Script Kiddiez Suck

Marcus J. Ranum

<mjr@nfr.net>

Chief Technology Officer, Network Flight Recorder, Inc.

http://www.nfr.net

1

What is this talk about?

- A call to change how we perceive security
- A call to change how we disclose problems
- A call to change accountability
- Some predictions

2

Script Kiddiez ***suck***

- There are way too many script kiddiez

  …Why?

  – Message "***It's OK***" ("Extreme Hacking" classes at conferences, etc.)

  – Loads of toolz in distribution

  – No consistent effort to stamp them out

  – No perceived downstream cost for being a lame script kiddie

3

The Targeting Problem

- ***Why*** must we reduce the number of script kiddiez?

  – They represent a great deal of noise that must be filtered out

  – It's imperative to reduce the script kiddie population in order to be able to meaningfully quantify the size and talent of the ***real*** threat

4

Changes in Perception

- I believe that the public at large is getting sick of hacking*
  - With increasing broadband-to-home access (and related security problems) security is beginning to have a ***personal*** impact on Joe Average
    - Joe Average tends to lash out in anger when he's hurt: hackers beware

*Call it whatever you like; you know what I mean

5

Hacking == Amateur Terrorism

- Many parallels exist (except that the kiddiez are mostly non-ideological)
- To win:
  - Good guys must defend everything
  - Bad guys must find a single flaw
- ***Counter-terrorism***: take the battle to the enemy where they live
  - Scorched earth, zero tolerance

6

The Gray Area

- Right now, we tolerate a very large "gray area" between "white hats" and "black hats"
  - There are too many people who fight on both sides of the battle
  - The grey area must evaporate as part of switching to a counter-terrorist model: separate the terrorists from their support base as thoroughly as possible

7

The Gray Area *(cont)*

- With apologies to some of my friends in the gray area:
  - We need to reduce that comfortable gray area into a very narrow line
  - We need to stop hiring ex-hackers as security consultants (selling reformed wolves as shepherds is an insult to the sheep)

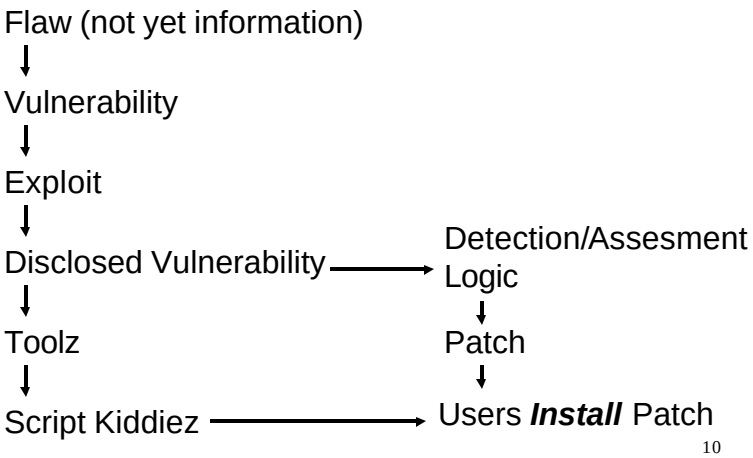
8

Changes in Full Disclosure

- The way full disclosure is being practiced today is self-defeating
  - It's creating hordes of script kiddiez
  - It's not (visibly, anyhow) making a positive impact on software quality
  - It's not (visibly, anyhow) making a positive impact on bug-fix turn-around times
  - It's not helping

9

Evolution of Vulnerability Information



10

One Question

- Is it possible that script kiddiez are a necessary evil?
  - They ***force*** end users to update their software
    - I say no: software should self-update or include auto-patching mechanisms
  - They make it impossible for vendors to hide their mistakes?
    - I say no: There are better ways to publicize

11

An Observation

- If full-disclosure ***works***, why isn't the state of security ***improving***?
  - It's not:
    - More vulnerability information is out there
    - Many users are not installing patches
    - More script kiddiez all the time
    - More break-ins all the time
    - Vendor software is still just as buggy as it was 5 years ago (if not worse)

