Parent-Centric Privacy Framework for a Safe Cyber Environment for Children

Dr. Sivadon Chaisiri (Boom) and Dr. Ryan Ko

Cyber Security Lab, Dept of Computer Science, The University of Waikato

Privacy Research Symposium, December 15th 2016
CROW – 1st Uni Cyber Security Lab in NZ

• First Cyber Security Lab in NZ, building on traditions of NZ Internet, Data Mining (Weka), networking group
• 20+ research students (Honours, PGDip, Master of Cyber Security, PhD)
• 30+ Alumni (now at Gallagher, Deloitte, INTERPOL, Cloud Security Alliance, LayerX, etc)
• 14 staff (6 academics, 8 staff)
• Funded by MBIE Endeavour Fund (STRATUS), Fulbright Commission, InternetNZ, Education NZ, and Office of the Privacy Commissioner

• Our Goal: To return control of data to users
Who we work with:
• NZ Cyber Security Challenge

Creators of the New Zealand Cyber Security Challenge (now 3rd year; 267 participants)
Our Privacy Good Research Fund
Supported Project

Parent-Centric Privacy Framework for a Safe Cyber Environment for Children

[Image of the SCKid logo]
Our Sponsors
Our Project Goal

• Assist parents in preventing cyber threats and dangers of privacy illiteracy
• Help children preserve their Internet privacy through parent-assisted tools
• Provide parents with best practice tools/knowledge to maintain a safe cyber environment
• Promote initiatives & campaigns related to security and privacy awareness
SCKid – An Overview

• A parent-centric framework designed for parents (incl. guardians and teachers) to preserve and raise awareness of their child’s privacy

• Combination of technological tools, knowledge base, and administrative policies to improve a safe cyber environment
Our Target Groups

Parents

Teachers

Children
What children use the Internet for

![Bar chart showing the activities children engage in online.]

- Online gaming: 53%
- Education / learning: 38%
- Using social media sites e.g. Facebook, Twitter etc: 37%
- Listening to music / radio: 34%
- Watching movies / videos online: 32%
- Downloading pictures/music, films, videos etc.: 32%
- E-mail: 28%
- Instant messaging / video calling (Skype, Google..): 22%
- Uploading / sharing pictures / music, films, videos etc.: 22%
- Downloading software / applications: 21%
- Reading news, articles, books, etc.: 19%
- Online shopping: 11%
- Online data storage (e.g. Dropbox, iCloud etc): 7%
- Visiting adult websites: 3%
- Any Of The Above: 83%

Reference: KASPERSKY LAB STUDY: CHILDREN ONLINE version 1.0, March 2015
Inappropriate contents

<table>
<thead>
<tr>
<th>Content</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chat</td>
<td>67.29%</td>
</tr>
<tr>
<td>Adult Content</td>
<td>59.56%</td>
</tr>
<tr>
<td>Gambling</td>
<td>26.66%</td>
</tr>
<tr>
<td>Weapons</td>
<td>20.29%</td>
</tr>
<tr>
<td>Profanity</td>
<td>19.93%</td>
</tr>
<tr>
<td>Violence</td>
<td>19.52%</td>
</tr>
<tr>
<td>Alcohol, Tobacco, Drugs</td>
<td>10.63%</td>
</tr>
<tr>
<td>Anonymous proxy</td>
<td>8.16%</td>
</tr>
</tbody>
</table>

Reference: KASPERSKY LAB STUDY: CHILDREN ONLINE version 1.0, March 2015
Internet Threats to Children

- Privacy violations
- Children’s posts affecting their lives
- Online scams
- Inappropriate contents
- Cyber bullying
- Pedophiles (cyberpredators, cyberstalkers)
- Malicious software (aka malware)
And many more…
Online Scams

New Zealanders lose $12m to scams

CHLOE WINTER
Last updated 12:01, January 1 2016

Vulnerable Kiwis falling victim to scams seems to be endless, with more than 8000 calls to ScamBusters over the past year.

As a result, people have lost in excess of $12 million to scammers between January and November.

Here are some of the worst – and most unusual scams – this year:

1. You've been caught watching porn*: Android users scammed with fake apps 'fixes' for viewing porn

A message claiming to be from the police cyber crime unit and the CCA8 told Android users they had to pay a $200 fine for accessing pornography or illegally shared movies.

