

# Conceptualising an Anti-Digital Forensics Kill Chain for Smart Homes

Mario Raciti

*ICISSP 2024*



SCHOOL  
FOR ADVANCED  
STUDIES  
LUCCA



Università  
di Catania

28/02/24 – Rome

# Agenda

- 1. Introduction**
- 2. The Problem with ADF**
- 3. The Idea of a Kill Chain**
- 4. Conclusions**

# Agenda

- 1. Introduction**
2. The Problem with ADF
3. The Idea of a Kill Chain
4. Conclusions

## Amazon ordered to give Alexa evidence in double murder case

An Echo smart speaker, which features the artificial intelligence voice assistant Alexa, was seized from a home in Farmington where two women were stabbed to death

Anthony Cuthbertson • Wednesday 14 November 2018 22:13 GMT • [Comments](#)



US police think Amazon's voice assistant Alexa may have witnessed a double murder (Getty Images)

Your 'smart home' is watching - and possibly sharing your data with the police

*Albert Fox Cahn and Justin Sherman*

Smart-home devices like thermostats and fridges may be too smart for comfort - especially in a country with few laws preventing the sale of digital data to third parties



📷 'The documents and data we access remotely every day can end up in a gray zone outside the clear protections afforded in our homes and offices.' Photograph: Smith Collection/Gado/Getty Images

Computer/Digital Forensics

## The role of home devices in police investigations

If a smart speaker captures the audio of a serious crime, can it be used as evidence by the police and prosecution at trial?

August 27, 2019 03:26 PM



There is a possibility that the use of recordings from smart speaker devices could significantly influence criminal trials.

Photo/Pixabay

“The use of *scientifically derived and proven methods* toward the **identification, collection, validation, examination, analysis, and presentation** of **digital evidence** while preserving the integrity of the information, including process repeatability, and maintaining a strict chain of custody for the data”.

---

- Definition of Digital Forensics (DFRWS, 2001)

# A Goldmine for Evidence Collection

Smart homes offer various **digital evidence**:

## **Device Logs**

*(e.g., activities, commands, status changes)*

## **Network Traffic**

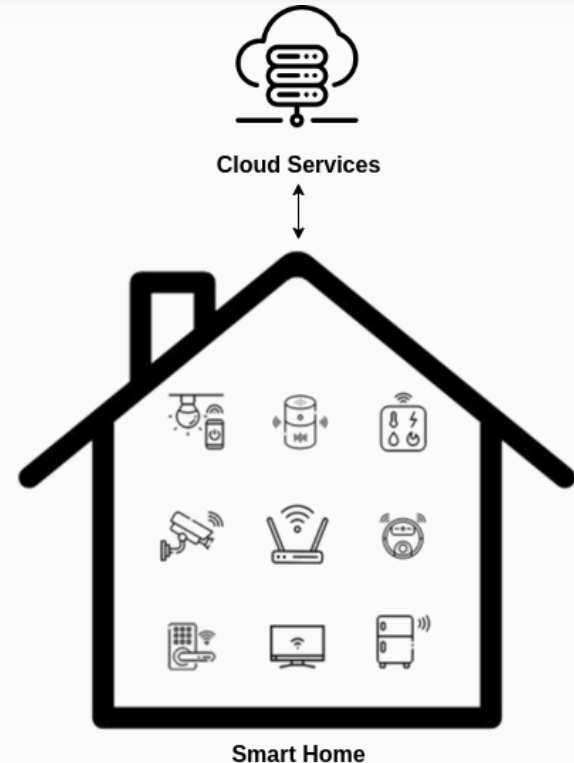
*(e.g., data flows between devices, patterns, anomalies)*

## **Sensor Readings**

*(e.g., temperature, motion, light)*

## **User Interactions**

*(e.g., behavioural patterns, schedules, preferences)*



# Not All That Glitters is Gold...

# Agenda

1. Introduction
- 2. The Problem with ADF**
3. The Idea of a Kill Chain
4. Conclusions



# Dealing with “Smart” Criminals



“Attempts to **negatively** affect the existence, amount and/or quality of **evidence** from a crime scene, or make the analysis and examination of evidence difficult or impossible to conduct”.

