Recent Results in Web Security
Content Sniffing Attacks, Insider Attacks, and Botnet Detection

Conrad Stansbury and Dennis Wang

Stanford University

December 1, 2014

Outline

State of Web Security

Server Side Content Sniffing Detection

Hybrid Schemes for Insider Attack Detection

Differentiating Botnets from Flash Crowds

Future Prospects and Challenges

Attacks Originating Outside the Network

State of the Art

- We have seen many techniques exist in ML for intruder detection
- Hybridized schemes allow the construction of strong IDS/IPS with acceptable FP rates
- High stakes game means lots of research (from the perspective of both detection and anti-detection advocates!)

Challenges

- Security is largely a reactionary field
- Intruders just have to evade whatever particular defenses are in use at their target
- In many cases, intruders just have to make their traffic look like typical traffic to get by, and there is a wide diversity of types of traffic and flow patterns

Attacks Originating Inside the Network

State of the Art

- Signature based schemes as well as anomaly detection schemes
- Today we will see a hybridized scheme that successfully bridges gaps in signature and models and HMMs

Challenges

- More and more attacks are insider attacks
- Difficult to defend because insiders often have increased privileges relative to outside connections–established trust
- Most security techniques defend against inbound traffic
  - High volume of attack from exterior
  - Unwanted disturbances of workflow not well tolerated

Outline

State of Web Security

Server Side Content Sniffing Detection

Hybrid Schemes for Insider Attack Detection

Differentiating Botnets from Flash Crowds

Future Prospects and Challenges

Outline

State of Web Security

Server Side Content Sniffing Detection

Hybrid Schemes for Insider Attack Detection

Differentiating Botnets from Flash Crowds

Future Prospects and Challenges

Outline

State of Web Security

Server Side Content Sniffing Detection

Hybrid Schemes for Insider Attack Detection

Differentiating Botnets from Flash Crowds

Future Prospects and Challenges

The Problem

Detecting Botnets in Light of Similar Signals

- Flagging malicious traffic on the basis of volume is insufficient
- Legitimate traffic often spikes as a result of world events
  - World events
  - Link aggregators and "virality"
- If we can't separate attack traffic from these natural surges we can't stop DDoS–blocking real traffic is a DoS

Anti-detection

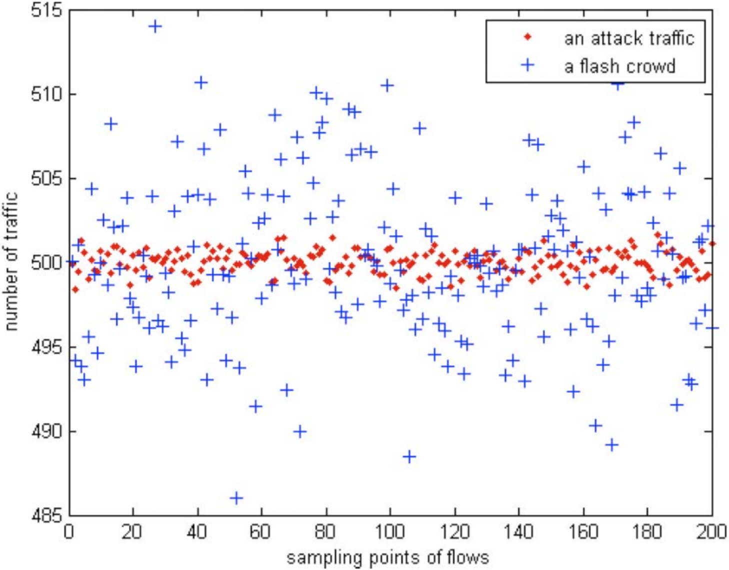
- Attackers would like to disguise their traffic by making it look like a flash crowd
- Flash crowd aware systems might accept attack traffic if it is sufficiently similar

