경량화 에이전트를 이용한 분산 웜 탐지 및 방지 모델

박연희[0], 김종욱[1], 이성욱[2], 김철민[3], 우즈만[4], 홍만표[5]
아주대학교 디지털 백신 연구실[0145], 신구대학교[2], 시스온칩[3]
{piaoyj[0], kju[1], usman[4], mphong[5]}@ajou.ac.kr, suleeip@shingu.ac.kr[2], cmkim@sysonchip.co.kr[3]

Distributed Worm Detection and Prevention Model with Light-Weight Agent

Yanji Piao[0], JongUk Kim[1], Seong-uk Lee[2], Cholmin Kim[3], Usman Tariq[4], Manpyo Hong[5]
Digital Vaccine Laboratory Ajou University[0145], Shingu College[2], SysOnChip(Inc)[3]

A worm is a malware that propagates quickly from host to host without any human intervention. Worms are able to propagate in a very short time and cause the entire networks to be paralyzed. Signature based virus detection mechanisms are commonly used by many security software vendors. Signature-based IDS [1,2] capture worm attacks based on pre-compiled signatures stored in database. Signature based detection mechanisms can detect well-known worms easily but it is hard for them to identify unknown worm. The threshold-based detection method [3] require relatively high threshold to reduce a false positive. Hence, it is poor to realize early detection. Our previous research of this paper [4] was Distributed Worm Detection Model based on packet marking. Each host informs the possibility of worm propagation to recipients using packet marking technique in Distributed Worm Detection Model. If a marking counter is larger than the threshold, the host considers this packet as worm packet and stops further transmission of packet. However, in this situation, blocking of packet transmission just happens in the host where its marking counter is greater than the threshold, and parent of the host still deliveries packets. Thus our previous method is not perfect and our new approach is complementary to this effort.

To increase effectiveness of proposed solution, in this paper we present mechanism of detection and prevention of worm in distributed fashion. Proposed model neither increases the network traffic nor requires any special processing servers. Now we explain the situation of the scenario of worm detection and prevention based on our idea in 6 steps. Step1 to Step5 are backward reporting scheme, Step6 is forward reporting scheme. Let's assume that the host 'A' has been infected by worm. **Step1**. The worm in host 'A' becomes active. It replicates itself and propagates to B, C, F, and G. Host 'A' embeds a marking counter value 1 and a report value (1 or 0) in fragmented IP header identification field before delivering the packets to next hop. **Step2**. After receiving the marking embedded packet at host B, C, F, and G, the receiving nodes will try to connect with other hosts; and the marking counter in packet will be increased to inform other hosts that it is a continuous connection. When one host gets packets with several different marking counters, we only considers the maximum value. **Step3**. If the marking counter in received packets is greater than the predefined threshold, these packets are considered as suspicious and the host stops delivering these packets. Thus the packet is considered as a worm if the depth of infection tree is over a certain value. **Step4**. Each host which has greater

than the predefined threshold decides whether it should report packet information to its parent by analyzing its report value in received packets. **Step5**. After receiving the report, host stops the delivery of packets and reports to its parents until the parent is discovered. **Step6**.Each host which has greater than the predefined threshold will report to its neighboring hosts and let neighbors turn into the immune state. In this case, we assume that a host knows all of its neighbors. From our results comparing the paper [4] (no reporting scheme) and forward reporting scheme in our research, we can confirm the intuitive result that forward reporting scheme can lower the peak of total amount of infected hosts. And we can confirm the result that raising the threshold value for the purpose of decreasing false positive can also prevent hosts from infecting. The greater the threshold is, the higher the peak of the number of infected hosts becomes with no reporting. But in Model 2, as the threshold goes higher, the peak value becomes little higher.

Upon worm detection, node will forward, an alert repot to neighboring node which helps to increase the immunity of the whole system and the number of infected hosts would be decreased even if worm propagation is continued. And our model neither needs to maintain a huge database of signatures nor needs to have too much computing power, that is why it is very light and simple. So, our proposed scheme is suitable for the ubiquitous environment. Simulation results illustrate better detection and prevention which leads to the reduction of infection rate.

References

[1] Martin Roesch. "Snort-lightweight intrusion detection for networks", In USENIX Large Installation Systems Administration Conference, Seattle.WA.USA. November 1999.

[2] Vern Paxson, "Bro: a system for detecting network intruders in real-time", Computer Networks, 1999.

[3] H.A.Kim, B.Karp, "Autograph: Toward Autumated, Distributed Worm Signature Detection", In Proc. Of 13th Usenix Security Symposium, August.2004.

[4] Kangsan Lee, Cholmin Kim, Seong-uck Lee, Manpyu Hong, "Macroscopic Treatment to Unknown Malicious Mobile Codes", Journal of KISS, 2006.