Economies of Scale in Hacking

Dave Aitel
Immunity

Ekoparty, 2008 (Argentina)

Demand Side/Supply Side Economies of Scale

- Networked increase in value

- High barrier of entry
- Cheaper as you get bigger

Applying this to hacking

The best offense is a good offense

Networked reverse engineering toolkits

Your source code wants to be free

Attack frameworks

The 10.0.0.0 and IPv6 problems

XSS vs Heap Overflows

Ignore the network effects to your own peril

- Case Studies:
  - AV
  - IDS
  - Static Analysis
- Questions to ask:
  - What is growing exponentially?
  - How did the technology handle that?

The Twitter Effect

- To Twitter: (verb) to fail under exponential growth

Anti-Virus

Allchin Suggests Vista Won't Need Antivirus

By Scott M. Fulton, III, BetaNews
November 9, 2006, 4:26 PM

During a telephone conference with reporters yesterday, outgoing Microsoft co-president Jim Allchin, while touting the new security features of Windows Vista, which was released to manufacturing yesterday, told a reporter that the system's new lockdown features are so capable and thorough that he was comfortable with his own seven-year-old son using Vista without antivirus software installed.

Allchin's staten
Vista would be
security feature
he said, his pe

Not a good sign

F-Secure: Malware Doubled in 2007

December 06, 2007 | by Geoff Duncan

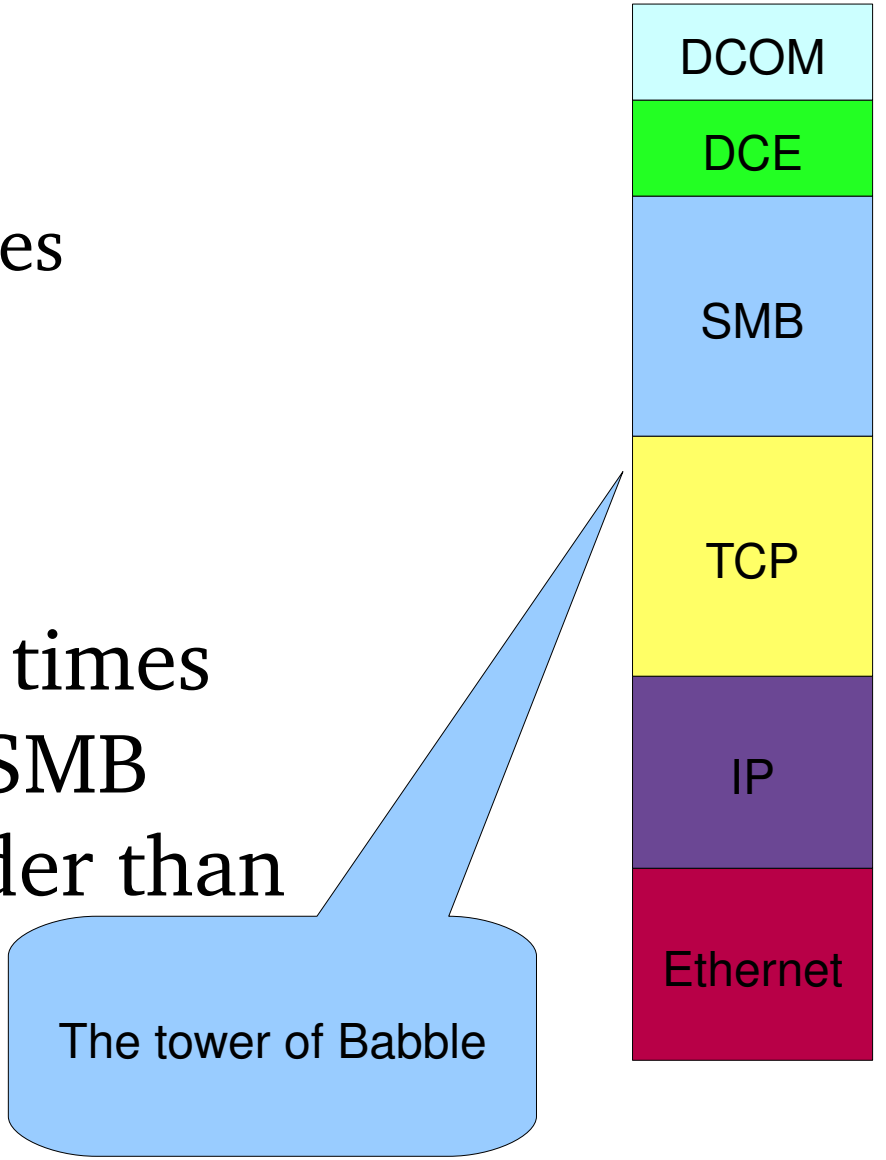
F-SECURE

Computer security firm F-Secure was tracking about 250,000 malware signatures at the beginning of 2007: now, they're tracking about 500,000.

