On Providing Automatic Parental Consent over Information Collection from Children

Karthik Channakeshava*, Kaigui Bian*, Michael Hsiao*, Jung-Min Park*, Robert Crossler†, France Belanger†, Payal Aggarwal‡ and Janine Hiller‡

*Bradley Department of Electrical and Computer Engineering
†Department of Accounting and Information Systems
‡Department of Finance, Insurance and Business Law
Virginia Tech, Blacksburg, VA 24061
E-mail: {kchannak,kgbian,mhsiao,jungmin,robc,belanger,payal,jhiller}@vt.edu

April 28, 2008

Abstract: Children’s privacy has become critical with the increasing use of the Internet for commercial purposes and corresponding increase in requests for information. 65% of children between the ages of 10 and 13 use the Internet for casual web surfing, chatting, games, schoolwork, e-mail, interactive learning, and other applications. Often, websites hosting these activities ask for personal information such as name, e-mail, street address, and phone number. The Children’s Online Privacy Protection Act (COPPA) of 1998 was enacted in reaction to the widespread collection of information from children and subsequent abuses identified by the Federal Trade Commission (FTC). COPPA is aimed at protecting a child’s privacy by requiring parental consent before collecting information from children under 13.

In this paper, we describe an automated tool for protecting child privacy called Parental Online Consent for Kids Electronic Transaction (or POCKET). The POCKET framework is a novel, technically feasible and legally sound solution to automatically enforce COPPA. Parents answer a simple questionnaire regarding their privacy requirements and the POCKET user agent automatically converts it into a privacy preferences file. These preferences are enforced when a child uses the Internet. Only websites that adhere to the preferences can receive the child’s information, while websites whose policies do not match are blocked. A merchant-specific privacy information package and a signed digital agreement are uploaded to the qualified merchant from the client (child’s machine). POCKET framework incorporates a secure handshake protocol to protect the data exchange between the client and the merchant. A local log file created by POCKET and the digital agreement are used to enforce merchant accountability.

Keywords: COPPA, children’s privacy, verifiable parental consent

1 Introduction

A paramount concern of individuals using the Internet is the protection of their privacy, especially children’s privacy. Recognizing the importance of protecting children’s privacy on the Internet, the Children’s Online Privacy Protection Act of 1998 (COPPA) requires parental consent before websites can collect information from children under the age of thirteen. The FTC has adopted regulations to enforce COPPA. Unfortunately, the current business practices used and the technical approaches employed to comply with COPPA, fail to protect children’s privacy effectively. The present research addresses this issue by: (1) evaluating the awareness and use of privacy protection tools by parents, and (2) developing a tool to provide or deny parental consent for online collection of information from children.

Recent surveys show that the awareness regarding personal privacy is growing. A Harris poll [1] designed by Privacy & American Business and sponsored by Microsoft found that 35% of Americans had “very high privacy concern.” 65% had refused to register at an e-commerce site because of privacy concerns while, 60%...
The outline of the paper is as follows: Motivation for the research is provided in Section 2. The architecture of POCKET and the framework we propose is outlined in Section 3. Section 4 details the implementation of POCKET and the various phases in the protocol interaction. Security features and the handshake protocol of POCKET is outlined in Section 5. The details of the prototype we have built for further evaluation is outlined in Section 6. Section 7 concludes the paper.

2 Motivation

Currently, there is no widely available, effective technology that implements a parent’s ability to choose what information is shared by a child with a commercial website. While children need protection online from the dangers of sharing personally identifiable information because they are socially immature and naive, they are correspondingly sophisticated about the use of the Internet and technology. Computers and Internet usage are ubiquitous, frustrating the busy and less technological savvy parent from fully protecting their child online. A recent example of this problem is the case of Xanga.com [3], an interactive social networking site that was fined $1 million dollars by the FTC for failing to effectively implement parental consent for children to use the site. Its failure was massive, with over 7 million children accessing the site, created profiles with birth dates indicating they were under 13. Further, Xanga.com failed to notify parents about their information collecting practices or provide access and control to the information collected from children. Social networking sites, where personal information abounds, can pose a special danger to children who may share offline identifying information that will allow them to be contacted or tracked. By implementing parental control over the personally identifiable information that a child can share, COPPA intends to empower parents to protect their children. Yet, as the Xanga.com case shows, the protocol as it now exists requires a website to contact the parent for consent, and children are adept at circumventing website procedures. POCKET is designed to reverse the procedure and will allow a parent to control access unless the website consents to the information collection parameters.

