Andbot: Towards Advanced Mobile Botnets

Cui Xiang Fang Binxing Yin Lihua Liu Xiaoyi Zang Tianning

Research Center of Information Security
Institute of Computing Technology, Chinese Academy of Sciences

Agenda

- Introduction
- Andbot Overview
- C&C Design
- Evaluation
- Countermeasures
- Conclusions and Future Works

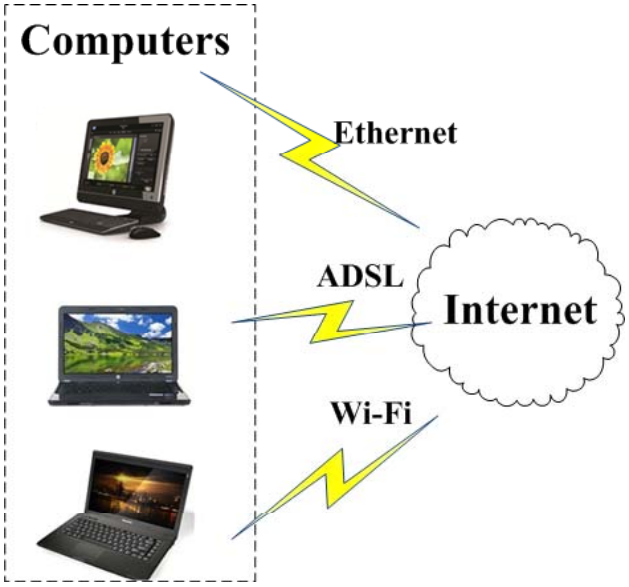
Introduction

- PC botnet

A group of compromised **computers** that are remotely controlled by botmasters via C&C channels.

- Mobile botnet

A group of compromised **Smartphones** that are remotely controlled by botmasters via C&C channels.



Introduction

- Mobile botnets in the wild

- **Name:** SymbOS.Yxes
- **Target:** Symbian
- **Discovered:** 2009

- **Name:** Ikee.B
- **Target:** iPhone
- **Discovered:** 2009

- **Name:** Geinimi
- **Target:** Android
- **Discovered:** 2010

- Simple HTTP-based C&C
- Suffers a single-point-failure

Introduction

- Mobile Botnets Challenges
  - Limited battery power
  - Cost-sensitive
  - Traffic abnormity
  - Absence of public/static IP addresses
- Mobile Botnets: an underlying trend
  - Widely used by billions of end users
  - More powerful computing capabilities
  - More easily to access Internet (i.e., using WiFi, GPRS and 3G)
  - More profitable than PC botnets
  - Absence of efficient host-level security softwares(i.e., AV and FW)

