



# Weaponizing the Nokia N900 (and some other stuff...)

Shawn Merdinger

TakeDownCon, Dallas, TX, USA

19 May, 2011



# Thoughts so far....

- Nice conference
- Solid speaker line-up
- Little smaller, more intimate, get to meet folks
- Good breaks, food, coffee
- Kudos to Leonard and Joyce 😊

# Obligatory Speaker Slide

- Network security analyst at University of Florida Academic Health Center & Shands Hospital
- Former Cisco Systems, Tippingpoint
- As independent security researcher
  - Reported to CERT/CC and US-CERT vulnerabilities in electronic door access control systems, VoIP phones, SCADA HMI...
  - *Limited* availability for product security evaluations
    - Typically under-NDA in exchange for donation to EFF

# Talk Objectives

- Weaponizing consumer grade gear
  - Nokia N900
  - Fonea 2100
  - Surprise device
- Goals
  - Review of several tools and attack vectors
  - Espionage and legitimate pen-testing
  - Focus on technical capability
  - Raise awareness
  - Demo



# Re-Boxing the Apple iPod

- Will not cover iPod for a number of reasons
  - Apple too controlling of hardware/software
- If you're determined...
  - Thomas Wilhelm's DEFCON 17 preso
    - [http://www.metacafe.com/watch/5815191/defcon\\_17\\_hacking\\_with\\_the\\_ipod\\_touch\\_2011/](http://www.metacafe.com/watch/5815191/defcon_17_hacking_with_the_ipod_touch_2011/)
  - Hakin9 Tutorials
- My renewed interest...
  - Joe McCray's excellent preso from yesterday 😊

# Apologies to the Apple FanBoys...



# Fonera 2100

- La Fonera 2100 wifi access-point
- Fon
  - Spanish company
  - Community-oriented: share wifi, get wifi on the road at 3 million worldwide hotspots
  - Low cost, find on eBay
  - Newer Fons, but 2100 is “classic”



# Weaponizing the Fon 2100

- Easiest to use Jasager
  - Simple re-flash firmware
  - OpenWrt based image
- Get you several things
  - Nice, clean Web interface
  - Framework, tools, scripts to set-up for attack
- Pairs *very well* with BackTrack
  - Easiest way to weaponize a wifi AP
  - With BackTrack, a solid learning platform





# Weaponizing the Fon 2100

- Karma
- Jasager scripts
  - Basic port scanning, probes
  - Customize and roll-your-own scripts
- Powerful with BackTrack
  - SSLstrip
  - SideJacking with Ferret/Hamster
  - SET (Social Engineering Toolkit)
  - Metasploit .....*'nuf said*



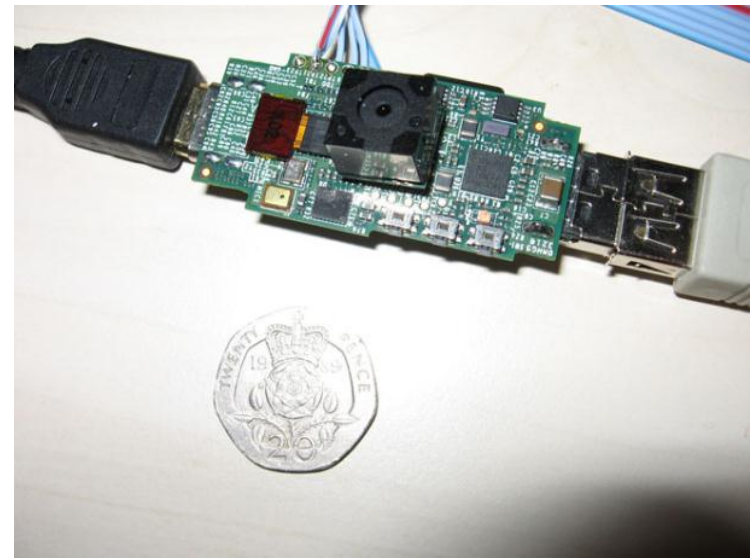
# Weaponizing the Fon 2100

- USB power hack
  - Run Fon off laptop USB port
    - See [Simple Nomad's "Hacking the Friendly Skies" talk](#)
  - Add Fon to a Sheeva / PwnPlug USB port
  - 5v Solar? Toss on target's roof?



