# Cyber Privacy

H. Jin, G. Liu, D. Hwang, S. Kumar, Y. Agarwal and J. I. Hong, "**Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes**," 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2022, pp. 303-320, doi: 10.1109/SP46214.2022.9833629.

This paper provides a unique Privacy-sensitive architecture to build applications for smart homes which use IOT devices to collect data. Such data is usually sent to cloud for analysis Data because of CPU and storage limitations in local devices. The paper walks through the current challenges in data collection by cloud-based software architectures. They are :

1. How can an app developer avoid collecting unnecessary data.
2. How can user verify what data is collected? Only way is reverse engineering these devices which collect data. No easy way to verify if data was minimized.
3. Even if developer use trusted cloud computing for encrypting data end-to-end, it is challenging for auditors to verify the same.

For example, drawback of Android apps is All or nothing access model for permissions. If an app needs SMS permission for one specific number, user has to give access to all numbers. The authors provide Solutions for above in this novel architecture called peekaboo.

1. Text-based Manifest to describe data collection behaviors including what are the conditions for data collection, where it is sent, granularity of data. Here even the user ad d conditions dynamically which will be processed using natural language and implemented on the go.
2. In order to enforce the guidelines declared in the manifest a Fixed set of operators is pipelined to pre-process raw data and minimize it before sending it out to the internet.

The benefits of this architecture as explained in this paper are:

1. Developers can collect sensitive data in fine-grained and flexible manner just by running the operators.
2. Auditors can inspect data collected by checking the manifest and any step in the pipeline to check actual data flow. Making data collection transparent, enforceable, centrally manageable.
3. User can customize privacy controls by adding conditions to the manifest before the data flows out.

Michalis Diamantaris, Serafeim Moustakas, Lichao Sun, Sotiris Ioannidis, and Jason Polakis. 2021. “**This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration**.” In Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21). Association for Computing Machinery, New York, NY, USA, 1065–1081. https://doi.org/10.1145/3460120.3485366

The paper discusses the potential threats to mobile sensors due to the absence of sufficient access control. Malicious apps and sites can use data captured from sensors, and attackers can use ads to deliver a wide range of attacks. The paper introduces a novel attack vector that misuses the advertising ecosystem for delivering sophisticated and stealthy attacks that leverage mobile sensors. These attacks do not depend on any special app permissions or specific user actions and affect all Android apps that contain in-app advertisements due to the improper access control of sensor data in WebView. The paper explains how motion sensor data can be used to infer users' sensitive touch input in two distinct attack scenarios, namely intra-app and inter-app data exfiltration. While the former targets the app displaying the ad, the latter affects every other Android app running on the device. The paper describes some serious flaws in Android's app isolation, life cycle management, and access control mechanisms that enable persistent data exfiltration even after the app showing the ad is moved to the background or terminated by the user. As in-app ads can "piggyback" on the permissions intended for the app's core functionality, they can also obtain information from protected sensors such as the camera, microphone and GPS. The ads in the wild are already accessing and leaking data obtained from motion sensors, highlighting the need for stricter access control policies and isolation mechanisms.

Toch, Eran & Bettini, Claudio & Shmueli, Erez & Radaelli, Laura & Lanzi, Andrea & Riboni, Daniele & Lepri, Bruno. (2018). “**The Privacy Implications of Cyber Security Systems: A Technological Survey**.” ACM Computing Surveys. 51. 1-27. 10.1145/3172869.

