ETSI
The Standards People

Security Conference

Implementing Design Practices with the Goal to Prevent Consumer IoT Enabled Coercive Control

Presented by: Alex Cadzow

C3L

18/10/2023

Introduction

- An Overview of ETSI EG 203 936 - Implementing Design Practices to Mitigate Consumer IoT-Enabled Coercive Control.
- ETSI Guide that recommends initial design practices to minimise the potential of coercive control by consumer Internet of Things (IoT) devices.
- The guide provides emerging design practices through examples and explanatory text for organisations involved in the development and manufacturing of Consumer IoT devices and associated services.

Understanding Consumer IoT Enabled Coercive Control

- Coercive control is entrapment in personal life, and it pertains to the set of control skills also used in other situations of captivity such as hostage situations and human trafficking to override autonomy and the sense of self and entrap a person.

- The misuse of novel telecommunications applications such as smartphones, tablets, social media, wearables, smart speakers, telecare systems, internet connected cars, internet connected home appliances, smart locks, smart thermostats and home security systems in the context of coercive control within intimate relationships often known as Consumer IoT Enabled abuses.

- These behaviours include but are not limited to stalking and omnipresence, surveillance (wiretapping, bugging, videotaping, geolocation tracking, data mining, social media mapping, and the monitoring of data and traffic on the internet), intimidation, impersonation, humiliation, threats, consistent harassment/unwanted contact, sexting, and image-based sexual abuse.

Types of Consumer IoT enabled Abuse

- Toxic content covers a wide range of attacks involving media that attackers send to a target or audience—e.g., bullying, trolling, threats of violence, and sexual harassment.
- Content leakage involves any scenario where an attacker leaks (or threatens to leak) sensitive, private information to a wider audience, typically with the intent to embarrass, threaten, intimidate, or punish the target.
- Overloading includes any scenario wherein an attacker forces a target to triage myriad notifications or comments via amplification, or otherwise makes it technically infeasible for the target to participate online due to jamming a channel.
- False reporting broadly captures scenarios where an attacker deceives a reporting system or emergency service—originally intended to protect people—to falsely accuse a target of abusive behaviour.
- Impersonation occurs when an attacker relies on deception of an audience to assume the online persona of a target to create content that will damage the target's reputation or inflict emotional harm.
- Surveillance involves an attacker leveraging privileged access to a target's devices or accounts to monitor the target's activities, location, or communication.
- Lockout and control involves scenarios where an attacker leverages privileged access to a target's account or device—including computers, or Consumer IoT devices—to gaslight the target or interfere with how they engage with the world.

Consumer IoT abuse tactics and harms

Coercion tactic	Purpose	Tech Abuse Example
Isolation	Isolation is a tactic used to deprive the target of social support.	Monitoring the target's online activity. This allows the attacker to control the target's online life and isolates the target by preventing them from communicating with others.
Monopolisation of perception	Attackers tend to use monopolization perception techniques to isolate the target from their friends and family. This makes it difficult for the target to recognise that abuse is taking place, to get a second opinion or to have someone to talk to who is not under the attacker's control.	Using Consumer IoT devices, the attacker may control what information the target has access to on their phone. This can include limiting their access to news, social media, or other forms of communication. This can make it difficult for the target to get help or to learn about their rights.
Monitoring	Monitoring is a tactic used by an attacker to track a target's activities and to ensure that they are not doing anything that the attacker disapproves of.	Using surveillance cameras within the house to monitor what the attacker does daily and track who comes and goes from the household.
Threats	Threats are used by attackers to make them feel like they have some level of control over the target.	Attackers can also threaten to remove or limit a target's access to Consumer IoT devices that they may depend on within their ecosystem for example, accessing the controls on the smart thermostats, smart door locks, smart TVs etc.
Deny Attack Reverse Victim and Offender (DARVO)	DARVO is used by attackers to deny any wrongdoing or abuse, and instead attack the target for attempting to hold the attacker accountable for their actions. The attacker then claims that they are the victim and that the person who was abused is the perpetrator.	Attackers may delete any evidence of abuse that may be stored on Consumer-IoT devices. In the absence of hard evidence, the target is forced to rely on their own memory which can be manipulated by the attacker.
Induced debility and exhaustion	Induced debility and exhaustion weakens the target's mental and physical ability to resist abuse as they feel drained.	The attacker use a smart speaker or smart music device to blare music at random times during the night which would prevent the target from sleeping and would also make them feel very uneasy, anticipating the next sound.