Andbot Overview

- Attack targets

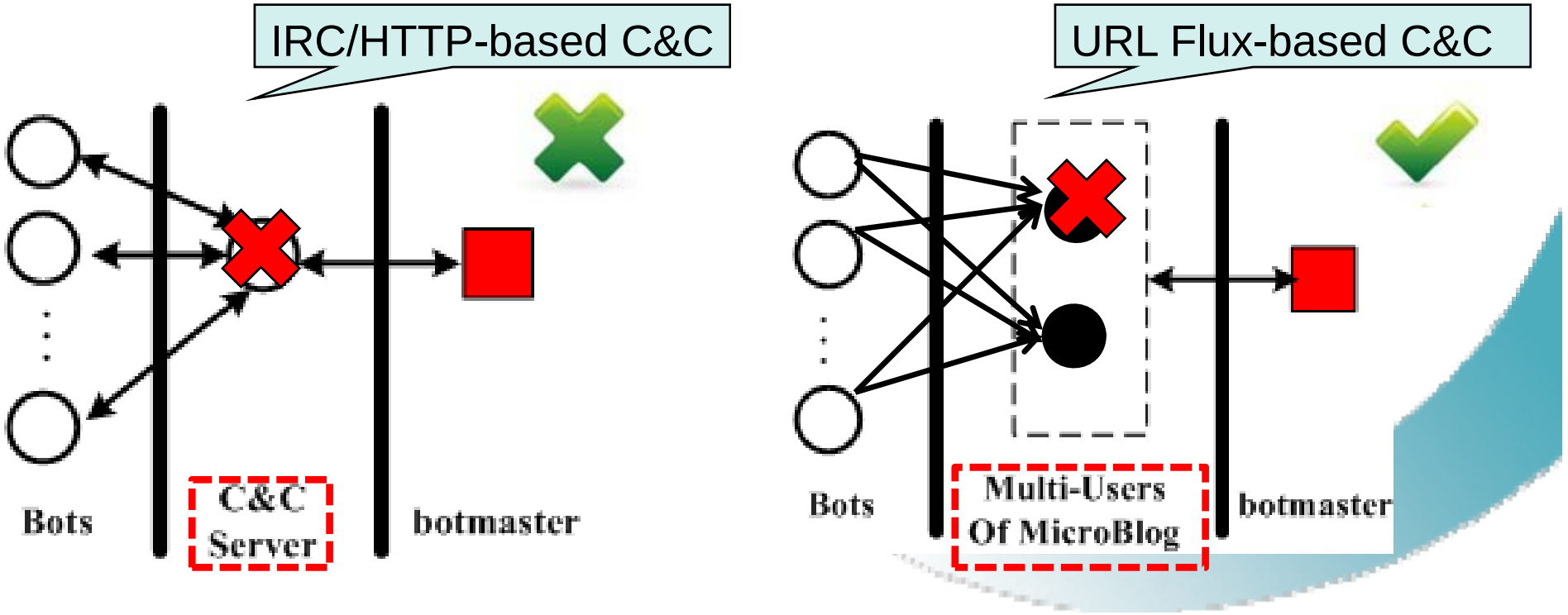
  Android platform

- Commands
  - CallHome
  - SMSDoS
  - SMSSpread
  - MonitorSMS
  - GenSMS
  - DenySMS
  - RelayCmd
  - Sleep

Commands Format
.CallHome#Channel#Address
.SMSDoS#MobileNumber#Num#Random#Content#Len
.SMSSpread#Content#Dest
.MonitorSMS#MobileNumber# Num#Channel#Address
.GenSMS#FakeFromNumber#DateTime
.DenySMS#FromNumber
.RelayCmd#CipherCmd#Num#MobileNumberList
.Sleep#Seconds

Andbot Overview

- C&C Overview
  - **Topology : Centralized**
  - **Protocol : URL Flux (PULL style)**
  - **Addressing:** Domain Name, Username Generation Algorithm



