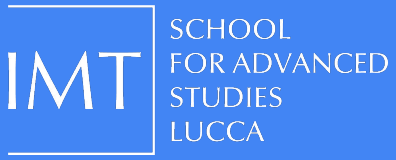
Conceptualising an Anti-Digital Forensics Kill Chain for Smart Homes

Mario Raciti

ICISSP 2024



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

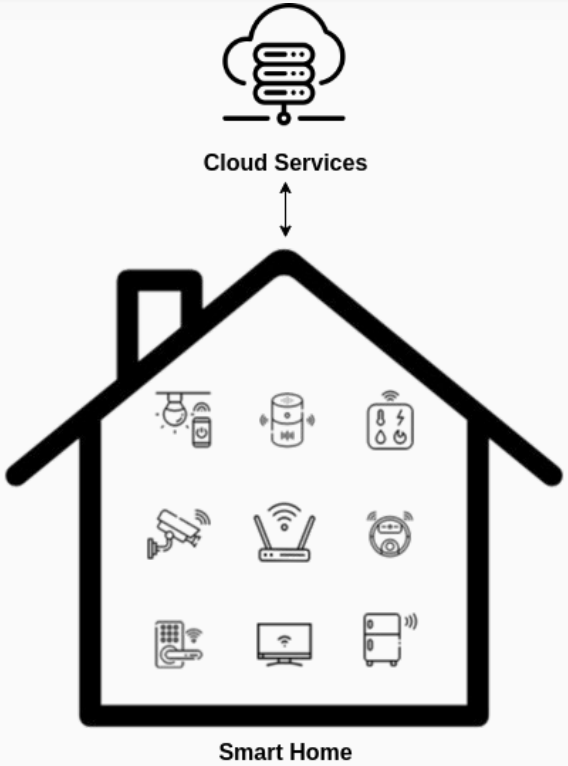
Smart homes offer various **digital evidence**:

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

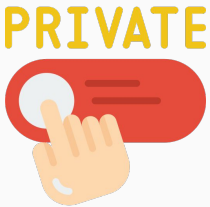
> Trail obfuscation

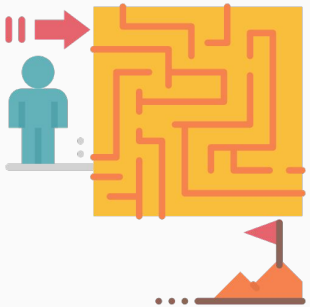
> Attacks against the forensic process and tool

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

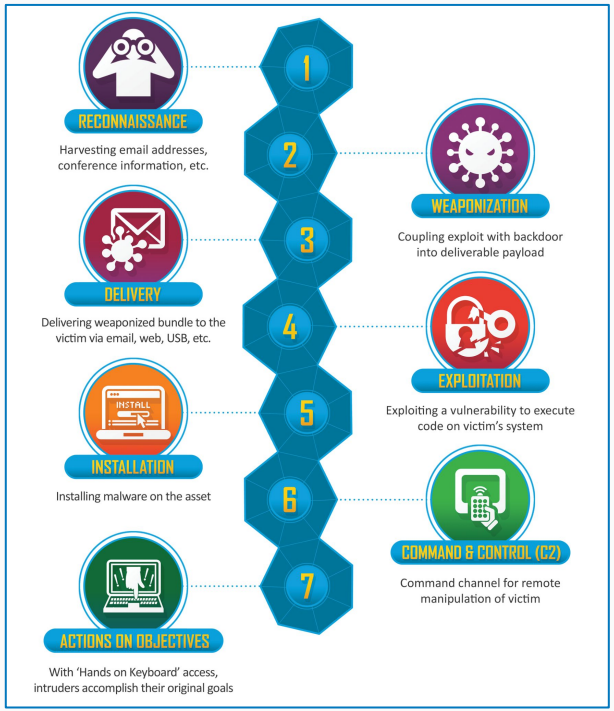
1. Introduction
2. The Problem with ADF
3. **The Idea of a Kill Chain**
4. Conclusions