Coercive Control-Resistant Design

- Coercive Control-Resistant Design can be defined as safeguarding or designing products with anti-abuse protections by default to minimise attackers' ability to use these tools to harm targets whilst not limiting the access to the device functionality by the intended user.

  These include but are not limited to:

  1. Build consensus and awareness on the nature of the problem.
  2. Identify dilemmas and build consensus on acceptable solutions.
  3. Harm considerations "built in, not bolted on".
  4. Minimise risks of harms arising.
  5. Disrupt harms that have arisen.
  6. Diverse design team.
  7. Privacy and Choice.
  8. Combat Gaslighting.
  9. Security and Data.

Omnipresence attacks & harms

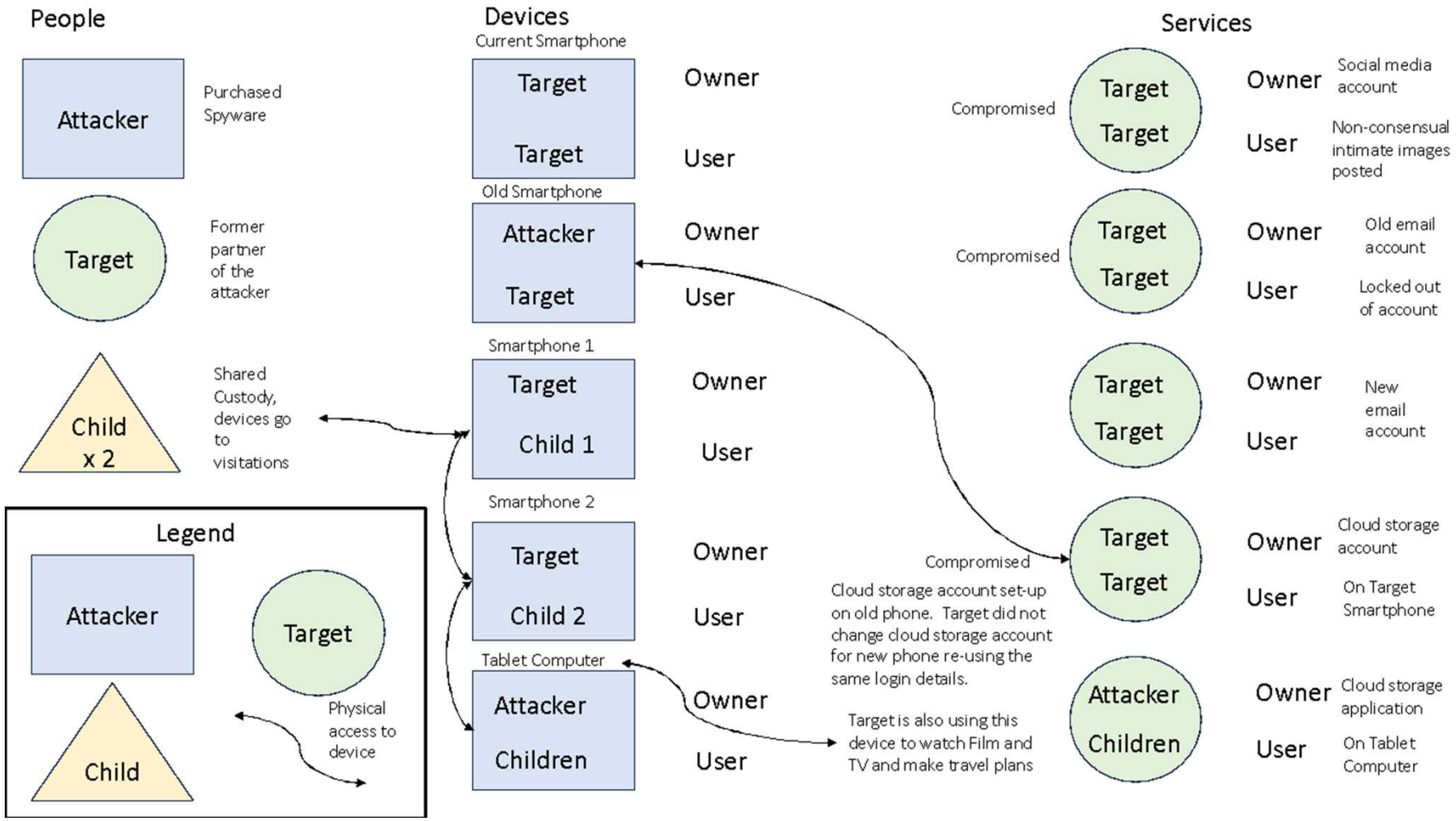
- Without the implementation of preventative strategies, the misuse of modern telecommunications applications could lead to a significant intensification in the level of oppression that attackers of coercive control are able to enact due to a concept termed “abuser omnipresence” whereby the attacker engages in micro-surveillance and micro-regulation of the target.

