Aggregate Site Analyzer

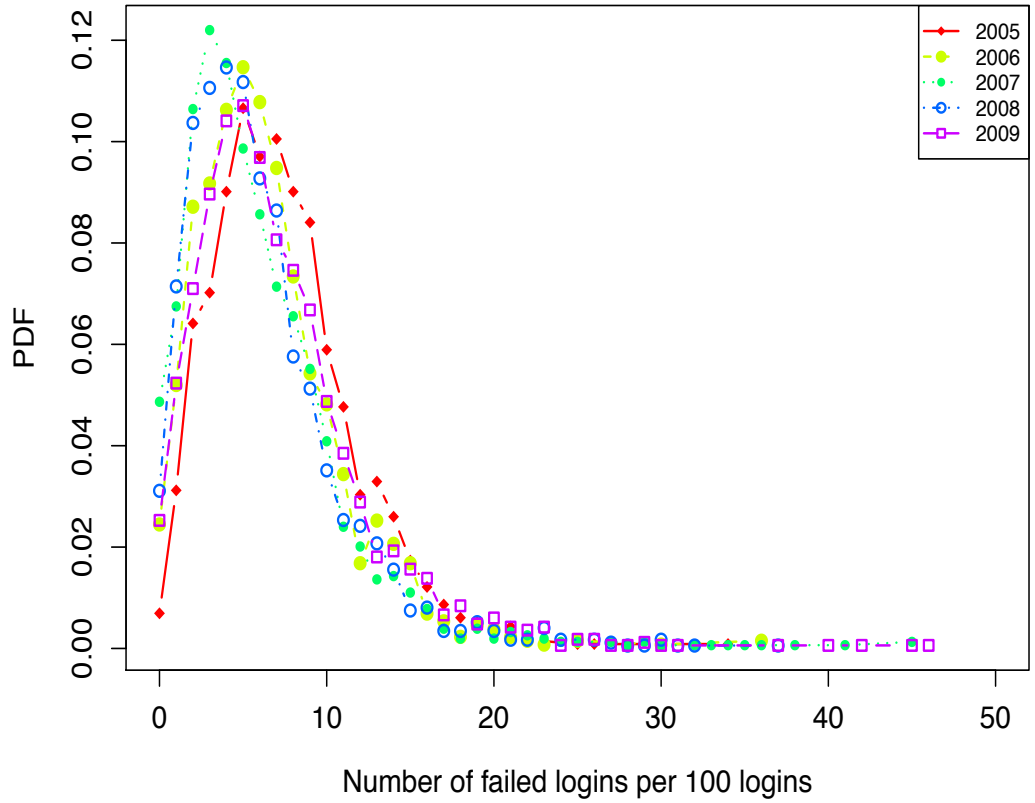
Site-wide parameter: Global Failure Indicator (GFI)

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

Aggregate Site Analyzer

Site-wide parameter: Global Failure Indicator (GFI)

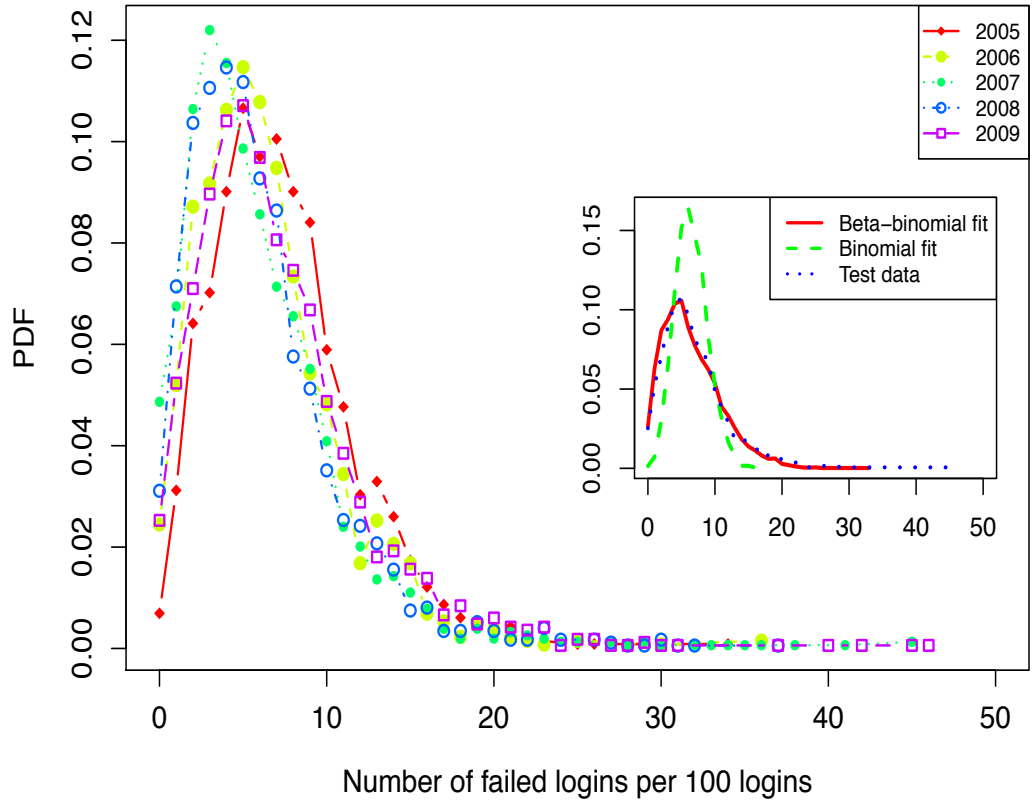
- Site-wide # of failed logins per batch of x logins



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)

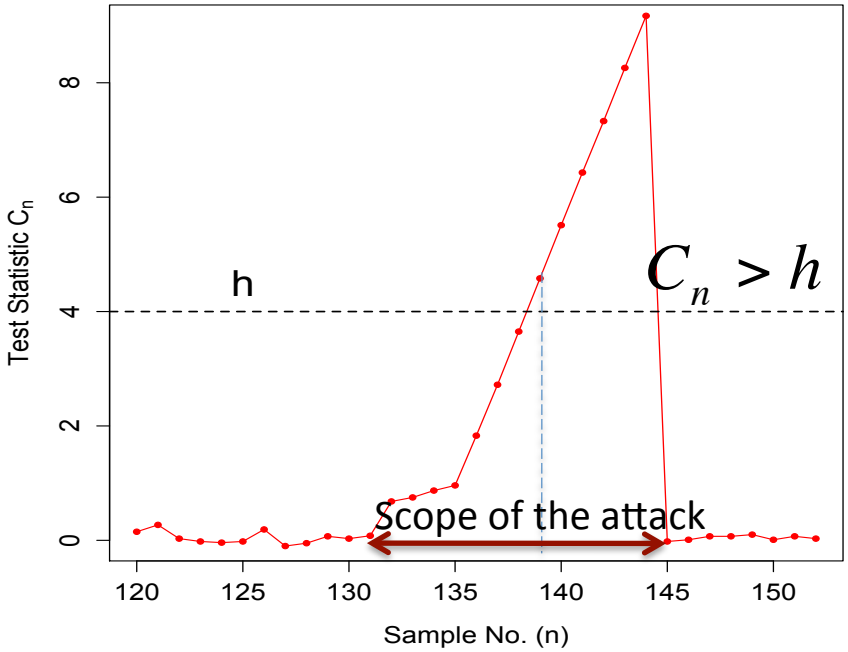
$$C_0 = 0$$

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

X_n – Random variable (GFI)

μ - Mean under normal behavior

k - Parameter based on magnitude of change to be detected



Aggregate Site Analyzer

Monitoring for Change (CUSUM Algorithm)

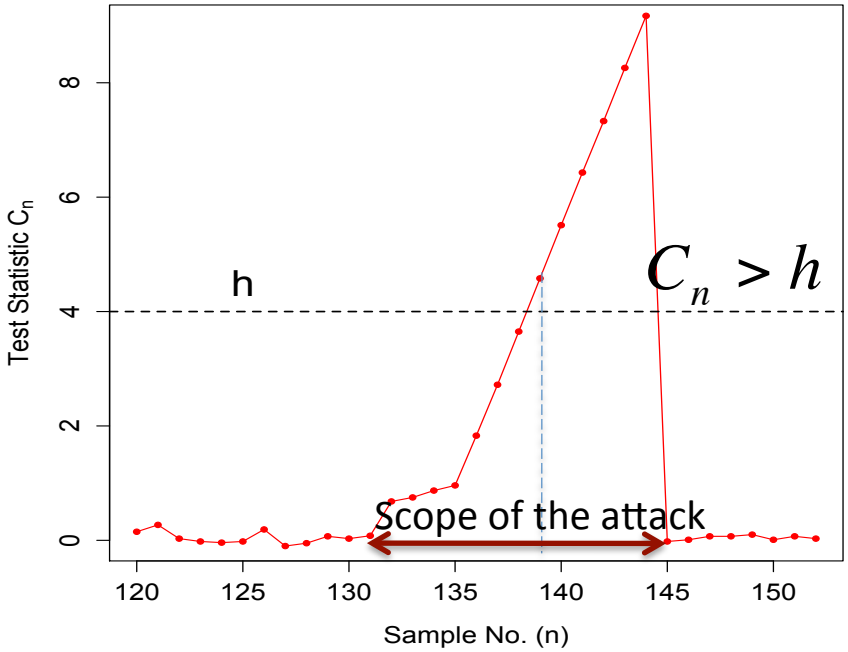
$$C_0 = 0$$

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

X_n – Random variable (GFI)

μ - 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	
Total number of attacks	**99**
Number of false attacks	9

