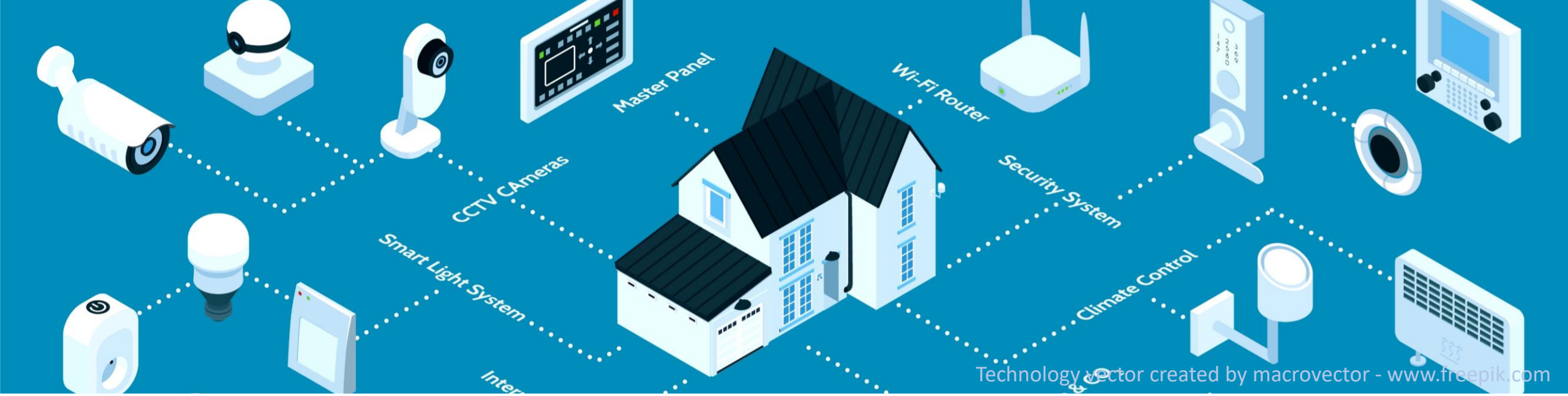


SoK: Context Sensing for Access Control in the Adversarial Home IoT

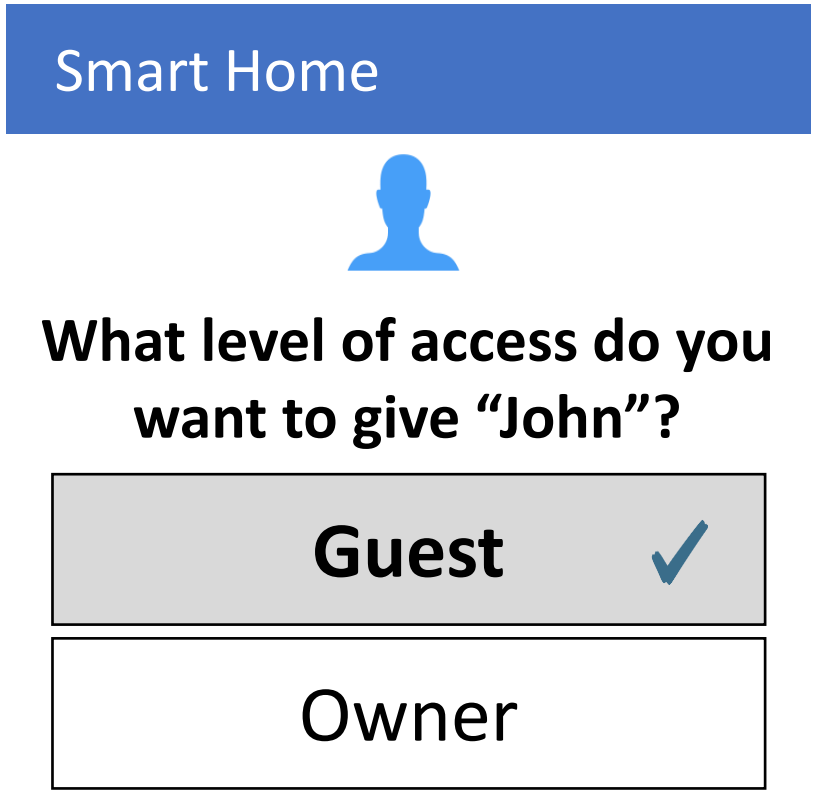
Weijia He (hewj@uchicago.edu), Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, Earlence Fernandes, Josiah Hester, Blase Ur