6 hours to defeat
10 AV's

IDS: What grows exponentially?

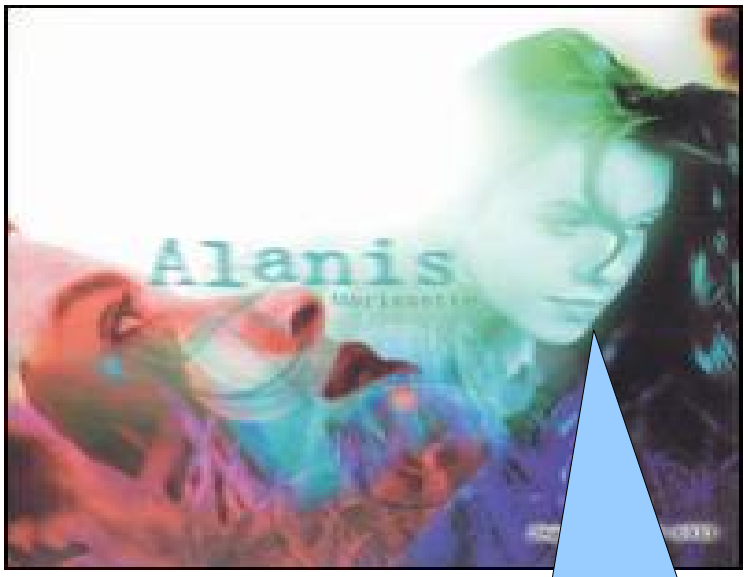
- Targets
  - And hence vulnerabilities
- Protocols
  - Protocol complexity
- IDS/IPS failed because decoding DCOM is ten times harder than decoding SMB which is ten times harder than decoding IP



Static Analysis: Checklists are not the answer

- NIST Static Analysis survey
  - 6 target programs (Java/C)
  - Lots of products and services
  - Extremely high false positive rate
  - Over 1 man year to sort through 47000 warnings
  - Guess how many 0day they found!?

Best of the 90's



Security Problem?