Differing Signatures Between Botnets and Flash Crowds

Key Observation

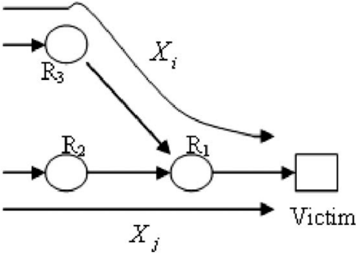
- Studies indicate that attack tools/dispatch scripts are homogeneous inside a single botnet
- Fewer bots than real users
- If an aggregate attack flow is composed of attack flows from many similar bots, it has a similar flow standard deviation to that of one bot
- We should expect that attack traffic has low standard deviation

Differing Signatures Between Botnets and Flash Crowds



Detection Scheme Overview

What is a flow?



$$r_{X_i,X_j}[k] = \frac{1}{N}\sum_{n=1}^{N} x_i[n]x_j[n+k].$$

$$\rho_{X_i,X_j}[k] = \frac{r_{X_i,X_j}[k]}{\frac{1}{N}\left[\sum_{n=1}^{N-1} x_i^2[n]\sum_{n=1}^{N-1} x_j^2[n]\right]^{1/2}}$$

Exploit Flow Correlations

- Flow is network exterior node traffic to a particular destination
- Compute pairwise correlation of discretized flow for different offsets of the flow vectors
- Choose correlation to be maximum among these
- Similarity measure: correlation coefficient

Detection Scheme Overview

Correlation Coeffient Cutoff for IDing Traffic

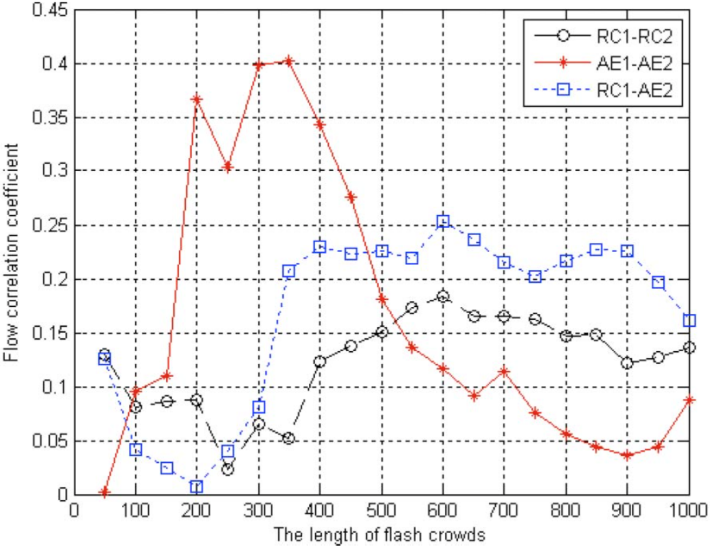
- Following premise that botnet traffic has higher correlation coefficient, choose some cutoff parameter δ
- Correlation at nodes i, j flagged as malicious ($I_{X_i,X_j} = 1$) if

  $$\max_k(\rho_{X_i,X_j}[k]) > \delta$$

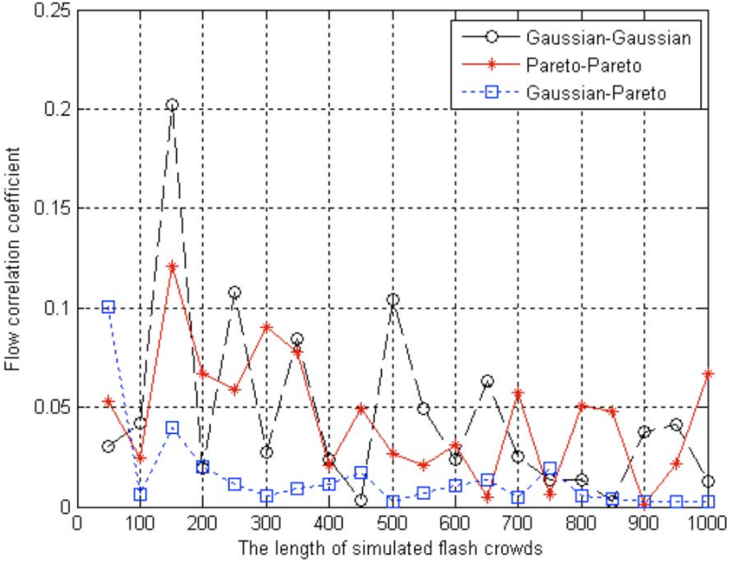
  not malicious ($I_{X_i,X_j} = 0$) otherwise
- Another independent parameter δ' is used to determine whether an attack is ongoing based on the I's
- Being attacked when