The increasing reliance on cyber-security systems by governments and corporations has led to the need for balancing security risks with privacy concerns. While these systems protect against cyber-attacks, they also create vulnerabilities for privacy violation by monitoring network traffic and accessing sensitive information. The challenge for policymakers and technology developers is to address these privacy risks while still maintaining effective cyber-security measures. The author here also mentions privacy concerns are among the reasons why some employees switch to personal devices for work-related activities and why some home-users avoid certain anti-virus applications. As mentioned in the paper, addressing privacy threats is crucial to ensure the acceptance and usage of cyber-security systems by organizations and individuals and ultimately reduce the number of threats for everybody. The paper discusses the increasing use of cyber-security systems to protect against network threats, but also highlights how such systems can impact individuals' privacy by monitoring network traffic and accessing personal information. The paper presents a taxonomy of privacy threats related to cyber-security technologies and demonstrates how this taxonomy can be applied to various technologies. The paper also emphasizes the importance of balancing security and privacy concerns and suggests future research directions for developing privacy-enhancing cyber-security mechanisms.

Barth, Susanne & De Jong, Menno & Junger, Marianne. (2022). “**Lost in privacy? Online privacy from a cybersecurity expert perspective.”** Telematics and Informatics. 68. 101782. 10.1016/j.tele.2022.101782.

Found this paper as an interesting read which says that despite concerns about personal data privacy, the number of app downloads continues to rise, and users often prioritize the immediate benefits of an app over potential privacy risks. This discrepancy between privacy concerns and actual behavior is known as the privacy paradox. Previous research has shown that both experts and lay users exhibit similar privacy-related behaviors and concerns, despite differences in knowledge and understanding of privacy risks. However, more in-depth research is needed to understand how privacy and security experts use and reflect on their knowledge, deal with uncertainties, and make decisions regarding online privacy on their own smartphones. Therefore, a qualitative interview study was conducted to investigate how privacy and cybersecurity experts approach personal online privacy and evaluate and use mobile apps. The paper xaddressed two research questions: (1) How do privacy and security experts value their personal online privacy? and (2) How do privacy and security experts evaluate and use mobile apps?

H. Takabi, J. B. D. Joshi and G. -J. Ahn, **"Security and Privacy Challenges in Cloud Computing Environments,"** in IEEE Security & Privacy, vol. 8, no. 6, pp. 24-31, Nov.-Dec. 2010, doi: 10.1109/MSP.2010.186.
Cloud computing is an evolving paradigm with tremendous momentum, but its unique aspects exacerbate security and privacy challenges. This article explores the roadblocks and solutions to providing a trustworthy cloud computing environment. The authors say it can significantly reduce costs and enhance collaboration, agility, and scale. However, the lack of appropriate security and privacy solutions designed for clouds is hindering its adoption. The paper talks about unique issues of cloud computing that exacerbate security and privacy challenges, such as shared infrastructure, multi-tenancy, and dynamic provisioning. The paper also discusses various approaches to address these challenges, including secure virtualization, data encryption, access control, and auditing. The authors suggest that a trustworthy cloud computing environment requires a holistic approach that considers technical, organizational, and legal aspects. The paper concludes with calls for future research to explore new security and privacy solutions for emerging cloud computing models, such as edge computing and fog computing.

## Zoom Discussion Details

One of the group members talked about following 2 papers:

1. ai Yang, Xiaodong Lin, Limin Sun,CShield: Enabling code privacy for Cyber–Physical systems,Future Generation Computer Systems,Volume 125, 2021, Pages 564-574, ISSN 0167-739X
   The paper proposes an automated, simple, and transparent CPS code obfuscation technique, CShield, to protect against adversaries' analysis of sensitive data. Code encryption issues in CPS due to use of machine learning algorithms. Framework to safeguard code privacy using TEE.

2. Rafał Leszczyna, Cybersecurity and privacy in standards for smart grids – A comprehensive survey,Computer Standards & Interfaces, Volume 56,2018,Pages 62-73, ISSN 0920-5489,
   Smart grid being critical infrastructure, paper compiles all the smart grid standards related to cybersecurity and provide information on their contents.

   **Recording Link:**
   https://purdue-edu.zoom.us/rec/share/BDyeRsNhfxtE2aLvsrfz9uvfHwRZgdmWl9_sbvE8nMWf-Rdt8RQTAjGYU4Km1UfF.4AkO_Gl_9vjkMmev
   Passcode: $t5MBj?+