

Use of Ratings from Personalized Communities for Trustworthy Application Installation

Pern Hui Chia Centre for Quantifiable Quality of Service in Communication Systems (Q2S), NTNU

Andreas P. Heiner Nokia Research Centre, Helsinki

N. Asokan Nokia Research Centre, Helsinki

NordSec 2010, Helsinki Finland, 27–30 Oct

Outline

- Problem
- Theories & Design guidelines
- Online questionnaire
- Prototype
- User evaluation
- Discussion & Future work
- Conclusions

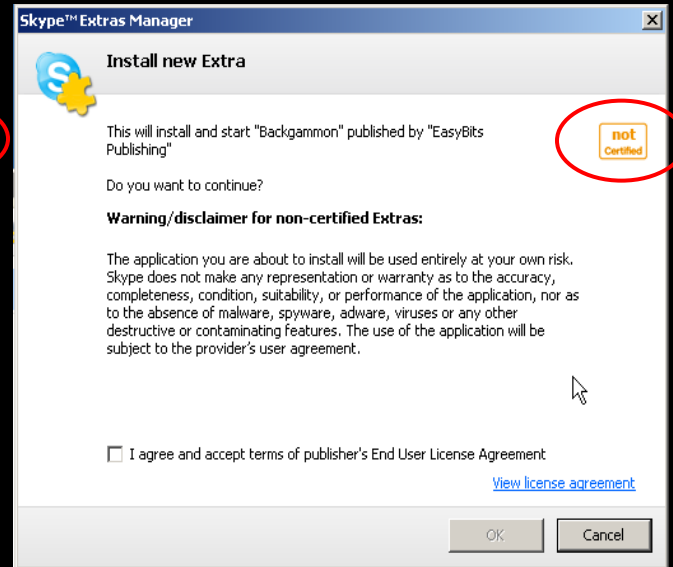
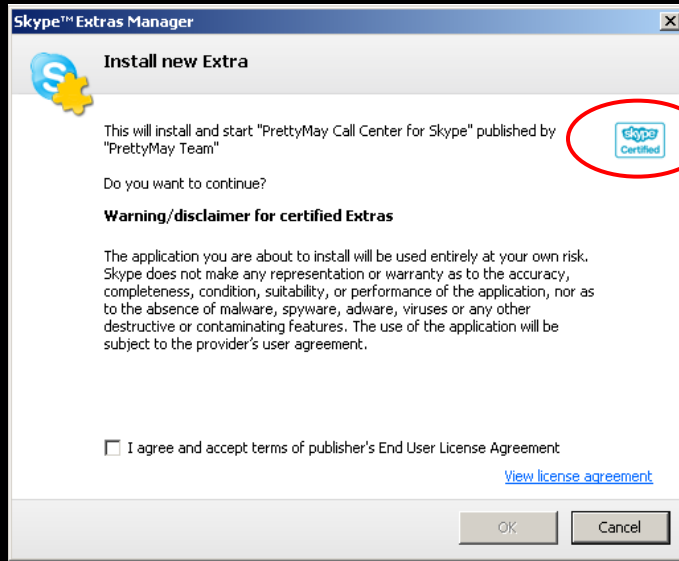
Problem

- Plenty of third party applications on mobile platforms
 - Vendors compete to attract developers
 - Requirement for app development lowered
 - Certification fees waived
 - Third party testing not required for basic apps
 - Easy tools to create simple apps: OviAppWizard (Nokia), AppWizard (Apple)
- What are inappropriate applications?
 - Malicious
 - Disregard user choice, consent or privacy
 - Offending certain cultural or social values

- Current approaches to software security => centralized
 - Flagging of ‘bad’ application by antivirus vendors
 - Certification of ‘good’ software by trusted entities / platform vendors
- Limitations
 - Apps are not clearly ‘bad’ or ‘good’
 - Certification \neq software security
 - Centralized means of signalling appropriateness is ineffective, leading to:
 - The risk of habituation
 - The risk of centralized judgment

