INTERNET CITIZENS BEWARE! YOU'RE BEING PHISHED!

This is totally phreaking me out!

“PHISHING” IS AN E-MAIL SCAM WHERE SOMEONE IS “FISHING” FOR FINANCIAL INFORMATION.

What the heck! Here's my account number and PIN!

IT DOES IT BY MIMICING THE LOOK OF A LEGITIMATE COMPANY'S WEB SITE.

Ooo. I've got e-mail on penis enlargement AND an urgent message from my BANK.
Lightweight Signatures for Email
(A Defense Against Phishing)

Ben Adida
ben@mit.edu
Cryptography and Information Security Group
CSAIL, MIT

6.857 - December 7th, 2005
(joint with David Chau, Susan Hohenberger and Ronald L. Rivest)
This Talk

• The evolution of phishing
• The email authentication problem
• Building an email authentication architecture
• Privacy concerns
• Some Cool Crypto

Assembling Techniques into Security Solutions
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!
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.
From: Susan Hockfield <med-survey@MIT.EDU>
Subject: Survey on Medical Care
Date: April 15, 2005 12:38:00 PM EDT
To: Benjamin Adida <ben@MIT.EDU>

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 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
Dear Presidential recognition.

I am pleased to inform you that a name check is required for Presidential recognition. 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 request a name check from the FBI, http://ostp.gov/FBINamecheck.pdf

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.

Thank you.

Mary Burgess-Gregg
Executive Director
NEOB
(202) 456-6130
(202) 456-6027 (fax)
MBurgess-Gregg@ostp.eop.gov

form should be faxed immediately,
Phishers have added a new lure to their tackle boxes: e-mails that ask people to fax sensitive information to bogus security investigators.
For Immediate Release
Tuesday, November 22, 2005

Washington D.C.
FBI National Press Office

FBI ALERTS PUBLIC TO RECENT E-MAIL SCHEME

E-mails purporting to come from FBI are phony
Cost of Phishing

• Some say > $1B/year
• Others say < $200M/year
• But the real cost of phishing is...
We cannot trust email

• “Never click on a link provided in an email asking for personal information.”
  
  American Banking Association (Dec. 2004)

• “Do be wary of clicking on links in e-mail messages.”
  
  Microsoft (Feb. 2005)

• “Don't automatically assume that any e-mail is from the ‘From’ address.”
  
  Bruce Schneier (Dec. 2004)
“Fear of phishing corrodes trust [...] in email as a vehicle”

“Don't click on links in emails from financial institutions and other organizations that have your personal information”

“Don't trust phone numbers in emails. These can be faked, too.”

“We hate to say that, because such email communications are supposed to make life easier.”
Phishing Everywhere!

New type of phishing could hit mobile phone users
René Millman 1 Nov 2005 13:13

Experts have warned of a new type of phishing that could siphon bank details from mobile phone users.

Mophophishing is where hackers send
Phishers trying to reel in taxpayers

E-mails urge recipients to access bogus site for tax refund

By Daniel Sieberg

Wednesday, November 30, 2005; Posted: 8:27 p.m. EST (01:27 GMT)

Expert: Cyber-crime Yields More Cash than Drugs

11.28.05

By Souhail Karam, Reuters

RIYADH—Global cyber-crime generated a higher turnover than drug trafficking in 2004 and is set to grow even further with the wider use of technology in developing countries, a top expert said on Monday.

Online scammers go spear-phishin'

By Timothy L. O'Brien

The New York Times

Published: December 4, 2005, 4:45 PM PST

About a year and a half ago, Amnon Jackont, an Israeli mystery novelist and Tel Aviv University history professor, became ensnared in a mystery of his very own: friends and students were receiving e-mail messages from him that he had never written.
Phishing reveals a serious problem with email
We need to fix the email platform
SMTP Today

DNS
foo.com
MX Record
mail.foo.com

Alice Bob

wonderland.com
outgoing mail server

mail.foo.com
incoming mail server

1
2
3
4
No Proof of Origin

Alice

Bob

wonderland.com
outgoing
mail server

mail.foo.com
incoming
mail server

phish.com

?
Many Proposals

- Web-based solutions: checking links, better passwords, DSS, ...
- Spam-like filtering identify bad emails by content
- Sender ID / Sender Policy Framework declaring authorized outgoing mail servers
- DomainKeys outgoing mail server signs all emails
A Platform of Trust