12

Myths of Full Disclosure

- #1:
  - The hackers already know these techniques so it's best for everyone to know them so they get addressed
    - The hackers do, the script kiddiez did not
    - Counter-intelligence on the white hat side is not awful; we find them out pretty fast anyhow
    - Many of the vulnerabilities being disclosed are researched and discovered for the ***purpose*** of being disclosed

13

Myths of Full Disclosure

- #2:
  - The vendors can't hide their bugs once they are disclosed
    - Sure, they can! (e.x.: Windows authentication no longer vulnerable to l0phtcrack)
    - There are better avenues for publicizing flaws that are just as harmful to the vendor and just as effective (e.x.: Tell NYT/WSJ/CNN about the flaw and how the vendor is covering it up)

14

Myths of Full Disclosure

- #3:
  - It's necessary to disseminate flaw information in order to make better systems in the future
    - 99% of the bugs found fall into well-known flaw taxonomies (e.g.: buffer overruns, config file protection, starting sub-processes)
    - It's not necessary to teach and test the specifics: teach and test the problems as a class

15

Myths of Full Disclosure

- #4:
  - It's for your own good
    - Actually, it's a tool for self-promotion, financial gain, and ego-massaging of practitioners of full disclosure
    - This is clearly demonstrated by the fact that vendors are no more responsive about patches and the population of script kiddiez is skyrocketing

16

Realities of Full-Disclosure

- What I see is rock-throwing being passed off as “beneficial” when in reality
  - It’s from people who’d rather hack but want to claim white hat status
  - It’s from people who don’t know how to build useful things; they’d rather publicize their ability to destroy
  - It’s market “assassination” (Microsoft is a prime target)

17

A Challenge

- For those in this room who produce toolz:
  - Why don’t you build a better firewall?
  - Why don’t you secure a browser?
  - Why don’t you develop an IDS?
  - Why don’t you make a secure O/S?
  - Why not do something ***productive*** and ***worthwhile*** to benefit the community?

18

Changes in Accountability

- Dramatically increase the level of accountability for security-related issues: we must accomplish ***both*** of:
  - People releasing tools or exploits irresponsibly must/will be held accountable for the consequences of their actions
  - Vendors that produce products with security bugs must/will be held to standards for providing fixes

19

Predictions

- I'm not sure I want to be right about these, but I suspect I am
  - E-mail me in 5 years if I'm wrong ;)

20

Prediction #1

- The good guys will take the battle to the enemy
  - Within the next 5 years

21

Prediction #2

- Authors and distributors of attack tools will be on the receiving end of high dollar civil liability lawsuits
  - Within the next 3 years
  - They will have the unmitigated gall to expect people to feel ***sorry*** for them when they do
  - Authors of attack tools will regret signing their workmanship

22

Prediction #3

(Follows from prediction #2)

- Attempts to deal with hacking via conventional law enforcement will be abandoned in favor of civil litigation
  - Within 5 years
  - Law enforcement has proven ineffective
  - Most knowledgeable people will be more scared of amazon.com's lawyers than the FBI, anyhow

23

Prediction #4

- Nothing melts away a gray area like a pile of lawsuits and resulting case law
  - Within the next 5 years the gray area will be all but eliminated
  - Hackers in the room: start thinking about how to build security-positive tools to give away instead of security-erosive tools - Your legal counsel would approve!

24

Conclusion

- I think we're at the end of the beginning of the Internet Security Era
  - Things will either get better or worse
  - The key factor will be social attitudes and our ability to change them
  - On one side: big business consistently suffering huge financial costs
  - On the other side: big egos, no financial backing, no organization, "hobbyists"

25

A Point To Remember

- The Huns didn't know how to ***build*** a Rome - they only knew how to ***sack*** it
  - We're giving too much credit to the "full disclosure" crowd and the toolz-writers
  - Let's start promoting the Rome-builders, not the Huns

26