Sniff For It

Scan for it

Demand Side Economies of Scale: Offense == More Offense

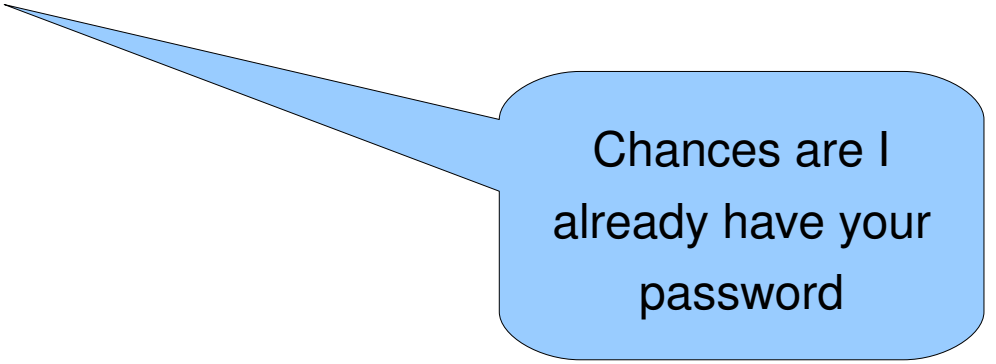
The best offense is a good offense

The best password cracker in the world

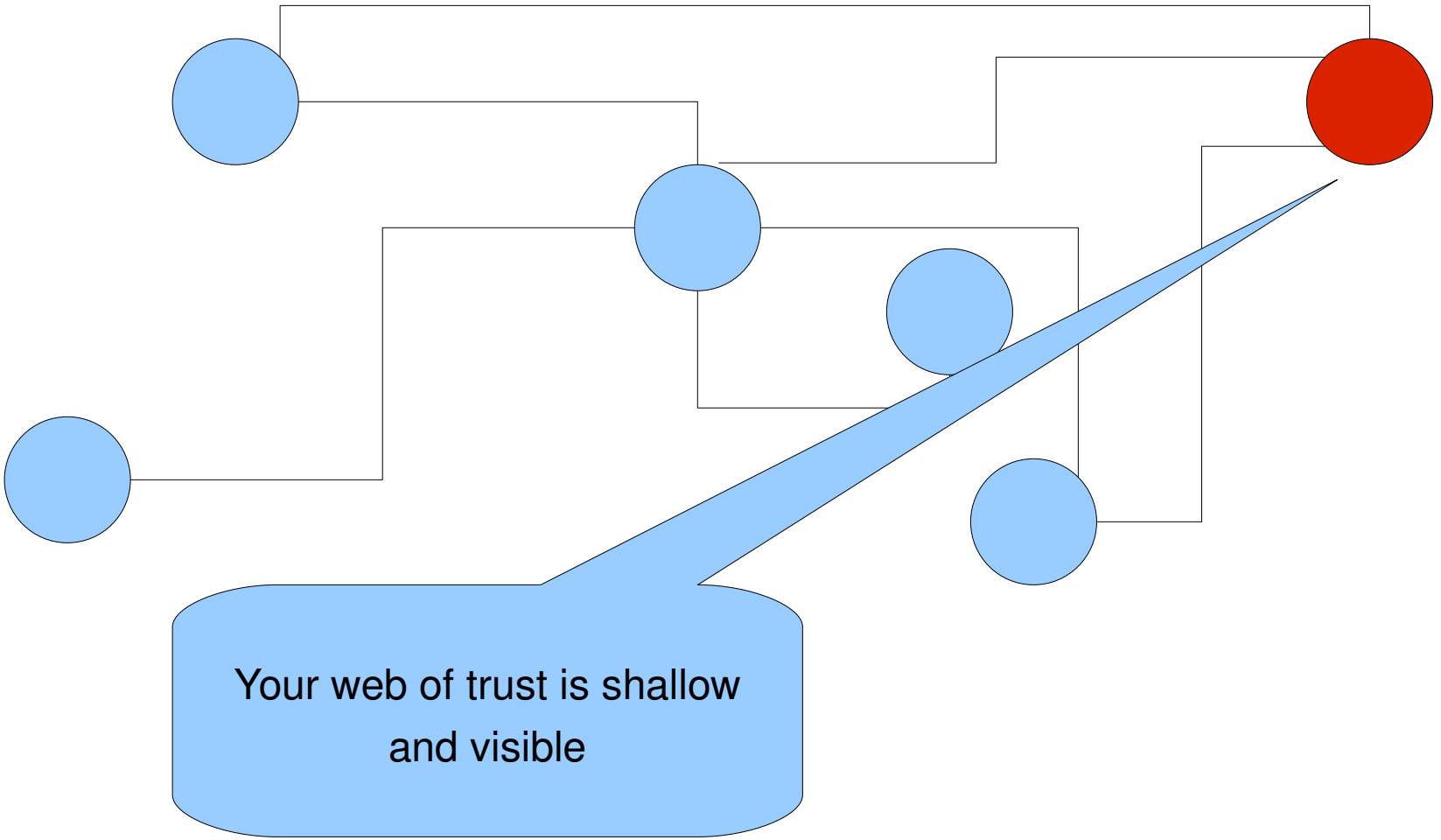
?

