

Introduction 1

20
2015-2016
CESNET
Detection and Analysis of SIP
Fraud Attack on 100Gb
Ethernet with NEMEA system
Jan Pliska (jpliska@cesnet.cz)
18th July 2016, IETF 10460 Workshop, Berlin

Introduction & Motivation

Flow based Monitoring

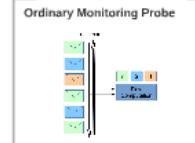
- Target especially on high speed links (traffic volume)
- Used for security analysis, performance evaluation, accounting...

Problems

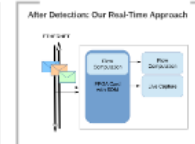
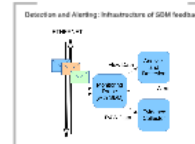
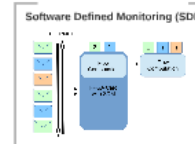
- Aggregated data is not enough for:
 - forensic analysis
 - anomaly pattern to measure anomaly detection
 - verification of detected events

Our goals

- Automatic flow capture on demand (driven by feedback)
- Store them continuously packet capture — Time Machine
- Algorithm containing packet in flow based principles



SDM Feedback 2



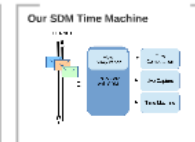
SDM Timemachine 3

Time Machine by Kornel & Paxson

- "Close Covert Approach"
- Proposed by Kornel, Paxson et al. "Building a time machine for efficient recording and retrieval of high-speed network traffic: The case study of the NSF GEANT2 backbone network" (Mansour et al., USENIX Security, 2005)
- Storage of packets on hard drives
- Long-term storage
- Closure: not all packets, just beginning of flows (containing headers)

Our SDM Time Machine

- Principle of our approach (for 100 Gbps):
 - storing packets in RAM (because of speed)
 - implement software replication
 - Time Machine stores for n packets of each flow and based on this stored and drops it
 - After alert is reported, we start the locking
 - If we have selected packets from the very buffer, we can look into the past

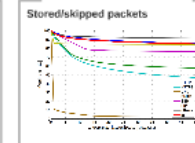
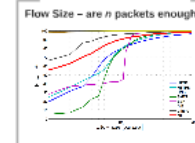


Measurements 4

Already Tested Scenarios

- Detection of network scans
- Communication channels via DNS
- Guessing SIP dial plan

Using SDM with Time Machine, we can get evidence and verification of detected events.



Configuration of network probe

- 24 CPU cores
- 64 GB RAM
- 80 Gbps COMBO card (capable of SDM)

- Using 512 GB,
- at 80 Gbps line,
- storing first 10 packets of each flow,
- we can store about 35 min of traffic.

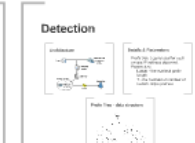
Note: it is highly dependent on traffic volume and distribution.



SIP Fraud Attack 5

SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
- A call to PSTN via the gateway require to guess a correct prefix.



Visualization 6

Netfox Detective

The screenshot shows a complex network visualization with various nodes and connections, representing the traffic captured during the attack.



Conclusion 7

Conclusion

- We can monitor 100 Gbps.
- Detection uses extended flow records
- Presented system provides:
 - Raw records
 - full packet capture of detected IP
 - history: beginning of each flow of detected IP - Time Machine

20
2015-2016
CESNET

Thank you!
Any questions?
@cesnet
<https://www.cesnet.org>

This presentation
Author: Jan Pliska
Contact: jpliska@cesnet.org
My contact
@cesnet



1996–2016

CESNET

Detection and Analysis of SIP Fraud Attack on 100Gb Ethernet with NEMEA system

Jan Pluskal (pluskal@cesnet.cz)

18th July 2016, IRTF NMRG Workshop, Berlin

Introduction 1

20
2015-2016
CESNET
Detection and Analysis of SIP
Fraud Attack on 100Gb
Ethernet with NEMEA system
Jan Pliska (jpliska@cesnet.cz)
18th July 2016, IETF 10460 Workshop, Berlin

Introduction & Motivation

Flow based Monitoring

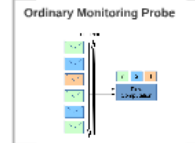
- Inevitable especially on high speed links (traffic volume)
- Limited for security analysis, performance evaluation, accounting

PIFalls

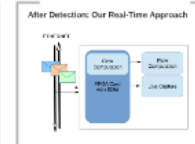
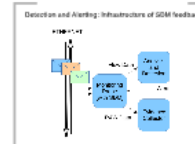
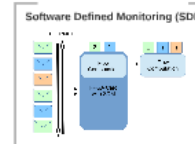
- Aggregated data is not enough for:
 - forensic analysis
 - anomaly pattern to measure anomaly detection
 - verification of detected events

Our goals

- Automatic flow capture on demand (driven by feedback)
- Short term continuous packet capture — Time Machine
- Alternative capturing packet in flow based principles



SDM Feedback 2



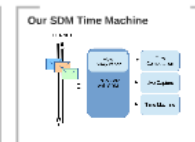
SDM Timemachine 3

Time Machine by Kornel & Paxson

- "Close Covert Approach"
- Proposed by Kornel, Paxson et al. "Building a time machine for efficient recording and retrieval of high-speed network traffic: The case study of the NSF GEANT2 backbone network" (Mansour et al., USENIX Security, 2005)
- Storage of packets on hard drives
- Long-term storage
- Closure: not all packets, just beginning of flows (containing headers)

Our SDM Time Machine

- Principle of our approach (for 100 Gbps)
- Storing packets in RAM (because of speed)
- Implemented software emulator
- Time Machine stores for n packets of each flow and begins data is stored and drop is avoided
- After alert is reported, we start the logging if we have exceeded packets from the very buffer, we can look into the past!



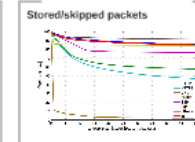
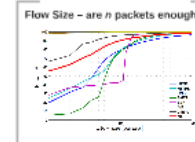
Measurements 4

Already Tested Scenarios



- Detection of network scans
- Communication channels via DNS
- Guessing SIP dial plan

Using SDM with Time Machine, we can get evidence and verification of detected events.

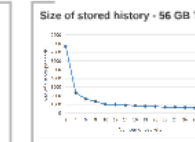


Configuration of network probe

- 24 CPU cores
- 64 GB RAM
- 80 Gbps COMBO card (capable of SDM)

• Using 512 GB,
• at 80 Gbps line,
• storing first 10 packets of each flow,
• we can store about 35 min of traffic.

• Note: it is highly dependent on traffic volume and distribution.



SIP Fraud Attack 5

SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures if any at all
- A call to PSTN via the gateway require to guess a correct prefix.



Visualization 6

Netfox Detective



Conclusion 7

Conclusion

- We can monitor 100 Gbps.
- Detection uses extended flow records
- Presented system provides:
 - Raw records
 - full packet capture of detected IP
 - history: beginning of each flow of detected IP - Time Machine

20
2015-2016
CESNET

Thank you!
Any questions?


github: <https://github.com/jpliska>
https://www.cesnet.org

My contact

Address: jpliska@cesnet.org
Phone: +420 221 911 111
Email: jpliska@cesnet.org
Twitter: @jpliska



Introduction 1



CESNET
1996 - 2016

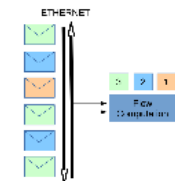
Detection and Analysis of SIP Fraud Attack on 100Gb Ethernet with NEMEA system

Jan Pluskal (pluskal@cesnet.cz)
18th July 2016, IRTF NMRG Workshop, Berlin

Introduction & Motivation

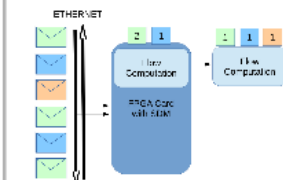
- Flow-based Monitoring**
- Needed especially on high speed links (traffic volume)
 - Useful for security analysis, performance evaluation, accounting, ...
- Pitfalls**
- Aggregated data is not enough for:
 - forensic analysis
 - learning patterns to improve detection/prevention
 - verification of detected events
- Our goals**
- Automatic live capture on demand (driven by feedback)
 - Short-term continuous packet capture — Time Machine
 - Altogether: combining packet- & flow-based principles

Ordinary Monitoring Probe

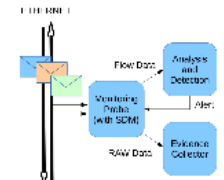


SDM Feedback 2

Software Defined Monitoring (SDM)



Detection and Alerting: Infrastructure of SDM feedback



After Detection: C



Timemachine 3

Time Machine by Kornexl & Paxson

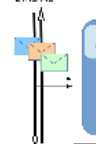
- "Clever Caveman Approach"
- Proposed in:
 - Kornexl, Stefan, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic." Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, USENIX Association, 2005.
- Storage of packets on hard drives
- Long-term storage
- Close to real-time business of flow



Our SDM Time Machine

- Principle of our approach (for 100 Gbps)
 - Storing packets in RAM (because of speed)
 - implemented software ring buffer
 - Time Machine stores first n packets of each flow and keeps them stored as long as possible
 - After alert is reported, we start live capturing
 - Plus we have historical packets from the ring buffer = we can look into the past!

Our SDM Tim



Introduction & Motivation

Flow-based Monitoring

- Needed especially on high speed links (traffic volume)
- Useful for security analysis, performance evaluation, accounting, . . .

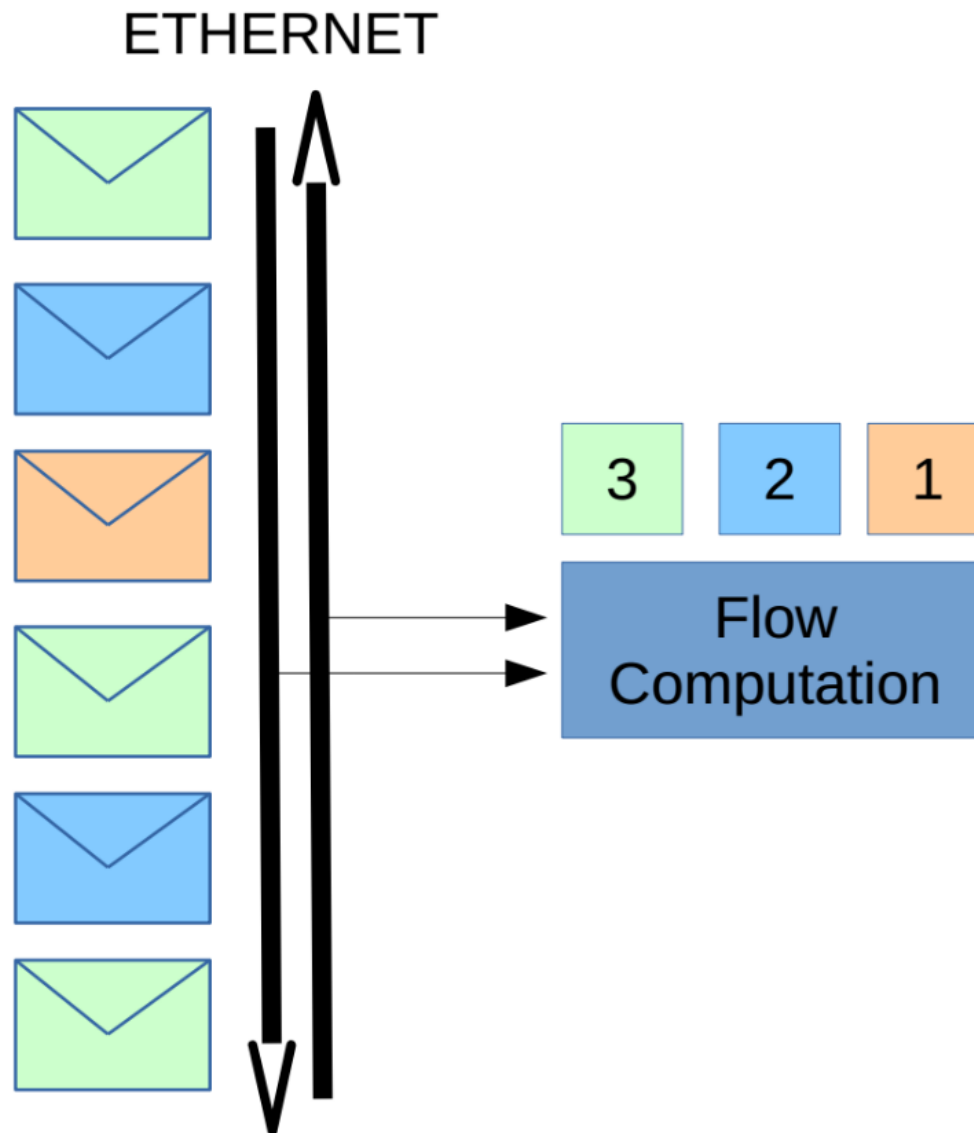
Pitfalls

- Aggregated data is not enough for:
 - forensic analysis
 - learning patterns to improve detection/prevention
 - verification of detected events

Our goals

- Automatic live capture on demand (driven by feedback)
- Short-term continuous packet capture — Time Machine
- Altogether: combining packet- & flow- based principles

Ordinary Monitoring Probe



Introduction 1

20
1996-2016
CESNET
Detection and Analysis of SIP Fraud Attack on 100Gb Ethernet with NEMEA system
Jan Pluskal (pluskal@cesnet.cz)
18th July 2016, IRTF NMRG Workshop, Berlin

Introduction & Motivation

Flow-based Monitoring

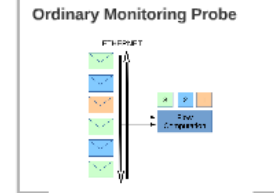
- Needed especially on high speed links (traffic volume)
- Useful for security analysis, performance evaluation, accounting, ...

