

Conceptualising an Anti-Digital Forensics Kill Chain for Smart Homes

Mario Raciti

ICISSP 2024



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



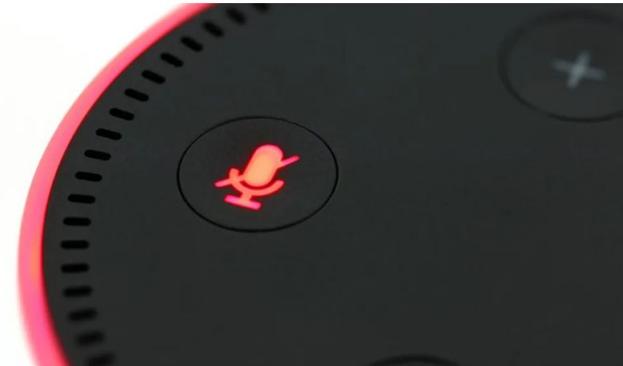
📷 'The documents and data we access remotely every day can end up in a gray zone outside the clear protections afforded in our homes and offices.' Photograph: Smith Collection/Gado/Getty Images

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

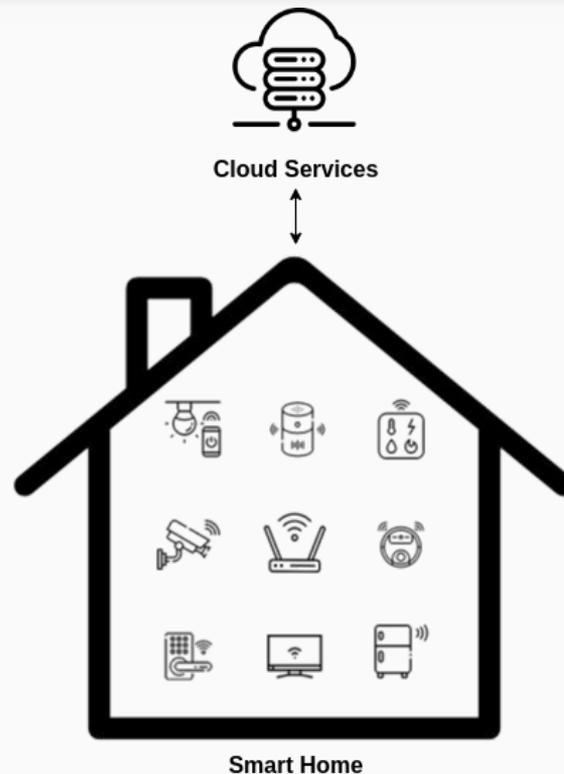
(e.g., data flows between devices, patterns, anomalies)

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**:

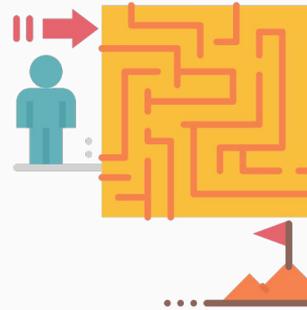
- > Data hiding
- > Artefact wiping
- > Trail obfuscation
- > Attacks against the forensic process and tool



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

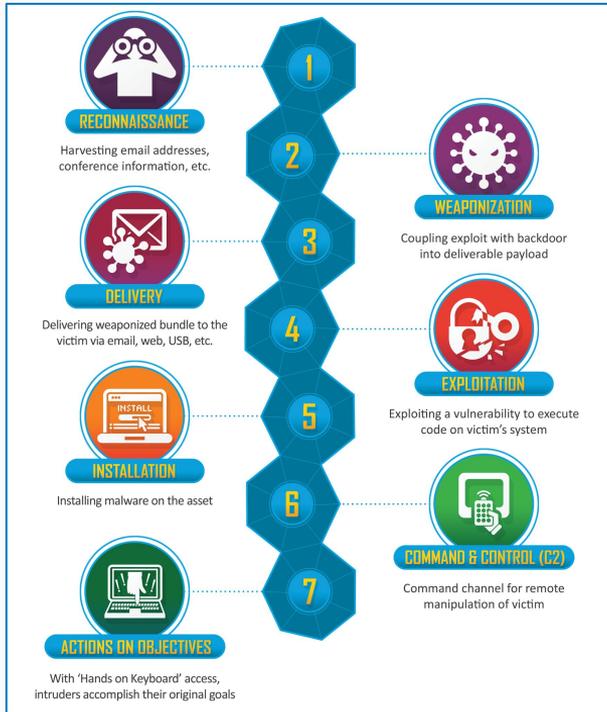
What is a Kill Chain?

