Lightweight Authentication for Email (and Web?)

Ben Adida

ben@mit.edu

PAW/DIG Meeting
June 30th, 2005

(joint work with Susan Hohenberger and Ronald L. Rivest)
From: eBay Billing Department <Billing@eBay.com>
Subject: Credit/Debit Update
Date: April 8, 2005 6:48:27 PM EDT
To: Ben Adida (E-mail)

Dear eBay member,

We at eBay are sorry to inform you that we are having problems with the billing information of your account. We would appreciate it if you would visit our eBay Billing Center and fill out the proper information that we are needing to keep you as an eBay member. If you don't comply until the 15 April 2005, your eBay membership may be suspended, or even deleted.

Click here to complete our web form.

As outlined in our User Agreement, eBay will periodically send you information about site changes and enhancements. Visit our Privacy Policy and User Agreement if you have any questions.

Thank you!
My eBay

New to eBay?
If you want to sign in, you'll need to register first.
Registration is fast and free.
Register >

or

Already an eBay user?
View all your bidding and selling activities in one location.

eBay User ID

Forgot your User ID?

Password

Forgot your password?

Sign In Securely >

Keep me signed in on this computer unless I sign out.

💡 Account protection tips
Be sure the Web site address you see above starts with https://signin.ebay.com/

Microsoft Passport users click here.
One in 20 'fall for online fraud'

One in 20 UK internet users say they have lost money through online scams, research into spam emails suggests.

Almost half say they have received so-called phishing emails aimed at tricking them into revealing details like online banking passwords.
this review is gathering information from community members on their usage of and satisfaction with medical care at MIT, and the Task Force has constructed a survey for students to provide their feedback.

Your time is valuable, especially at this busy time of year, but I hope that you might be willing to take about fifteen minutes to complete a web-based questionnaire. Your participation is entirely voluntary, and you may answer as few or as many questions as you wish. Your response will be treated as confidential, and data gathered will be reported in summary format. I urge you to be as candid as possible in your answers, as this is a very important issue for you and for the students who will follow you at MIT.

You may enter the survey from <http://web.mit.edu/surveys/medical/>. This survey authentication requires a current MIT certificate.

If you have any questions, please send them to med-survey@mit.edu.

Sincerely,
Susan Hockfield
Beware: E-Mailed Surveys May Involve 'Phishing'

Scammers Seek Bank Account Numbers

By Audrey Laganas
From: Burgess-Gregg, Mary  
Sent: Thursday, December 02,  
Subject: Presidential Recognition

I am pleased to inform you that I am more specific at this point be candidates.

I am contacting you now because we need to request a name check from the FBI, as we do with all persons being considered for Presidential recognition. In light of procedures put in place by the White House Counsel's Office, we must receive your written consent prior to requesting the name check. The

http://ostp.gov/FBINamecheck.pdf

request a name check from the FBI,

NOT send a hard copy by mail. If you have questions about this process, please contact Mary Burgess-Gregg at (202) 456-6130 or MBurgess-Gregg@ostp.eop.gov.

Mary L. Burgess-Gregg  
Executive Office of the President  
Office of Science and Technology Policy  
NEOB  
(202) 456-6130  
(202) 456-6027 (fax)  
MBurgess-Gregg@ostp.eop.gov
Distributed Phishing

- Friends and Colleagues
- Jakobsson & Young 2005
No Proof of Origin

Alice

Bob
ID-Based Crypto

A keyserver stores the master secret key (MSK). Bob's public key (PK\textsubscript{bob}) is retrieved from the keyserver using his identifier ("bob@foo.com"). The keyserver also generates Bob's secret key (SK\textsubscript{bob}). Alice encrypts her message (M) using Bob's public key (PK\textsubscript{bob}). Bob decrypts the message using his secret key (SK\textsubscript{bob}).
ID-based Domains

$MPK_{\text{wonderland.com}}$

$MSK_{\text{wonderland.com}}$

$SK_{\text{alice@wonderland.com}}$

$SK_{\text{bob@foo.com}}$

$MPK_{\text{foo.com}}$

$MSK_{\text{foo.com}}$

wonderland.com

foo.com

keyserver

keyserver

Alice

Bob
DNS to distribute Master Public Keys

[DomainKeys]
Email-Based Authentication

[Gar2003]
Tweaks & Optimizations

- **Key Revocation** - expiration date in the ID string: “ben@mit.edu - 2005-04-26”

- **Domain Policies**
  immediate deletion of spoofed emails.

- **Alternate Keyserver**
  bootstrap individual users. Different Trust.
Repudiability is about Privacy
Ad-Hoc Group Sigs

From: Alice
To: Bob
Subject: Account

Your monthly balance is available at:
http://wonderbank.com

Signed:
Alice or Bob
Hijacking Keys for AHGS

I signed this message, OR
I have your secret key

- Signature or Encryption key
- Factoring-, DL-, BM-based algorithms
- All known keypairs work!

[AHR2005]
Putting it All Together

[AHR2005]

1. Publish $MPK_{bank}$

2. Alice

3. $MPK_{foo}$

4. "bob@foo.com"

5. From: Alice
   To: Bob
   Subject: Account
   Signed: Alice or Bob
   Your monthly balance is available at: http://wonderbank.com

6. $MPK_{bank}$

7. "alice@wonderbank.com"

8. $PK_A$

9. Publish $MPK_{bank}$
Web Authentication?

Request for Authentication

Request for Resource

Signature on Nonce, Repudiable Against PK

Web Server
PK

Alice
Questions?