Details

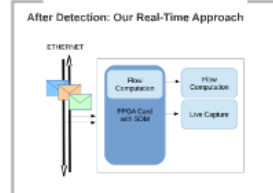
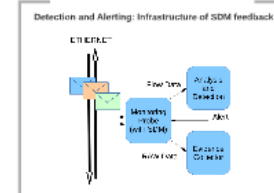
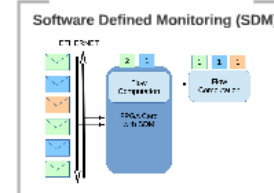
- Aggregated data is not enough for:
 - Forensic analysis
 - Learning patterns to improve detection/prevention
 - Verification of detected events

Our goals

- Automatic live capture on demand (driven by feedback)
- Short-term continuous packet capture — Time Machine
- Allgeherer: combining packet- & flow-based principles



SDM Feedback 2



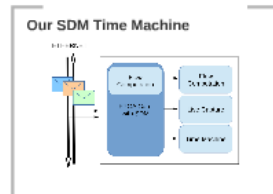
SDM Timemachine 3

Time Machine by Kornell & Paxson

- "Clever Cavanan Approach"
- Proposed in:
 - Stanislav Stefan, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic". Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, USENIX Association, 2005.
- Storage of packets on hard drives
- Long-term storage
- Clever = not all packets, just beginning of flows (containing headers)

Our SDM Time Machine

- Principle of our approach (for 100 Gbps)
- Storing packets in RAM (because of speed)
- Implemented software ring buffer
- Time Machine stores first n packets of each flow and keeps them stored as long as possible
- After alert is reported, we start live capturing
- Plus we have historical packets from the ring buffer = we can look into the past!

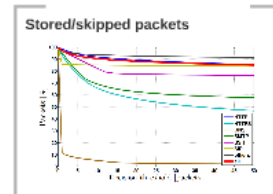
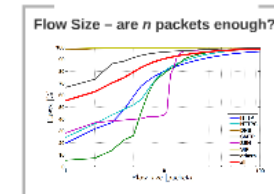


Measurements 4

Already Tested Scenarios

- Detection of network scans
- Communication tunnels via DNS
- Guessing SIP dial plan

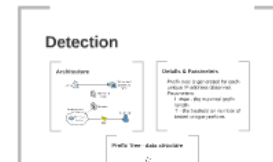
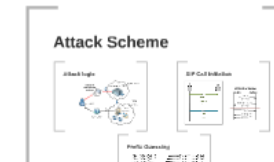
Using SDM with Time Machine, we can get evidence and verification of detected events.



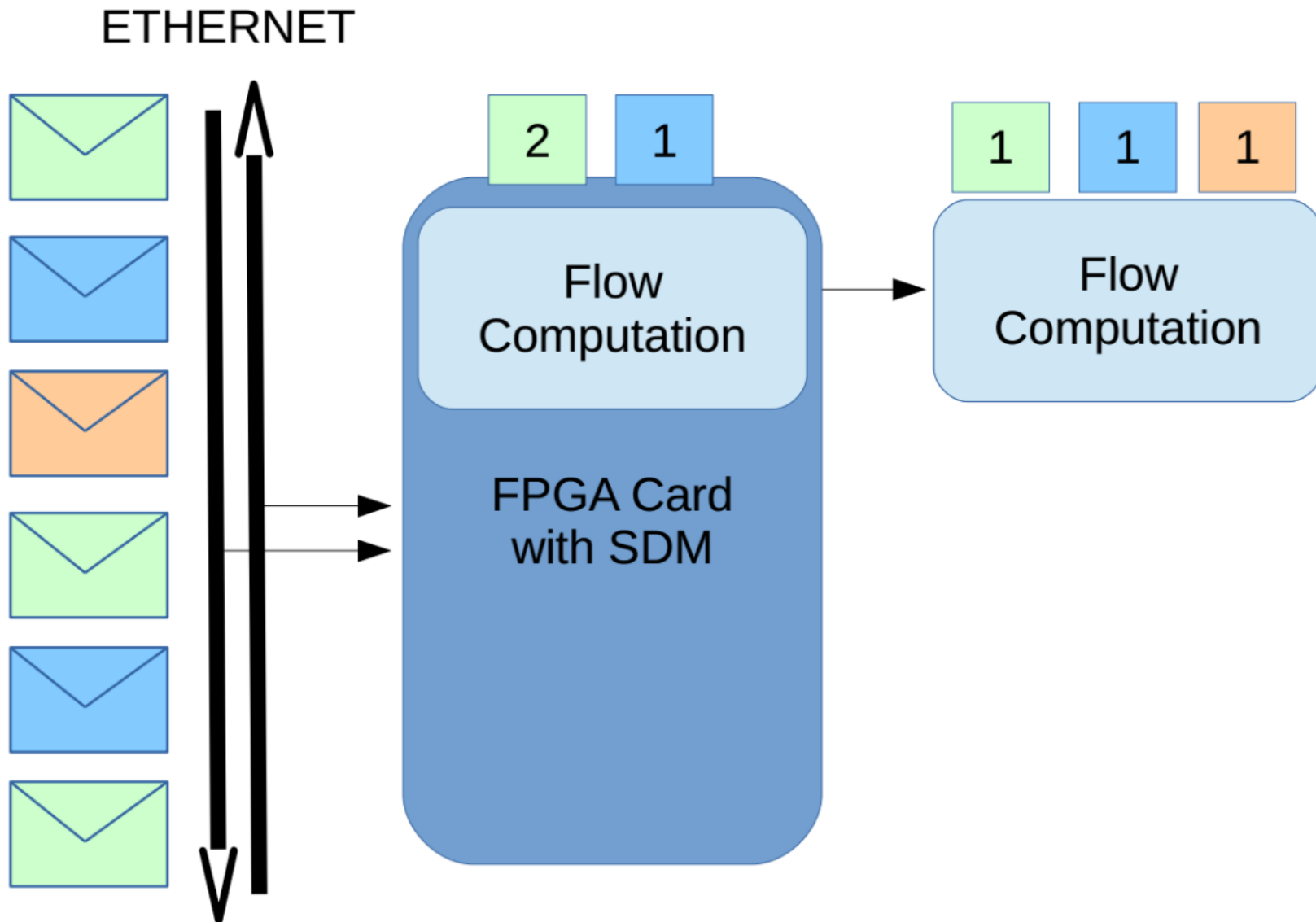
SIP Fraud Attack 5

SIP Fraud Attack

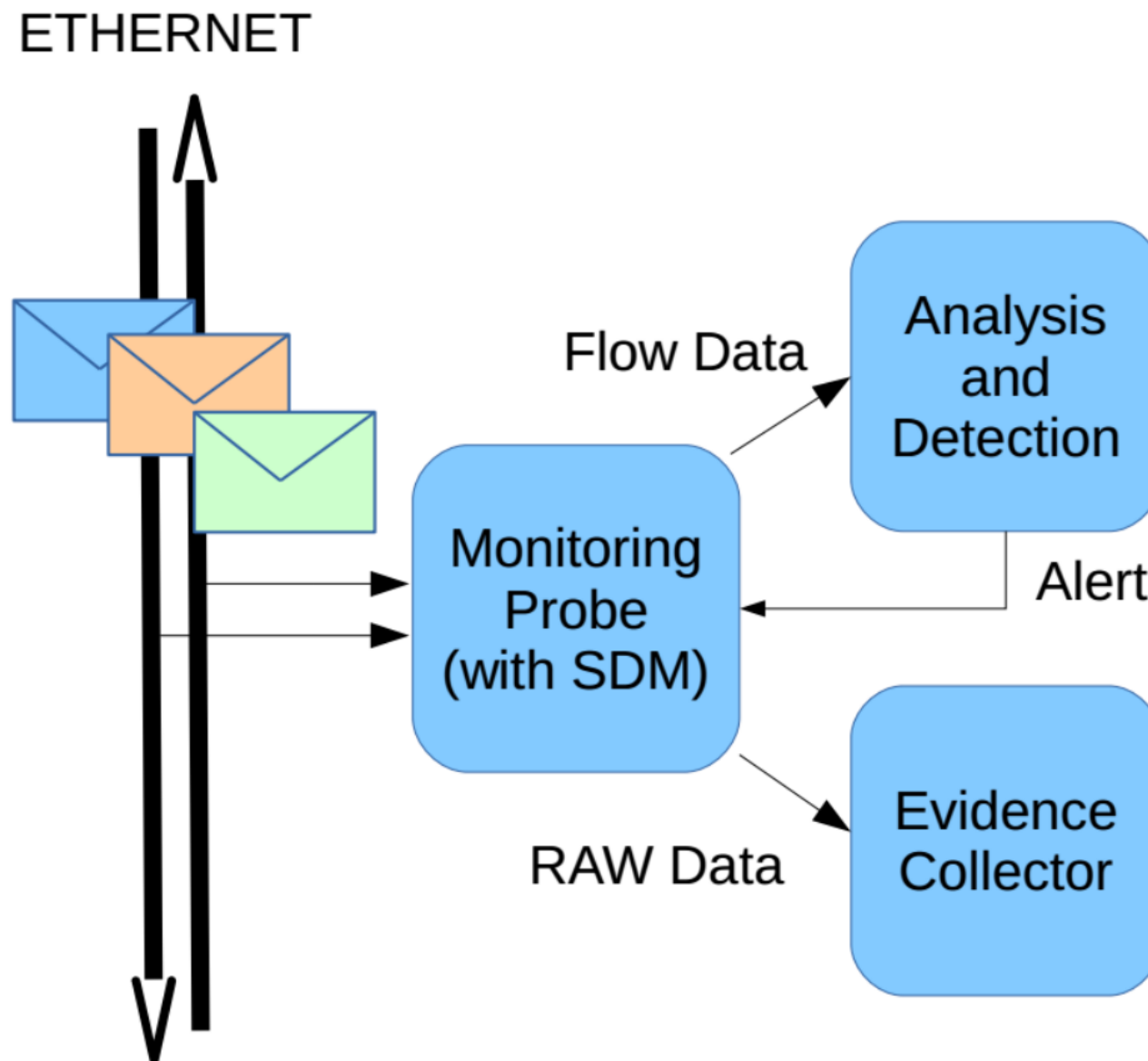
- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
 - A call to PSTN via the gateway require to guess a correct prefix.



