# News Corp. and Mobile Hacks

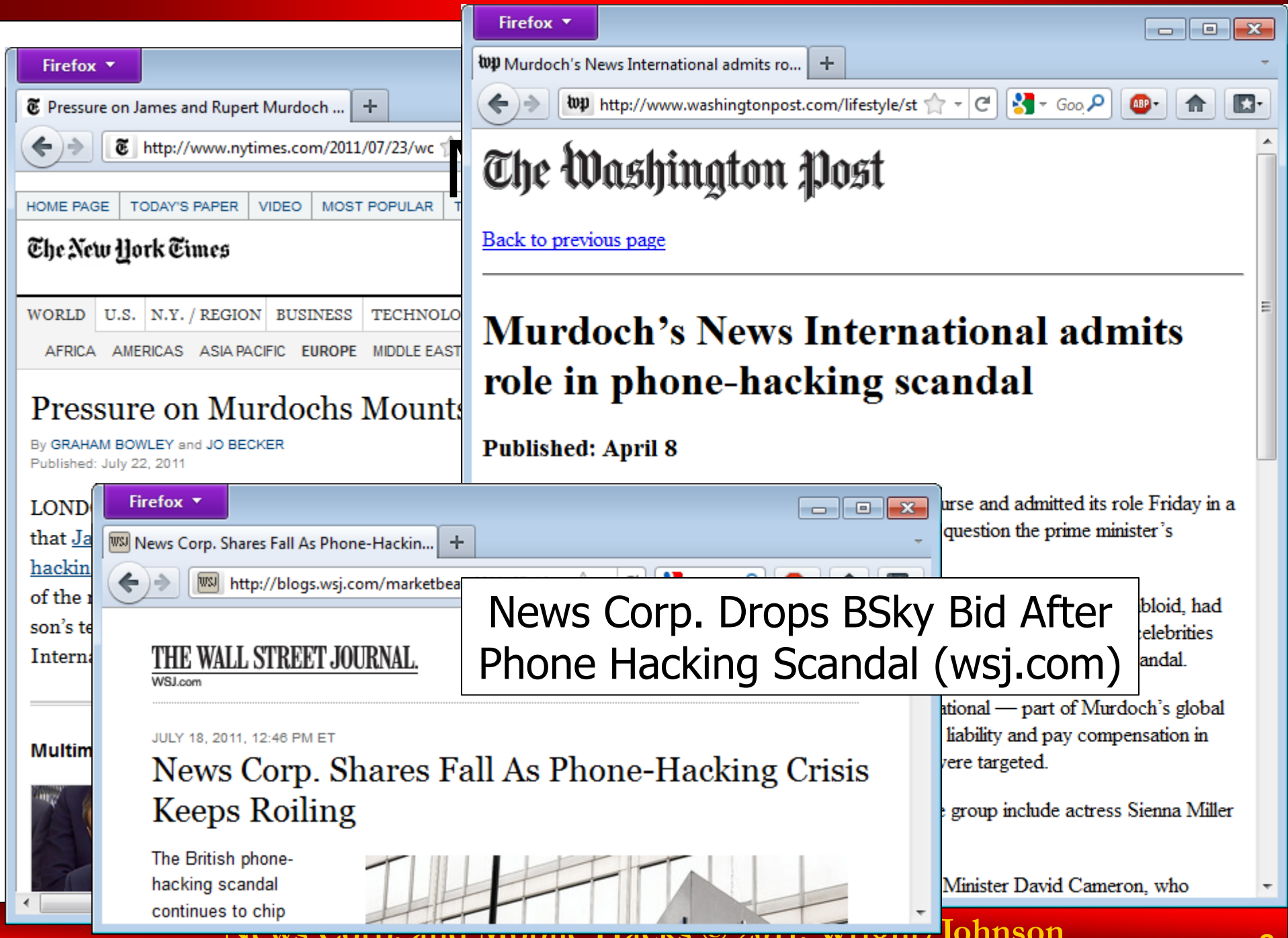
Joshua Wright
jwright@willhackforsushi.com