The best password cracker in the world

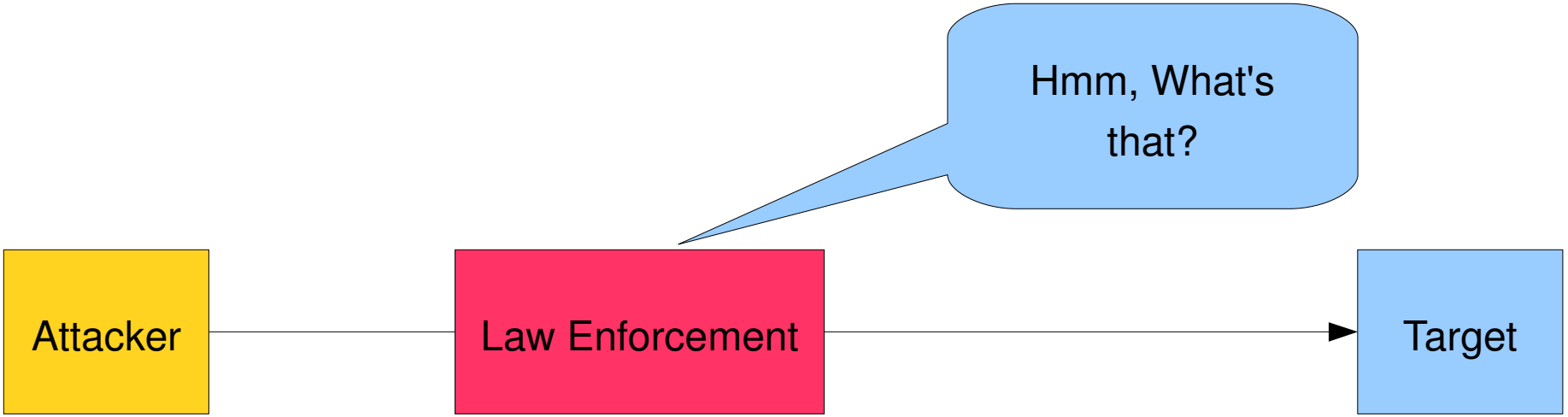
grep targetname passwords.txt



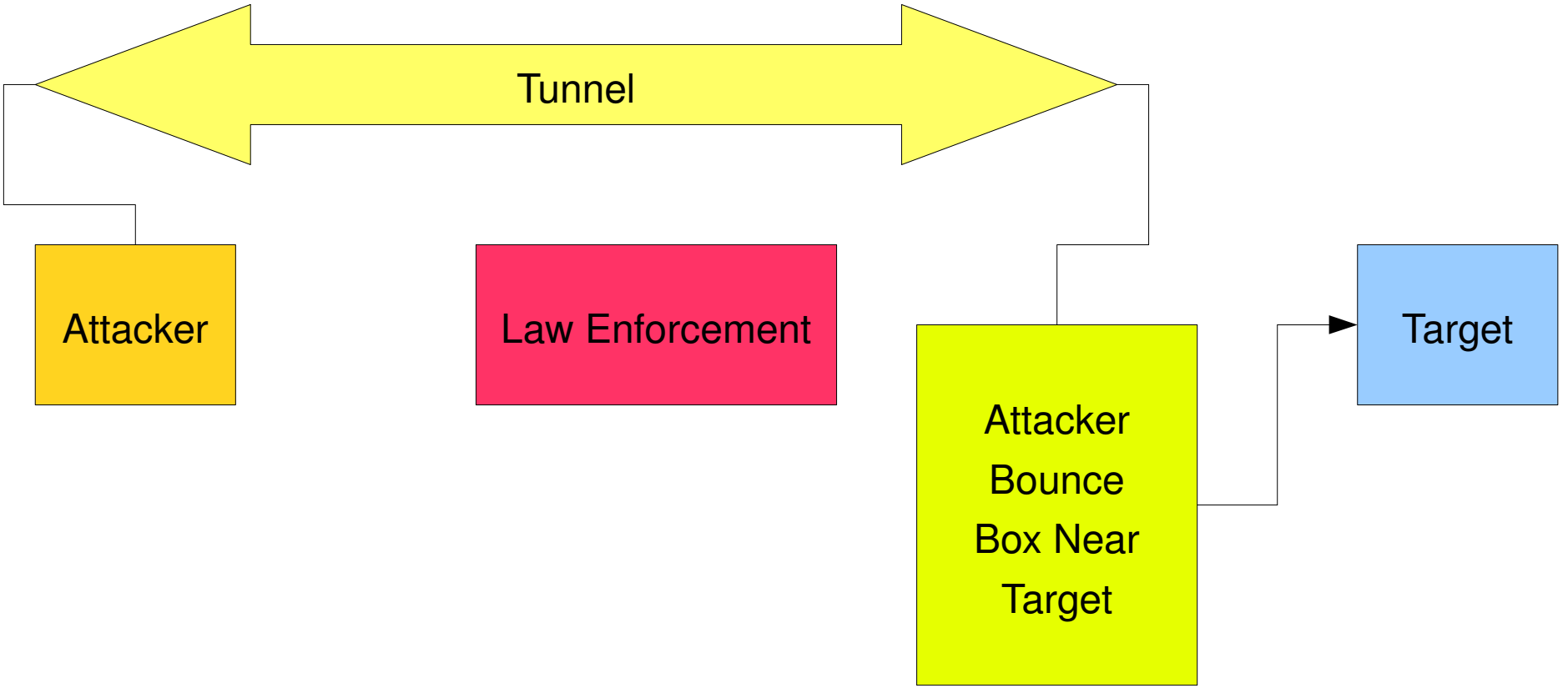
To a hacker who is everywhere...



