CONTEXT-AWARE SECURITY POLICY AGENT FOR MOBILE INTERNET SERVICES[1]

George Yee and Larry Korba
Institute for Information Technology, National Research Council Canada, 1200 Montreal Road, Bldg. M-50, Ottawa, ON, Canada K1A 0R6;
{george.yee, larry.korba}@nrc-cnrc.gc.ca

Abstract: The recent proliferation of e-services on the Internet (e.g. e-commerce, e-health) and the increasing attacks on them by malicious individuals have highlighted the need for e-service security. E-services on the mobile Internet (mi-services) are no exception. However, for mi-services, the level and type of security may depend on the user's security preferences for the service, the power of the mobile platform, and the location of the mobile platform (we label these UPL). For example, if the user is traveling through a particularly dangerous area known for previous attacks, the security protection should be adjusted to use mechanisms that are resilient to these attacks. We propose the use of a security policy that allows for various security options commensurate with UPL, in conjunction with a context-aware security policy agent that notifies the service provider to activate new security appropriate to a change in UPL.

Keywords: context-aware; software agent; security policy; mobile Internet; services.

1. INTRODUCTION

Internet-based e-services for banking, shopping, learning, healthcare, and Government Online have been growing rapidly and are now spreading themselves within the mobile Internet (Ho and Kwok, 2003; Mallat et al, 2004). However, these services are subject to malicious attack in one form or another. This leads to concerns over their security (Josang and Sanderud, 2003; Ghosh and Swaminatha, 2001; Joshi et al, 2001).

In order for mobile Internet services (mi-services) to be successful, they must be secured from malicious individuals who continuously try to compromise them. An effective and flexible way of managing security for mi-services is to make use of security policies. A mi-service security policy

is a specification of what security measures will be used to protect the mi-service from security attacks. It should be noted that a security policy by itself does not guarantee that its stated security measures will be put in place or be complied with. That is an area of policy compliance that is outside the scope of this paper.

A mi-service provider makes use of a security policy to specify the security measures that it will use to protect its mi-services. However, this security policy may not match up with the security needs of the mi-service, depending on the user's security preferences for the service, the computational power of the mobile platform, and the location of the mobile platform. For example, suppose the security measure for an e-learning application is user authentication by means of a password. This authentication approach is known to be insecure. A security-sensitive consumer such as, for example, a defense contractor, may wish to add biometric authentication for an e-course on advanced weapons research. In such a case, the defense contractor would not want to use the provider's mi-service that only has password authentication. As another example, suppose the security measure is access control. The provider's security policy may provide access to 5 features of a mi-service, whereas a particular consumer may need access to only 3 features. In this case, the consumer may be reluctant to make use of this provider's mi-service, especially if the consumer can find another provider that only offers the features needed and at a lower price. As a third example, suppose the security measure for a mobile banking application calls for encrypting the communication channel using AES (Advanced Encryption Standard). However, the user's cell phone has insufficient computing power to compute AES with reasonable performance. Again, the consumer would find it unsafe (or impossible) to use the mobile banking mi-service. As a final example, suppose there is an area of a large city that is notorious for man-in-the-middle attacks against mi-services. Mi-service consumers try to avoid this area but occasionally they have to traverse it in order to get to their destination. Unfortunately, the mi-service provider cannot target this particular area for more effective security against man-in-the-middle attacks so that once again, the service consumer is faced with a difficult situation.

As a solution to these issues, we propose the use of a context-aware security policy agent that would initiate the best available security measures for a mi-service depending on the user's security preferences for the mi-service, the computational power of the user's mobile platform, and the location of the user's mobile platform. We refer to this combination of user preferences, power, and location as UPL. Thus, referring to the examples above, the agent would trigger biometric authentication according to the user's preference, trigger access control for 3 features instead of 5, initiate a less computational resource intensive encryption algorithm (with acceptable loss in effectiveness), and invoke more aggressive defenses against man-in-

the-middle attacks, according to the values of UPL. We further propose that the available best security alternatives be stated in a mi-service security policy that is negotiated and agreed between the mi-service consumer and the mi-service provider prior to using the service. Security policy negotiation is outside the scope of this paper but is described in Yee and Korba (2005).