Kevin Johnson
kevin@secureideas.net

The SANS Institute

# Outline

- News Corp. and Mobile Phone Hacking
- Bluetooth Headset Eavesdropping
- Attacking Smart Phone Networking
- Mobile Phone Privacy Attacks
- Manipulating Caller ID for VM Access
- Conclusion




News Corp. Drops BSky Bid After Phone Hacking Scandal (wsj.com)

# Mobile Device Attacks

- Increasingly popular target for adversaries
  - Tremendous information disclosure opportunities (calendar, email, contacts)
- Immature from a security perspective (patching, maintaining)
- We teach mobile device attacks at SANS
  - Raising awareness, developing defensive and offensive skills

# Outline

- News Corp. and Mobile Phone Hacking
- Bluetooth Headset Eavesdropping
- Attacking Smart Phone Networking
- Mobile Phone Privacy Attacks
- Manipulating Caller ID for VM Access
- Conclusion

# Bluetooth Headsets

- Ubiquitous accessory for mobile phones
  - Motivated  by convenience and hands-free driving laws
- Very limited device, preference for small, simple configuration
  - Fixed PIN of "0000" most common deployment
- Attacker opportunity for eavesdropping
  - Not intercepting active conversations, but recording/injecting audio while not in a call

# Video Demonstration

# Outline

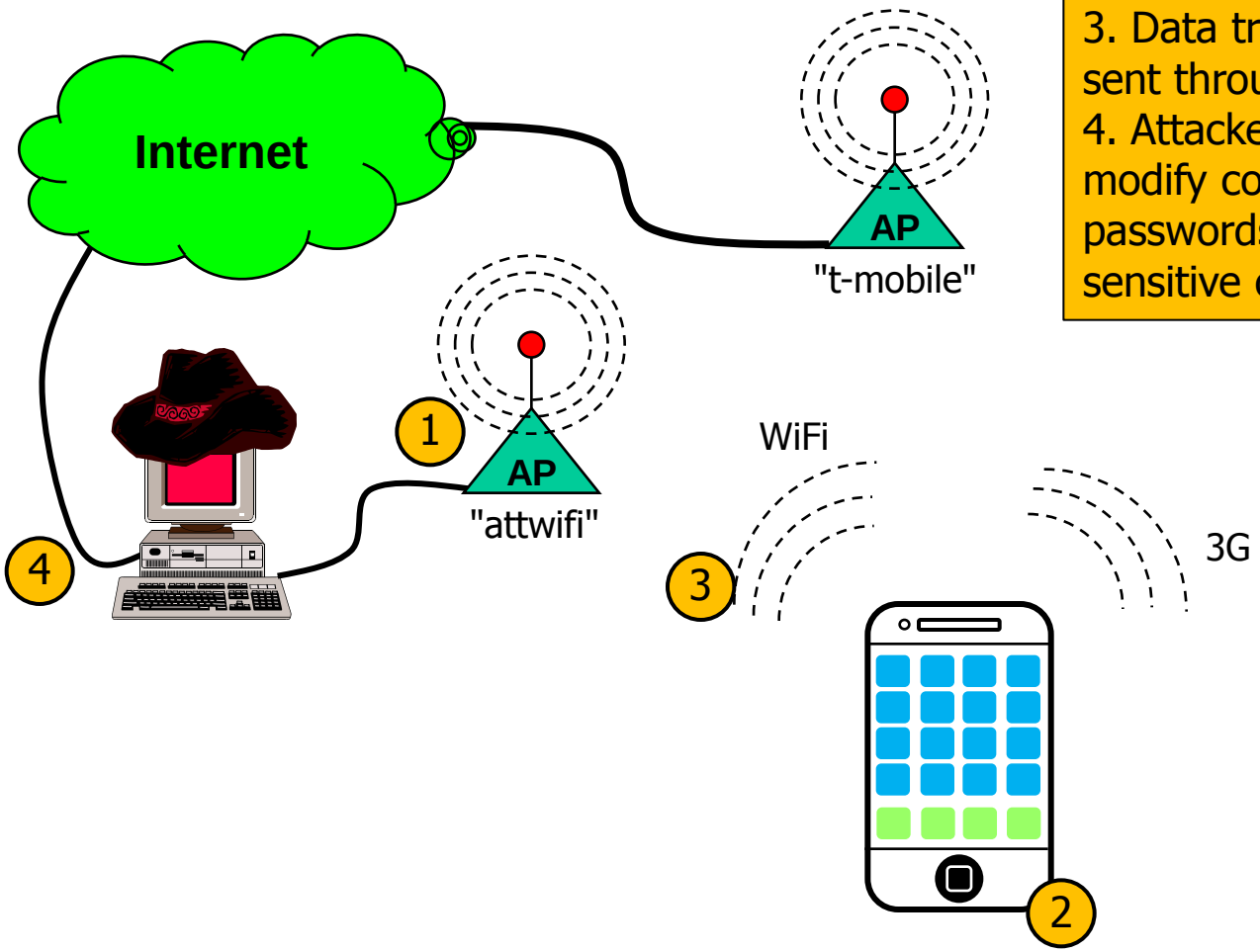
- News Corp. and Mobile Phone Hacking
- Bluetooth Headset Eavesdropping
- Attacking Smart Phone Networking
- Mobile Phone Privacy Attacks
- Manipulating Caller ID for VM Access
- Conclusion

