Improved Approach on Modeling and Reasoning about PKI/WPKI

Mingde ZHANG [1], Xuefeng ZHENG [1], Shuwang LV [2], Yike YU [1]
1. School of Information Engineering, University of Science and Technology Beijing, Beijing, China
2. State Key Laboratory of Information Security, Beijing, China
rickchina@263.net

***Abstract*—In order to describe PKI/WPKI trust models with greater precision, a predicate-based improved approach on modeling and reasoning about PKI/WPKI is proposed. By analyzing new practices such as certificate-type, certificate and organization of CA, security-risks of key-holder, web-based trust model and WAP-based trust model, six predicates are defined, nine inference rules are deduced and a four-step reasoning method is presented. This approach takes into account authenticity of private-key, recommendation for certificate-type and certificate, trust anchor, and security of entity and certificate-type, thus being applicable to a variety of trust models. Two examples for reasoning web-based and WAP-based trust models are given to demonstrate how to use this approach.**

Keywords-PKI; WPKI; Inference Rule; Reasoning Method; Trust Model

I. INTRODUCTION

In open networks, it is a prerequisite for successful e-transactions that how to establish trust relationships between participants who are unfamiliar or distrust each other. PKI and WPKI are good solutions to the above problem of establishing trust relationships in wireless environments (e.g. notebook PC and mobile phone using WLAN, Bluetooth, GPRS, and 3G). WPKI has mainly optimized PKI protocols, certificate format as well as cryptographic algorithms and keys; hence there are no differences between modeling PKI and modeling WPKI [1].

For the sake of accurately modeling and reasoning about PKI/WPKI, many models and methods have been proposed. For the first time, Maurer proposed an approach for modeling and reasoning about PKI from users' point of view by defining four predicates; this model takes into account recommendations for the trustworthiness of entities [2]. Based on similar logic, two approaches presented by Bakkali and Kaitouni could consider PKI trust model from a global view, by taking into account constraints concerning certificate policies, certification practices and certification path length; this approach abandoned recommendation mechanism [3][4]. LIU Hailong inherited four predicates proposed by Maurer; he distinguished the difference of entities and CAs, and introduced two restriction conditions such as certification path length and certificate policies [5]. XIE Hongbo proposed a conditional predicate logic and probabilistic model; this model still used three predicates except "recommendation", but added trust extension rule to transfer trust [6]. HU Yingsong improved the two approaches provided by Bakkali and Kaitouni by simplifying representing method of restriction conditions [7]. However, all the above research ignored security-risks which influence trustworthiness of key-holder and recommendation for certificate, thus resulting in hardly being applicable to new PKI practices such as certificate-type [8], web-based trust model [9] and WAP-based trust model [10][11].

In order to describe PKI/WPKI trust model with greater precision and avoid limitations of the above models and methods, a predicate-based improved approach on modeling and reasoning about PKI/WPKI is proposed. Comparing with the existing work, this approach takes into account authenticity of private-key, recommendation for certificate-type and certificate, trust anchor, and security of entity and certificate-type, thus improving the accuracy and objectivity of modeling and reasoning about PKI/WPKI. Two examples are also given to demonstrate how to use this approach.

The rest of this paper is organized as follows. In Section II, an improved approach on modeling and reasoning about PKI/WPKI is proposed, including six predicates definition, nine inference rules and four-step reasoning method. Section III gives two examples to demonstrate how to use this approach. Finally, concluding remarks are made in Section IV.

II. MODELING AND REASONING FOR PKI/WPKI

A. Symbols and Signs

Symbols used in this paper are defined as follows:

e: a PKI/WPKI entity. It is divided into 3 categories: CA, KH (Key-Holder), RP (Relying-Party) [12]. CA only signs certificate for KH. RA, Repository, CRL Issuer and PKI Portal could be regarded parts of CA [13] [10].

ca: a CA. It is one PKI /WPKI entity.

kh: a KH or a certificate-holder. It is one PKI/WPKI entity. In this document, the terms, "key-holder" and "certificate-holder" are used interchangeably.

rp: a RP. It is one PKI/WPKI entity.

rca: a root CA.

bca: a bridge CA.

ct: a CT (Certificate-Type).

c: a X.509 certificate.

c(e): the certificate whose subject is the entity "e".