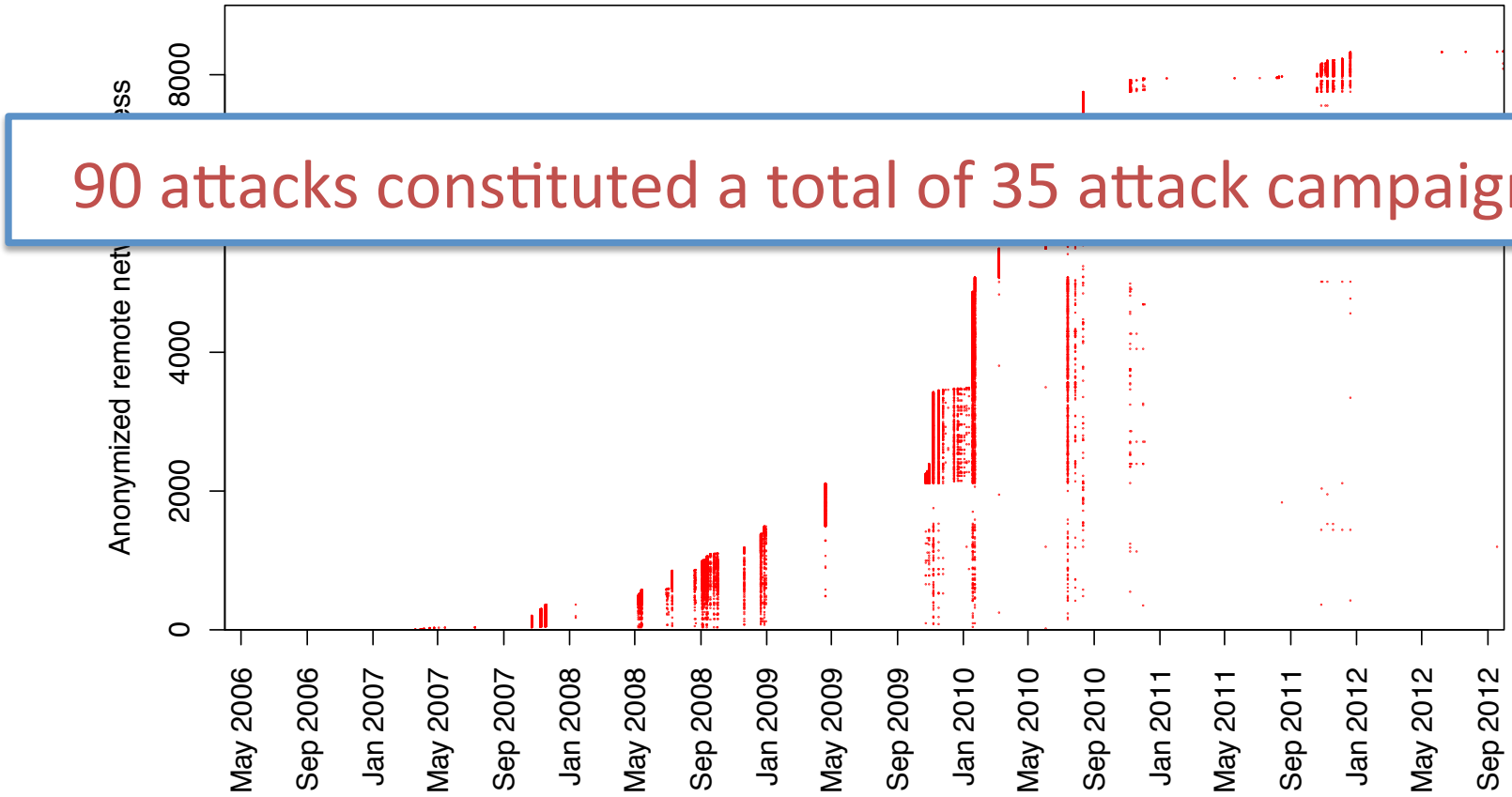
Determined by Attack Participants Classifier

Attack Participants Classifier	
Number of attack hosts	**9,306**
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)

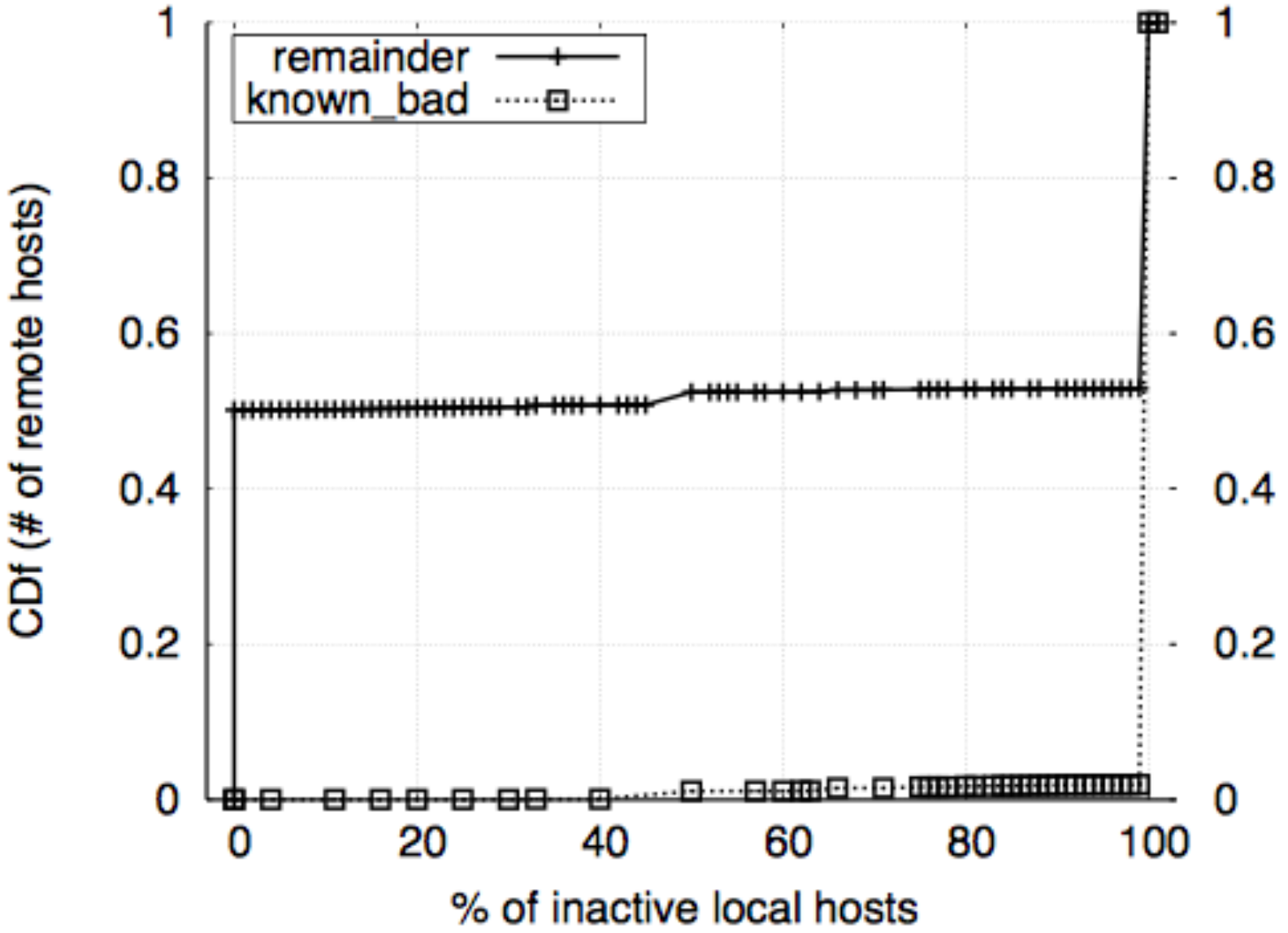
On average 2 attempts per local machine per hour

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

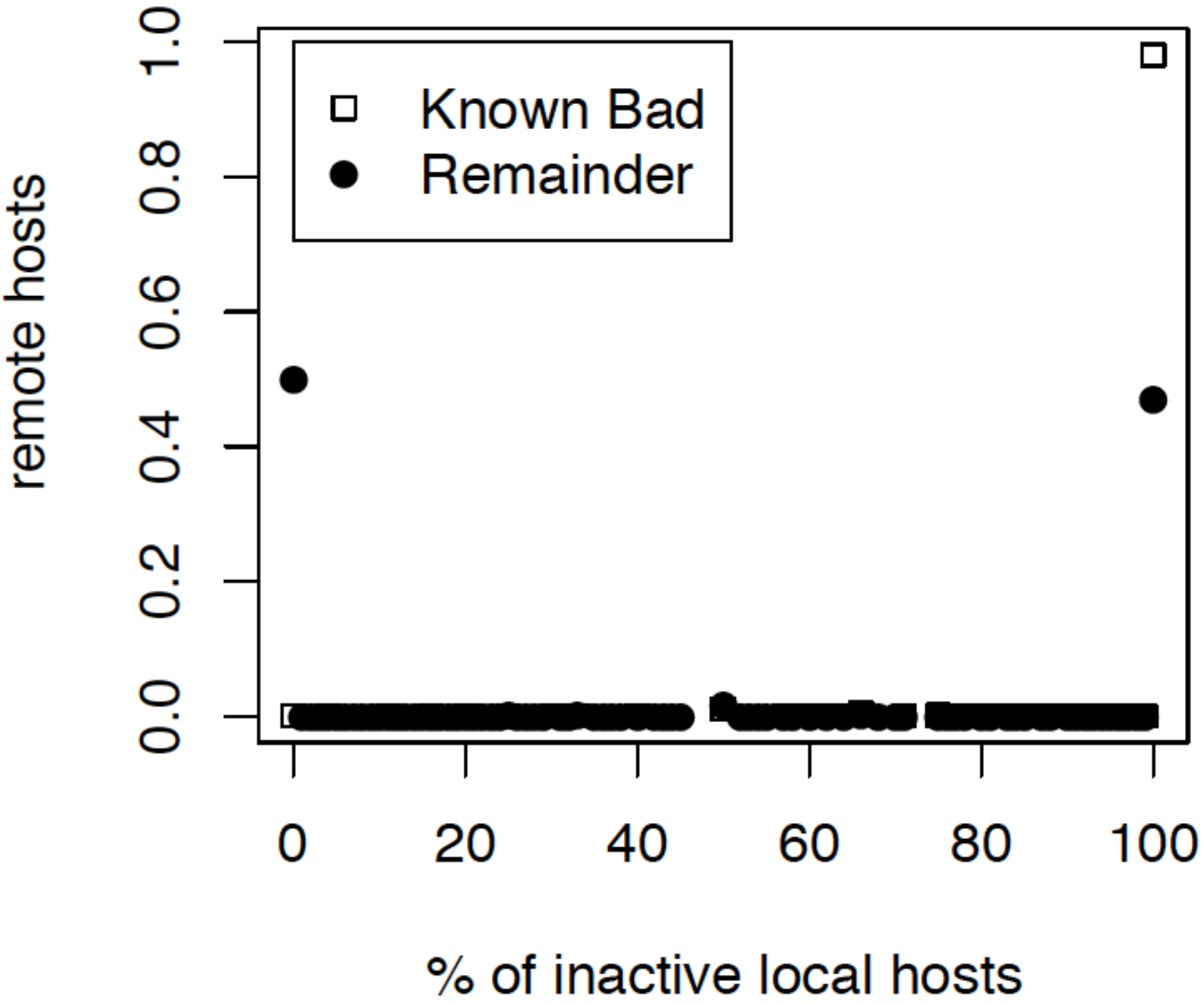
(31/35 – Partially detectable)

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

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


remainder
known_bad
CDf (# of remote hosts)
% of inactive local hosts
0
0.2
0.4
0.6
0.8
1
0
20
40
60
80
100

(a) LBL


Known Bad
Remainder
remote hosts
0.0
0.2
0.4
0.6
0.8
1.0
0
20
40
60
80
100
% of inactive local hosts

