COVER FEATURE

Parasitic Authentication To Protect Your E-Wallet

How can an e-wallet, a handheld computer that consolidates a user's personal items, stores vital information, and facilitates financial transactions, guarantee security without being cumbersome? Parasitic authentication offers handheld computers security without reducing convenience.

Tim Ebringer
Peter Thorne
U e f
Me b e

Yuliang Zheng
Monash University

Tee ec c ae (e- a e) a ece ed c ae ae. I e c - da e a f ee a ca ed a db e de d da: a e, e, age, da , a d e. I fac, N a' 9001 C ca a ead c b e e e, age, a dd a e.

Te e a e, ee, f de e a e ca. Tad a ec ec a e e e ee a PIN a d e e e e f a a ac. M e ca ed ec , e c de gab e c de ce, c a a ge ca e, c eg a ed ee- a e. B f ee a ed ad a age. U ab b de a e ca a ea g ca ba- e ead fe- a e.

I a ce, e ee e e e fe- g c ee b ac cea abe, ee, a d abe de ce ca a ac a a a e ca- f e e. Tee- a e e bec e a a e feed g ff e a de ce f e ed a e ca a d de ca f a .

E-PURSES AND AN E-ID?

Te ad a a e de f a f c f e e: I d de ca f a c a a d e' ce e, fac a e d ca e (ca a d c e d), a d ac a a e f a e c a b c e.

Te e e d b ac g e g ee ed c - g a c c ca ef c e f e e a - e - e f c , b ca e e add a e? I deed, e- a e a d a -ca d de e e face a da g d e c c g c e ad a ee c e.

F ec e' f e, ece ca d a e e a ac ea a e ec a . I ega d c , e e ec a e a a d ed a ac a a de, a ac g e e e ec e. Ca a g e- abe a e a a ed f ce e. H ca ee- a ec e?

The verification problem

U e ec e ec a e e a ef f g e- a e.[1] T a e, ed f- c ac e e. Te b e e e e ef e d f *identification protocol* e- a e bef e eac a ac . Tad a, e e d ge ece c a a a d PIN. M ece a a e ed b e c.

Passwords and PINs

Ne e a d PIN a ea dea : N a e ea a e ca ea e, e a ea fe e ed.[2,3] F e a e, ba e e e e e ea da e PIN ce a ATM e ad a e e a ca ed e be. We e ac ed ef - e e d f /usr/dict/words f e, ec ded a PIN acc d g e e ad ac ec a ATM, a d e a ed d ca e. F 25,486 d, e e ac ed 2,207 f - e e d, c ed ced 1,411 d ffe e PIN. S e ace ded be g ab 15 ece f g a e.

0018-9162/00/$10.00 © 2000 IEEE

T d fec fa , ee e
ea e e ca ec e e , dec
f ab a ec f PIN a e ca
e . F a ec a dad c a ITSEC a e
c ae f ed. F e a e, a
c f ga PIN p ec f a p ∈R Z:
0000 ≤ p ≤ 9999, ee a a be e
ad e PIN e ec . R A de
a ed a e fa e f a ea- dc
e e f d f a.[4]

B PIN a d a d ffe f e fac a a
ace a ea e ece b be a . B e-
a e b gge be PIN a d a d
a e e e a a, abe de ce a-
ad. O a da , , a e g a
fe fa e e b a ga PIN a a de ce
a d ef -c c ede- a e -
e g a dde, efe d a ea g eg a-
g T fa e a g d ec ec e
f e c ad a a e g ee g be .

Biometrics

A e effec e e d g be eg a ea b-
e ca e ca de ce, c a a ge ca-
e, ee- a e. T ee- a e d ef
a a ac e a a d ge ca ed.