The goal of this research is to develop a tool that provides a reliable, trustworthy technology option for obtaining verifiable parental consent as required by COPPA. The tool’s effectiveness will depend upon meeting parental acceptance and business standards. The proposed tool, called the Parental Online Consent for Kids Electronic Transaction (POCKET) is described further in this paper. POCKET provides an easy-to-use interface for parents to configure privacy choices for their child, and then automatically enforces these policies. By maintaining an activity log of the interaction with the websites it provides a way to ensure accountability in case of disputes.
2.1 Available Technology and Seal Solutions

P3P specifies privacy policies in well defined language constructs so that automated tools can compare them with user preferences and indicate (to the user) when there is a mismatch. However, research into the implementation of P3P found errors in policy implementation, violations of policy, and incomplete policies [4], leading the authors to recommend the use of a third party to certify compliance. Even if P3P could be implemented in a dependable manner, the privacy language constructs are not fine grained enough to address the specific choices that a parent would make regarding the exact information that a website could or could not collect or share. The Nintendo privacy policy recognizes the limitations of P3P for explaining human privacy concepts in machine readable code [5] and claims that the Privacy Policy has precedence over the P3P policy as it accurately represents data collection practices. Lastly, and most importantly, P3P does not incorporate any method whatsoever for inserting the parent’s consent over the child’s information; it is a two party negotiation system only.

Privacy seal programs have been implemented in order to address concerns that websites were not honestly revealing their practices to consumers, and that lack of privacy was discouraging consumers from participating in electronic commerce. However, researchers have also found that privacy seals in general do not engender trust from online consumers [6]. Because privacy seals in general have not been successful, it is unlikely that COPPA compliant seals will fare any better. The following section, confirms this intuition.

2.2 Parental Control and Awareness

COPPA seeks to protect children by giving parents control over what information their children can share. For parents to protect their children, they must be aware of website information collection practices and their right and ability to control this. We used a focus group approach to understand privacy protection awareness, elicit requirements for POCKET, and receive feedback on the prototype.

For these focus groups a protocol was developed, tested, and modified several times. Parents were invited to participate in one of four focus groups without knowledge of focus group details (to avoid self selection bias). The session lasted 60 minutes. Each focus group had between 3 and 6 people who ranged in age from 29 to 48 years old with children under the age of thirteen: for a total of 14 females and 4 males. Eleven browsed the web everyday, two several times a week, four once a week, and one once or twice a month. Five of the parents are high school graduates, three graduated from a two-year college, five have bachelor’s degrees and five have graduate degrees. Twelve of the parents’ children browsed the web more than several times a week, three once a week, two once a month, and one never. Two researchers attended and moderated the focus groups, which were recorded.

Results from the focus groups indicate that while most parents warn children not to give information online, they are not sure children respect that; one of them knew of laws protecting children’s information online; none of them knew if merchants do anything to protect children’s privacy online; two had been asked for their consent by a website for their children’s information; and, none knew where to report fraudulent web activity. None had ever “heard of” Children’s Advertising Review Unit (CARU) [7]. All but one had “never heard of” PRIVacy Vaults Online (PRIVO) [8], Entertainment Software Rating Board (ESRB) [9], or TRUSTe [10]; one had “vaguely heard of it.” Ways parents use to control what children view online include placing stations in plain view; telling children they could track sites browsed (though admitting they didn’t know how); one uses the AOL age block and tracking service; and one uses software called “Content Protect.”