# Surprise future device: Raspberry Pi

- \$25 embedded PC on USB stick
  - Target market: kids in developing countries
- 700 mhz chip, 128 RAM, HDMI, WiFi
- Browser, OpenOffice, Python, etc.
- <http://www.raspberrypi.org>



# SmartPhones

"The public doesn't realize the power they're holding in their hands...They have eyes and ears in their hand that can be exploited. It's intruding into their lives if it's not handled properly."

[FBI Special Agent in Charge Alan Peters](#)

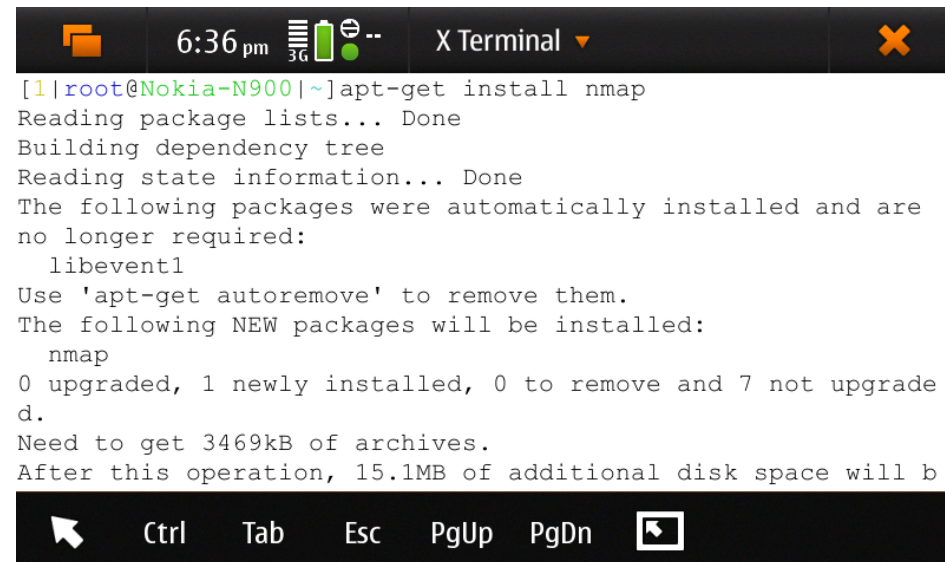
# Nokia N900



- Smartphone / Tablet
- Basic specs
  - OMAP 3430 ARM Cortex A8 @ 600mhz
  - 128 MB RAM, 1 GB virtual memory, 32 gb total memory, MicroSD
  - 802.11 Wifi, Bluetooth, 5MP camera back, 2MP camera front, GPS, USB
- Linux-based OS is standard
  - Maemo 5
  - MeeGo 1.2 (special developer edition for N900)

# N900 Apps

- Many stable, tested and free apps available
- GUI app manager or CLI via Debian APT
- Extra Debian repositories
  - Thousands more packages
- Solid community docs
  - [www.maemo.org](http://www.maemo.org)
  - Nokia supportive



```
[1|root@Nokia-N900|~]apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are
no longer required:
  libevent1
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
  nmap
0 upgraded, 1 newly installed, 0 to remove and 7 not upgrade
d.
Need to get 3469kB of archives.
After this operation, 15.1MB of additional disk space will b
```

# N900 Attack Tools

- Several of the “classic” security tools
  - Fyoder’s Top 100 list
- Maemo pre-packaged
  - A few examples
    - Nmap, Kismet, Ettercap, SSLstrip , Aircrack-NG
    - Pwnitter (like Firesheep for N900)
    - Trucrypt, OpenVPN, TOR
    - MobileHotspot
    - Wireshark / tshark

# N900 Challenges

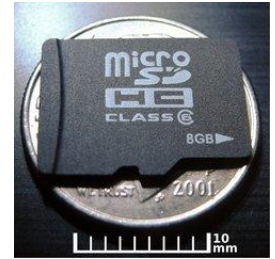
- Some security tools require an advanced kernel
  - Wireless attacks like injection, de-authentication
- Tools may require a certain level of tweaking
  - Linking libraries, conflicts, OpenSSL versions, etc.
- Not easy to install ALL the cool attack tools
- N900 is for you if you want the following...
  - a real Linux box in your pocket
  - to “get your geek on”
  - target specific pen-testing objectives
  - a “Poor Man’s [Immunity SILICA](#)”





