Context, CC/PP, and P3P

Patrik Osbakk
Computing Laboratory
University of Kent
Canterbury, Kent
CT2 7NF, UK
+44 1227 823824
pjo2@ukc.ac.uk

Nick Ryan
Computing Laboratory
University of Kent
Canterbury, Kent
CT2 7NF, UK
+44 1227 827699
N.S.Ryan@ukc.ac.uk

ABSTRACT
In this extended abstract we describe how CC/PP, a framework for describing user preferences and device capabilities, can be extended to support general contextual information. Whilst there has been some concern for privacy issues in the intended uses of CC/PP, this more general use increases the need for protecting sensitive contextual information. We describe how an additional 'privacy profile' can be used together with P3P, to determine what information is revealed

Keywords
Context, Privacy, CC/PP, P3P

INTRODUCTION: CC/PP and Context
Composite Capabilities/Preference Profiles (CC/PP) [1] provides a way for user agents, typically browsers, to specify metadata about device capabilities and user preferences. Using this information, services and content might be adapted to the client's capabilities and needs with much greater flexibility than can be achieved using, for example, the information in existing HTTP headers.

The information contained in a CC/PP profile can be considered as contextual information in the sense that it describes the environment in which the device operates and the user desires to operate. As such, it represents just a small part of the information domain of context-aware systems [2]. By extending CC/PP beyond its original limited base it can be used to specify different types of context, such as user identity and contact details, location and current activity, as well as information about their environment, such as noise levels or weather conditions. Indeed, one of the very few published examples of a CC/PP profile that recognises a use beyond device description includes location and weather conditions in a "UserSituation" component [3]. Such information can be used to improve the personalisation process, both for content adaptation and as part of a user's interaction with a context-aware service. It can also provide a standardised platform-independent structure that can be used to communicate context information in a ubiquitous computing environment.

Extending CC/PP to this role is straightforward. New components and vocabularies may be defined for any purpose. The context information that could be included in a CC/PP profile will be limited only by available vocabularies and the encoding format. A standardised vocabulary and encoding format would give the greatest interoperability between systems, but private vocabularies may also be defined to suit application specific needs.

CC/PP and Privacy
For some users, revealing even the basic device information contained in a typical CC/PP profile may be a cause for concern. When the profile contains more general contextual information, privacy becomes a major issue. To use a secure communication channel is not enough as the profile content might be used without the users knowledge and for purposes that they would not welcome. It is therefore important to provide a way for users to protect their privacy.

Several possible approaches to protecting a user's privacy might be taken when working with CC/PP. The whole profile might be protected and disclosed only to trusted parties. An initial 'minimal profile' might first be sent as part of a process to determine whether a service can be trusted [7]. Alternatively, the selection of which parts of the profile are disclosed could be made dependent on knowledge about the service. This latter approach has been investigated in more detail because of its potential flexibility.

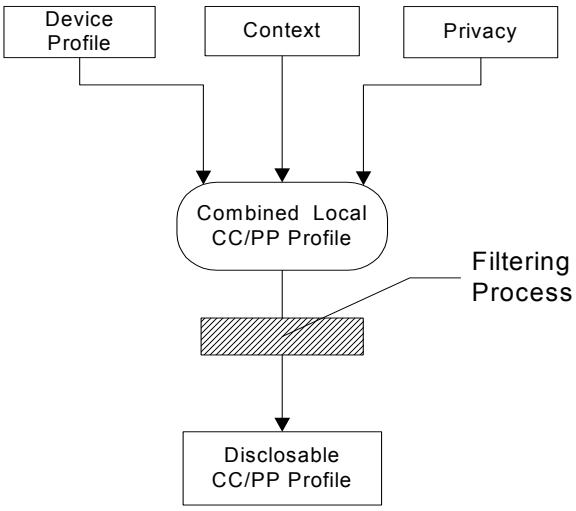
To be able to make automatic decisions regarding which parts of the profile to disclose or withhold, information about the user's privacy preferences needs to be available. The idea of a classification and clearance scheme has been used in this work to structure the privacy preferences. Each part of the profile is given a classification level that indicates the sensitivity of the information. For experimental purposes, a level from 0 (public) to 5 (private) has been used. Sites are then assigned a level of clearance depending on how trusted they are and what profile information they should be able to access. This scheme is somewhat limited and we anticipate using a more formal and flexible scheme, e.g. using a Role Based Access Control (RBAC) model [4], in the future. Below, we describe how the clearance level assignment can be automated using P3P.