Poor Attacker



Rich Attacker



Trust the Source

Your source code wants to be free

“Damage” is strategic, not monetary

Re: Kevin Mitnick

Dear Kathleen:

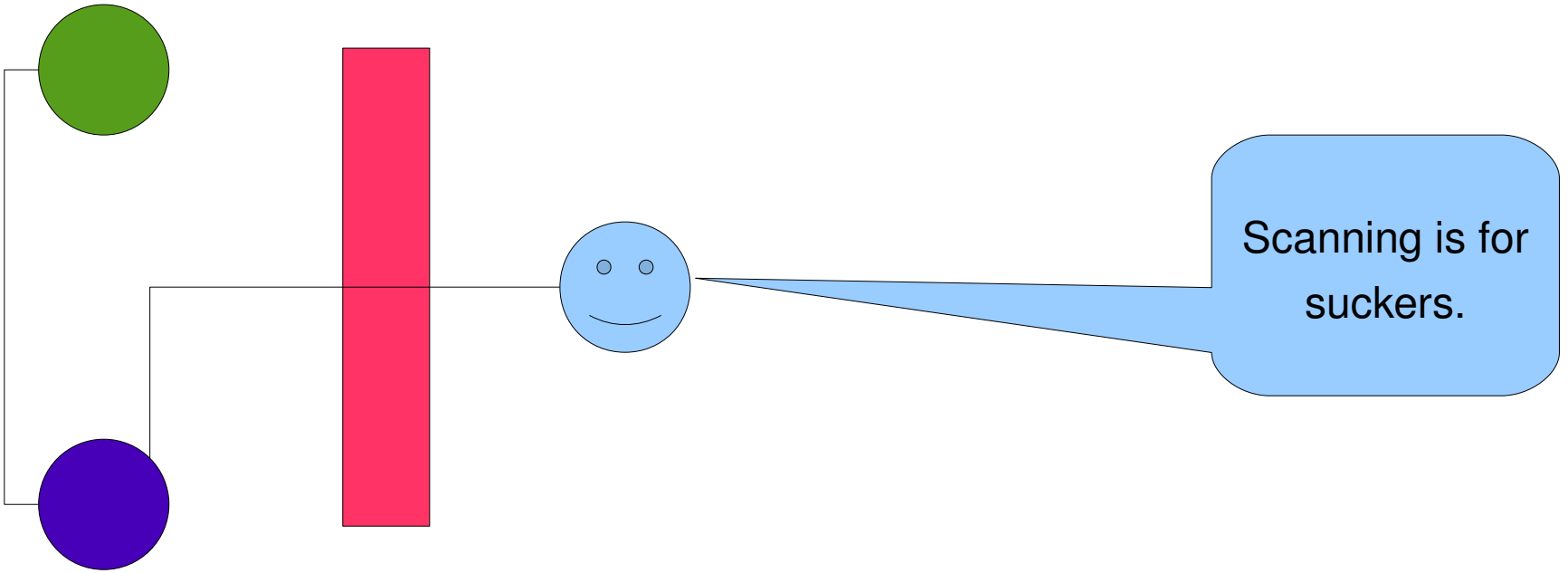
Congratulations on the arrest of Kevin Mitnick. Pursuant to your request, I asked our Cellular group to assess the damages caused to Fujitsu Network Transmission Systems, Inc. ("FNTS") by Mitnick's theft of the source code for the PCX telephone. The information provided to me is as follows:

Software development expenses... $1,100,000.00
Research & development expenses.. 1,000,000.00
 Total... $2,100,000.00

Networks, plural.