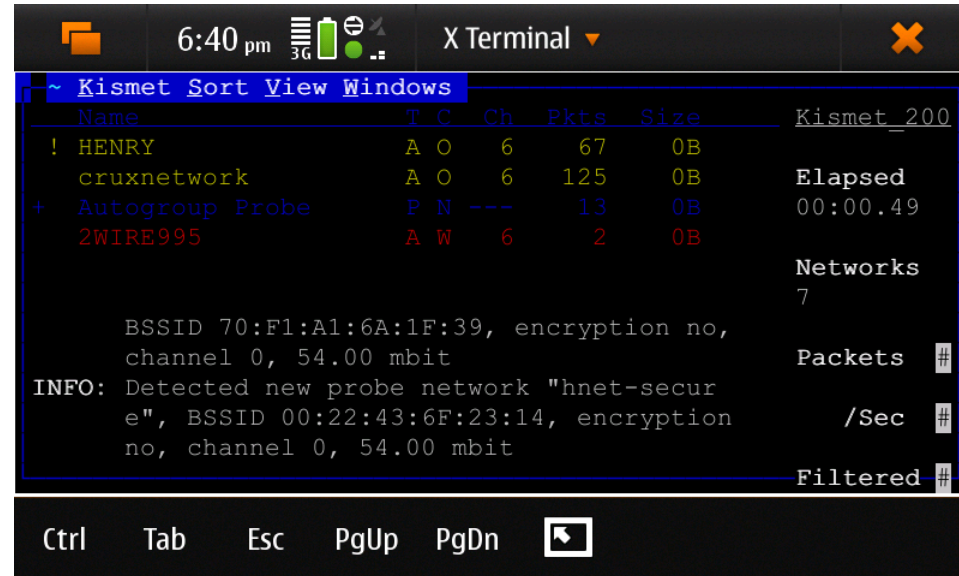
# N900 Data Exfiltration Capability

- On board storage is 32 GB
- MicroSD card up to 16 GB
- Via network paths
  - Evernote
  - DropBox
  - TOR
  - Stunnel
    - Tunnel over SSL
  - Iodine
    - Tunnel over DNS requests



# N900 Wireless Attacks

- Rouge AP
  - <http://zitstif.no-ip.org/?p=459>
  - With SET hotness!
- Packet injection
  - <http://zitstif.no-ip.org/?p=473>
- Mitm
  - Ettercap + SSLstrip
- Sniffing
  - Kismet
  - Tcpdump, ngrep, dsniff
- Can sniff GSM interface
  - Potential for GSM attacks? - Karsten Nohl's [26C3 GSM Sniffing](#)
  - Personal to do: crack my own A5/1 crypto key



The screenshot shows a terminal window titled "Kismet Sort View Windows" with a dark background. At the top, the system tray shows the time "6:40 pm", signal strength, battery, and network icons. The terminal content includes a table of detected networks and an informational message.

Name	T	C	Ch	Pkts	Size	Kismet_200
! HENRY	A	O	6	67	0B	
cruxnetwork	A	O	6	125	0B	Elapsed
+ Autogroup Probe	P	N	---	13	0B	00:00.49
2WIRE995	A	W	6	2	0B	

Networks  
7

BSSID 70:F1:A1:6A:1F:39, encryption no,  
channel 0, 54.00 mbit

INFO: Detected new probe network "hnet-secu  
e", BSSID 00:22:43:6F:23:14, encryption  
no, channel 0, 54.00 mbit

Packets #  
/Sec #  
Filtered #

Ctrl Tab Esc PgUp PgDn

# N900 Wireless Attacks

- [Wireless de-authentication attack](#)
- Via Simon @ KnowNokia.ca

“Sometimes I’m hanging with friends of mine who are big on Android and iPhone, and they make feeble attempts to **mock my N900**.”