Just as context information can be represented in a CC/PP profile by specifying a context vocabulary so also can privacy information with a privacy vocabulary. The design of the vocabulary would be dependent on what privacy

scheme is used and how it is implemented. But, because the privacy information is local to the client device and is never disclosed, the vocabulary and its implementation may vary from system to system.

Profile Filtering

A single CC/PP profile is used to combine device capabilities, user preferences, context, and privacy information. This combined profile is for local use only and needs to be passed through a filter to produce the revealed CC/PP profile, or profile differences, to be sent with a request. The filtering process enforces the privacy requirements by creating a profile that contains only the information that the user desires to disclose to the recipient. If a site has not been assigned a clearance level only public level information is disclosed.



P3P

The Platform for Privacy Preferences (P3P) [5] is a privacy-enhancing technology. It allows a privacy policy to be described in a machine-readable standardised format. The P3P policy is intended to be used to make informed decisions about the interaction between a user and a remote service. But P3P can also be used to protect a CC/PP profile [6] [7].

The way P3P has been used to protect the users privacy in this investigation has been to use it to establish the level of clearance to assign to a site. This is important as not all recipients of a CC/PP profile are likely to be known in advance and so clearance levels cannot be pre-assigned. If a RBAC model was used P3P could be used to establish what role to assign instead. To establish the level of clearance, a site's P3P policy is retrieved and compared with defined rule sets.

There can be one rule set defined for each clearance level, except for the public level 0. In the rule sets a user can specify what a P3P policy must and must not declare for a clearance level to be attained. If a rule set is not defined for a clearance level it is assumed that it cannot be attained by evaluating a P3P policy. The comparison in this investigation has been done with a modified version of the JRC P3P Appel Evaluator [8]. The comparison starts with the rule set that grants the highest clearance level. If the evaluation results in a positive result the site is assigned the current clearance level temporarily. If the result is negative the comparison continues with the next lower clearance level rule set. The comparison continues until a clearance level has been assigned or no more rule sets are available, resulting in a clearance level of 0 being assigned.

Conclusion

We have described how CC/PP can be used to communicate context, how the users' privacy can be protected and how this protection can be automated using P3P. The use of P3P and CC/PP profile filtering has been described in a typical user agent/web server scenario. Other experiments have shown that this approach is also applicable where the profile can be queried by a remote system that can supply a P3P policy, either in a peer-to-peer environment or through an intermediate context service. It is hoped that technologies like CC/PP and P3P may help to make context-aware personalisation services more readily available.

REFERENCES

1. Composite Capability/Preference Profiles (CC/PP): Structure and Vocabularies [W3C Working Draft 15 March 2001], World Wide Web Consortium (W3C).
2. B. Schilit, N. Adams and R. Want, 'Context-Aware Computing Applications', IEEE Workshop on Mobile Computing Systems and Applications, 85-90, 1994.
3. CC/PP Implementors Guide: Harmonization with Existing Vocabularies and Content Transformation Heuristics [W3C Note 20 December 2001], World Wide Web Consortium (W3C).
4. Sandhu, R. S., Coyne E. J., et al. Role-Based Access Control Models. *IEEE Computer* 29,2 (1996), 38-47.
5. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification [W3C Recommendation 16 April 2002], World Wide Web Consortium (W3C).
6. Nilsson, M., Lindskog, H., Fischer-Hübner, S. Privacy Enhancements in the Mobile Internet. *Proceedings of the IFIP WG 9.6/11.7 working conference on Security and Control of IT in Society*. (Bratislava, June 2001).
7. CC/PP Implementors Guide: Privacy and Protocols [W3C Working Draft 20 December 2001], World Wide Web Consortium (W3C).
8. Hogben, G. JRC P3P Appel Evaluator Java Module. Available at http://p3p.jrc.it/.