SECURING YOUR MOBILE DEVICE

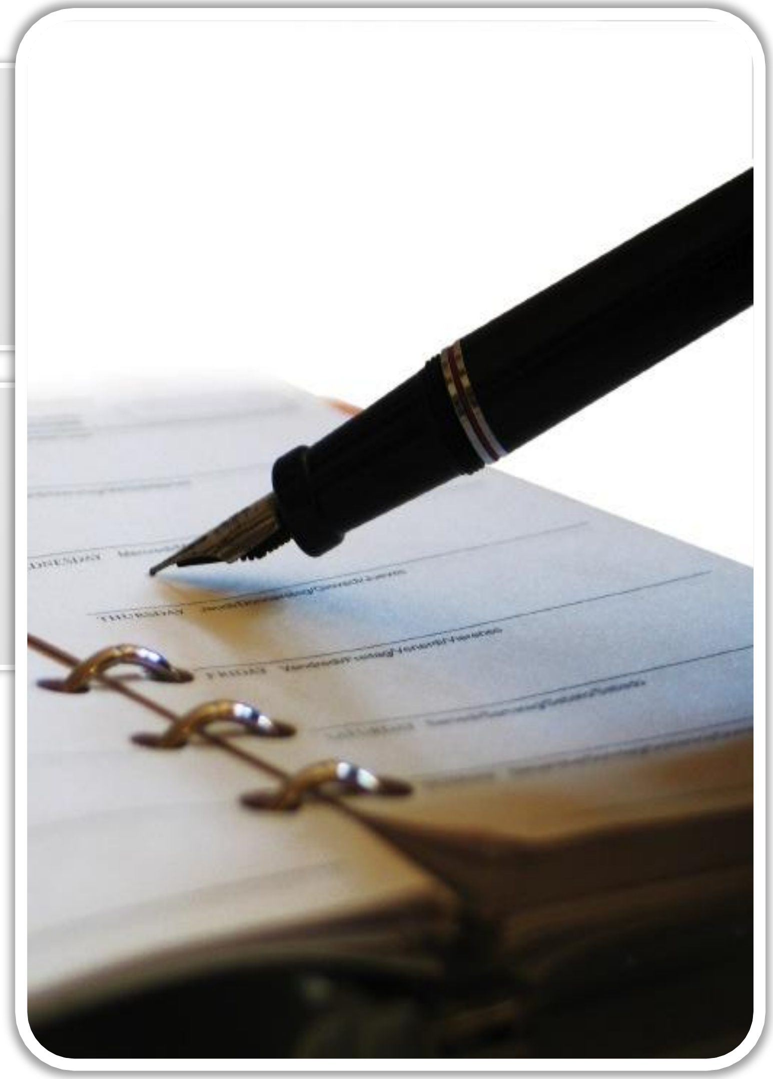
Leslie K. Lambert
Juniper Networks
VP & Chief Information Security Officer

June 29, 2011

AGENDA

Today’s Shifting Threat Landscape

Mobile Device Security



TODAY'S SHIFTING THREAT LANDSCAPE

The Sophisticated Cybercriminal

- Cybercriminals - from students to well paid organized professionals
- Advanced Persistent Threats - Sophisticated and strategic efforts aimed at intelligence gathering and espionage

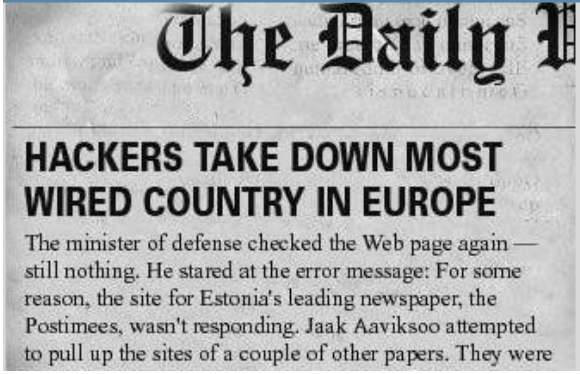
The Threat from Within

- Insiders with and without malicious intent
- The mobile device as Trojan Horse

CHANGE IN ‘ATTACKER BEHAVIOR’