*“That thing is a brick”. “Nice resistive touch screen. Made in the 90’s?”. “Does it have apps?”. “Hey, let’s all play iScrabble!”*

# ohnoez!

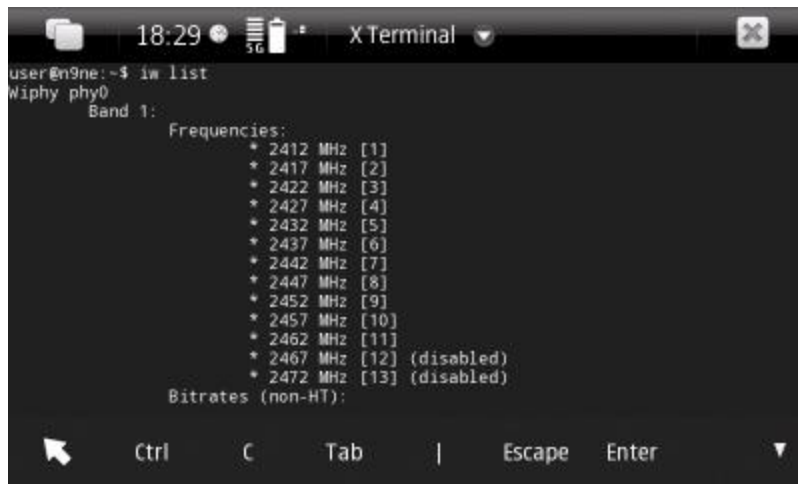


“I’ve learned to **quietly brush off their comments**, calmly finish replying to my text message and **enter a few key commands** and **place the N900 in my pocket.**”

```
08:26 25% 08:26 X Terminal
user@n9ne:~$ sudo aireplay-ng -0 0 -e RiVERDALE wlan0
08:26:14 Waiting for beacon frame (ESSID: RiVERDALE) on channel 1
Found BSSID "00:1D:7E:DD:7E:2F" to given ESSID "RiVERDALE".
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
08:26:14 Sending DeAuth to broadcast -- BSSID: [00:1D:7E:DD:7E:2F]
08:26:15 Sending DeAuth to broadcast -- BSSID: [00:1D:7E:DD:7E:2F]
08:26:16 Sending DeAuth to broadcast -- BSSID: [00:1D:7E:DD:7E:2F]
08:26:16 Sending DeAuth to broadcast -- BSSID: [00:1D:7E:DD:7E:2F]
08:26:17 Sending DeAuth to broadcast -- BSSID: [00:1D:7E:DD:7E:2F]
08:26:17 Sending DeAuth to broadcast -- BSSID: [00:1D:7E:DD:7E:2F]
```

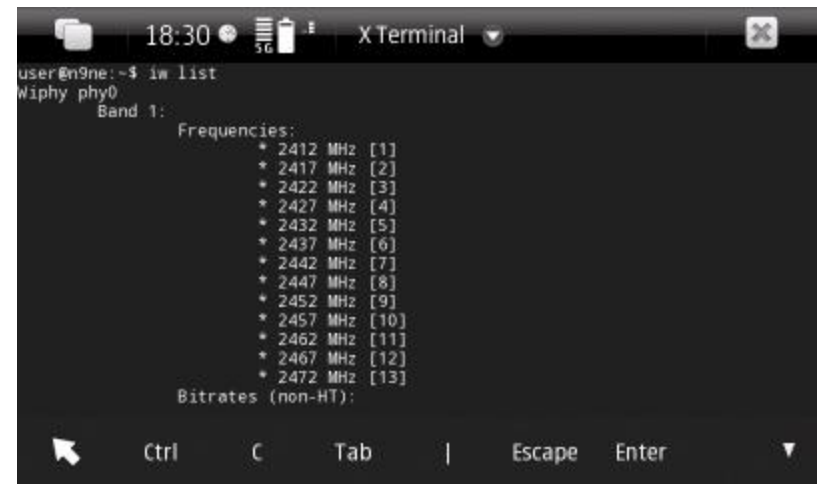
# Unlocking N900 Wifi Frequencies

“If you **live like a criminal** and run your 802.11 networks on the **upper channels of 12, 13 or 14** in North America...” – [Simon @ knowknokia](#)



```
user@n9ne:~$ iw list
Wiphy phy0
  Band 1:
    Frequencies:
      * 2412 MHz [1]
      * 2417 MHz [2]
      * 2422 MHz [3]
      * 2427 MHz [4]
      * 2432 MHz [5]
      * 2437 MHz [6]
      * 2442 MHz [7]
      * 2447 MHz [8]
      * 2452 MHz [9]
      * 2457 MHz [10]
      * 2462 MHz [11]
      * 2467 MHz [12] (disabled)
      * 2472 MHz [13] (disabled)
    Bitrates (non-HT):
```

