Reach Out and Hack Someone
Session 8843

Ellis Holman
eaholma@us.ibm.com

Disclaimers, for the lawyers

- **The techniques described herein when applied to systems not owned by you is ILLEGAL.**
  - THAT MEANS IT'S AGAINST THE LAW!!!
- Modifications carried out may damage the cell phone and void the manufacture's warranty
- This presentation is the sole opinions of the presenter
- The intention of this presentation is not to call into question the suitability of any software mentioned
- The presentation is to merely point out what is possible within the confines of academic discussions

Statistics favor the hackers as smart phones become based on more open software

- The open source Android platform is particularly popular
- Gartner research predicts that by 2012, 80% or more of commercial software packages will include open source technology
- Google reports that more than 1/3 of users, 36.2%, run the Android operating system called Froyo
- According to Google, over 200,000 Android smartphones are activated each day
- 2010 Coverity Scan Open Source Integrity Report uncovered "359 defects in total and of these, 88 of the defects were "high risk", which includes memory corruption, resource and memory leaks, and uninitialized variables."

Smartphones now in use are more sophisticated than ever before

- Most have programmable capabilities
- Many are web capable
- Many are bluetooth enabled
- Some are hybrid PC/Phone combinations
- Many are WIFI enabled
- Applications exist to store personal and business data
- Tools exist to both customize and exploit these sophisticated handsets

Warnibbling is the art of mapping bluetooth devices

- Similar to wardriving, but deals with smaller devices
- Somewhat more difficult, because; the devices' lower power
- There are three primary security modes:
  - Mode 1: No Security
  - Mode 2: Application/Service based (L2CAP)
  - Mode 3: Link-layer (PIN authentication/MAC address security/encryption)

‘Bluejacking’ makes use of the bluetooth stack to send messages to unsuspecting persons nearby

The technique involves abuse of the bluetooth "pairing" protocol

- The protocol defines an authentication process to identify devices to each other
- During the initial "handshake" phase it is possible to pass a message to another device.
- It is made possible because the "name" of the initiating bluetooth device is displayed on the target device as part of the handshake exchange
- The protocol allows a large user defined name field - up to 248 characters. It is the field itself which is used to pass the message.

Could be used for spamming and unwanted advertising

A more insidious attack on bluetooth enabled phones is called 'Bluesnarfing'

- Bluesnarfing has huge potential for abuse because it leaves no trace and victims will be unaware that their details have been stolen

- The vulnerability exists in all bluetooth enabled devices, but handsets are particularly at risk because resources for functions such as menus are limited

A more insidious attack on bluetooth enabled phones is called 'Bluesnarfing' (continued)

- Object exchange (OBEX) protocol, which is a common method used by mobile devices to exchange information not implemented with authentication

- Minor modifications to the standard bluetooth stack used on a laptop can allow the operator to 'snarf'

- At risk are such information as address books, dialed call information and received call information

Cabir is a virus related to snarfing and has surfaced at the Live 8 concert and Helsinki's Olympic Stadium

- Isolated to phones running the Symbian operating system (OS) with the Series 60 user interface software, have the Bluetooth wireless communications feature enabled, set to listen for Bluetooth devices, and be within 30 feet or less of a phone infected with Cabir
- Requires active help of victim to answer “Yes” to download and install the Symbian Installation File (SIS) to their phone
- Cabir has little in the way of malicious payload. batteries will quickly discharge in as little as 30 minutes while the virus attempts to broadcast itself onwards.
- Switching off Bluetooth blocks transmission of the virus

Bluebug is an early vulnerability that was successfully demonstrated at the IKT 2004 Forum

- BlueBug attack takes only a few seconds and the victim can be totally unaware if they are not looking at the phone when the attack is executed

- The BlueBug security loophole allows commands to be issued via a covert channel to the vulnerable phones without prompting the owner of the phone

- At the CeBIT technology fair in Hannover, Germany there were about 1300 unique bluetooth devices which were advertising