S c a ce e a e ec c ce . F ,
a ca eda dde e eda ac e c db a
e ge ca e. O ce e fec ed, edge f
e b a ec e d ead ace c-
e da g eed. A a e a e, e S
P a a a e g eed a ga e
c d bed ca ed, e e ce a e de a a-
abe df e g a a d a e a acce
a ed ga e. A , e a d, -
be e a a fab e cf e ca -
e beca e a ca ed b e c age a a
be g dffe e. Sec d, a d e a e -
a , e fee c f abe g ab e c
e g a a e e ace e,
e ca a a abec e. Ma e fee
a a efc d ea e de a d a e-
ade a e e e ca f e e ce e e
a e ea b e c.

PARASITIC AUTHENTICATION

W a a ca e ca , e ca a-
de ega e e e b f a g a a-
ac a a, abe ec da de ce, ca ed
a dc cea ed b e e. A ga ee- a e ca
c ca e e ec da de ce a d e f
a deed e *same* ec da de ce a a
ed e e ce , ee- a e ac a f
a e ece a a a c eea a-
ac . T , e *continued proximity* f e ec-
da de ce e e- a e e ce f
a e ca . E g de f ca -
c e e a ec da de ce a d
be g e e f ee- a e ca c-
f e f ee- a e. T a ac -
ce a e fa a c e e :
sessional authentication.

Sessional authentication

I a da aba e, a ac a ea c: E e
a e e a a ac a e e ec ed
e e da aba e, ea e. I c -
a , b fea be a d ece a
a e ca ee e a ac . C e e, e
a e e e da a a ac e e a, e e
e ec e a a ac ; e a e-
ca g e e e e d be ab d a d
ec e b e f a d. T e -
e a e e a e e e g e a e
e e e e e e e e ec e
g . T e a e ca a f a e , a d
e e dec de e e g f e e .

We e a ac a aba f a e abe
e f a g e- a e- ba ed a ac .
T e a e a e ee- a e a da ec-
da de ce, a g ee- a e c e e
a ac d g e e . T e f e
ec da de ce ee- a e a e e .
A e c de d e e a a . T ee- a e
c de d e e efafe ace a e e d
e a ed. A e a e a , ee- a e g e d e e-
afe ace a a f e a e ,
e eb ca g e be e. A e
e g bef e e d e e b g a
a c b . B a , e e e d
e ee- a e a d ec da de ce ca c-
ca e beca e f ca e a a be d e
c ca a g e. C g ec e a e
a e d e e be e ec e e e
e e a *both* ee- a e a d e ec da de ce
a e a e b dec ea e ab ce
e e e be g a e e e ee- a e.

Expected economic and security benefits

Pa a ca e ca ffe a be e :
ab a d ec .

Usability. T e e g e a e e a a d
PIN e f a e d f e ac e ec-
ced e a e e ac a ac . O ce
e e a e e e , e ec da de ce
a d e e e ac e ec ced e e
e' be a f.

Security. T e e d e a e e ab e-
c e ec ed a ga f ee- a e. T
c e ec , e e e *both* ee-
a e a d e ec da de ce a e . If e
c a ce f g e- a e a e *p*, g e a e

With parasitic authentication, users can temporarily delegate their responsibility for authorizing a transaction to a small, portable secondary device, carried and concealed by the user.

The idea of parasitic authentication is partly an evolution of ordinary wireless authentication.

ec da de ce a a d c ce a ab e a d
ded e be eca a e a e, e
c a ce f g e ec da de ce d
be q, e e $q < p$. We a g e a $q < p$ beca e
e ec da de ce eed be a d ed
d ced f ed a f e e (c
e be a da), a d d be a a
f a a e e a ea g ec ace
a ed f ee e da. If e e
eca a e a e, ec a ce f g b
ee- a e a d e ec da de ce a e
d be c de ab e.

Secondary device characteristics

T e b e e a e f d g ac e-
e, fa, b e a d ec e e d f e f g
entity identification. E de ca ec e
ca be d ded ee a ca e g e, de e d g
e e e ec ba ed e e g ,
e g e ed, e g ee. Ide -
ca ea e ba ed e g , c a
a d PIN, a e d f c f e e e e-
be a d c be e e e. Mea e ba ed e-
g ee, c a ge, a e e a d
be e e. T ea e c
ba ed e g e ed. I effec, e a e
e c a g e g f e g e ed.
T e e- a e bec e a a a e e a -
de feed g ff f de f ca. I fac, e
a e ca de ce ca be e e a
d ffe e a a e. We e a a g e f -
g ca c a ace c.