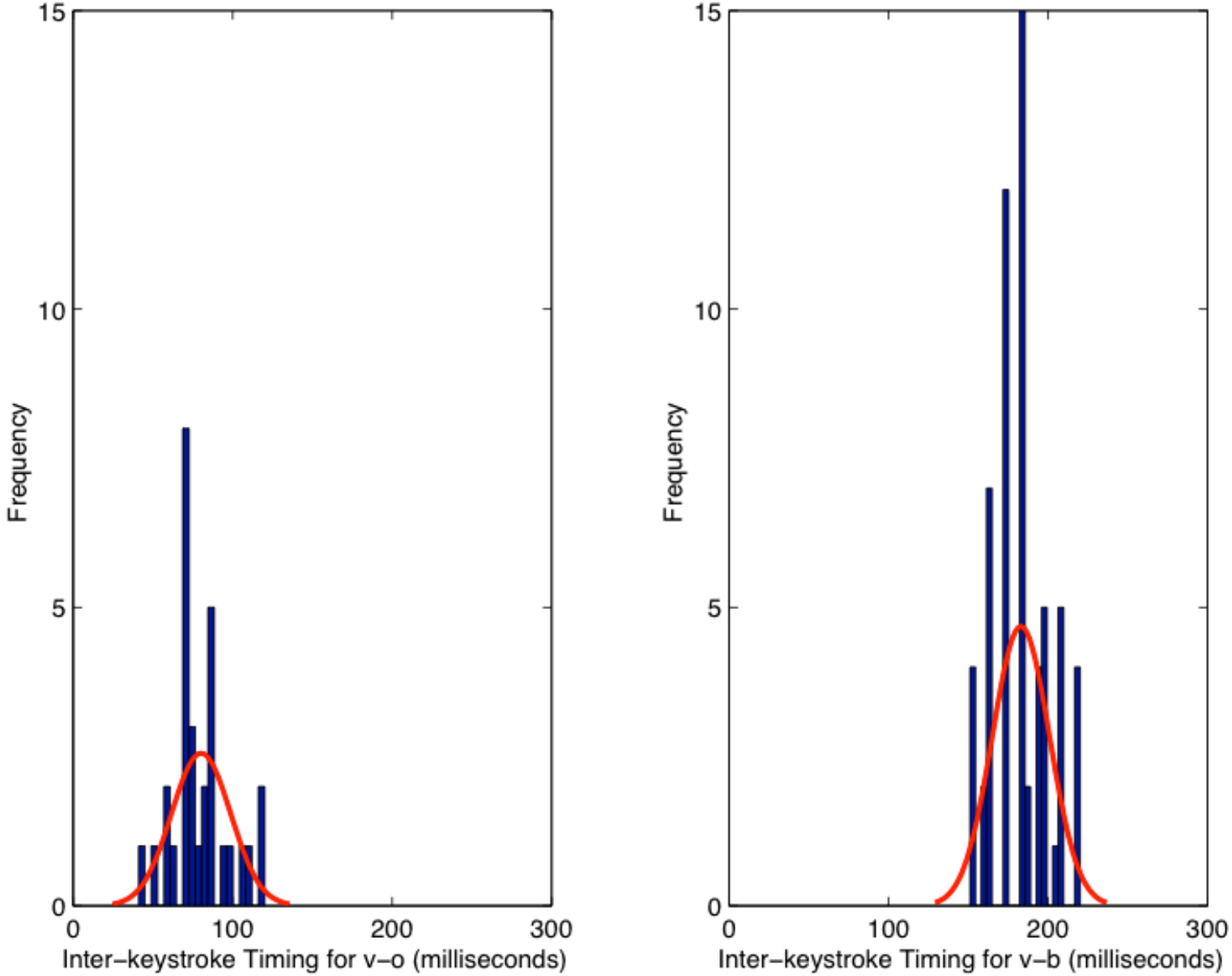


Figure 3: The distribution of inter-keystroke timings for two sample character pairs.

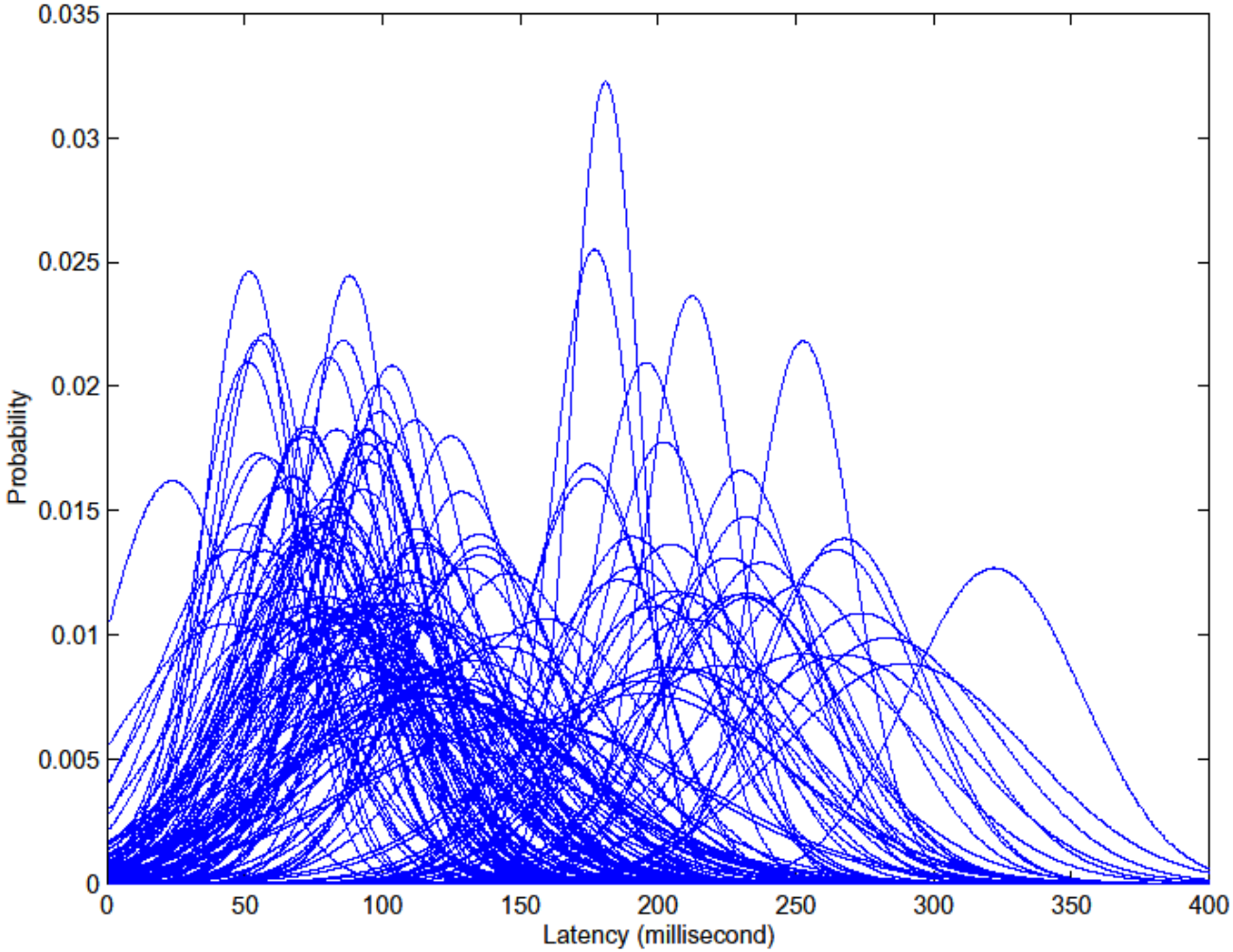


Figure 5: Estimated Gaussian distributions of all 142 character pairs collected from a user.

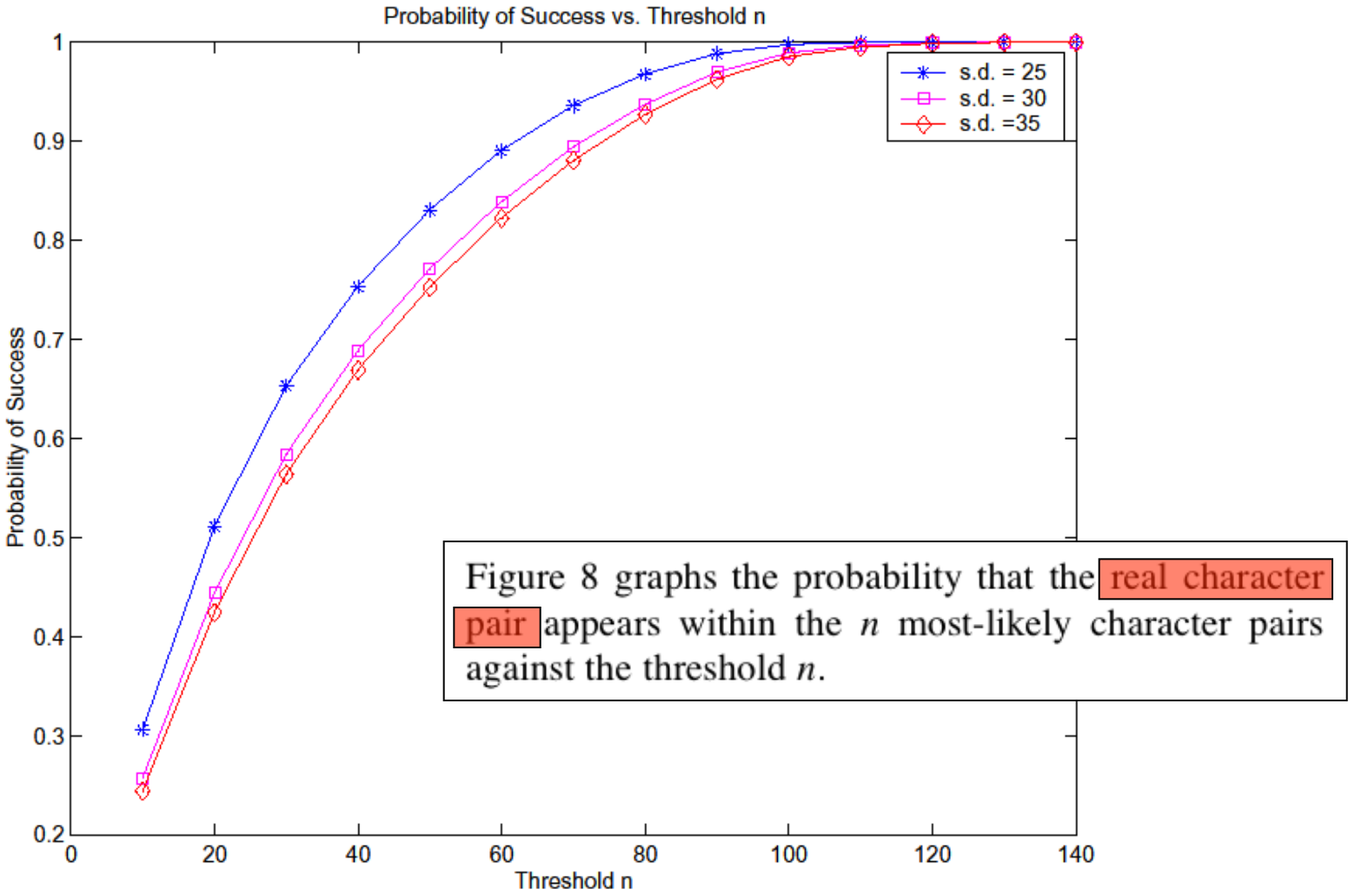


Figure 8 graphs the probability that the real character pair appears within the n most-likely character pairs against the threshold n.