The Risk of Habituation

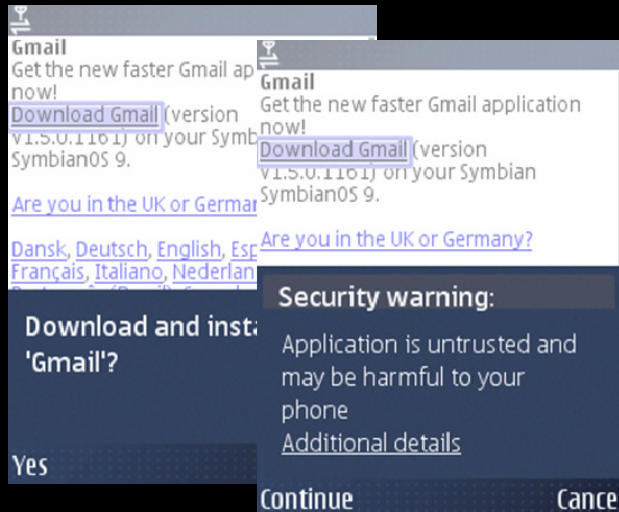
- Installers display **warning** or **disclaimer notices** when an app is not certified



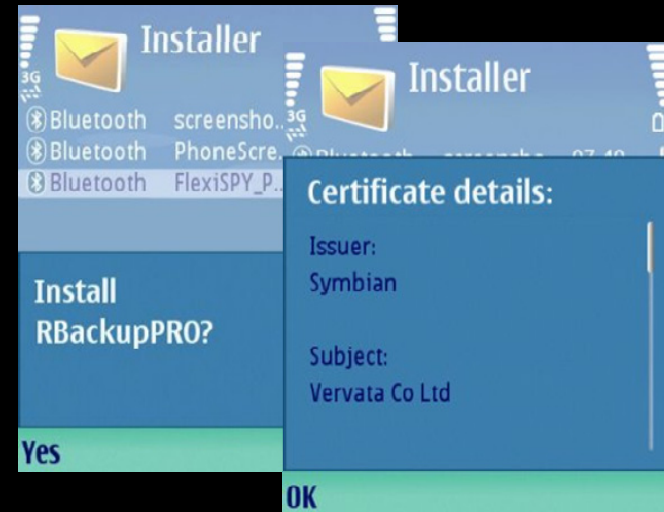
- But, they:
 - are context irrelevant
 - have low visual salience
 - result in a high false positive rate
- ⇒ user **habitually click-through** them

The Risk of Centralized Judgment

Gmail is not certified, so warned as untrusted and may be harmful.



FlexiSpy is regarded as Spyware by F-Secure, but it is certified.



- Apple determines which apps can be distributed in AppStore
 - Use hidden criteria (at least until recently)
 - Protests from developers and Electronic Frontiers Foundation

Cognition during installation

- Warning and disclaimer notices always look the same!
 - **Dual processing theory** ^[1] :
Controlled => automated (habituated) due to context constancy
- Search > Decide > Download > Warned [**too late**]
 - Security by designation ^[2] : Should discourage the unsafe decisions early

Information flow & risk signalling

- **Two step flow theory** ^[3] :
Information flows better through people than in the hypodermic needle style
- Signals from personalized community are trustworthy ^[4]
- Personified risks are perceived greater than anonymous risks ^[5]

Obj. A trustworthy application installation process

G1. Avoid requiring actions that can be easily habituated

- Normal and frequent context should be made implicit
- Use Attention Capture to signal deviation from normal context

G2. Employ signals that are visually salient, relevant and impactful

G3. Incorporate mechanisms to gather and utilize feedbacks from user's personal community

- Hypothesize that personalized signals is effective due to higher relevance & impact

Online Questionnaire

- To survey the behaviours during installation
- To evaluate the potentials of personalized communities
- 106 valid entries (>10mins each, completed all 105 Likert items)
- Participants are highly educated
 - 61% have IT/Eng background
 - 39% from Finance, Social science, Art, Science

Results:

- Information during installation is mostly ignored

	Seldom read		Usually abort installation
93%	Privacy policy	76%	If warned by antivirus software
83%	EULA	69%	If unnecessary questions asked
75%	Disclaimer notices	30%	If presented with system warnings

- Security vendors, experts & friends are important sources of digital risks info
- Users are motivated to inform friends and family members rather than online community members about digital risks

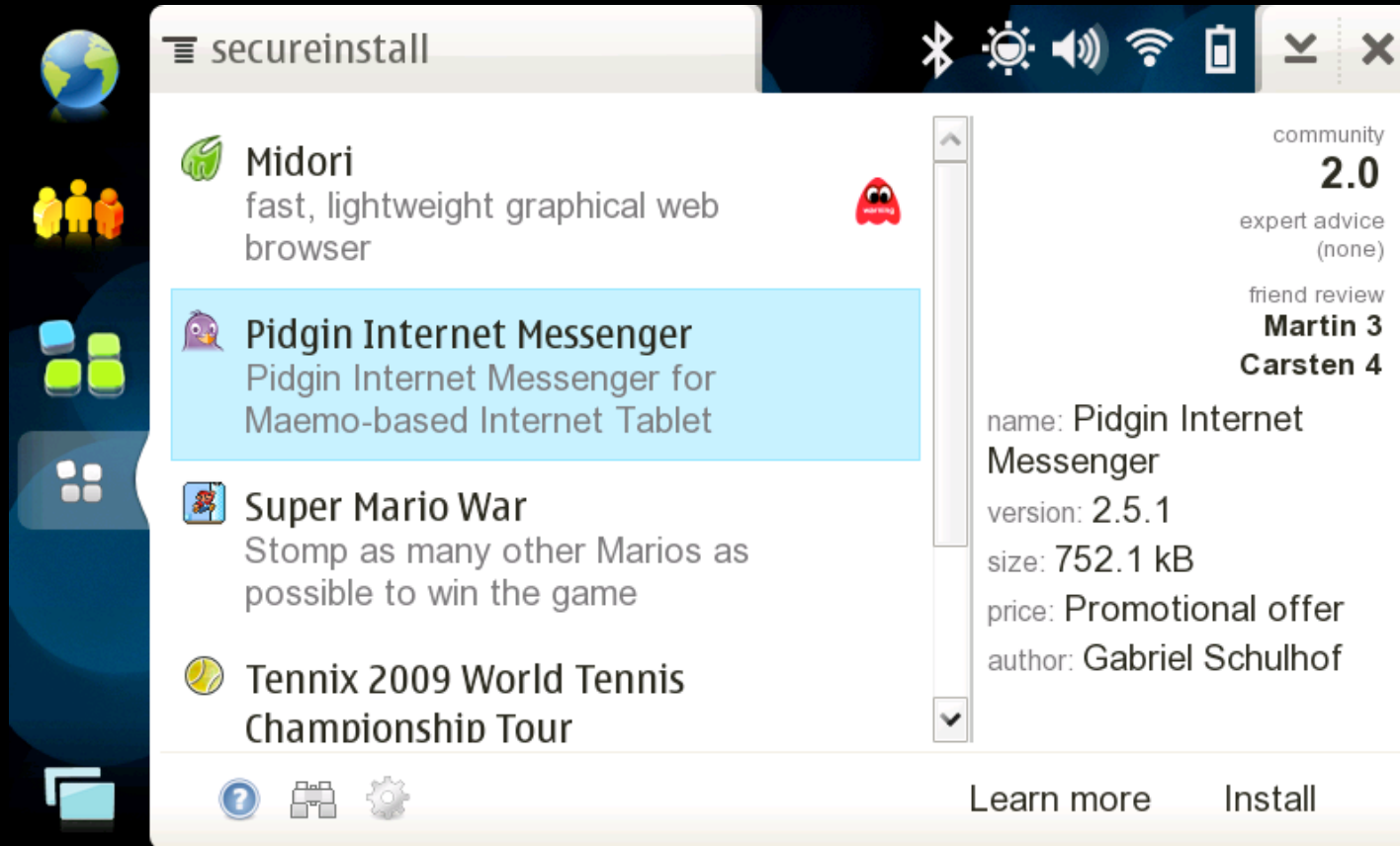
	Would always inform
62%	Friends or family member
15%	Online community members
11%	Experts
6%	Antivirus vendors