Notoriety

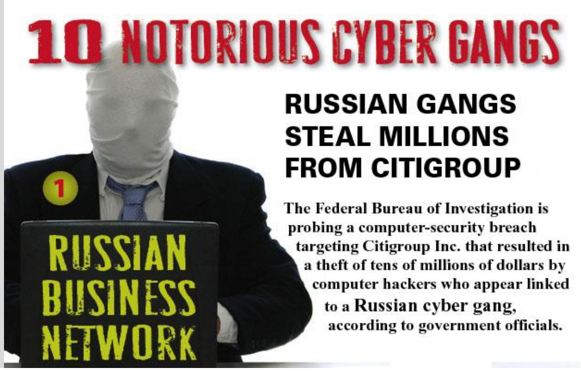
Profitability



The Daily

HACKERS TAKE DOWN MOST WIRED COUNTRY IN EUROPE

The minister of defense checked the Web page again — still nothing. He stared at the error message: For some reason, the site for Estonia's leading newspaper, the Postimees, wasn't responding. Jaak Aaviksoo attempted to pull up the sites of a couple of other papers. They were



10 NOTORIOUS CYBER GANGS

RUSSIAN GANGS STEAL MILLIONS FROM CITIGROUP

The Federal Bureau of Investigation is probing a computer-security breach targeting Citigroup Inc. that resulted in a theft of tens of millions of dollars by computer hackers who appear linked to a Russian cyber gang, according to government officials.