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 (3) 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 Technical Databases (2) Search Open Websites/Domains (3) Search Victim-Owned Websites	Acquire Access Infrastructure (2) Drive-by Compromise (3) Exploit Public-Facing Application (2) Develop Capabilities (4) Establish Accounts (2) Obtain Capabilities (4) Stage Capabilities (4) Valid Accounts (4)	Content Injection (2) Drive-by Compromise (3) Exploit Public-Facing Application (2) External Remote Services (4) Hardware Additions (2) Phishing (4) Replication Through Removable Media (2) Supply Chain Compromise (2) Trusted Relationship (2) Valid Accounts (4)	Cloud Administration Command (2) Command and Scripting Interpreter (2) Container Administration Command (2) Deploy Container (2) Exploitation for Client Execution (2) Inter-Process Communication (2) Native API (2) Scheduled Task/Job (2) Serverless Execution (2) Shared Modules (2) Software Deployment Tools (2) System Services (2) User Execution (2) Windows Management Instrumentation	Account Manipulation (2) BITS Jobs (2) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Browser Extensions (2) Compromise Client Software Binary (2) Create or Modify System Process (4) Create or Modify System Process (4) Domain Policy Modification (2) Escape to Host (2) Event Triggered Execution (16) External Remote Services (2) Hijack Execution Flow (12) Implant Internal Image (2) Modify Authentication Process (4) Office Application (2) Valid Accounts (2)	Abuse Elevation Control Mechanism (2) Access Token Manipulation (3) Account Manipulation (4) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (3) Boot or Logon Initialization Scripts (3) Create or Modify System Process (4) Domain Policy Modification (2) Execution for Defense Evasion (2) Event Triggered Execution (16) Exploitation for Privilege Escalation (2) Hijack Execution Flow (12) Process Injection (12) Scheduled Task/Job (2) Valid Accounts (2)	Abuse Elevation Control Mechanism (2) Access Token Manipulation (3) BITS Jobs (2) Build Image on Host (2) Exploitation for Credential Access (2) Deobfuscate/Decode Files or Information (2) Deploy Container (2) Direct Volume Access (2) Domain Policy Modification (2) Execution Guardrails (3) Exploitation for Defense Evasion (2) File and Directory Permissions Modification (2) Hide Artifacts (11) Hijack Execution Flow (12) Impair Defenses (11) Impersonation (2) Indicator Removal (6) Indirect Command Execution (2) Masquerading (2)	Adversary in-the-Middle (3) Route Forward (2) Credentials from Password Stores (3) Exploitation for Credential Access (2) Forced Authentication (2) Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (2) Multi Factor Authentication Interception (2) Multi Factor Authentication Request Generation (2) Network Sniffing (2) OS Credential Dumping (4) Seal Application Access Token (2) Steal or Forge (2)	Account Discovery (4) Application Window Discovery (2) Browser Information Discovery (2) Cloud Infrastructure Discovery (2) Cloud Service Dashboard (2) Cloud Storage Object Discovery (2) Container and Resource Discovery (2) Debugger Evasion (2) Device Driver Discovery (2) Domain Trust Discovery (2) File and Directory Discovery (2) Group Policy Discovery (2) Log Enumeration (2) Network Share Discovery (2) Network Sniffing (2) Password Policy (2)	Exploitation of Remote Services (2) Internal Spearphishing (2) Lateral Tool Transfer (2) Remote Service Session Hijacking (2) Remote Services (4) Replication Through Removable Media (2) Software Deployment Tools (2) Taint Shared Content (2) Use Alternate Authentication Material (4) Network Share Discovery (2) Network Sniffing (2) Password Policy (2)	Adversary in-the-Middle (3) Automated Collection (2) Audio Capture (2) Content Injection (2) Browser Session Hijacking (2) Clipboard Data (2) Dynamic Resolution (2) Encrypted Channel (2) Fallback Channels (2) Ingress Tool Transfer (2) Local System (2) Data from Network Shared Drive (2) Data from Removable Media (2) Data Staged (2) Email Collection (2) Input (2)	Application Layer Protocol (4) Communication Through Removable Media (2) Exfiltration Over Alternative Protocol (2) Exfiltration Over C2 Channel (2) Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (2) Encrypted Channel (2) Fallback Channels (2) Ingress Tool Transfer (2) Multi Stage Channels (2) Non-Application Layer Protocol (2) Non-Standard Port (2) Protocol Tunneling (2) Proxy (4) Remote Access Software (2)	Automated Exfiltration (3) Data Destruction (2) Data Encrypted for Impact (2) Data Manipulation (2) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Financial Theft (2) Firmware Corruption (2) Inhibit System Recovery (2) Network Denial of Service (4) Resource Hijacking (2) Service Stop (2) System Shutdown/Reboot (2)	

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.

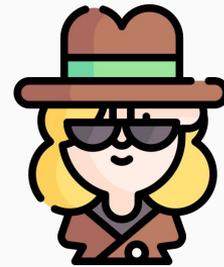
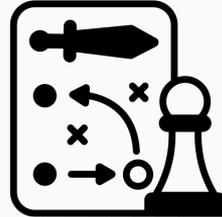
Mrs. Y applies the ADF Kill Chain for Digital Forensics purposes, bringing out Mr. X's tactics to **counteract** the digital alibi fabrication.



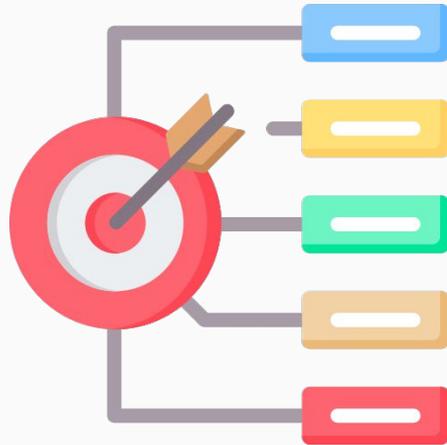
An ADF Kill Chain for Smart Homes

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**

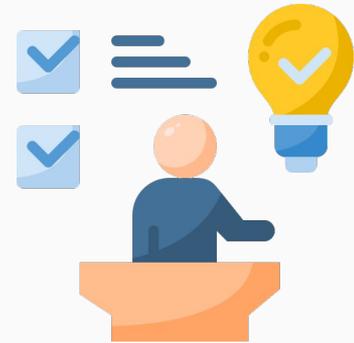
Conclusions

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 - mario.raciti@phd.unict.it

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

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

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



Non-malicious QR (maybe)