THE UNIVERSITY OF CHICAGO

WISCONSIN
UNIVERSITY OF WISCONSIN-MADISON

Northwestern University

Access Control in Smart Homes



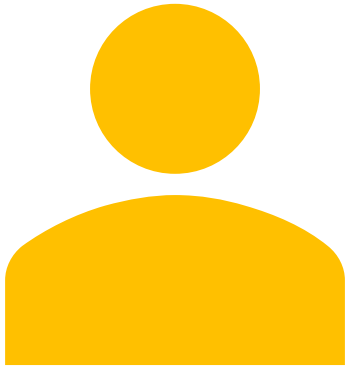
Users Desire More Context-Aware Policies

[They can have access] If they are **within a set range of the device**.

Context: User proximity to device

Users Desire More Context-Aware Policies

A child can only have access to the device when **an adult is around**.



Contexts: User age; people in the same room

Users Desire More Context-Aware Policies

Identity / Role at home

Age (Adult Nearby)

Emergency (e.g., Fire)

No one nearby

People asleep nearby

Owner's away

We identified 10 common contexts.

Users in the same house as the device

People in the same house as the user

Users in the same room as the device

People in the same room as the user

Desired Contexts

Identity / Role at home

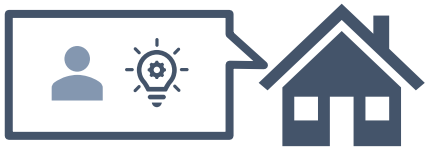
Age (Adult Nearby)

Emergency (e.g., Fire)

