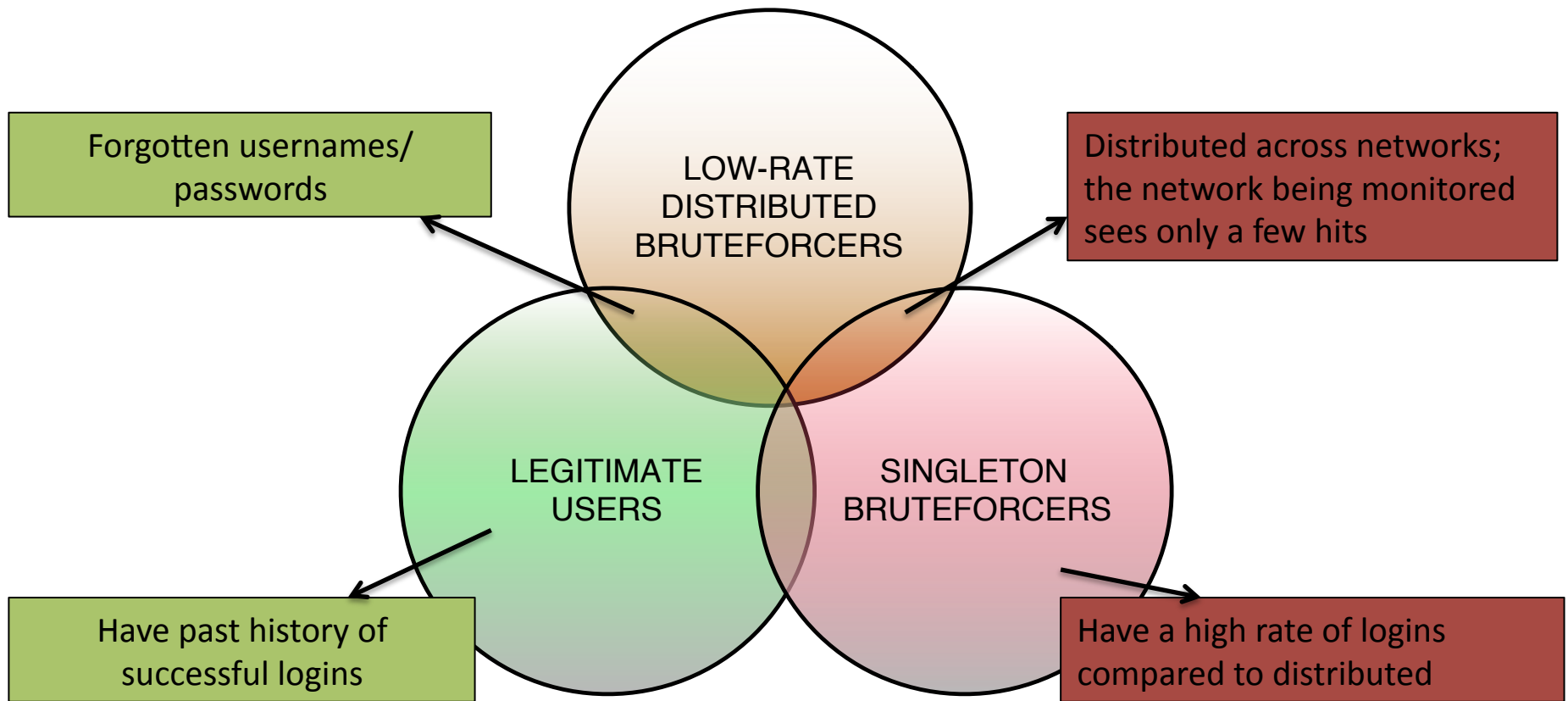


# User Populations



Characteristics overlap of legitimate users and bruteforcers

Time span	Jan 2005–Dec 2012
SSH servers	2,243
Valid users	4,364
Distinct valid user/server pairs	10,809
Login attempts	12,917,223
Login successes	8,935,298
Remote clients	154,318
Attempts using passwords	5,354,833
successes	1,416,590
remote clients	119,826
SSH border flows	215,244,481
remote clients seen in flows	140,164
High-rate brute-forcers	7,476
Mean attempts per high-rate brute-forcer	382.84
Mean daily password login attempts	486.13 ( $\sigma = 182.95$ )
Mean daily users	116.44 ( $\sigma = 32.41$ )

Table 1: Summary of LBNL syslog and flow data.