978-1-4244-3709-2/10/$25.00 ©2010 IEEE

c(e|ca): the certificate whose subject is the entity "e" and this certificate is signed by the entity "ca". When e is a CA, the certificate is called cross-certification or sub-CA certificate.

c(e@ct): the certificate whose subject is the entity "e" and this certificate belongs to the Certificate-Type "ct".

ct(c): the Certificate-Type that the certificate "c" belongs to.

k: a key.

k(e): the key alleged by the entity "e".

pk(e): the public-key alleged by the entity "e". In this document, pk(e) and c(e) are used interchangeably.

vk(e): the private-key alleged by the entity "e".

vk(c(e)): the private-key that is corresponding with the public-key in c(e).

B. Analyzing new practices

1、CT (Certificate-Type) [8]

In order to adapt to complex applications, most CAs define several CTs such as personal-certificate, organization-certificate, browser-certificate, web-certificate.

Different CT has different security policies and certificate policies, thus resulting in different security-risks, e.g. KH's private-key might be cracked or stolen, or KH's certificate might be signed with unconscious error, etc. So, KH's trustworthiness would be influenced by security-risks of its CT.

2、Certificate and Organization of CA [8]

CA includes its own certificate and its organization (includes devices, systems, people and etc.). In some applications, RP may know about both, however, in others, RP may know about only either or none. Actually only CA's certificate is called trust anchor.

CA's organization has many security-risks, e.g. CA's private-key might be cracked or stolen, or KH's certificates might be signed without complying with rules, etc. So, KH's trustworthiness would be influenced by security-risks of its CA.

3、Security-risks of KH [8]

KH includes person and device (e.g. notebook PC, mobile phone) used by person.

KH has many security-risks, e.g., KH's private-key might be hijacked, or KH might leak its private-key, etc. So, KH's trustworthiness would be influenced by its own security-risks.

4、Web-based trust model [9]

In this trust model, some CAs' certificates are preinstalled in a standard browser in notebook PCs. Most RPs might know none about certificates and organizations of these CAs, and only trust the browser software and its developer.

When needed, as an agent of RP, the browser would automatically perform to verify if KH's certificate is valid and display the result to RP.

5、WAP-based trust model [10][11]

In this trust model, some CAs' certificates are preinstalled in a standard browser in mobile phones. Most RPs might know none about certificates and organizations of these CAs, and only trust the browser software and its developer. Most RPs also knows none about WAP-Gateway.

When needed, as an agent of RP, the browser and WAP-Gateway would automatically perform to verify if KH's certificate is valid and display the result to RP.

C. Predicates definition

The four predicates proposed by Ueli Maurer are: Authenticity of public key, Trust, Certificate and Recommendations. [2]

Based on the above analysis of new practices, this paper inherits and extends the work of Ueli Maurer by redefining these four predicates and adding two new predicates.

Definition 1: Six Predicates are defined as follows:

(1). Authenticity of Key.

Auth(rp, k(e)) denotes rp's belief that the key k(e) alleged by entity e is authentic. The k(e) can be vk(e), pk(e), or c(e).

(2). Trust in entity.

Trust(rp, e) denotes rp's belief that entity e is trustworthy or that e will behave exactly as rp expects.

(3). Certificate.

Cert(ca, c(e@ct)) denotes the fact that the certificate c(e) is issued and signed by entity ca according to the related policies of ct. The entity e can be ca or kh.

(4). Recommendation for entity, certificate or certificate-type.

Rec(e1, e) denotes that entity e1 issues a recommendation that entity e is secure. The entity e can be ca or kh.

Rec(e1, c) denotes that entity e1 issues a recommendation that certificate c is authentic.

Rec(e1, ct) denotes that entity e1 issues a recommendation that certificate-type ct is secure.

(5). Anchor of Trust.

Anch(rp, c(ca)) denotes that rp regards c(ca) as a trust anchor.

(6). Security of entity or certificate-type.

Sec(rp, e) denotes rp's belief that entity e is secure. The entity e can be ca or kh.

Sec(rp, ct) denotes rp's belief that certificate-type ct is secure.

D. Inference rules

According to Definition 1, nine inference rules can be deduced.

