SmartSiren: Virus Detection and Alert for Smartphones

Jerry Cheung, Starsky Wong,
Hao Yang and Songwu Lu

MOBISYS 2007

Premise

- Smartphones have become increasingly popular.
- So have viruses for smartphones (among the hackers)!
  - These quickly spread using SMS or Bluetooth and sometimes IP-based applications.
- SmartSiren is a system that performs virus detection and quarantine.
  - Use of behavioral analysis
  - Inform potential victims of attack.

Contributions

- Demonstrate the vulnerability of Window Mobile Smart Phones by implementation of proof-of-concept viruses.
- Design of SmartSiren towards detection and targeted alerts
- A new ticketing scheme that is a part of SmartSiren to help preserve User privacy.

Roadmap

- Introduction to smartphones/viruses
- Requirements for virus infestation/ implementation
- SmartSiren Architecture
  - Collection of Data for Analysis
  - Detection of Viruses
  - Privacy Preservation
- Implementation
- Evaluations (based on simulations)

SmartPhone Viruses

- Cabir
  - released in 2004
  - can self-replicate but does not harm phones
- Comm Warrior
  - An infected smartphone will send out a copy of itself to each smartphone on the user's contact list.
- Others

Infection Vector	Examples
Cellular Network	CommWarriors, Mabir
Bluetooth	Cabirs, CommWarrior
Internet over WiFi/GPRS/EDGE	Skulls, Doomboot
USB/ActiveSync/Docking	Crossover, Mobler
Peripherals	Cardtrap

What does SmartSiren target?

- Viruses that use the SMS and Bluetooth interfaces.
  - Why ?
    Internet based, Peripheral based (floppy) or Docking based viruses, the host device needs to be infected first.
    - Hopefully antivirus systems help.

Requirement for an attack

- The requirement is that the phone should allow third party applications to run.
- Microsoft along with Symbian has taken the approach to implement policies to disallow unknown applications.
- However, approach does not work. Why?
  - Software bugs and vulnerabilities may still exist.
  - Time and economic pressures -- certification time consuming and expensive. Consumers feel frustrated since they cannot run apps.
  - SIM unlocking of the phone requires application unlocking -- very common in other countries.

Implementing a virus

- Implement a virus that mimics Cabir and Flexispy.
  - Use function calls in Bluetooth to discover the devices that are in close proximity.
  - Once these devices are discovered, a simple for loop to send them messages continuously.
  - 8 KB on a HP iPaq Smartphone.
- Prompts the users -- asks if it should be saved (more innovative ways possible)
  - If yes then, saves the virus and does what it is supposed to do.

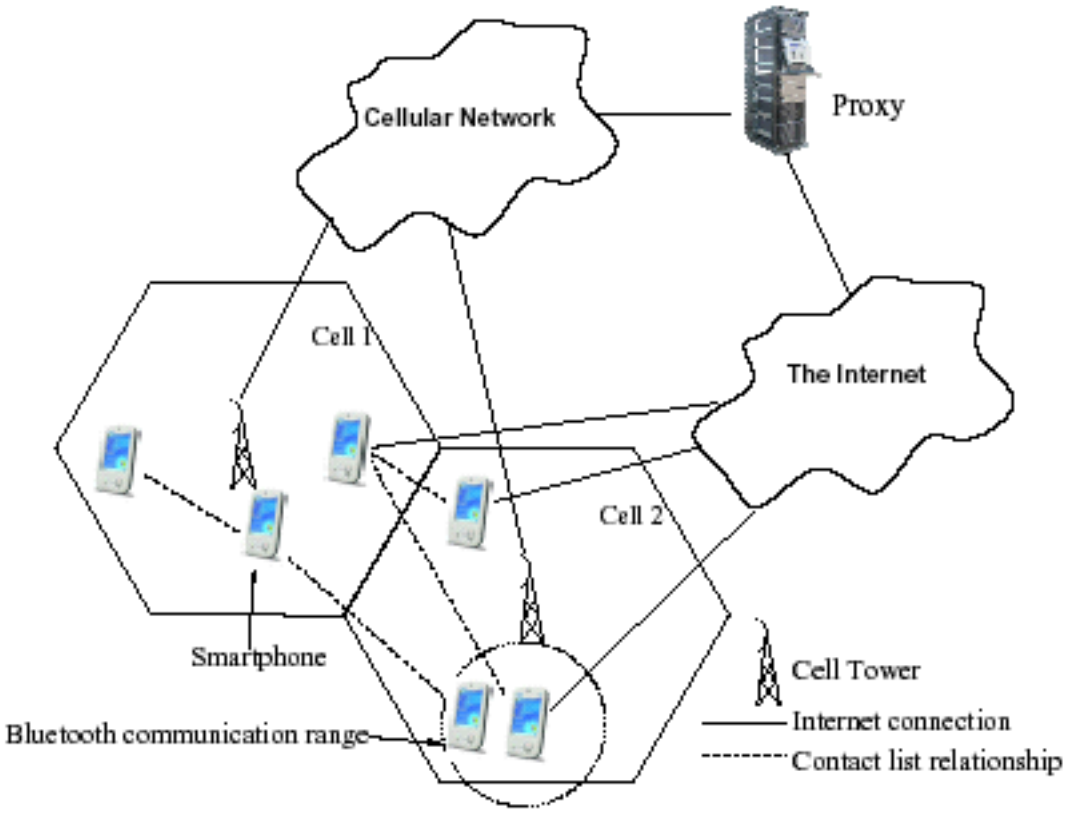
Why are traditional methods inadequate ?

