

Security for SMS and Cell phones

Attacks and Theories



Caleb Sima

csima@spidynamics.com

Agenda

Presentation Agenda:

- Security of SMS
- SMS Flooding
- Buffer Overflows
- Bluetooth
- Pocket PC Issues
- Phones and Corporate Security
- References

Security of SMS

- SMS is not a secure messaging medium
 - A jealous boyfriend gets 2 employees of O2 in the UK to intercept text messages sent by his girlfriend's phone in order to catch her cheating on him
 - Security flaw reported at Verizon's SMS service
- Companies including RSA, T-mobile, Sprint, AT&T etc. all send sensitive information over SMS

DoS Attacks: SMS/Email Flooding

Ease of Attack:

- Most cell phones allow the ability to receive SMS/email messages.
- Messages can be sent anonymously thru a multitude of free services.
- Only a phone number is needed to attack someone.
- The ability to receive SMS cannot be turned off (Only tested T-Mobile)

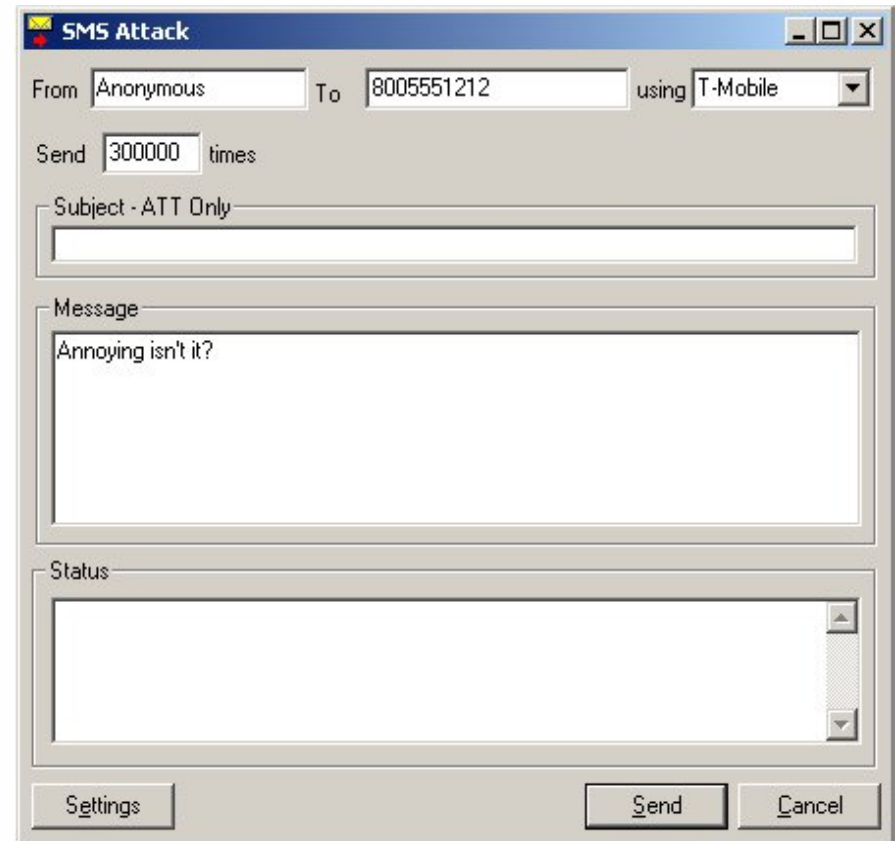
Impact:

- Run up the targets phone bill (\$0.5 per SMS over 50, T-Mobile)
- Effectively deny the ability to make or receive calls on phones
- Becomes a large annoyance and can make the phone extremely slow or unresponsive to menus.

DoS Attacks: SMS/Email Flooding

- Program to DoS phones is easily creatable
- Imagine this being distributed or a worm using it
- Phones that are vulnerable
 - Orange SPV/SPVx Smartphone
 - Pocket PC Phone 2002/2003
 - Treo 300/600
 - Nokia 3595

*Results based on 1 hour worth of testing with phones in our office



SMS Flooding at Work?

Democracy confounds 'Idol' nation

By Bill Keveney, USA TODAY

American Idol is no different from other national elections: Controversy seems built in.



Some *Idol* viewers question why John Stevens continues to be a top vote-getter despite flubbing lyrics and singing off-key.

Fox

"The viewer voting is absurd," says fan Karen Austen, a massage therapist from Freeport, Maine.