We want to provide Just Enough Trust
# Raising the Bar

<table>
<thead>
<tr>
<th>Spoof Outgoing</th>
<th>Intercept Incoming</th>
</tr>
</thead>
<tbody>
<tr>
<td>connect to port 25 of Bob’s mail server, send data.</td>
<td>crack Bob’s IMAP/POP authentication or sniff Bob’s network consistently</td>
</tr>
</tbody>
</table>

Alice → Bob
Building Lightweight Signatures
Basic Signatures

Alice

SK_{alice}

PK_{alice}

Authority

Wonderland

SK_{wonderland}

PK_{wonderland}

sign_{wonderland}(PK_{alice}, "alice@wonderland.com")
DNS to distribute Domain-Level Keys

DNS

wonderland.com
PK_wonderland.com
foo.com
PK_foo.com

Component

[DomainKeys]

Publish

wonderland.com
SK_wonderland.com
Email Authentication

Scenario

From: Alice
To: Bob
Subject: 6.857
I can't wait for 6.857 lecture today!
That TA Chris is so cute! Too bad he's taken...

Alice
alice@wonderland.com

Authority

wonderland
SK_{wonderland}

DNS

wonderland.com
PK_{wonderland}

PK_{alice}

SK_{alice}

Alice
alice@wonderland.com

From: Alice
To: Bob
Subject: 6.857
I can't wait for 6.857 lecture today!
That TA Chris is so cute! Too bad he's taken...

Alice

sign_{alice}(message)

PK_{alice}

sign_{wonderland}(PK_{alice}, “alice@wonderland.com”)

Bob
bob@foo.com
Email Authentication

Scenario

- certifying a user’s public key can add significant overhead.
- distributing the secret key to all user access points is tricky.

...unless we rethink the security requirements a bit.
Email-Based Authentication

[Gar2003]
Server-Managed User Keys

**Scenario**

Alice
alice@wonderland.com

Authority

\[ SK_{wonderland} \]

\[ PK_{wonderland} \]

DNS

wonderland.com

Alice

From: Alice
To: Bob
Subject: 6.857

I can't wait for 6.857 lecture today!
That TA Chris is so cute! Too bad he's taken...

Alice

\[ sign_{alice}(message) \]

\[ PK_{alice} \]

sign_{wonderland}(PK_{alice},
"alice@wonderland.com")

Bob
bob@foo.com
DomainKeys

Scenario

Authority

wonderland

$SK_{wonderland}$

DNS

wonderland.com

$PK_{wonderland}$

From: Alice
To: Bob
Subject: 6.857
I can't wait for 6.857 lecture today! That TA Chris is so cute! Too bad he's taken...

Alice

From: Alice
To: Bob
Subject: 6.857
I can't wait for 6.857 lecture today! That TA Chris is so cute! Too bad he's taken...

Alice

Bob

bob@foo.com
DomainKeys

Scenario

- intra-domain authentication?
- SK must be online
- mail forwarding services?

... can we do better?

Alice
alice@wonderland.com

Authority

wonderland
SK_{wonderland}

From: Alice
To: Bob
Subject: 6.857

I can't wait for 6.857 lecture today! That TA Chris is so cute! Too bad he's taken...

Alice

alice@wonderland.com
Can we get the benefits of both user keys and domain keys?
ID-Based Crypto

"bob@foo.com"

keyserver

\[ MSK \]

\[ MPK \]

\[ PK_{bob} \]

\[ SK_{bob} \]

Alice

Bob

Component
ID-based Domains

Bob

Alice

$SK_{alice@wonderland.com}$

$MSK_{wonderland.com}$

$MPK_{wonderland.com}$

$wonderland.com$

keyserver

$MSK_{foo.com}$

$MPK_{foo.com}$

$foo.com$

keyserver

$SK_{bob@foo.com}$

Bob

Alice
DNS to distribute Master Public Keys

Publish

wonderland.com
key server

wonderland.com

fo.com

DNS

wonderland.com

MPK

foo.com

MPK

Publish
Email-Based Authentication for User Secret Keys

- wonderland.com keys server
  \[ MSK_{\text{wonderland.com}} \]