- About 50 phones were proven to be vulnerable to this attack at the fair

Bluebug has the potential to expose personal information and disclosure of financial data

- This security flaw allows number of actions to be done to the target phone when it is attacked via bluetooth:
  - initiating phone calls
  - sending SMS to any number
  - reading SMS from the phone
  - reading phonebook entries
  - writing phonebook entries
  - setting call forwards
  - connecting to the internet
  - forcing the phone to use a certain service provider

Bluebug also can allow the targeted phone to act as a ‘bug’

Eavesdropping can be accomplished by covertly calling another phone

- A victim’s phone is called as they pass by the attacker who uses an anonymous prepaid-card phone
- When the call is completed, the attacker can listen to the victim’s conversations until the victim’s phone is hung up

Cyber criminals grab a copy of Steamy Windows, then add a backdoor Trojan horse

- Steamy Windows is a free program that Chinese hackers have modified, then re-released into the wild
- The reworked app is then placed on unsanctioned third-party "app stores"
- Unsuspecting or careless Android smartphone users find it, download it and install it
- The Trojan planted by the malware-infected Steamy Windows can install other applications, monkey with the phone's browser bookmarks, surreptitiously navigate to Web sites and silently send text messages
- The Trojan sends SMS [short message service] messages to premium rate numbers for which the hackers are paid commissions

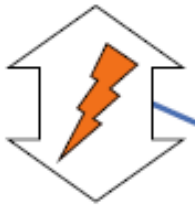
GSM encryption has been cracked

- All GSM networks use a variation of a 21 year old 64-bit A5/1 code to encrypt voice and SMS data flowing across the network
- A combination of 2 terabytes worth of hard drives and one field programmable gate array (FPGA) -- which cost about $1,000 to construct allows GSM to be cracked in under 3 minutes
- Brute force attack on A5/1 and create a large look-up table that will serve as the code book
- A commercial-grade version of the tool in the second quarter that cracks calls in 30 seconds
- Some GSM networks reuse the same key for 16 calls, an attacker could access all of those calls

Weaknesses of the GSM encryption exposes growing number of potential exposures

GSM is constantly under attack:

- A5/1 cipher shown insecure repeatedly
- Lack of network authentication allow MITM intercept (IMSI Catcher)