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

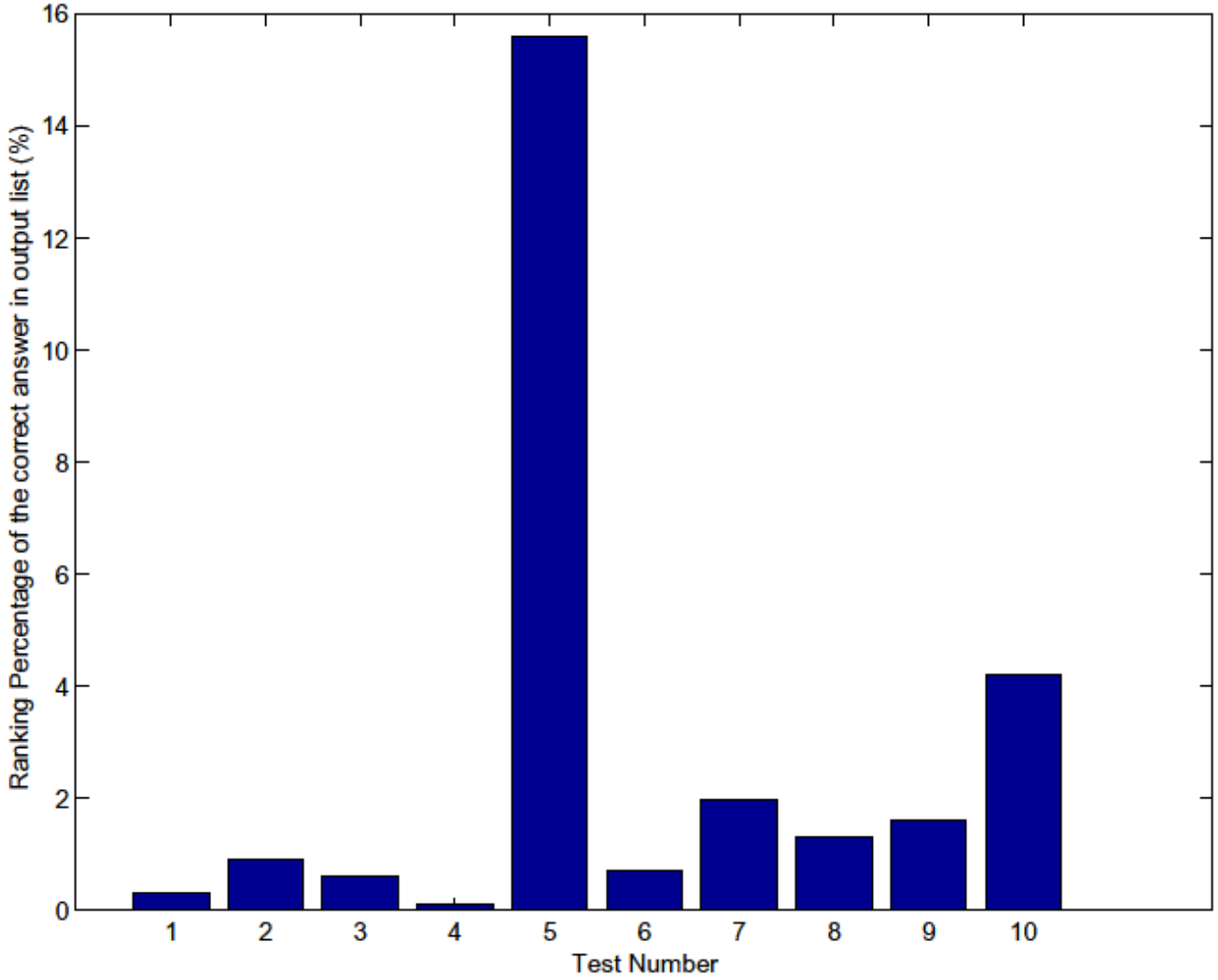
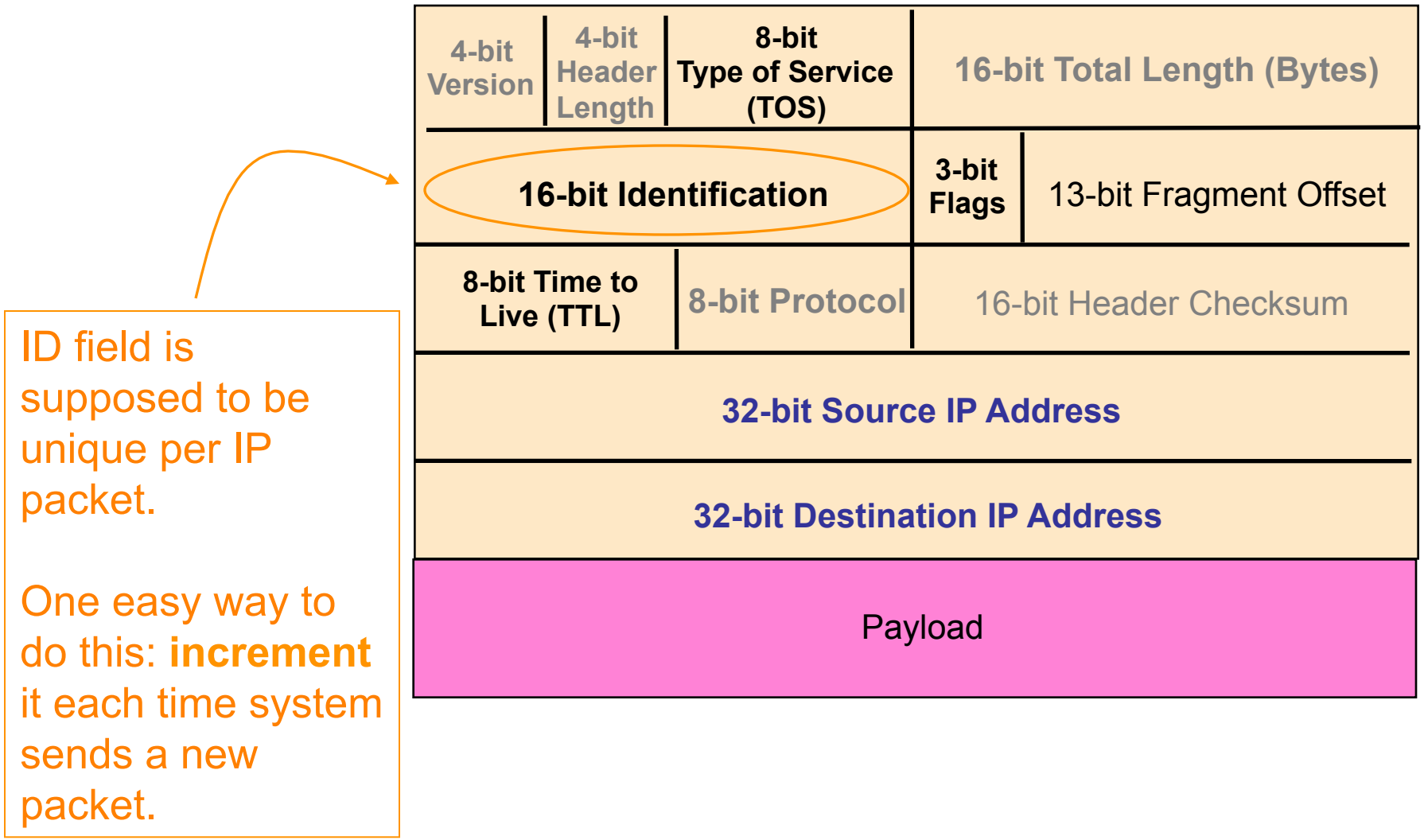
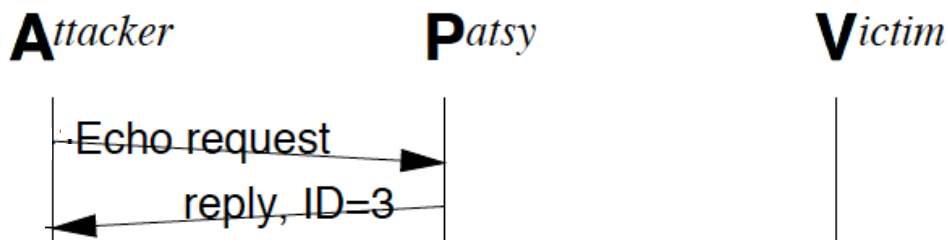
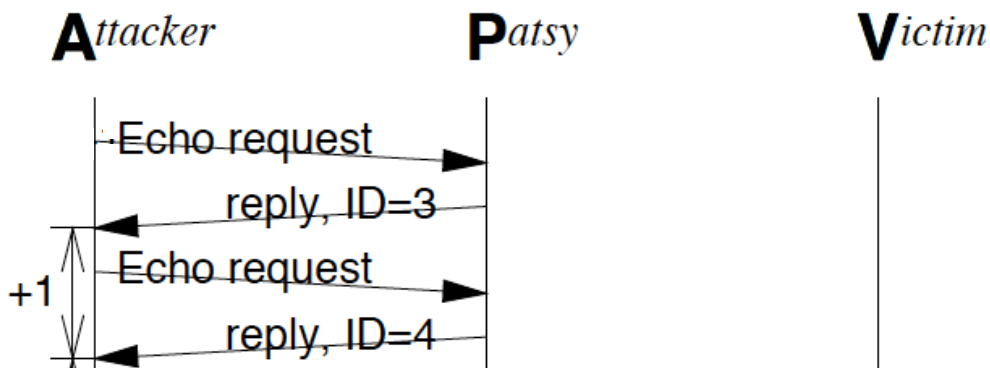


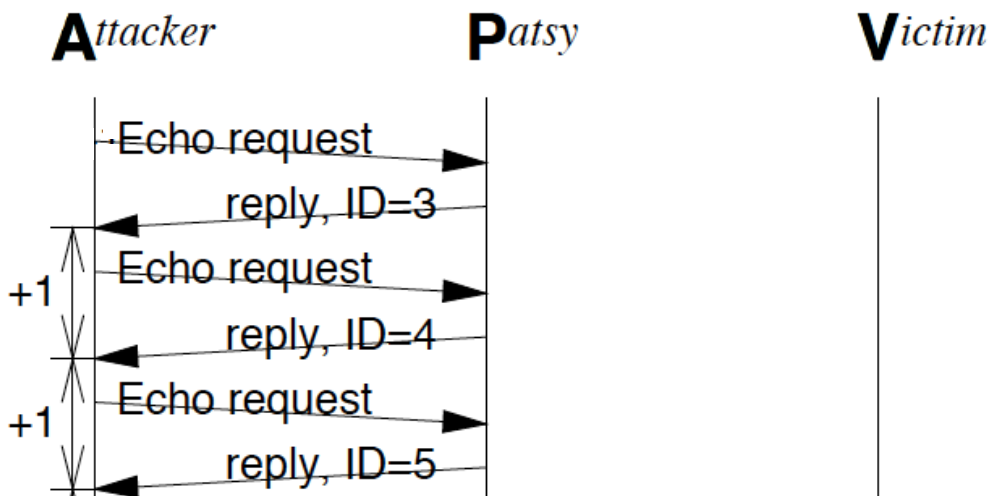
Figure 10: The percentage of the password space tried by Herbivore in 10 tests before finding the right password.