Software Defined Monitoring (SDM)

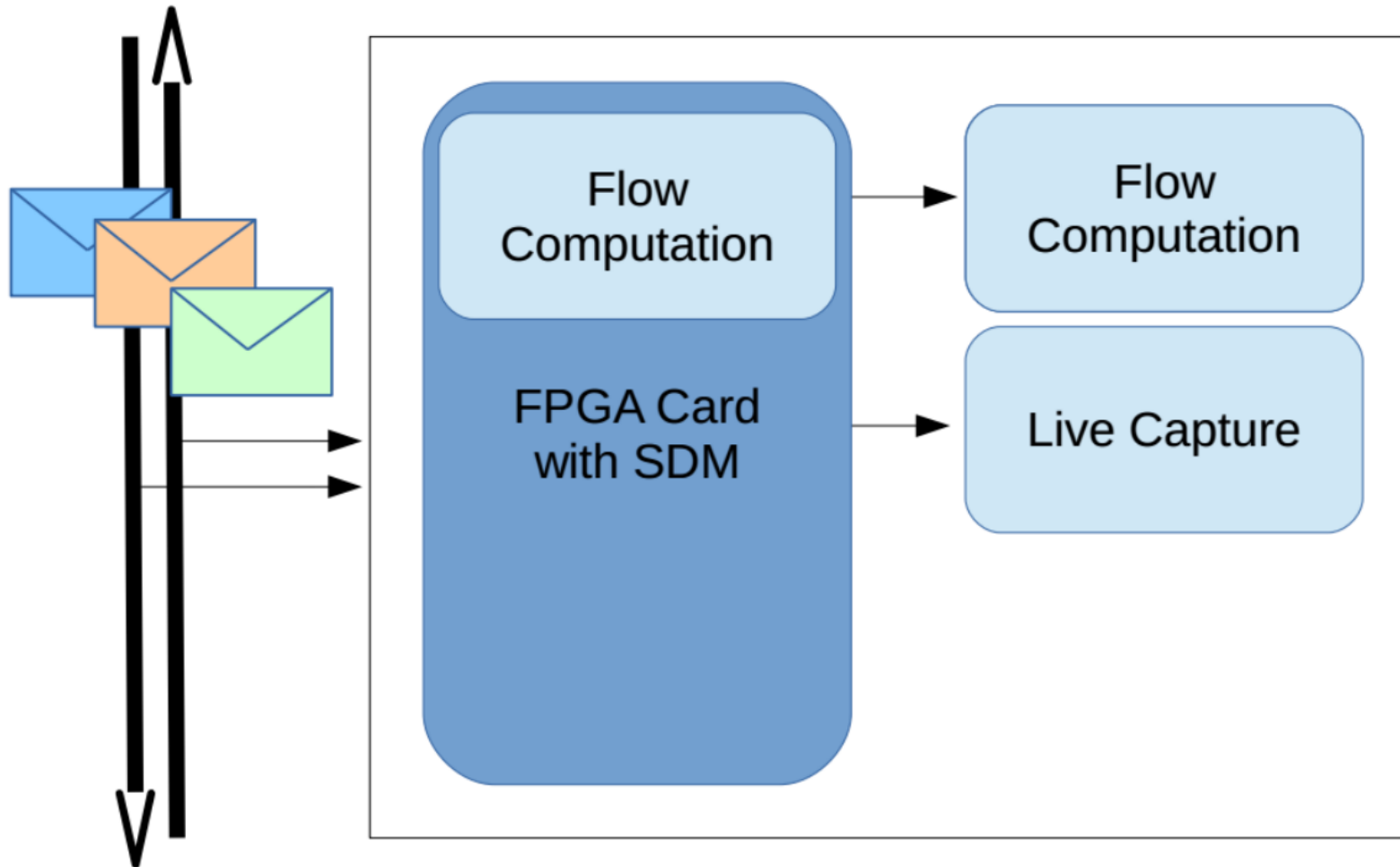


Detection and Alerting: Infrastructure of SDM feedback



After Detection: Our Real-Time Approach

ETHERNET



Introduction 1

20
1996-2016
CESNET
**Detection and Analysis of SIP
Fraud Attack on 100Gb
Ethernet with NEMEA system**
Jan Pluskal (pluskal@cesnet.cz)
18th July 2016, IRTF-NMRG Workshop, Berlin

Introduction & Motivation

Flow-based Monitoring

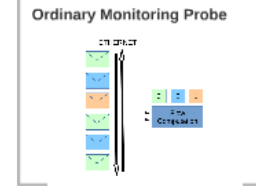
- Needed especially on high speed links (traffic volume)
- Useful for security analysis, performance evaluation, accounting, ...

Details

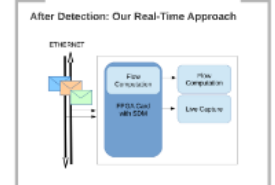
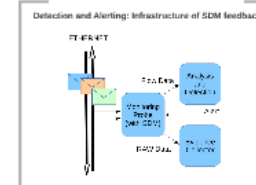
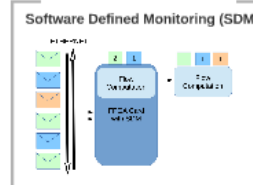
- Aggregated data is not enough for:
 - forensic analysis
 - learning patterns to improve detection/prevention
 - verification of detected events

Our goals

- Automatic live capture on demand (driven by feedback)
- Short-term continuous packet capture — Time Machine
- Altogether: combining packet- & flow-based principles



SDM Feedback 2



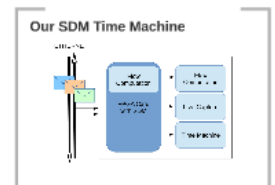
SDM Timemachine 3

Time Machine by Kornelx & Paxson

- "Clever Civilization Approach"
- Proposed in:
 - Kornel, Stefan, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic." Proceedings of the SIGCOMM SIGCOMM conference on Internet Measurement, USENIX Association, 2005.
- Storage of packets on **hard drives**
- Long-term storage
- Clever = not all packets, just beginning of flows (containing headers)

Our SDM Time Machine

- Principle of our approach (for 100 Gbps)
- Storing packets in RAM (because of speed)
- Implemented software ring buffer
- Time Machine stores first n packets of each flow and keeps them stored as long as possible
- After alert is reported, we start live capturing
- Plus we have historical packets from the ring buffer => we can look into the past!

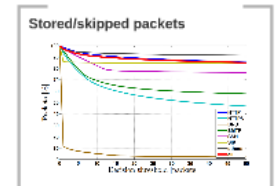
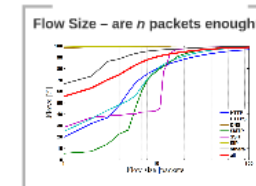


Measurements 4

Already Tested Scenarios

- Detection of network scans
- Communication tunnels via DNS
- Guessing SIP dial plan

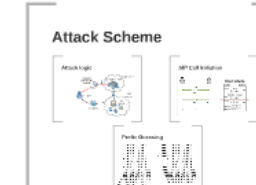
Using SDM with Time Machine, we can get evidence and verification of detected events.



SIP Fraud Attack 5

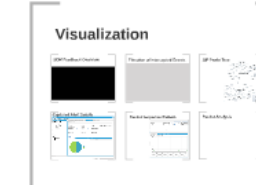
SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
 - A call to PSTN via the gateway require to guess a correct prefix.



Visualization 6

Netfox Detective



Time Machine by Kornexl & Paxson

- “Clever Caveman Approach”
- Proposed in:
 - Kornexl, Stefan, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic. "Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement. USENIX Association, 2005.
- Storage of packets on **hard drives**
- **Long-term** storage
- Clever = not all packets, just **beginning of flows** (containing headers)

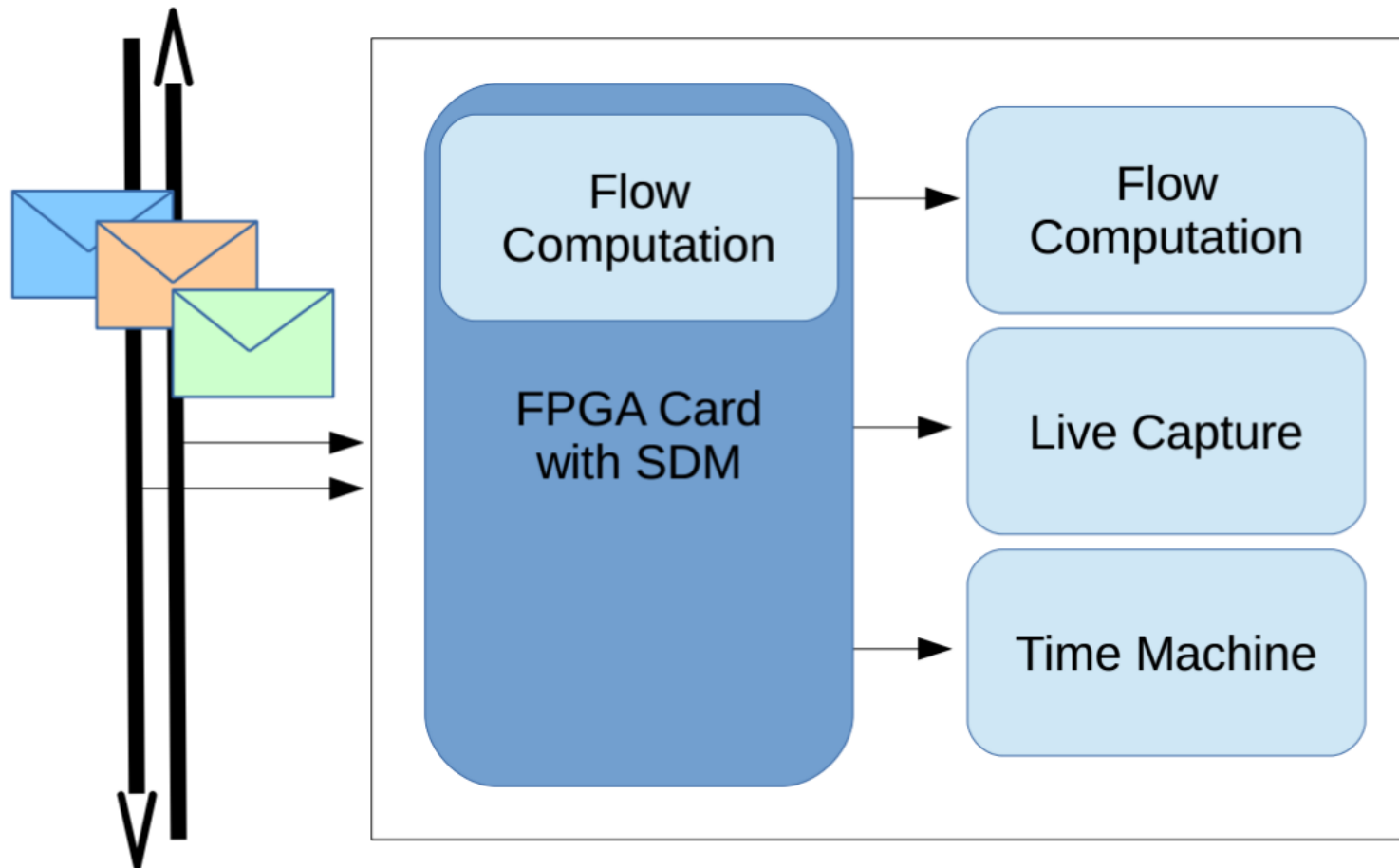


Our SDM Time Machine

- **Principle of our approach (for 100 Gbps)**
 - Storing packets in **RAM** (because of speed)
 - Implemented *software ring buffer*
 - Time Machine stores *first n packets* of each flow and keeps them stored *as long as possible*
 - After alert is reported, we start *live capturing*
 - Plus we have *historical packets* from the ring buffer
= we can look into the past!

Our SDM Time Machine

ETHERNET



Introduction 1

2016 CESNET
Detection and Analysis of SIP
Fraud Attack on 100Gb
Ethernet with NEMEA system
Jan Pláskal (plaskal@cesnet.cz)
18th July 2016, RTF/KMRO Workshop, Berlin

Introduction & Motivation

Flow based Monitoring

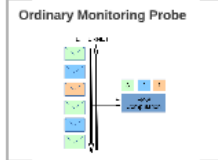
- Used especially on high speed links (traffic volume)
- Useful for security analysis, performance evaluation, accounting.