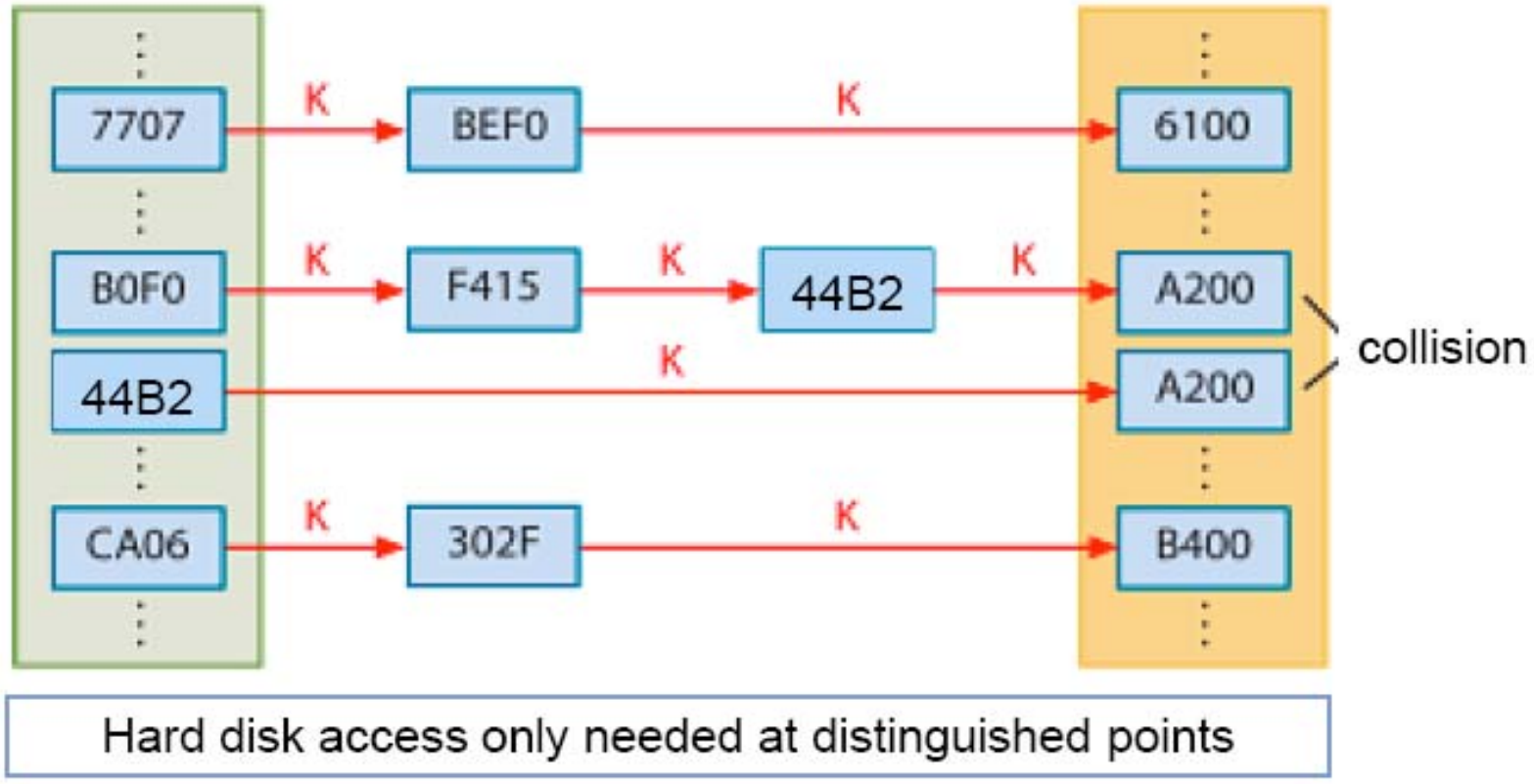
Security expectations divert from reality

However, GSM is used in a growing number of sensitive applications:

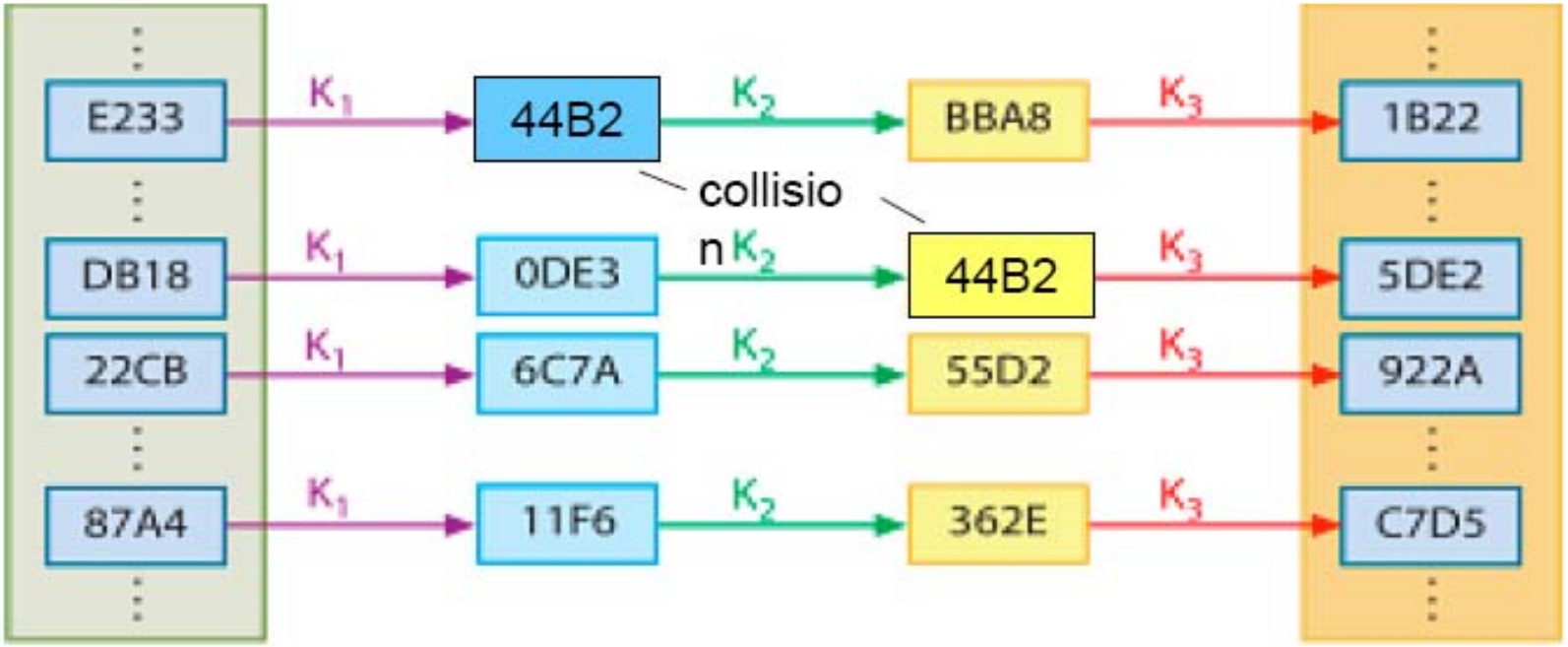
- Voice calls, obviously
- SMS for banking
- Seeding RFID/NFC secure elements for access control, payment and authentication

- To rectify the perception of GSM's security, we demonstrate its weaknesses
- The community has computed the cryptographic base for a public demonstration of cracking GSM
- This presentation details motives, approach and next steps of the "A5/1 Security Project"

Distinguished table lookups speed the cracking process by reducing disk access



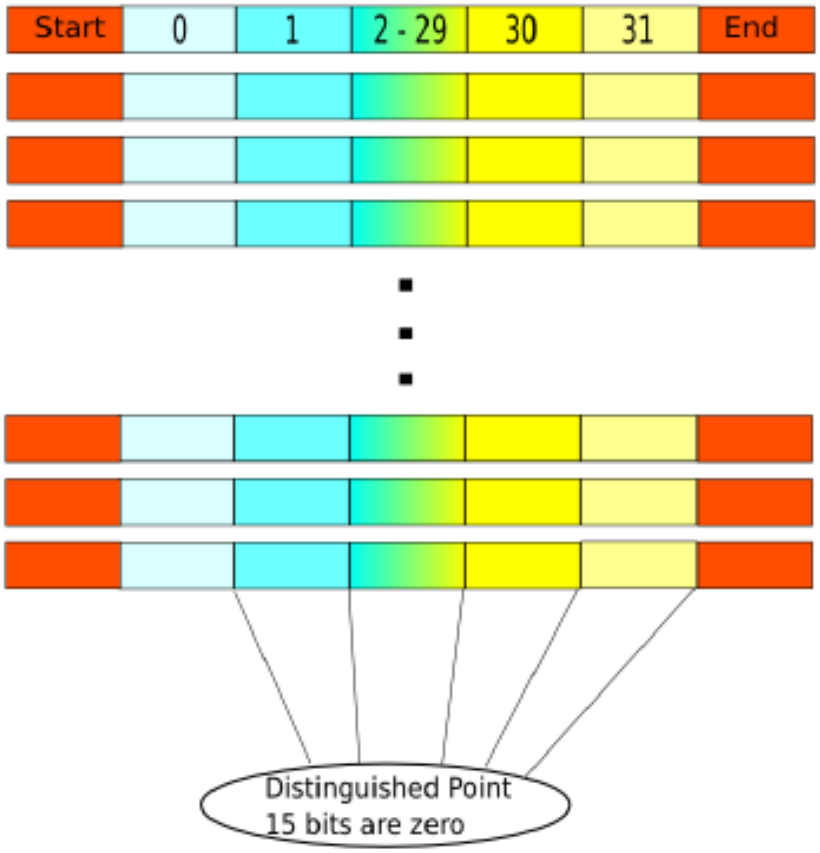
Rainbow tables have reduced collisions so their output is more accurate