- The surveillance capabilities and opportunities for micro-regulation conferred by modern telecommunications applications e.g., a notification on a joint banking app, tracking information on an internet connected car, a tracking device on a set of keys, a smart doorbell that alerts the attacker when the target is leaving the property, for example, enables an attacker to establish a sense of omnipotent omnipresence in the targets’ life. Those attackers who seek to misuse telecommunications applications in this way can be considered dangerous to the psychological, emotional, financial and physical well-being of the targets.

- By understanding how omnipresence is established and how it evolves, it may be possible to mitigate this troubling aspect of consumer IoT facilitated domestic abuse.

Types of Omnipresent Behaviour	Examples of the Omnipresent Behaviour
Establishing omnipresence	Attackers are account holders for family plans set passwords. Device mirrored to keep track of targets. Installs CCTV cameras around the home. Turns on location tracker on targets phone to make sure they are OK getting the bus.
Overt omnipresence	Attacker checks target phone in front of them. Installs CCTV cameras and then texts to ask, “What are you watching on TV?” Spoofs phone number to bypass blocking.
Covert omnipresence	Happens in tandem with overt omnipresence, continuing and intensifying after separation. Dual-use tracking capability misused. Plants GPS on vehicle to keep track of target often after separation when they no longer have smartphone access.
Retributive omnipresence	Attackers “change the project” from attempting to keep their target in the relationship to destroying them for leaving it. Delete important emails and important official documentation. Revenge porn sites to upload images and survivor’s contact details. Doxing.

Visualisation of the proliferation of personal data



A hypothetical simplified example of a technogram illustrating the digital footprint and entanglements of the target and their children with an attacker.

Implementing Coercive Control-Resistant Design

- **Online Harms Policy**
  - There is an expectation from user that companies will have measures in place to ensure duty of care to keep their users safe from harm.
- **Security and Safety of Consumer IoT design**
  - No universal default passwords in consumer smart products.
  - Device producers should establish and maintain a vulnerability disclosure policy. This means there would be a clear route for users to report security vulnerabilities when they are discovered, and a process for remediation.
  - The device producers should explicitly state how long a product will receive software security updates for.
  - Threat modelling paired with usability analysis for the design and development of safer systems.
  - Incorporating privacy and security by default, during the design process.
  - Companies should get users' permission before collecting and sharing location data. So, this could mean disabled by default. Also, they should inform users how they can stop the collection of such information, and its deletion if requested which is under GPDR right to be forgotten.