The 10.0.0.0 and IPv6 problems

10.0.0.owned



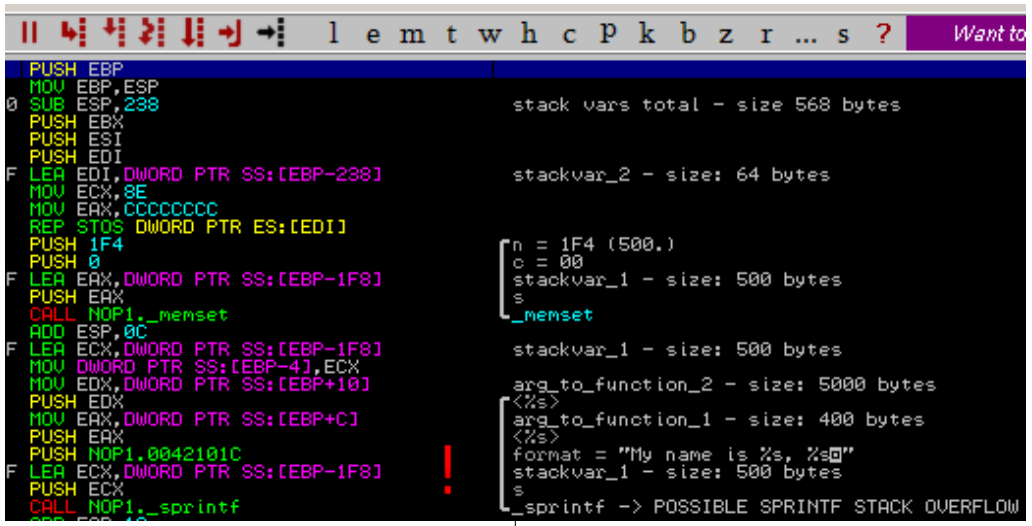
OS Detection

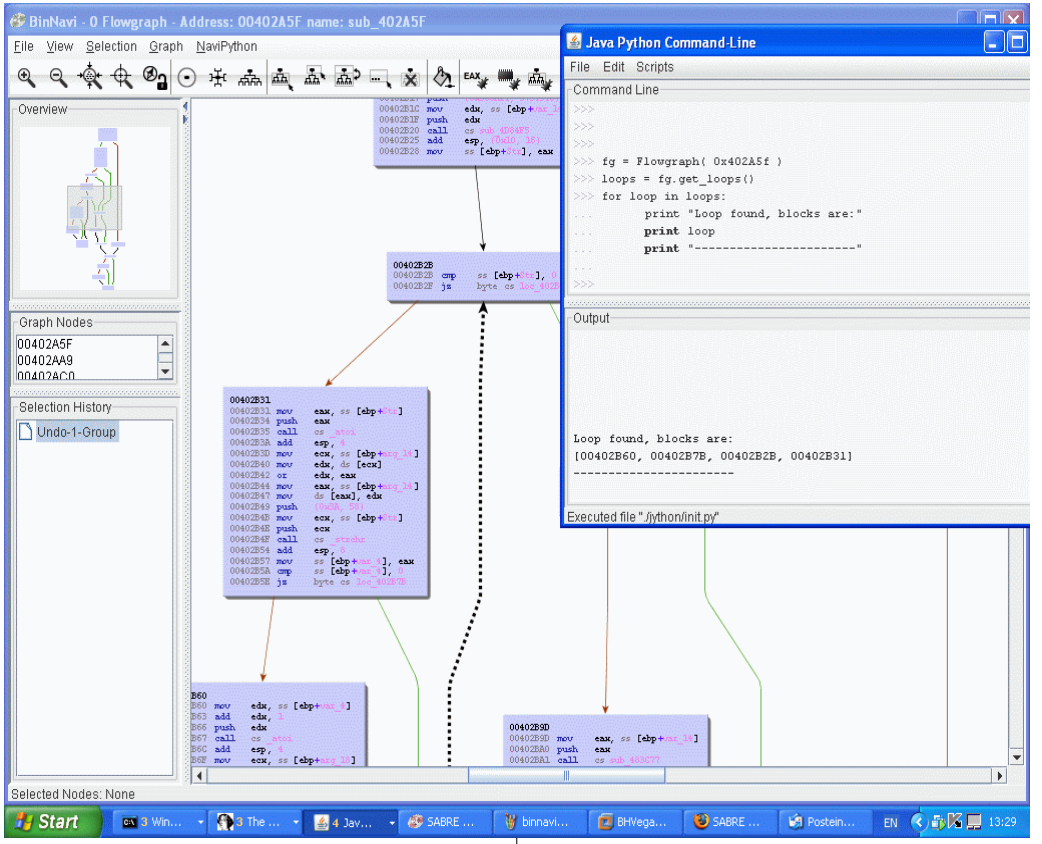
- Knowing a host is Windows 2000 is great for scanner reports
- To get beyond the scanner reports we need to think beyond “OS” to a concept of “is this vulnerable” and “will this be vulnerable”.
  - Automated statistical techniques can do this on a large scale

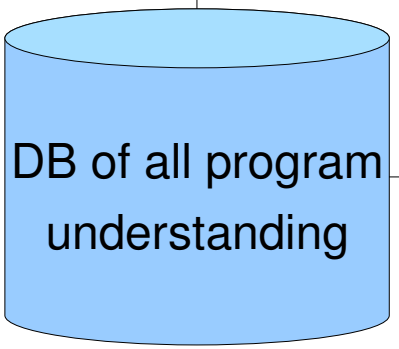
GIT + ASM = GITASM?

