Alexander Lash

TAKING BACK YOUR CELLPHONE

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - Light Modification
  - Heavy Modification
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

This Talk is NOT

- …an endorsement
- …a detailed guide
- …about a particular phone
  - …except when it is.
- …about carriers
  - …ok, fine, it's mostly about carriers.

More Disclaimers!

- This can break your phone
  - …keep backups
- This may break your contract
  - …if your carrier finds out
- Your carrier CAN and WILL charge you
  - …don’t use BitTorrent on a tether
- This targets the USA cell market
  - …your mileage will vary elsewhere

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - Light Modification
  - Heavy Modification
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

A Brief History of Tethering

- Of course you can! (circa 2000)
  - Cheap data cables, too!
- Try Customer Service. (circa 2002)
  - Two hours and a special password needed.
- You need the secret code. (circa 2004)
  - ##DIALUP? Thanks, Motorola!
- That's $60/month. (circa 2006)
  - Yes, it was free on your last phone.

Other “Innovations”

- Crippled Bluetooth
  - Buying headsets good, ringtones bad!
- Scare Tactics
  - The legendary $20,000 cellphone bill
- Media Transfer Fees
  - Yay DRM!
- Locked Application Platforms
  - Yay $10 Solitaire!
- …and many more.

In Memoriam

- 7868w (pickup truck)
- VX4400 (four-story fall)
- v710 #1 (broken camera)
- v710 #2 (class action replacement)
- e815 (dead display controller)
- v3c #1 (dead memory controller)
- v3c #2 (killed by Verizon's software updater)
- v3m #1 (broken microSD slot)
- v3m #2 (broken radio)
- k1m #1 (still not sure)

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - CDMA
  - GSM
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

Dealing With Your Carrier

- Use Automated Systems First
  - NOTE: CDMA carrier lock is…carrier-side
- Be Circumspect
  - Find faults in features you're paying for
- Be Courteous
- Keep Talking
  - Stress simple points
  - Stress that you **need to make calls**
    - …unless you're not paying for that feature.

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - General Tips
  - CDMA
  - GSM
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

What's a Feature Phone?

- A non-smartphone
  - Many tricks will still work on smartphones
- Your average cellphone
  - Generally running a proprietary OS
  - Generally running only sandboxed apps
- A much less expensive alternative
  - …with many more locks
  - …with far fewer features
  - …I guess that's why it's a "feature" phone?

General Essentials

- Data Cable
  - Surprise! eBay.
- Serial Terminal Software
  - Look for the “GSM AT Command Set”
- Bitpim / Gammu / Gnokii
- Qualcomm PST (Product Support Tools)
  - CDMA only
  - Not, generally, available to anyone but carriers
- Manufacturer PST
  - Not, generally, available…to anyone.
- Some Form of Unlimited Data
  - …you’ll need it.

Your Grail: Manufacturer PST

- The real bricking alert
  - Even when used properly
  - ESPECIALLY when used properly
  - Read as: find someone else who's tried it first
- High risk
  - ...high rewards
- Get rid of the proprietary UI
  - ...for now
- Change from Qualcomm BREW to J2ME
- Unlock Bluetooth profiles
- Unlock USB Mass Storage mode
- Flash features from newer phones

Stupid Phone Tricks

- **Enter these codes quickly!**
- Motorola: #0SETUP* (#073887*)
- LG: [MENU] 0
- Sony Ericsson: R*LL*L* or U*DD*D*
- Samsung: 147*369*126874#
  - Use # to open hidden menus elsewhere
- Credit to howardforums.com
  - More plugs for them later

What Next?

- Break your phone
- Tweak odd settings
  - There are some things worse than breaking...
- “Free” WAP on CDMA ONLY!
  - Use your own HTTP proxy
  - Look for “Web Sessions” right now, if you like
- Cable enabling
  - Some phones won't accept a data cable!
- NAI changer
  - Covered in detail later
- “Free” tethering

Tethering

- Carrier-authenticated
- Requires a valid context
  - GSM: APN (Access Point Name)
  - CDMA: NAI (Network Access Identifier)
- How do I get a valid context?
  - Buy one
    - Feature phone data plans are cheap!
  - Find one
    - Exploits a CDMA carrier hole…back later.