1
RUSSIAN BUSINESS NETWORK

.gov /.com

.me / .you / .edu

MOBILE SECURITY IS IMPACTED BY TWO TRENDS

Industry Trends

Computers, Smartphones, Tablets

Everyone's Mobile

Consumerization

Security Trends

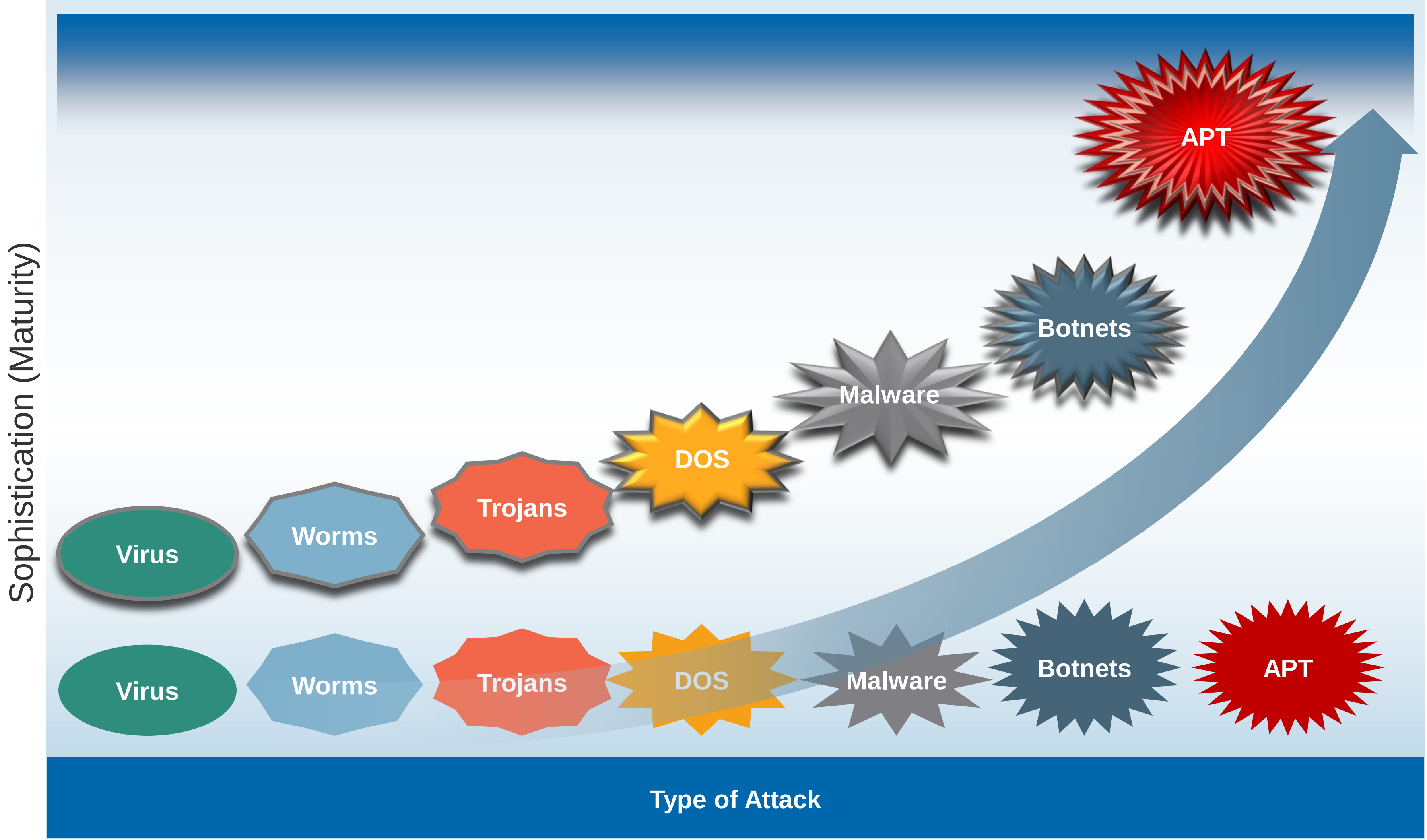
Evolving Threat Vectors

New Attack Targets

Attacker behavior

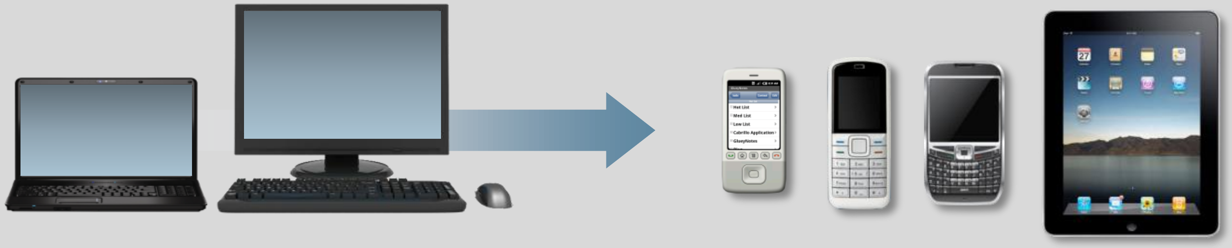
INDUSTRY TRENDS
MORE ABOUT CONSUMERIZATION

SECURITY TRENDS
EVOLVING THREAT VECTORS

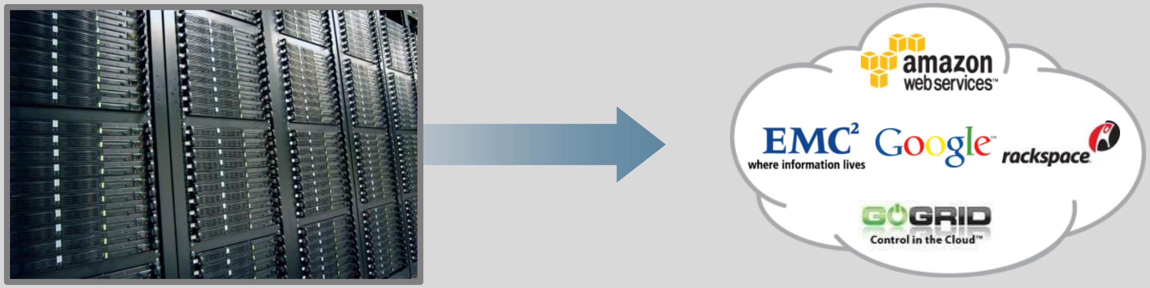


NEW TARGETS – ANY DEVICE, ANY LOCATION, ANY APPLICATION

New Devices



New Cloud Services

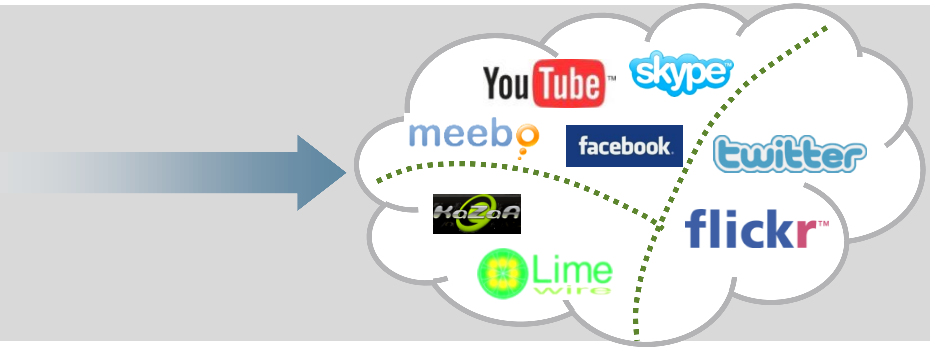


New Applications

Windows Server
Internet Information Services

*.ppt

*.xls

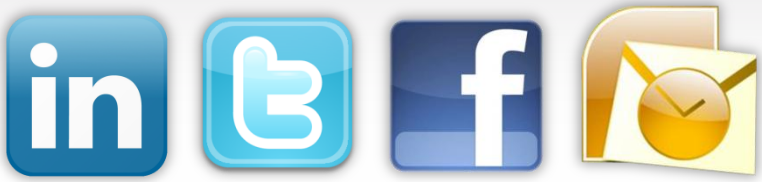


THE MOBILE INTERNET IS THE NEW INTERNET

Proliferation of Devices

Number of smartphones sales to exceed PC sales in 2012*

Connected Socialization



Content Consumption

*Source: Morgan Stanley, 2010

www.juniper.net