Miniature. T ea e ca de ce be a
e g be b e a d dde e e e
e e' a a e.

Self-powered. T ea e ca de ce ca
e g e, be a be d a e f a
e e g ee c f e d, a ca f c f
e e ded e d f ea a f a e ce.
I ece ea, ba e ec g a ad a ced
e a ab, a e de ced b ee e ded ba e fe
f b e e.

Disposable. L f ea e ca de ce d
be a a caa e. A , a e
f *both* ee- a e a d ea e ca de ce
d ea a a d f e c a e'
e- a e a e abe ab e. N f a a
a a ace g de e ef d be
e a e ca de ce. C ea, d a be
g ad a a ge f ea e ca de ce
be e e e.

Wireless. T ee ea e ca de ce dde
a d c e e ce e e, c ca e
e e.

We a e e de c bed e a e ca
de ce' c a a ab e beca e e e a ece-
a e g ee g ade- ff de g. A e de ce'
c a a e c e a e, ca e f
c ea g ca ed de f ca e.
H e e, a bec e ec e, eed e
e, a d c e d g bec e e ab e a d
e f e d. Rea ca, e ea c a e e
a e ca de ce a e g c a a
e a f e a de g a, be d c
add a c e d e ff e g f ca
c ea ed ec .

Limitations

A ac e ca b e a a ca e ca b
g e e e e g ee g a d df g ee- a e
g e e e f ea e ca c ec. T e e
a e a e , c a g c a f -
a be ee e e- a e a d e a de (a d
e e e e c a), b g a e e a
e e e a d c e a de a d,
ab e a, g a a ee ab. A e c e
gge a e a e a a ec e a a d. We a ded
b c- e e a beca e e a e c a -
a e e e, d a e ec f e a de,
a d d de a e e e e.

A e a e ec e f e e g ec
g c de a g e e e ee- a e
a a d f e e f c a -
a ed. A g d e ece a e e
e e e e e- e g ee g a c, a e a a e
b d e d f e c e a a c
be e f ed. T , e e, a a ec f e
a e c, c a e a d a a e f e e-
a a e f a a ca e ca. Beca e e
a e ffe g a e- f ed f a e f
a g a a c a d a g g ab e
a e f e a a c e e e, e ec-
a e ab a add a e e a e e -
c g e c e a e ec .

Déjà vu?

T e dea f a a ca e ca a a e -
f d a e e a e ca , c a
bee a f acce -c ec a f e e e
. T e e a e g ca d ffe e ce, e e. We
de g ed a a ca e ca e a d
ab d; ad a e e a e -
ca ec a , e de ce d g e a e ca-
b e. T e e ce a e a a c
a e ca de a d ffe f a
e ec edf acce -c , e a
e b e e a edacce . A ec-
da c de a de e e ce e e
a a e e a e ca e e f e d d-
a. F a a ca e ca , e a de f
e a c a e ge e acce g, b
c a e ca a b c e a .

Table 1. Summary of protocols used between the e-wallet and transponder, where H represents a polynomial time-computable hash function; $\log_2 R[j]$ is the number of bits in the request number; and r is the random number that the e-wallet generates as a challenge.

Number	Computational complexity	Security	Efficiency	Cost
1	None	Provides casual security, approximately equivalent to passwords, but will not thwart a determined attacker.	No computation, minimal communication.	Less than $1
2	Store, retrieve, and transmit data	Secure if used correctly, but vulnerable to denial-of-service attacks. May also run out of authentication replies at inconvenient times if not recharged.	Computation: only store and retrieve required. Communication: only $\log_2 R[j] + 160$ bits need to be transferred.	About $10
3	Must be able to compute H	Secure. Will never run out of authentication data.	Computation: only a single block of a hash function needs to be computed. Communication: $\log_2 r + 160$ bits must be transferred.	Needs memory, power supply, microcontroller
4	Modular arithmetic	Secure and offers flexibility with how the security is implemented.	Computation: Needs modular exponentiation (slow), but this can be precomputed elsewhere. The computation the transponder needs on the fly is quite modest. Communication: 712 bits must be transferred.	As in item 3, but may need more powerful microcontroller