- Firewall and IDS difficult -- communication with peer devices using bluetooth and SMS.
- Up-to date antivirus software may be difficult to maintain -- intermittent Internet connectivity -- viral signatures may not be identifiable.
- Quarantining viruses during mobility difficult.
- Smartphone may not have storage/power to have a complex on-device anti-virus solution.

Architecture of SmartSiren

- Large number of smartphones that want to be protected.
- A proxy that communicated through either cellular or IP-based connections.
- A lightweight agent on each smartphone that logs device activities.
  - Logs periodically reported to proxy

SmartSiren Architecture



In a nutshell…

- Upon receiving logs, proxy performs per-device viral behavior analysis as well as aggregated system-wide analysis.
- Identifies infected smartphones.
- Proxy alerts infected smartphone users.
- It also alerts other smartphone users that may be vulnerable to attacks.
- Proxy based architecture chosen since smartphones may have limited capabilities.
  - Offloads processing burdens.
- One can think of multiple proxies to alleviate centralized bottleneck.

Smartphone agent

- Consists of Four Modules
  - Logging
    - Logs activities -- SMS and bluetooth
  - Privacy Protection
    - Protection of user privacy (later)
  - Reporting
    - Decides when to report activities -- daily or pro-active (abnormal activities)
  - Communication
    - IP-based in implementation.
    - Leverage SMS gateway -- use SMS messages to send e-mails.

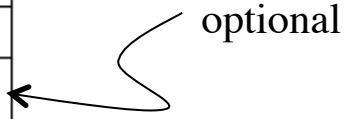
Proxy

- Four Modules also
  - Report Collection
    - Interact with smartphone agents to collect information.
  - Privacy Protection
    - Works with privacy protection module of smartphone agent.
  - Data Analysis
    - Performs analysis of data to detect whether there is a virus spreading in smartphone population.
  - Alerting
    - Upon identification of outbreak, alert infected devices using SMS.
    - Also alert potential victims (direct contact with infected devices)

Registering Information

- Smartphone registers its static configuration with proxy during initial registration.

Category	Value
Phone Number	555-123-4567
Email Address	john.doe@domainname.com
Network	T-Mobile
Phone Model	Dopod 577w
Bluetooth	Yes
OS type	Windows Mobile
Contact List Info	Jane: 555-321-7654 Bob: 555-213-6745 ....
Mobility Profile	Cell ID 1234 Cell ID 9971 Cell ID 756



Reporting Dynamic Activity

- Smartphone dynamically reports activity during operational phase.
  - For now ignore privacy concerns.
- Activities available in logging folders
  - SMS logging done by checking “Sent” folders
  - Logging of Bluetooth activities using properties of *ConnectionsBluetoothCount* and *ConnectionBluetoothDescription* in Windows Mobile OS.
- Reports sent daily (using SMS or Internet)
- In addition, when last daily report exceeds the long term average of daily usage + one standard deviation, device immediately sends report.
- Why ?
  - Periodic reports help detect trojans --> don’t exhibit strong epidemic behavior (Flexispy)
  - proactive reporting to report aggressive replication of virus

Example of a dynamic report

Category	Value
Identity	555-123-4567
Authentication	digital signatures
[Optional Privacy]	Submission Tickets
Log Date	Dec 4, 2006
Mobility Profile	CellID 1234 CellID 756 CellID 3215
Message Sent	555-111-1111 555-222-2222 555-333-3333 ....
Bluetooth Sent	11:11:11:50:11:11 22:22:22:22:22:22 33:33:33:33:33:33 ....

