

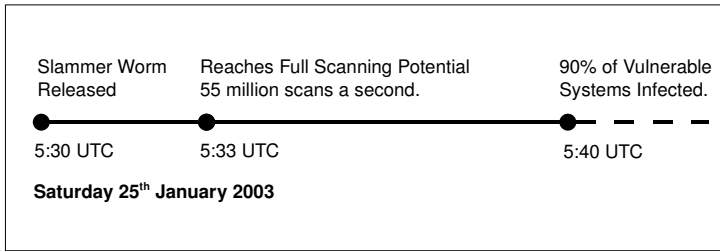
# Software Vulnerabilities

## The Slammer Worm and MS Blaster

Michael Clarke  
mfc5@aber.ac.uk

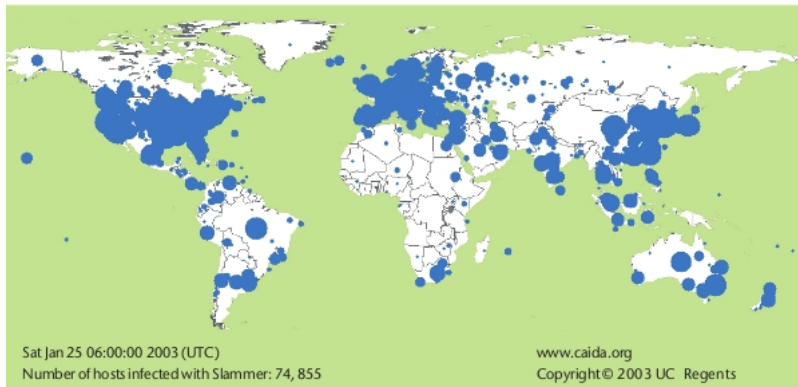
November 24, 2009

# The Slammer Worm



- ▶ It is estimated the worm infected over 75,000 systems, affecting 911 data-entry terminals, airline flights, interfering with elections and causing ATM failures!

# Within 30 minutes...



# The Slammer Worm

- ▶ Slammer was the first real-world demonstration of a high-speed worm.
  - ▶ Vern Paxson and Nicholas Weaver.
- ▶ It was the fastest computer worm in history.
  - ▶ Two orders of magnitude faster than Code Red (359,000 hosts in 37 minutes).
- ▶ The only thing slowing it down was a lack of network bandwidth!

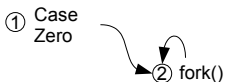
# How Slammer Chose Victims

$$x' = (x \cdot a + b) \bmod m$$

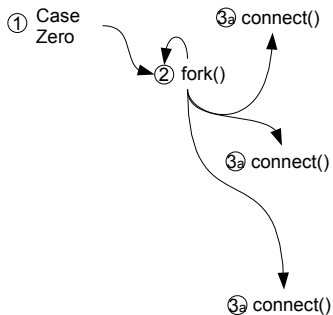
# So, why was it so fast?

① Case  
Zero

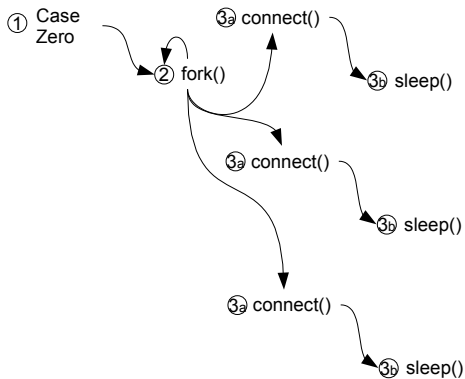
# So, why was it so fast?



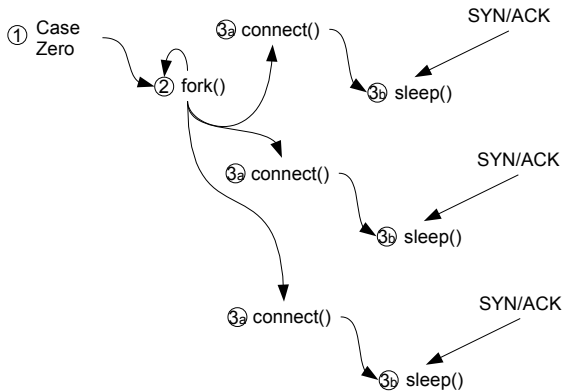
## So, why was it so fast?



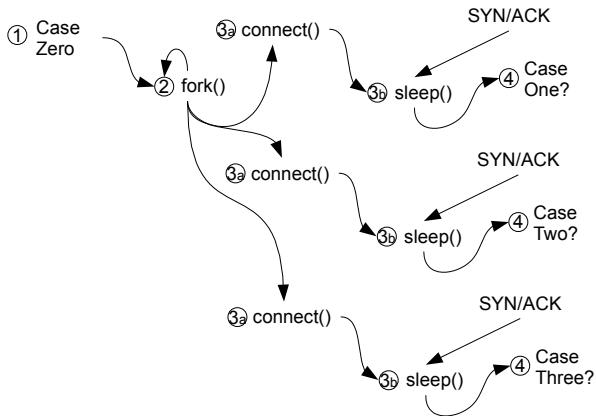
## So, why was it so fast?



## So, why was it so fast?



# So, why was it so fast?



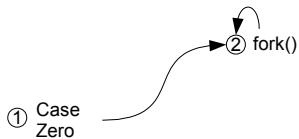
## But there is a problem...