NEW RESEARCH REVEALS A GAP BETWEEN BEHAVIOR AND THE DESIRE TO BE SAFE

40%
use smartphones for both personal and business

72%
share or access sensitive info (banking, credit card, social security, medical records)

80%
access their employer's network without permission – 59% do it everyday

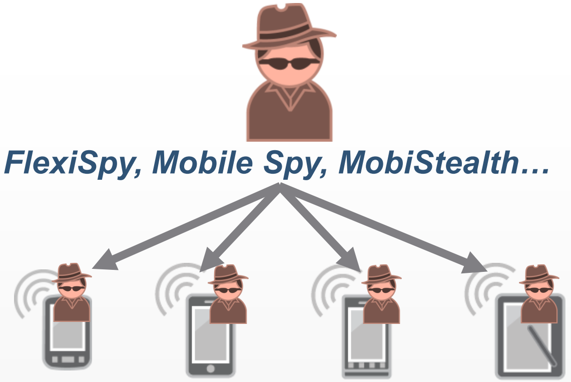
50%+
are very concerned about loss, theft and identity theft resulting from their mobile usage

Sources: KRC Research and Juniper Mobile Threat Center

EVOLUTION OF MOBILE MALWARE

Criminals now using PC-style malware attacks to infect mobile devices

Greatest mobile malware risk comes from rapid proliferation of applications in app stores



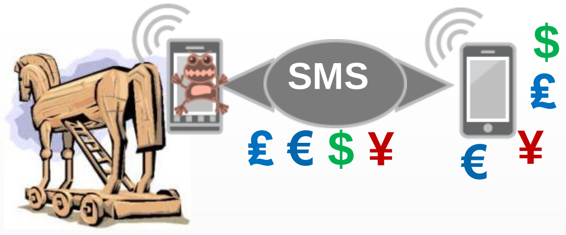
Mobile spyware is prevalent and now commercialized

2009 → **2010**

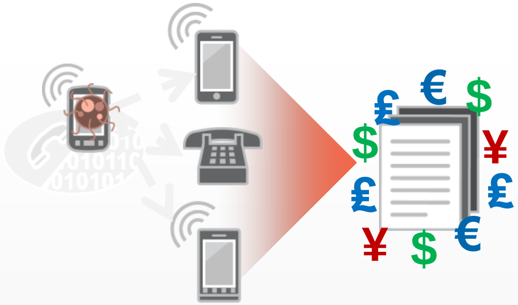
Between 2009 and 2010, reported increase in mobile threats of 250%*

*Information obtained from analysis of Junos Pulse Mobile Security Suite virus definition database dated 10/15/2010