In the literature, there are many papers related to security policies. Security policies have traditionally been used to specify security requirements for networks and distributed systems (Varadharajan, 1990). More recently, they have been applied to manage security for distributed multimedia services (Duflos, 2002) and for very large, dynamically changing groups of participants in, for example, joint command of armed forces for some time period (Dinsmore et al, 2000). In addition, Ventuneac et al (2003) describe a policy-based security framework for web-enabled applications, focusing on role-based security policies and mechanisms. None of these authors use security policies containing selectable alternatives as we do in this work.

We note here that our use of context-aware security policy agents for mi-services is a form of service personalization. A key difference between mi-services and stationary Internet services is that mi-services are more personal (Chae and Kim, 2003). Ho and Kwok (2003) state that mobile service personalization is sought after by service consumers. Therefore our proposal for the use of context-aware security agents as a form of personalization should be welcomed by mi-service consumers.

The remainder of this paper is organized as follows. Section 2 defines mi-services, derives requirements for security policies, and gives an example of a security policy with alternatives that can be used with our context-aware agents. Section 3 describes our context-aware security policy agents and how they are used. Section 4 presents a discussion on operational and implementation requirements for the agents. Finally, Section 5 gives our conclusions and areas for future research.

2. MI-SERVICES AND SECURITY POLICIES

2.1 Mi-Services

A mi-service for the purposes of this paper is an Internet service accessible using a mobile device such as a cell phone or wireless PDA. Figure 1 shows a network view of mi-services. In this figure, the mobile ISP (Internet Service Provider) provides mobile wireless access to the Internet. The mi-service provider provides the actual service.

The mi-service provider has a security policy that specifies what UPL alternative security measures it will use to secure its service(s). The

consumer has security preferences for the UPL alternative security measures that will be implemented for the mi-service. In addition, the security policy implemented for the mi-service is transparent to the mobile ISP, i.e. the latter does not need to provide any kind of special support for implementation of the security policy, beyond what it normally provides for secure communication (the security policy is implemented at a higher architectural layer). This is important since involving the mobile ISP in the security policy would introduce further necessity for negotiation and agreements and possibly overload the mobile ISP in terms of processing requirements. Examples of current mi-services accessible via a wireless PDA are Amazon.com (online retailer), optionsxpress.com (online stockbroker), and WebMD.com (health information and technology solutions provider).

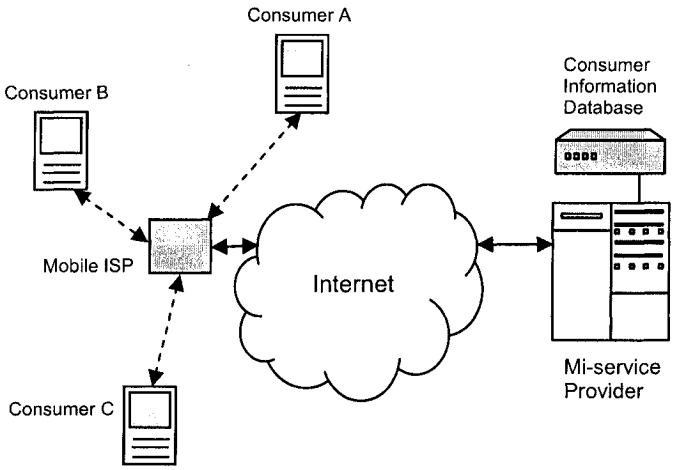

Figure 1. Network view of mi-services

2.2 Security policy requirements

Requirements for mi-services security policies address what security measures should be covered in a mi-service security policy. Since mi-services fall under the category of open systems, we begin by looking at requirements prescribed by ISO 7498-2, the reference model for security architectures by the International Organization for Standardization (International Organization for Standardization, n.d.). This standard identifies 5 main categories of security services: 1) Authentication, 2) Access Control, 3) Data Confidentiality, 4) Data Integrity, and 5) Non-repudiation.