Pros:

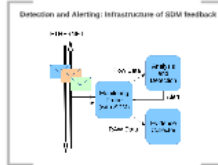
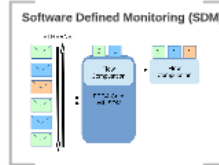
- Aggregated data is not enough for:
 - Traffic analysis
 - Learning patterns to improve detection/prevention
 - Verification of detected events

Our goals

- Address how capture on demand (from by feedback)
- Short term continuous packet capture — Time Machine
- Altogether combining packet & flow based principles



SDM Feedback 2



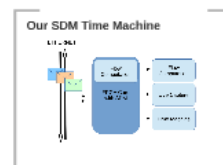
Time Machine 3

Time Machine by Komex & Paxson

- "Clear Capture Approach"
- Presented in:
 - Komex, Daini, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic." Proceedings of the SIGCOMM/SIGCOMM conference on Internet Measurement, USENIX Association, 2005
- Storage of packets on hard drives
- Long-term storage
- Clear most of packets, just beginning of flows (containing headers)

Our SDM Time Machine

- Principle of our approach (for 100 Gbps):
 - Storing packets in RAM (because of speed)
 - Implemented subsecond ring buffer
 - Time Machine uses first n packets of each flow and keeps them stored on ring as possible
 - After alert is triggered, we start live capturing
 - Plus we have historical gateway from the ring buffer — we can look into the past!

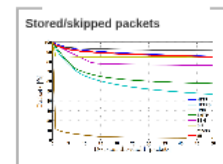
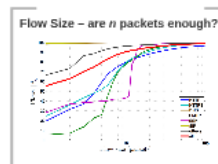


Measurements 4

Already Tested Scenarios

- Detection of network scans
- Communication tunnels via DNS
- Guessing SIP dial plan

Using SDM with Time Machine, we can get evidence and verification of detected events.



Configuration of network probe

- 24 CPU cores
- 64 GB RAM
- 80 Gbps COMBO card (capable of SDM)

Using 56 GB,
at 80 Gbps line,
storing first 30 packets of each flow,
we can store about 25 min of traffic.

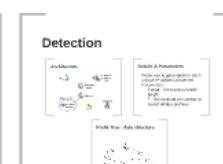
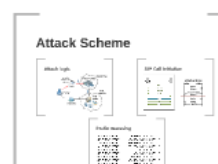
Note: it is highly dependent on traffic volume and distribution.



SIP Fraud Attack 5

SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
- A call to PSTN via the gateway require to guess a correct prefix.



Visualization 6



Conclusion 7

Conclusion

- We can monitor 100 Gbps.
- Detection uses extended flow records
- Presented system provides:
 - flow records
 - full packet capture of detected IP
 - history: beginning of each flow of detected IP - Time Machine

20 Thank you!
Any questions?
CESNET
1996-2016
October
<https://www.cesnet.org>

This presentation

My contact

- Address: Prague
- Phone: +420 224 123 456
- More info

Jan Pláskal

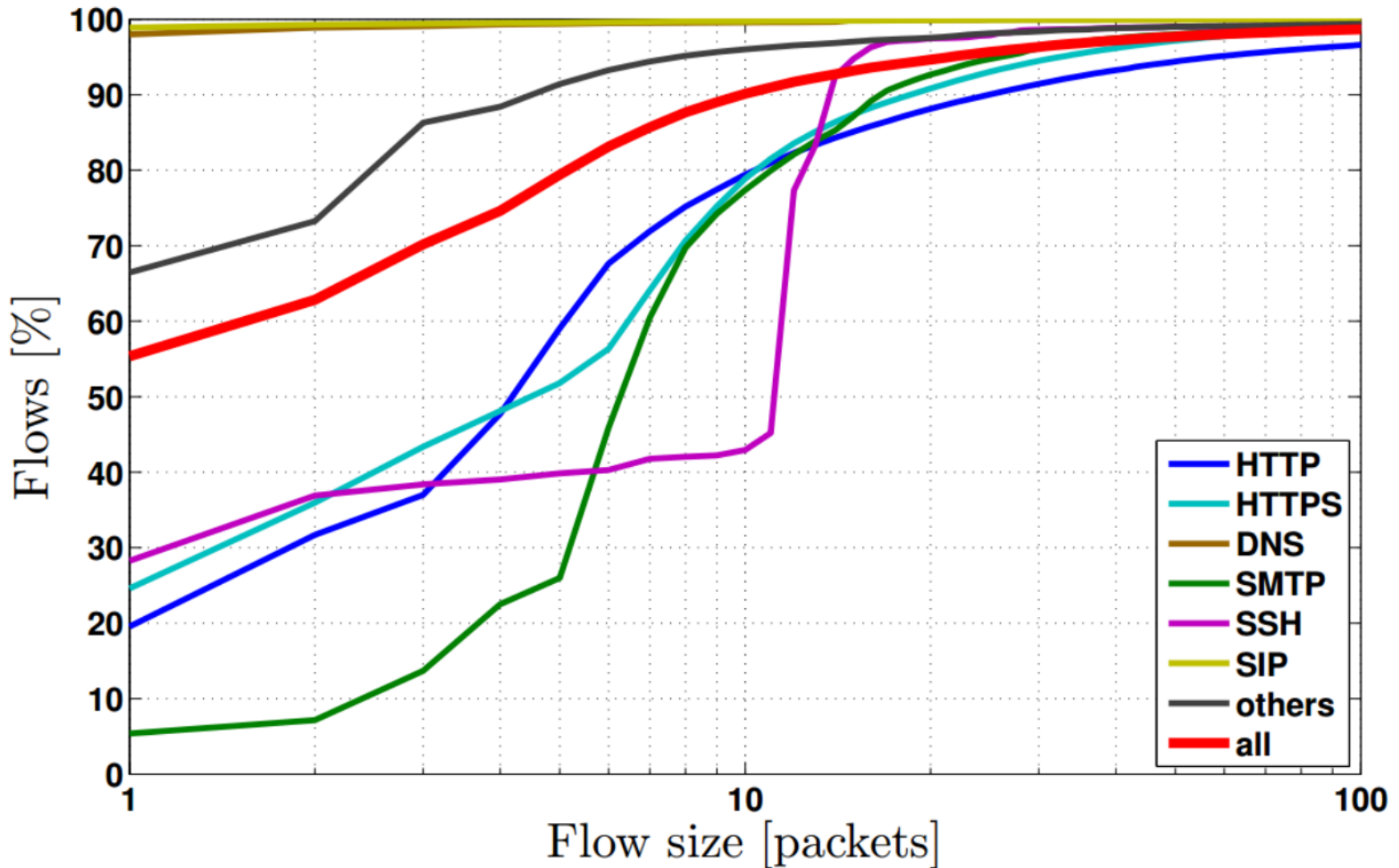
Already Tested Scenarios



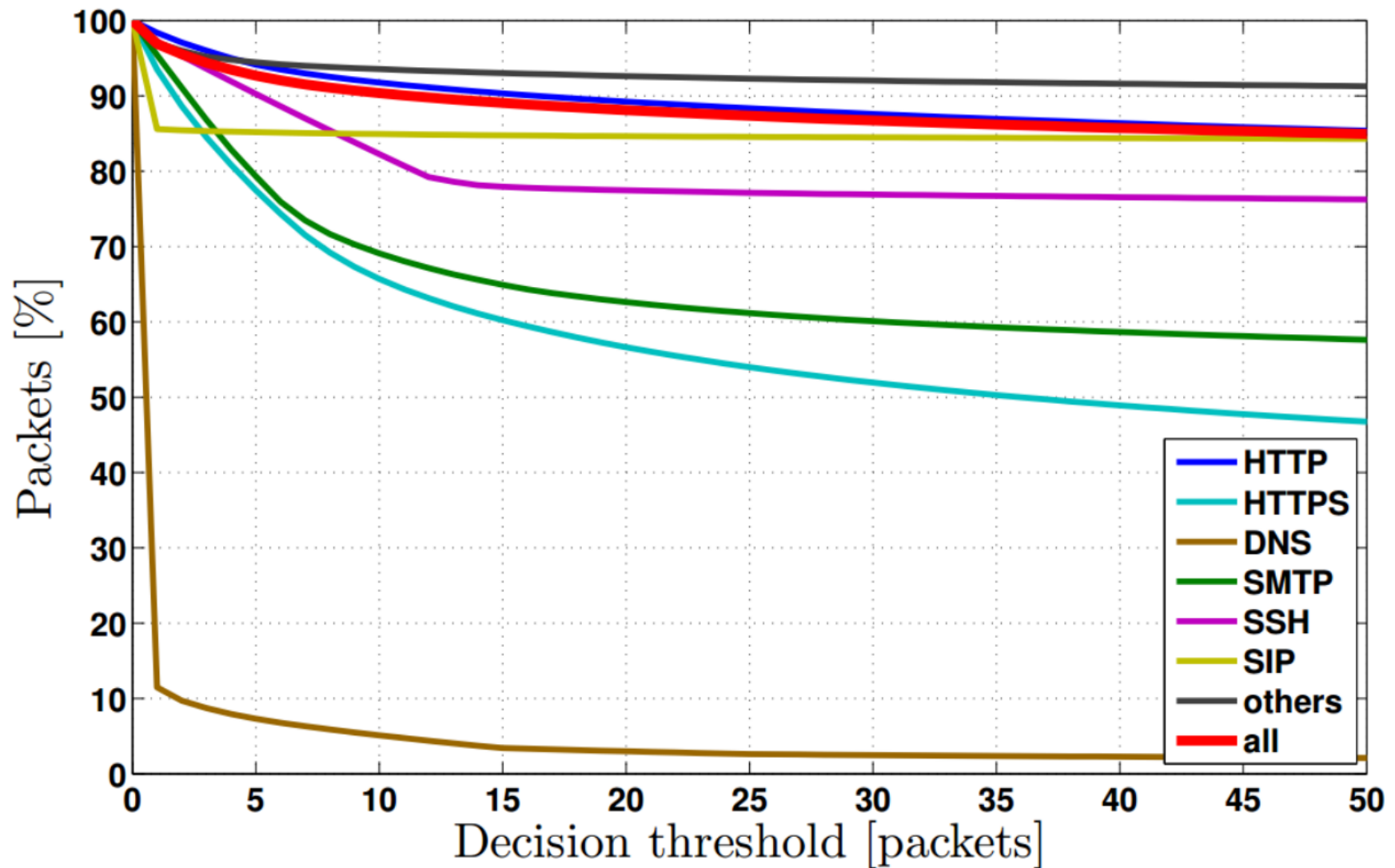
- Detection of network scans
- Communication tunnels via DNS
- Guessing SIP dial plan

Using SDM with Time Machine, we can get evidence and verification of detected events.

Flow Size – are n packets enough?