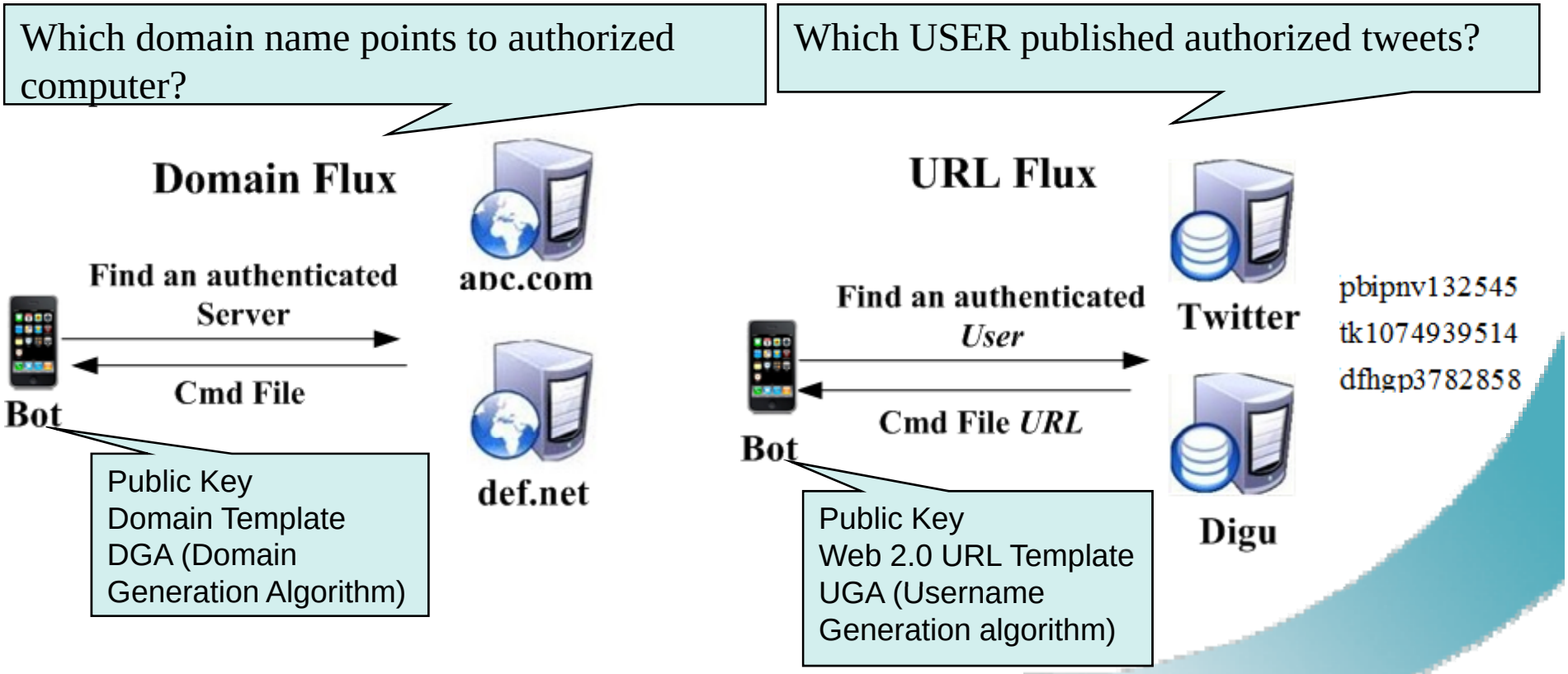
C&C Design

- Desirable C&C of Mobile Botnets
  - **Stealthy:**
    - The capability to bypass botnet detection system;
  - **Resilient:**
    - Resistant to most of public known defense strategies
    - Recover C&C in an accepted time delay
  - **Low-Cost:**
    - Low money costs
    - low traffic and
    - battery power consumption