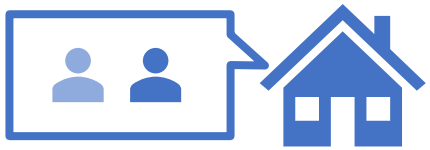
No one nearby

People asleep nearby

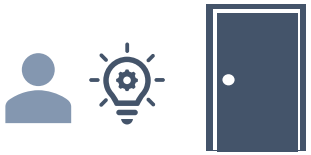
Owner’s away



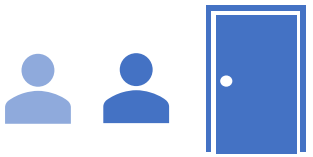
Users in the same house as the device



People in the same house as the user



Users in the same room as the device



People in the same room as the user

Literature Review

Literature Review

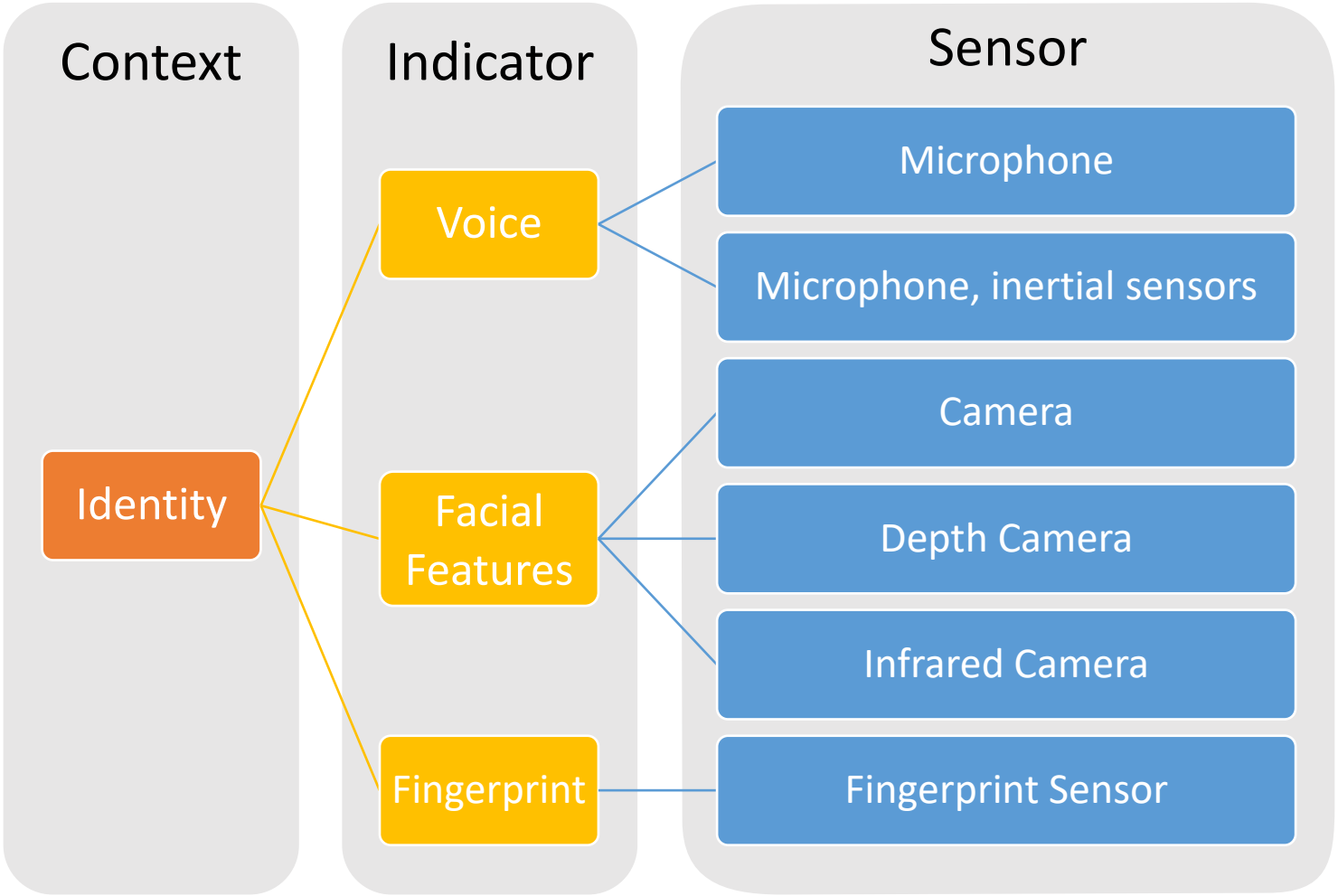
Sensing: SenSys, MobiSys, MobiCom

Ubiquitous Computing: UbiComp/IMWUT

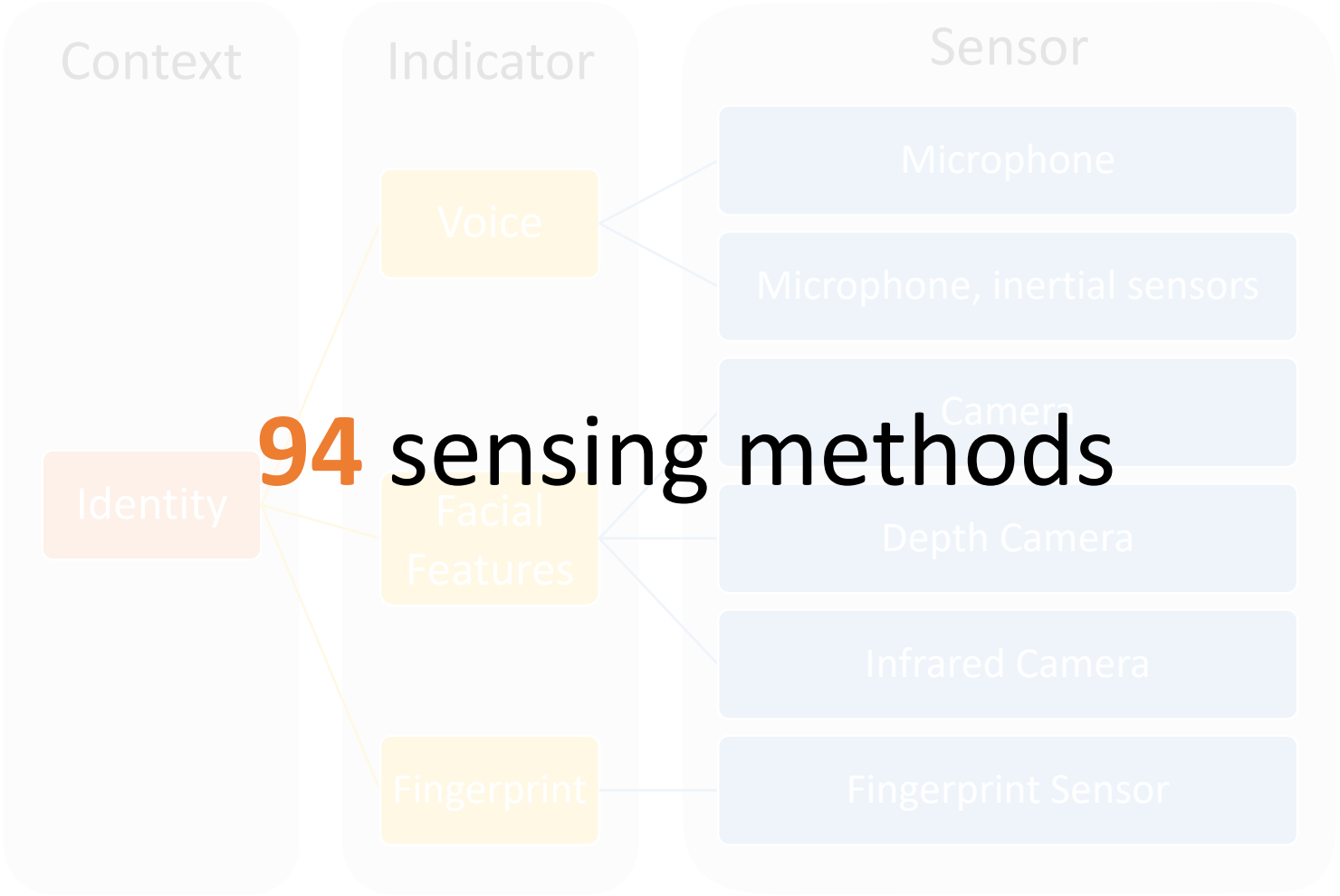
HCI: CHI, UIST

Commercial Products