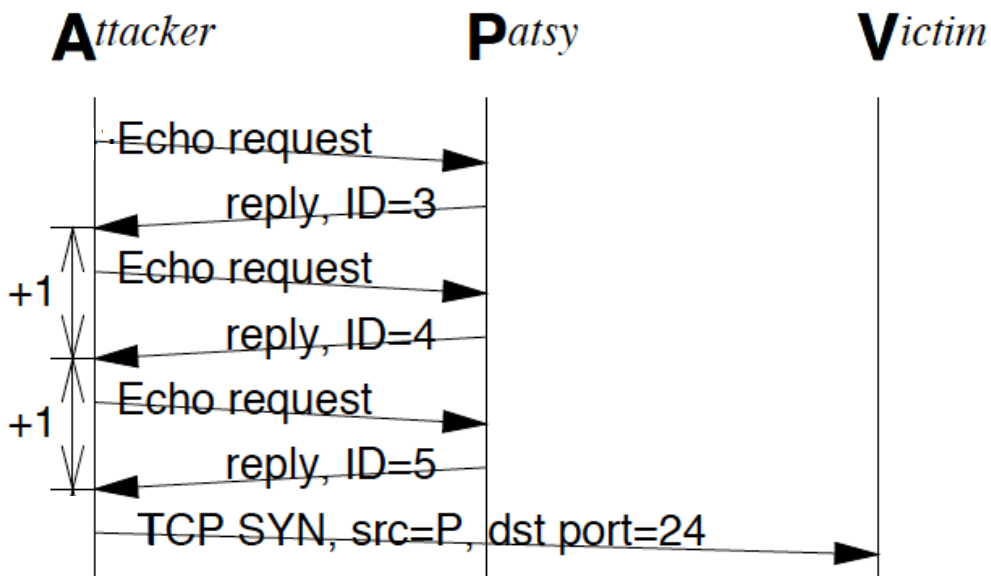
IP Header Side Channel

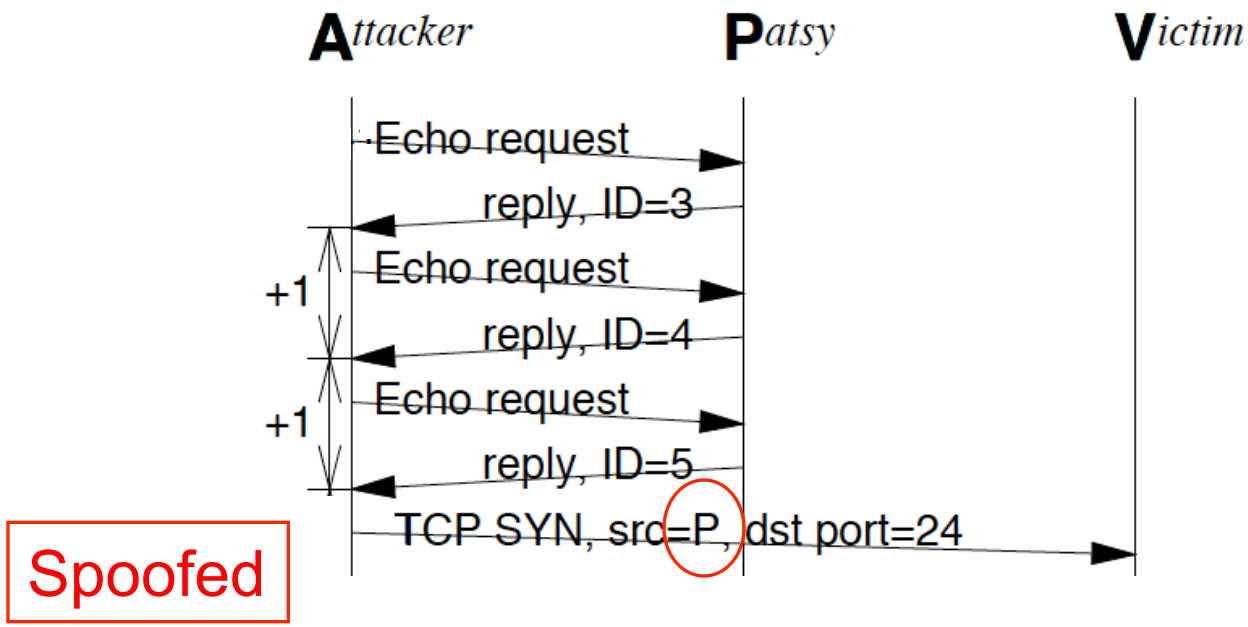


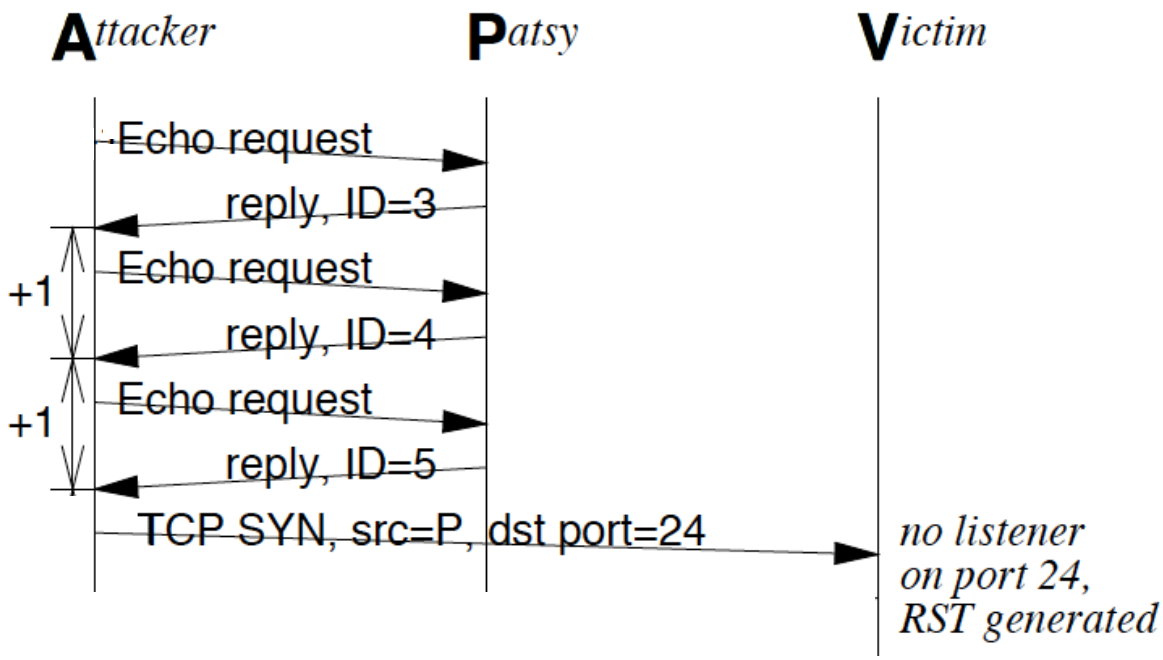

Attacker
Patsy
Victim
Echo request
reply, ID=3

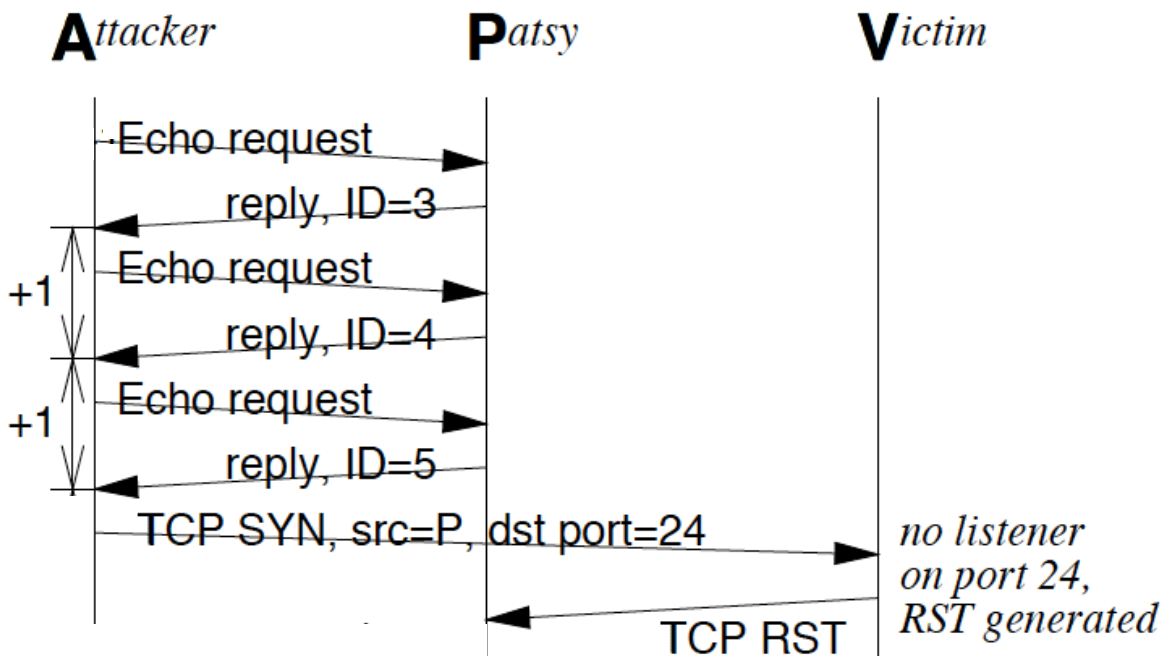

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
reply, ID=4
+1

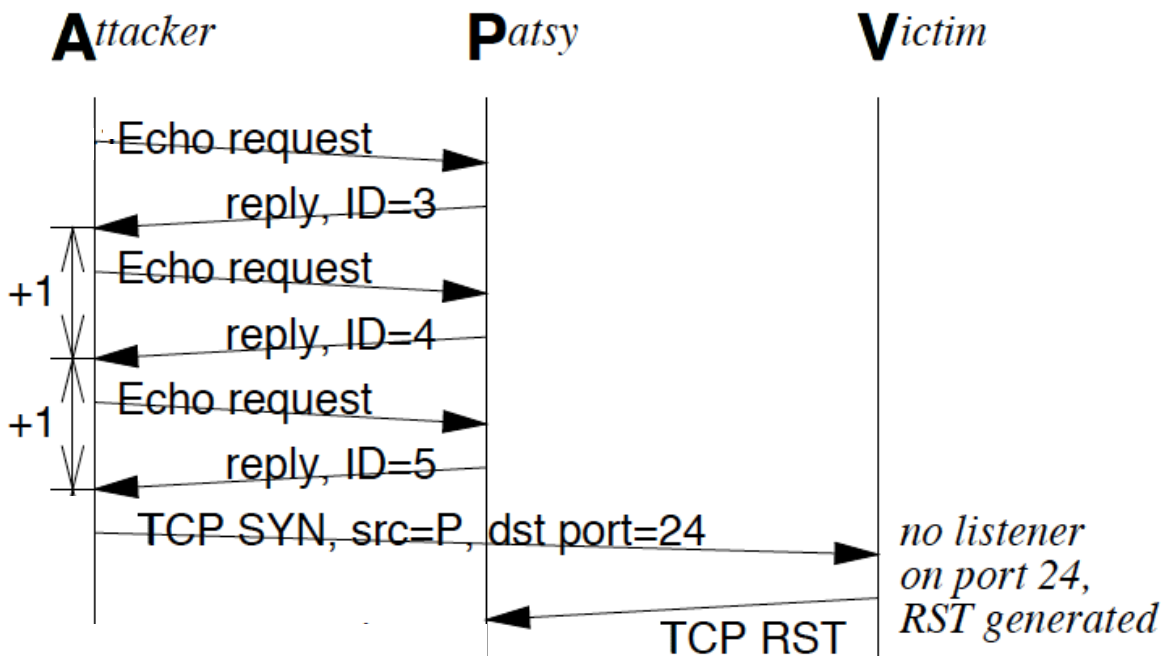

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5


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

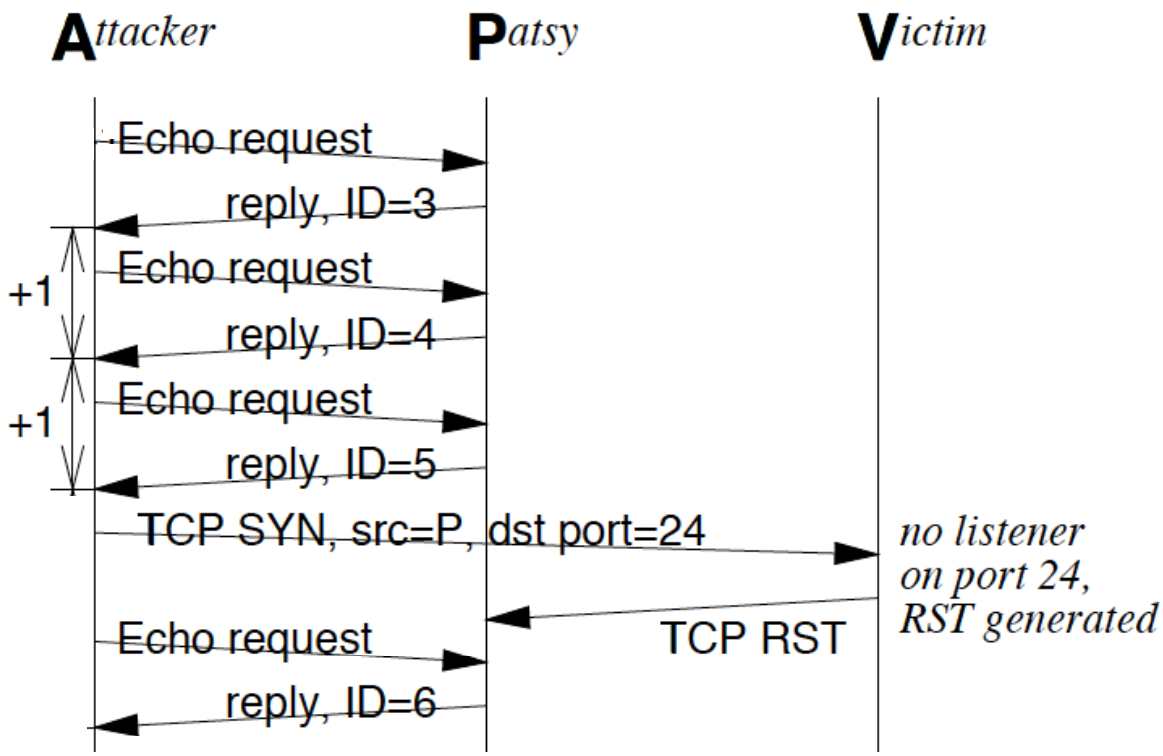

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24
Spoofed

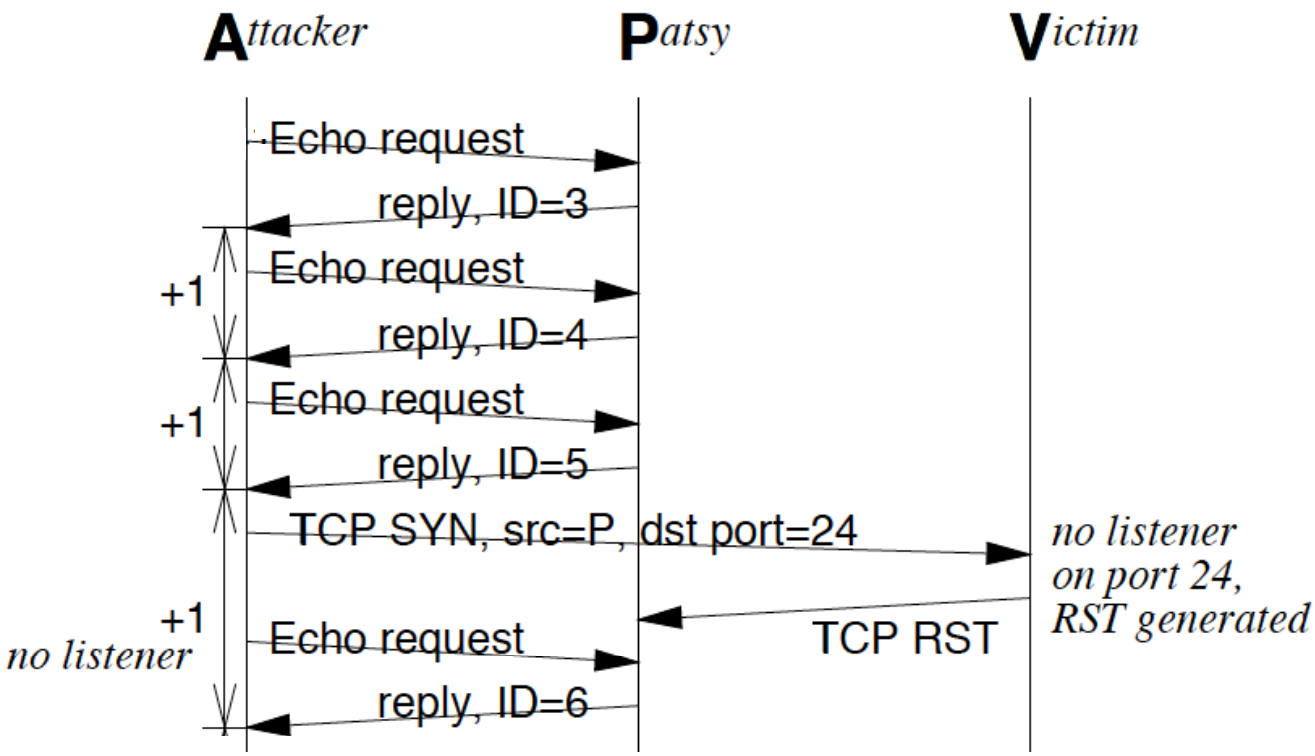

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated

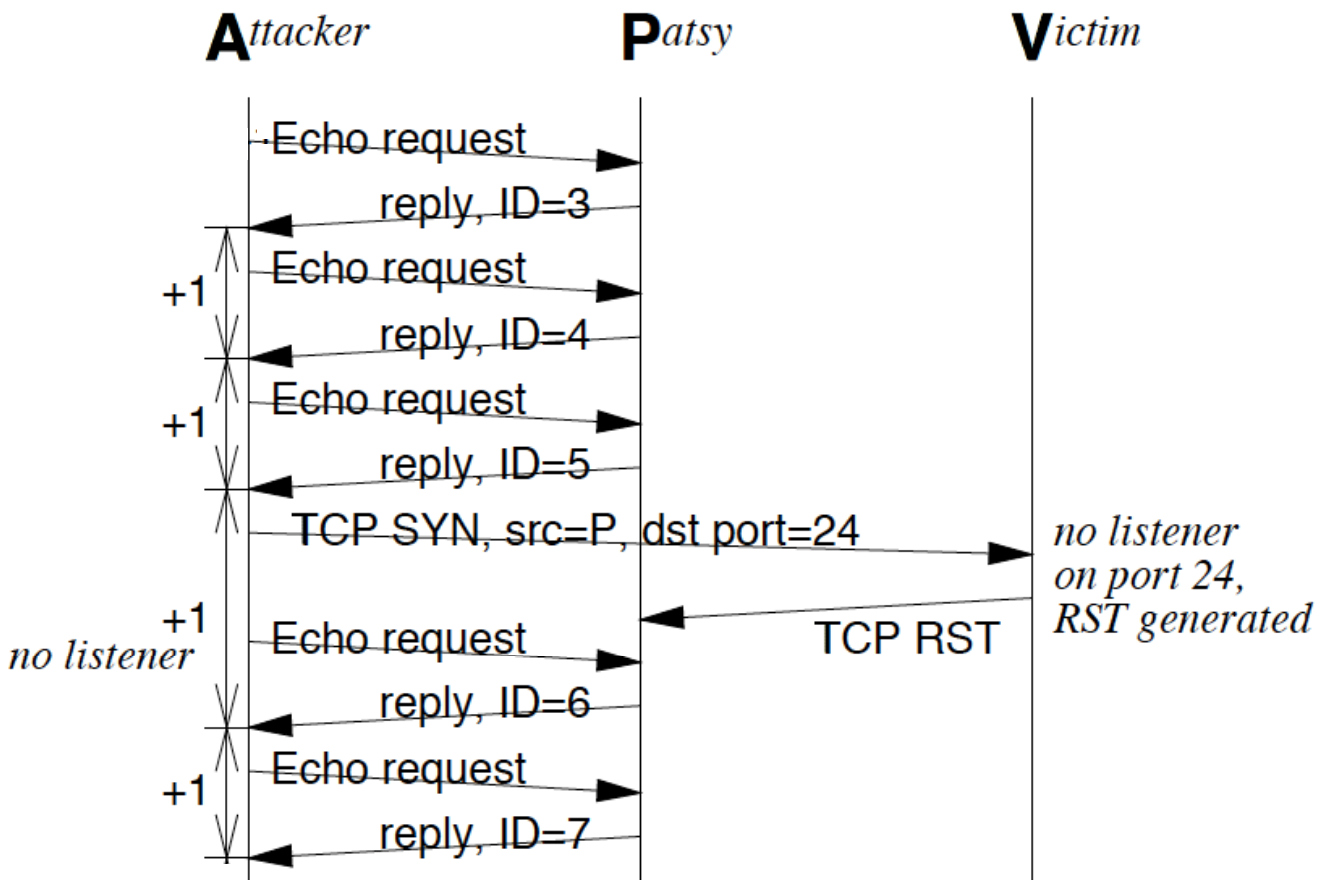

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST

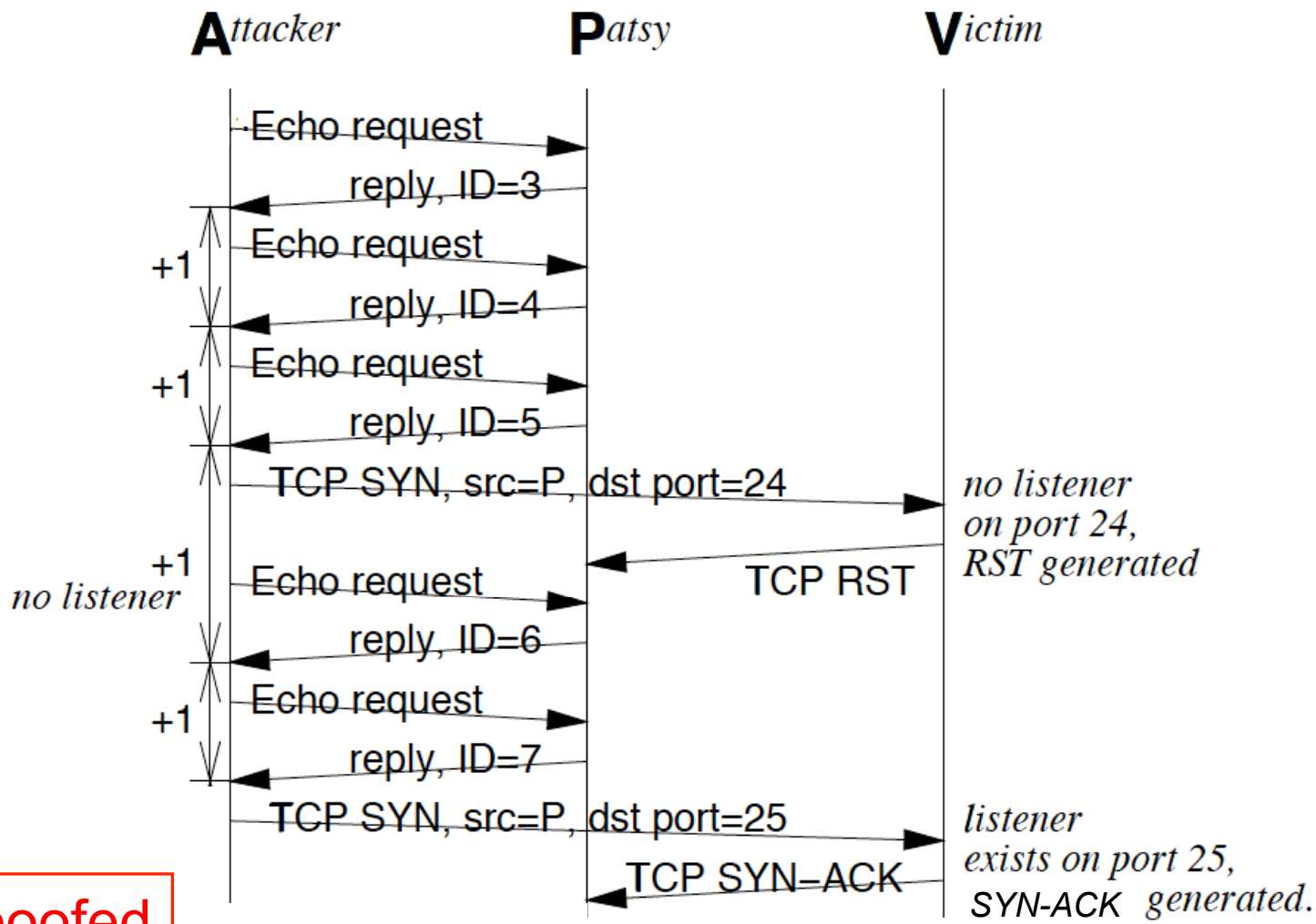