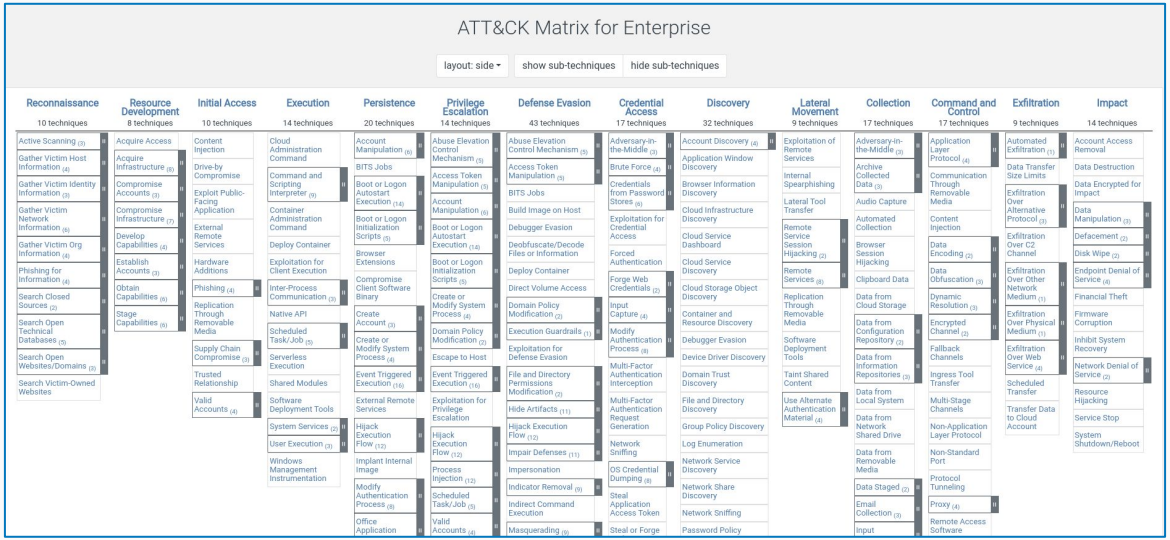
What is a Kill Chain?

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

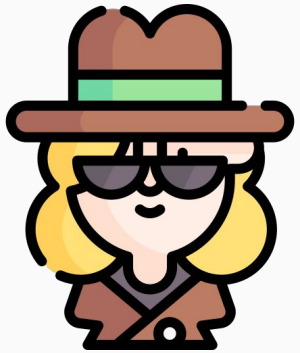
Understanding a cyber kill chain means
having *knowledge* about TTPs ⇒ **effective defence strategies**.

CySec Kill Chain Examples





A Double Scenario



A Double Scenario (1)

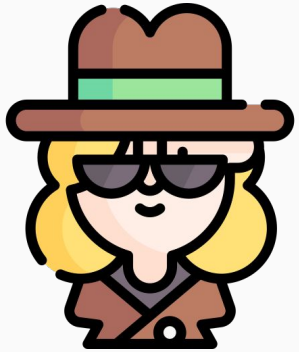
Mr. X seeks to *evade DF detection* by tampering with and destroying digital evidence from Smart Home IoT devices.

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.

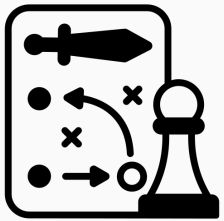


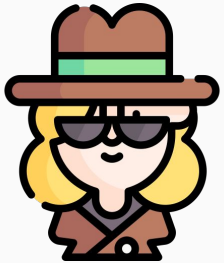
An ADF Kill Chain for Smart Homes

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.

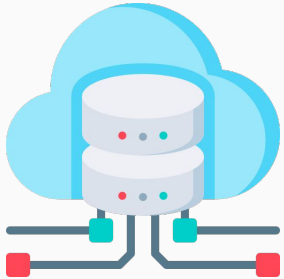
Step D — Cloud Data Manipulation

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

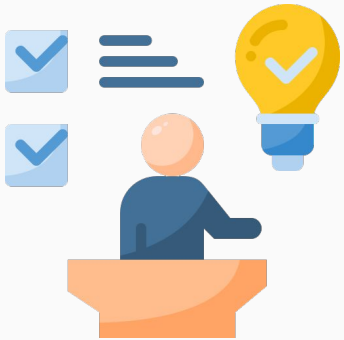
Agenda

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://linkedin.com/in/marioraciti

Non-malicious QR (maybe)