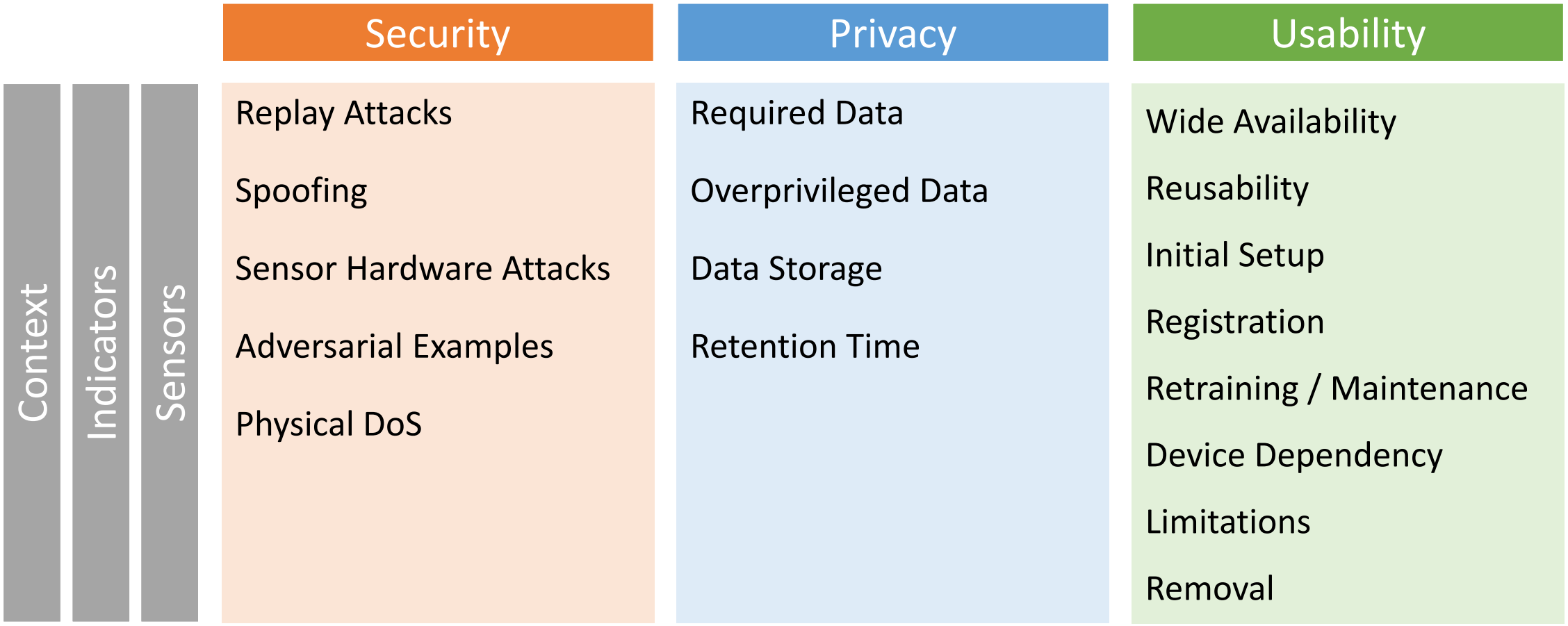
Context Sensing for Access Control



Context Sensing for Access Control



Decision Framework



A Threat Model

Remote Attackers

A New Threat Model - Attackers

Local Attackers

Non-Technical / Technical

Access to devices / Proximate to devices

Familiar wit the victim

A New Threat Model – Goals

A child can only have access to the device when **an adult is around**.

Impersonation

A New Threat Model – Goals

Invisibility

Security

Replay Attacks

Spoofing

Sensor Hardware Attacks

Adversarial Examples

Physical DoS

Impersonation

Invisibility

Privacy

Required Data	Data that must be collected for functionality.
Overprivileged Data	Data that is collected but not necessary for functionality.
Data Storage	Where the data needs to be stored for functioning.
Retention Time	How long the data must be retained for functioning.

Privacy

Facial Identification

Required Data

Facial features

Overprivileged Data

Surroundings, bystanders, etc.

Data Storage

Cloud (video/image processing can be expensive in both storage and computation)

Retention Time

The model data must be stored for identification.

