Aggregate Site Analyzer

Site-wide parameter: **Global Failure Indicator (GFI)**

– Site-wide # of failed logins per batch of x logins
Aggregate Site Analyzer

Site-wide parameter: Global Failure Indicator (GFI)

– Site-wide # of failed logins per batch of x logins

![Graph showing PDF of number of failed logins per 100 logins]

- Beta - binomial fit
- Binomial fit
- Test data
Aggregate Site Analyzer

Site-wide parameter: Global Failure Indicator (GFI)

- Site-wide # of failed logins per batch of x logins

GFI well-modeled as Beta–binomial (Binomial with beta-prior on probability of success)
Aggregate Site Analyzer

Monitoring for Change (CUSUM Algorithm)

\[ C_0 = 0 \]
\[ C_n = \max(0, C_{n-1} + X_n - \mu - k) \]

- \( X_n \) – Random variable (GFI)
- \( \mu \) – Mean under normal behavior
- \( k \) – Parameter based on magnitude of change to be detected

Graph showing test statistic \( C_n \) with sample no. (n) and scope of the attack.
Aggregate Site Analyzer

Monitoring for Change (CUSUM Algorithm)

\[ C_0 = 0 \]
\[ C_n = \max(0, C_{n-1} + X_n - \mu - k) \]

- \( X_n \) – Random variable (GFI)
- \( \mu \) – Mean under normal behavior
- \( k \) – Parameter based on magnitude of change to be detected

- CUSUM process modeled as a Markov chain
- Gives a framework to tune detector according to desired time-to false-alarm and detection
- After detection, use clustering of active remotes to identify distributed population
# Evaluation

## Aggregate Site Analyzer

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total number of attacks</strong></td>
<td>99</td>
</tr>
<tr>
<td><strong>Number of false attacks</strong></td>
<td>9</td>
</tr>
</tbody>
</table>

Determined by Attack Participants Classifier

## Attack Participants Classifier

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of attack hosts</strong></td>
<td>9,306</td>
</tr>
<tr>
<td><strong>Number of false attack hosts</strong></td>
<td>37</td>
</tr>
</tbody>
</table>

Determined by future successful activity/ Site Incident Database
Characterization of Attacks

Overlap of attack sources over different attacks

90 attacks constituted a total of 35 attack campaigns
Characteristics of Attack Campaigns

Stealthiness

<table>
<thead>
<tr>
<th>DETECTION COMPARISON</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>• Point-wise Host detector (0/35)</strong></td>
</tr>
<tr>
<td>On average 2 attempts per local machine per hour</td>
</tr>
</tbody>
</table>

Two of the campaigns succeeded in breaking-in; one undetected by the site

**31/35 – Partially detectable**

High-rate hourly activity in total number of failed attempts/ number of local hosts contacted

**• Undetectable by any point-wise detector (4/35)**
(a) LBL
Figure 3: The distribution of inter-keystroke timings for two sample character pairs.
Figure 5: Estimated Gaussian distributions of all 142 character pairs collected from a user.
Figure 8 graphs the probability that the real character pair appears within the $n$ most-likely character pairs against the threshold $n$.

Figure 8: The probability that the $n$-Viterbi algorithm outputs the correct password before the first $n$ guesses, graphed as a function of $n$. 
Figure 10: The percentage of the password space tried by Herbivore in 10 tests before finding the right password.
**IP Header Side Channel**

- **4-bit Version**
- **4-bit Header Length**
- **8-bit Type of Service (TOS)**
- **16-bit Total Length (Bytes)**
- **16-bit Identification**
- **3-bit Flags**
- **13-bit Fragment Offset**
- **8-bit Time to Live (TTL)**
- **8-bit Protocol**
- **16-bit Header Checksum**
- **32-bit Source IP Address**
- **32-bit Destination IP Address**
- **Payload**

**ID field is supposed to be unique per IP packet.**

One easy way to do this: **increment** it each time system sends a new packet.
Attacker  Patsy  Victim

Echo request
reply, ID=3
Attacker

Echo request
reply, ID=3

Patsy

+1
Echo request
reply, ID=4

Victim
Attacker | Patsy | Victim

- Echo request
  reply, ID=3
+1
- Echo request
  reply, ID=4
+1
- Echo request
  reply, ID=5
**Attacker**  
- Echo request  
  - reply, ID=3  
- Echo request  
  - reply, ID=4  
- Echo request  
  - reply, ID=5  
- TCP SYN, src=P, dst port=24  

**Patsy**  

**Victim**
Spoofed
**Attacker**

- Echo request
  - reply, ID=3
- Echo request
  - reply, ID=4
- Echo request
  - reply, ID=5
- TCP SYN, src=P, dst port=24

**Patsy**

**Victim**

no listener on port 24, RST generated
The diagram represents a sequence of network packets between three parties: Attacker, Patsy, and Victim.