Types of Attacks

Targets	Virus Communicated	Content Communicated	
		Personal Information	Unrelated Information
From-Virus From-Device Randomized	DoS [CommWarrior] Infection	[Flexispy] Info Leak [PBstealer]	[Redbrowser] Spam Spam

- From virus: Virus brings set of targets
- From device : Device's contact list
- Randomized : Anyone !
- Solution attempts to identify and react to virus goals through logging and use of "statistical monitoring" and "abnormality monitoring"

Statistical Monitoring

- U_{thresh}: sum of 7 days moving average of number of communications initiated by a user + standard deviation.
- U_{today} : Number of communications users initiate today.
- If $U_{today} > U_{thresh}$, report over-usage report.
- In addition, a global equilibrium P_{avg} is maintained.
  - P_{avg} : on average, each day, how many of the population exceed Uthresh.
  - When P_{today} exceeds wildly from P_{avg} : viral outbreak.
  - Authors use P_{today} > Detection Threshold Multiplier times P_{avg} --> DTM * P_{avg}

Abnormality Monitoring

- Goal to combat slow infecting worms.
- Virus may seek to achieve some form of financial gain or information theft -- RedBrowser or Flexispy.
- It may seek to slowly replicate and infect other phones -- Comm Warrior.
  - Note these are not mutually exclusive -- Comm Warrior may have payload with Flexispy virus
- A virus either hard codes communication destination or retrieves victim's info from contact list.
- For first type -- monitor if a destination is contacted often
- For second type -- insert a non-existent phone number in contact list
  - Normal users won't contact this number!

Alerting

	Bluetooth Virus Alert	Messaging Virus Alert
Infected Units	B_I	M_I
Connected Units	B_C	M_C

- Above table -- types of alert messages
- Upon receiving B_I, smartphone knows it is infected -- shuts down Bluetooth interface and displays a visual alert to the user.
- When B_C is received, user knows he frequents a location (cell tower ID) that is frequented by infected users.
  - He then will shift to a non-discoverable mode to avoid contact with infected user.
- When M_I is received, infected unit should shut off outgoing SMS interface.
  - However Window Mobile does not offer this.
  - Thus, the authors simply display warning message
- When M_C is received, using Windows Mobile intercept incoming message to filter out infected users' messages.

Privacy Protection

- Critical -- information collected from smartphone may have sensistive information
  - call records, SMS records, network usage.
- Trade-off between virus protection and privacy
  - If you don't provide contact list, then cannot notify acquaintances.
- SmartSiren does not provide perfect privacy
- It only tries to ensure that proxy cannot infer user's daily activity from collected data.

Ways of ensuring privacy

- Obfuscation -- hide actual data in reports (encryption or hashing)
  - Not good since proxy needs this info.
- Anonymization
  - hides who submitted reports.
- SmartSiren includes an anonymous and ticketed report submission scheme.

Key Idea

- Smartphones can submit its report in an anonymous manner.
- However, to prevent bogus reports (now that no one claims responsibility), a unique cryptographic ticket is needed to submit report.
- To create anonymity, smartphones can exchange tickets using a proxy-oblivious scheme.

Anonymous Report Submission

- To ensure anonymity, a device submits its activity only through IP based channels.
- IP address can change --DHCP, different wireless connections.
- If other means used, the reporting may be faster (if no IP connection is available) -- but privacy is compromised to some extent
  - A trade-off between privacy and performance.

Ticketed Report Submission

- Goal -- limit number of reports but allow anonymity.
- Proxy has a Key K_P
- Each user has his own key.
- Proxy divides the users into traders and tradees.
- Traders query proxy requesting a ticket exchange.
- Proxy validates that ticket exchange is legitimate
  - User can issue a report
- The trader contacts tradee
- Tradee needs to have a similar validation
- Once they have validated each other, key exchange can happen.
- Key idea is that validation happens independently

Commutative Encryption

- The key idea exploited in order to facilitate this private communication is what is called Commutative Encryption.
- For any message M and two keys K_1 and K_2, a commutative cipher satisfies:

$$E_{K_1}(E_{K_2}(M)) = E_{K_2}(E_{K_1}(M))$$

The Process --1

- Let K_P be proxy's key and K_A be A's key.
- When trader A chooses a tradee it constructs a transaction description message TD as : $M = (A, B, t)$
  - t is the current time.
- A encrypts the message and sends $E_{K_A}(M)$

together with its identity to the proxy.