Looking at these results we strongly feel that the POCKET framework is the best solution. It is an easy to use, automated tool that can be used by a technologically unsophisticated parent and deployed to protect children’s privacy. It puts control into the hands of the parent and identifies the website visitor as a child. POCKET allows parents to implement the choice that NO information be collected from their child. Automatation provides the advantage that the parents do not have to constantly supervise and worry about disclosure of personal information by their children. Once deployed it will provide a way to enforce the parental consent requirement of COPPA. In the next few sections we discuss more details regarding the POCKET framework and the security protocols involved to ensure childrens’ privacy.

3 The POCKET Framework

The POCKET framework utilizes and extends the P3P framework by (1) incorporating a trusted third party (TTP) during interaction, (2) extending the merchant policy to include data elements as required by COPPA, the use and handling of data collected, and (3) automated exchange of personal information between the client and server. POCKET user agent allows merchants to identify the client as a child and automatically obtain parental authorization for information collected from the child.
Mont and Bromhall [11] and Mont et. al. [12] proposed increased user control over the disclosure of information and merchant accountability for using the data collected. Our technical solution extends this work by employing a stronger mechanism for ensuring merchant accountability. We employ a four entity architecture for security and enforcement. The first two entities are the parent/guardian and the child. The parent/guardian (denoted as the “user”) enforces the privacy preference for the child (denoted as the “client”) and in this way provides a form of verifiable parental consent as required by COPPA. The privacy preference implemented on the client’s side is called the user privacy preference and the XML format file containing the preferences is called the user privacy preferences file (UPPF). The third entity is any merchant or website the client visits. The privacy policies of the merchant are specified in a merchant privacy policy file (MPPF). The trusted third party (TTP) forms the fourth entity involved in POCKET.

The use of a TTP is derived from the 3-entity architecture proposed for identity based encryption (IBE) [11]. In POCKET the role of a TTP is to provide mutual authentication—the merchant and client authenticate each other’s policies (similar to trust seals), public key distribution and assignment of a (one time) TTP signed ticket to each client for access to POCKET compliant merchant websites. TTP also serves as an enforcement agency in case of disputes between the merchant and the client.

The existing P3P vocabulary can be easily modified to include additional categories to recognize the data collected from children. Since this is not the focus of this paper, we use a simple yet effective XML-based vocabulary set instead of P3P. Figure 1 shows an example POCKET preferences file created at the client side. The merchant side policy includes only the PREF tag for each category of information and the corresponding option value.

Websites provide hypertext markup language (HTML) forms to collect client’s information. POCKET implements automatic information transfer and avoids forms completely. Some advantages of doing this in the context of protecting child privacy are: (1) It prevents the websites from collecting more information than specified in the UPPF. Forms may collect information that is optional and a child is not mature enough to know what information to disclose and what not to disclose. (2) The POCKET client (once validated) is guaranteed to provide only information that is absolutely necessary. (3) The information package is transmitted securely to the website without the risk of being eavesdropped. On the merchant’s side, POCKET is implemented by augmenting websites with an additional policy targeted towards children. This requires changes to the P3P policy file oriented towards the children visiting the website and the information collected from them.

4 Implementation of POCKET
The software implementation of POCKET consists of a user agent (UA) and browser helper object (BHO). Once deployed on the client machine, the four entities exchange messages based on a protocol divided into three phases – registration, setup and transaction. The software installer package is available for download from the TTP server during the parent registration phase. The UA has two modes – parent-mode and child-mode. The software can be setup on the client machine in the parent-mode. During setup, the UA provides a questionnaire to the parent. The parent’s responses are converted to an UPPF and stored on the client machine. When the UA enters the child-mode it installs the BHO and enforces the preferences. The BHO coupled with the browser can intercept user communication with the Internet. For security purposes, the UA requires the parent’s password for any modification of the privacy preferences. The details of the phases in the POCKET framework is provided below.

