

Review of:

## Inside the Slammer Worm

•Paper by:

- David Moore (UCSD),  
Vern Paxson (ICSI, LBL),  
Stefan Savage (UCSD),  
Colleen Shannon (Data Analysis),  
Stuart Staniford (Silicon Defense), and  
Nicholas Weaver (Silicon Defense, UC Berkeley)

•Published in:

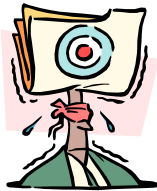
- IEEE Security and Privacy
- July 2003

•Review by:

- Jing Lu

## Portrait of Slammer

- Release date: Slightly before 5:30 UTC on Saturday, 25 Jan. 2003
- Author: Unknown
- Interest: Attack Microsoft's SQL Server or MSDE 2000
- Transportation: UDP port 1434
- Feature: Surprisingly high propagation speed
- Accomplishment: Took over 90 percent of vulnerable hosts within 10 minutes; infected at least 75000 hosts; caused significant disruption to financial, transportation, and government institutions.



## Why Microsoft SQL Server?

- Microsoft's SQL Server 2000 exhibits two buffer overflow vulnerabilities that can be attacked remotely without having to be authenticated to the server.
  - Stack based buffer overflow
    - Saved return address is overwritten with an address that contains a "jmp esp" instruction, when procedure returns, the attacker's code is executed.
  - Heap based buffer overflow
    - [www.nextgenss.com/advisories/mssql-udp.txt](http://www.nextgenss.com/advisories/mssql-udp.txt)

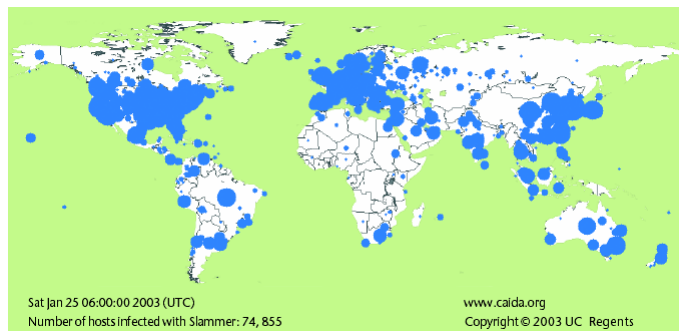


Fig 1. The geographical spread of Slammer in the 30 minutes after its release

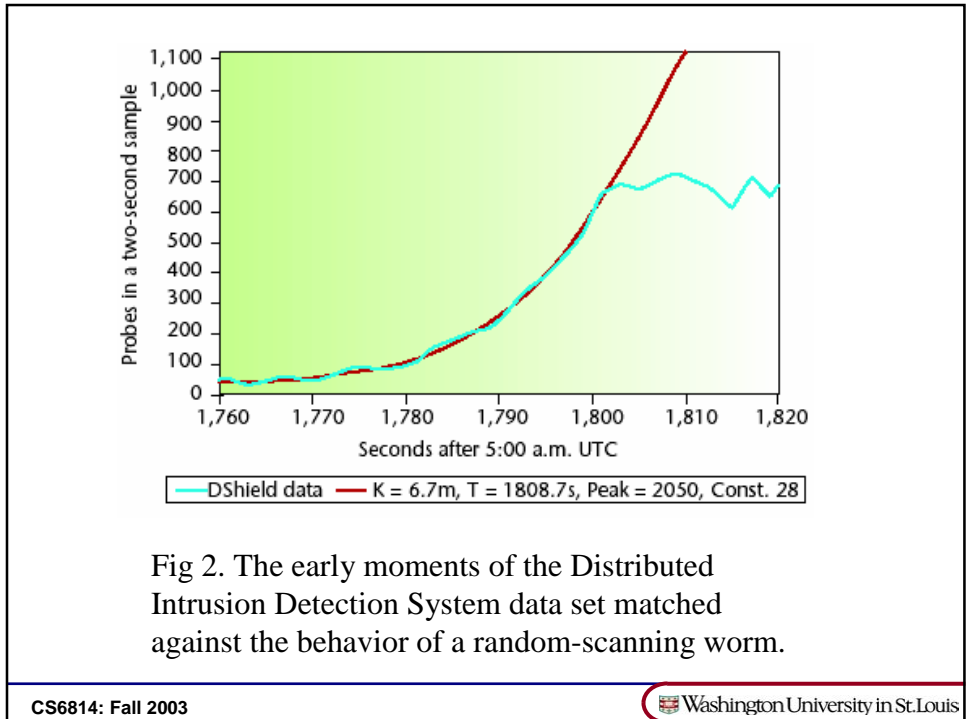
## Why Slammer so fast?

Slammer	Code Red
Single 404-byte UDP packet	4K bytes
Connectionless, replicate itself as fast as possible	Via TCP connection, wait for responses from potential victims
Limited by connection bandwidth of the infected machine	Limited by waiting latency for responses

## How Slammer chose its victims

- Slammer randomly selects IP address to probe.
- Initially spread exponentially, but slow down as a large number of infected hosts retry infected or immune addresses.





**What Slammer's author did wrong**

$$x' = ((x) * a + b) \bmod 2^{32}$$

$a = 214013$  (0x343FC),  $b = 2531011$  (0x269EC3)

- Three mistakes in the random number generator:
  - 2's complement vs. inverting (0xFFD9613C)
  - SUB vs. ADD
  - Use OR instead of XOR to clear an important register, leaving the previous content intact (0x77F8313C, 0x77E89B18, or 0x77EA094C)
  
- The 25<sup>th</sup> and 26<sup>th</sup> bits in the scan address remain constant in any worm execution instance. Because the seed is chosen with good randomization (GetTickCount) and the number of worms are huge, it is likely that all IP addresses are probed equally.

CS6814: Fall 2003 Washington University in St. Louis

## How the Internet responded

- Although people responded quickly to Slammer (within an hour, many sites began filtering all UDP packets with a destination port of 1434 via router or firewall), it was long after Slammer had infected almost all susceptible hosts.
- Slammer has distinctive filterable signature. It exploited a uncommonly used service vulnerability, so that all traffic blocked were mostly worm-scanning traffic.

## Why Slammer caused problems

- Grateful to Slammer's author: **Payload is not malicious**
- Slammer caused significant disruption to financial, transportation, and government institutions, due to the saturated Internet links by worms' packets and equipment failures by exhausting CPU or memory resources.
- **Warnings:**
  - To prevent a few machines from monopolizing network resources using this kind of DoS attack, critical networks should employ traffic shaping, fair queuing, or similar techniques.
  - Although Slammer is the first super-fast worm released so far, techniques exist for smaller and faster worm in the future.
  - Vulnerabilities of less popular software become more and more attractive to the attacks.
  - New techniques and tools need to be developed to automatically detect and respond to worms.