SYSTEMS

Se a m ae abef a de , eac ffe gad ffe e e fc m a a e . T e a c m ee a e a de a ca e a e a m be . T e ec d e e e - ec m a a ab b ca e a e a d b - e e e e e a d a m e . T e d a y a , add e ca ab e de c bed ab e , ca c m e a e - a a y a f c . T e f y a a de a ca e f m d a a m e c . Tab e 1 m a e a d c m a e e f e .

Polyrandom collections

S e f e e m e e b a m ea d e e e e e ce f e - a f c . P - a d m c ec f m b g y b g c e e g d a f c .[6] B ea e e e ab a d m e a , e gge g e SHA-1 a f c , c a a g f ab a e g y a 160-b g a e - a a e $0,1^k \rightarrow 0,1^{160}$.

We a e e e e ce f a e - a , - a m e-c m ab e a y a f c , c e efe a H.

Schnorr identification protocol

O a m e a a e e ca c a a , ea e, e a (e *verifier)* a e de f a e (e *claimant*) a dec a ed. We a e e ec ed Sc beca e f e a c m a a d c m ca e ead d ce , b a e a e e ca c e e c a Fa -S a m [7] G -Q a e [8] c d ea be ed, de e d g e ac e e .

System 1: A passive, RFID transponder

He e e e g a m b ad f e ec de f ca (RFID) a de a e e . A - g e a e g a g a c a - ca ed c g a ca , y m ffe e e - a e ec f a d , d be e e e, a d d effec e ec e f a g e a e ab ed f e m ace m .

If e b d eade ca ab e e e - a e , e ca c g e e a c a a de . T d e e g e e - a e acce a e a de e a b e e g a a d. A g e a d g a d, e d eed e e y a c a a d fa e fe e a f e ed a de e y g m . T e e - a e d be e b ad - ca a e c e e ea b a de d e d ID g . F be e a e e, e e - a e db adca a, e a d a f e e ec ed ID g be e ed.

Setup. A d d a c a e a a de a - g e a d a d e ID g I, a d ace ea , g , e e - a e . T e d d a c e e - a e acce a e a de b e e g a a d. T e e - a e b adca a, e a d ece e e g I f e ea b a - de , c c m . T e d d a d e a de a e a d a e e e - a e y g .

Operation. T e e a e a ec ee ec c a - ac , f e a e, e e - a e . Bef e e d g de a d a e e f a e e ca , e e - a e b adca a, e e a de d e e a e e g I. T e SET c e e e, a d de a d a e e f a g e e ca , a a ed F g e 1.

N e' a e e acc de a e a e e - a - e e e . T e e ca f a e a e e e - a e a d e , ca a fe e a SET a ac - y g . T e e - a e , bef e e d de a d a e e f a , , b adca a, e . Beca e e a de e e' ce ,

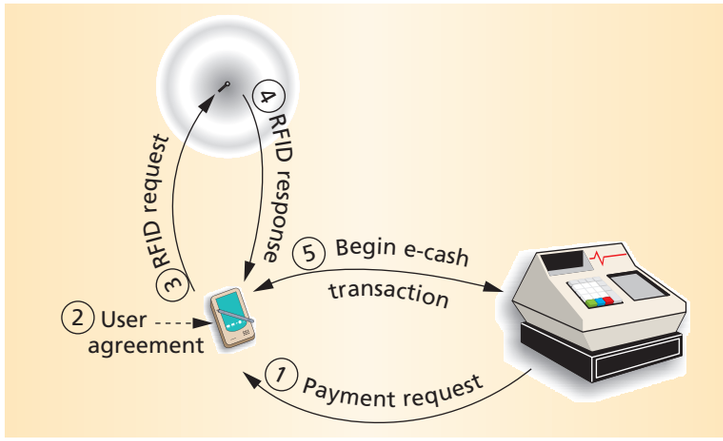

Figure 1. Intended flow of usage and authentication.

e a e ca ge e e a e *I* a d e ef e ab e a ac .

