

Worm Defense #1

10th March, 2008

Ashima Atul

1 Review of previous lecture

- Discussed historic worms like Code Red, Slammer, Nimda and many more.
- Talked about the trajectory of CDC (Center for Disease Control)

Note: Figure 6 in the paper shows that the mathematics related to the spread of the worm is correct.

2 Worm study (Continued)

2.1 Finding Targets

- Worms discussed in the previous lecture used random scanning to find targets. This technique can be biased.
 - It is said that the huge address space provided by IPv6 may make worms ineffective. This may not be the case in the real world since people tend to use the same type of addresses like x.x.x.1, x.x.x.2 and so on.
- Hit-lists
 - The worm author collects lists of vulnerable machines in advance.
 - Some worms like the Witty worm used this technique.
 - Hit-list does not have to be fully accurate.
 - With this technique the target gets a much better range of vulnerable population.
 - Scans used to build the hit-list can go undetected as background noises.
 - Attackers can also use brute-force scanning or outsource the scans.
- Permutation scanning
 - Assumption: Worm can detect that a particular machine is already infected by it.
 - Worms require random permutation of address space.

- In permutation scanning, all worms have a common pseudo random permutation of the IP address space.
- A 32-bit cipher and key generates the permutation.
- Encrypt the index to get the corresponding address and decrypt to get the index back.
- A newly infected machine jumps to a part in the address space by generating a random value and applies cipher to it to get the address. If the machine is already infected, it chooses a new, random value and proceeds from there.
- If you find infected addresses too often then you know the worm has spread completely. This technique can also be used for worm killing/cleaning.
- This scheme will generate less scans.
- This technique is provably perfect and it is easy. Any decent block cipher will work for this.
- Topological scanning
 - Uses local information of the machine for selecting new targets. Morris worm used this technique.
 - It is harder to detect this type of scanning because the connections made are plausible.
 - Can be used in peer-to-peer applications and web servers.
- Meta-Server
 - Similar to topological scheme.
 - Metaservers can be queried to discover the vulnerable machines (example gaming servers).
 - A worm using this can quickly spread even when the vulnerable population is small.

2.2 Worm Defense

- White worms - They basically counter the effect of a worm when it is detected. These are not effective because a worm can easily fix itself before detection, and there are also issues of control over the worm and legality if machines accessed belong to others.
- Autopatching - involves quick spreading of fix across addresses.
 Note, there has been work at Columbia University that involves taking a worm and automatically synthesizing a patch for the worm. This approach is risky because the patch might cause damage.

2.3 Worm Approaches

- Flash Worms
 - Build an entire hit-list in advance and then run it using divide and conquer.
 - A single well connected node (“detonator”) infects first 10,000 addresses, sending each a list of 100 addresses to infect in turn. Thus, no network stress other than at top level.
 - *Solution:*
 - * Techniques that can spread fast like flash worms.
 - * Do not allow fast spreading thus reducing the fast fan out from the detonator.
- Contagion worm - Nimda had a form of this.

2.4 Command and Control (C&C)

- Goal is resiliency of C&C.
- Similar thinking is in botnet C&C.
- It will be problematic if the attackers design C&C well.

2.5 Worst case worm

- It is not hard to find exploits.
- An attacker can attain hosts using firewall crossing techniques.
- Worm quality depends on the quality of the testing lab of the attacker.
- Geographic targeting is not hard.
- What’s the damage?
 - Alter data/export data - difficult to understand/detect this.
 - Disk wipeout.
 - Reformatting BIOS so that the machine does not boot.
 - It can be at the level of a natural disaster but clean assessment is not clear.

3 Polygraph

3.1 Extracting Signatures

- Signature based techniques use a model where a machine is already infected.
- These techniques are not used to save a machine that is already infected. Instead their aim is to share the signatures of the worms to save other non-infected machines.
- It does not defend sites in isolation.

3.2 How to get the pool?

- Honeycomb
 - Malicious pool provided by honeypot traffic.
 - There is no benign pool since benign users should not be using honeypot.
 - Uses longest substring match method.
- Autograph
 - Polygraph's predecessor.
 - Uses pools of malicious and benign traffic.
 - Takes byte streams and breaks them into blocks.
 - Can do it in a cheap way.
 - Runs hash over a window. At some point it will match a host you found before.
 - Need flows to be coming from different sources.
 - Brings in the behavioral aspect of worms.
- Earlybird
 - Developed in the same time as Autograph.
 - Does not need the pool.
 - Keeps watch for every flow.
 - This has been commercialized. It is used for detecting clustered information.
 - This technique found worms that had not been publically found.

Note: Defense papers should be viewed as a step towards solving a problem and not as proposing a complete solution.

3.3 Polymorphism

Assumptions:

- Using signatures is not robust because attackers can change the attack using polymorphism.
- Each worm sample contains code that is encrypted with a key. The execution of a worm starts from a routine that does decryption. An obfuscator generates different bytes for each worm sample.
- Obfuscator is small and there are many variants, thus it is difficult to fingerprint it.

3.4 Method

All the signatures are built from tokens

- Conjunction signatures - A set of n tokens found in the payload.
- Subsequence signatures - Ordered set of tokens found in the payload.
- Bayesian signatures - Likely to be a worm if it has enough tokens to be above the threshold.

Polygraph uses the notion of clustering in case of multiple signatures

3.5 Analysis of the paper

- Putting aside the issue of degrees of freedom in polymorphism, it is not clearly stated how general their model is.
- Top part of figure 5 is blank. It is not clearly stated what the blank part means.
- The paper does a decent job thinking about adversarial attacks. The Long tail attack discussed in paper is not at all obvious.

3.6 How to attack such systems

- Poisoning the training data.
- Limit the number of invariants in polymorphic traffic. For example Slammer worm has one invariant byte and that is the request. Thus, it is difficult to handle such kind of worms.