Parental control solutions are widely used to help digital parenting and protect children. Can introduce serious security and privacy risks to children and parents, due to their elevated privileges and having access to a significant amount of privacy-sensitive data.

We used our experimental framework for systematically evaluating security and privacy issues in parental control software and hardware solutions. Our analysis uncovers pervasive security and privacy issues that can lead to leakage of private information, and/or allow an adversary to fully control the parental control solution, and thereby may directly aid cyberbullying and cyber predators.

**Potential Security and Privacy Issues**

- **Vulnerable client product**: Allowing sensitive information disclosure or even full product compromise.
- **Vulnerable backend**: The use of remotely exploitable outdated server software, and misconfigured or unauthenticated backend API endpoints.
- **Improper access control**: Failure to properly check whether the requester owns the account before accepting queries at the server-end.
- **Insecure authentication secrets**: Plaintext storage or transmission of authentication secrets.
- **SSLStrip attack**: The parent’s online interface is vulnerable to SSLStrip attacks.
- **Online password brute-force**: No defense against unlimited login attempts on the online parental login interface.
- **Uninformed suspicious activities**: No notifications to parents about indicators of possible compromise.
- **Insecure PII transmission**: PII from the client-end is sent without encryption, allowing an adversary to eavesdrop for PII.
- **PII exposure to third-parties**: Direct PII collection and sharing with third-parties.

**Contributions**

- Developed an experimental framework for analyzing security and privacy issues in parental control solutions.
- Conducted the first comprehensive study of parental control solutions on multiple platforms.
- Identified 172 vulnerabilities across 54 different solutions.

**Analyzed Solutions**

Analyzed 54 solutions from popular online marketplaces including:

- Android apps (28 solutions, 46 apps)
- Network devices (8)
- Windows apps (8)
- Chrome extensions (10)

**Methodology**

1. Triggering parental control mechanisms
   - Mimicking regular users’ operations for each solution.
2. Hybrid analysis
   - Combined dynamic (primarily traffic and usage) and static (primarily code review/reverse engineering) analysis.
3. Analyze parental web interface
   - Assess the password-related issues and test the SSLStrip attack against the login page.

**Example Vulnerabilities**

1. **Insecure firmware update - Blocksi (network device)**
   1) Request a firmware update
   2) Firmware binary + Hash via HTTP
   3) Intercept and replace firmware with malicious code
   4) Modified binary + Hash

2. **Insecure authentication - SecureTeen (Android)**
   Authentication requires: only parent’s email
   1) https://cp.secureteen.com/...[email]
   2) Authentication cookie

**Contributions**

- Developed an experimental framework for analyzing security and privacy issues in parental control solutions.
- Conducted the first comprehensive study of parental control solutions on multiple platforms.
- Identified 172 vulnerabilities across 54 different solutions.