  $$\frac{\sum_{i \neq j} I_{X_i,X_j}}{\binom{M}{2}} > \delta'$$

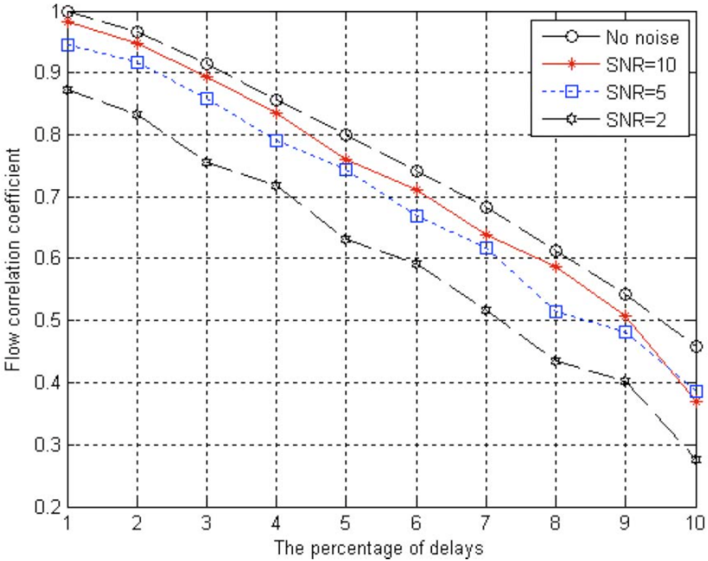
Results: World Cup



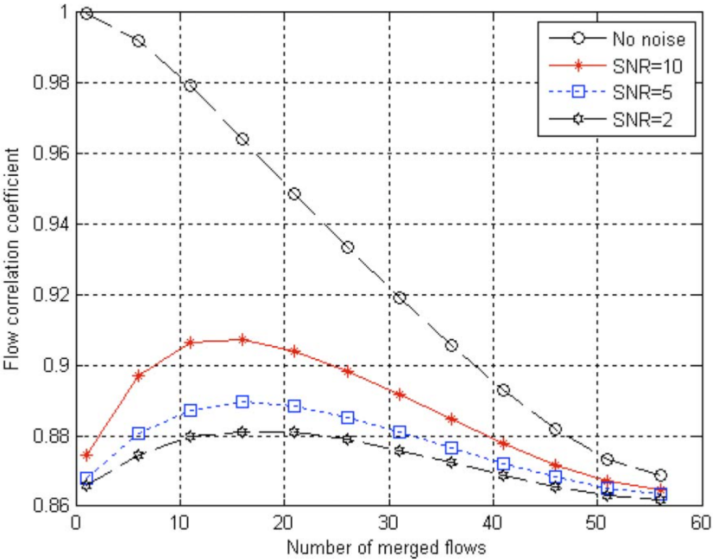
Results: General Flash Crowds



Results: Attacks with Delays



Results: Aggregate Attack Merging



Outline

State of Web Security

Server Side Content Sniffing Detection

Hybrid Schemes for Insider Attack Detection

Differentiating Botnets from Flash Crowds

Future Prospects and Challenges

Where is the Field Headed?

Where is the Competition Headed?

Questions?

References

- Shui Yu and Wanlei, J. et al. 2012, Parallel and Distributed Systems IEEE. Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient
- Byungha Choi and Kyungsan Cho. 2012. Detection of Insider Attacks to the Web Server
- Barua, A. and Shahriar, H. and Zulkernine, M. 2011, Software Reliability Engineering IEEE. Server Side Detection of Content Sniffing Attacks