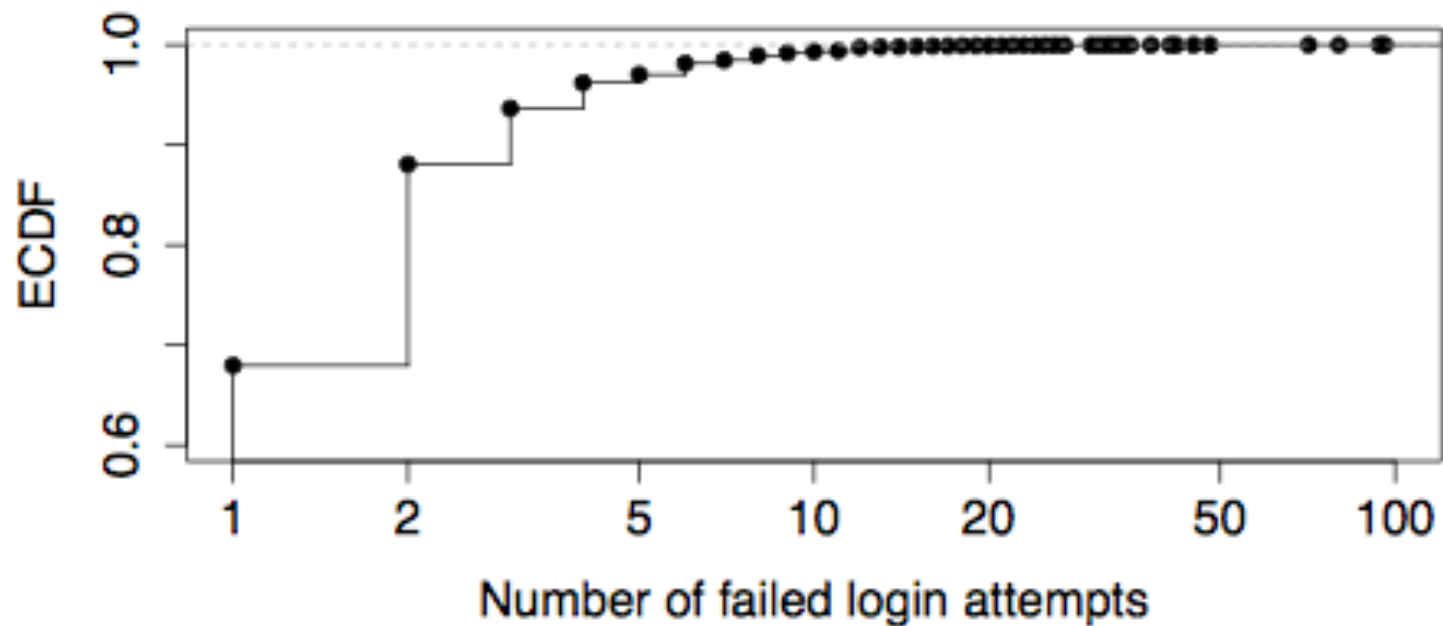
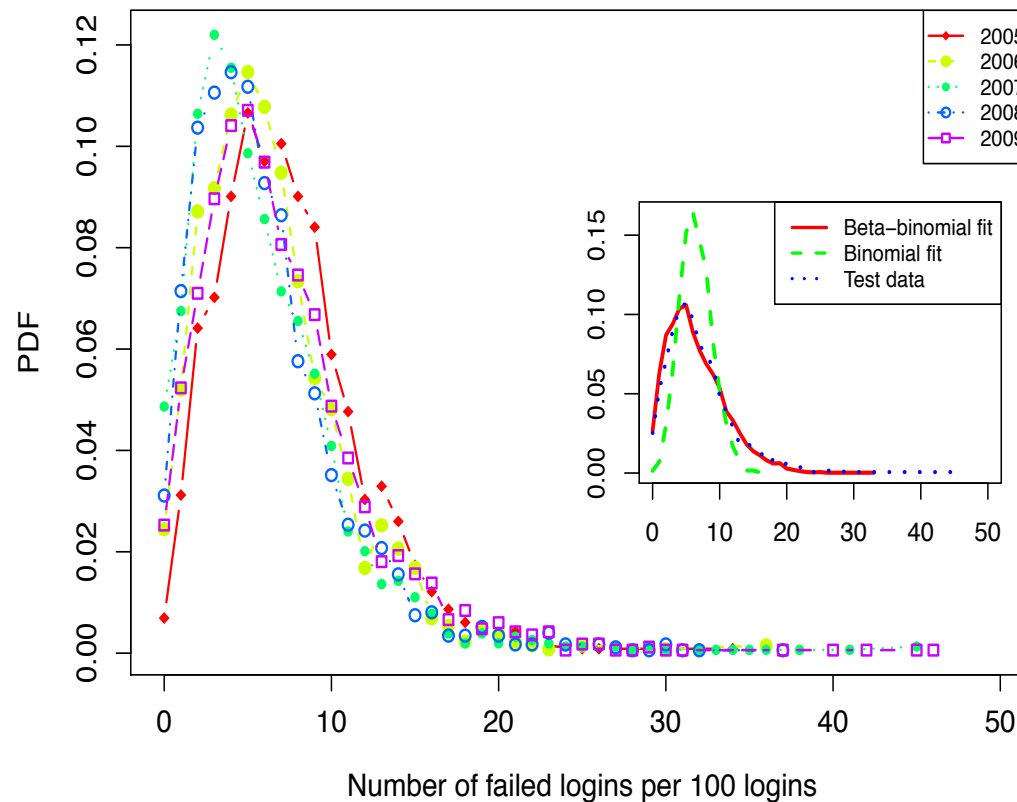


Figure 1: Empirical CDF of the number of failed login attempts per hour until a success for legitimate user login efforts with forgotten or mistyped usernames/passwords.

# 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)

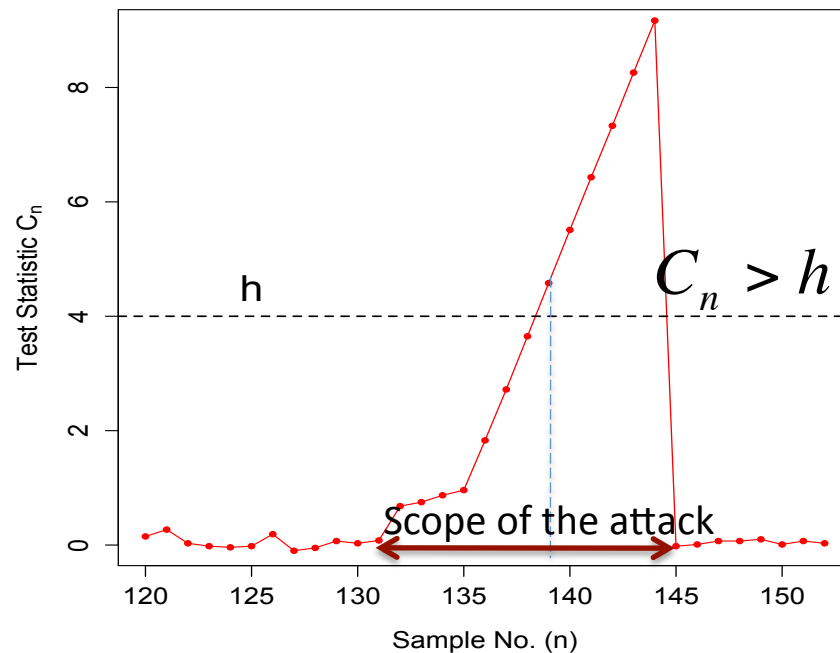
$$C_0 = 0$$

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

$X_n$  – 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	
<b>Total number of attacks</b>	<b>99</b>
Number of false attacks	9

