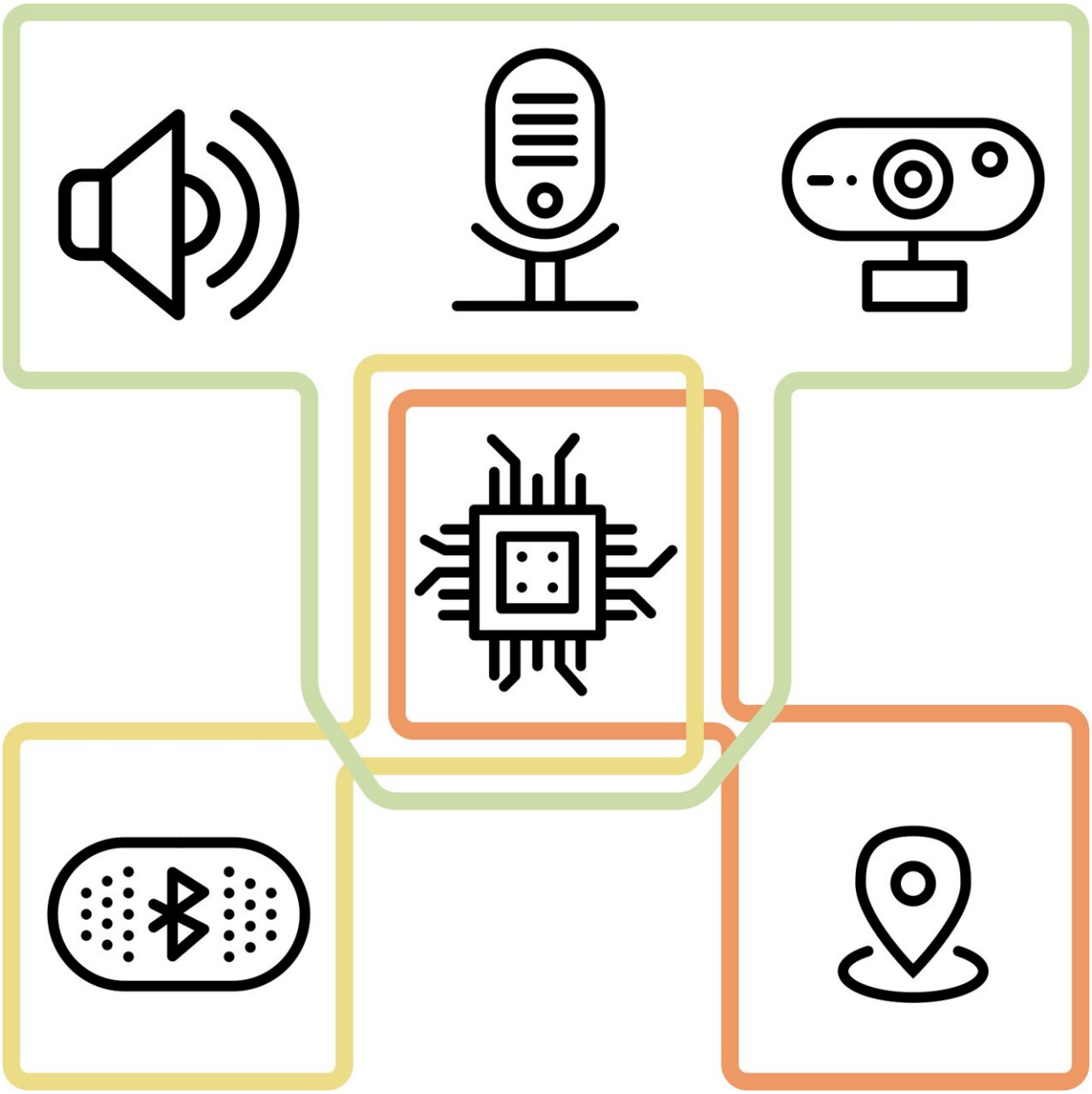
An architecture that gives users full control of their smartphones

December 2 2022, by Ingrid Fadelli



With TEEtime, the user can define isolated domains, which can run different software and have access to different peripherals. In this example, the user defined a domain which runs a contact tracing app with access to Bluetooth (yellow), a navigation app with access to the GPS module (orange), and a domain for running a legacy OS such as Android and associated apps with access to all other peripherals (green). Credit: Groschupp et al.

In recent years, many smartphone users have become concerned about the privacy of their data and the extent to which companies might have access to this data. As things stand today, the applications that users can run on their phone and what they can do with these applications is determined by a few big tech companies.

Researchers at ETH Zurich have recently set out on a quest to change this current trend, through the development of a new smartphone architecture called TEEtime. This architecture, introduced in a paper pre-published on *arXiv*, allows users to flexibly choose what resources on their smartphone they will dedicate to legacy operating systems, such as Android or iOS, and which they wish to keep for their own proprietary software and data.

"This work was inspired (in part) by our experiences in developing (Swiss) contact tracing applications, where we quickly noticed how limited we are as researchers/developers in accessing some basic services on 'our' phones," Srdjan Capkun, one of the researchers who carried out the study, told TechXplore.

"This experience taught us that even governments need to negotiate with prominent phone OS vendors (Apple/Google) to gain specific access, such as Bluetooth radios. This example caused us to look more broadly into restrictions we face today on 'our' smartphones, which have political

and economic implications for citizens, companies, and governments."

