The Insecurity of Open Source Intrusion Detection Systems: A Case for Cryptographically-Inspired IDS Design

Syed Ali Khayam
Assistant Professor
Wireless & Secure Networks (WiSNet) Research Lab
School of EE&CS (SEECS)
National University of Sciences and Technology (NUST)
Islamabad, Pakistan
Malware Trends...

- Symantec reported a **468% increase** in previously-unseen attacks over a six month period in 2007.

- Symantec reports 1,656,227 malicious code threats detected in 2008 which represents over **60 percent** of the approximately 2.6 million malicious code threats that Symantec has **ever** detected.

- “We are projecting a **10-fold increase** in malware objects (in 2009 as was) detected in 2008” .....Ryan Naraine, the security evangelist for Kaspersky.
Current State-of-the-Art in IDS

**On Network Endpoints**

Current State-of-the-Art in IDS

100% accuracy!

On Network Gateway

Why do IDSs still fail?

The malware detection techniques rely on statistical testing and therefore can be fooled by test simulability. In other words whenever the underlying detection methodology is known, it is possible to build an attack to evade the IDS.

- social engineering
- reverse engineering
- fingerprinting
- trial and error
- polymorphic blending attacks
- mimicry attacks
- portscans, etc.

Reference:
Aim: Our main aim, as an attacker, is to estimate the *evasion margin* for the IDS. This evasion margin is the bound on the number of attack packets \( t \) that an attacker can send to a target entity (host/network) without detection!
Breaking Maximum Entropy IDS

~Configuration Parameters
- Threshold: $t_{KL}$
- Baseline distribution: $p(w)$
- Real-time distribution: $q(w)$

~Detection Principle

$$D_{p|q}(w) = p(w) \log \left( \frac{p(w)}{q(w)} \right) > t_{KL}.$$ 

Markovian stochastic model

$$H_{\text{max}} = \max_{i,j \{1,2...n\}} H(p_j \mid p_i)$$

- Real-time Observation
- Brute force
Breaking TRW-based IDSs

~Configuration Parameters

- Threshold: \( t_1 \)
- A priori probabilities:
  \[
  \Pr[Y_i = 0 \mid H_0] = q \quad \Pr[Y_i = 1 \mid H_0] = 1 - q = q_0
  \]
  \[
  \Pr[Y_i = 0 \mid H_1] = q \quad \Pr[Y_i = 1 \mid H_1] = 1 - q = q_1
  \]
  \[q_0 > q_1\]

~Detection Principle

\[
\Lambda(Y) = \prod_{i=1}^{n} \frac{\Pr[Y_i \mid H_1]}{\Pr[Y_i \mid H_0]} < \eta_1
\]

- Estimates if the local/remote host is a scanner
- Per host basis
Breaking TRW-based IDSs

Normalizing likelihood at the endpoint

Getting close to $\tau_1$

Likelihood ratio

Y_1 Y_1 Y_2 Y_3 Y_4 Y_5 Y_6 Y_7 Y_8 Y_9

$\tau_1$

NO ALARM!
IDSs under Configuration Estimation Attack

On Network Endpoints

IDSs completely Paralyzed!!!!!!
IDSs under Configuration Estimation Attack

On Network Gateway

IDSs completely Paralyzed !!!!!!
Lessons Learnt

- Current State-of-the-Art IDSs provide acceptable accuracy dividends on specific deployment points
- Cannot scale to different points of network deployment
- Statistical IDSs provide highest accuracy
- Trivial to break statistical IDSs with stochastic analysis
Cryptographically-Inspired Intrusion Detection

There is a need to revisit the IDS detection design philosophy in accordance with Kerckhoff’s principle of cryptography.
“The attacker has full knowledge of the workings of the system.”
Modeling IDS detection as an Information Channel Coding problem

\[
p(Y/X) = \begin{bmatrix}
  p(y_0/x_0) & p(y_1/x_0) & \cdots & p(y_{|Y|-1}/x_0) \\
  p(y_0/x_1) & p(y_1/x_1) & \cdots & p(y_{|Y|-1}/x_1) \\
  \vdots & \vdots & \ddots & \vdots \\
  p(y_0/x_{|X|-1}) & p(y_1/x_{|X|-1}) & \cdots & p(y_{|Y|-1}/x_{|X|-1})
\end{bmatrix}
\]

Transformation

\[
p(x) \rightarrow p(y)
\]

Thresholding

\[
q_{B,M}(x) \hat{\in} \{\text{anomaly, benign}\}
\]

\[
q_{B,M}(x)
\]
Modeling IDS detection as a Information Channel Coding problem

Minimizing the mutual information between input $p(x)$ and the output $p(y)$

$$\min_{p(y; q / x)} I(X; Y) = \min_{p(y; q / x)} \hat{a} \hat{b} p(x, y) \log \frac{p(y; q / x) \hat{b}}{p(x) \hat{a}} \hat{a} \hat{b} p(x, y) \log \frac{p(y; q / x) \hat{b}}{p(x) \hat{a}} \hat{a} \hat{b}$$
Modeling IDS detection as an Information Source Coding problem

\[ p(x) \rightarrow p(y) \rightarrow q_{B,M}(x) \in \{ \text{anomaly, benign} \} \]

\[ p(x) \rightarrow p(y) = p(x)p(y; q | x) \]

Uniform transition matrix defined as a function of the similar instances in the baseline distribution.
Intrusion detection on the non-overlapping boundary region between $p(x)$ & $p(y)$:

$$D(p(x) \parallel q_{B,M}(x)) \gg D \gg D(p(y) \parallel q_{B,M}(x)) \gg 2D.$$

Intrusion detection on the overlapping boundary region between $p(x)$ & $p(y)$:

$$D(p(x) \parallel q_{B,M}(x)) \gg D \gg D(p(y) \parallel q_{B,M}(x)) \ll D \gg 0.$$

Benign traffic window:

$$D(p(x) \parallel q_B(x)) \ll D \gg D(p(y) \parallel q_B(x)) \widehat{\ll} \{(< 2D \gtrless D) \hat{=} \gg D\}.$$
Thank you!

- Contact Information:
  - Email: ali.khayam@seeecs.nust.edu.pk
  - Web: http://wisnet.seeecs.nust.edu.pk