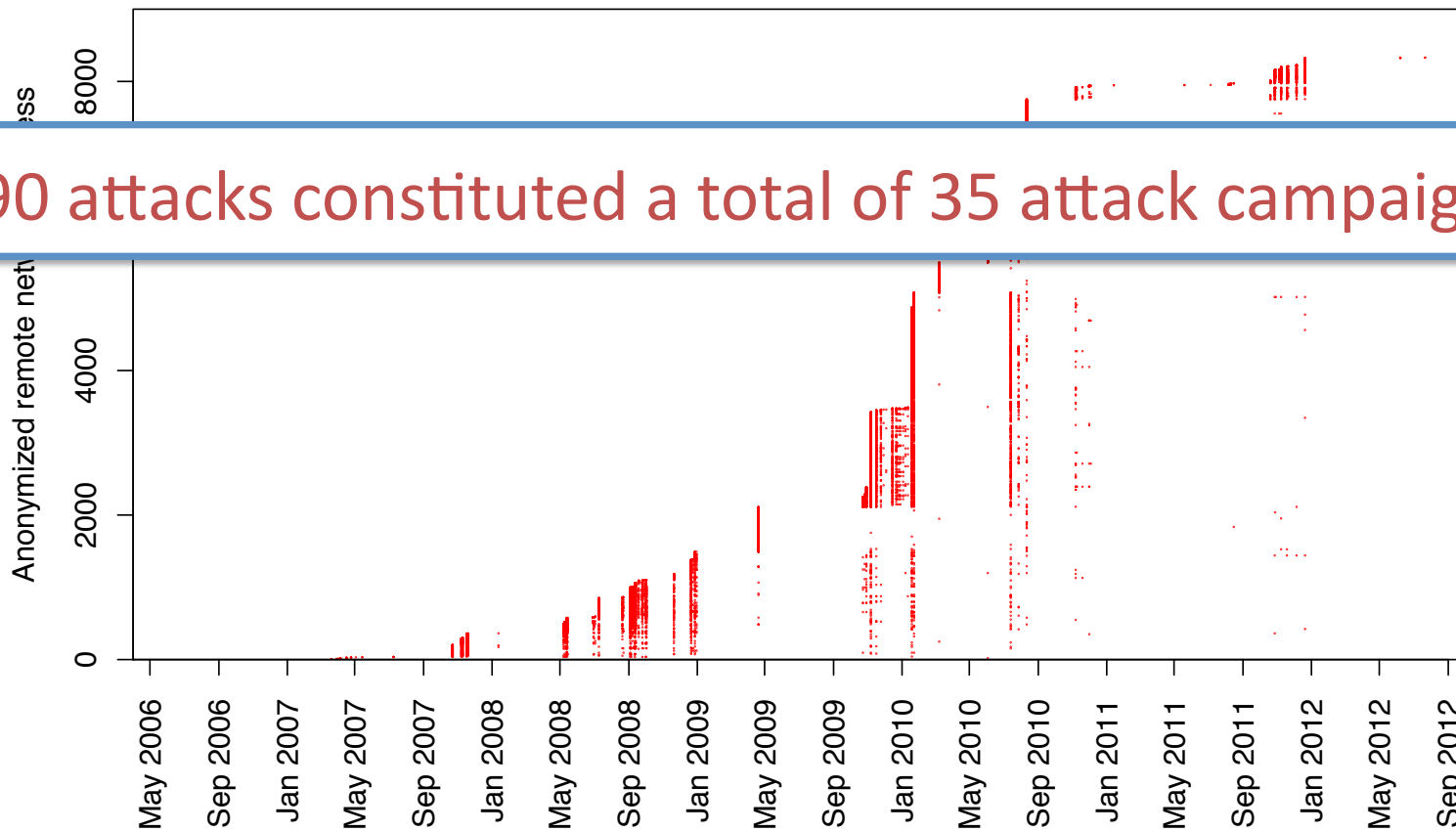
Determined by Attack Participants Classifier

Attack Participants Classifier	
<b>Number of attack hosts</b>	<b>9,306</b>
Number of false attack hosts	37

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

### DETECTION COMPARISON

- Point-wise Host detector (0/35)

On average 2 attempts per local machine per hour

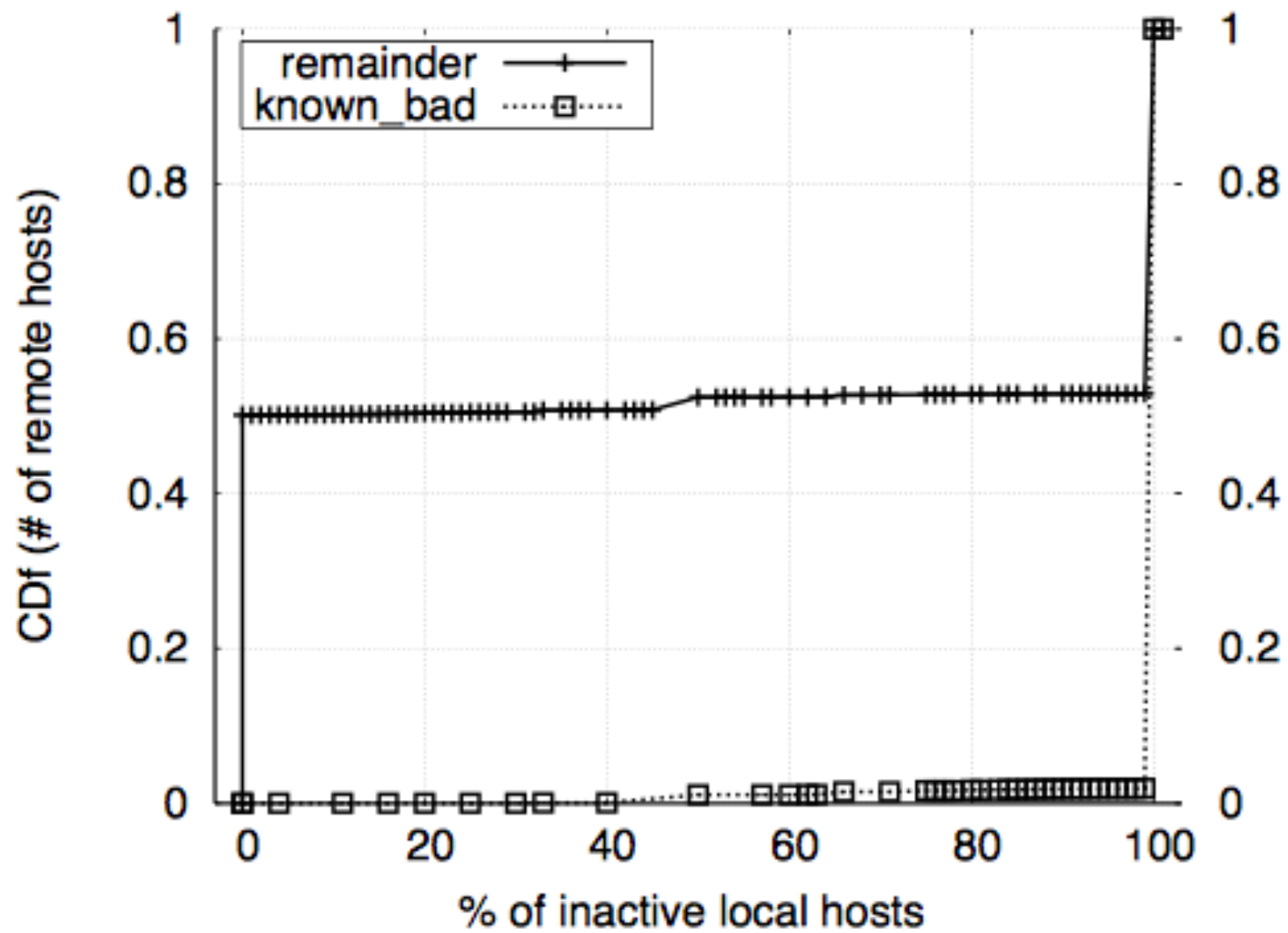
Two of the campaigns succeeded in breaking-in; one undetected by the site

