Hey KIMYA!

Is My Smart Speaker Spying on Me?

Taking Control of Sensor Privacy Through Isolation and Amnesia

Piet De Vaere and Adrian Perrig
ETH Zürich
Smart speakers come with a paradox.

Require a high-level of trust in vendor honesty & competence

Vendors have repeatedly broken this trust

*Apple contractors 'regularly hear confidential details' on Siri recordings*

*Workers hear drug deals, medical details and people having sex, says whistleblower*
Today’s status indicators are opaque & (probably) not very secure.

Can we do better?
First attempt: a microphone gateway.

Problem: when to grant access?
Second attempt: event-detection container.

Problem: no control over storage
Solution: **amnesic** event-detection container.
KIMYA segments the Microcontroller (MCU) into five memory regions.
KIMYA introduces 4 different MCU phases.

**IDLE**
**KIMYA introduces 4 different MCU phases.**

**ACQUIRE**
KIMYA introduces 4 different MCU phases.

PROCESS
If an event has been detected, the MCU is **TRIGGERED**

![Diagram showing memory allocation and notification generation](image)

- Buffer A
- Buffer B
- Scratch
- IMYA container
- All other memory
- Sensor
- Notification generated
- Read + Write
- Read only
Each $0.5 T_{\text{lifetime}}$, buffers are alternated and wiped.

$\Rightarrow$ Maximum data age: $T_{\text{lifetime}}$
In the paper:
Implementation with TrustZone on Cortex-M.

What is an “interaction”? When does it \textit{start}, when does it \textit{end}?

How to enforce \textit{isolation} ... ... in a way that’s compatible with \textit{existing OSes} ... without \{\textit{timing, cache, peripheral, ...}\} \textit{covert channels}
Kimya introduces 1 ms of latency

No additional HW required

Evaluated using on-chip keyword-spotting pipeline (mel spectrum + CNN)

only 1.19 ms of latency (spread = 0.03 ms)

Detailed benchmarks in paper
Conclusion

Smart speakers come with a paradox & current protections are insufficient

**KIMYA** provides an isolated and amnesic event-detection container that
- Introduces low overhead,
- does not restrict which algorithms can be used,
- and is independent of crypto.

Questions? Job offers?
→ piet@devae.re