---

- Definition of Anti-Digital Forensics

# Classification of Anti-Forensics

**Anti-Digital Forensics** can be classified into **four categories**:

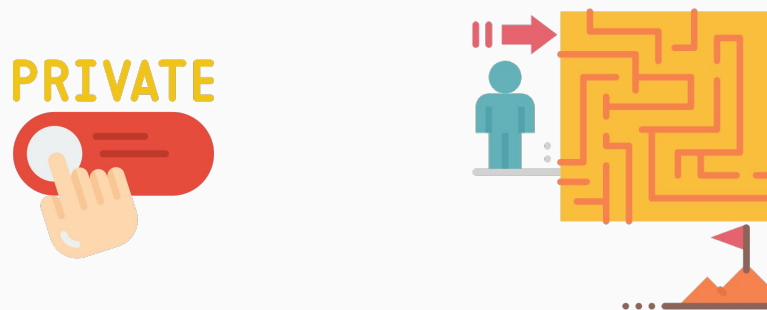
- > Data hiding
- > Artefact wiping
- > Trail obfuscation
- > Attacks against the forensic process and tool



# Implications of ADF

**ADF** may be used for *legitimate purposes* (e.g., privacy).

However, it adds **complexity** to digital investigations.



It is essential to understand ADF to *anticipate and counter* emerging **threats**.

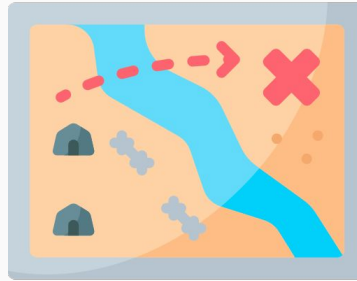
RQ: What are the ADF steps  
in a Smart Home ecosystem?

# Agenda

1. Introduction
2. The Problem with ADF
- 3. The Idea of a Kill Chain**
4. Conclusions

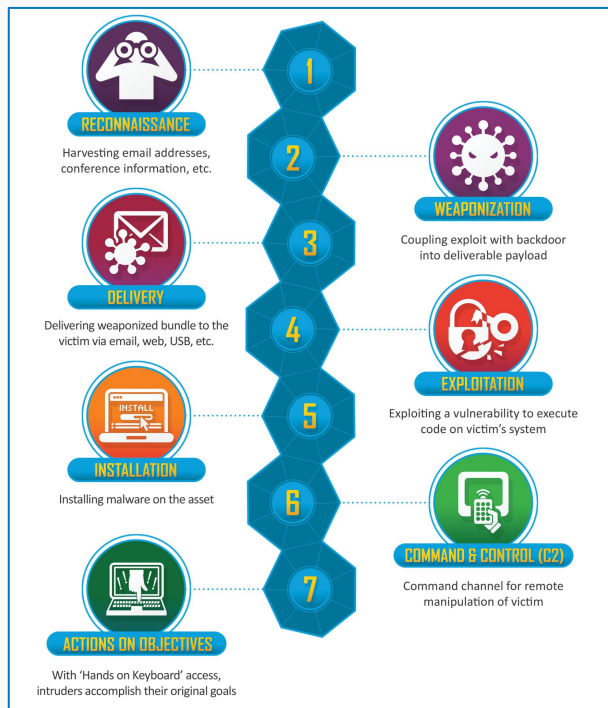
# What is a Kill Chain?

A **kill chain** is a military concept that identifies the structure of an attack.



Understanding a cyber kill chain means  
having *knowledge* about TTPs ⇒ **effective defence strategies**.