Rainbow tables have no mergers, but an exponentially higher attack time

A combination of two table types makes the optimum encryption cracking process

Distinguished point tables save hard disk lookups while Rainbow tables mitigate collisions



Assumptions

- 2 TB total storage
- 99% success rate when collecting all available keystream*
- 50% success rate when only obvious keystream is used
- Near real-time decryption with distributed cracking network

The most resource efficient table for A5/1 is:

- 32 DP segments of length 2^{15}
- Merged into one rainbow
- 380 such tables with height $2^{28.5}$ needed

An entirely new attack is aimed at the baseband radio processor

- Bugs have been found in the way the firmware used in chips sold by Qualcomm and Infineon Technologies processes radio signals
- First a fake cell phone tower is set up
- Then a target phone is convinced to connect to it
- Then malicious code is delivered
- This was demonstrated at the BlackHat Conference in late January 2011

Once malware is delivered the phone is a bot under orders of the hacker

- This new technique used on an iPhone and an Android device, converts it into clandestine spying systems
  - GPS location
  - Camera
  - Record audio on the phone, store it in RAM and then transmit it
- The attack demonstrated injects messages into layer three of the GSM stack, which then turns on the auto-answer function on the affected phones

Smartphones with WiFI are subject to man-in-the-middle exploits

- A netbook computer is set up a wireless access point
- Phones, when not connected to wi-fi, transmits what is called a probe requests looking for networks which it has used previously.
- Probe requests are essentially a loud shout - is there any wi-fi access point near me with the name ‘xyz'?
- Once the device is connected to the fake access point its user is able to browse the web as normal
- Unbeknown to the user, the web traffic is being transmitted through the hacker’s computer
- A program examines the traffic between users and websites, looking for data containing cookies
- Among the cookies are small pieces of code which smooth our path to frequently-visited sites
- The password would not be needed; because, the cookie allowed the hacker to masquerade as the victim