References: http://www.stuff.co.nz/business/money/75536670/New-Zealanders-lose-12m-to-scams
Privacy Violations

- Data monitored/collected by Internet-connected services/apps
- Online scams (incl. phishing)
- Parental-control software
- Malware (e.g. spyware, adware)
- Children’s privacy illiteracy
Cyber Bullying

- Nearly 43% of kids have been cyber bullied
- 25% of them have experienced cyber bullying more than once
- 10% of cyber bullying victims will inform a parent of their abuse
- Cyber bullying victims are 2-9 times more likely to consider committing suicide

Family of 12-year-old who died suddenly warn of the dangers of online bullying

Reference:
Relate work – Parental Control

• Only 22% of parents use parental control solutions (*KASPERSKY LAB, 2015*)
• Most parental control tools strictly use hard-control which can violate children’s privacy
• Yet another open question: How can we balance privacy and safety/security?
Example – KidLogger, Parental Control App for Android, Windows, Mac

What KidLogger can do

• Web history monitor
• Time tracking
• Record keystrokes (i.e. keylogger)
• Remote screenshots
• Record used files/folders
• Track used apps
• Voice monitoring
• Monitor messengers (e.g. Facebook, WhatsApp, etc)
• Record call voice (mobile version)
• Remotely view all photos created with camera (mobile ver.)

And many more…
Balance between security & privacy for kids

Security

Privacy

Freedom of expression
Related Acts

• **Children’s Online Privacy Protection Act 1998 (US)**
  – Protect privacy of children under 13
  – Place parents in control over children’s information collected by operators

• **Privacy Act 1993 (NZ)**
  – Define 12 privacy principles

• **Harmful Digital Communications Act 2015 (NZ)**
  – Help victims affected by harmful digital communications (e.g. cyberbully)
  – Penalise perpetrators causing harmful digital communications
Requirements of the SCKid Framework

- Control
- Audit
- Remediation
- Evidence Collection
- Knowledge
Implemented SCKid Prototype

**Mobile Device Management**
Empower parents & children to secure websites and mobile applications

**Web-based Privacy Management**
Enable parents to guard children's mobile and social network usage

**Knowledge-base**
Educate children & parents about privacy preservation and encourage communication
SCKid Prototype – Mobile App

Android app (compatible with Android 4.4+)

• Web blocking (incl. requestable access)
• App blocking
• Panic button
• Context-aware security (only Proof-of-Concept)
SCKid Prototype – Web App

Web app (based on Laravel, a PHP MVC framework, and Wordpress)

- Social network logging and feedback (supporting Facebook & Twitter)
- Mobile device logging (SMS, call, GPS)
- Web access control (based on OpenDNS)
- Mobile app control (blocking/unblocking apps)
- Knowledge-base (articles about online privacy, security, and safety)
Screenshots of SCKid Prototype
Website: sckid.org
PARENTAL CONTROLS READY IN YOUR COMPUTER

INTRODUCTION TO PARENTAL CONTROLS

Parental controls are special features used on televisions, computers, and mobile devices (e.g., cellphones and tablets) to control children's access to harmful and offensive material. They can also be used to restrict children's access to a number of digital applications or media based on the time spent on the devices or a specific time. Parental controls on mobile phones can also be used to track the location of the children at any given time.

WHY USE PARENTAL CONTROLS

The use of parental controls on devices is critical to ensure children's experiences on the Internet are safe, enjoyable, and a positive learning environment. Parents can use parental controls for a number of different reasons, e.g., protecting children from harmful material on the Internet (e.g., using a browser to access pornographic websites), enforcing a time to stop using mobile applications such as Facebook or Instagram, ensuring children can only play games and use applications that are child-friendly, tracking the child's location if they are lost on the way home, seeing how much time the children spend on Facebook and other social media sites, among others.

WHAT PARENTAL CONTROL OPTIONS ARE AVAILABLE?

Parental controls can be grouped into 4 different types, namely websites, enforcing a time to stop using mobile applications such as Facebook or Instagram, ensuring children can only play games and use applications that are child-friendly, tracking the child's location if they are lost on the way home, seeing how much time the children spend on Facebook and other social media sites, among others.
<table>
<thead>
<tr>
<th>Contact</th>
<th>Phone Number</th>
<th>Start Time</th>
<th>End Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Isayas</td>
<td>451-820-6891</td>
<td>2016-12-07 15:02:40</td>
<td>2016-12-07 19:21:43</td>
</tr>
<tr>
<td>Lisandro</td>
<td>+1-517-969-7296</td>
<td>2016-12-02 13:23:50</td>
<td>2016-12-04 18:42:41</td>
</tr>
<tr>
<td>Sivadon Chaisiri</td>
<td>02102405106</td>
<td>2016-12-12 19:22:54</td>
<td>2016-12-12 19:22:58</td>
</tr>
<tr>
<td>Sivadon Chaisiri</td>
<td>02102405106</td>
<td>2016-12-12 19:22:54</td>
<td>2016-12-12 19:22:58</td>
</tr>
<tr>
<td>Sivadon Chaisiri</td>
<td>02102405106</td>
<td>2016-12-12 19:22:54</td>
<td>2016-12-12 19:22:58</td>
</tr>
<tr>
<td>Sivadon Chaisiri</td>
<td>02102405106</td>
<td>2016-12-12 19:22:54</td>
<td>2016-12-12 19:22:58</td>
</tr>
</tbody>
</table>