(31/35 – Partially detectable)

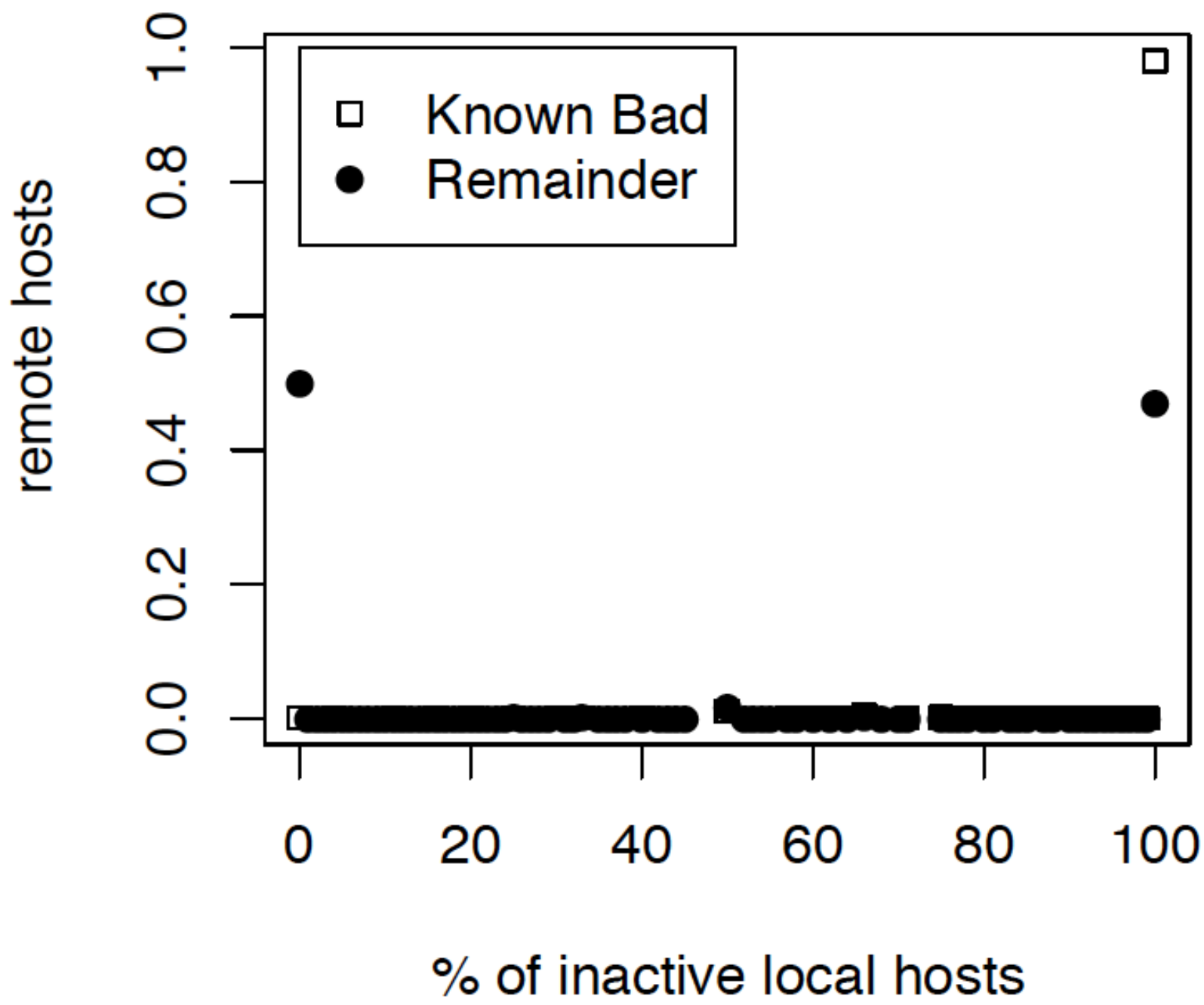
High-rate hourly activity in total number of failed attempts/ number of local hosts contacted

- Undetectable by any point-wise detector (4/35)