Networked reverse engineering toolkits

There's no I in hacking.







Applying this to hacking

Attack frameworks

Know Your Customer

- “iTunes” for Exploits
- “Facebook” for trojans
- Customer Relationship Management for targets

This is not your father's heap

XSS vs Heap Overflows

The Bazaar

- Good offensive security research is being driven underground
  - It's too expensive to give away!
  - Not just a “Vulnerability Marketplace”:
    - Audit technologies
    - Bug classes
    - Exploit techniques

Show me the MONEY!

Why are memory corruption bugs so expensive

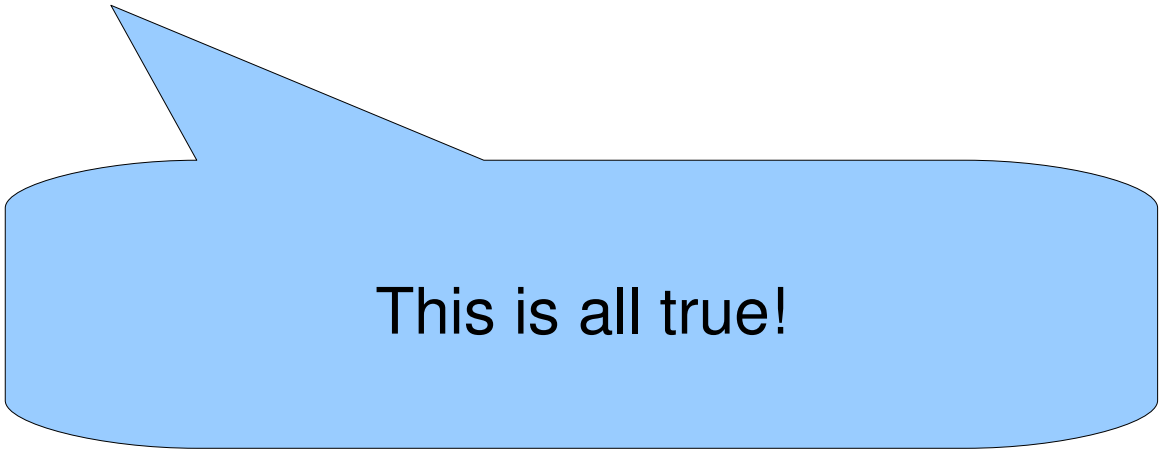
- **Heap/Stack cookies (/gS)**
- SafeSEH
- **ASLR**
- **DEP/NX/W^X/PAX**
- Process Isolation
- System call ACLs
- Automated code review programs
- **Managed languages**

Security made the news

- Security built into development lifecycles
  - And compiler tools
- Security responses driving vendor differentiation
- Security being built into platforms

A gathering storm

- “But this doesn't affect me - I write web applications in Ruby on Rails”
- “There hasn't been a real remote overflow in IIS since version 5”
- “What part of **managed** language don't you understand?”



$->$$$

- Vulnerability research is so expensive it cannot be funded out of your marketing budget anymore
- Not only are bugs expensive but the techniques for reliably exploiting bugs becomes expensive
  - You no longer know if you are really at risk!

The market is reacting

- The memory corruption problem is “solved”
- The worm problem is “solved”
  - Hence, the slow takeup of IPS – it's just not worth the pain!
- Microsoft Exploitability Index
  - Q: What are you going to do when for months on end everything is “pretty much not exploitable”
  - A: Stop patching
  - A: Stop investing in security

Exploit 7 Impossible Bugs Before Breakfast

Things you can do at large scale

- Defeat Secure Development Lifecycles
- Attain a significant advantage by combining different levels of information

Attack the next big mistake

- C/C++
  - Memory corruption
- Ruby on Rails, Java, C#, Python, etc.
  - No buffer overflows (we're MANAGED)
  - Threading!

The Conclusion

Hacking has a strong trend towards natural monopoly!