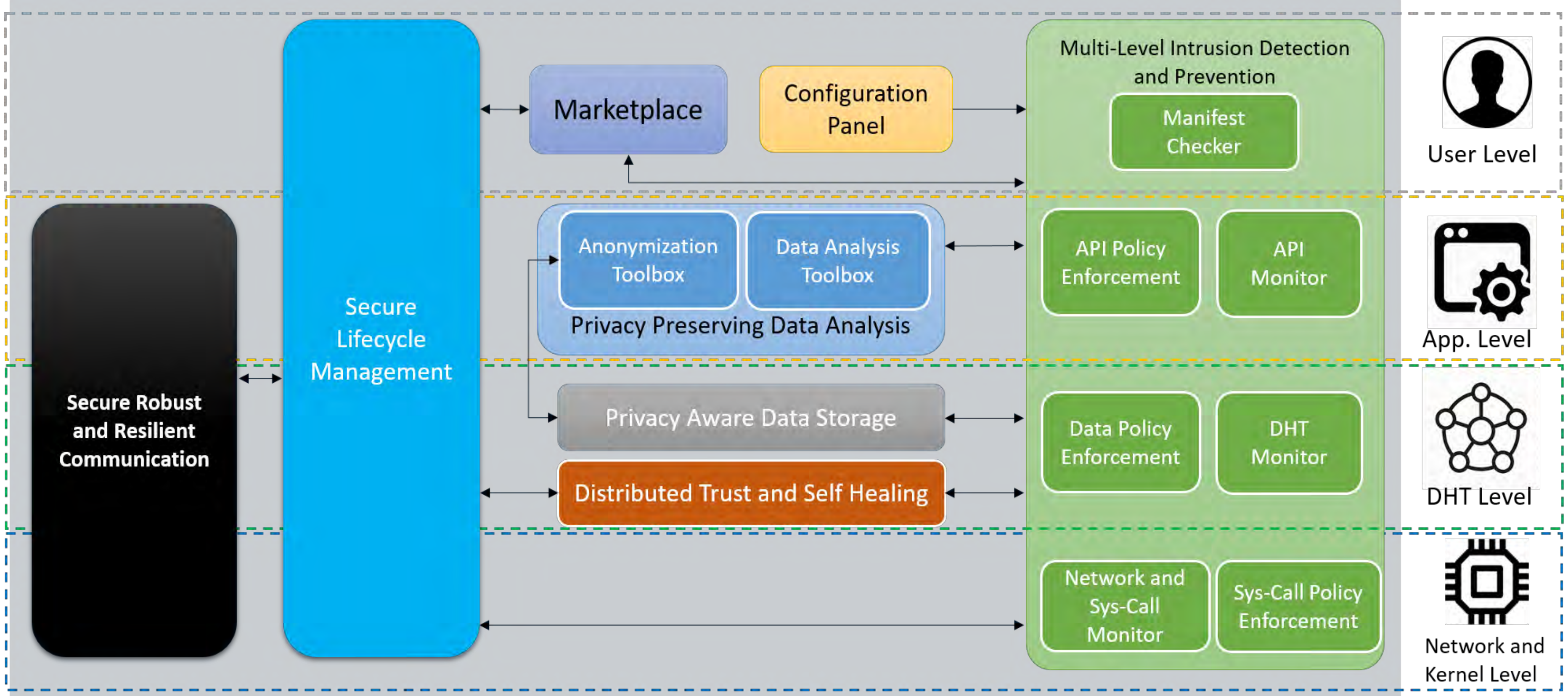
SIFIS-Home Framework

SIFIS-Home Solution

DEVELOPMENT TOOLS



SIFIS-HOME FRAMEWORK


Secure Robust and Resilient Communication
Secure Lifecycle Management
Marketplace
Configuration Panel
Multi-Level Intrusion Detection and Prevention
Manifest Checker
Anonymization Toolbox
Data Analysis Toolbox
Privacy Preserving Data Analysis
API Policy Enforcement
API Monitor
Privacy Aware Data Storage
Distributed Trust and Self Healing
Data Policy Enforcement
DHT Monitor
Network and Sys-Call Monitor
Sys-Call Policy Enforcement
User Level
App. Level
DHT Level
Network and Kernel Level

Full-Stack of the SIFIS-Home Security Architecture

MORE INFO

- Website: www.sifis-home.eu
- Twitter: @SifisHome
- LinkedIn: https://bit.ly/3f54GCZ

SIFIS-Home

THANKS FOR YOUR ATTENTION

Email: andrea.saracino@iit.cnr.it
Web: andreasaracino.it
Twitter: @iorisecurity

ISTITUTO
DI INFORMATICA
E TELEMATICA