(a) LBL



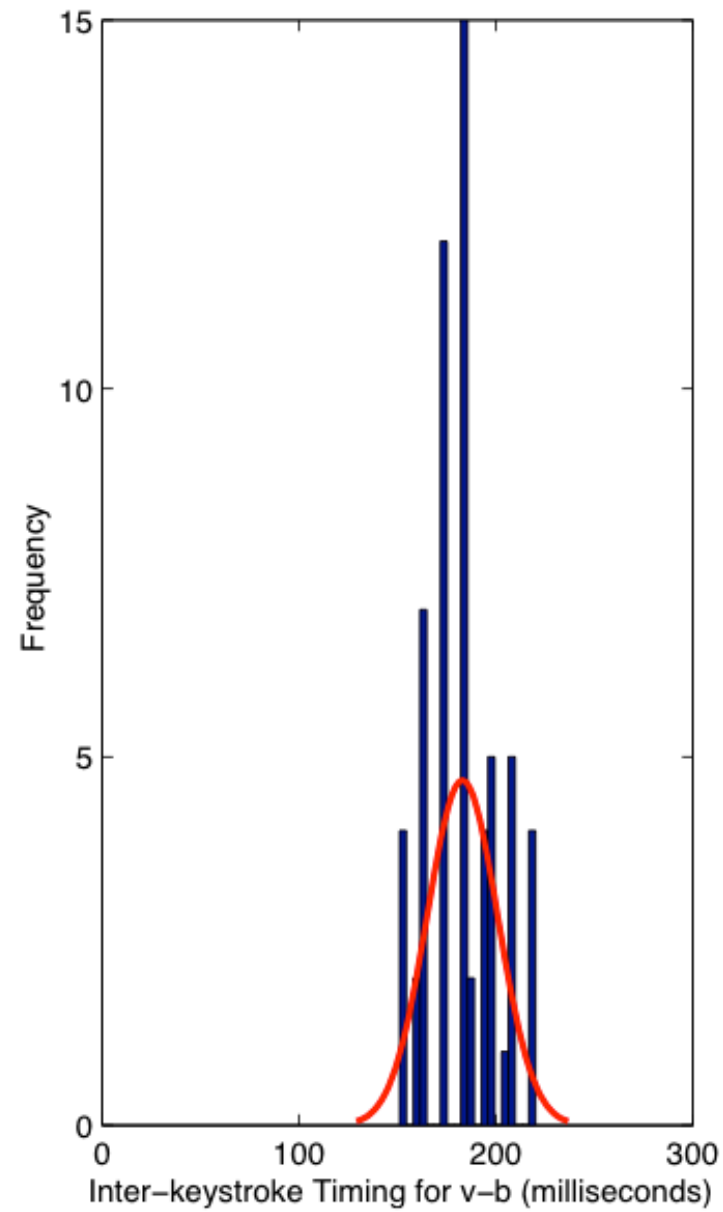
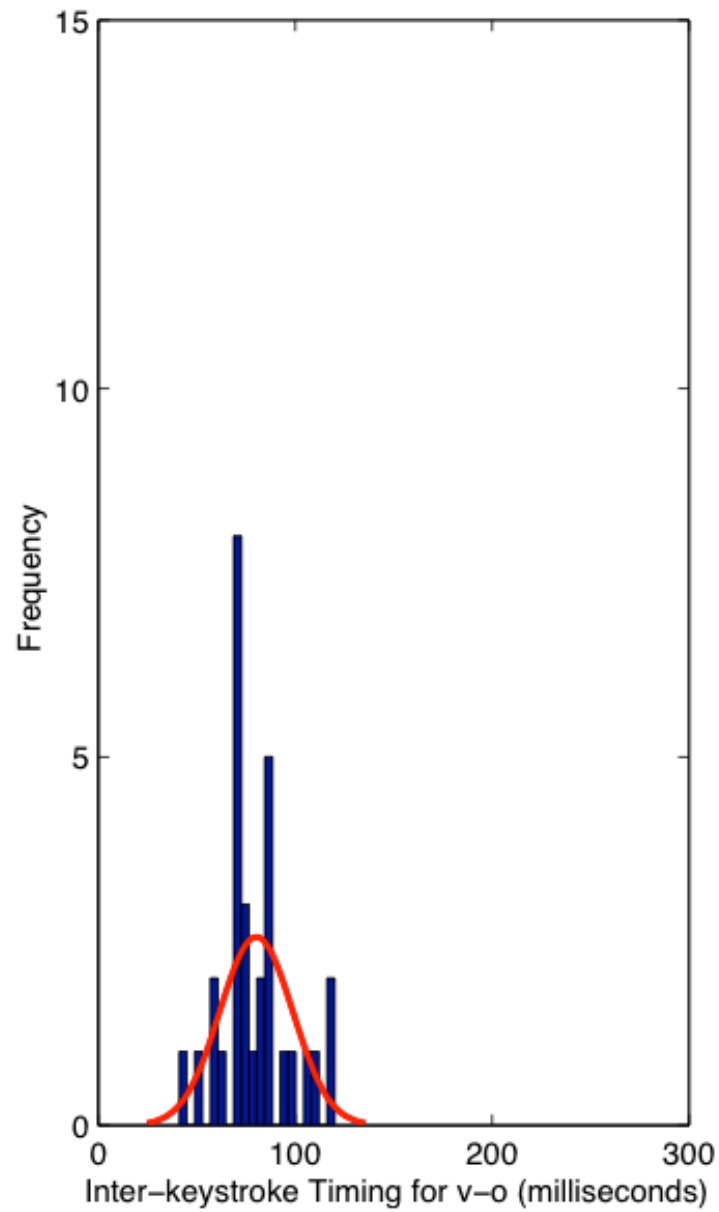


Figure 3: The distribution of inter-keystroke timings for two sample character pairs.