# CySec Kill Chain Examples



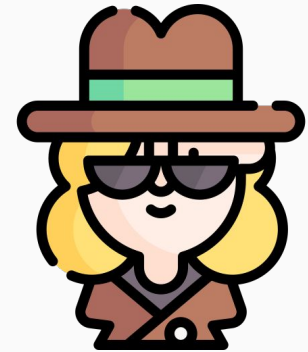
ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (2) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (3) Gather Victim Org Information (4) Phishing for Information (4) Search Closed Sources (2) Search Open Websites/Domains (3) Search Victim-Owned Websites	Acquire Access Infrastructure (4) Compromise Accounts (2) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (4) Stage Capabilities (4)	Content Injection Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Cloud Administration Command Command and Scripting Interpreter (2) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Native API Scheduled Task/Job (2) Serviceless Execution Shared Modules Software Deployment Tools System Services (2) User Execution (2) Windows Management Instrumentation	Account Manipulation (2) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Browser Extensions Compromise Client Software Binary Create Account (2) Create or Modify System Process (4) Event Triggered Execution (16) External Remote Services Hijack Execution Flow (12) Implant Internal Implant Modify Authentication Process (4) Office Application Valid Accounts (2)	Abuse Elevation Control Mechanism (3) Access Token Manipulation (3) BITS Jobs Account Manipulation (4) Boot or Logon Autostart Execution (4) Boot or Logon Initialization Scripts (3) Boot or Logon Initialization Scripts (3) Create or Modify System Process (4) Domain Policy Modification (2) Domain Policy Modification (2) Execution Guardrails (3) Exploitation for Defense Evasion Escape to Host Event Triggered Execution (16) File and Directory Permissions Modification (2) Hide Artifacts (11) Hijack Execution Flow (12) Impair Defenses (11) Impersonation Indicator Removal (3) Indirect Command Execution Valid Accounts (2) Masquerading (2)	Abuse Elevation Control Mechanism (3) Access Token Manipulation (3) Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (3) Exploitation for Defense Evasion Escape to Host File and Directory Permissions Modification (2) Hide Artifacts (11) Hijack Execution Flow (12) Impair Defenses (11) Impersonation Indicator Removal (3) Indirect Command Execution Valid Accounts (2) Masquerading (2)	Adversary-in-the-Middle (2) Brute Force (4) Credentials from Password Stores (3) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (4) Multi-Factor Authentication Request Generation Network Sniffing OS Credential Dumping (3) Seal Application Access Token Steal or Forge	Account Discovery (4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource Discovery Debugger Evasion Device Driver Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Log Enumeration Network Service Discovery Network Share Discovery Network Sniffing Password Policy	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (4) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4) Data from Local System Data from Non-Application Layer Protocol Data from Removable Media Data Staged (2) Email Collection (3) Input	Adversary-in-the-Middle (2) Archive Collected Data (3) Audio Capture Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Data from Configuration Repository (2) Data from Information Repositories (3) Data from Local System Data from Non-Application Layer Protocol Data from Removable Media Data Staged (2) Email Collection (3) Input	Application Layer Protocol (4) Communication Through Removable Media Content Injection Data Encoding (2) Data Offuscation (3) Dynamic Resolution (2) Encrypted Channel (2) Fallback Channels Exploitation Over Web Service (4) Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software	Automated Exfiltration (3) Data Transfer Size Limits Exfiltration Over Alternative Protocol (2) Exfiltration Over 12 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Medium (1) Exfiltration Over Web Service (4) Scheduled Transfer Transfer Data to Cloud Account System Shutdown/Reboot	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Endpoint Denial of Service (4) Financial Theft Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot



# A Double Scenario



# A Double Scenario (1)



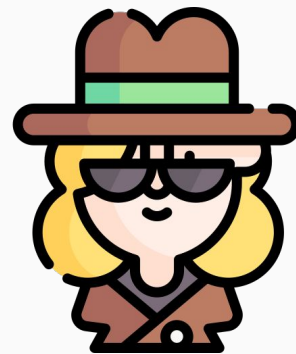
**Mr. X** seeks to evade *DF* detection by tampering with and destroying digital evidence from Smart Home IoT devices.

Believing he can create a *false narrative* to defend against charges, **Mr. X** leverages the Kill Chain to carry out his **digital alibi** fabrication scheme.

# A Double Scenario (2)

**Mrs. Y** aims to understand the steps Mr. X took to hinder the investigation in the Smart Home crime scene.

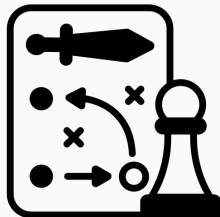
**Mrs. Y** applies the ADF Kill Chain for Digital Forensics purposes, bringing out Mr. X's tactics to **counteract** the digital alibi fabrication.