Rule 1: Trust-Anchor Rule

$$Anch(rp,c) \Rightarrow Auth(rp,c)$$

Rule 2: Authenticity Rule for Certificate

$$Auth(rp,c(ca)), Cert(ca,c(e@ct)), Sec(rp,ca), Sec(rp,ct) \\ \Rightarrow Auth(rp,c(e \mid ca@ct))$$

Rule 3: Authenticity Rule for Private-Key

$$Auth(rp,c(e)) \Rightarrow Auth(rp,vk(c(e)))$$

Base on reasonable authentication protocols, rp can verifies if the signature to specified data by vk(c(e)) is true using c(e).

Rule 4: Recommendation Rule for Entity

$$Trust(rp,e1), \mathrm{Re}\,c(e1,e2) \Rightarrow Sec(rp,e2)$$

Rule 5: Recommendation Rule for Certificate-Type

$$Trust(rp,e1), \mathrm{Re}\,c(e1,ct) \Rightarrow Sec(rp,ct)$$

Rule 6: Recommendation Rule for Certificate

$$Trust(rp,e1), \mathrm{Re}\,c(e1,c) \Rightarrow Auth(rp,c)$$

Rule 7: To-Trust Rule

$$Auth(rp,vk(c(e))), Sec(rp,e) \Rightarrow Trust(rp,e)$$

Rule 8: From-Trust Rule

$$Trust(rp,e) \Rightarrow Auth(rp,c(e)), Sec(rp,e)$$

Rule 9: Certificate Rule

$$Cert(ca,c(e@ct)) \Rightarrow Auth(ca,c(e)), Auth(e,c(ca)) \\ ,Sec(e,ca), Sec(e,ct)$$

E. Reasoning method

Based on the above six predicates and nine inference rules, this paper presents a four-step reasoning method.

Definition 2: Four-step reasoning method is defined as follows:

(1). to write down all initial formulas according to trust model.

(2). to find out all possible hypotheses.

(3). to specify objectives to obtain.

(4). to begin reasoning from initial formulas and hypotheses using the above nine inference rules. If objectives could not be reached, need to add new hypotheses or initial formulas.

III. Application to PKI/WPKI trust model

A. Web-based trust model

As shown in Figure 1 for web-based trust model, suppose that web is a KH, vca (verisign CA) signs the certificate c(web|vca@ct) for web, rp visits web using IE developed by ms (Microsoft), and c(vca) is preinstalled in IE.

Initial formulas: $Cert(vca,c(web@ct))$.

Hypotheses: $Trust(rp,ms)$, $Trust(rp,IE)$, $\mathrm{Re}\,c(ms,vca)$, $\mathrm{Re}\,c(IE,c(vca))$, $\mathrm{Re}\,c(vca,ct)$, $\mathrm{Re}\,c(vca,web)$.

Objectives to obtain: $Trust(rp,web)$.

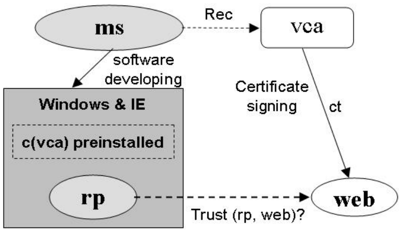

Figure 1. Web-based trust model

Reasoning process:

(1). Rule 4: $Trust(rp,ms), \mathrm{Re}\,c(ms,vca) \Rightarrow Sec(rp,vca)$

(2). Rule 6: $Trust(rp,IE), \mathrm{Re}\,c(IE,c(vca)) \Rightarrow Auth(rp,c(vca))$

(3). Rule 3: $Auth(rp,c(vca)) \Rightarrow Auth(rp,vk(c(vca)))$

(4). Rule 7: $Auth(rp,vk(c(vca))), Sec(rp,vca) \Rightarrow Trust(rp,vca)$

(5). Rule 5: $Trust(rp,vca), \mathrm{Re}\,c(vca,ct) \Rightarrow Sec(rp,ct)$

(6). Rule 4: $Trust(rp,vca), \mathrm{Re}\,c(vca,web) \Rightarrow Sec(rp,web)$

(7). Rule 2: $Auth(rp,c(vca)), Cert(vca,c(web@ct)), Sec(rp,vca), Sec(rp,ct) \Rightarrow Auth(rp,c(web \mid vca@ct))$