- ▶ Using TCP means that:
  - ▶ We have to wait for the remote host to acknowledge the connection, slowing us down.
  - ▶ We have overheads such as error checking, slowing us down.
- ▶ So, create more threads?
  - ▶ The OS will have limits!
- ▶ But, if we're small enough (404 bytes!), use UDP...

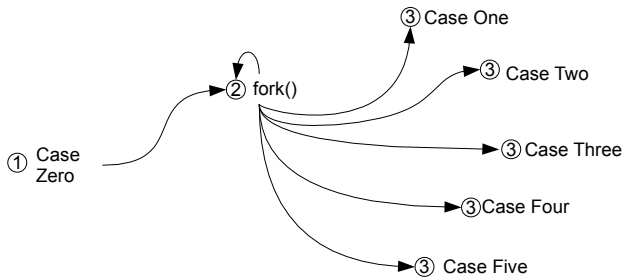
# So, why was it so fast?

① Case  
Zero

# So, why was it so fast?



## So, why was it so fast?



## But, Slammer wasn't perfect...

- ▶ The developer(s) of Slammer made a number of mistakes:
  - ▶ Had Slammer limited its own speed at spreading it could have infected significantly more machines.
  - ▶ The implementation of the random number generator has mistakes resulting in a portion of the IP address space unaffected.

# Defeating Slammer

- ▶ Due to the rapid speed no human could intervene quickly enough to prevent the spread of the worm.
- ▶ After a few hours, general filtering of UDP port 1434 was successful in limiting further spread of the worm.
- ▶ Had Slammer used another port (80 for example) this kind of filtering would not have been so effective, or even possible in some cases!

# What can we learn from Slammer?

- ▶ Previously smaller populations of hosts not considered a target by worms:
  - ▶ 20,000 hosts, how long before you find another vulnerable target?
  - ▶ However, Slammer could infect 20,000 systems in 1 hour!
  - ▶ Makes smaller networks more vulnerable now than ever before.
- ▶ We need to find ways to automate against these kind of worms.
- ▶ We should consider such 'fast worms' to be another tool in a attackers arsenal.

# Enter Blaster

- ▶ 16<sup>th</sup> July 2003: Security Bulletin MS03-026:
  - ▶ Included a patch.
  - ▶ CERT issue advisories over next few days.
- ▶ 26<sup>th</sup> July 2003: HD Moore publishes working exploit example.
- ▶ 11<sup>th</sup> August 2003: MSBlast (Blaster) released.
- ▶ One week later more than 100,000 systems infected.
- ▶ Blaster is still spreading a year later!

# What Blaster Does

- ▶ Runs at first infection, and subsequent restarts.
- ▶ Starts propagating:
  - ▶ Choosing a random address from the same Class B network as the infected host.
  - ▶ Choose a completely random address.
  - ▶ 60% of the time use the complete random address.
  - ▶ 80% of the time assume infecting a Windows XP system.
- ▶ Once vulnerable host identified, uses RPC exploit to open TCP port 4444 and then uses TFTP (UDP Port 69) to transfer the full worm and then executes it.
- ▶ Start a thread to DoS Microsoft's Windows Update website.

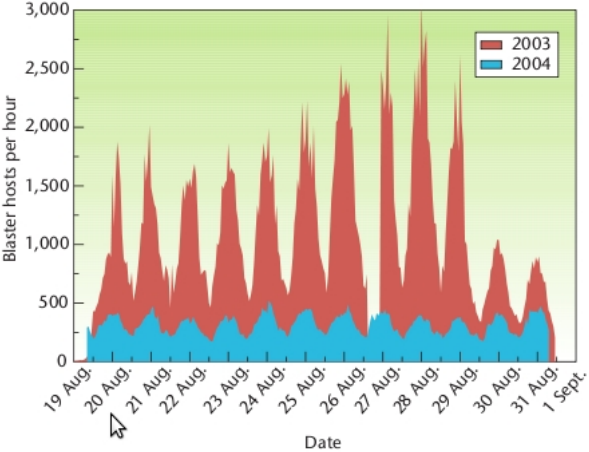
# The Impact of Blaster

- ▶ Survey of 19 research universities identified that each spent an average of \$299,579 during a five week period cleaning up infected systems.
- ▶ Growing view that worms are serious criminal offences and not just internet vandalism.
- ▶ Author of Blaster.A was never caught, but author of Blaster.B was caught and sentenced.

# The Blaster Life-Cycle

- ▶ Blaster is a prime example of a worm's life-cycle.
- ▶ Blaster went through four stages:
  - ▶ Latency - discovering the vulnerability and then the worm in the wild.
  - ▶ Growth - spreading and propagation of the worm.
  - ▶ Decay - infected systems, patched, removed from network, spread of worm slows.
  - ▶ Persistence - consistent levels of activity.

# Blaster, One Year Later



# Conclusions

- ▶ It is clear there are two types of worms:
  - ▶ Fast worms such as Slammer
  - ▶ Persistent worms such as Blaster
- ▶ It seems that persistent worms are more of a threat, causing more damage over prolonged periods of time.
- ▶ Fast worms seem to restrict their own propagation too quickly.
- ▶ We don't really have a way to fight either type of worm.
- ▶ All these worms attacked Microsoft products - use UNIX!