Usability

Wide Availability

Reusability

The sensor can be used for multiple sensing methods (e.g. camera)

Initial Setup

Registration

Retraining / Maintenance

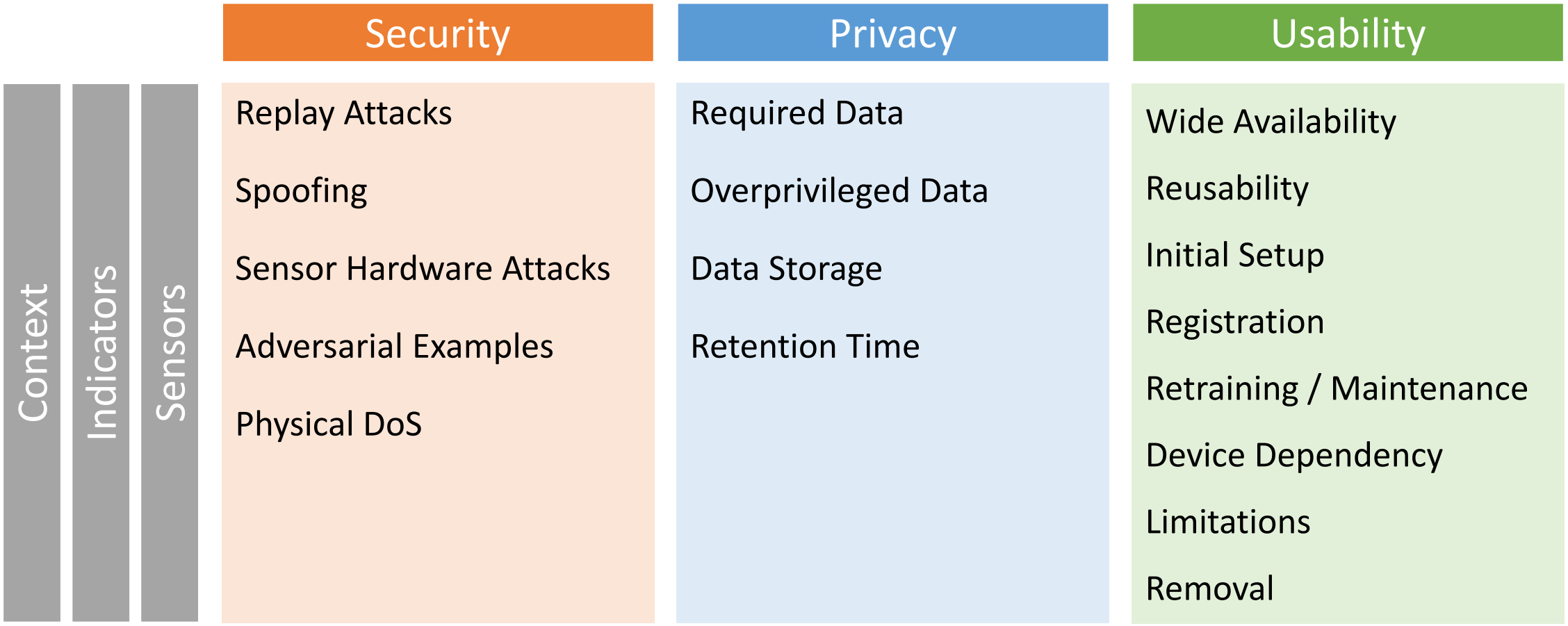
Device Dependency

Limitations

The sensing method doesn’t work for some groups of people.