Stored/skipped packets



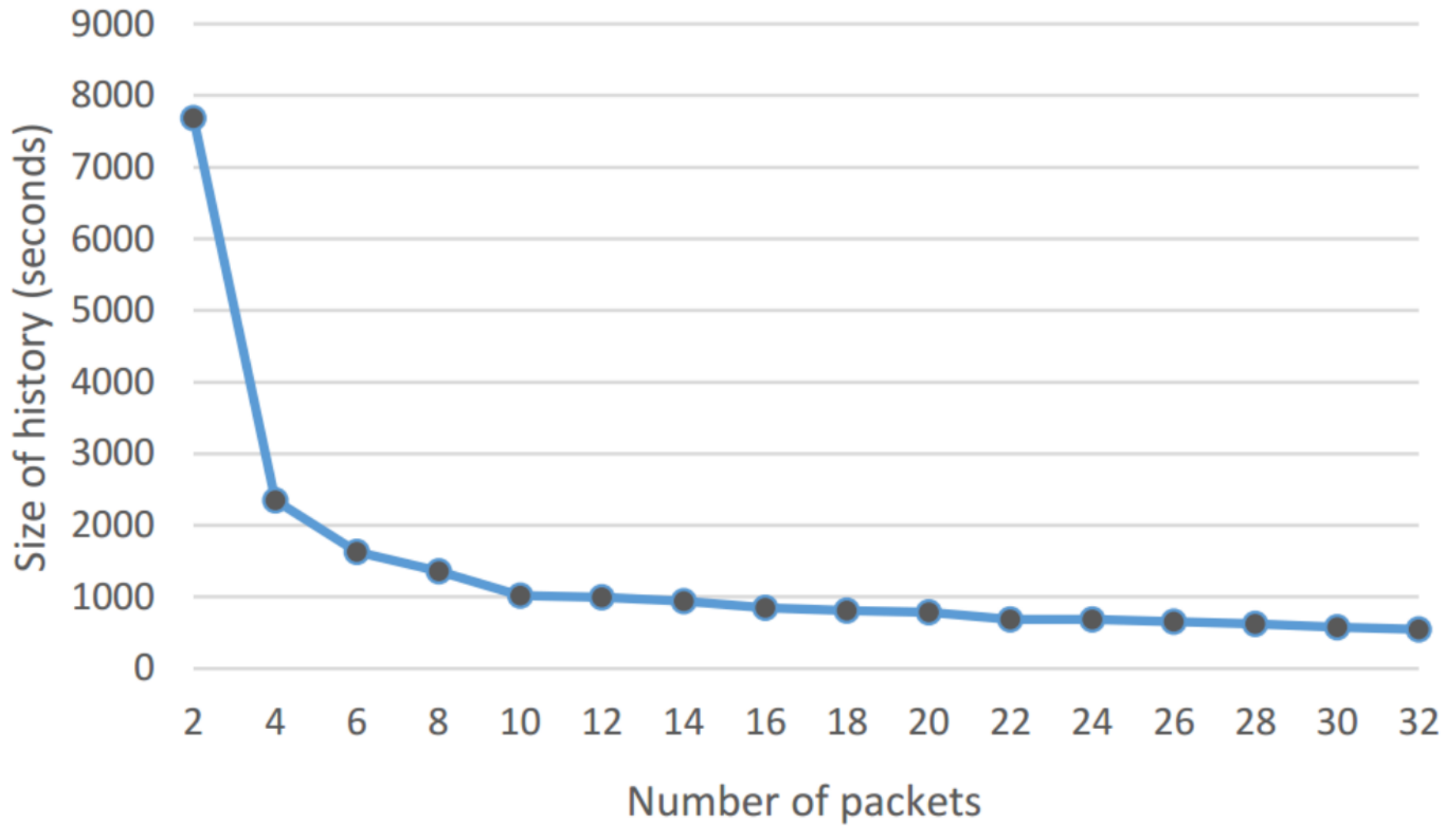
Configuration of network probe

- *24 CPU cores*
- *64 GB RAM*
- *80 Gbps COMBO card (capable of SDM)*

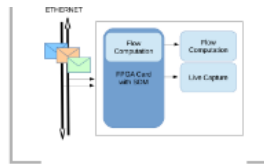
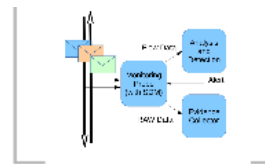
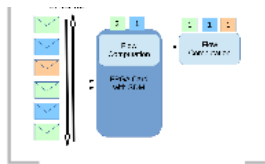
- *Using 56 GB,*
- *at 80 Gbps line,*
- *storing first 10 packets of each flow,*
- *we can store about 15 min of traffic.*

- *Note: it is highly dependend on traffic volume and distribution.*

Size of stored history - 56 GB TM



SDM Feedback 2



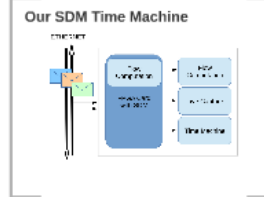
SDM Timemachine 3

Time Machine by Kornel & Paxson

- "Clever Caveman Approach"
- Proposed in: Kornel, Stefan, et al. "Building a time machine for efficient recording and retrieval of high-volume network traffic." Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, USENIX Association, 2006.
- Storage of packets on hard drives
- Long-term storage
- Clever = not all packets, just beginning of flows (containing headers)

Our SDM Time Machine

- Principle of our approach (for 100 Gbps)
- Storing packets in RAM (because of speed)
- Implemented software ring buffer
- Time Machine stores first n packets of each flow and keeps them stored as long as possible
- After alert is reported, we start live capturing
- Plus we have historical packets from the ring buffer = we can look into the past!

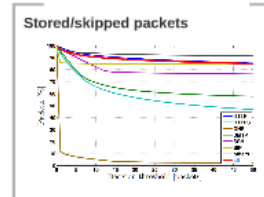
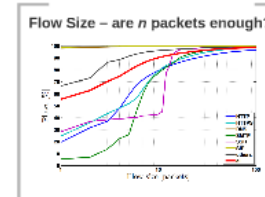


Measurements 4

Already Tested Scenarios

- Detection of network scans
- Communication tunnels via DNS
- Guessing SIP dial plan

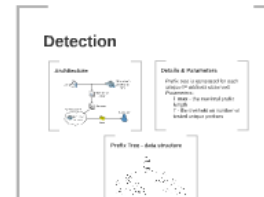
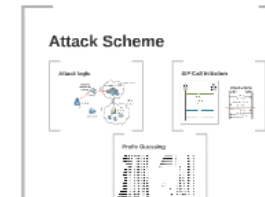
Using SDM with Time Machine, we can get evidence and verification of detected events.



SIP Fraud Attack 5

SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
- A call to PSTN via the gateway require to guess a correct prefix.



Visualization 6

Netfox Detective

Visualization

Conclusion 7

Conclusion

- We can monitor 100 Gbps.
- Detection uses extended flow records
- Presented system provides:
 - flow records
 - full packet capture of detected IP
 - history: beginning of each flow of detected IP - Time Machine

20 Thank you! Any questions?

1996-2016 CESNET

© CESNET
<https://www.liberouter.org>

This presentation

- Acknowledgments:
 - Tomas Galia
 - Zdenek Hlavac
 - Tomas Jirasek
 - Viktor Pras

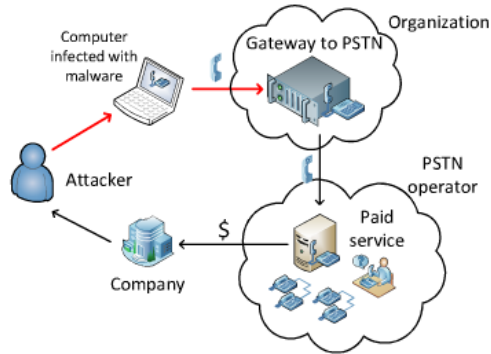
My contact

SIP Fraud Attack

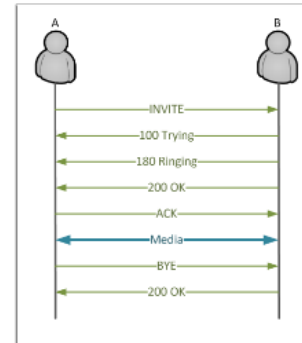
- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
 - A call to PSTN via the gateway require to guess a correct prefix.