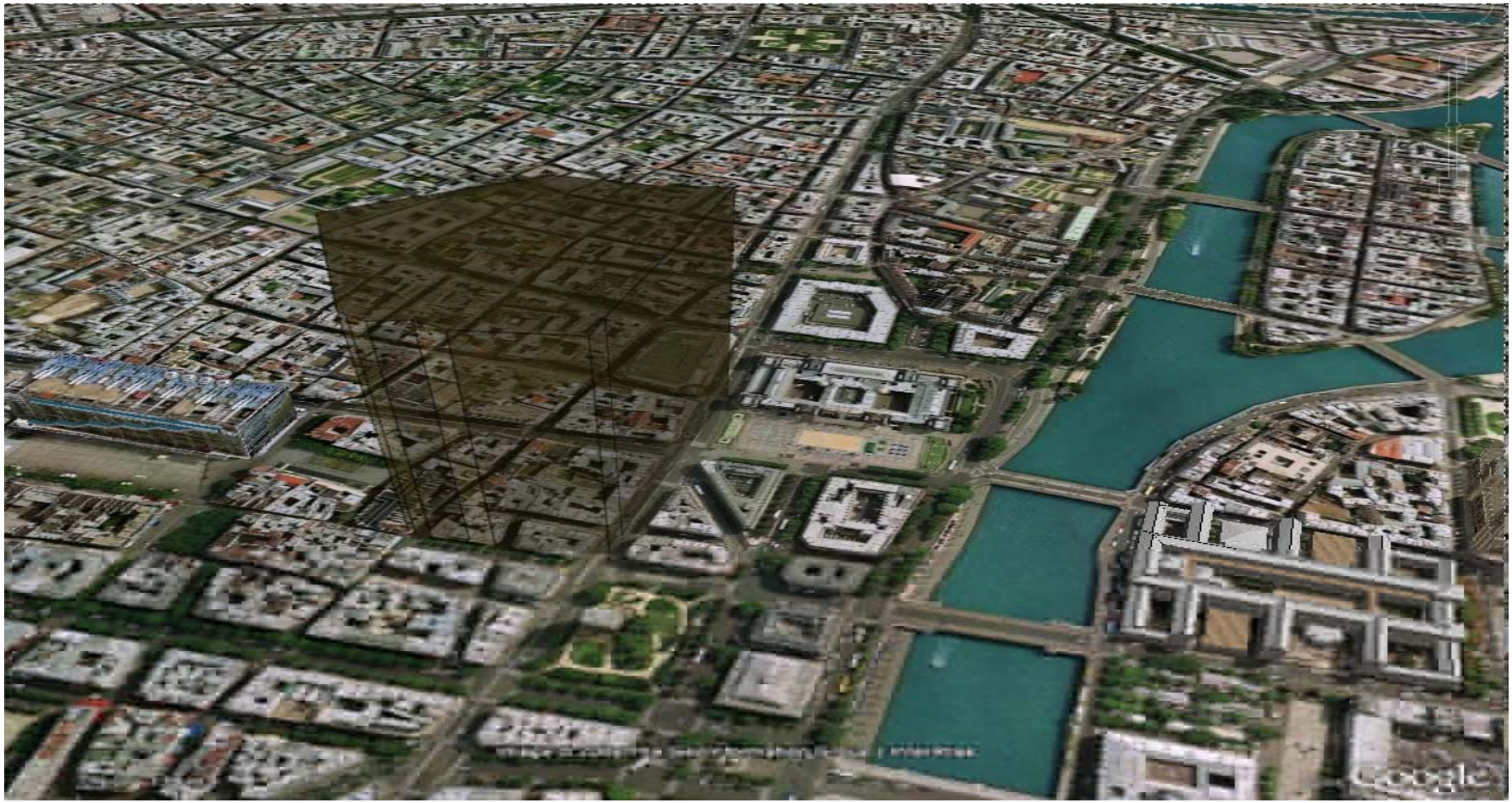
Something as innocent as a business card can be the hackers key

- Once they have a phone number — yours for instance —
- A hacker can easily determine your name by taking advantage of a vulnerability in the Caller ID system
- Using special software, they can "spoof" a call — that is, make a call that appears to the phone company as though it's coming from your number
- They can then call themselves using your number and watch as their Caller ID device lights up with your name
- Once a name is the one associated with a number, they can query the cellular network to see where that phone is at that moment
- After enough time, this bit of digital spycraft will yield a fairly clear picture of where a target goes and when

Using available technology a hacker can determine where a phone (and its user) is located

- Advanced systems determine the sector in which the mobile phone resides and roughly estimate also the distance to the base station
- Further approximation can be done by interpolating signals between adjacent antenna towers
- Qualified services may achieve a precision of down to 50 meters in urban areas where mobile traffic and density of antenna towers (base stations) is sufficiently high
- Rural and desolate areas may see miles between base stations and therefore determine locations less precisely

How the ‘cell’ looks interposed over a city block map



A combination of freeware, a PC and a smartphone can let you slave other smartphones

- Recent growth of smartphones, particularly those that run Internet Explorer have shown weaknesses in SMS (short message service)
- Hack, known as 'Midnight Raid', takes its name from the time of day it preys on its victims, many of whom are business users with unsecured smartphones
- SMS automatically opens Internet Explorer on the victim's phone, starts up an executable file, steal some data off the victim's smartphone and send it back to the hacker's phone via SMS