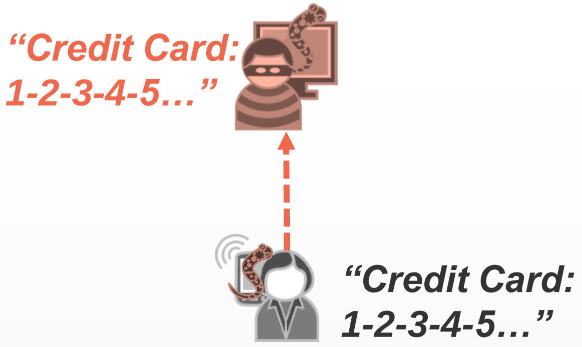
FAST PROLIFERATING MOBILE MALWARE THREATS



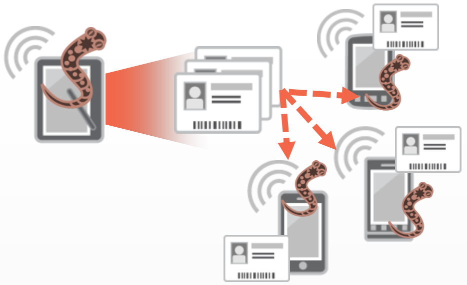
Trojans that send SMS messages to premium rate numbers



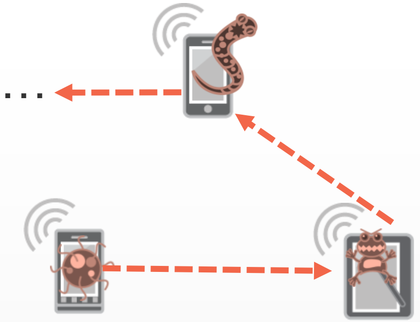
Background calling apps that rack up exorbitant long distance bills



Keylogging applications that compromise passwords and credit card or bank account numbers



Self-propagating code that infects devices and spreads to additional devices listed in a user's address book



Malware growing more sophisticated, now with polymorphic attacks

MOBILE DEVICE LOSS AND THEFT

A survey of consumer users found that one out of every three users lost their mobile device[1]

Approximately 2 million smartphones were stolen in the U.S. in 2008[2]

Over 56,000 mobile devices were left in the back seats of the city of London taxi cabs during a 6-month period between 2008 and 2009

Over the 2010 holidays, in the U.K. alone, a total of 5,100 smartphones and 3,844 notebook computers were lost at 15 different airports[3]

In Paris, 75% of 991 violent crimes that took place in October 2010 happened because of mobile phone theft[4]

[1] Information obtained from Junos Pulse Mobile Security Suite internal transaction logs; [2] Forrester Research; [3] Credant Technologies; [4] The Sydney Morning Herald, 12/10/10

WHY IS MOBILE DEVICE LOSS AND THEFT AN ISSUE?