4.1 Registration Phase
Figure 2 shows the pictorial representation of the registration phase. The user performs a one time registration accessing the TTP through a website. During this phase the user registers with the TTP server and creates an account. Although not particularly specified in the POCKET protocol, parental verification will be implemented at the time of registration. The parental verification ensures that the person’s real world identity matches with their virtual identity. Since, the user does not have to authenticate interaction with every website (POCKET employs one-time verification), the verification can be thorough. Though the actual method used to achieve this is outside the scope of the paper, tools like Idology’s ExpectID® IQ [13] can be used. The one time verification is necessary because the password created by the parent at this time will be used for authentication during subsequent interactions with the TTP. The TTP server assigns a unique ID to the user (parent/guardian). Registration provides the parent with the POCKET installer containing the UA, BHO and a TTP-signed ticket (used during the transaction phase).

The merchant also registers with the TTP server for participating in the POCKET protocol. The merchant provides answers to a questionnaire regarding the websites’ data collection practices and use policies. The
answers to the questionnaire are converted into a machine readable XML format file and the MPPF is created. The merchant is required to deploy this file in a prescribed location on the merchant website. During the transaction phase, this file is compared with the UPFF. The TTP also provides the merchant with a POCKET complaint certificate during registration. The client uses this certificate to authenticate the merchant during transaction phase.

4.2 Setup Phase

The parent configures the POCKET UA by executing an installer and activates it before deploying it. The UA also requires the user to create a login and password (on the client machine). This login is only for the purpose of protecting the POCKET’s configuration on the client machine. The parent chooses the child’s personal information that the merchant can collect. The client’s information may include personal information (for example, full name, address and phone number), sibling data, school information among others. The parent can also configure the POCKET UA such that no information is collected from the child. The UA then converts the parent’s preference into a UPFF and stores it on the client’s machine. The POCKET UA automatically enables the BHO after this configuration is complete. The BHO enforces the preferences specified in an UPFF.

4.3 Transaction Phase

Figure 3 shows the interaction between the client and the merchant website during the transaction phase. When the client enters the merchant website’s uniform resource locator (URL) in the browser, the BHO installed on the client’s browser (without client involvement) requests the MPPF, the POCKET certificate and the merchant information collection practices. Here, we are assuming that the merchant complies with POCKET’s requirement and places the MPPF in a prespecified location. The POCKET agent decides to allow or block a website after comparing the MPPF and UPFF. If the policy and preferences do not match, the BHO displays a “privacy policies do not match” message to the client and blocks the website. In the event the merchant is not registered in POCKET (or does not have MPPF in prespecified location), the current implementation blocks the website altogether. If the MPPF and UPFF match, the client creates a merchant specific privacy information package (PIP). The PIP only includes the personal information requested by the merchant and is a subset of the information that was given consent (by the parent) to be disclosed. Using a secure handshake protocol, the client side BHO uploads the PIP to the merchant site and allows the browser to display the website. The POCKET agent on the client machine maintains a log file entry showing the access. The release version of the POCKET software will include uploading of a digital contract1 along with the PIP. The log file and the digital contract are useful in enforcing merchant accountability.

5 POCKET’s Security Features

The data exchange protocol, especially the transaction phase, between the client and the merchant website is vulnerable to several attacks. Specifically, the transaction phase is vulnerable to unauthorized uploads and man-in-the-middle attacks. In this section, we analyze them and propose relevant countermeasures in the various phases of the client interaction with POCKET.

With POCKET system in place merchant websites accept client’s privacy information package and store it for further processing. The parental verification during parent registration (Section 4.1) ensures that the attacks from the anonymous user uploading spurious and harmful data is avoided. Without authenticating legi-

1A digital contract is a legal agreement between the client and the merchant regarding the collection and use of information gathered.
The man-in-the-middle attack is another type of attack that can be launched against this system. This attack happens when a valid packet is intercepted and manipulated or processed for information. Potential problems with a man-in-the-middle attack are: (1) eavesdropping on sensitive and personal information, (2) information modification, and (3) packet replay at a later time. In addition to mutual authentication, the TTP performs the role of a key distributor and employs a pretty good privacy (PGP) framework [14]. With public-key exchange between a client and a merchant, the confidentiality and integrity of data can be protected by encryption with a session key and a digital signature respectively. The replay packets can be identified and ignored by employing a typical challenge/response handshake protocol. An attacker cannot eavesdrop on, or modify the contents of a valid packet. The following sections provide more details on how the proposed mechanisms are implemented in the POCKET framework.