- SK_{alice@wonderland.com}

- wonderland.com incoming mail server

- Alice
Lightweight Signatures

Our Scenario

1. PUBLISH
   - wonderland.com
   - key server

2. "SK_A"
   - Alice
   - Wonderland.com Network

3. From: Alice
   To: Bob
   Subject: 6.857!
   I've decided Matt is cooler.
   Signed: Alice

4. “alice@wonderland.com”

5. MPK_{wonderland}

6. Bob
   - foo.com Network

From: Alice
To: Bob
Subject: 6.857!
I've decided Matt is cooler.
Signed: Alice

DNS
- wonderland.com
  - MPK_{wonderland}
- foo.com
  - MPK_{foo}

PUBLISH
- foo.com
  - key server
Realistic Deployment

• **Incremental Protection**
  Each domain can implement Lightweight Sigs when it wants to protect its users from spoofing.

• **Minimized User Intervention**
  With domain policies, there is no grey area: emails are either good or bad and require no user judgment.
Deployment Flexibility

• Upgrade the Mail Client & Deploy an Internal Keyserver
  ➡ mail client performs sign & verify
  ➡ keyserver distributes user secret keys

• Upgrade the Mail Server
  ➡ sign at outgoing mail server
  ➡ verify at incoming mail server
Origin of Lightweight Sigs

Classic PGP or S/MIME

Domain-Managed User Keys

Domain-Level Key

Lightweight Signatures
Privacy Concern!
Every email is now publicly verifiable.
So What?

- Alice likes Bob
- Eve likes Bob
- Bob likes to gloat.

This changes the nature of email.

bob.blogspot.com

December 7th, 2005

Check out what Alice sent me! Who knew!....

This changes the nature of email.
Ring Signatures

From: Alice
To: Bob
Subject: Coffee?

Hey Bob,

Wanna meet for coffee? I'd love to get to know you better.

Signed:
Alice or Bob
Identity-Based Sigs, again

• Public Keys are available \textbf{before} user has generated them.

• Public Keys are available using only the domain-based master public key in the DNS.

• If a domain has an MPK, then it can be used for repudiation.
A Bit of Crypto
Schnorr ID Protocol

\[ Z_p^*, \text{generator } g \]

Prover

\[ x \]

\[ t = g^r \]

Verifier

\[ y = g^x \]

\[ c \leftarrow Z_p^* \]

\[ s = xc + r \]

\[ g^s \overset{?}{=} y^c t \]
Schnorr is a PoK

Proof of Knowledge: Extraction

\[ t = g^r \]

\[ s_1 = xc_1 + r \]

\[ s_2 = xc_2 + r \]

\[ x = \frac{s_1 - s_2}{c_1 - c_2} \]
Schnorr Zero-Knowledge

1) Pick a random \( c \)
2) Pick a random \( s \)
3) compute \( t \) to solve the above equation

\( t = g^r \)

\( g^s = y^c t \)

\( t = \frac{g^s}{y^c} \)

\( s = xc + r \)

\((t,c,s) \) is correctly distributed.
Fiat-Shamir

Building a Signature Scheme from a Proof of Knowledge

Prover $t$ Verifier

$c = H(t||m)$

If the protocol is a PoK of a secret key, then $(t,c,s) = \text{sign}(m)$
Guillou-Quisquater Signatures

\[
\begin{align*}
M PK &= (n, e) \\
MK SK &= d \\
PK_{ID} &= H(ID) \in Z_n^* \\
SK_{ID} &= H(ID)^d \in Z_n^*
\end{align*}
\]

Prover

\[
c \leftarrow Z_n^*
\]

\[
s = rSK_{ID}^c
\]

\[
Verifier
\]

\[
t = r^e
\]

\[
s^e \overset{?}{=} tPK_{ID}^c
\]
GQ Properties (I)

Zero-Knowledge: Simulation

\[ s^e \equiv tP K_{ID}^c \]

1) Pick a random \( c \)
2) Pick a random \( s \)
3) compute \( t \) to solve the above equation

\( (t,c,s) \) is correctly distributed.
GQ Properties (II)

