Slide #1:

Hi, my name is Cliff Zou. I will talk about our work on worm modeling and analysis under dynamic quarantine defense.

Slide #2:

First, the motivation. In recent years, fast spreading worms, such as Code Red, Nimda, Slammer, and Blaster, have created serious challenge and security threats to our Internet. These worms spread out very quickly, infected most vulnerable hosts before people took any actions. The SQL Slammer was a super fast worm that infected 90% of vulnerable SQL servers on the whole Internet within just 10 minutes. For these fast-spreading worms, human's manual counteractions cannot match with worm's speed.

Automatic mitigation is the only way to defend them. However, current automatic mitigation has the problem that the false alarm cost is too high. For unknown worms, automatic mitigation relies on anomaly detection, and anomaly detection systems usually have problem of high false alarm rate. In addition, traditional quarantine is a dramatic action, changing from no quarantine at all to quarantine a whole network for a long time until security staffs finish inspection. Because human's response is much slower than machine time, many healthy hosts will be quarantined for too long time and the false alarm cost is too high.

Slide #3:

When we study automatic mitigation, we think that since Internet worms are very similar to epidemic diseases in the real world, why can't we learn from the experiences in real-world epidemic disease control, such as SARS incident in this summer? After study, we find out that people have used two quarantine principles in epidemic disease control.

Principle #1, "preemptive quarantine". In other words, the principle is "assuming guilty before proven innocent". For example, during this summer, if a patient in Hong Kong exhibits fever symptom, the patient will immediately be quarantined, even though maybe the patient only has 1% probability to be infected by SARS virus.

Principle #2, "feedback adjustment". People will take more aggressive quarantine actions when they anticipate that the epidemic is more serious, the disease is more infectious. For anther example of SARS, during the summer, if a patient in US exhibits fever symptom, the patient will not be quarantined. But, if at that time, US had the same epidemic situation as in Hong Kong or Beijing, the patient will probably be quarantined immediately. It means that in real-world epidemic control, quarantine action is not just

based on disease symptom; it is largely based on people's anticipation of the epidemic situation. In this way, the epidemic disease control is in fact a feedback system.

The SARS incident in this summer has proven that these two principles are effective and necessary in controlling contagious diseases.

Slide #4:

Based on the first principle in real-world epidemic disease control, we design a dynamic quarantine system. In the context of worm defense, the first principle, "assuming guilty before proven innocent", means that: when we find a host is sending out suspicious traffic, we will quarantine this host immediately, though we may wrongly quarantine some healthy hosts. Then we will release the quarantine after a short time automatically. Why do we want to automatically release quarantine? Because if we only release quarantine after security staffs inspect those quarantined hosts, then the false alarm cost will be too high. So the quarantine system we present here is a graceful automatic mitigation.

The quarantine system can use any host-based or subnet-based anomaly detection method. And the quarantine action is on each individual host or subnet, not a whole network-level. Note that the quarantine here means that we only block traffic to the suspicious port on a quarantined host. In this way, all other Internet connections to the quarantined host will not be affected.

Slide # 5:

Based on the second principle, the feedback principle in real-world epidemic disease control, we propose this feedback control dynamic quarantine system. Here is the host-level feedback dynamic quarantine system. We first introduce the quarantine system where quarantine action is on each host. In the context of worm defense, the feedback principle means that when we suspect more that we are under attack by a worm, we will take more aggressive quarantine actions.

This feedback control system uses the same idea. I_t is the number of quarantined hosts, and K_i is the anomalism of each alarmed host. When they increase, we have higher probability to anticipate that current alarm incident is caused by a worm, and the damage will also be higher. Then we should take more aggressive action: we should quarantine alarmed hosts longer (increase T_t), and we should let anomaly detection to be more sensitive to worm's traffic (decrease alarm threshold H_t).

Slide #6:

On the whole Internet level, we cannot do quarantine on each host. Thus we propose this two-level hierarchical feedback control dynamic quarantine system. The lower level is on each local network, using the host-level feedback quarantine system presented in previous slides. On the Internet scale, we can set up a higher level feedback control dynamic quarantine system: the quarantine is implemented on each edge router or gateway of local networks. Each local network sends observation data I_t to the Malware Warning Center. The MWC makes decision and sends back recommended values of quarantine time and alarm threshold. In the feedback quarantine system in a local network, the alarm threshold and quarantine time are determined both by local worm detection system and by the advisory from MWC.

Slide #7:

In this paper, we take the first step towards that feedback control system. We first study the simple case where there are no feedback and optimization issues. We just consider the dynamic quarantine system with fixed quarantine time and alarm threshold. Based on two traditional epidemic models, in this paper we have derived worm propagation models for such dynamic quarantine system. We show that a worm still propagates according to epidemic models, but the dynamic quarantine efficiently reduces worm's spreading speed. It will give people precious time to take counteractions at the cost of temporarily quarantine some healthy hosts. Because the quarantine time is small, such cost will not be too big. In addition, dynamic quarantine will raise the epidemic threshold of a worm, making it to have smaller chance to spread out.

Slide #8:

Because our models are extended from two traditional epidemic models, here we first introduce these two epidemic model. First, the simple epidemic model. This model assumes that a host is either susceptible, or infectious. And the state transition can only be susceptible to infectious. It assumes that the number of contacts between the group of infectious and the group of susceptible are proportional to the product of their sizes. Thus the simple epidemic model for fixed population system is this. I(t) is the number of infectious hosts at time t; S(t) is the number of susceptible. N is the population size. This curve shows the number of infectious hosts I(t) as a function of time t. It is also called logistic curve, or simply "S" curve.

Slide #9:

The next model, Kermack-Mckendrick model, is extended from the previous simple epidemic model. It considers that some infectious hosts will either recover and immune to the disease, or die from the disease. Thus some hosts will be removed from infectious as shown in this state transition diagram.