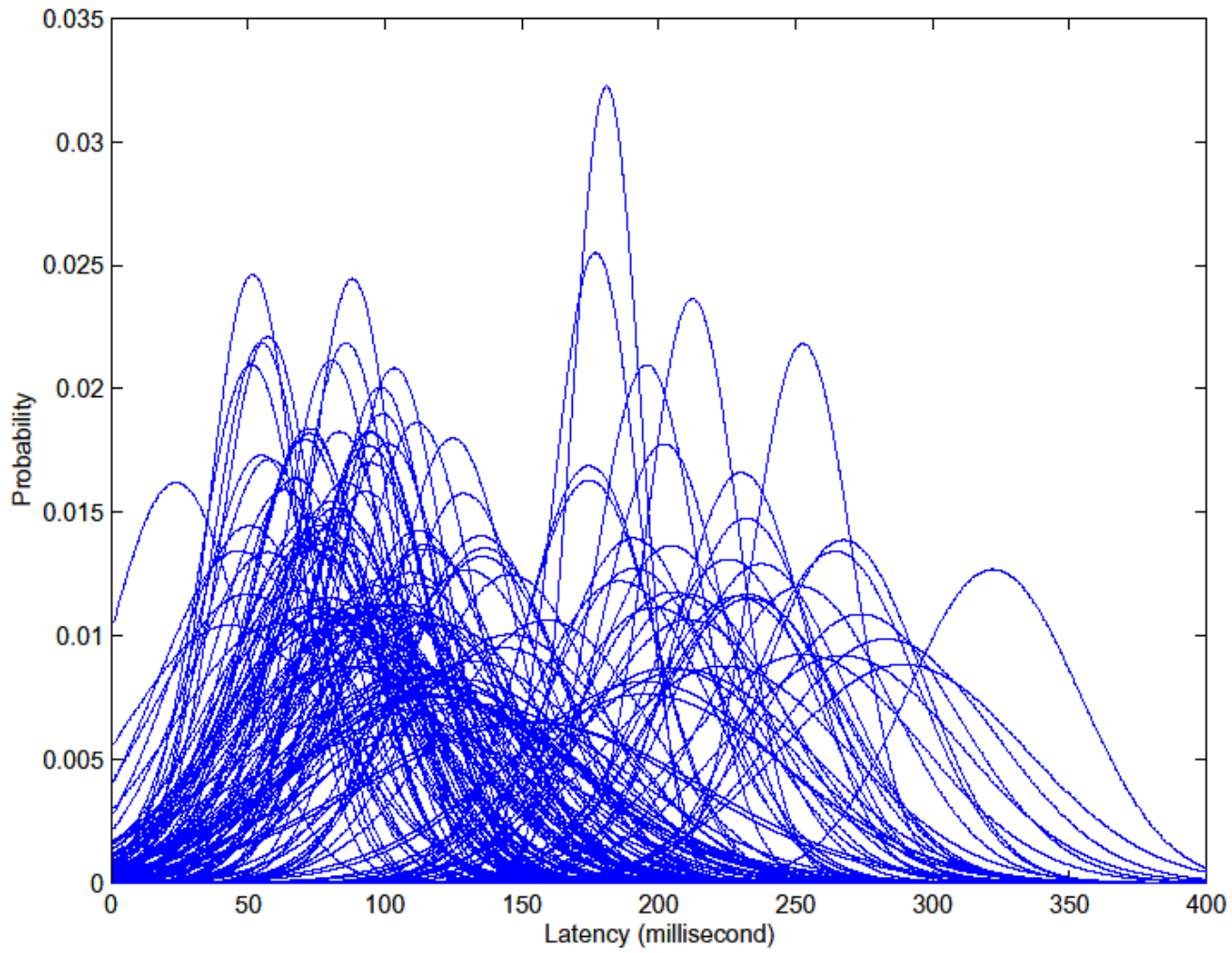


Figure 5: Estimated Gaussian distributions of all 142 character pairs collected from a user.

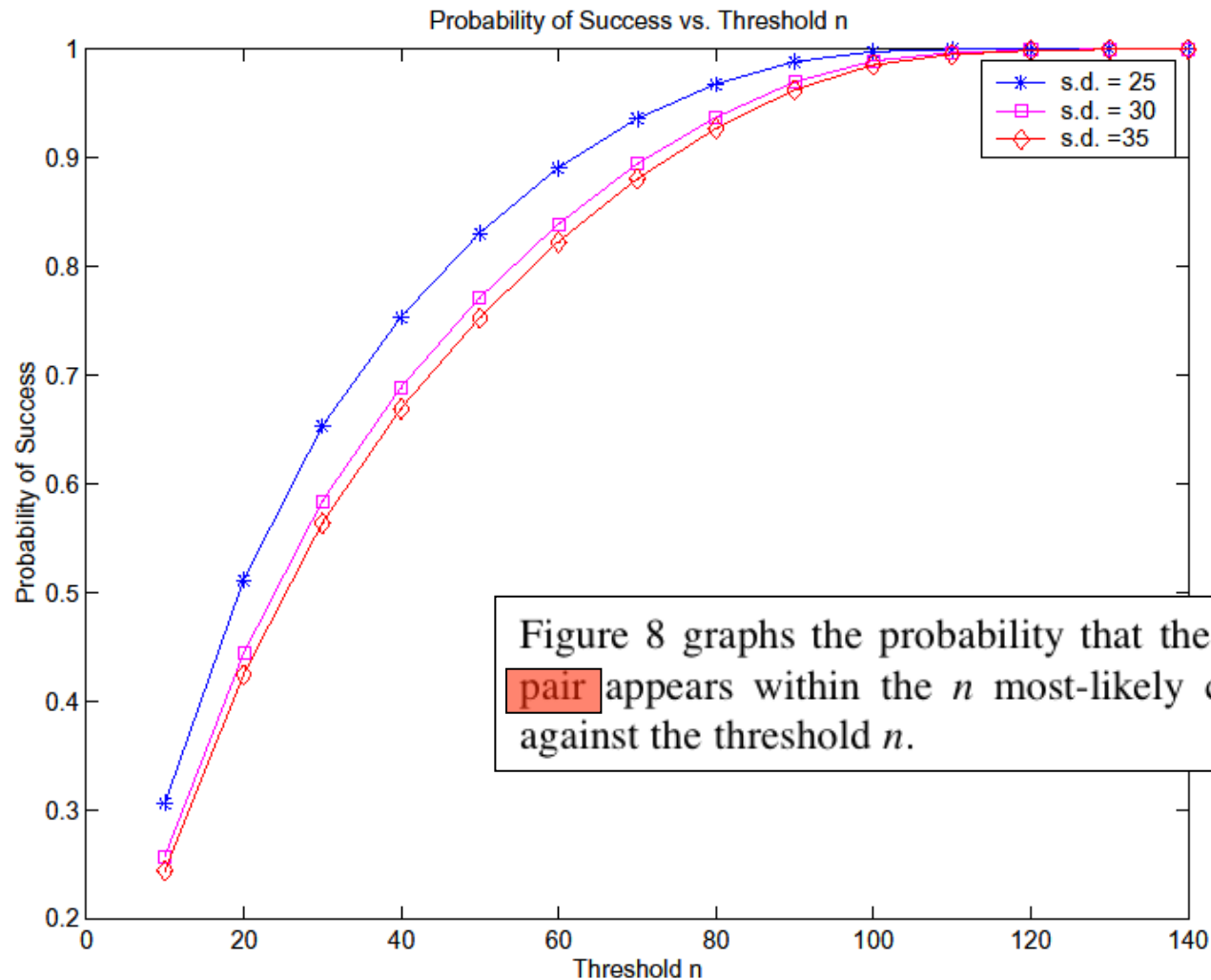


Figure 8: The probability that the  $n$ -Viterbi algorithm outputs the correct ~~password~~ before the first  $n$  guesses, graphed as a function of  $n$ .