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) provides Recommendation X.800, Security Architecture for OSI (Open Systems Interconnection) (International Telecommunication Union, n.d.) that lists the same 5 main categories of security services as above. We propose that these 5 categories of security services be covered in a mi-services security policy. We would add the following security services: 6) Secure Logging – of user transactions by the provider, 7) Certification – user or provider would use a certifying authority to certify credentials, 8) Malware Detection – user or provider would use some anti-malware software to detect and eliminate malware from their computing platforms, and 9) Application Monitoring – user mobile platform monitoring for licensed, verified, and permitted applications.

We thus have 9 security services that should be specified in a mi-service security policy. Figure 2 identifies where these security services are typically applied using a mi-service network view.

The above standards also list specific security services under the main security service categories. As an example, non-repudiation has the specific services (with the obvious meanings): "Non-repudiation, Origin" and "Non-repudiation, Destination". As well, security mechanisms (e.g. digital signature) are used to support security services, i.e. security policy requirements. We will employ specific security services and mechanisms to formulate our mi-services security policy.

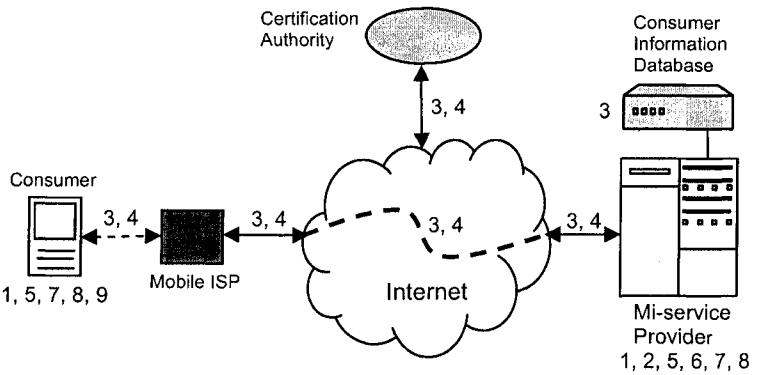

Figure 2. Application of security services (numbers correspond to security services in Section 2.2)

2.3 Mi-Service security policy

Based on the requirements of Section 2.2, and using example values and security mechanisms, we propose the example mi-service security policy shown in Table 1.

Table 1. Example mi-service security policy in schematic form

Policy Use: **My Service** ***Valid:*** **unlimited**	***Owner:*** **My Service Provider, Inc.**
CONSUMER PROVISIONS	**PROVIDER PROVISIONS**
Consumer Authentication *Implement:* yes (default) *P1: Mechanism:* password *P2: Mechanism:* V+F biometrics	**Provider Authentication** *Implement:* yes (default) *P1: Mechanism:* security token *P2: Mechanism:* digital signature
Consumer Non-Repudiation *Implement:* yes (default) *Mechanism:* digital signature	**Provider Non-Repudiation** *Implement:* yes (default) *Mechanism:* digital signature
Consumer Certification *Implement:* yes (default) *Mechanism:* certificate	**Provider Certification** *Implement:* yes (default) *Mechanism:* certificate
Consumer Malware Detect *Implement:* yes (default) *Mechanism:* Norton	**Provider Malware Detect** *Implement:* yes (default) *Mechanism:* Norton
Application Monitoring *Implement:* yes (default) *Mechanism:* IIT-ISG	**Data Store Confidentiality** *Implement:* yes (default) *Mechanism:* 3DES encrypt
	Communication Confidentiality *Implement:* yes (default) *P1: Mechanism:* SSL *P2: Mechanism:* VPN
	Communication Integrity *Implement:* yes (default) *Mechanism:* MD5 Hash
	Secure Logging *What:* order transactions *Mechanism:* 3DES encrypt *What:* user input *Mechanism:* 3DES encrypt
	Access Control *User Role:* Secretary *Resource:* scheduling module *Resource:* admin module *User Role:* President *Resource:* admin module *Resource:* salary module