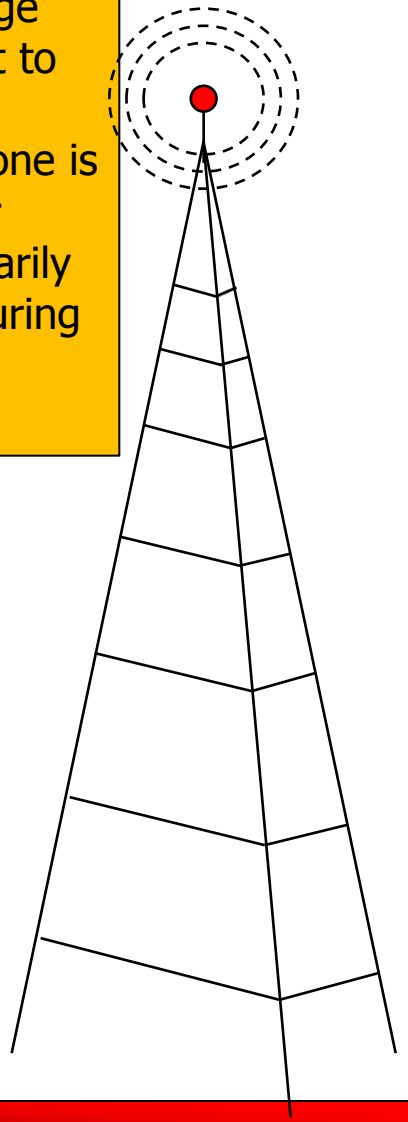
# Smart Phones and WiFi Hotspots

- Many smart phones will automatically connect to WiFi hotspots
  - Carriers are motivated to offload data traffic to a less-expensive medium
- Hotspot networks are unauthenticated
  - Can be impersonated by an attacker
- Once on the attacker's hotspot, multiple attacks are possible

# Hotspot Impersonation

1. Attacker impersonates "attwifi" with mobile AP, connected to the Internet
2. iPhones within range automatically connect to attacker
3. Data traffic on iPhone is sent through attacker
4. Attacker can arbitrarily modify content, capturing passwords and other sensitive content.