Bookmarked bank accounts with passwords set to auto-complete

Contacts with pictures and addresses tied to the contact

Pre-connected personal data compilation sites

Social media accounts

Calendar events

Personal photos

Pre-connected e-mail accounts

Sensitive research data and IP

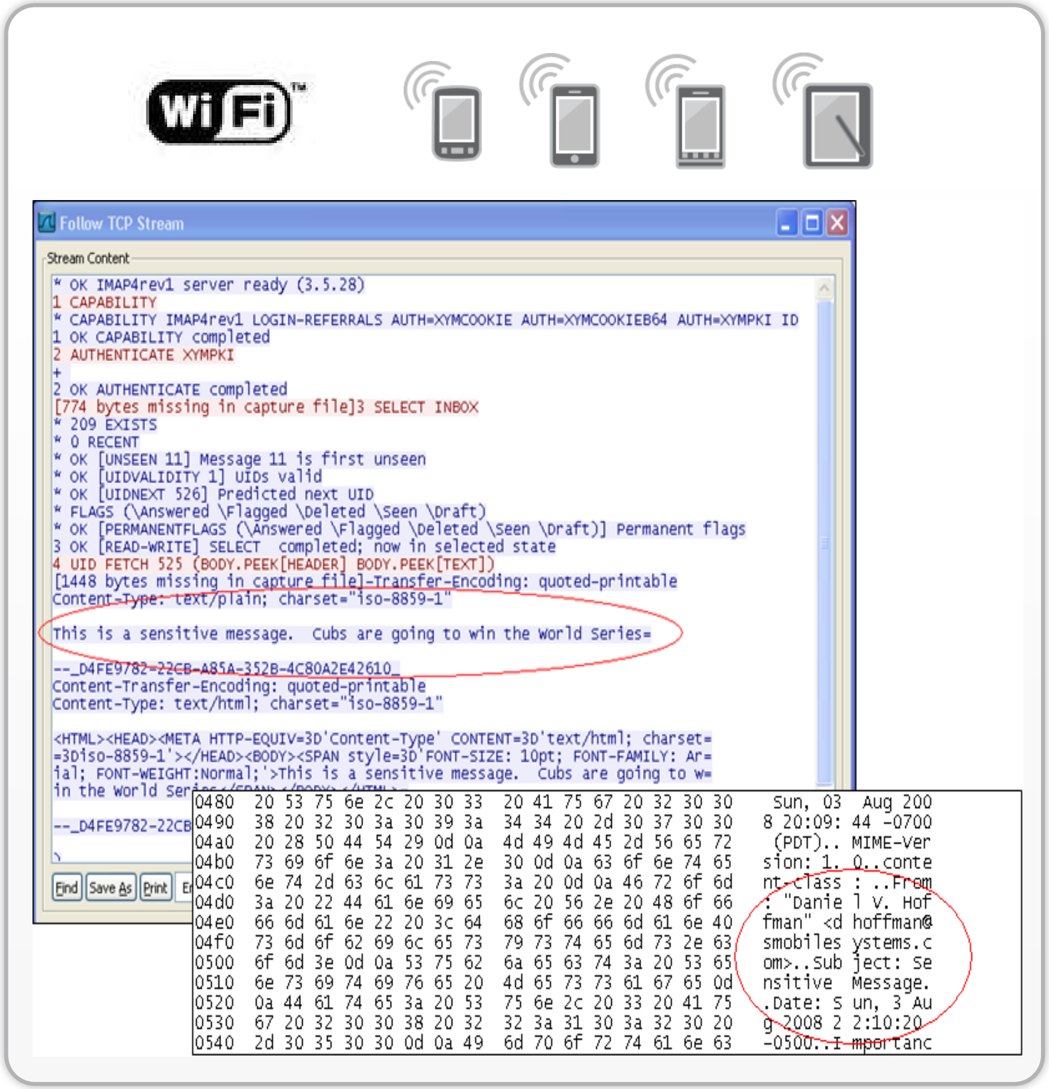
COMMUNICATION INTERCEPTION

~ 50% of all smartphones today are Wi-Fi capable[5]

~ 90% of all mobile devices will be Wi-Fi capable by 2014[5]