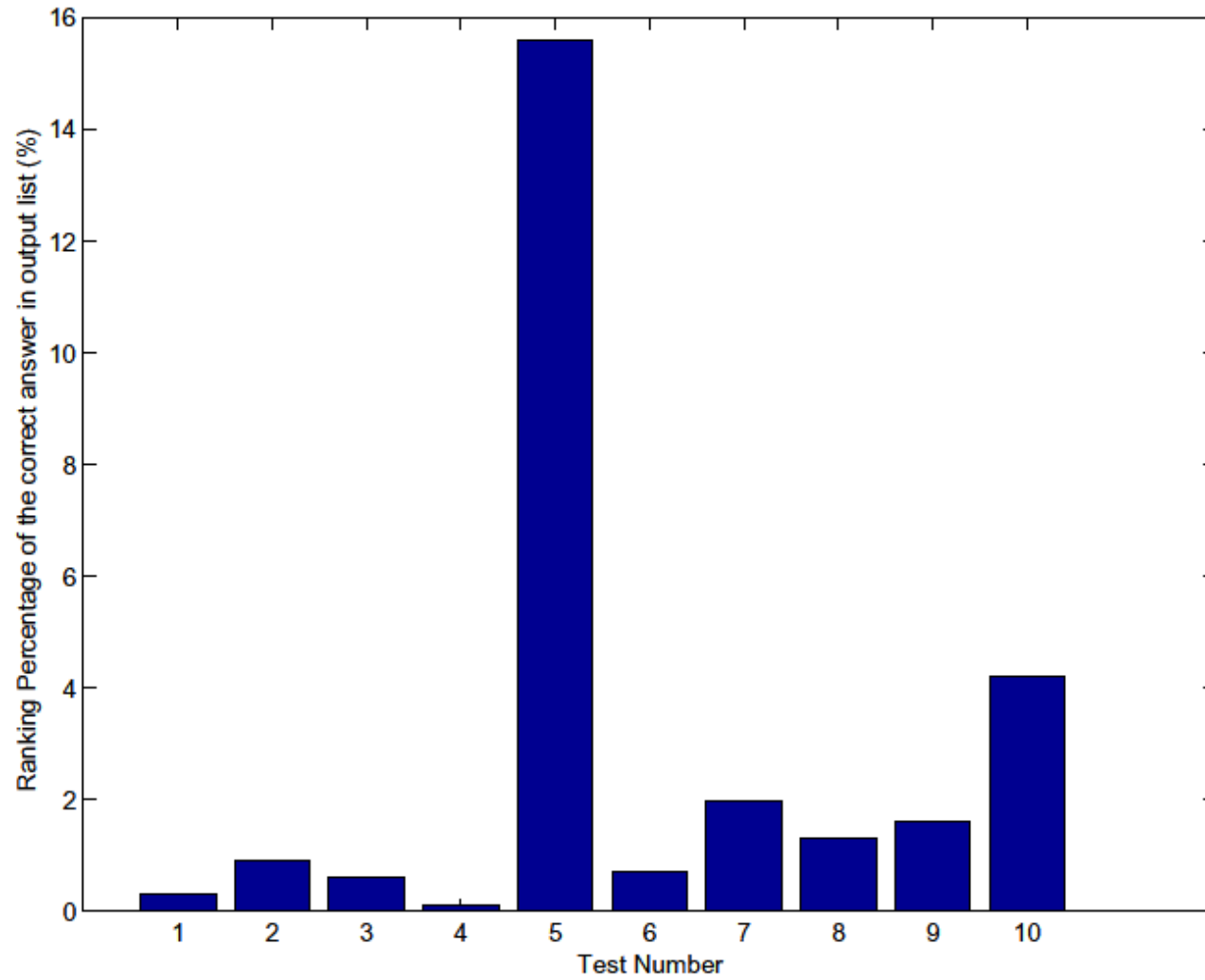
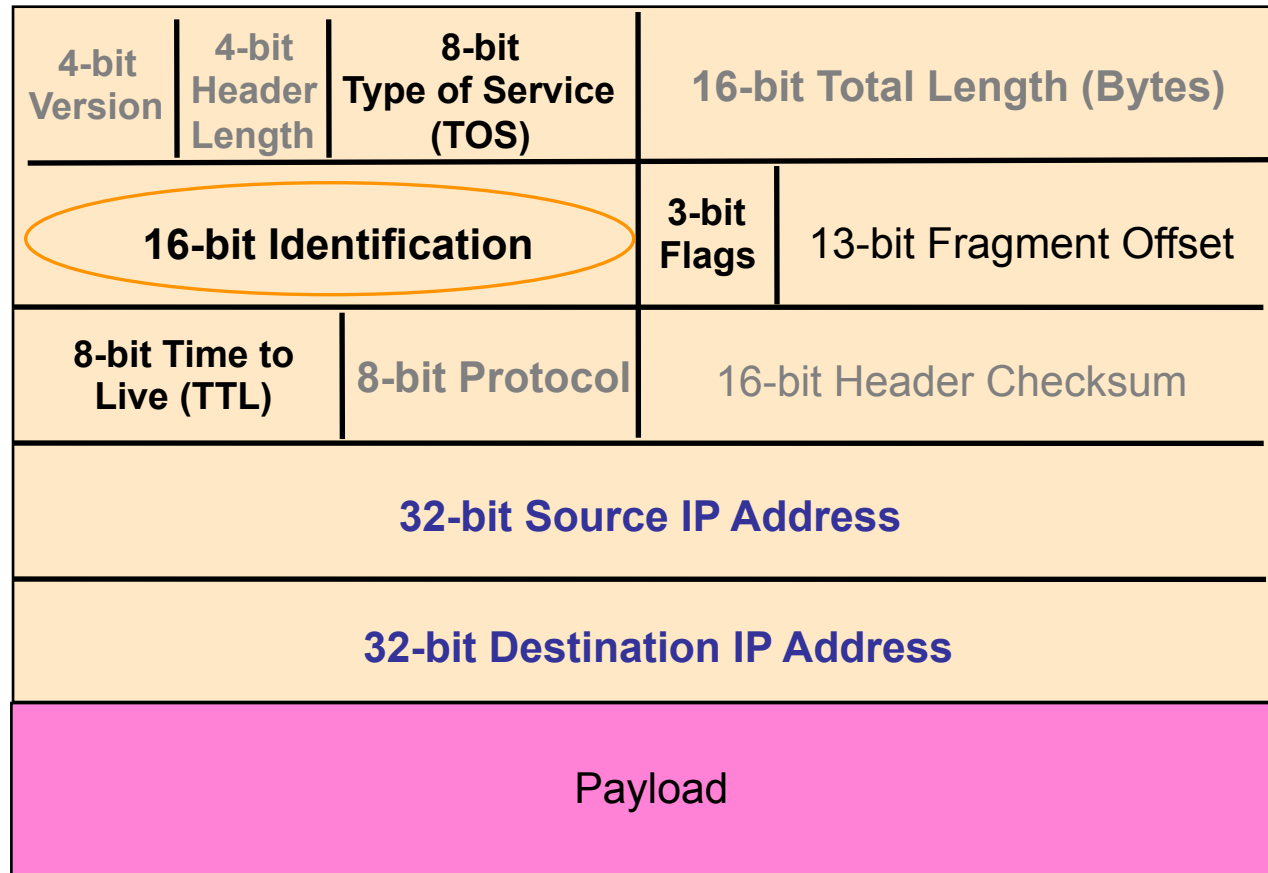