# Outline

- News Corp. and Mobile Phone Hacking
- Bluetooth Headset Eavesdropping
- Attacking Smart Phone Networking
- Mobile Phone Privacy Attacks
- Manipulating Caller ID for VM Access
- Conclusion

# Mobile Targets

- Attackers target devices to get private information from victims
  - Mobile platforms are currently an easy target
- The more information the attacker has, the more attack opportunities
  - Information regarding the owner, where he is and how the device connects is valuable

# Mobile Phone CNAM Lookup

- Telephone service has a feature similar to reverse DNS known as CNAM lookup
  - Allows us to get name and location information about a phone number
- Several free services with limited per-day lookups
  - Limits are based on source
- Commercial services available at $0.009 per query

# Carmen Sandiego Project

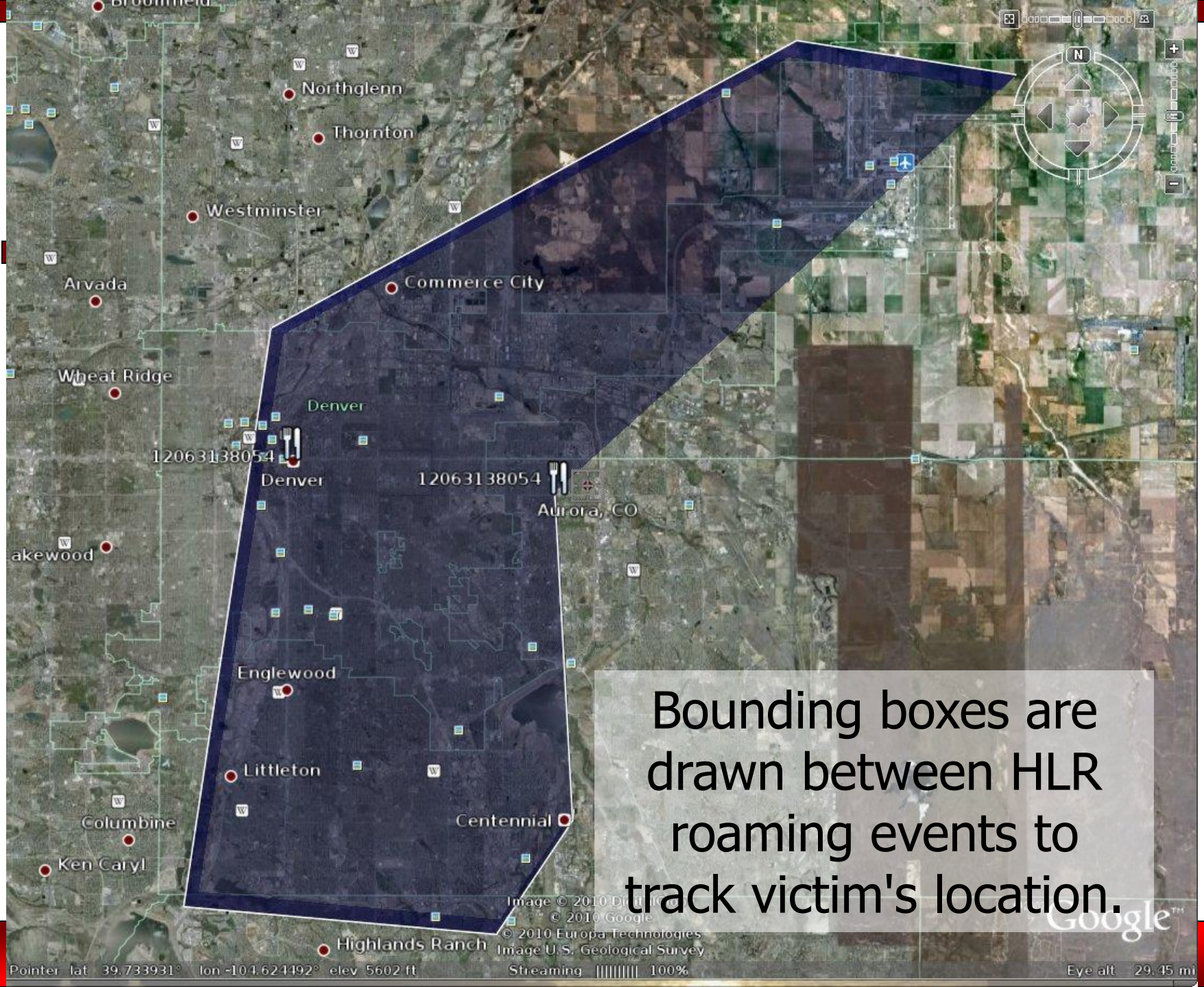
- Leverages software PBX with public provider intended for VoIP connectivity
- Researchers called *from* a software PBX *to* a software PBX
  - *From* caller spoofed their phone number to a search entity
  - Recipient logs call number and CNAM information
- Impersonated phone numbers for many exchanges to map our CNAM information

```
mysql> SELECT * FROM cnam_lookup WHERE cnam LIKE '%emb%' OR cnam LIKE '%govt%' OR
 cnam LIKE '%trac%' OR cnam LIKE '%shell%' OR cnam LIKE '%wits%' OR cnam LIKE '%p
aragon%' OR cnam LIKE '%moore%h%';
+------+---------------------+-----------+------------------+
| id   | date                | num       | cnam             |