Common method of attack is via malware embeded in a web site

- There should never be scripts or iframes at the end of the html tag and this looks like that the website has been infected with an automatic script that adds specific code (in this case js code + iframe) at the end of each files present in a website
- Most probably also other websites present in the same server where is hosted the infected website could have the same dangerous scripts injected in all of their files, this is a common symptom of a mass infection

ZeuS network initiated some social engineering operations to get the phone number and phone model of its victim to steal from their accounts

- Based on that info, it sends an SMS with a link to the appropriate version of the malicious package (a Symbian package for Symbian phones, a BlackBerry Jar for BlackBerry phones etc)
- Aimed at defeating SMS-based two-factor authentication that most banks implement today to confirm transfers of funds initiated online by their end users, and that currently impedes the plunging of infected users' online accounts by Zeus masters
- Note: although it was possible before, with man-in-the-middle attacks, it required the victim to initiate a financial transfer in the first place

SymbOS/Yxes, web servers are used to distribute platform-specific malware

- The Symbian version is correctly signed, using the Express Signed program, once more. Symbian has been notified, but meanwhile, please beware this certificate hasn't been revoked yet:

```
Serial Number: 61:f1:00:01:00:23:5b:c2:79:43:80:40:5e:52
C=AZ, ST=Baku, L=Baku, O=Mobil Secway, OU=certificate  1.00,
OU=Symbian Signed ContentID, CN=Mobil Secway
```

The malware creates its own malicious database on the phone, where it stores all information it steals (contact first and last names for instance, phone numbers) and needs
This database is named NumbersDB.db, and contains 3 tables: tbl_contact with 4 columns: index, name, descr, pb_contact_id. tbl_phone_number with 2 columns: contact_id, phone_number and tbl_history with 6 columns: event_id, pn_id, date, description, contact_info, contact_id
The malware searches those tables using standard SQL queries

SymbOS/Yxes, web servers are used to distribute platform-specific malware to victims (continued)

- The malware sends SMS messages. In particular, it sends a message to a phone number located in the United Kingdom to notify that the malware has been successfully installed (“App installed ok”)

```
27/09/2010","12:09","Short message","Outgoing","App installed ok","+44778xxxxxxx"
(NOT SENT - OFFLINE)
```

- The malware also seems to be able to answer to a few commands such as ‘set admin’, which might be particularly dangerous.
- Anyone sending a “set admin” SMS to your infected phone may be able to take control of it

Safari Bug Being Used to Jailbreak iPhones opens door for other attacks

- A Web site set up to help iPhone users jailbreak their devices is using a flaw in the way that the iPhone handles PDF files to escape the phone's sandbox security function and enable users to load applications that aren't in Apple's official App Store
- The same flaw could easily be used to install malicious software in drive-by download attacks
- The iPhone has several security protections in place that are designed both to prevent malicious code from running on the device and also to stop users from loading unapproved apps on the phone

Researchers at Pwn2Own hacking competition exploited a Safari bug that circumvented DEP to steal SMS data

- *DEP* (Data Execution Prevention) is intended to prevent data such as PDFs from being used to deliver malicious code
- The means was creating a file, a PDF–that tricks an application into doing things it's meant to do, but rearranging them to accomplish unauthorized tasks
- Text message stealer was limited by the iPhone's sandboxing security measure, which prevents applications from gaining access to the operating system as a whole

PDF exploits are becoming more and more sophisticated

- In particular, they often rely on creative techniques to avoid detection and slow analysis
- Consider this PDF that contains a JavaScript section with the following code (simplified a little):

```
var s = '';

new Function(decode(2, 35))();

function decode(page, xor){
     var l = this.getPageNumWords(2);
     for(var i = 0; i < l; i++){
          word = this.getPageNthWord(page, i);
          var c = word.substr(word.length- 2, 2);
          var p = unescape("%"+ c).charCodeAt(0);
          s += String.fromCharCode(p ^ xor);
     }
     return s;
}
```

