Open Source Warfare

Origins

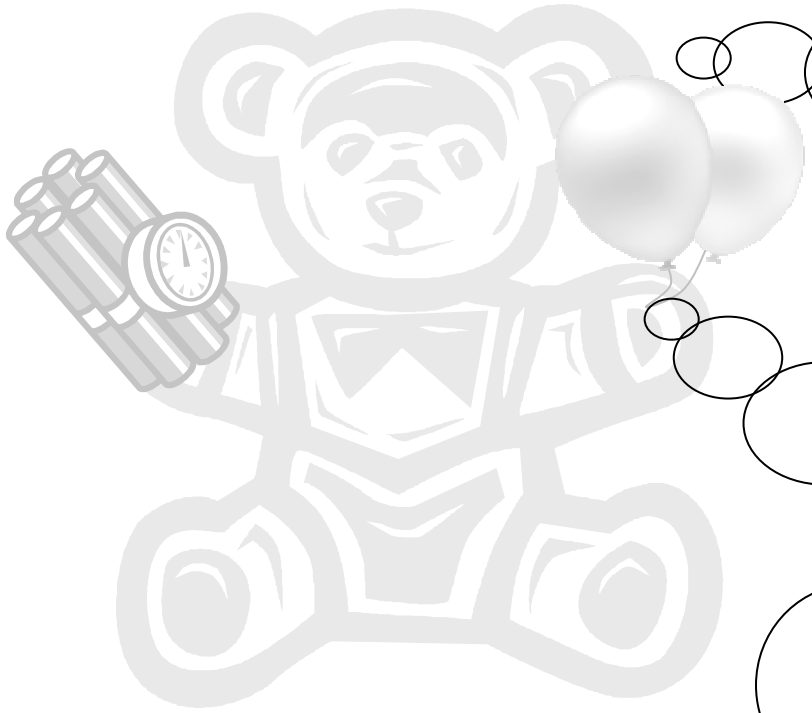
Use

Transformations

Day Three: Sunday, August 10

10:30 am

Track 3



Gosh….
What is Open Source Warfare
•Who uses it
•Who is it used against
•Are there any defenses
•Is it successful
•Where is it used

…Oh my….
What is Asymmetric Warfare
•Is it purely defensive
•Does it rely on traditional concepts
•How does an established fighting group use it
•Does it overlap with other computer security issues

Warnings

A few things to remember:

- Although this stuff in very interesting it is used primarily in warfare….that means people actually die
- If you think you're smart enough to try this on your own you are wrong! …and you could go to jail….
- Because of all this we will keep the examples simple, well known and generic…
- Importantly, this is a value neutral technical presentation: that means that we'll only look at techniques and not evaluate whether the people using these methods are "right" or "wrong", "justified" or "unjustified"

What types of things are used in OSW

- In a funny way this is a lot like McGyver
- Almost anything can be used…toothpicks, tin foil, matchbooks, string…..
- But on the contemporary battlefield it depends more heavily on things like mobile phones, microwave ovens, remote controlled aircraft, toy robots, digital cameras, sniffer tools

Let's look at telecommunications

- Lebanon is a good example
  - You may remember a few months ago that there was tremendous upset when the government attempted to quash third-party telecommunications networks
  - In fact, it led to major fighting in the street
  - To complicate matters the country also faces a number of external forces, Syria, Iran, Israel
  - As well as a number of internal forces

Let's look at telecommunications

- So what was the problem
  - Third party groups had co-opted the telecom network set up by the government
    - This was accomplished by "extending" copper networks
    - Creating new optical networks
    - Piggybacking on Mobile networks
  - This also required technical knowledge as well as a heavy reliance on openly available public encryption, VOIP, chat room, message boards, anon email etc. communication methods
  - So big did this become that it pretty much became an unsolvable issue for the government

So, let's take a look at this map with overlays:

•First we see the regional context
•Next lets look at the geographic issues
•Now, the overlays of the networks (click, click)

•Secondly, lets look at why it was so difficult for these networks to be eliminated

•Thirdly, lets look at why publically available software/hardware tools have been so essential to the "success or failure" of the parties

•Finally, a word about undersea cables disruptions

Variants of this: Las Vegas

- Let's look at the concept of triangulation
- Here's a pretty picture of Las Vegas:

Variants of this: Las Vegas

- Now, let's see it as a "protocol" map (click, click)
- This is all open source!

Variants of this: Las Vegas

- How do we triangulate?
- You can run but you can't hide
- Now let's think of this picture as a battlefield
  - We'll add some conceptual drones
  - And figure out how to target an individual or group
  - Note: this is a very useful method already employed – think in terms of sniffer networks, GPS networks, geo-location web 2.0 tricks
- IT'S ALL ABOUT THE MATH!!!!!

Open Source Platform

- Let's take a look at OS surveillance platforms
- Here is a series of pictures of a RC helicopter with HD cam (*next slide, pics only provided live at Defcon 16*)
- Range: 2000 ft, 1 mile radius, 20 min battery life, encrypted com link
- Price $400.00 off the shelf
- *(no, I don't have the vendors name, sorry)*

A quick look at OS uses in the field

- Microwaves, IEDs, and the battle space
- Robotics at Ground Zero, Sept 2001
- Defeating LED and surveillance cameras
  - Quick word on a counter measures
- The mobile phone quandary
  - And the jamming quandary

A quick look at OS derivates

- Defcon 15 presentation regarding GPS device hacking
  - Here's a simulation example
- Defcon 14 presentation regarding rocketry
  - Here's a simulation example
  - And here is an open source example of how model rockets utilize telemetry for guidance
  - (yikes!)

And Finally

- Overview of “mass-communication” methods meant to influence a populace
  - Prep for a pending “attack”
  - Mass influence techniques
  - Reliance upon the “hacker” community for tools and methodology
  - Utilizing existing structures (e.g. social networks) for influence (good or ill)
  - Setting up a “Zeitgeist” scenario for influence

Thank you

- Since this is a very brief presentation feel free to contact me after this for any additional input
- Thanks again!!!