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - General Tips
  - CDMA
  - GSM
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

BitPim

- Access to your phone filesystem
- Open source alternative to…
  - …expensive tools
  - …proprietary tools
    - GAGIN, anyone?
  - …nonexistent tools
- Works on every CDMA phone
  - …since the LG VX4400
  - Support gets better every day
- Make backups with it frequently!

Uses of BitPim

- Add ringtones ($2 per ringtone)
- Add pictures ($1 per picture)
- Download pictures ($1 per picture)
- Add video (Do what?)
- Download video (What, to a computer?)
- Back up your phone
  - Need the *In Memoriam* slide again?
- Modify system files
  - Another plug for howardforums.com
  - Sky is nearly the limit

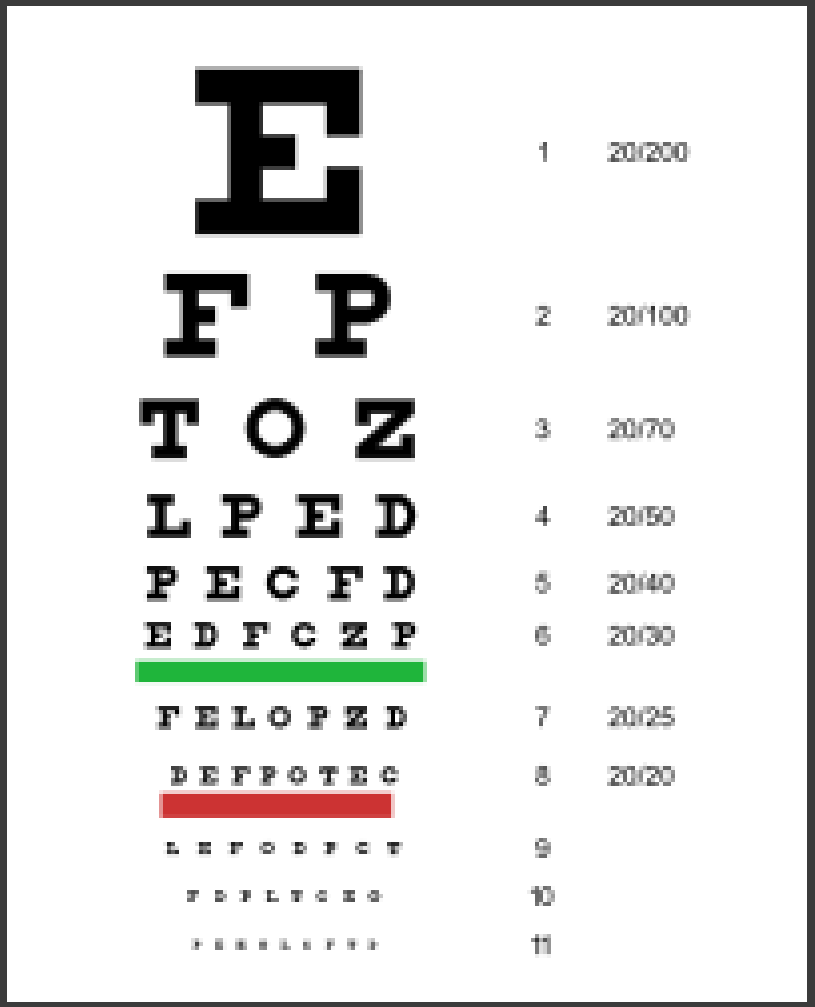
Qualcomm PST

- Yet another bricking alert
  - Yes, even though it's a carrier tool
- Backup service programming
  - Restore it to a new phone, activate it online
- Modify service programming
  - For tethering, mostly
  - Sure-fire Network Access Identifier changer