In Table 1, the top shaded portion is the policy header. The header contains the following administrative fields: *policy use* identifies for which mi-service the policy is provided, *owner* identifies the name of the provider of the mi-service, and *valid* specifies the end date after which the policy is no longer valid. The *valid* field can also specify "initial" or "continuing" to indicate that the security policy is enforced only initially or continuously. The table also shows that some security services can have alternative

mechanisms (e.g. consumer authentication using password or biometrics). These alternatives are prefixed by "Pn", where n is a number. The Pn are used by the context-aware security policy agent to select the associated mechanism for any particular invocation of the service. Further, secure logging and access control can have additional items (e.g. secure logging can log additional information and access control can have additional resources under each role). (Note: V+F biometrics refers to voice and fingerprint, IIT-ISG (Institute for Information Technology, Information Security Group) refers to a mechanism we are developing in our group.)

The security policy in Table 1 serves as the provider's security policy for a particular mi-service that the provider offers to consumers. It also reflects the consumer's security policy for the mi-service, since it contains provisions that the consumer agrees to follow. Upon locating the mi-service on the mobile Internet and prior to activating the service, the consumer examines the provider's security policy (Table 1) for the service comparing it to her own security preferences. If the consumer agrees with the provider's policy, the consumer can engage the mi-service. Otherwise, the consumer negotiates the security policy with the provider (Yee and Korba, 2005). If this negotiation is successful, the mi-service can start. Otherwise, the consumer needs to find a similar mi-service from a different provider (or find ways to match the security requirements of the present mi-service but it is probably easier to just find another mi-service), and repeat this process again. The security policy resulting from negotiation would be similar to Table 1, possibly with some security services not listed, and possibly with different alternative mechanisms or additional items for secure logging and access control.

3. CONTEXT-AWARE SECURITY POLICY AGENT

A context-aware security policy agent (CASPA) is an intelligent software agent that resides in a mobile device and is responsible for selecting security services and mechanisms from the provider's security policy for a particular mi-service, according to the values of UPL. The behaviour of a CASPA is described by the state machine in Figure 3, where the arrow labels are in the form "condition / action".

In Figure 3, the *Idle* state is exited once the service is ready to begin (i.e. the service has been found and the security policy agreed to between consumer and provider).

In the *Initialization* state, the CASPA accounts for the U and P of UPL (i.e. reflects the user's security preferences and the computational power of the device) by setting the options in the provider's security policy to implement appropriate security services and mechanisms (see Table 1). For

example, suppose the consumer has several mobile devices that she uses with the same security policy, including a PDA and a less powerful cell phone. CASPA would set security services and mechanisms that both reflect the consumer's security preferences and be appropriate to the computing power of each device. It would be straight forward to program a CASPA to perform this task.