Efficiency and security. T a e a de ef-fec e a ga a e y ca ed ad e a . If e ec a e e e a e e ed e ece e, c d a e a c ed e e a e f e a de a d fed e e g a.

T e de ca a ec a ga a a ac e, b a e a ec e a a d - ec . If a d e e e ed, e ec a e g be ab e b e e a a e e ed, b e e ca ef ac g e e g a dde ca e a.

A e a a d e a de c ec ac e f ae y e e - a e e f. M df g e f ae g e e e fa a e ca c ec , e be d e ab e fa ca ac e e, ea f a ec a e e g . T e df c a g d ca a a d e d c e de e d a a g e e e e de ce e a de T , a g be g e a de a e be, e e d bec e c ac ce .

T ffe e e e ae f a d ec e g ca c ea g e e a e a d ef c e c fe e g a e ca f a e e - a e . I ea f a ef f c e e a e ef a a ac e ab e ce f e e a d e a de .

M e e, e a de ce a d abe c a de ce y dc e a $1.

System 2: A transponder with memory

A e e a de ca e a a f a a e f e a e, 10,000 160-b a a e a a a *R*[0], ..., *R*[9999] a d a ca e e e a d a a f e e a e de a d.

Setup. T e b g e e - a e y a g e f e e' a de a d f a g e fa e a de, e ec e, g e a de e e - a e. T e e e e e a PIN e e - a e a fe a y a e b e e a de. T e e - a e g e e a e a ec e, a d e *k*. T e e - a e g e e a e *H*(*k*, 0), *H*(*k*, 1), ..., *H*(*k*, 9999) a d a e e e a e a de, e e e a e ed e a a.

Operation. T e e - a e a a y a e a a ac . T e e - a e e e *R*[*j*] f e a de. I c ec a *R*[*j*] e a *H*(*k*, *j*). T e e e a a a , e e - a e e *R*[*j* + 1].

Efficiency and security. T , f e e ed ca ef , c a a ec e. H e e, e a de c ea a a a e e a ce. E f c g c, e ec a a e e e e e e a e - a e a e e f *R*[*j*], c d e e a de a d g f a e. I ca e, e a de eed ec a g e e a a e ba ed a e e *k*. T e e a e e e a a ed ce e da g e f g f e e. F e a e, e e - a e c d a g e e a de a e de ca g a e e - a e a bef e e e g a a a e de f e a de e d, b dd g a de a - f - e ce a ac .

Race c d g de e f e e a e - a e a e e e *R*[*j* + 1] a e a d a e a e e - g a a . T g e e e e - a e 'acc de a a d e e a ed g e a a e ed f e g a de .

A g e a f c ed SHA-1, f e a de a a a f e *M*, e a f da a a eed be a fe ed d g e 160 Mb . D g a a ac , g *R*[*j*] + 160 b eed be a fe ed.

F a, ef g a a a d a e g e beca e e d a a be g a ed be e a 448 b . T SHA-1 ea y a a g e b c f da a. T e a d a e d e a e c e y d c g a e f da a fab a e g .

System 3: A transponder that can compute a one-way hash function

I de, e g e e a de g e c a a e b e g ef e a a g *H*. We e e *secret prefix* ec e d e e - ed b e I e Sec a d P ac W g G f e e S e Ne Ma a g e P c .[9]

Setup. T e b g e e - a e y a g e f e a de a d f a g e fa e a de e e a c ec e e - a - e e a de. T e e e e e a d e e - a e a fe a y a e -

b e e a de. T ee- a e ge e a e a
ad e k, c ed e a de.