A Brief History of CDMA Data

- QNC (14.4kbit/sec) aka 2G
  - Phone as a simple modem
  - DO NOT USE THIS
- 1xRTT (300kbit/sec) aka 2.5G
  - Phone carries certain authentication
    - Usually trivial to modify/override
  - Does not differentiate between phone and tether
- EV-DO (1.5mbit/sec) aka 3G
  - Phone has difficult-to-modify authentication
    - One set for the phone (Phone NAI) for WAP, etc
    - One set for the tether (Tethered NAI)
  - Ignores external authentication
  - No other checks
    - Besides carrier data log auditing

Another Eye Chart



The NAI

- Authenticates you for data connections
  - 8005551234@vzw3g.com look familiar?
- Most phones have two
  - One for WAP/carrier services
    - Unlimited access on this NAI? ~$10/month
    - Non-plan access generally bills as airtime
  - One for tethering
    - Unlimited access on this NAI? ~$45/month
    - Non-plan access generally gets rejected

Demo Time!

- Who wants to brick their phone?
- Anybody?
- Anybody?
- If you're reading this, you're getting this from the CD and you missed me showing off in front of a live audience.

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - General Tips
  - CDMA
  - GSM
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

What Makes GSM Different?

- GSM Data
  - …wasn't an accident.
- All voice plans have per-kB charges
  - No "Free Nights and Weekends" on data
- GSM Phones
  - …are sold in free countries
  - …generally support J2ME out of the box
  - …rely on carrier locks

The APN

Anything look familiar?

- Authenticates you for data connections
  - wap.cingular look familiar?
- Most phones have two
  - One for WAP/carrier services
    - Unlimited access on this NAI? ~$10/month
    - Non-plan access generally bills per kB
  - One for tethering
    - Unlimited access on this NAI? ~$45/month
    - Non-plan access generally gets rejected

Good News, Everyone!

- The APN is rarely stored on the phone
  - Special AT commands can set it on connect
- Unlimited WAP access…
  - …becomes unlimited tethering!

Carrier Unlocking

- Software/Firmware Modding
  - Generally manufacturer-specific
    - Sometimes phone-specific
  - Generally difficult
- Hardware Modding
  - Still manufacturer-specific
  - Still difficult
- Outside the scope of this talk
  - I could easily spend three hours on this

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - General Tips
  - CDMA
  - GSM
- Smartphones
  - BlackBerry
  - Windows Mobile
  - Symbian
  - iPhone

BlackBerry Devices

- Generally behave like feature phones
- Generally come with very few locks
  - A recurring smartphone theme!

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - General Tips
  - CDMA
  - GSM
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

Symbian Devices

- Generally behave like feature phones
- Generally come with very few locks
  - A recurring smartphone theme!
- Seriously. Recurring.
- Open Source Symbian may be terrifying

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - General Tips
  - CDMA
  - GSM
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

Windows Mobile Devices

Unfortunately, due to time constraints, I was not able to get approval to include these slides in the DEFCON CD edition.

An updated deck will be available immediately after my presentation at DEFCON 16, including as much of this information as possible.

Outline

- Disclaimers
- Why I Do This
- Basic Skills
- “Feature” -phones
  - General Tips
  - CDMA
  - GSM
- Smartphones
  - BlackBerry
  - Symbian
  - Windows Mobile
  - iPhone

The iPhone

The slide deck for the DEFCON CD had to be prepared prior to the release of the iPhone v2, and as a result these slides could not be prepared.

An updated deck will be available immediately after my presentation at DEFCON 16, including far more than you wanted to know about the iPhone.

Wait, What About Android?

- What about it?
- Extremely few details
- Extremely questionable concept
- Extremely open design
  - Very interesting to see carrier reactions

Thanks for coming to the talk!

Feel free to send questions and comments to:

alexander.lash@gmail.com

Check out www.devalue.org for an updated deck and tools.

QUESTIONS?