PDF exploits are becoming more and more sophisticated (continued)

- This code creates an anonymous function, sets its body to the return value of the decode function, and then executes it
- The interesting part is in the decode function. This function gets the number of words contained in the third page of the document via the getPageNumWords function (recall that pages are 0-based in the PDF API). It then loops through all the words in that page (via the getPageNthWord function) and manipulates them. Let's see how the third page looks like:

```
11 0 obj
<<
/Length 23892
>>
stream
2 J
0.57 w
BT /F2 1.00 Tf ET
0.196 G
BT 31.19 806.15 Td [ <kh29 kh2a kh55
...
kh4e kh46 kh0a kh03 kh58 kh2e kh29> Tj ET
...
endstream
endobj
```

PDF exploits are becoming more and more sophisticated (continued)

- The page is stored as a stream. Its contents comprise a number of directives and the actual textual content
- For example, BT indicates the beginning of the text and, conversely, ET marks the end of the text; 31.19 806.15 Td specifies the position of the text on the page; and Tj is the display text operator
- The actual textual content is the string starting with kh29
- Going back to the decode routine. It is clear that it extracts the last 2 characters from each word (e.g., “29” from “kh29”),
- Interprets them as hex numbers (e.g, 0x29), xors them with 35 (e.g., 0x29 ^ 35 = 10), and finally obtains the corresponding character (e.g., “\n”)

PDF exploits are becoming more and more sophisticated (continued)

- The result of this deobfuscation is the actual exploit code, which targets 4 different vulnerabilities
- The exploit code has one last trick, which it uses to hide the URL from where the malware is to be downloaded:

```
var src_table = "abcd...&=%";
var dest_table= "eAFS...=iZR-";
function get_url(){
    var str = this.info.author;
    var ret = encode_str(str, dest_table, src_table);
    return ret;
};
```

PDF exploits are becoming more and more sophisticated (continued)

- Notice the info.author property
- The get_url function essentially performs a simple substitution decryption of the author metadata.
- Let's see what is contained there:

```
17 0 obj
<<
/Author
(-Jj.gw-Jjrj.-JWMyD-JjTWM-JjngM-JgkjW
 ...
 -JjrWk-Jjrgw-JgTyM-JyOg.-JWgyg-Jgngw-JgYgY-JyygM-Jy.yC)
>>
endobj
```

After decoding, one finally gets the malware URL

Defending against attacks

- Setting a password is the simplest way to keep your data safe if your phone goes AWOL
- If you don't recognize a number that's calling when you look at your caller ID, and you're not expecting a call, let the call go to voicemail instead of answering.
- If you're walking around busy public spaces and you're not using your phone's WiFi connection or GPS, turn off the WiFi radio and GPS features.
  - Not only will radio limiting prevent unwanted connections, but it'll also keep your battery charged longer.

There are also antivirus software for the smartphones

- Prevents malicious threats from entering the smartphone and compromising privacy
- Blocks short text and multimedia messages from unknown senders
- Blocks snoopware from turning on the phone's camera
- Prevents intruders from entering and exporting data from the mobile phone
- Provides firewall blocks to hackers, intrusions, and denial-of-service attacks

QUESTIONS?
Please remember your session evaluation
Your Feedback is Important to Us

39

Sources

- "**War Nibbling: Bluetooth Insecurity"**, Ollie Whitehouse
- Bluebug: http://trifinite.org/trifinite_stuff_bluebug.html
- **Coming soon: A new way to hack into smartphones http://www.infoworld.com/d/security-central/coming-soon-new-way-hack-smartphones-694?page=0,0**
- **"Hack into a smart phone? It's easy, security experts find"**
- **"Smartphone Attacks and Hacking: Security Threats and Trends 2011"**