Denote U(t) to be the number of removed hosts from infectious. \gamma is the removal rate. Then this is the dynamic equation: this part (black one) is the original equation for simple epidemic model; KM model adds this term (U(t)) in. The figure shows the worm propagation under different removal rate. Gamma equals to zero gives the simple epidemic model. One important theorem from Kermack-Mckendrick model is the epidemic threshold theorem: If the number of initially vulnerable hosts is smaller than a threshold, \rho, then the worm will not spread out because under this situation, the worm's infection speed is slower than its removal speed. \rho can be called epidemic threshold.

Slide #10:

Now we analysis worm's dynamics under the dynamic quarantine defense. T is the quarantine time. R(t) is the number of quarantined infectious hosts; Q(t) is the number of quarantined vulnerable hosts. For the anomaly detection system in the quarantine system, the detection threshold can be formed into two parameters: \lambda_1 is the quarantine rate of infectious, which should be as high as possible to detect an infected host quickly; \lambda_2 is the quarantine rate of susceptible, which should be as low as possible to have less false alarms.

First, we consider the worm propagation that no infected hosts will be removed. Since any quarantine host will be released from quarantine after the quarantine time T, then at time t, all quarantined hosts in R(t) are quarantined during time t-T to t. The quarantine rate is \lambda_1, thus this is the number of quarantined during small time interval d\tau.

However, we cannot solve this integral equation directly, but we can solve it by using approximation. Remember that the quarantine time T is not big, if R(t) and I(t) do not change much during the small time interval t-T to time t, then we can roughly treat R(t) and I(t) as constants in this time period. Therefore, the integral equation becomes this linear equation and it turns out that R(t) is proportional to I(t). This is the ratio. We can use the same way to derive Q(t) like this.

Slide #11:

Suppose in the original system before we implement quarantine, a worm propagates according to simple epidemic model. When we add dynamic quarantine in the system, this figure shows the interactions between the susceptible group and infectious group: all hosts in Q(t) and R(t) are isolated, thus the number of contacts is proportional to this. The dynamics of the worm follow this simple epidemic model before the quarantine, and follow this equation after the dynamic quarantine. It shows that a worm still propagates according to simple epidemic model, but with slower infection rate \beta.

Slide #12:

We run simulations to verify our analysis. We use the simulation parameters similar to Slammer worm. The red curve is the worm's propagation in the original system where there is no quarantine. After we implement dynamic quarantine, the worm propagates much slower, but still follows simple epidemic model.

The second figure shows the I(t), R(t), and Q(t) as time goes on. Because the false alarm rate is small, Q(t) is much smaller than R(t), thus we multiply Q(t) with 500 in order to show them in the same figure.

The third figure shows the ratios p_1 and p_2 from the experiment and compares them with their theoretical values. It shows that our analysis is accurate for most part of worm propagation. At the beginning, p_1 is not accurate because this equation of R(t) uses \lambda_1. Its accuracy relies on law of large number: at the beginning, I(t) is very small, thus this equation is not accurate for the beginning part. It is also the reason for the large oscillation of p_2 in the later part because there are not many susceptible hosts left during this time period.

Slide #13:

Suppose in the original system before we implement quarantine, a worm propagates according to Kermack-Mckendrick model. This part of the equation is the formula for simple epidemic model case. When we add dynamic quarantine in the system, we should consider the removed hosts in this formula. R(t) is still proportional to I(t), but with different ratio, q_1.

Because only infectious hosts can be removed, the removal will not change susceptible hosts. Thus the formula of Q(t) is not changed; the ratio q_2 is equal to p_2.

Before quarantine, a worm follows this Kermack-Mckendrick model. After quarantine, the worm still follows KM model, but with slower infection rate \beta, and higher epidemic threshold \rho.

Slide #14:

This figure shows the number of infectious hosts, I(t), for the original system and the quarantine system. The third figure shows the ratios q_1 and q_2 from the experiment and compares them with their theoretical values. It shows that our analysis is accurate for most part of a worm's propagation.

Slide #15:

In previous slides, we have extended two traditional epidemic models to consider dynamic quarantine defense. However, a more realistic dynamic quarantine scenario is this: Security staffs do not have time to inspect every host in the system --- they only have time to check part of those quarantined hosts.
Thus not like KM model, the removal here is only from quarantined infectious hosts. The relationships of Q(t) and R(t) are the same as in KM model case, the only change is that here it is R(t) instead of I(t). When we implement such dynamic quarantine in the system, the worm propagates slower, and we have created this epidemic threshold.

Slide #16:

Here we show the simulation results. This blue curve is the worm's propagation under dynamic quarantine defense. If we do not implement dynamic quarantine, the worm will propagate like this (red curve). The ratios in this (third) figure show that our analysis is accurate for the major part of worm propagation.

Slide #17:

Summary. In this paper, we find out that in the epidemic disease control in real world, people have used two principles: preemptive quarantine, and feedback adjustment. They have been proven to be efficient and necessary. Based on these two principles, we present a two-level hierarchical feedback control dynamic quarantine framework. The central idea is: when we suspect more that current alarm incidents are caused by a worm, we will take more aggressive quarantine actions. The optimal control objective is to make a trade-off between defense strength and false alarm cost. Since in the feedback control dynamic quarantine system, the quarantine action is adaptively adjusted by the network situation, so we believe that with careful design, the system can take appropriated quarantine actions under different situations. For the open-loop system where quarantine time and alarm threshold are fixed, we present several worm propagation models. These models show that dynamic quarantine defense can slow down worm's propagation, thus security staffs can have precious time to take counteractions. The dynamic quarantine also can raise or generate the epidemic threshold, making a worm to have less chance to spread out.