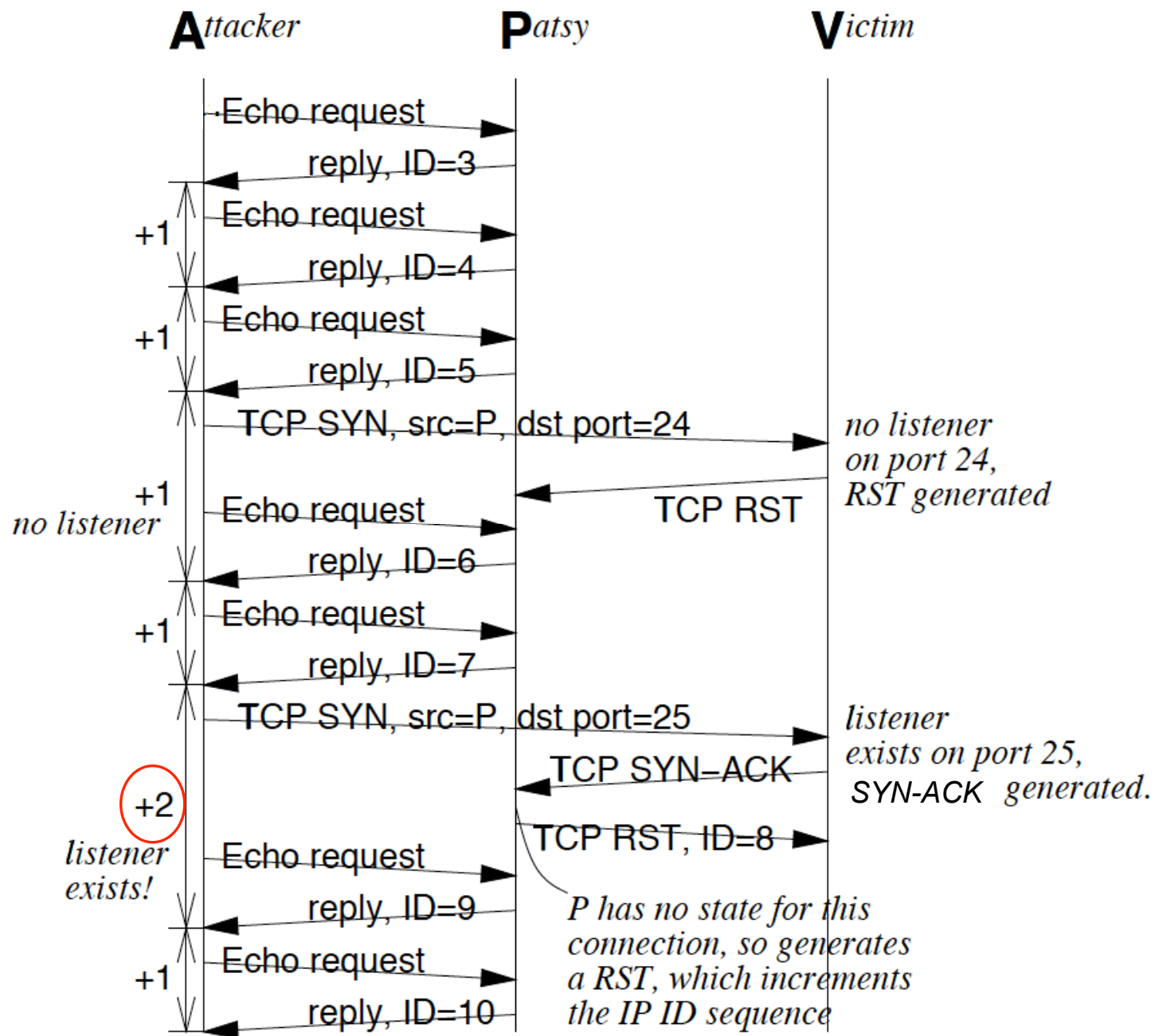
Figure 10: The percentage of the password space tried by Herbivore in 10 tests before finding the right password.

# IP Header Side Channel



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.







Search products by name

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

## PAIN RELIEF

[Vicodin ES](#)[Hydrocodone](#)[Percocet](#)[Lortab](#)[Darvocet \(Proxyvon\)](#)[Codeine](#)[View all products](#)

## ANTI-ANXIETY

[Xanax](#)[Valium \(® ROCHE\)](#)[Ativan \(® Wyeth\)](#)[Klonopin \(generic\)](#)[Valium \(generic\)](#)[Anti-Anxiety Pack](#)[Atarax](#)[View all products](#)

## ADHD Treatment

[Adderall](#)[Brand Ritalin](#)[View all products](#)

## WEIGHT LOSS

[Phentermine](#)

# 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](http://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](http://www.rxsup24.com)**

---



Search products by name

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

## PAIN RELIEF

[Vicodin ES](#)[Hydrocodone](#)[Percocet](#)[Lortab](#)[Darvocet \(Proxyvon\)](#)[Codeine](#)[View all products](#)

## ANTI-ANXIETY

[Xanax](#)[Valium \(@ ROCHE\)](#)[Ativan \(@ Wyeth\)](#)[Klonopin \(generic\)](#)[Valium \(generic\)](#)[Anti-Anxiety Pack](#)[Atarax](#)[View all products](#)

## ADHD Treatment

[Adderall](#)[Brand Ritalin](#)[View all products](#)

## WEIGHT LOSS

[Phentermine](#)

# 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](http://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](http://www.rxsup24.com)**

---



Search products by name

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

## PAIN RELIEF

[Vicodin ES](#)[Hydrocodone](#)[Percocet](#)[Lortab](#)[Darvocet \(Proxyvon\)](#)[Codeine](#)[View all products](#)

## ANTI-ANXIETY

[Xanax](#)[Valium \(@ ROCHE\)](#)[Ativan \(@ Wyeth\)](#)[Klonopin \(generic\)](#)[Valium \(generic\)](#)[Anti-Anxiety Pack](#)[Atarax](#)[View all products](#)

## ADHD Treatment

[Adderall](#)[Brand Ritalin](#)[View all products](#)

## WEIGHT LOSS

[Phentermine](#)

# 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

10s of seconds later

**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](http://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](http://www.rxsup24.com)**

---



Search products by name

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

## PAIN RELIEF

[Vicodin ES](#)[Hydrocodone](#)[Percocet](#)[Lortab](#)[Darvocet \(Proxyvon\)](#)[Codeine](#)[View all products](#)

## ANTI-ANXIETY

[Xanax](#)[Valium \(® ROCHE\)](#)[Ativan \(® Wyeth\)](#)[Klonopin \(generic\)](#)[Valium \(generic\)](#)[Anti-Anxiety Pack](#)[Atarax](#)[View all products](#)

## ADHD Treatment

[Adderall](#)[Brand Ritalin](#)[View all products](#)

## WEIGHT LOSS

[Phentermine](#)

# 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**

1 month later

***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](http://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](http://www.rxsup24.com)**