- **Technology Design**
  - Diversity. Ensuring a diverse design team to broaden the understanding of user habits.
  - Privacy and choice. Allowing users to make informed choices about their privacy settings.
  - User Awareness. Making it clear when settings have been changed and how this affects the functionality of the devices.
  - Security and data. Ensuring that products only collect and share necessary data, limiting the risk that data are used maliciously.
  - User Experience. Giving users greater confidence to use technology by making it simpler to understand, limiting the risk of attackers exploiting a target's lack of technical ability.
- **Education and Resources**
  - Many organisations have produced guidance on the safe use of technologies and how individuals can implement better privacy protections. Some organisations have also produced specific guidance on technology abuse for the targets (victims) and professionals working with targets (victims). These include guidance on how to document technology abuse, information about spyware and surveillance, and guidance on privacy and security features of social media platforms.
- **Role Technology can Play in Supporting Targets**
  - Technology can offer a lifeline to targets, enabling them to access support services and information. It can also provide a way for them to record evidence of their abuse. There are different ways in which technology may help targets including:
  - Finding information.
  - Accessing support services and networks.
  - Connecting with other targets.
  - Gathering evidence.
  - Protecting and alerting targets.

Trauma Informed Design

Trauma Informed Design can be defined as recognising understanding how people's trauma affects their experiences. The informed design is seeking to avoid exacerbating this trauma in the process of discovery and design and creating solutions which could make a positive impact to their recovery. These are:

1. Enable users to secure privacy from an intimate attacker in threatening situations.
2. Ease of use of personal security functions.
3. Common design of personal security functions across devices and applications.
4. Information transparency, including who can see what information about you, when and where easily accessible and standardised.
5. Consideration of degree of danger, likelihood of escalation of abuse, impact of target blaming, deleterious impacts on ability to self-advocate, emotions, cognition, and execution of complex tasks due to abuse.
6. Useful onward help signposted appropriately.

Design Principles

Trauma-informed design includes the personal interaction between the abused person and the company contacts responsible for customer service with the target, and any helping interventions such as a chat bot trained to deal with an abusive situation to provide information to a person.

Relational Safety Principles

Relational safety needs to be established with the target that are mindful of the complex deleterious effects of abuse. In general, relational safety involves establishing trust, transparency, safety, and predictability and could look like:

- Non-judgmental validation of a person's experience of abuse.
- Non-judgemental validation of the target's choices in how to deal with the abuse.
- Clear boundaries with clearly defined roles for the helper. This includes communicating to the person experiencing coercive control that they have the right to set limits or end the interaction.
- To provide this level of care, those directly involved with targets of abuse at a minimum need to be emotionally mature and able to contain the potentially strong emotional affective states of the abused person without emotional reactivity, criticism, giving advice or becoming defensive to avoid re-traumatisation. Training in the effects of trauma or bringing in trauma-informed professionals is needed.

Policy Guidance

In relating to targets, the companies need to avoid:

- Taking the power-over stance in the helper-helped relationship,
- Shaming, Victim blaming,
- Denial and minimisation of the abuse,

Overall, companies should seek to support the target in reaching an independent decision in their own best interests rather than being told what to do and do their best to avoid re-traumatisation by seeking expert input on how best to provide this support.

Customer Support Guidance

The training of frontline agents / customer support staff to be better prepared for tech enabled attack cases is critical for supporting the targeted users. Equipping customer support agents with a basic understanding of Consumer IoT / Technology enabled abuse and the caution needed for a proper response is also vital to prevent inadvertent harm, such as escalating abuse by removing spyware without further precautions or making misleading promises.

- Introduce Consumer IoT-Enabled Coercive Control to customer support agents. Discuss the prevalence of it, including how the technology is misused to facilitate abuse and non-technical aspects (e.g., the targets and attacker's social entanglements and the need for holistic safety planning). Explain why agents should be committed to learning how to support the targets.

- Identify mental health resources for customer support agents. Provide resources (e.g., therapeutic sessions and peer support groups) for agents who might be experiencing coercive control or suffering secondary trauma from handling such cases.

The training should make customer support agents aware of unique risks and nuances in consumer IoT enabled coercive control, help them pick up cues that indicate customers experiencing coercive control, and teach them how to share resources safely and respectfully.

Thank you for your attention

Publicly Available Draft Version

Follow us on:

Any further questions?

Contact me:

alex@Cadzow.com.com