(8). Rule 3: $Auth(rp,c(web \mid vca@ct)) \Rightarrow Auth(rp,vk(c(web \mid vca@ct)))$

(9). Rule 7: $Auth(rp,vk(c(web \mid vca@ct))), Sec(rp,web) \Rightarrow Trust(rp,web)$

B. WAP-based trust model

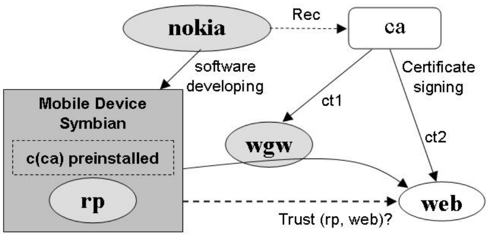

Figure 2. WAP-based trust model

As shown in Figure 2 for WAP-based trust model, suppose that web is a KH, ca signs certificates c(wgw |ca@ct1) for WAP-Gateway and c(web|ca@ct2) for web respectively, rp visits web using symbian developed by nokia, and c(ca) is preinstalled within symbian.

Initial formulas: $Cert(ca,c(wgw@ct1))$, $Cert(ca,c(web@ct2))$, $Anch(wgw,c(ca))$.

Hypotheses: $Trust(rp,nokia)$, $Trust(rp,symbian)$, $\mathrm{Re}c(nokia,ca)$, $\mathrm{Re}c(symbian,c(ca))$, $\mathrm{Re}c(ca,ct1)$, $\mathrm{Re}c(ca,ct2)$, $\mathrm{Re}c(ca,wgw)$, $\mathrm{Re}c(ca,web)$.

Objectives to obtain:

$Trust(rp,wgw)$, $Trust(wgw,web)$, $Trust(rp,web)$.

Reasoning process:

(1). Rule 4: $Trust(rp,nokia),\mathrm{Re}c(nokia,ca)\Rightarrow Sec(rp,ca)$

(2). Rule 6:

$Trust(rp,symbian),\mathrm{Re}c(symbian,c(ca))\Rightarrow Auth(rp,c(ca))$

(3). Rule 3: $Auth(rp,c(ca))\Rightarrow Auth(rp,vk(c(ca)))$

(4). Rule 7: $Auth(rp,vk(c(ca))),Sec(rp,ca)$
$\Rightarrow Trust(rp,ca)$

(5). Rule 5: $Trust(rp,ca),\mathrm{Re}c(ca,ct1)\Rightarrow Sec(rp,ct1)$

(6). Rule 4: $Trust(rp,ca),\mathrm{Re}c(ca,wgw)\Rightarrow Sec(rp,wgw)$

(7). Rule 2: $Auth(rp,c(ca)),Cert(ca,c(wgw@ct1)),$
$Sec(rp,ca),Sec(rp,ct1)$
$\Rightarrow Auth(rp,c(wgw\,|\,ca@ct1))$

(8). Rule 3: $Auth(rp,c(wgw\,|\,ca@ct1))$
$\Rightarrow Auth(rp,vk(c(wgw\,|\,ca@ct1)))$

(9). Rule 7: $Auth(rp,vk(c(wgw\,|\,ca@ct1))),Sec(rp,wgw)$
$\Rightarrow Trust(rp,wgw)$

(10). Rule 1: $Anch(wgw,c(ca))\Rightarrow Auth(wgw,c(ca))$

(11). Rule 3: $Auth(wgw,c(ca))\Rightarrow Auth(wgw,vk(c(ca)))$

(12). Rule 9: $Cert(ca,c(wgw@ct1))\Rightarrow Sec(wgw,ca)$

(13). Rule 7: $Auth(wgw,vk(c(ca))),Sec(wgw,ca)$
$\Rightarrow Trust(wgw,ca)$

(14). Rule 5: $Trust(wgw,ca),\mathrm{Re}c(ca,ct2)\Rightarrow Sec(wgw,ct2)$

(15). Rule 4: $Trust(wgw,ca),\mathrm{Re}c(ca,web)\Rightarrow Sec(wgw,web)$

(16). Rule 2: $Auth(wgw,c(ca)),Cert(ca,c(web@ct2)),$
$Sec(wgw,ca),Sec(wgw,ct2)$
$\Rightarrow Auth(wgw,c(web\,|\,ca@ct2))$

