Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions

Suzan Ali, Mounir Elgharabawy, Quentin Duchaussoy, Mohammad Mannan, Amr Youssef

ACSAC 2020 - Virtual Conference, Dec 9, 2020
Childhood in the Digital Age

- 1/3 of the internet users are under 18 years old
- Emergence of the “bedroom culture”
- A new parenting role

Parental Control Solutions

May help digital parenting and protect children...

...but also introduce serious security and privacy risks
Recent Incidents

TeenSafe (2019)
- Over 1 millions users
- Exposed emails and Apple ID credentials

Family Orbit (2018)
- 280 GB of data
- Screenshots, Child’s photo and video
Related Work

• Smart Sheriff Application (Anderson et al., 2015)

• COPPA compliance analysis of Android apps (Reyes et al., 2018)

• Privacy analysis of mobile parental control apps (Feal et al., 2020)

But other platforms remain largely unexplored…
Solution Platforms

Desktop Applications

Mobile Apps

Network Routers

Browser Extensions
Security Evaluation Methodology
Methodology

We perform three types of analysis:

1. Dynamic analysis
2. Static analysis
3. Online interface analysis
Dynamic Analysis

- Is traffic decryptable?
  - Yes: Analyze URLs and APIs
  - No: Check for communication flaws

- Extract domains contacted

- Insecure PII transmission
- Insecure authentication secret
- Improper access control
- Vulnerable backend
- 3rd parties trackers
Static Analysis

1. Is code accessible?
   - No: Extract/download source code
   - Yes: Perform code analysis

2. Vulnerable client product
Online Interface Analysis

- Has an online interface?
  - Yes: Assess password related issues
  - No: End

Assess password related issues:
- Weak password policy
- Online password brute-force
- Uninformed suspicious activities
- Lack of HSTS enforcement
Challenges

Traffic interception
- Network-based solutions
- Embedded certificate store
- VPN and certificate pinning

Traffic attribution
- Binding processes and network packets
Results and Sample Findings
Overall Results

We found a total of **135** vulnerabilities across 39 solutions.

- 78 vulnerabilities in 13 Android solutions
- 10 vulnerabilities in 10 Chrome extensions
- 30 vulnerabilities in 8 network devices
- 17 vulnerabilities in 8 Windows applications
Insecure Firmware Update - Blocksi (network device)

1) Request a firmware update
2) Firmware bin over HTTP
3) Intercept and replace firmware with malicious code
4) Modified bin

Blocksi device

Attacker

Blocksi backend

2) Unkeyed HASH over HTTP

Sample Findings
Insecure Authentication - Blocksi (network device)

**Blocksi Backend API:**
- Blocksi API authentication relies on 2 parameters: parent’s email and device serial number (SN)
- Can recover SN using parent’s email

![Diagram](sample_diagram.png)
Insecure Authentication - SecureTeen (Android)

Authentication using parent’s email

GET request:
   ?productName=secureteen&j_username={parent@email.com}

(2) Authentication Cookie
Full URL Logging - MetaCert Adult Content Blocker (Chrome Extension)

URL query strings might contain:

- Authentication tokens
- User IDs on different websites
- Private information (such as name, email, etc...)
Summary of 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 135 vulnerabilities across 39 different solutions
Thank you!

This work was funded by

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Mounir Elgharabawy
m_elghar@encs.concordia.ca