Registration Phase Ticket Distribution — In the registration phase, the user is required to create an account on the TTP server. This account creation is run inside a secure HTTP tunnel. The TTP server generates a public/private key pair, assigns a user ID (UID), and issues a certified service ticket. The parent downloads the installer before the end of the session. The UA on the client’s machine uses the ticket to prove the client’s identity. The public/private key pair is used for exchanging the session key and preventing unauthorized access to the merchant server.

One Ticket Authentication Protocol — In POCKET, entity authentication between the client and the merchant is provided via an authentication protocol. The keys and tickets needed in the protocol are distributed by the TTP. Like the Kerberos [15, 16] authentication system, the POCKET’s authentication protocol uses a ticket to authenticate the client to the merchant website. The current implementation of POCKET employs a single ticket but can be easily extended to use a new ticket for each session of the transaction.

Secure Transaction Phase — The secure transaction phase implements a protocol similar to the pretty good privacy (PGP) [14] framework to provide confidentiality, authenticity and integrity. If the merchant site is deemed POCKET compliant, a client machine uploads the PIP to the merchant. The confidentiality during this phase is provided by encrypting messages to be transmitted. Integrity and non-repudiation of messages sent by the client to the merchant server are ensured by attaching a digital signature to each message (obtained during the registration phase). Only clients with a valid TTP-issued ticket are allowed to upload data to the merchant server.

6 POCKET Software Prototype

We have completed a prototype of POCKET UA and BHO on Windows XP operating system. The current implementation of the BHO works for Microsoft’s Internet Explorer version 6.0 (IE6) and can be easily extended for other versions and browsers. POCKET con-
sists of a UA and BHO implemented in Visual C++. The UA is a simple dialog based application that is used to configure POCKET on the client machine. The POCKET installer stores the keys and the certified ticket on the client machine for the UA’s use during the transaction phase. The parent configures POCKET with a setup password and protects the parent-mode from unauthorized access or modification. After installation, the UA automatically presents the parent with the privacy preferences configuration dialog. By selecting the items the parent is allowing the merchant to collect particular information from the child. The UA converts the parent’s selections into an UPPF and stores it in the client’s machine. The UA then requires the parent to enter the actual information for the preference elements configured in this dialog. After configuration, the UA automatically enters the child-mode, starts the BHO and enforcing this UPPF when the client visits any website. Any shift from the child-mode to the parent-mode needs the parent’s setup password. To prevent the client from disabling POCKET UA, terminating the POCKET UA also requires the parent’s authentication.

A BHO is a DLL module designed as a plug-in to Microsoft’s Internet Explorer web browser. The BHO API provides hooks to attach to the document object model (DOM) of the current page. The API controls the navigation within the page. POCKET BHO implements an XML parser for making comparisons between the MPPF and the UPPF. For XML parsing we use the Xerces XML parser [17]. If the UPPF and the MPPF match, the BHO builds the PIP based on the merchant needs (specified in the MPPF) and uploads the PIP using a secure protocol to the merchant site. We use the Crypto++ API [18] to implement the security protocol of POCKET.

We have created mock merchant websites that support the MPPF required by the POCKET BHO. We have tested the software implementation using these mocked websites. We used a simplified XML file format that is consistent with the P3P specifications to create the privacy preference files.

7 Conclusion

In this paper, we have presented a new privacy-enhancing framework called POCKET and have implemented a prototype for protecting children’s privacy online. POCKET implements an automatic way to obtain verifiable parental consent as required by COPPA. It is an easy-to-use tool that technologically unsophisticated parents can deploy to protect their child’s privacy. With POCKET, parents can control the personal information collected by websites from the child without constantly monitoring their activities online. The client’s preferences and the merchant policy files have a format that is consistent with the P3P specifications. POCKET assumes the merchant policy file is placed in a specified location on the server, and POCKET includes a secure protocol for uploading personal information from the client to the merchant. It also establishes mechanisms for merchant accountability by maintaining activity logs. With mock merchant websites, the prototype demonstrated its promise in offering a COPPA-compliant platform.

References