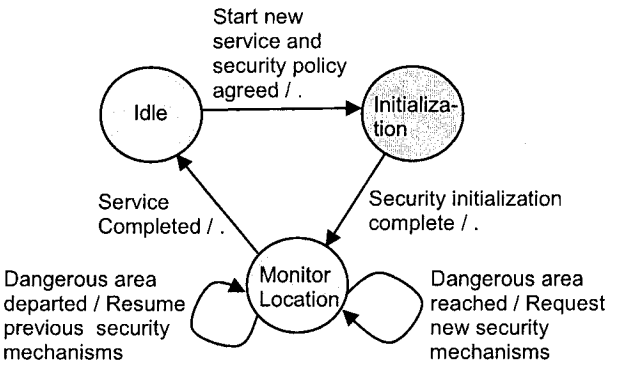

Figure 3. Behaviour of context-aware security policy agent

In the *Monitor Location* state, the agent is monitoring the device's location using GPS. Note that this location is only used by the CASPA and is not reported to either the mobile ISP or the provider of the service so that there should be no privacy concerns (more on this in Section 4). An alternative way of determining the consumer's location is the use of signaling analysis by the mobile ISP. However, the latter would then learn the consumer's location leading to privacy concerns. When a dangerous area (i.e. an area with a high number of attackers) is entered, the agent messages the service provider to initiate a more powerful security mechanism for communication to defend against the attackers (Section 4 discusses how this dangerous area can be known). Of course, this more powerful mechanism consumes more computing resources and should only be used when necessary. When the dangerous area is exited, the agent messages the provider that the normal security mechanism for communication may be resumed. The CASPA executes concurrently with the mi-service. However, the mi-service does not begin until the CASPA has completed the initialization.

The CASPA communicates with the provider during *Initialization* and *Monitor Location* using the following secure protocol:

1. $C \rightarrow P$: Sig_C *(M, nonce)*
2. $P \rightarrow C$: Sig_P *(nonce-1)*

where C is the consumer, P is the provider, Sig_C is the consumer's digital signature, Sig_P is the provider's digital signature, M is the message, and the

nonce is used to prevent replay attacks and as a confirmation of receipt by the provider.

For *Initialization*, the message *M* has the form:

M = [INIT, security component 1, security component 2, ..., security component k],

where *security component j = security service j,* if this security service has no alternative security mechanisms, or *security component j = (security service j, mechanism idj),* if it has alternative mechanisms and *mechanism idj* is the mechanism the user wants.

For Monitor Location, upon entering the dangerous area, the message *M* has the form:

M = [NEW, (security service 1, mechanism id1), (security service 2, mechanism id2), ..., (security service m, mechanism idm)]

which sets the new mechanism of each security service that the consumer wants to implement for the dangerous area, for appropriate security services having alternative mechanisms. As we have alluded to above, in most cases the only security services of concern would be communication confidentiality and integrity. Upon exiting the dangerous area, the message M is: *M = [REVERT]* which tells the provider to revert to the previous mechanisms.

4. OPERATIONAL REQUIREMENTS AND DISCUSSION

The CASPA would need to know the user's security preferences, including the preferences for P and L from UPL, in order to formulate the messages *M.* These could be input via a UI for the CASPA. This information can be provided by the consumer once before any mi-services are used, and then verified with the agreed-to security policy for each service. The security preferences in *M* have to be realizable within the agreed-to security policy. In addition, the agreed-to security policies need to be expressed in a machine processable language such as XACML (eXtensible Access Control Markup Language) (OASIS, n.d.).

The provider needs to have software to receive the messages from the CASPA and apply them to the mi-service's security policy. This software could take the form of an agent as well, a counterpart to CASPA that acts on behalf of the provider.

In the *Monitor Location* state, an appropriate UI would be needed to interrupt the service temporarily while one or more security mechanisms are changed. This interruption occurs twice – once for entering the dangerous area and once for departing the dangerous area. Further, these changeovers need to occur quickly, in order not to annoy the user and to prevent any

openings for attack. Dangerous areas may be determined as a result of feedback to a government website by users who have been attacked. The CASPA can periodically and automatically check this website for the latest dangerous areas.

The location obtained using GPS is only used by the CASPA and not reported to the providers which should not lead to privacy concerns. However, the dangerous areas are known to the service provider as well. The latter may infer the location of the consumer when the CASPA signals for higher security. We assume that this small breach of privacy is acceptable to the consumer in return for greater security, since the consumer's location may not be pinpointed exactly due to the possibility of more than one dangerous area and the fact that the consumer may enter a dangerous area at many different locations.