Attack Scheme

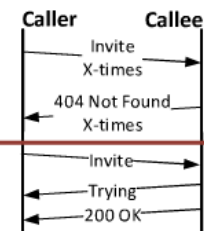
Attack logic



SIP Call Initiation



Attack scheme

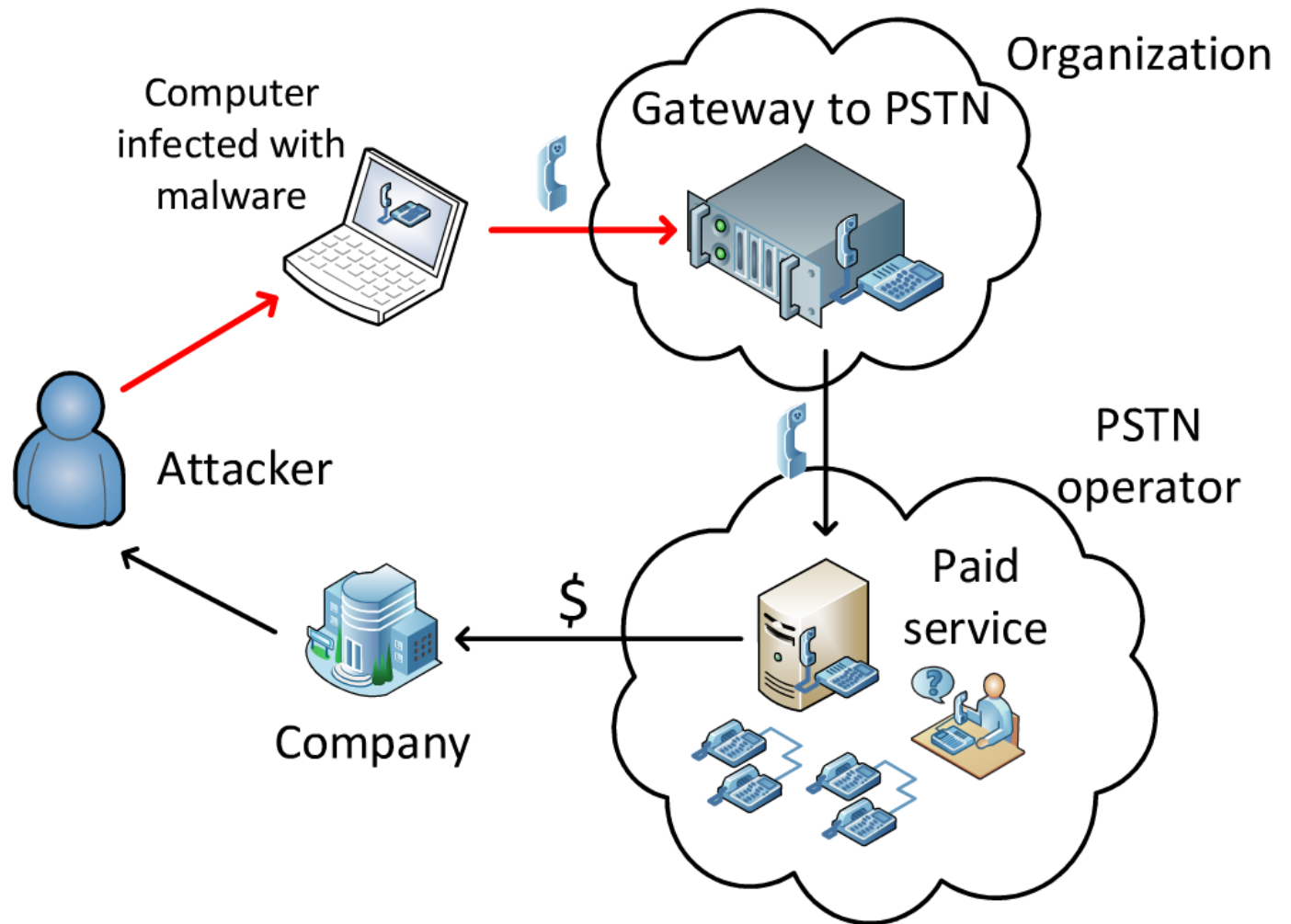


Prefix Guessing

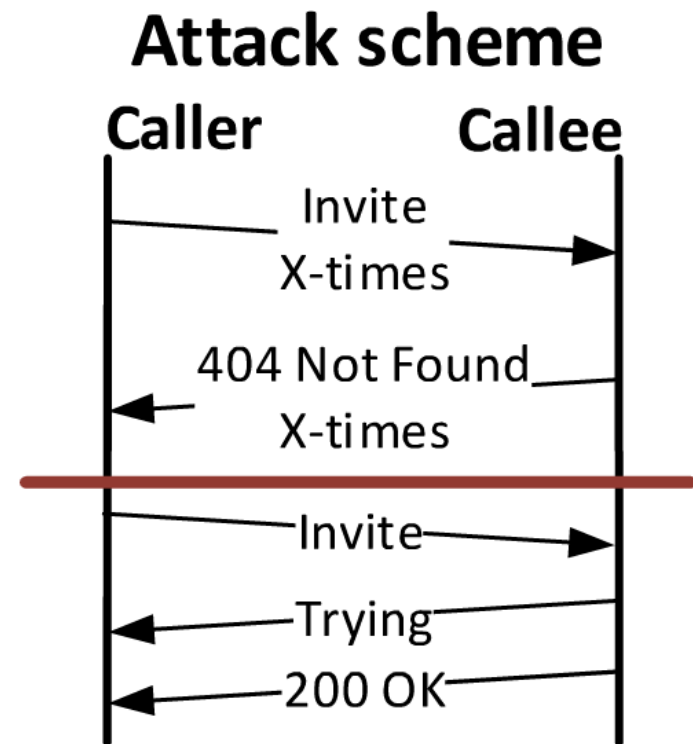
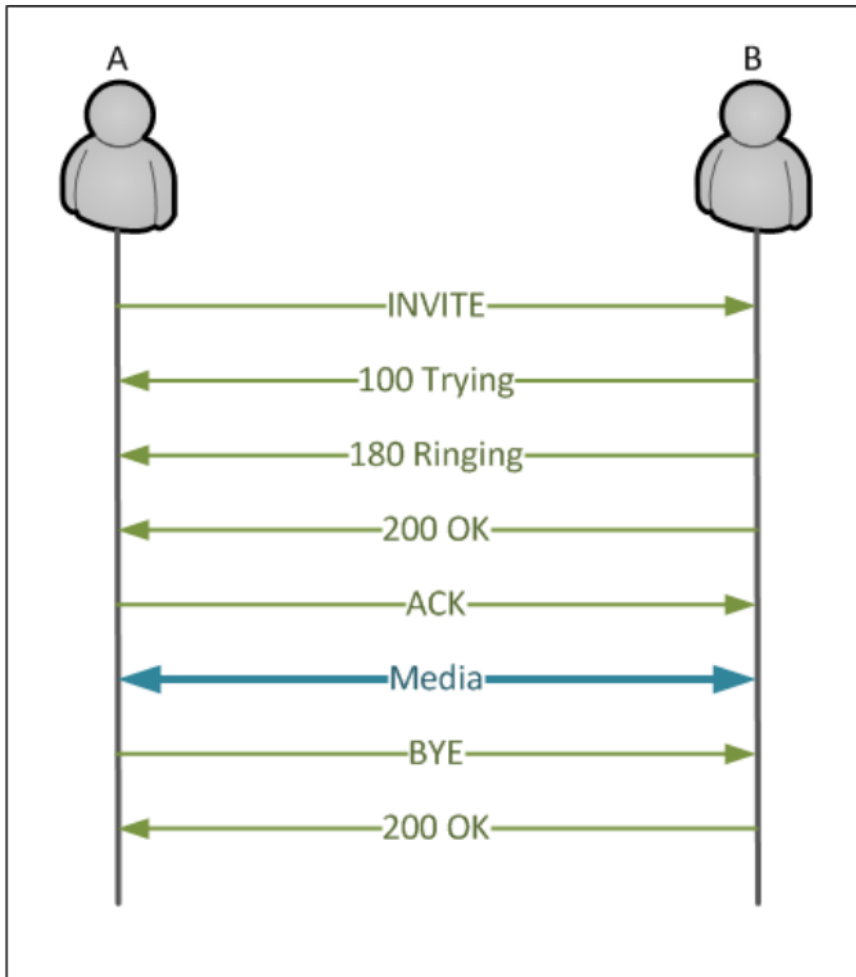
00972592577956@A.B.C.D
 000972592577956@A.B.C.D
 900972592577956@A.B.C.D
 +972592577956@A.B.C.D
 972592577956@A.B.C.D
 100972592577956@A.B.C.D
 800972592577956@A.B.C.D
 600972592577956@A.B.C.D
 700972592577956@A.B.C.D
 400972592577956@A.B.C.D
 300972592577956@A.B.C.D
 200972592577956@A.B.C.D
 500972592577956@A.B.C.D
 99900972592577956@A.B.C.D
 999900972592577956@A.B.C.D
 9999900972592577956@A.B.C.D

99999900972592577956@A.B.C.D
 999999900972592577956@A.B.C.D
 9999999900972592577956@A.B.C.D
 99999999900972592577956@A.B.C.D
 999999999900972592577956@A.B.C.D
 9000972592577956@A.B.C.D
 0972592577956@A.B.C.D
 0000972592577956@A.B.C.D
 0000000972592577956@A.B.C.D
 00000000972592577956@A.B.C.D
 000000000972592577956@A.B.C.D
 0000000000972592577956@A.B.C.D
 91000972592577956@A.B.C.D
 9900972592577956@A.B.C.D
 9100972592577956@A.B.C.D
 ...

Attack logic



SIP Call Initiation



Prefix Guessing

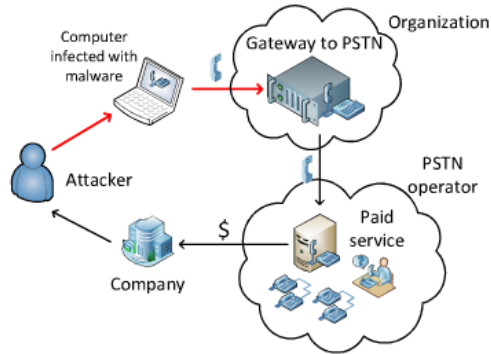
00972592577956@A.B.C.D
000972592577956@A.B.C.D
900972592577956@A.B.C.D
+972592577956@A.B.C.D
972592577956@A.B.C.D
100972592577956@A.B.C.D
800972592577956@A.B.C.D
600972592577956@A.B.C.D
700972592577956@A.B.C.D
400972592577956@A.B.C.D
300972592577956@A.B.C.D
200972592577956@A.B.C.D
500972592577956@A.B.C.D
99900972592577956@A.B.C.D
999900972592577956@A.B.C.D
9999900972592577956@A.B.C.D

999999900972592577956@A.B.C.D
9999999900972592577956@A.B.C.D
99999999900972592577956@A.B.C.D
999999999900972592577956@A.B.C.D
9999999999900972592577956@A.B.C.D
9000972592577956@A.B.C.D
0972592577956@A.B.C.D
0000972592577956@A.B.C.D
0000000972592577956@A.B.C.D
00000000972592577956@A.B.C.D
000000000972592577956@A.B.C.D
0000000000972592577956@A.B.C.D
91000972592577956@A.B.C.D
9900972592577956@A.B.C.D
9100972592577956@A.B.C.D

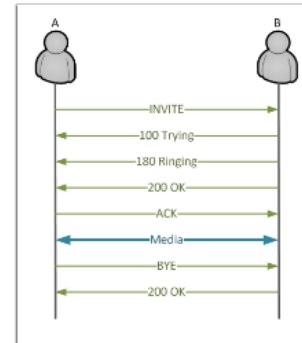
...

Attack Scheme

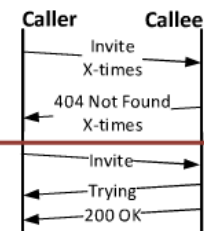
Attack logic



SIP Call Initiation



Attack scheme



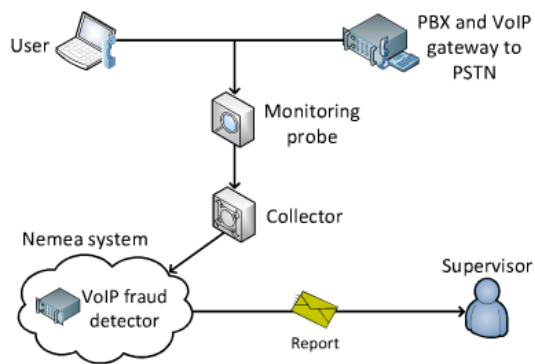
Prefix Guessing

00972592577956@A.B.C.D
 000972592577956@A.B.C.D
 900972592577956@A.B.C.D
 +972592577956@A.B.C.D
 972592577956@A.B.C.D
 100972592577956@A.B.C.D
 800972592577956@A.B.C.D
 600972592577956@A.B.C.D
 700972592577956@A.B.C.D
 400972592577956@A.B.C.D
 300972592577956@A.B.C.D
 200972592577956@A.B.C.D
 500972592577956@A.B.C.D
 99900972592577956@A.B.C.D
 999900972592577956@A.B.C.D
 9999900972592577956@A.B.C.D

99999900972592577956@A.B.C.D
 999999900972592577956@A.B.C.D
 9999999900972592577956@A.B.C.D
 99999999900972592577956@A.B.C.D
 999999999900972592577956@A.B.C.D
 9000972592577956@A.B.C.D
 0972592577956@A.B.C.D
 0000972592577956@A.B.C.D
 0000000972592577956@A.B.C.D
 00000000972592577956@A.B.C.D
 000000000972592577956@A.B.C.D
 0000000000972592577956@A.B.C.D
 91000972592577956@A.B.C.D
 9900972592577956@A.B.C.D
 9100972592577956@A.B.C.D
 ...

Detection

Architecture



Details & Parameters

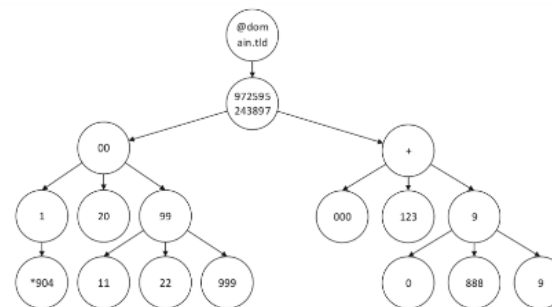
Prefix tree is generated for each unique IP address observed.

Parameters:

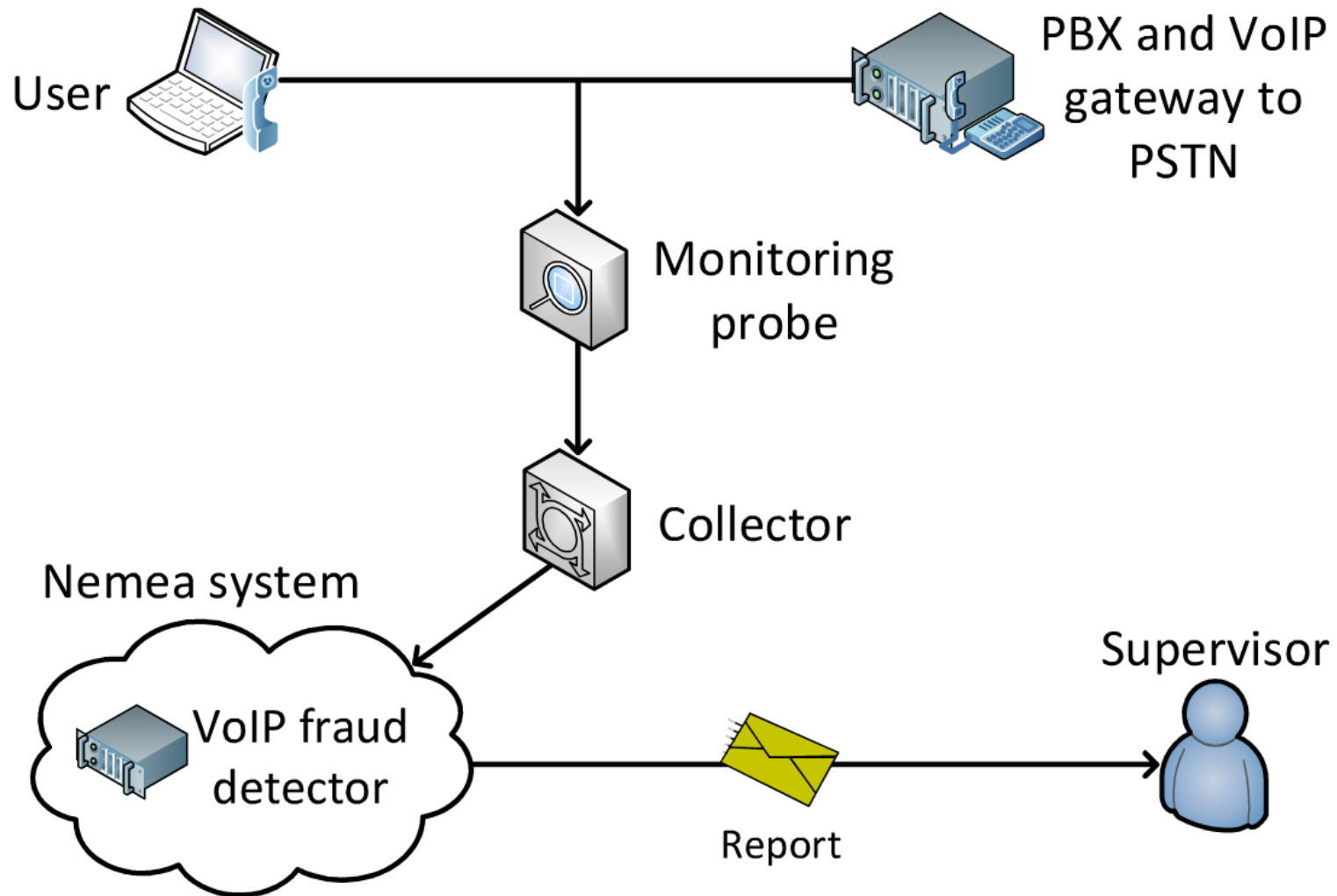
I_max - the maximal prefix length

T - the treshold on number of tested unique prefixes

Prefix Tree - data structure



Architecture



Details & Parameters

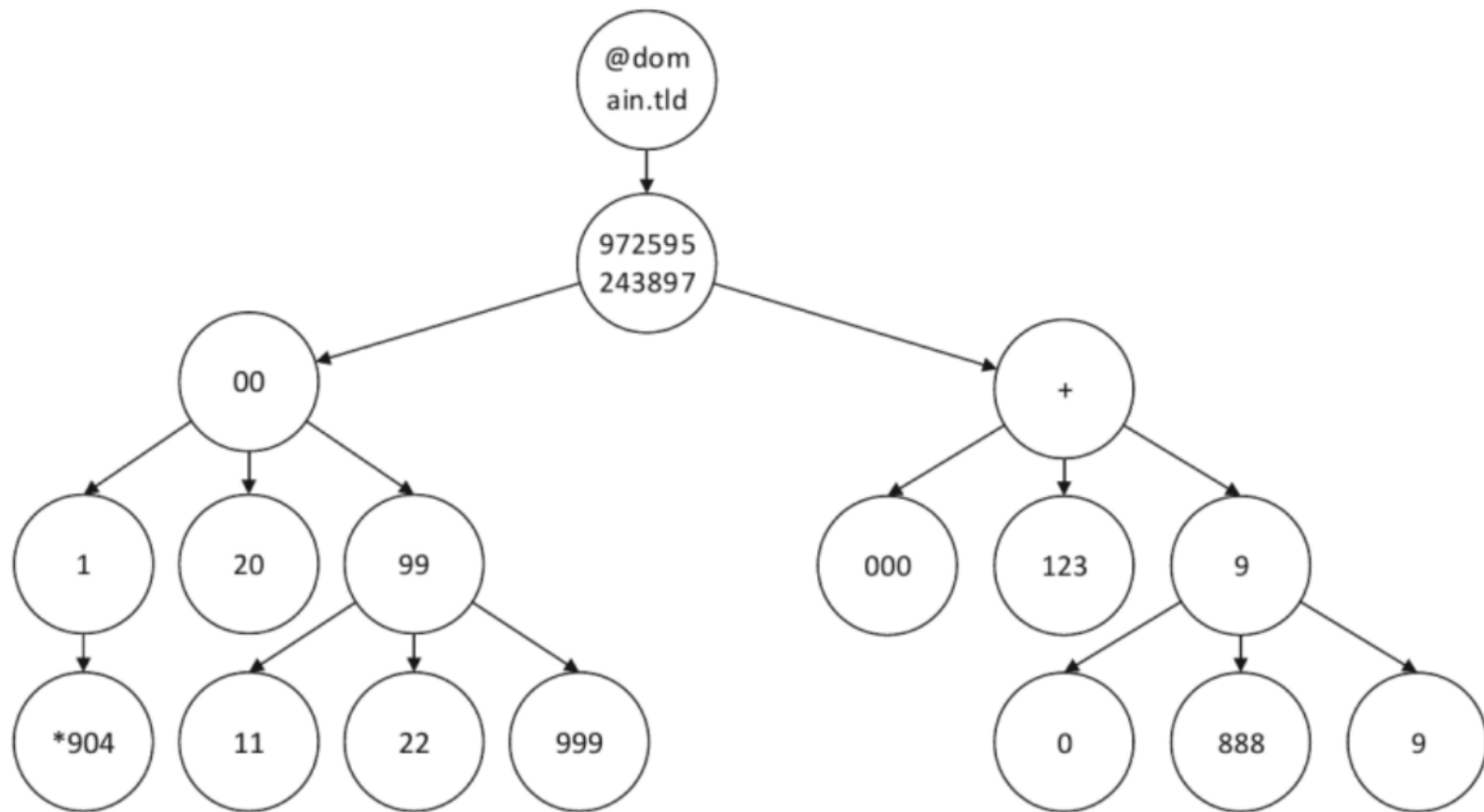
Prefix tree is generated for each unique IP address observed.

Parameters:

l_max - the maximal prefix length

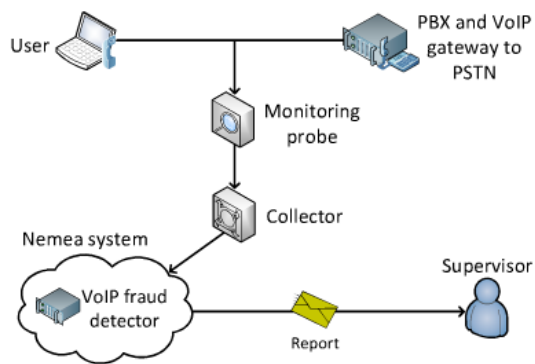
T - the threshold on number of tested unique prefixes

Prefix Tree - data structure



Detection

Architecture



Details & Parameters

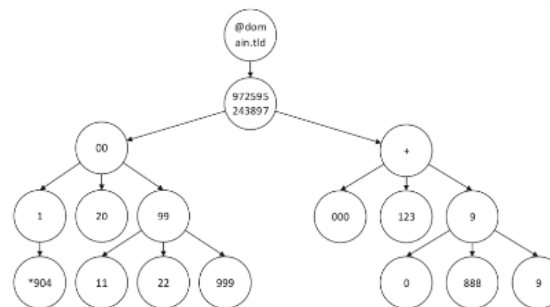
Prefix tree is generated for each unique IP address observed.

Parameters:

I_max - the maximal prefix length

T - the treshold on number of tested unique prefixes

Prefix Tree - data structure



Measurements 4

Fraud Attack 5

Visualization 6

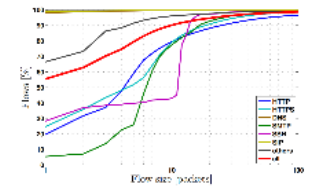
Conclusion 7

Already Tested Scenarios



- Detection of network scans
 - Communication tunnels via DNS
 - Guessing SIP dial plan
- Using SDM with Time Machine, we can get evidence and verification of detected events.

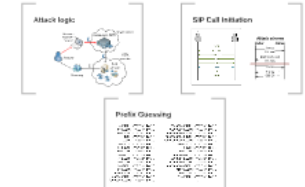
Flow Size – are n packets enough?



SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
 - A call to PSTN via the gateway require to guess a correct prefix.

Attack Scheme



Netfox Detective



Visualization



Conclusion

- We can monitor **100 Gbps**.
- Detection uses **extended flow records**
- Presented system provides:
 - **flow records**
 - **full packet capture** of detected IP
 - **history**: beginning of each flow of detected IP - **Time Machine**

Thank you!
Any questions?
@librouter
<https://www.librouter.org>

This presentation
 https://prez.com/bsen_2005/

My contact
Acknowledgment
• Tomas Cejpa
• Zdenek Ross
• Tomas Jansky
• Viktor Pus
 Jan Pleštil

Netfox Detective



WEB

HTTP
SSL/TLS

IM

XMPP
YMSG
OSCAR

Emails

IMAP
POP3
SMTP

Webmail

Gmail
Seznam.cz
Yahoo
Email.cz
MS Live
Centrum.cz
Atlas.cz
Mujmail.cz
Roundcube
Horde
Etc...

VoIP

RTP
SIP

Games

Minecraft
Warcraft

Social Networks

Facebook

Crypto currencies

BitCoin



SDM Feedback Overview

The screenshot displays the Netfox Detective interface with the following components:

- Navigation:** DETECTIVE, INVESTIGATION, VIEW, ANALYZERS, HELP
- Workspace:** Investigation explorer, Workspace manager, Investigation manager, SIP Fraud overview
- Left Panel (Investigation explorer):**
 - Captures: voip_alert_2354(12), voip_alert_2354(12)_tm
 - Logs
 - Detected Events: voip_alert_2354(12)
 - Exports: RTP (0), SIP (15), voip_alert_2354(12) [15]
- Main Content Area:**
 - Summary:** SIP fraud attack, SIP fraud analyzer, SIP fraud prefix trie
 - Invites: 16900
 - Callers: 16900
 - Callees: 16900
 - Calls per caller: 16900
 - Suspicious IPs: 93.115.28.176
 - Extraction Process Diagram:** 100GE TAP → FPGA → CPU → IPFIX → Collector → NEMEA (Detection). Includes PCAP capture to Hard drive and Delay buffer.
 - Attack Scheme:** Sequence of messages between Caller and Callee: Invite (16900), 404 Not found (16900), Invite, 100 Trying, 200 OK.
 - Progress:** Capturing progress: [Progress bar]
- Bottom Panel (Main output):**
 - 6/9/2016 11:40:24 AM Copying capture file voip_alert_2354(12)_tm
 - 6/9/2016 11:40:24 AM Copying capture file has finished voip_alert_2354(12)_tm
 - 6/9/2016 11:40:24 AM Adding capture voip_alert_2354(12)_tm
 - 6/9/2016 11:40:24 AM Capture file added voip_alert_2354(12)_tm
 - 6/9/2016 11:40:25 AM Starting export application data 15 conversations to group "voip_alert_2354(12)"
 - 6/9/2016 11:40:26 AM Application data export finished Target group "voip_alert_2354(12)"

Filtration of Intercepted Events

The screenshot displays the Netfox Detective interface. The main window is titled "SIP Fraud overview" and shows a table of intercepted SIP events. The table has columns for From, To, Contact, Method, StatusInfo, and StatusCode. A filter dialog is open on the right, allowing selection of status codes (100, 180, 200) and filtering rows based on values.

Workspace manager: Investigation manager SIP Fraud overview

SIP fraud attack SIP fraud analyzer SIP fraud prefix trie

Shown item: 68

Drag a column header and drop it here to group by that column

From	To	Contact	Method	StatusInfo	StatusCode
<sip:48422725851@31.186.86.14>	<sip:426326629@31.186.86.14>	<sip:48422725851@212.51.198.238:20000>	BYE		
<sip:48422725851@31.186.86.14>	<sip:426326629@31.186.86.14>	<sip:48422725851@212.51.198.238:20000>	BYE		
<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@212.51.198.238:20000>	REGISTER		
<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@212.51.198.238:20000>	REGISTER		
<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@212.51.198.238:20000>	REGISTER		
<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@212.51.198.238:20000>	REGISTER		
<sip:48422725870@31.186.86.14>	<sip:422565152@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	INVITE		
<sip:48422725870@31.186.86.14>	<sip:422565152@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	INVITE		
<sip:48422725870@31.186.86.14>	<sip:422565152@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	ACK		
<sip:48422725870@31.186.86.14>	<sip:422565152@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	ACK		
<sip:48422725870@31.186.86.14>	<sip:422565152@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	INVITE		
<sip:48422725870@31.186.86.14>	<sip:422565152@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	INVITE		
<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@212.51.198.238:20000>	REGISTER		
<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@212.51.198.238:20000>	REGISTER		
<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@31.186.86.14>	<sip:umed_trunk3@212.51.198.238:20000>	REGISTER		
<sip:48422725870@31.186.86.14>	<sip:422565130@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	ACK		
<sip:48422725870@31.186.86.14>	<sip:422565130@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	ACK		
<sip:48422725870@31.186.86.14>	<sip:422565130@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	CANCEL		
<sip:48422725870@31.186.86.14>	<sip:422565130@31.186.86.14>	<sip:48422725870@212.51.198.238:20000>	CANCEL		
<sin:48422725870@31.186.86.14>	<sin:422565130@31.186.86.14>	<sin:48422725870@212.51.198.238:20000>	INVITE		

Filter dialog options:

- Select All
- [null]
- 100
- 180
- 200

Show rows with value that

Is equal to [dropdown]

And [dropdown]