Upon receiving RST, Patsy ignores it and does **nothing**, per TCP spec.

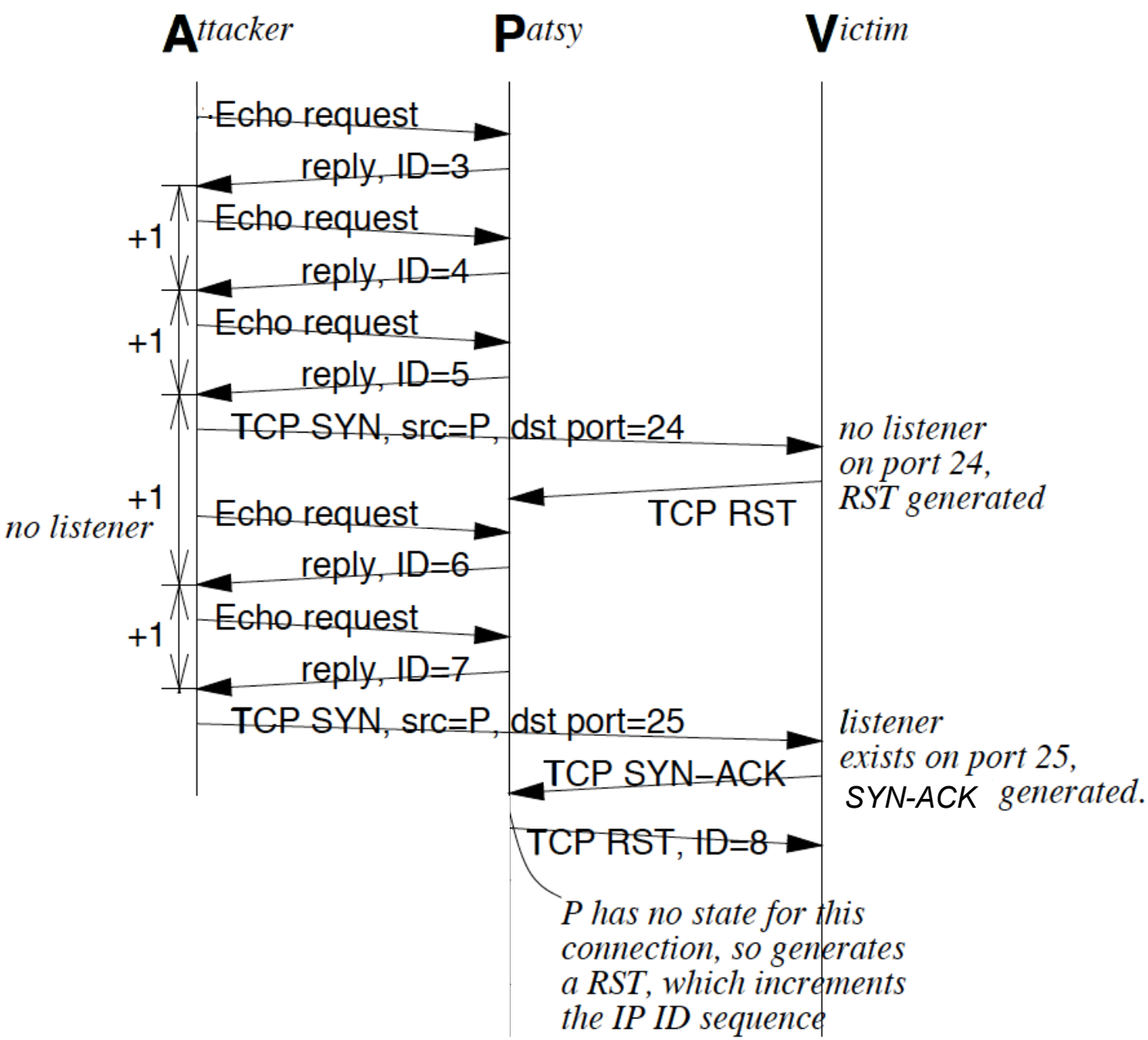

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
+1
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
Echo request
reply, ID=6

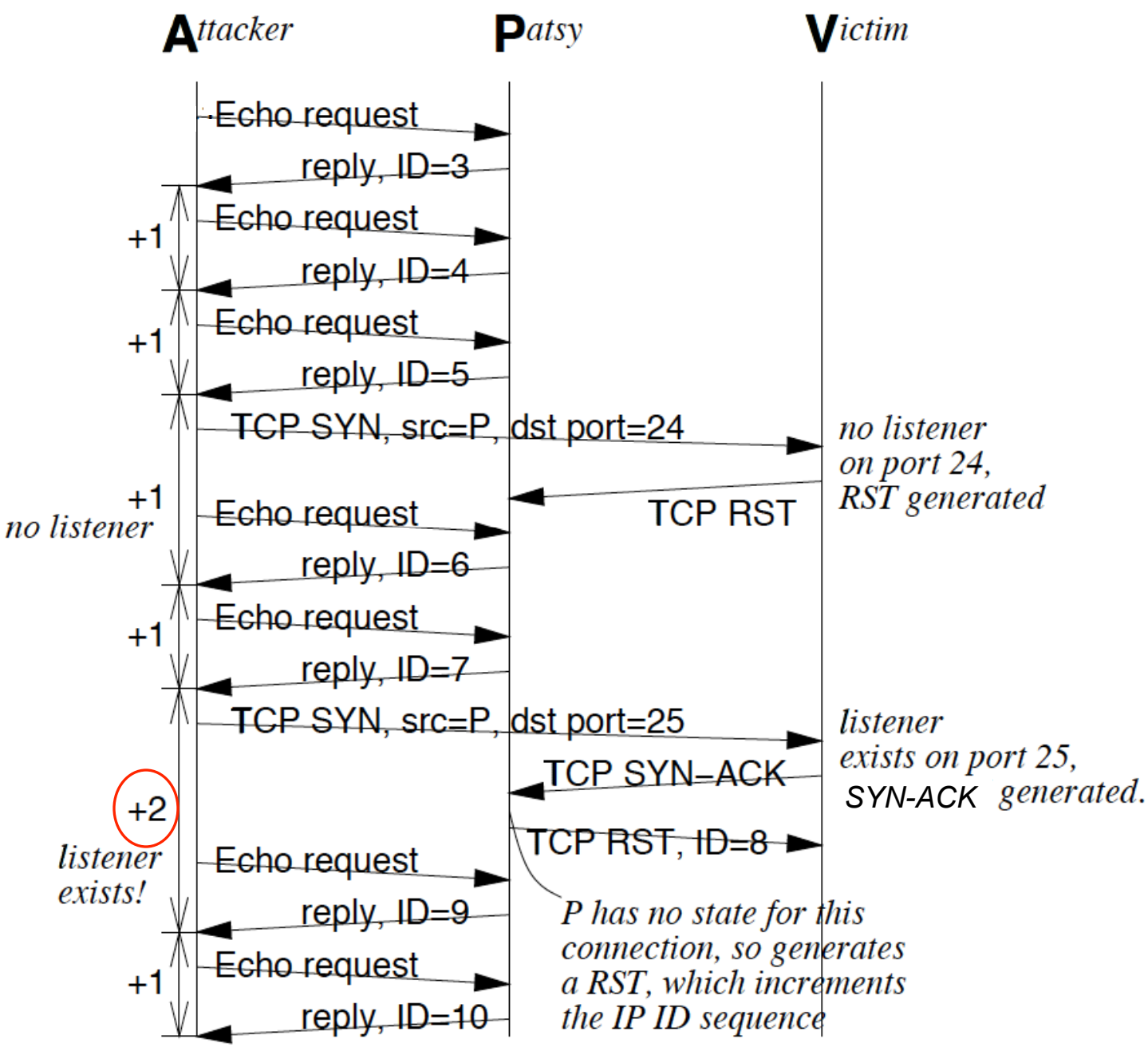

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6


Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7


Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener on port 24, RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener exists on port 25, SYN-ACK generated.
TCP SYN–ACK

Spoofed


Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
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
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener on port 24, RST generated
+1
no listener
Echo request
TCP RST
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener exists on port 25, SYN-ACK generated.
TCP SYN–ACK
+2
TCP RST, ID=8
listener exists!
Echo request
reply, ID=9
P has no state for this connection, so generates a RST, which increments the IP ID sequence
+1
Echo request
reply, ID=10

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
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

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
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

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
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

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
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

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.