- This message is called the Request to Encryption message and the proxy has a list of all such messages received within the last Tm seconds -- the minimum time between two consecutive reports from a device.

The Process -- 2

- Proxy checks to see if it already has a RE from A in its cache
  - If yes, drop RE
  - If not, do the following.
- Encrypt $E_{K_A}(M)$ using its own key.
- Return the result $X_1 = E_{K_P}(E_{K_A}(M))$

to A.

- A decrypts the result with its key and sends the result $E^{-1}_{K_A}(X_1)$ to B.

The Process -- 3

- B encrypts the received message using its key K_B.
- It sends the result $E_{K_B}(E^{-1}_{K_A}(X_1))$, X_2 to proxy in a Request for Decryption (RD) message.
- Proxy decrypts X_2 with its key (does not know who B got the message from) and sends the message $E^{-1}_{K_P}(X_2)$ back to B.
- B decrypts the received message $E^{-1}_{K_B}(E^{-1}_{K_P}(X_2))$
- Let this message be X_3.

The process succeeds

because :

$$X_3 = E_{K_B}^{-1}(E_{K_P}^{-1}(E_{K_B}(E_{K_A}^{-1}(E_{K_P}(E_{K_A}(M)))))) = M$$

- Note that the commutative cipher property is key here!

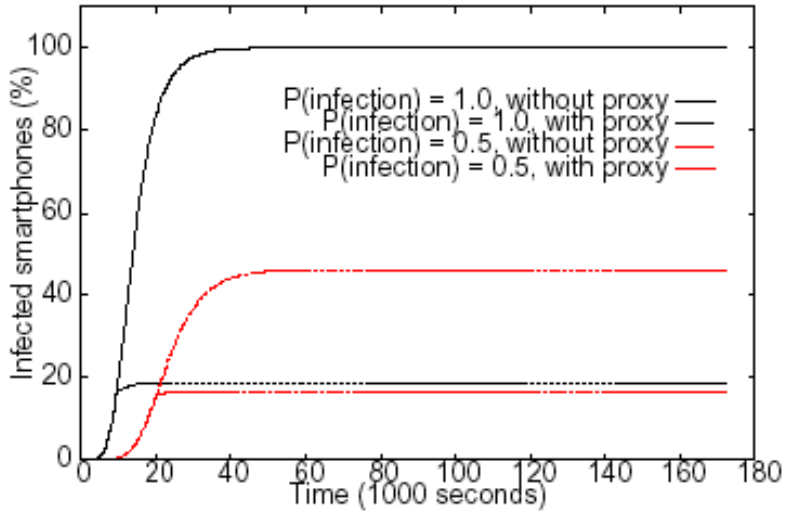
Implementation

- They implement SmartSiren on a Dopod 577w phone.
- Logging, Alerting and other modules implemented.
- They do not do experiments (cannot because need help of provider).
- Only interesting thing : locating cell ID using AT commands -- helps determine locations visited by smartphone.

Evaluation

- Leverage 3-week SMS trace collected from a cellular service provider in India.
- 3.91 million users
- They simulate infection behavior of Comm Warrior.
  - Once a device is infected, virus sends a copy of itself to each smartphone on the user's contact list.

Spreading Trend of Virus



- As infection probability increases, higher levels of spread.
- Proxy helps drastically control spread.

Message Analysis

Message Type	without proxy	with proxy
User	5027903 (31.72%)	5027903 (38.2%)
Virus	10823617 (68.29%)	3703404 (28.2%)
Detection	Nil	879606 (6.7%)
Alert	Nil	3539081 (26.9%)
Total	15851520	13149994

- There is some overhead required to disseminate information about attack.
- After reduction, significantly lower number of messages sent.

Other results

- Show that sometimes, a global view is helpful -- single users may not send much but a single destination is targeted.
- Bluetooth spreading trends -- similar in spirit.

My take

- Interesting paper
- Identifies an important real world problem -- tries to find a solution.
- Cannot solve problem -- real constraints
  - However show implementation.
  - Simulations from traces may be something we may want to consider.