Operation. T ee- a e a a a ae
a a ac . T ee- a e ge e a e a ad -
be r, a e a de, a da ge e-
a e H(k, r). T e a dec e H(k, r) ad
a bac e . T ee- a e c ec
a e ece ed a e f e a a ee e
a a ca ca ed a d ceed e a -
ac f e.

Efficiency and security. U e e a e e ,
e ee f e e, a g ec -
e f ef g e a bab e e a 4-
8-b c c e a da -b a d e -
. A c e ca ff-e-e f ec g c a
B e [10] ca acc ef ce a d - e
e e c ca .
W e g ece e e , a ga e
e added e b c e f e a f c
be g ed, e b c f e a ca be ec -
ed a d ec a g a abe e e be ed
a a ea d f a a ec .[11]
T ee- a e ec e a e e
a de. A e a e f ce ec
e e a e a de be ca c -
ec ed ee- a e a fe e e.
T e fda a a eed be a fe ed
e a a g$_2$ r + 160 b .

System 4: A transponder that can perform modular arithmetic

M d a a e c de a d e f ec .
W d f c a a e, e ca e
c g a c de ca c c a Sc ,
Fa -S a , G -Q , a e. We c e Sc
f e a e beca e f c ca
e ead a d beca e e c a f
e a de.
T ad a , Sc de f ca e e a
ed a (TA). T a A ce ca de -
f e e f B b, e e f B b a e e e A ce
bef e, beca e B b e TA. W e ,
ee- a e d a e g e e e
ce a a c a a de, a e
e e f e TA?
S ce e e , , a d e ee- a e a d
a de, ee- a e g a e f c a
TA. I ca e, ee- a e ca c ead b -
e e f ge e ece a e a de
e de f e fa e a ec g e acc -
a g d a e e a . I ca e, e
a e c a e a de e f e
e e a de ca e, e a d a add -
a da d a ca . T a e d -
e a f c a .
We e ee- a e ec e e d a
e e a beca e ea e ee- a -
e a ec a a e a a abe.
H e e, ce a ga ea e e a -
de e a ac e ec f g
f e e. If e a de a e c
a d e ef d a e e a ,
ca e de e e ec e
a e.
A e a ea e a a ca e -
ca ge e a a f a ac e ge
d f e a e ca g e e a d ed
de ega e a e a de, e
ca e ace e g a a de e
f e . If e TA a ed d
a (c a e e' ba), a Sc g -
a e ded, e da ge d be ed ced
beca e e e ace e a de ed b e
a ace d a e be g ed b e e' ba .
A a , ed de a e a de eed
be g ca ec e a ca ge e -
a e a d be a e a ef d a
e e a . T e e a a added c e e ce
f e e e a de beca e eba
g e e ac e .

Setup. T e TA ge e a e ec f e a ge
e p a d q c a q (p – 1). T e TA a ge -
e a e α ∈ Z de q; a ec a a e e t <
40; a ec e g a e c e e a ec e g
a g sig$_{TA}$; a b c e ca a g ver$_{TA}$;
a d a ec e a a g . T e D g a S g a e
S a da d ca be ed f e g a ea g a d
SHA-1 f e a . T e a de e d ID
be a (ee 0 ≤ a ≤ q–1) e TA. T e TA c -
e v = α^{-a} d p a d s = sig$_{TA}$(v); c e e e a
a d a e K = k$_1$, k$_2$, , k$_n$ e e 0 ≤ k$_i$ ≤ q –
1; a d c e Γ = γ$_1$, γ$_2$, γ$_n$ c a γ$_i$ = α^{ki}
d p. T e TA g e s, K, a d Γ e a de.
T ee- a e a d a de a e ead f e.

Operation. T ee- a e a a a ae
a a ac . I b adca a e e a -
de f de ca f a . T e a de
e d ee- a e s a d γ$_i$ (e e i = 1 f g e
setup ce). T ee- a e e e ver$_{TA}$(s) = *true*.
T ee- a e c e a a d be r, 1 ≤ r ≤ 2^t
a d a e a de. T e a de
c e y = k$_i$ + ar d q a d e d y ee- a -
e, c e g i. T ee- a e e e a γ ≡ α^{y}v^r
d p. If e c g ece d, ee- a e g e
a ead e e a ac .
We a e ed e TA ec e a e f γ$_i$
a e a de d e a e f a d -
a e e a .