The lack of user control over resources on smartphones is typically justified by operating system developers and phone providers as a necessary means to offer security and privacy. Specifically, one might argue that opening smartphone systems would endanger users (i.e., increasing their vulnerability to attacks) and adversely affect their overall navigation experience.

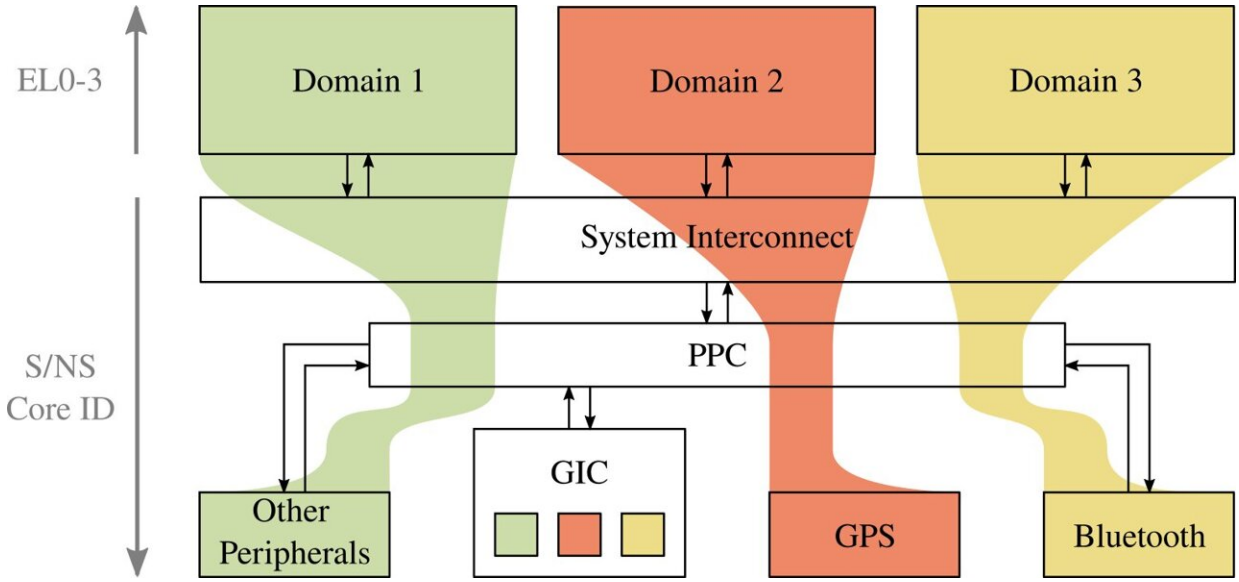
The key objective of the recent work by Groschupp et al. was to show that one could potentially grant users greater control over their phone while retaining existing operating systems, with their functionalities and security measures. To do this, the team developed TEEtime, a new smartphone design architecture that allows different 'domains' running simultaneously to coexist on a smartphone.

"With TEEtime, we provide concurrently executing 'domains'—that are protected from each other—using hardware features incorporated in current CPUs/platforms," Groschupp explained. "Users can run several domains on their phones, e.g., a full Android/iOS, with all the convenience and security that they provide, and in parallel a proprietary software running in another domain."

Essentially, TEEtime isolates different domains, allowing users to decide the extent to which each of these domains has access to resources on their phone. This means that users could, for instance, run a navigation application in their own isolated domain, giving GPS access only to this domain and thus preventing Android/iOS from accessing their GPS data. The same could also be done with other peripherals, such as Bluetooth or the phone's in-built microphone and camera.

"The introduction of domains has two main advantages in terms of giving users control over their devices," Groschupp explained. "Firstly, it

gives users full control of the privacy of their data, for instance allowing them to store their photos in a separate domain, where the user can make sure that no client-side scanning is performed. Note that in current phone ecosystems these features can be silently introduced without the user even noticing or having the possibility to opt-out."



High-level overview of domain isolation in TEEtime: Access to peripherals is enforced with a partition controller (PPC). The interrupt controller (GIC) is shared among domains, such that all domains can handle interrupts concerning their peripherals. Credit: Groschupp et al.

The second advantage of the TEEtime architecture is that it can prevent censorship or increase resistance to it. In other words, if their operating service providers blocks an application or prevents them from installing it, they can still run it in a separate domain.

So far, the researchers tested a prototype of their architecture on an

ARM emulator, a software tool often used to test operating systems and other smartphone software. These initial evaluations were promising, as they suggested that TEEtime works well and does not impact a system's security.

"We show that it is indeed possible to run software that is mutually distrusting on one phone, with hardware primitives that already exist," Groschupp said. "We hope this leads to a change in the public perception of the smartphone ecosystem. Usability, security, and user control are not mutually exclusive. An important design choice for us was to refrain from leveraging hypervisors, as we wanted to avoid complex high-privileged software on the phones, since this would require again trusting large commercial entities with its development and updates."

In the future, the architecture developed by this team of researchers could pave the way for the creation of other software solutions that give users greater control over their smartphone. In the meantime, Groschupp and her colleagues plan to develop TEEtime further, to overcome limitations that could potentially hinder its large-scale implementation.

"Our ambition is to develop a fully working phone prototype and through it inspire phone manufacturers to support this design," Groschupp added. "We are currently working on a number of remaining issues, including securing user interactions with our system and investigating changes to hardware that would make our solution simpler to integrate and even more efficient."

More information: Friederike Groschupp et al, It's TEEtime: Bringing User Sovereignty to Smartphones, *arXiv* (2022). DOI: 10.48550/arxiv.2211.05206