+------+---------------------+-----------+------------------+
| 1284 | 2010-04-19 03:18:02 | 617[redacted] | MOORE RICHARD    |
| 1410 | 2010-04-19 13:16:28 | 303[redacted] | MOOREJOHN        |
| 2315 | 2010-04-19 17:00:38 | 407[redacted] | SATELLITE TRACK  |
| 2363 | 2010-04-19 17:05:26 | 407[redacted] | SATELLITE TRACK  |
| 2413 | 2010-04-19 17:10:00 | 407[redacted] | SATELLITE TRACK  |
| 2435 | 2010-04-19 17:11:48 | 407[redacted] | SATELLITE TRACK  |
| 2461 | 2010-04-19 17:13:57 | 407[redacted] | SATELITE TRACKI  |
| 2463 | 2010-04-19 17:14:08 | 407[redacted] | SATELLITE TRACK  |
| 2571 | 2010-04-19 18:48:47 | 202[redacted] | EMBASSY OF UKRA  |
| 3887 | 2010-04-19 23:52:46 | 713[redacted] | SHELL COMPANIES  |
| 3888 | 2010-04-19 23:52:52 | 713[redacted] | SHELL COMPANIES  |
| 3889 | 2010-04-19 23:52:58 | 713[redacted] | SHELL COMPANIES  |
| 3891 | 2010-04-19 23:53:11 | 713[redacted] | SHELL COMPANIES  |
| 4187 | 2010-04-20 00:18:48 | 713[redacted] | US GOVT F B I    |
| 4203 | 2010-04-20 00:19:33 | 713[redacted] | US GOVT F B I    |
| 4489 | 2010-04-20 21:03:48 | 202[redacted] | WITS3            |
| 4490 | 2010-04-20 21:04:12 | 202[redacted] | WITS 2001        |
| 4492 | 2010-04-20 21:05:03 | 202[redacted] | PARAGON SYSTEMS  |
| 4501 | 2010-04-20 21:07:46 | 202[redacted] | WITS 2001        |
| 4529 | 2010-04-20 21:13:23 | 512[redacted] | MOOREH           |
+------+---------------------+-----------+------------------+
20 rows in set (0.01 sec)

mysql>
```