Andbot C&C = Stealthy + Resilient + Low-Cost

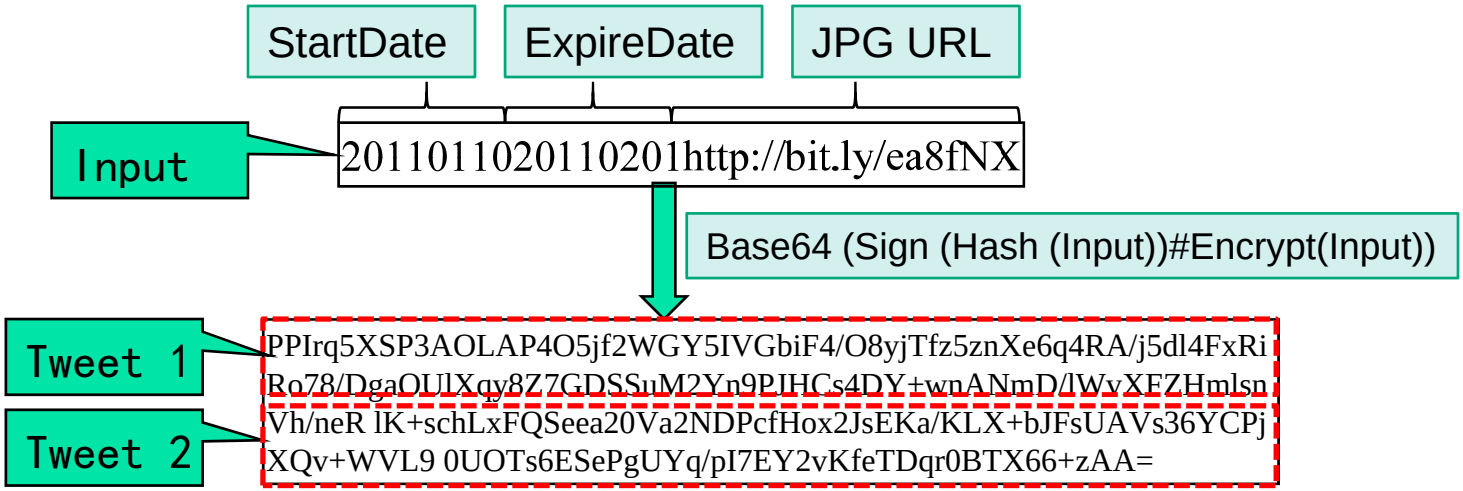
C&C Design - URL Flux

Domain Flux vs. URL Flux



C&C Design - URL Flux

Making and Publishing Secure & Secret Tweets



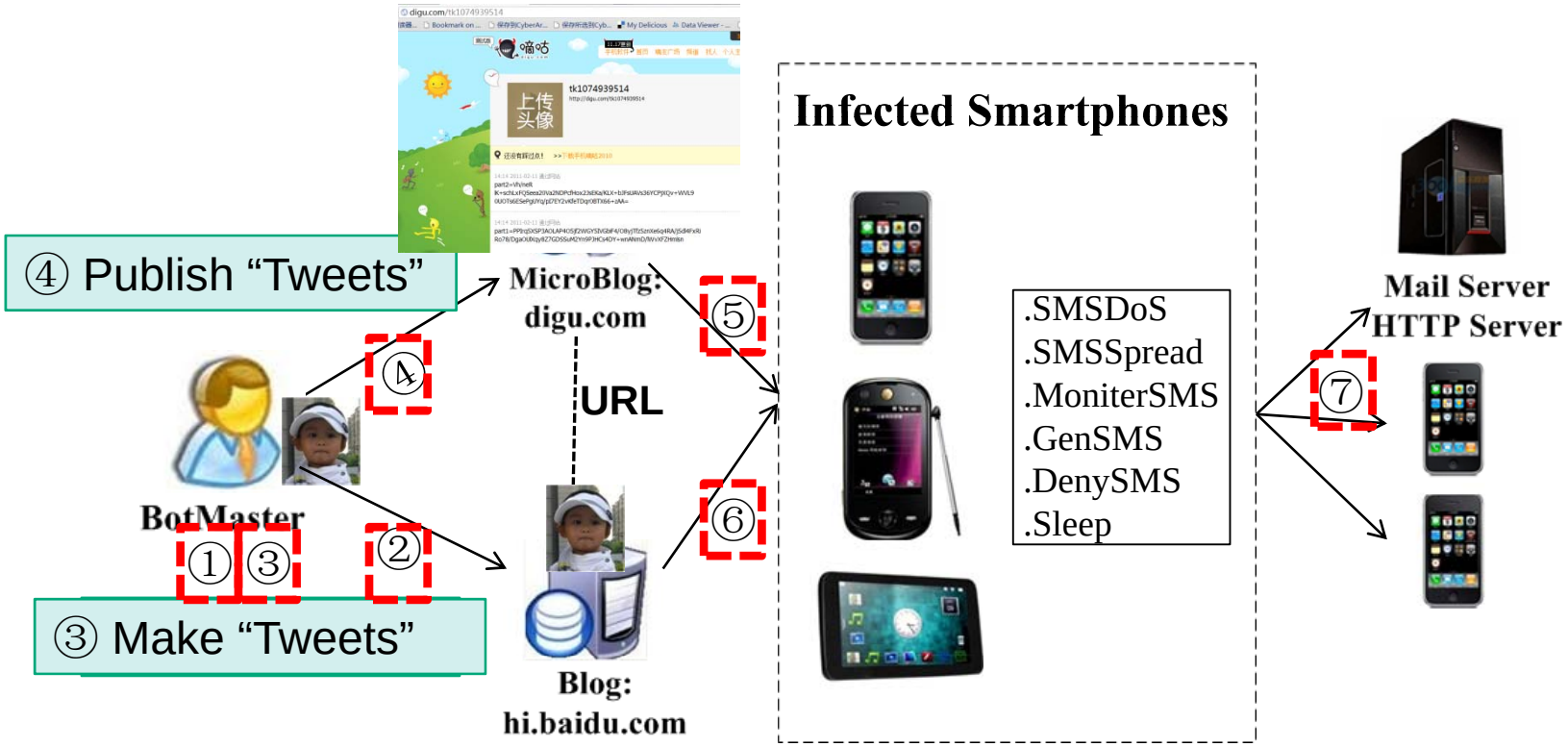
C&C Design - URL Flux

Making and Publishing Secure & Secret Tweets

Making and Publishing Secure & Secret Tweets

C&C Design - URL Flux

The complete URL Flux procedures



C&C Design – Low Cost

- Low Cost
  - **IP-only**
    - Cheaper than SMS significantly
    - GPRS is usually accessible
    - Wi-Fi may be free of charge
  - **RSS and GZIP compression**
    - Decrease traffic
  - **URL Caching**
    - Cache authorized URL in its period of validity
  - **Sleep**
    - Sleep for some time based on the command of botmasters
    - When sleeping, no resource consumption

Evaluation

- Traffic Consumption
  - The most important evaluation factor
  - Influenced by many C&C parameters
    - the interval between two commands requesting
    - the half-yearly and monthly username count
    - if RSS and GZIP should be used
    - if the bot should keep active only when smartphones in sleeping state
    - the total num of different Microblogs

Evaluation

Part of the a URL(http://digu.com/statuses /rss/tk1074939514.rss)

Register Users in Microblog i.e., tk1074939514

The round trip delay between first packet and last packet

Send bytes/Recv bytes/ Total bytes(including connection, and all packets headers etc)

SubURL	User Name	Gzip	Avg. Time Delay(s)	Request/Response/Total Traffic(Byte)
/statuses/rss/pbipnv132545.rss	Not Exist	No	7.618	164/348/1188
/statuses/rss/tk1074939514.rss	Exist	No	13.745	141/1972/2995
/statuses/rss/tk1074939514.rss	Exist	Yes	2.706	164/1062/1902

Evaluation

Locate the first Authorized **user**

Available Username Num		Time Delay(S)	Total Traffic(KB)
Half- Year	5%	30.61s	12.87