Removal

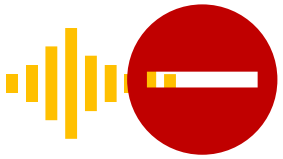
Decision Framework



Evaluation

Contexts	Indicators	Sensor	Example	Security						Privacy				Usability						
				Error	*Replay Attacks*	*Adversarial Examples*	*Physical DoS*	*Sensor Hardware Attacks*	*Spoofing*	*Required Data*	*Overprivileged Data*	*Data Storage*	*Retention Time*	*Wide Availability*	*Initial Set-up / Removal*	*Registration*	*Retraining*	*Reusability*	*Device Dependency*	*Limitations*
User's identity	Voice	Microphone, inertial sensors	[37]	0.1%					!	A,Bm	👎	🏠	○	👎	👍	👍	👍	👎	👎	👎
		Microphone-only	[75]	5-6%						A, C, M	👎	🏠	●	👎	👍	👎	👍	👍	👎	👎
			[46]†	—	!	!	!	!	!	A	👎	☁	○	👍	👍	👍	👍	👍	👍	👎
	Breathing patterns	Microphone	[19]	0.4-2%	?	!				A	👎	🏠	●	👍	👍	👍	👎	👍	👍	👎
	Facial features	Camera	[102]†	Variable	!	!	!			V	👎	☁	●	👍	👍	👍	👍	👍	👍	👍
		Depth camera	[8]†	<0.001%		!	!			P'	👎	🏠	●	👍	👍	👍	👍	👍	👍	👎
		Infrared (IR) camera	[93]†	<0.001%			!			P'	👎	🏠	●	👍	👍	👍	👍	👍	👍	👍
		Camera, inertial, light sensors	[20]	4.7%			!			V, C, E	👎	☁	●	👍	👍	👍	👍	👎	👍	👍
	Eye features	Iris scanner	[119]†	—	!		!			P'	👎	🏠	●	👎	—	👍	👍	👎	👍	👎
	Fingerprint	Fingerprint sensor	[9]†	0.002%	?					F	👍	🏠	●	👎	👍	👍	👍	👎	👍	👎
		Microphone	[116]	2-16%			!	!		A	👎	🏠	●	👍	👍	👍	—	👍	👍	👎
	Body shape	Radar (RF) sensor	[68]	10-21%			!			B	👍	🏠	●	👎	👍	👎	👍	👍	👍	👎
	Bioimpedance	Bioimpedance sensor	[26]	2%						El	👍	🏠	●	👎	👍	👍	👍	👎	👎	👎
			[122]	11-21%						El	👍	🏠	●	👎	👍	👎	—	👎	👍	👎
	Cardiac motion	Radar sensor	[83]	1.39%			!			Bm	👍	🏠	●	👎	👍	👍	👍	👎	👍	👎
		Camera	[85]	1.4-4.5%			!	!		Bm	👎	🏠	●	👍	👍	👍	👍	👍	👍	👎
	Hand gestures	IMU sensors	[115]	10-36.2%			!	!		M	👍	🏠	●	👎	👍	👍	👍	👎	👍	👍

Security Implications



68.1% of sensing methods are vulnerable towards physical DoS attacks.

Redundant sensors of different types

Carefully constructed default policies

Naïve audio- and video-based sensing methods can be vulnerable to all attacks.

Defenses should consider both impersonation and invisibility.

Privacy Implications

79.8% of sensing methods do not require computationally heavy processing.

Federated learning or edge computing can also mitigate the privacy concerns.

Audio- and video-based sensing methods are invasive, but also indispensable.

Contexts like "age" cannot be detected otherwise.

Mitigations (e.g., blurring images) may weaken security.

Another Use Case

As a smart home designer…

Scenario: A child can only have access to smart oven when **an adult is around.**

Involved Contexts: *Age, People present in the same room as the user*

Priority: *Security*

Solution: Use a microphone with liveness detection for age estimation, and a RF sensor for people detection. Extra default policy is required.

On-going Efforts

The evaluation table is available on GitHub and accepts Issues (for changes) and Pull Requests (for new sensors).

https://github.com/UChicagoSUPERgroup/eurosp21

New threat model that considers local attackers

Decision framework for security, privacy, and usability

Trade-offs in deploying sensors for access control

SoK: Context Sensing for Access Control in the Adversarial Home IoT

Weijia He, Valerie Zhao, Olivia Morkved, Sabeeka Siddiqui, Earlence Fernandes, Josiah Hester, Blase Ur

THE UNIVERSITY OF CHICAGO

WISCONSIN
UNIVERSITY OF WISCONSIN–MADISON

Northwestern University