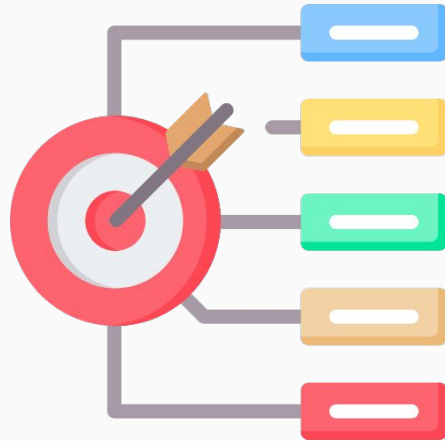
# An ADF Kill Chain for Smart Homes

The **ADF Kill Chain** aim is twofold:

- > *Malicious actors* can leverage it as a tool for the exploitation of forensic vulnerabilities.
- > Understanding adversary tactics to empower *law enforcement* to counter those efforts.



# Research Goals



Review of **ADF in Smart Home**

Intersection of **Privacy and ADF**

Integration of **AI** for ADF in Smart Home

Design of **ADF Kill Chain for Smart Home**

**Case studies** and real-world applications

# A Preliminary Conceptualisation

## Step A — Tampering with Digital Traces

Objective: Manipulate or erase digital traces to obstruct forensic investigation.

Activities: Tampering with audio recordings, video footage, and device interaction logs. Implementing techniques to make forensic analysis challenging.

## Step B — Concealing Identities

Objective: Conceal the identity of malicious actors involved in ADF activities.

Activities: Masking IP addresses and digital footprints. Falsifying user identities associated with Smart Home devices.

## Step C — Misleading Investigators

Objective: Introduce false information to mislead forensic investigators.

Activities: Planting deceptive digital breadcrumbs and manipulating timestamps and metadata.

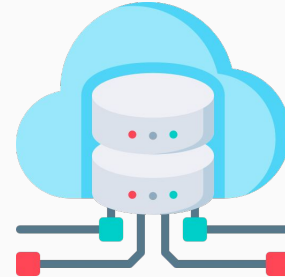
## Step D — Cloud Data Manipulation

Objective: Manipulate data stored in cloud services associated with Smart Home devices.

Activities: Getting remote access to cloud services where Smart Home data is stored. Tamper with or delete such data remotely, ensuring techniques to avoid logging.

# Expected Challenges

1. Device heterogeneity
2. Resource constraints and scalability
3. Forensic readiness
4. Cloud services



# Takeaways

- Kill two birds with a chain
- Better discernment of ADF



# Agenda

1. Introduction
2. The Problem with ADF
3. The Idea of a Kill Chain
- 4. Conclusions**

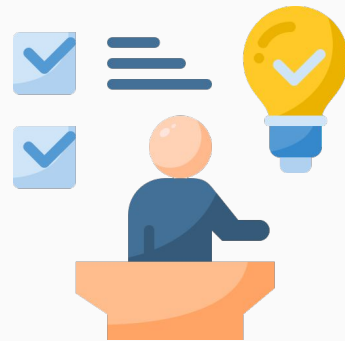
# Conclusions

This paper encouraged future research to **enhance the comprehension** of **ADF**, in particular within *Smart Home* ecosystems.

*Ethical concerns* for a criminal-supported Kill Chain are alleviated by the **dual outcome** of understanding adversarial tactics (**Anti-Anti-Forensics**).

## Future work:

- Fulfil research objectives
- Overcome expected challenges



# Thanks for your attention!

For more information or questions:

 [mario.raciti@imtlucca.it](mailto:mario.raciti@imtlucca.it) – [mario.raciti@phd.unict.it](mailto:mario.raciti@phd.unict.it)

 <https://tsumarios.github.io/>

 [@tsumarios](https://twitter.com/tsumarios)

 <https://linkedin.com/in/marioraciti>



*Non-malicious QR (maybe)*