# From Bad to Worse

- Several EU providers offer access to lookup cell phone information for SMS spamming
- For a nominal fee, attacker can identify the Home Location Register (HLR) for a given phone
- Attacker can identify:
  - If your phone is on or off
  - Who your cell phone provider is
  - The lat./lon. of the central switching center you are currently connected to (often, the city you are in)


Northglenn
Thornton
Westminster
Arvada
Commerce City
Wheat Ridge
Denver
12063138054
Denver
12063138054
Aurora, CO
Englewood
Littleton
Columbine
Centennial
Ken Caryl
Highlands Ranch
Bounding boxes are drawn between HLR roaming events to track victim's location.
Image © 2010 DigitalGlobe
© 2010 Google
© 2010 Europa Technologies
Image U.S. Geological Survey
Google
Pointer lat 39.733931° lon -104.624492° elev 5602 ft
Streaming 100%
Eye alt 29.45 mi

# Outline

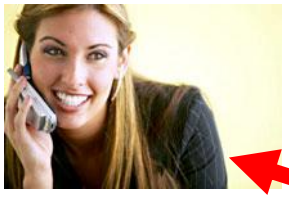
- News Corp. and Mobile Phone Hacking
- Bluetooth Headset Eavesdropping
- Attacking Smart Phone Networking
- Mobile Phone Privacy Attacks
- Manipulating Caller ID for VM Access
- Conclusion

# Caller ID Spoofing

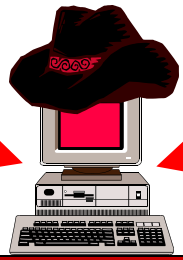
- Caller ID has become an integral part of how we use our phones
- Most people and systems *trust* the caller ID shown
  - Even though they don't know where it originates
- Attackers can use this *trust* to gain access to sensitive information
- An attacker can perform the spoofing via various means
  - Commercial services are available
  - PBX or VoIP systems also can be used

# Scenario 1: Three Way Calling

- Eavesdropping on conversations is potentially a source of information
  - People *trust* that calls are private
- An attacker creates a three-way call
  - Spoofing each of the other caller's ID
  - "Hello?", "Hello?". "You called me?", "No, you called me". "Weird, so I wanted to talk to you about this project…"



**Victims don't realize they weren't called**

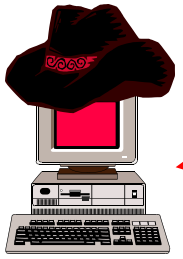


**Attacker generates a 3-way call spoofing each side's caller ID**

# Scenario 2: Voicemail Access

- AT&T, Sprint and T-Mobile voicemail allows access without a password
  - Access permission is based on caller ID
- An attacker can spoof caller ID to gain access to voicemail
  - Listen to and delete any message on the system

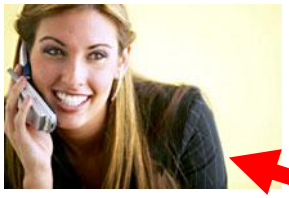
**Attacker spoofs caller ID to gain access to voicemail**



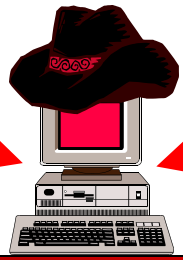

T-Mobile

# Scenario 3: Three Way Call into Voicemail

- Some voicemail providers require PIN authentication
  - Inconvenient for the attacker
- An attacker creates a three-way call
  - Spoofs the victim's number to the voicemail
  - Spoofs the voicemail's number to the victim
- The victim instinctively enters their PIN
  - The attacker disconnects the victim and retains access to the voicemail



**Victims don't realize they weren't called**

**Attacker generates a 3-way call spoofing each side's Caller ID**

verizon

# Outline

- News Corp. and Mobile Phone Hacking
- Bluetooth Headset Eavesdropping
- Attacking Smart Phone Networking
- Mobile Phone Privacy Attacks
- Manipulating Caller ID for VM Access
- Conclusion

# Conclusions

- Mobile devices are everywhere
- Most of the issues are based on the device or user *trusting* too much
  - Most of the trust is built into the system
- Controls need to be built to help prevent these types of attacks (while retaining usefulness)
- Education is the best control
  - Teaching people the risks help prevent the attacks
  - Mobile device developers also need to be educated
  - Ethical hackers to evaluate impact, confirm exposure

# News Corp. and Mobile Hacks

Joshua Wright
jwright@willhackforsushi.com

Kevin Johnson
kevin@secureideas.net

The SANS Institute