(17). Rule 3: $Auth(wgw,c(web\,|\,ca@ct2))$
$\Rightarrow Auth(wgw,vk(c(web\,|\,ca@ct2)))$

(18). Rule 7:

$Auth(wgw,vk(c(web\,|\,ca@ct2))),Sec(wgw,web)$
$\Rightarrow Trust(wgw,web)$

(19). Rule 5: $Trust(rp,ca),rec(ca,ct2)\Rightarrow Sec(rp,ct2)$

(20). Rule 4: $Trust(rp,ca),rec(ca,web)\Rightarrow Sec(rp,web)$

(21). Rule 2: $Auth(rp,c(ca)),Cert(ca,c(web@ct2)),$
$Sec(rp,ca),Sec(rp,ct2)$
$\Rightarrow Auth(rp,c(web\,|\,ca@ct2))$

(22). Rule 3: $Auth(rp,c(web\,|\,ca@ct2))$
$\Rightarrow Auth(rp,vk(c(web\,|\,ca@ct2)))$

(23). Rule 7: $Auth(rp,vk(c(web\,|\,ca@ct2))),Sec(rp,web)$
$\Rightarrow Trust(rp,web)$

IV. Conclusion

Because the existing work are hardly applicable to new practices such as certificate-type, web-based trust model and WAP-based trust model, a predicate-based improved approach on modeling and reasoning about PKI/WPKI is proposed. This approach takes into account authenticity of private-key, recommendation for certificate-type and certificate, trust anchor, and security of entity and certificate-type, thus improving the accuracy of describing PKI/WPKI and being applicable to a variety of trust models.

References

[1] Chan Yeob Yeun, and Tim Farnham, “Secure M-Commerce with WPKI”, proceedings of 1st International Workshop for Asian PKI, October 2001, Korea.

[2] Ueli Maurer, “Modelling a Public-Key Infrastructure”, Proc. 1996 European Symposium on Research in Computer Security (ESORICS' 96), E. Bertino (Ed.), Lecture Notes in Computer Science, Berlin: Springer-Verlag, 1996, vol. 1146: 325-350

[3] Hanane El Bakkali, Bahia Idrissi Kaitouni, "A Logic-based Reasoning About PKI Trust Model", Sixth IEEE Symposium on Computers and Communications, 2001: 42-48

[4] Hanane El Bakkali, Bahia Idrissi Kaitouni, "A Predicate Calculus Logic for the PKI Trust Model Analysis", IEEE International Symposium on Network Computing and Applications, 2001: 368-371

[5] LIU Hailong, ZHANG Qishan, WU junpei, "A conditional predicate calculus logic for PKI trust model analysis", Journal of China Institite of Communications, November 2002, vol. 23, no. 11: 14-20

[6] XIE Hongbo, ZHOU Mingtian, "PKI Trust Model Analysis Based on Probabilistic Model and Conditional Predicate Calculus Logic", Mini-Micro Systems, January 2006, vol. 27, no. 1: 69-71

[7] HU Yingsong, GAO Gongying, "An Improved Approach to the Logical Inference on the PKI Trust Model", Computer Engineering and Science, 2007, vol. 29, no. 8: 7-10

[8] Mingde Zhang, Xuefeng Zheng, etc., "Research on Model of Trust Degrees for PKI", ias, vol. 2, pp.647-650, 2009 Fifth International Conference on Information Assurance and Security, 2009

[9] Carlisle Adams, Steve Lloyd, "Understanding PKI - Concepts, Standards, and Deployment Considerations" (Second Edition), Boston, MA, Pearson Education Inc., October 2002: 139-142

[10] "Wireless Application Protocol Public Key Infrastructure Definition", WAP Forum, April 24, 2001

[11] "wPKI Specification", E3P Work Group, May 9, 2007

[12] M. Shimaoka, Ed., N. Hastings, R. Nielsen, "Memorandum for Multi-Domain Public Key Infrastructure Interoperability", RFC 5217, IETF, July 2008

[13] Shashi Kiran, Patricia Lareau, Steve Lloyd, "PKI Basics – A Technical Perspective", PKI Forum’s Business Working Group (BWG), November 2002