Before



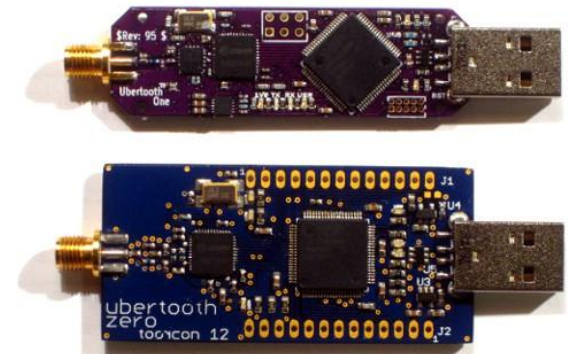
```
user@n9ne:~$ iw list
Wiphy phy0
  Band 1:
    Frequencies:
      * 2412 MHz [1]
      * 2417 MHz [2]
      * 2422 MHz [3]
      * 2427 MHz [4]
      * 2432 MHz [5]
      * 2437 MHz [6]
      * 2442 MHz [7]
      * 2447 MHz [8]
      * 2452 MHz [9]
      * 2457 MHz [10]
      * 2462 MHz [11]
      * 2467 MHz [12]
      * 2472 MHz [13]
    Bitrates (non-HT):
```

After

**Got Stealth?**

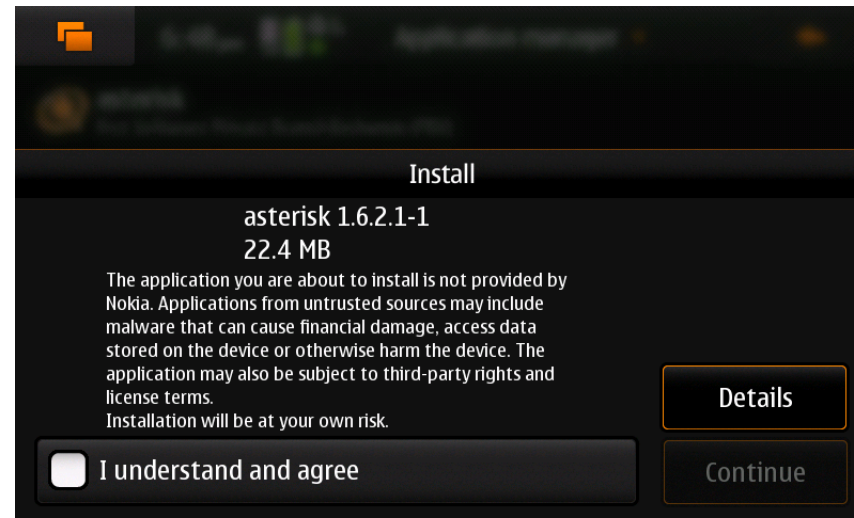
# Other Wireless: Bluetooth and Zigbee

- Two key projects to watch
  - USB dongle to N900
  - New attack capabilities
- [Ubertooth Project](#)
  - Michael Ossmann
  - Expanding Bluetooth attack surface exploration
- [KillerBee](#)
  - Joshua Wright, InGuardians
  - Zigbee attack framework
- Possible future statement?
  - “Dude, I just Pwned your smartmeter with my N900 and a Zigbee USB dongle”



# N900 VoIP Capabilities

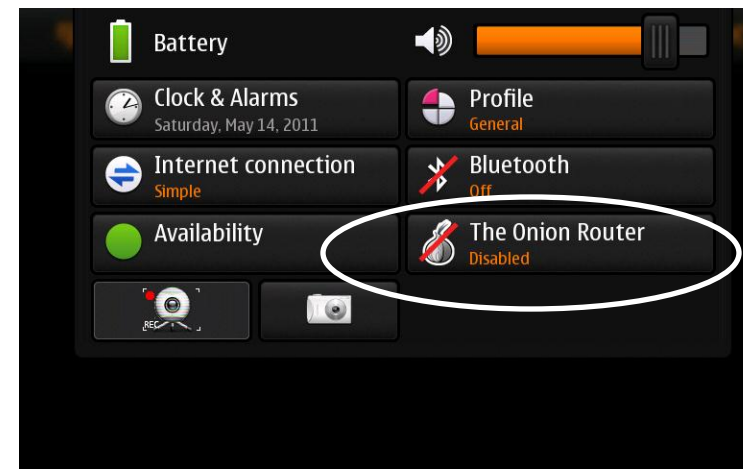
- VoIP capabilities nicely integrated
  - Skype by default
  - Google Voice app
  - SIP clients
- Asterisk – is that a telco in your pocket?
  - Opens many attack and stealth possibilities
  - See [VOIPSA security tool list](#)
    - SIP attacks, spitter
  - N900 + Asterisk
    - IPsec tunnel
    - IAX crypto
    - Zfone client