	10%	14.85s	7.07
	50%	4.46s	2.43

Download the JPG

JPG File Size(Byte)	Cipher Cmd Len(Byte)	Time Delay(S)	Traffic Cost(Byte)
2326	213	3.06s	3705

6(KB) <=Traffic Consumption <= 16(KB)

Countermeasures

- Building International Coordinated Mechanism
  - **Web 2.0 Abuse Response**
    - Using Microblog to publish malicious messages
    - Using Blog, Google Sites and YouTube to host malicious image files
  - **Cloud Computing Platform Abuse Response**
    - Using Google App Engine to receive messages (i.e., CallHome, Identity)
    - Using Amazon EC2 to host malicious C&C servers

Countermeasures

- Monitoring at SMSC side and Verify in Cloud Sandboxes/VMs
  - **Mobile Worm Detection at SMSC side**
    - Multi-SMS as input
    - Similar to PC worm detection system such as Autograph, Early-birds
    - Generating signatures automatically
  - **Verification via Cloud Sandboxes/VMs**
    - Verify the found worms
    - Verify the softwares to be published
- Infiltration
  - **First analysis C&C protocol**
  - **Then program an infiltrator**

Conclusions and Future Works

- Smartphones are attractive targets to hackers
- Constructing a practical mobile botnet is feasible
- URL Flux is very suitable for mobile botnet C&C
- Andbot is stealthy, resilient, and low cost, posing potential threat
- Defenders should pay more attention to advanced mobile botnets

Conclusions and Future Works

- **Dynamic Username Generation Algorithm (DUGA)**
  - Querying the most active topic as seed for UGA
  - Making blocking username registration in advance difficult
- **Eliminating Time-Space Similarities via Randomization**
  - Injecting packet and flow-level noise
  - Adding a random delay when communicate
- **Emergency C&C**
  - Exploiting SMS as C&C when distributing urgent tasks
  - Recovering C&C in case all Web 2.0 resources unavailable

Thank You!