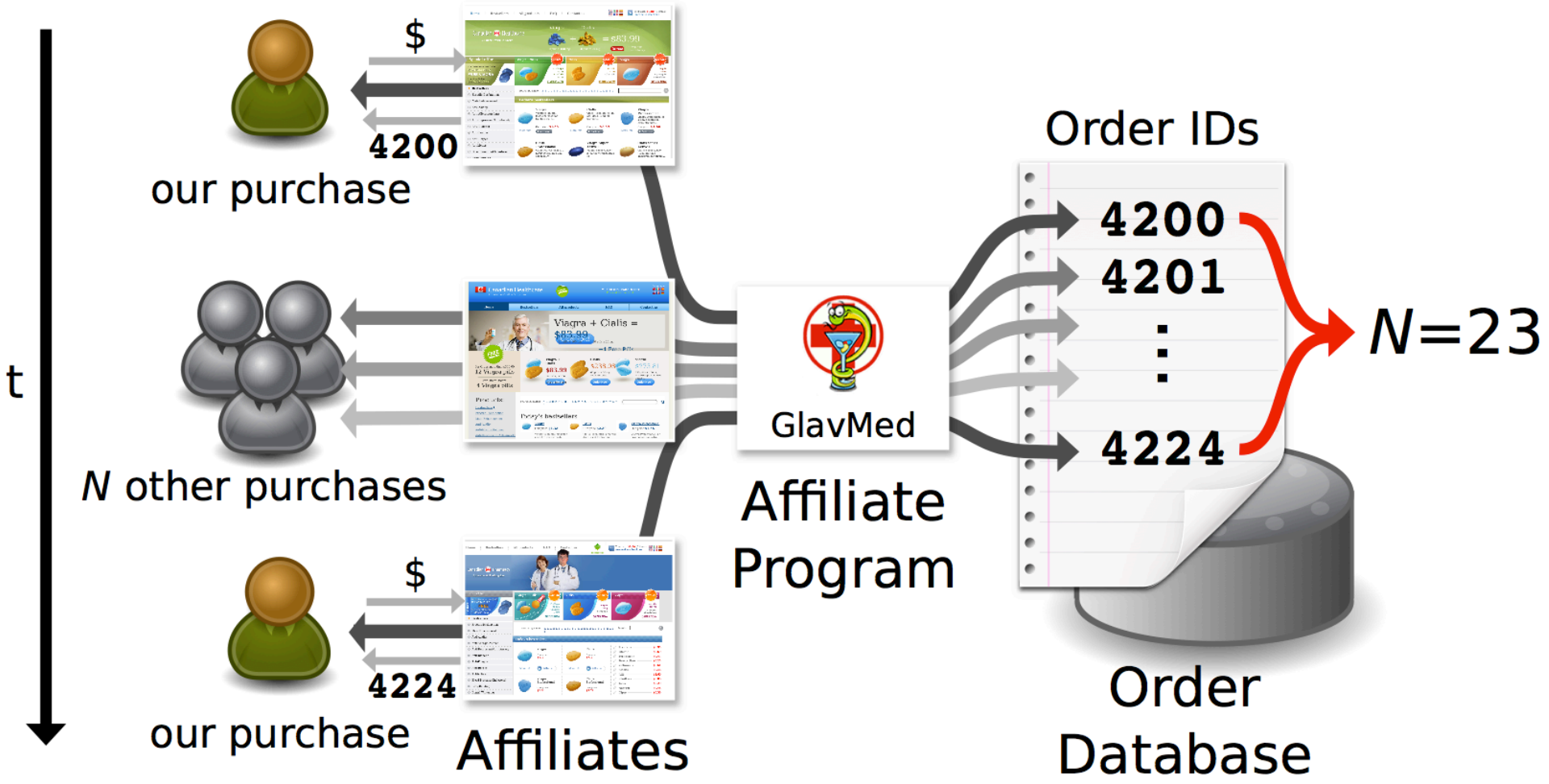
NOTE: Contact us about your order only through customers support system www.rxsup24.com
Before contact us and ask about time for delivery please read our shipping policy.

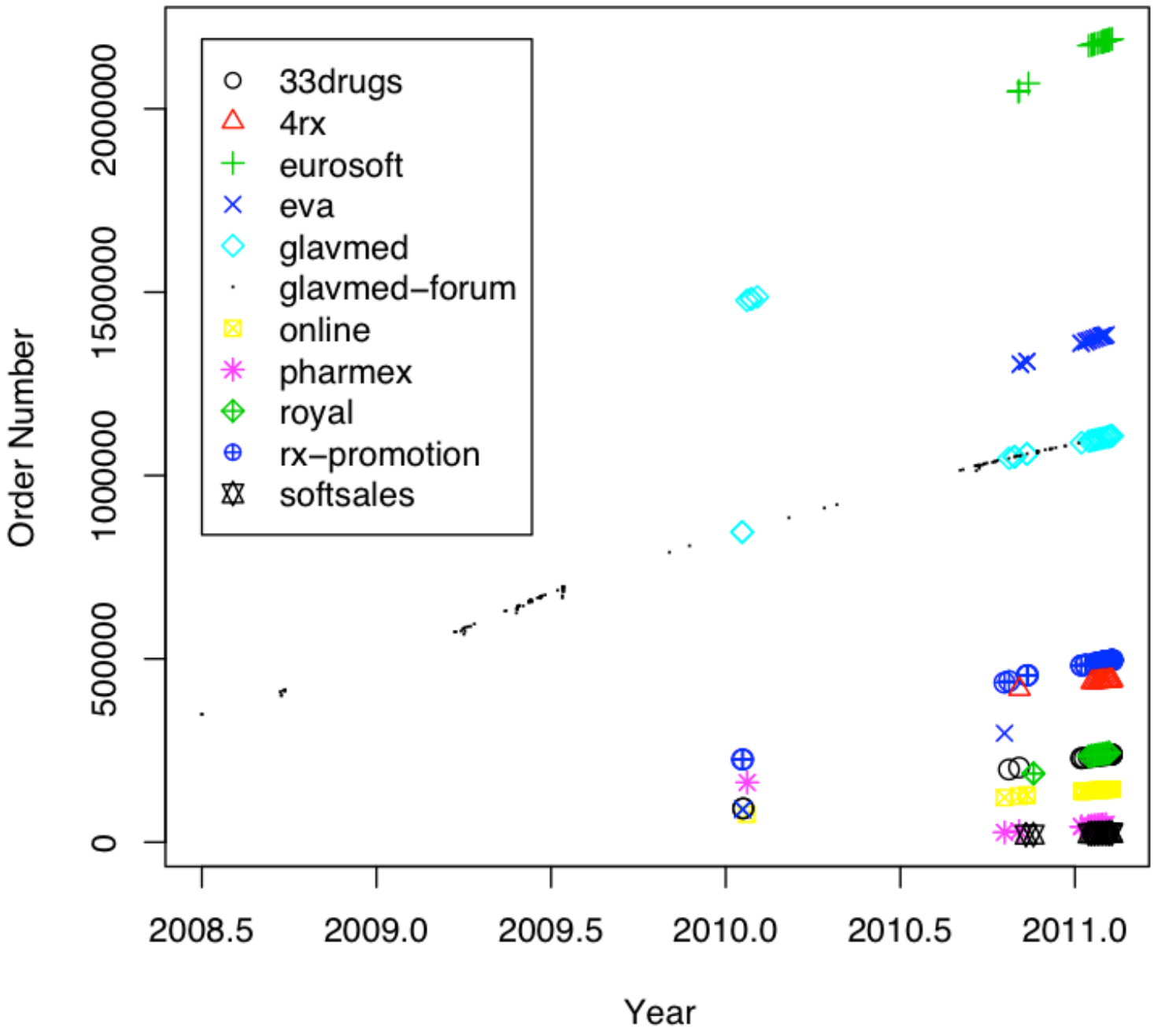
ORDER STATUS, TRACKING NUMBER, FAQ ABOUT DELIVERY:

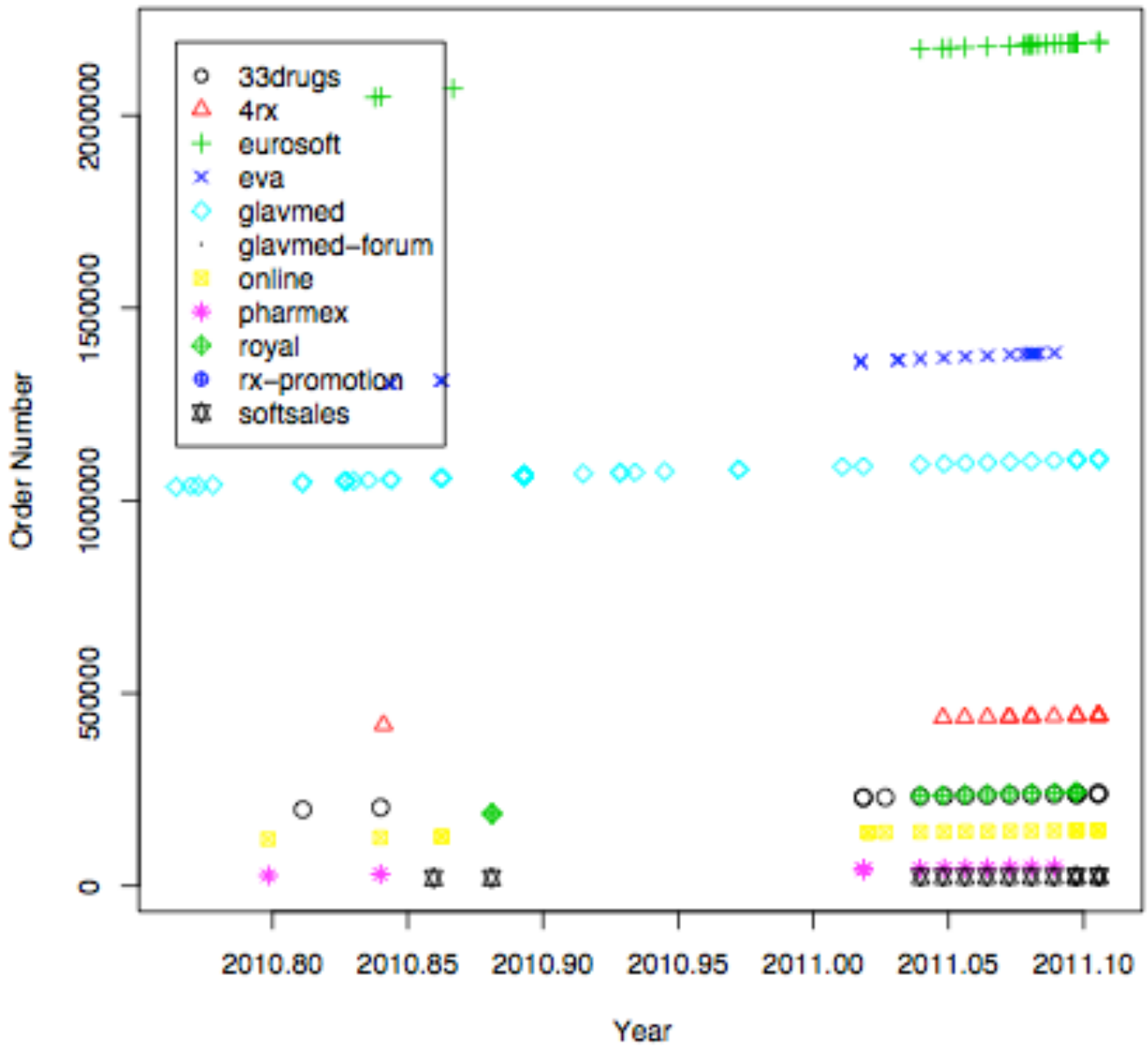
Website menu --> Order status

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

Customers support system: www.rxsup24.com


t
$
4200
our purchase
N other purchases
$
4224
our purchase
Affiliates
GlavMed
Affiliate Program
Order IDs
4200
4201
4224
N=23
Order Database


33drugs
4rx
eurosoft
eva
glavmed
glavmed−forum
online
pharmex
royal
rx−promotion
softsales
Order Number
0
500000
1000000
1500000
2000000
2008.5
2009.0
2009.5
2010.0
2010.5
2011.0
Year


33drugs
4rx
eurosoft
eva
glavmed
glavmed−forum
online
pharmex
royal
rx−promotion
softsales
Order Number
0
500000
1000000
1500000
2000000
2010.80
2010.85
2010.90
2010.95
2011.00
2011.05
2011.10
Year