Proof of Knowledge: Extraction

\[ t = r^e \]

\[ s_1 = rSK_{ID}^{c_1} \]

\[ s_2 = rSK_{ID}^{c_2} \]

\[ SK_{ID} = \left( s_1 \right) \left( c_1 - c_2 \right)^{-1} \]
Bilinear Maps

\(G_1, G_2, \text{ both of order } q\)

\(e : G_1 \times G_1 \rightarrow G_2\)

\(g, h \text{ generate } G_1\)

\(Z = e(g, h) \text{ generates } G_2\)

\(e(g^a, h^b) = e(g, h)^{ab}\)

\(e(ug, h) = e(u, h)e(g, h)\)
Boneh-Franklin Keys

Public Parameters: $G_1, G_2, q, g, H$

\[ MSK = s \in \mathbb{Z}_q \]
\[ MPK = g^s \in G_1 \]
\[ PK_{ID} = H(ID) \]
\[ SK_{ID} = H(ID)^s \]

Note that: $e(PK_{ID}, MPK) = e(SK_{ID}, g)$
HVZK PoK of Bilinear Map Pre-Image

given $Q \in G_2$, $x \in G_1$

$\exists \alpha \in G_1, e(\alpha, x) = Q$
$g, g^a, g^b \in G_1$

$Q = e(g^a, g^b)$

What is the BM pre-image of $Q$ with respect to $g$?

$e(\alpha, g) = Q \rightarrow \alpha = g^{ab}$
HVZK PoK BMPI

\[ \text{Prover}(Q, \alpha, x) \]

\[ Q = e(\alpha, x) \]

\[ r \xleftarrow{R} \mathbb{Z}_q \]

\[ t = e(g^r, x) \]

\[ c \xleftarrow{R} \mathbb{Z}_q \]

\[ s = \alpha^c g^r \]

\[ e(s, x) \overset{?}{=} Q^c t \]

\[ e(\alpha^c g^r, x) \overset{?}{=} e(\alpha, x)^c e(g^r, x) \]
PoK: Extraction

Prover\((Q, \alpha, x)\)  
\[ Q = e(\alpha, x) \]

Verifier\((Q, x)\)  
\[ r \leftarrow Z_q \]
\[ t = e(g^r, x) \]

\[ s_1 = \alpha c_1 g^r \]
\[ s_2 = \alpha c_2 g^r \]

\[ \alpha = \frac{s_1 (c_1 - c_2)^{-1}}{s_2} \]
ZK: Simulation

c ← \mathbb{Z}_q

s ← G_1

t = e(s, x)

t, c, s \text{ is correctly distributed}
Fiat-Shamir PoBMPI

Prover($Q, \alpha, x$)

$Q = e(\alpha, x)$

Verifier($Q, x$)

$r \xleftarrow{\text{R}} \mathbb{Z}_q$

$t = e(g^r, x)$

$c = H(t || m)$

$s = \alpha^c g^r$

$e(s, x) \overset{?}{=} Q^c t$

$e(\alpha^c g^r, x) \overset{?}{=} e(\alpha, x)^c e(g^r, x)$
Signing with BF Keys

\[ MSK = s \in \mathbb{Z}_q \]
\[ MPK = g^s \in G_1 \]
\[ PK_{ID} = H(ID) \]
\[ SK_{ID} = H(ID)^s \]

\[ Q = e(PK_{ID}, MPK) \]
\[ Q = e(SK_{ID}, g) \]

Prove knowledge of pre-image of Q with respect to g.

[Hess2002]
Applying CDS PoK of PK

prove knowledge of $SK_{ben}$ or $SK_{sha\,fi}$

generate $(t_1, c_1, s_1)$ for $SK_{sha\,fi}$

$(t_2, c_2, s_2)$ must have been generated correctly
• Identity-Based Signatures are well understood.

• Signatures can be thought of as Proofs of Knowledge of a Secret Key, made non-interactive with Fiat-Shamir.

• Proofs of Partial Knowledge: I know Alice’s secret key OR I know Bob’s secret key.
Implementation

• Working prototype using a web-based key distribution, simple DNS server, and Emacs Rmail client.

• More involved usability study in the next few months, multiple domains, real mail client.
Summary

- Phishing reveals an email trust problem
- Lightweight Signatures is one interesting approach
  - end-to-end support of all email apps
  - client-side or server-side computation
- Don’t forget about privacy!
- Assembling crypto tools to solve real problems is fun!
Questions?