Carrier Pigeon

BRANDON DIXON

GOOD TO KNOW

- XMPP/Jabber
- Transports
- Short mail
- Internet to mobile communications

PROBLEMS WITH SHORT MAIL

- Number + Carrier = Victim
- Users get email message with subscription (texting)
- Received as a text message and not an email
- Cost equivalent to standard text message

ATTACKING SHORT MAIL

- Conventional spamming techniques
  - Mass emailers
  - Spoofing the source address
- Carrier can be identified by services online
  - Scriptable
- Short mail is accepted by default

LIMITATIONS

- Anything past 160 characters may be dropped
- Carrier must be properly identified for message to go through
- No delivery confirmation

WHY IS IT BAD?

- Incoming text = charge to the user
- Send short mail from any mail client
- Turned on by default
- Carrier offers limited methods to stopping the attack

CARRIER CAPABILITIES

- Sprint
  - 50 max email/domain blocked
  - Can’t block everything
- Verizon
  - 10 max email/domain blocked
  - Can block everything
- AT & T
  - 15 max email/domain blocked
  - Cant block everything

FIXING THE ISSUE

- Short mail should not be directly tied into SMS
  - Possible flagged of message to identify origin
- Feature should be easily adjusted by the user
  - Should be turned off by default
- More power should be given to block unwanted messages

XMPP/ JABBER

- Communications through XML
- Setting up your own server is easy
  - Multiple options for different platforms
- Allows for bonding to legacy chat implementations
- Control of message flow
  - No rate limiting

INTERNET TO MOBILE

- Google Talk, Yahoo, AIM, MSN (in some areas)
- Input a user's phone number and their now a contact
- Messages get sent in the form of an SMS message

SO WHAT'S NEW?

- Google forces a user to respond after a chat is initiated
  - No response after a few messages = no more talk
- Yahoo forces a user to respond after a chat is initiated and performs throttling
- AOL does NOT force a user to respond but does throttle

ABUSING AOL

- Rate limiting is imposed when sending messages too fast
- Messages past 160 characters are split into multiple messages and NOT dropped
  - 1 message = 13 messages (2000 byte max)
- Acceptance must be made the first time for chatting (this was not always the case)
- Abuse can be programmatically done

XMPP/JABBER TRANSPORTS

- Transport is a bolt-on to a jabber server
- Shows up in service directory for the hosted jabber domain
- Users can bond to “legacy” services
  - Jabber_Name -> AOL
    - Log in to jabber and see AOL contacts
    - User looks like: AOLcontact@myJabber.com
- Jabber name can bond to multiple AOL names (each must be on a different transport)
- Public transports are available

PHONES AND JABBER

- Internal Jabber server with AIM transport service
- Bond internal jabber accounts with AOL accounts
- Send messages to phones using internal jabber account
- Connection, bonding and authorization can be done programmatically

ABUSING PHONES

- Generate phone list
- Generate AOL account list (you must own these)
- Read through list and send one giant message per number (1000 messages per second)
- Send multiple messages to one number (must add delay to avoid rate limits)

LIMITATIONS

- AOL is the single point of failure
- Rate limiting is a pain
- Phone carriers queue messages
    - Limited bandwidth
        - Some messages could be dropped
- AOL provides support to combat against spam and allows users to block messages

BENEFITS

- Send messages at a high rate of speed
- Some transports have support for SOCKS proxies (tor)
- Public transports are often found in other countries with a large user base (good for hiding)
- All attacks can be done programmatically without interaction

FIXING THE PROBLEM

- AOL needs to follow Yahoo and Google's implementation design
- Protection has gotten better since testing first began a year ago
    - ToC servers appear to no longer support Internet to mobile communications

WEB APPLICATION

- Eliminates dependencies with libraries
- Could easily be made into a framework with modules
- Can be accessed anywhere by many people
- Proof-of-Concept allows
  - Bonding of names
  - Sending messages through a choice of transports
  - Sending spoofed short mail messages
  - Identifying public transports
  - More could be added

DEMO