User Populations

- **Forgotten usernames/passwords**
  - Characteristics of **LEGITIMATE USERS**
  - Have past history of successful logins

- **Low-rate distributed bruteforcers**
  - Distributed across networks; the network being monitored sees only a few hits

- **Singleton bruteforcers**
  - Have a high rate of logins compared to distributed

Characteristics overlap of legitimate users and bruteforcers
<table>
<thead>
<tr>
<th>Time span</th>
<th>Jan 2005–Dec 2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH servers</td>
<td>2,243</td>
</tr>
<tr>
<td>Valid users</td>
<td>4,364</td>
</tr>
<tr>
<td>Distinct valid user/server pairs</td>
<td>10,809</td>
</tr>
<tr>
<td>Login attempts</td>
<td>12,917,223</td>
</tr>
<tr>
<td>Login successes</td>
<td>8,935,298</td>
</tr>
<tr>
<td>Remote clients</td>
<td>154,318</td>
</tr>
<tr>
<td>Attempts using passwords</td>
<td></td>
</tr>
<tr>
<td>successes</td>
<td>1,416,590</td>
</tr>
<tr>
<td>remote clients</td>
<td>119,826</td>
</tr>
<tr>
<td>SSH border flows</td>
<td>215,244,481</td>
</tr>
<tr>
<td>remote clients seen in flows</td>
<td>140,164</td>
</tr>
<tr>
<td>High-rate brute-forcers</td>
<td>7,476</td>
</tr>
<tr>
<td>Mean attempts per high-rate brute-forcer</td>
<td>382.84</td>
</tr>
<tr>
<td>Mean daily password login attempts</td>
<td>486.13 (σ = 182.95)</td>
</tr>
<tr>
<td>Mean daily users</td>
<td>116.44 (σ = 32.41)</td>
</tr>
</tbody>
</table>

Table 1: Summary of LBNL syslog and flow data.
Figure 1: Empirical CDF of the number of failed login attempts per hour until a success for legitimate user login efforts with forgotten or mistyped usernames/passwords.
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

- 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>Total number of attacks</td>
<td>99</td>
</tr>
<tr>
<td>Number of false attacks</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>Number of attack hosts</td>
<td>9,306</td>
</tr>
<tr>
<td>Number of false attack hosts</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>• Point-wise Host detector (0/35)</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: 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

<table>
<thead>
<tr>
<th>4-bit Version</th>
<th>4-bit Header Length</th>
<th>8-bit Type of Service (TOS)</th>
<th>16-bit Total Length (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>16-bit Identification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-bit Flags</td>
<td>13-bit Fragment Offset</td>
</tr>
<tr>
<td>8-bit Time to Live (TTL)</td>
<td>8-bit Protocol</td>
<td>16-bit Header Checksum</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32-bit Source IP Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>32-bit Destination IP Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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.
Attack \hspace{1cm} \textbf{PATSY} \hspace{1cm} \textbf{Victim}

- **Echo request**
  - reply, ID=3
- **Echo request**
  - reply, ID=4
- **Echo request**
  - reply, ID=5
  - TCP SYN, src=P, dst port=24
  - no listener on port 24, RST generated
- **Echo request**
  - reply, ID=6
- **Echo request**
  - reply, ID=7
  - TCP SYN, src=P, dst port=25
  - listener exists on port 25, SYN-ACK generated.
- **Echo request**
  - reply, ID=8
  - TCP RST, ID=8
  - 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: 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