Though some fans are convinced that it's all fixed, *Idol* executive producer Ken Warwick says no way. He, too, was "very surprised" by London's finish and says the 20-million-vote tally, tabulated by Telescope, is accurate. The show does try to screen out bloc-voting schemes.

Warwick acknowledges that the voting results have been more erratic this season and attributes it to a better balance of talent.

Buffer Overflows

Areas of Interest:

- Ability to send ring tones, images even video thru MMS
- Communication with Bluetooth
- Applications on the phone (browser)
- AIM

Impact:

- Gain total control of the targets phone
- API's exist that can allow
 - Dialing of phone numbers
 - Turning on the phones voice recorder
- Gain access to contact list and personal notes

Buffer Overflows

Some Theories:

- Find an overflow in the sending of a ring tone thru an SMS message
- Make the payload dial my very expensive 900 number
- Mass broadcast my crafted SMS message to every phone available
- Live in the Caymans and collect tons of cash

- Modify the above attack to be a worm
- Grab all the existing contacts in the phone
- SMS attack each of the contacts
- Infect them and dial the 900 number
- Rinse and repeat

Wireless: Bluetooth/802.11

Areas of Interest:

- Bluetooth devices can be discovered and communicated with
- Bluetooth traffic can possibly be monitored
- Wireless ability opens up the device for direct attack
- All wireless security issues are relevant to the device
- Programs like 'Bluesnarf' can download all the data from a vulnerable Bluetooth device.

```
Bluetooth Scanner 0.1 (Scanning) Mon Jul 14 15:50:34 2003
File Record Scan

Devices
HW Address
00:80:98:00:1E:41
00:80:98:02:1E:41

Last Seen
2006-09-13 07:29:31

First Seen
2003-07-13 21:42:51

Device Name
lame device

Version
1.1

Manufacturer
cisco

Class
phone

Features
none

Signal Strength
#####80%#####

Link Quality
##### 33%

<ESC> to cancel the drop-down menu
<TAB> to move among the widgets
<ENTER> to view details of the device
Use arrows for scrolling
```

Pocket PC Issues

Device Security:

- Memory protection for running programs almost non-existent
- Insecure booting process: allows the ability to flash ROM from SD card
- Access to sensitive API's when booted in boot loader mode

Impact:

- Programs can be created that dumps entire memory revealing sensitive information
- Almost no limitation on what a program can do including completely disabling the device or locking the user out
- Physical security for the device can be disabled by modifying the ROM

Phones & Corporate Security

- Camera and video phones
- Trojans that are activated on the network thru syncing the phone
- No outbound data control – Connecting to the Internet via phone is simple
- Phones can now be audio transmitters

- A phone is the same as a laptop – a pc that is connected to an insecure network at home and is reconnected to the secure network at the office

References

Actual attacks:

- Nokia's 6210 SMS Format string attack in vCards found by @stake
 - <http://www.atstake.com/research/advisories/2003/a022503-1.txt>
- ITSX SMS flaw that breaks Nokia 6210, 3310 and 3330
 - <http://www.theregister.co.uk/content/55/23080.html>

Tools:

- WAP Assesment toolkit
 - Used for assessing WAP gateways and also has abilities to use the WAP gateway as a proxy to attack devices
 - http://www.atstake.com/research/tools/vulnerability_scanning/WAP_Assesment_ToolKit.zip
- FuzzerServer
 - Used as a proxy for testing client side applications for overflows/format string errors in phone based applications
 - http://www.atstake.com/research/tools/vulnerability_scanning/FuzzerServer.zip

References

Bluetooth:

- Bluetooth sniffing tool
 - <http://bluesniff.shmoo.com>
- Bluetooth whitepaper
 - http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf
- Bluetooth security issues
 - <http://www.bluestumbler.org/>

Pocket PC:

- XDA Developers Site
 - <http://www.xda-developers.com/>
- ITSX Site
 - <http://www.itsx.com/home-index.html>

References

- Articles
 - http://www.cellular.co.za/news_2003/081203-security_flaw_reported_at_verizo.htm
 - http://www.theregister.co.uk/2002/11/27/sms_security_risks_highlighted_by
 - <http://www.cellular.co.za/phones/spyphones/spyphone-1.htm>

Closing

Contact Information:

SPI Dynamics Headquarters
115 Perimeter Center Place, N.E.
Suite 270
Atlanta, GA 30346

Toll-Free: (866) 774.2700
Telephone: (678) 781.4800
Fax: (678) 781.4850

Caleb Sima
CTO & Co-Founder
S.P.I. Dynamics, Inc.

csima@spidynamics.com
www.spidynamics.com