**Attacker** sends an *Echo request* to **Patsy** with an ID of 3. Patsy replies with *Echo reply* with ID 4, and the Attacker responds with *Echo request* and ID 5. Patsy sends a *TCP SYN* to the Victim with source port P and destination port 24.

The Victim does not have a listener on port 24 and responds with a *TCP RST*.

The text in the diagram indicates that no listener was found on port 24, and an RST was generated.
Upon receiving RST, Patsy ignores it and does nothing, per TCP spec.
A (Attacker) -> P (Patsy)

- Echo request, reply, ID=3
- Echo request, reply, ID=4
- Echo request, reply, ID=5
- TCP SYN, src=P, dst port=24
- Echo request, reply, ID=6

V (Victim)

TCP RST

no listener on port 24, RST generated
- Echo request, reply, ID=3
- Echo request, reply, ID=4
- Echo request, reply, ID=5
- TCP SYN, src=P, dst port=24
- Echo request, reply, ID=6

no listener

TCP RST

no listener on port 24, RST generated
**Attacker**

- Echo request, reply, ID=3
- Echo request, reply, ID=4
- Echo request, reply, ID=5

TCP SYN, src=P, dst port=24

**Victim**

- no listener on port 24, RST generated

**Patsey**

- Echo request, reply, ID=6
- Echo request, reply, ID=7

+1
**Spoofed**

- **Attacker**
  - Echo request, reply, ID=3
  - Echo request, reply, ID=4
  - Echo request, reply, ID=5
  - TCP SYN, src=P, dst port=24

- **Patsy**
  - no listener

- **Victim**
  - TCP RST
  - no listener on port 24, RST generated
  - Echo request, reply, ID=6
  - Echo request, reply, ID=7
  - TCP SYN, src=P, dst port=25

- **TCP SYN-ACK**
  - listener exists on port 25, SYN-ACK generated.
**Attacker**

- Echo request
  - reply, ID=3

+1

- Echo request
  - reply, ID=4

+1

- Echo request
  - reply, ID=5

- TCP SYN, src=P, dst port=24

**Patsy**

- TCP RST, ID=8

**Victim**

- no listener on port 24, RST generated

- listener exists on port 25, SYN-ACK generated.

- TCP SYN-ACK

- TCP RST, ID=8

P has no state for this connection, so generates a RST, which increments the IP ID sequence.
**Attacker**

- Echo request
  - reply, ID=3
- Echo request
  - reply, ID=4
- Echo request
  - reply, ID=5
  - TCP SYN, src=P, dst port=24
- Echo request
  - reply, ID=6
- Echo request
  - reply, ID=7
  - TCP SYN, src=P, dst port=25

**Victim**

- no listener on port 24, RST generated

**Patsy**

- TCP RST

**Victim**

- listener exists on port 25, SYN-ACK generated.

**Attacker**

- listener exists!

- TCP SYN-ACK
- TCP RST, ID=8

**Victim**

- P has no state for this connection, so generates a RST, which increments the IP ID sequence.
Order approved

Your transaction has been approved.

Your order ID: 138730
First name: Geoff
Last name: Voelker
Card used with this order: 46****2205
Total amount charged: $64.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Geoff Voelker, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
Order approved

Your transaction has been approved.

Your order ID: 138731
First name: Kirill
Last name: Levchenko
Card used with this order: 46****2288
Total amount charged: $52.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Kirill Levchenko, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
Order approved

Your transaction has been approved.

Your order ID: 138730
First name: Geoff
Last name: Voelker
Card used with this order: 46****2205
Total amount charged: $64.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Geoff Voelker, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com
Order approved

Your transaction has been approved.

Your order ID: **138731**
First name: Kirill
Last name: Levchenko
Card used with this order: 46****2288
Total amount charged: $52.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

**NOTE:** Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Kirill Levchenko, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: **www.rxsup24.com**
Order approved

Your transaction has been approved.

Your order ID: 144571
First name: Geoff
Last name: Voelker
Card used with this order: 46*****4029
Total amount charged: $64.95

The following billing descriptor appear on your credit card statement:

medissue.com +12175686119

Tracking number will be sent on your email once medications will be shipped.

NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

Website menu --> Order status

Dear Geoff Voelker, if you have any questions regarding your order, shipping, please contact us at:

Customers support system: www.rxsup24.com