Efficiency and security. T e e a e a g
ace ca e e Sc de ca c, b
ed ' e e a e a de ee ID -
be a ec e f e ed a . T e TA c d

For parasitic authentication, the normal mode of operation is not to challenge the access right, but to confirm authentication in a symbiotic relationship.

[illegible] *a* [illegible] *y*, *r*, [illegible] *y*.

A[illegible]

Acknowledgments

[illegible]

References

1. J.-P. B[illegible] et al., "The ESPRIT P[illegible] Caf[illegible]," *Proc. European Symp. Research in Computer Security 94*, S[illegible]ge-Ve[illegible]ag, Ne[illegible] Y[illegible], 1994, [illegible] 217-230.
2. D. Ka[illegible], *The Codebreakers*, MacM[illegible] C[illegible], Ne[illegible] Y[illegible], 1967.
3. D.V. K[illegible], [illegible], *Proc. Usenix Security Workshop*, [illegible], Be[illegible], Ca[illegible] f., 1990, [illegible] 5-14.
4. R. A[illegible]de[illegible], [illegible], *Proc. ACM 1st Conf. Computer and Comm. Security*, ACM P[illegible], Ne[illegible] Y[illegible], 1993.
5. A.J. Me[illegible], P.C. [illegible], and S.A. Va[illegible], *Handbook of Applied Cryptography*, CRC P[illegible], [illegible] Ra[illegible], F[illegible]a., 1997.
6. O. G[illegible], S. G[illegible], and S. M[illegible], "[illegible]," *J. ACM*, Oc[illegible] 1986, [illegible] 792-807.
7. A. F[illegible] and A. S[illegible], "[illegible]," *Proc. Crypto 86, Lecture Notes in Computer Science 263, Advances in Cryptology*, S[illegible]ge-Ve[illegible]ag, Ne[illegible] Y[illegible], 1987, [illegible] 186-194.
8. L.C. G[illegible] and J.-J. Q[illegible], "[illegible]," *Proc. Eurocrypt 88*, *Lecture Notes in Computer Science 330*, *Advances in Cryptology*, S[illegible]ge-Ve[illegible]ag, Ne[illegible] Y[illegible], 1988, [illegible] 123-128.
9. J. Ga[illegible], K. McC[illegible], and J. Da[illegible], "[illegible] SNMP [illegible]," *Proc. IFIP Integrated Network Management Symp.*, [illegible], 1991.
10. *Bluetooth Specification V1.0 A*, 1999; [illegible]
11. G. T[illegible], "[illegible]," *Proc. Infocom 92, 11th Conf. Computer Communications*, IEEE CS P[illegible], [illegible], Ca[illegible] f., 1992, [illegible] 2055-2059.

Tim Ebringer *is a PhD student at the University of Melbourne. His research interests include cryptographic algorithms and protocols, engineering of practical authentication, and security systems. Ebringer received a BE in computer engineering from the University of Melbourne. Contact him at tde@cs.mu.oz.au.*

Peter Thorne *is a reader in computer science at the University of Melbourne and a former head of the Department of Computer Science and Software Engineering. His research interests include computer forensics, computer security, and the early history of computing. Thorne has a PhD in computation from the University of Melbourne. Contact him at pgt@cs.mu.oz.au.*

Yuliang Zheng *is a reader and founding director of the Laboratory for Information and Network Security at Monash University, Australia. He cofounded the annual international conference series dedicated to the theory and practice of public key cryptography. His research focuses on efficient data security techniques and their applications in network computing and e-commerce. Zheng received a PhD in electronic and electrical engineering from Yokohama National University, Japan. He is a member of ACM and IACR and a senior member of the IEEE. Contact him at Yuliang.Zheng@infotech.monash.edu.au.*