Our use of digital signatures and nonces implies that the mobile device needs at least the capability to process a digital signature and generate random numbers. In addition, there would need to be a key distribution technique, as well as the capability for the device to securely store a private key. However, these are minimal capabilities required to implement security services. Further, we require the mobile device to have a GPS capability, which is becoming more and more common. These requirements imply that the mobile device should probably have the computing power of a PDA. However, less powerful devices would be accommodated by the CASPA where possible.

We note that since the security policy is executed by the provider of the mi-service, the mi-service consumer can transparently use different mobile ISP's as she roams with her mobile device.

5. CONCLUSIONS AND FUTURE RESEARCH

We have presented a proposal for the use of a context-aware security policy agent to customize the security services for a mi-service to the consumer's preferences. In addition, this customization allows accounting for the mobile device's available computing power and the consumer's movement into a dangerous area with a higher number of attackers, where more powerful security mechanisms are needed. The use of a CASPA is a form of service personalization that studies have shown is attractive to consumers (Ho and Kwok, 2003). For future research, we would like to prototype the CASPA to study performance characteristics and refine our approach. Another area of interest is to develop a technique that would automatically and accurately determine the nature and extent of dangerous areas in a mobile network.

References

Chae, M. and Kim, J. (December 2003), What's So Different About the Mobile Internet?, *Communications of the ACM*, Vol. 46, No. 12.

Dinsmore, P. et al, 2000, Policy-Based Security Management for Large Dynamic Groups: An Overview of the DCCM Project, proceedings, *DARPA Information Survivability Conference and Exposition, 2000 (DISCEX'00)*, Vol. 1, pp. 64-73.

Duflos, S., 2002, An Architecture for Policy-Based Security Management for Distributed Multimedia Services, proceedings, *Multimedia '02*, Juan-les-Pins, France.

Ghosh, A.K. and Swaminatha, T.M. (February 2001), Software Security and Privacy Risks in Mobile E-Commerce, *Communications of the ACM*, Vol. 44, No. 2, pp. 51-57.

Ho, S.Y. and Kwok, S.H. (January 2003), The Attraction of Personalized Service for Users in Mobile Commerce: An Empirical Study, *ACM SIGecom Exchanges*, Vol. 3, No. 4, pp. 10-18.

International Organization for Standardization, ISO 7498-2, Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture; http://www.iso.org/

International Telecommunication Union Telecommunication Standardization Sector (ITU-T), Recommendation X.800, Security Architecture for OSI; http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-X.800-199103-I

Josang, A. and Sanderud, G., 2003, Security in Mobile Communications: Challenges and Opportunities. Australasian Information Security Workshop (AISW2003), *Conferences in Research and Practice in Information Technology*, Vol. 21, C. Johnson, P. Montague and C. Steketee, Eds.

Joshi, J. et al (February 2001), Security Models for Web-Based Applications, *Communications of the ACM*, Vol. 44, No. 2, pp. 38-44.

Mallat, N., Rossi, M., and Tuunainen, V.K. (May 2004), Mobile Banking Services, *Communications of the ACM*, Vol. 47, No. 5, pp. 42-46.

OASIS, eXtensible Access Control Markup Language; http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Varadharajan, V., 1990, A Multilevel Security Policy Model for Networks, proceedings, *Ninth Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM 90)*, Vol. 2, pp. 710-718.

Ventuneac, M., Coffey, T., Salomie, I., 2003, A Policy-Based Security Framework for Web-Enabled Applications, proceedings, *1st International Symposium on Information and Communication Technologies*, pp. 487-492, Dublin, Ireland.

Yee, G. and Korba, L., 2005, Negotiated Security Policies for E-Services and Web Services, proceedings of the *2005 IEEE International Conference on Web Services (ICWS 2005)*, San Diego, California.

---

[1] NRC Paper Number: NRC 48236