# Making the N900 (a bit more) Anonymous

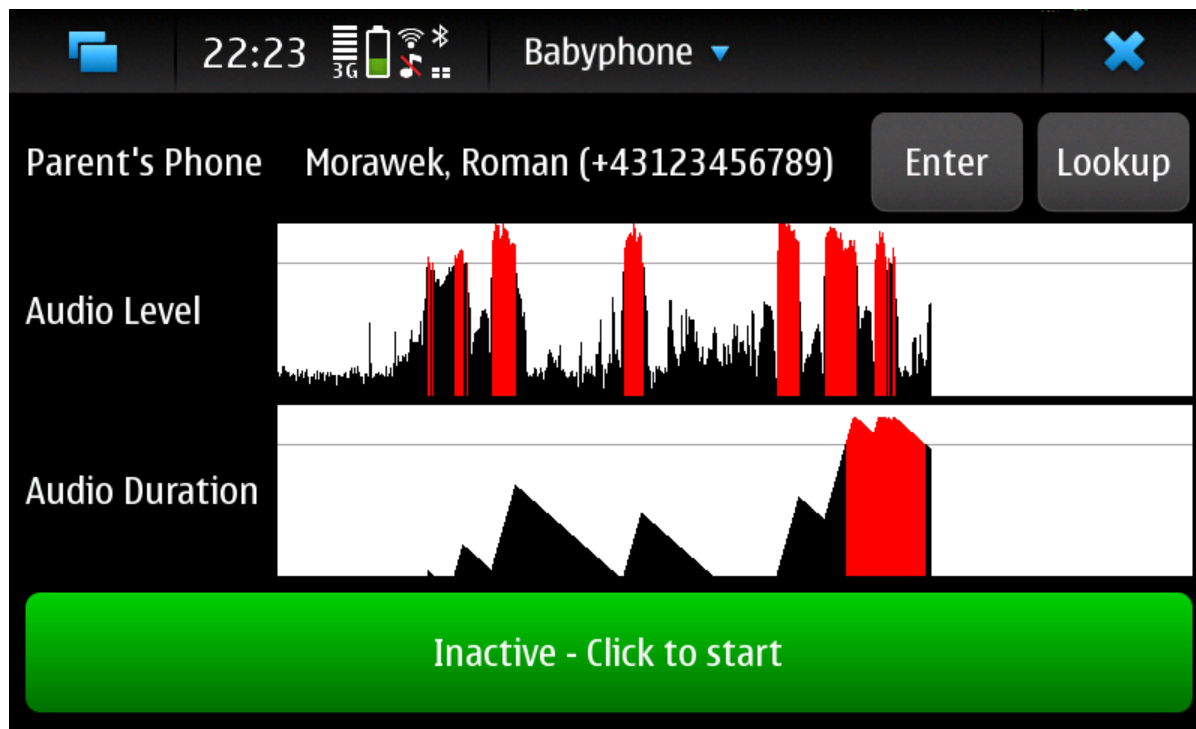
- [Steps Towards Anonymizing the Nokia N900](#)
- Via Kyle Young @ <http://zitstif.no-ip.org>
  - Disabling tracking
    - Location tracking (GPS and triangulation)
    - Auto connect to Internet
  - Enabling Privacy
    - TOR
    - ProxyChains
    - TruCrypt





# BabyPhone

- Simple, effective snooping tool
  - Measure audio level, hit threshold, start phone call
  - From babyroom to boardroom...