Showing 1 to 7 of 7 entries
### SMS Logging

**SMS History**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Contact</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-12-13</td>
<td>36:02:20</td>
<td>+642102405106</td>
<td>Hans... How are you?</td>
</tr>
<tr>
<td>2016-12-13</td>
<td>36:00:31</td>
<td>7461</td>
<td>Welcome to Spark. For internet access through our network check your device APN settings are set to internet. Go to <a href="http://www.spark.co.nz/apn">www.spark.co.nz/apn</a> on a PC for help</td>
</tr>
<tr>
<td>2016-12-12</td>
<td>20:22:04</td>
<td>Sivadon Chaisiri</td>
<td>+642102405106 Help me please</td>
</tr>
<tr>
<td>2016-12-12</td>
<td>20:22:04</td>
<td>Sivadon Chaisiri</td>
<td>+642102405106 Help me please</td>
</tr>
<tr>
<td>2016-12-12</td>
<td>20:22:04</td>
<td>Sivadon Chaisiri</td>
<td>+642102405106 Help me please</td>
</tr>
<tr>
<td>2016-12-12</td>
<td>20:22:04</td>
<td>Sivadon Chaisiri</td>
<td>+642102405106 Help me please</td>
</tr>
<tr>
<td>2016-12-12</td>
<td>20:22:04</td>
<td>Sivadon Chaisiri</td>
<td>+642102405106 Help me please</td>
</tr>
<tr>
<td>2016-12-12</td>
<td>20:22:04</td>
<td>Sivadon Chaisiri</td>
<td>+642102405106 Help me please</td>
</tr>
<tr>
<td>Status</td>
<td>Picture</td>
<td>Comments</td>
<td>Posted Time</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------</td>
<td>-----------</td>
<td>---------------</td>
</tr>
<tr>
<td>Don't know what to eat today... Any suggestion?</td>
<td>No picture</td>
<td>No comments</td>
<td>2016-12-13 01:46:42</td>
</tr>
<tr>
<td>A photo</td>
<td></td>
<td>No comments</td>
<td>2016-12-13 01:25:48</td>
</tr>
<tr>
<td>My phone number is 555-1234</td>
<td>No picture</td>
<td>No comments</td>
<td>2016-12-13 01:21:27</td>
</tr>
<tr>
<td>My address is 123 fake street, Hamilton</td>
<td>No picture</td>
<td>No comments</td>
<td>2016-12-13 01:21:18</td>
</tr>
<tr>
<td>I'm going to a party</td>
<td>No picture</td>
<td>No comments</td>
<td>2016-12-13 01:20:57</td>
</tr>
<tr>
<td>Yay my new FB account</td>
<td>No picture</td>
<td>No comments</td>
<td>2016-12-13 01:20:49</td>
</tr>
</tbody>
</table>
# Mobile Applications

Change App settings below: **Hans**  |  **Apps**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Status (Blocked/Allowed)</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="android.png" alt="Android" /></td>
<td>com.android.cts.priv.ctsshim</td>
<td>Blocked</td>
</tr>
<tr>
<td><img src="youtube.png" alt="YouTube" /></td>
<td>YouTube</td>
<td>Blocked</td>
</tr>
<tr>
<td><img src="android_services_library.png" alt="Android Services Library" /></td>
<td>Android Services Library</td>
<td>Allowed</td>
</tr>
<tr>
<td><img src="phone_messaging.png" alt="Phone and Messaging Storage" /></td>
<td>Phone and Messaging Storage</td>
<td>Blocked</td>
</tr>
<tr>
<td><img src="commio.png" alt="CommIO" /></td>
<td>CommIO</td>
<td>Allowed</td>
</tr>
<tr>
<td><img src="google.png" alt="Google App" /></td>
<td>Google App</td>
<td>Blocked</td>
</tr>
</tbody>
</table>
SCKid Launcher

Device Registration

Step 1: Register Device
Verify Code

Step 2: Upload Application List

Step 3: Registration Complete
Current Device ID:
d66abdf0-5768-4129-80e4-53501015d954

Application Phone has been Banned.
Please enter your PIN code to Override.

Unlock PIN Code
REQUEST UNBLOCK CANCEL UNBLOCK

Google Drive Play Play Store
Demo Clip : SCKid Prototype
You've gone incognito

Pages that you view in incognito tabs won't stick around in your browser's history, cookies, or search history after you've closed all of your incognito tabs. Any files you download or bookmarks you create will be kept.

However, you aren't invisible. Incognito doesn't hide your browsing from your employer, your Internet service provider, or the websites that you visit.

LEARN MORE
Open Discussion – Q&A

Contact us:
sivadon.chaisiri@waikato.ac.nz
ryan@waikato.ac.nz