- Users consider reviews from trusted sources during installation helpful
- Results unchanged when excluding those with IT or Eng background

Prototype

- Implemented a simple *Rendezvous server*
 - to issue user certificates, manage user database, social graphs and reviews
- Software review
 - signed and validated on device
 - shared through rendezvous server or in a decentralized manner
- Redesigned the installation task flow
 - For ‘good’ apps, removed unnecessary steps that can become habituated
 - For apps ‘flagged’ by personalized community,
 - Show a warning cue prominently and early
 - Require users to attend to all negative reviews
 - Use habituation-breaking mechanisms

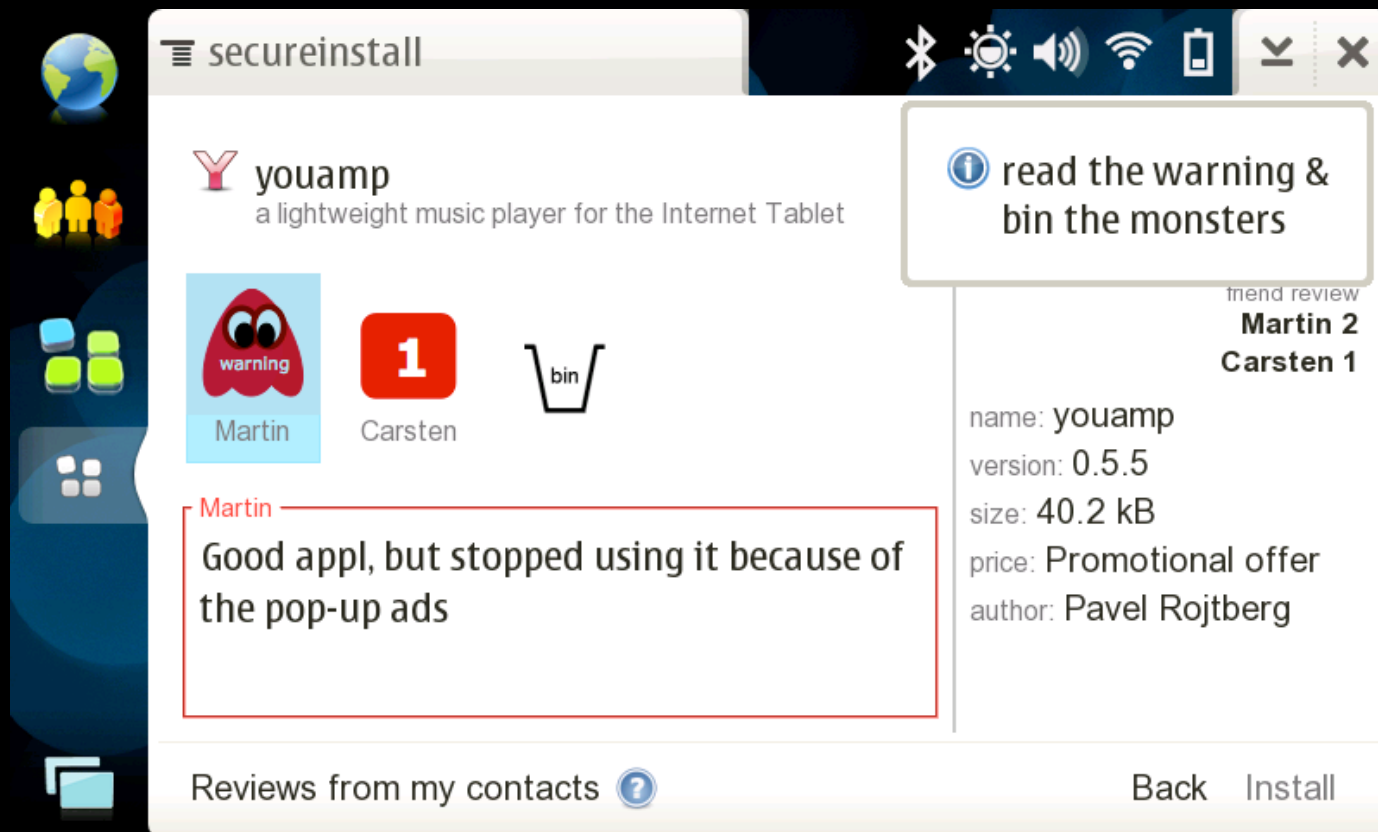
Example: Installing Pidgin is direct and easy