Wi-Fi interception increases as number of Wi-Fi capable mobile devices increase

Mobile devices on Wi-Fi networks are susceptible to attacks[6]



```
* OK IMAP4rev1 server ready (3.5.28)
1 CAPABILITY
* CAPABILITY IMAP4rev1 LOGIN-REFERRALS AUTH=XYMCOOKIE AUTH=XYMCOOKIEB64 AUTH=XYMPKI ID
1 OK CAPABILITY completed
2 AUTHENTICATE XYMPKI
+
2 OK AUTHENTICATE completed
[774 bytes missing in capture file]3 SELECT INBOX
* 209 EXISTS
* 0 RECENT
* OK [UNSEEN 11] Message 11 is first unseen
* OK [UIDVALIDITY 1] UIDs valid
* OK [UIDNEXT 526] Predicted next UID
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen \Draft)] Permanent flags
3 OK [READ-WRITE] SELECT  completed; now in selected state
4 UID FETCH 525 (BODY.PEEK[HEADER] BODY.PEEK[TEXT])
[1448 bytes missing in capture file]-Transfer-Encoding: quoted-printable
Content-Type: text/plain; charset="iso-8859-1"

This is a sensitive message.  Cubs are going to win the World Series=

--_D4FE9782-22CB-A85A-352B-4C80A2E42610_
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="iso-8859-1"

<HTML><HEAD><META HTTP-EQUIV=3D'Content-Type' CONTENT=3D'text/html; charset=
=3Diso-8859-1'></HEAD><BODY><SPAN style=3D'FONT-SIZE: 10pt; FONT-FAMILY: Ar=
ial; FONT-WEIGHT:Normal;'>This is a sensitive message.  Cubs are going to w=
in the World Ser

--_D4FE9782-22CB
```

```
0480  20 53 75 6e 2c 20 30 33  20 41 75 67 20 32 30 30   Sun, 03  Aug 200
0490  38 20 32 30 3a 30 39 3a  34 34 20 2d 30 37 30 30  8 20:09: 44 -0700
04a0  20 28 50 44 54 29 0d 0a  4d 49 4d 45 2d 56 65 72   (PDT).. MIME-Ver
04b0  73 69 6f 6e 3a 20 31 2e  30 0d 0a 63 6f 6e 74 65  sion: 1. 0..conte
04c0  6e 74 2d 63 6c 61 73 73  3a 20 0d 0a 46 72 6f 6d  nt-class : ..From
04d0  3a 20 22 44 61 6e 69 65  6c 20 56 2e 20 48 6f 66  : "Danie l V. Hof
04e0  66 6d 61 6e 22 20 3c 64  68 6f 66 66 6d 61 6e 40  fman" <d hoffman@
04f0  73 6d 6f 62 69 6c 65 73  79 73 74 65 6d 73 2e 63  smobiles ystems.c
0500  6f 6d 3e 0d 0a 53 75 62  6a 65 63 74 3a 20 53 65  om>..Sub ject: Se
0510  6e 73 69 74 69 76 65 20  4d 65 73 73 61 67 65 0d  nsitive  Message.
0520  0a 44 61 74 65 3a 20 53  75 6e 2c 20 33 20 41 75  .Date: S un, 3 Au
0530  67 20 32 30 30 38 20 32  32 3a 31 30 3a 32 30 20  g 2008 2 2:10:20
0540  2d 30 35 30 30 0d 0a 49  6d 70 6f 72 74 61 6e 63  -0500..I mportanc
```

[5] http://www.wi-fi.org/news_articles.php?f=media_news&news_id=969;
[6] http://threatcenter.smobilesystems.com/?p=1587

SUGGESTIONS TO DEFEND AGAINST TODAY'S MOBILE DEVICE THREATS

Proactive Protection

- Remember, you are carrying a small, yet powerful, mobile "computer" that can be infected with malware or compromised just like your laptop or desktop computer
- All mobile devices are NOT created equal, e.g., iOS vs. Android
- ALWAYS protect the physical security of your mobile device
- Enable the password or passcode feature to access your mobile device
- NEVER share your passwords or passcodes with ANYONE
- Disable or turn off wireless access on your mobile device unless you are actively using it
- Install anti-virus/anti-malware software on your mobile device
- Enable encryption on your mobile device, if available

SUGGESTIONS TO DEFEND AGAINST TODAY'S MOBILE DEVICE THREATS

Proactive Protection (cont'd)

- ONLY download mobile device apps from web sites you TRUST and KNOW are secure
- Do not plug in "mysterious" thumb drives / cards to your mobile device
- BEWARE that many mobile device applications are location-aware
- Enable remote wipe or erase feature for your mobile device, and learn how to use it
- REMEMBER to regularly perform a backup or synchronize your mobile device with a **reliable** backup destination

SUGGESTIONS TO DEFEND AGAINST TODAY'S MOBILE DEVICE THREATS

Safeguards Against Communication Interception

- AGAIN, disable or turn off wireless access on your mobile device unless you are actively using it
- Connect ONLY to trusted wireless networks, e.g., at CSUN, the csun_wpa2 wireless network is trusted and communications are encrypted
  - Instructions found on IT website – www.csun.edu/it
  - Need help? Call IT Help Center at ext. 1400
- NEVER click on or select links in email messages you receive from users you do not know!
- When entering private information into a web page, make certain to do so on trusted web sites that use encryption, e.g., HTTPS vs. HTTP

SUGGESTIONS TO DEFEND AGAINST TODAY'S MOBILE DEVICE THREATS

Safeguards Against Communication Interception (cont'd)

- NEVER send **confidential** or **personal information** via email, EVER!
  - CSUN, your bank, your medical doctor, and any other trusted institutions or providers will NEVER ask you for this type of information via email
- Do not store **protected** or **sensitive data** on your mobile device – if you must, only if the mobile device is encrypted
- Limit the number of email messages downloaded to your mobile device

PRACTICE SAFE MOBILE COMPUTING!
THANK YOU!

everywhere