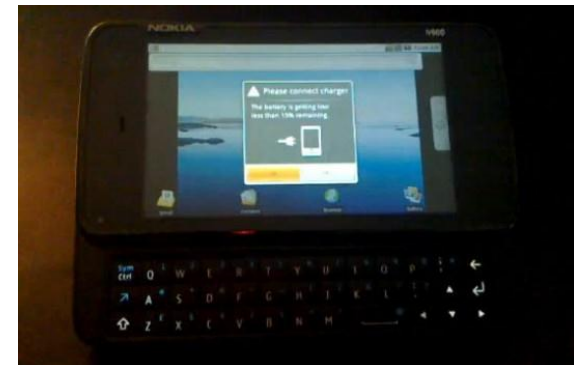
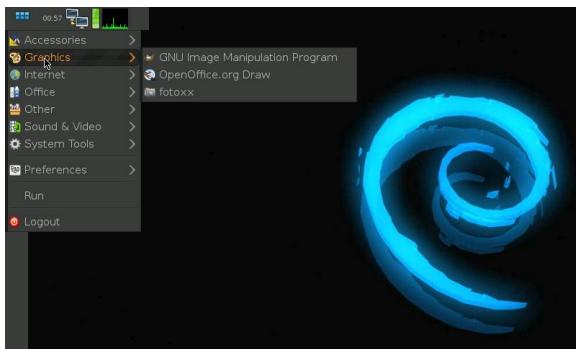
# LiveCast Mobile

- Stream live audio/video from N900 to web
- Others browse to webpage, listen or watch
- Flexible archive options
  - None, N900-only, Web-only, N900+Web
- Use front or back camera
- One-click and you're broadcasting



# Running another OS on N900

- [Easy Debian OS](#)
  - Like VMware w/ full Debian desktop
    - useful for tools like **full Nessus install**
- Backtrack 5 ARM version
- Dual Booting with Maemo and Android
- Roll-your-own OS! See [BackupMenu tool](#)



# Booting a PC with the N900

- USB cable + bootable image on MicroSD card
- Useful for on-the-spot support
- Potential evil espionage
  - Boot-up and walk away
  - Corporate office, Internet cafes, Kiosks
- Tested with BackBox Linux, Backtrack 5



# Buying a Pre-weaponized N900

- Lazy, in a hurry or want technical support...
- Best bets as of today
  - [PwnieExpress.com N900 PwnPhone](http://PwnieExpress.com)
  - NeoPwn project seems kinda AWOL



**PWNIE EXPRESS** ▼ View cart

News Products Documentation FAQ

### The PWN Phone

- A full pentesting suite for the Nokia N900
- Includes Aircrack, Metasploit, Kismet, GrimWEPA, SET, Fastrack, Ettercap, nmap, and more
- Custom pentesting screen with shortcuts to macchanger, injection on/off, etc.
- Built-in wireless card supports packet injection, monitor mode, and promiscuous mode.
- [More Info](#)

[Pwn Phone Screenshots](#)

# Demo: SMSCON

- Control N900 via SMS messages
  - Read Python scripts to see behind-the-scenes 😊
- Pre-configured scripts
  - Snap front cam picture, GPS Location and email to you
  - Lock screen, reboot, “wipe” device data
  - Start **reverse-ssh** session
    - Connect **back** to N900 root shell via external ssh server
    - For fun – hcitool bluetooth, espeak, Kismet
- Locate your stolen N900...*and* exact some justice
  - For lulz, see Zoz’s [“Pwned by the owner”](#) DEFCON 18

# SMSCON & SMSCON Editor

1:09 pm 3G SMSCON Configuration

General | Email | SSH | **Commands** | Init | Test

Check

Location

TrackOn

TrackOff

Camera

1:10 pm 3G SMSCON Configuration

General | Email | SSH | **Commands** | Init | Test

**INFO:**  
Test here some of the important parts to ensure that functionality is still valid with the newly updated settings.  
*Remember to press done after the completion of the tests*

1:09 pm 3G SMSCON Configuration

General | **Email** | SSH | Commands | Init | Test

email address

mailserver  port

username

password

1:08 pm 3G SMSCON Configuration

General | **Email** | SSH | Commands | Init | Test

Mobile number to contact:  GPS Settings:   Send Coordinates:

*will change on first command* *timeout* *method* *interval*

Send SMS Replies on:  Each Command  Battery Status  Slider Open

On First Command:  Lock Device  Silence the phone

General Settings:  Disable SMS replies  Unlock on new SIM

# Thank you!

- Thank you for your time 😊
- Contact me: [shawnmer@ufl.edu](mailto:shawnmer@ufl.edu)
- Watch infosecisland.com for more N900 posts
- gr33tz to [Kyle Young](#), [Simon@knownokia.ca](mailto:Simon@knownokia.ca)