But not for Midori that has been flagged by user's friends ..
(Just for illustration purposes. Midori is a good and useful browser application in reality.)

Prototype (3)

- a. Directed to the review page
- b. Must attend to each negative review
- c. With a delay, user can drag each monster into bin if chooses to disregard warning
- d. Can only install when all monsters disappear = binned



User evaluation

- 20 participants, mainly from universities
- ~1 hour per session = 2 movie tickets




Activities

- Brief interview
- Consider whether to install apps in 4 scenarios with positive/negative reviews from friends/community
- Experience for design choices
- Debrief
 - inform the participants that reviews are created for experimental purposes only

Main results

- We found no evidence that negative community reviews overrule positive reviews by friends
- Negative reviews by friends overrule positive community reviews ($p < 0.001$)
- Overall strength of reviews by friends is stronger than that of community reviews ($p < 0.01$)

Experience with Monster risk symbol

- Draws attention, but may not give a clear message
 - Require efforts to educate users
- No strong preference of  over conventional  or 

Experience with habituation-breaking mechanism

- Mean score = 3.5 / 5.0 [variance = 1.5]
- Trade off convenience with safer user actions => hard to satisfy all users
- “Bin-the-monster” found to have weakly reduced the strength of risk signals
 - Fun mechanisms construed as a non-serious problem?
 - Designing a good habituation-breaking mechanism is an active research area

Experience with integrated social rating

- Mean score = 4.4 / 5.0 [variance = 0.6]
- Could be a nice device feature!

Discussion & Future work

- Reliability
 - Inputs from friends may be incorrect or not objective
 - + Evaluation can be structured into sub-ratings and aggregated wisely
- Coverage
 - + Notion of *expert users* to provide critical risk information
 - + Users learn about new software via friends
- Scalability
 - + Should integrate with existing social networks
- Incentives
 - Challenges in initiating and sustaining user efforts
 - + But, different from global systems where success is public good, personalized systems encourage unselfish behaviours of known contacts

Conclusions

- Guidelines grounded on theories for a trustworthy software installation process
- Prototype with review sharing & a redesigned installation task flow
- We find:
 - high relevance of inputs from friends and family members
 - user motivation to protect them when know of digital risks
 - high impact of risk signals from friends
- “Social rating integrated with application installation” is well received
 - Has potentials to mitigate the risks of centralized judgment and habituation

Reference

1. Kahneman, D. Maps of Bounded Rationality: Psychology for Behavioral Economics, *The American Economic Review*, 93(5):1449-1475, 2003.
2. Yee, K. P. Aligning security and usability. In *IEEE Security and Privacy*, 2(5):48-55, 2004.
3. Lazarsfeld, P., Berelson, B., and Gaudet, H. The people's choice, 1944.
4. Burt, R. S. The social capital of opinion leaders. *Annals of the American Academy of Political and Social Science: The Social Diffusion of Ideas and Things*, 566:37–54, 1999.
5. Camp, J. L. Reliable, usable signaling to defeat masquerade attacks. In *WEIS 2006*.
6. Schneier, B. The psychology of security, 2008. <http://www.schneier.com/essay-155.html>

Kiitos. Questions?

Project web: <http://aurora.q2s.ntnu.no/tsi>

Pern Hui Chia

chia@q2s.ntnu.no

www.q2s.ntnu.no/people/chia/

Andreas P. Heiner

andreas.heiner@nokia.com

N. Asokan

n.asokan@nokia.com