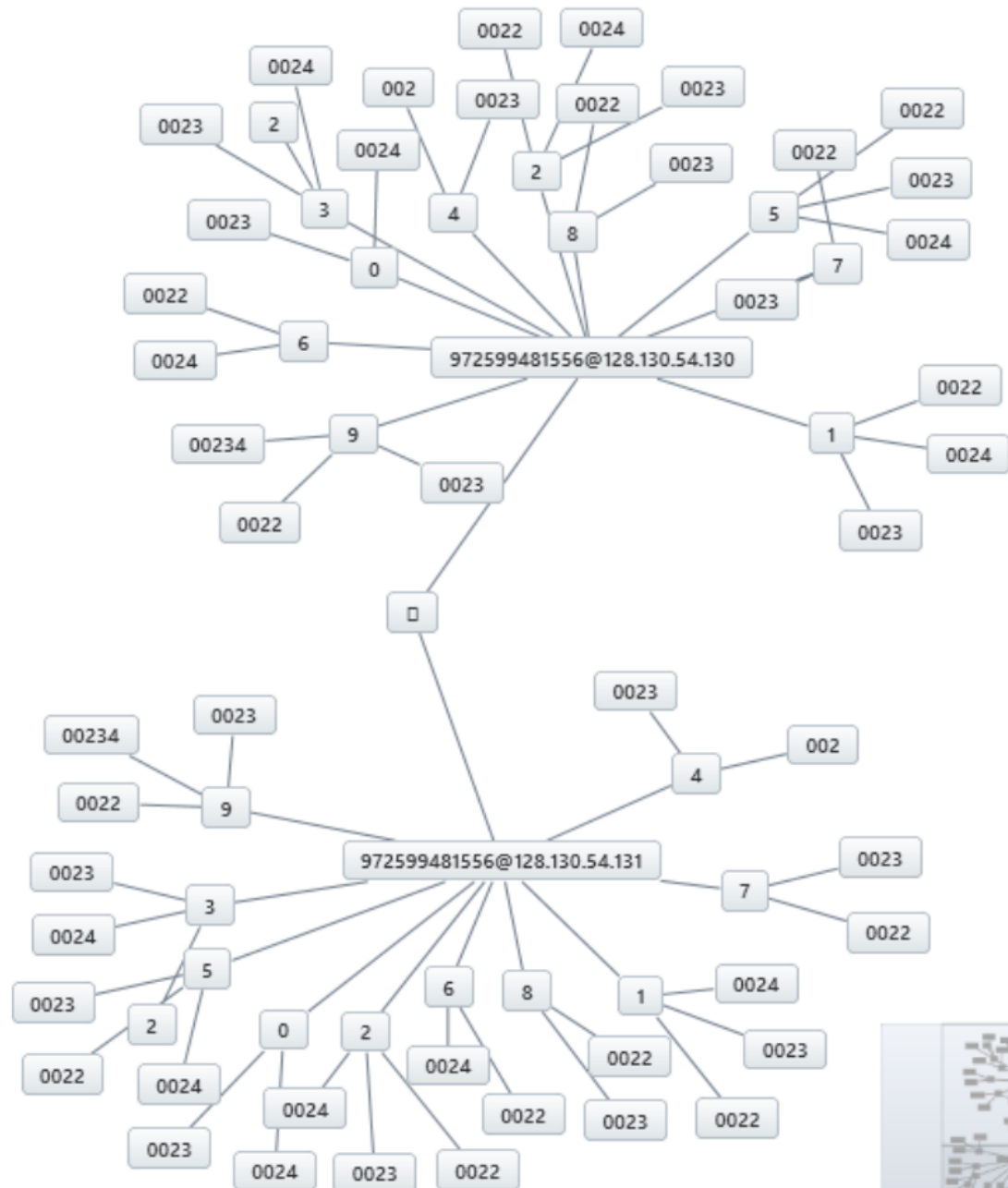
Is equal to [dropdown]

Filter Clear Filter

Main output

Running tasks : 0

SIP Prefix Tree



Captured Alert Details

Netfox Detective

DETECTIVE INVESTIGATION VIEW ANALYZERS HELP

Investigation explorer Workspace manager Investigation manager SIP Fraud overview **Conversations detail** Conversations overview

Conversations detail

Statistics

Conversations:	14	Total Frames:	0	Period:	4/28/2016 7:33:30 AM - 4/28/2016 7:36:34 AM
Recognized Protocols	2	Unique Hosts:	2		
Up Flow Frames:	124	Up Flow Bytes:	49040	Up Flow TCP Lost Bytes:	0
Down Flow Frames:	31275	Down Flow Bytes:	5379300	Down Flow TCP Lost Bytes:	0
Total Flow Frames:	31399	Total Flow Bytes:	5428340	Total TCP Lost Bytes:	0
IPv4 Conversations:	14	TCP Conversations:	0	Total TCP Bytes:	0
IPv6 Conversations:	0	UDP Conversations:	14	Total Lost (TCP) %:	0

[Get details](#) [Show VoIP over](#)

Structure

Application protocols Transport protocols Timeline Hosts Traffic Conversations

Protocol	Total Bytes	%
multiple-protocols	2739464	50.46596
rtp	2688876	49.53404

Main output

Running tasks : 0

Packet Sequence Pattern

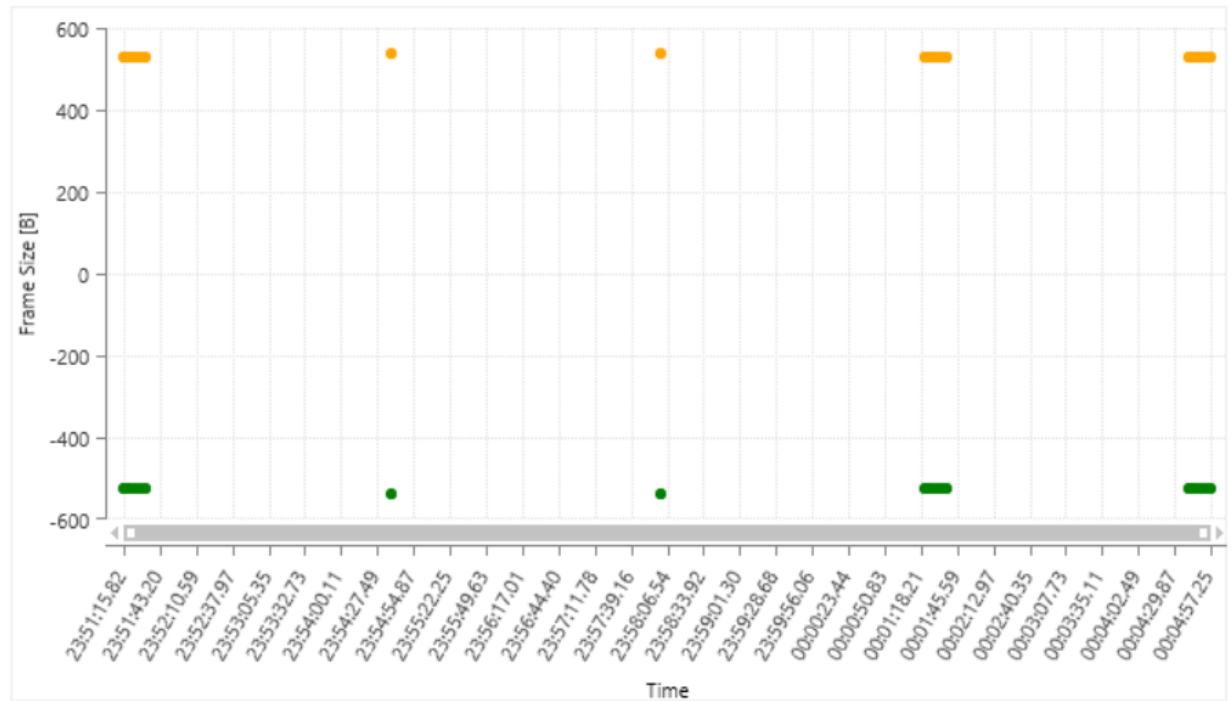
↔ 212.51.218.242:0 - 185.40.4.95:0 [conversation taxonomy](#) [reassembled stream](#)

Transport Layer:	IP	Up Flow Packets/Bytes:	0 / 0	Start:	1/1/0001 12:00:00 AM
Application Layer:		Down Flow Packets/Bytes:	46 / 22358	End:	1/1/0001 12:00:00 AM
Client Host Address:	212.51.218.242:0	Server Host Address:	185.40.4.95:0		
Malformed Frames:	0	Missing Frames:			
Extracted Bytes:		Missing Bytes:	(0 %)		

[Advanced protocols recognition](#)

Packets Sequence Chart Frames list Data quality Exports

PACKET NUMBER: TIME: SOURCE: TARGET:



Packet Analysis

The screenshot displays the Netfox Detective interface for packet analysis. The main window shows the details of Frame No. 5, which is a User Datagram Protocol (UDP) packet containing SIP application data. The structure pane on the left lists the protocol layers: Ethernet, Internet Protocol, User Datagram Protocol, and UDP Application data. The raw content pane on the right shows the hexadecimal and ASCII representation of the packet payload, which is a SIP INVITE message.

Structure

- Ethernet = smac: 88E0F3622FC0, dmac: 0026982CF4C8
- Internet Protocol = sa: 148.81.190.140, da: 185.40.4.95
- User Datagram Protocol = sp: 5060, dp: 5074, len: 579
 - Source Port = 5060
 - Destination Port = 5074
 - Length = 579
 - Checksum = 21989
- UDP Application data = Length : 571B
 - ASCII Data = SIP/2.0 401 Unauthorized
 - Via: SIP/2.0/UDP 185.40.4.95:5074;branch=z9hG4bK-de2f90bcd49c6a34c1e79058988b2148;received=185.40.4.95;rport=5074
 - From: 8888 <sip:8888@148.81.190.140>;tag=d780d7e8
 - To: 1100972595746420 <sip:1100972595746420@148.81.190.140>;tag=as31668c90
 - Call-ID: de2f90bcd49c6a34c1e79058988b2148
 - CSeq: 1 INVITE
 - Server: Asterisk PBX 11.17.1
 - Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
 - Supported: replaces, timer
 - WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="359bc469"
 - Content-Length: 0

Raw content

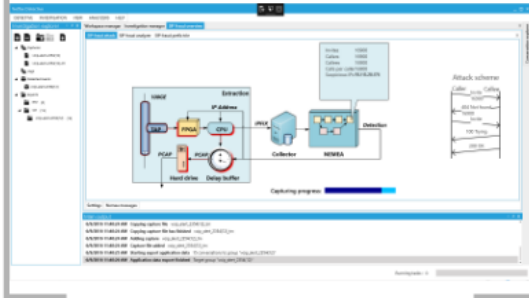
Offset	00	01	02	03	04	05	06	07	ASCII
0000	00	26	98	2C	F4	C8	88	E0	.6.....
0008	F3	62	2F	C0	08	00	45	00	.b/...E.
0010	02	57	38	20	00	00	3C	11	.W8...<.
0018	34	11	94	51	BE	8C	B9	28	4..Q...{
0020	04	5F	13	C4	13	D2	02	43	_.C
0028	55	E5	53	49	50	2F	32	2E	U.SIP/2.
0030	30	20	34	30	31	20	55	6E	0.401.Un
0038	61	75	74	68	6F	72	69	7A	authoriz
0040	65	64	0D	0A	56	69	61	3A	ed..Via:
0048	20	53	49	50	2F	32	2E	30	.SIP/2.0
0050	2F	55	44	50	20	31	38	35	/UDP.185
0058	2E	34	30	2E	34	2E	39	35	.40.4.95
0060	3A	35	30	37	34	3B	62	72	:5074;br
0068	61	6E	63	68	3D	7A	39	68	anch=z9h
0070	47	34	62	4B	2D	64	65	32	G4bK-de2
0078	66	39	30	62	63	64	34	39	f90bcd49
0080	63	36	61	33	34	63	31	65	c6a34c1e
0088	37	39	30	35	38	39	38	38	79058988
0090	62	32	31	34	38	3B	72	65	b2148;re
0098	63	65	69	76	65	64	3D	31	ceived=1
00A0	38	35	2E	34	30	2E	34	2E	85.40.4.
00A8	39	35	3B	72	70	6F	72	74	95;rport
00B0	3D	35	30	37	34	0D	0A	46	=5074..F
00B8	72	6F	6D	3A	20	38	38	38	rom:.888
00C0	38	3C	73	69	70	3A	38	38	8<sip:88
00C8	38	38	40	31	34	38	2F	38	888148 8

Main output

Running tasks : 0

Visualization

SDM Feedback Overview



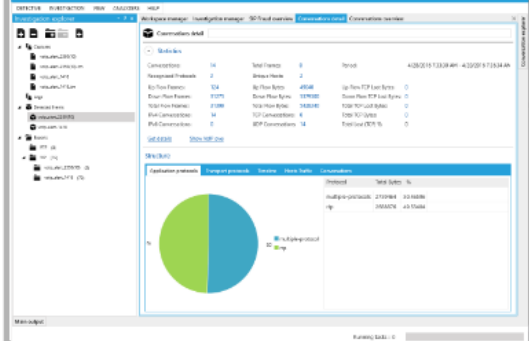
Filtration of Intercepted Events

From	To	Content	Interval	Substrate	Link/Conn. ID
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2
10.0.0.1	10.0.0.2	HTTP/1.1 200 OK	10.0.0.1:80-10.0.0.2:80	10.0.0.1	10.0.0.1-10.0.0.2

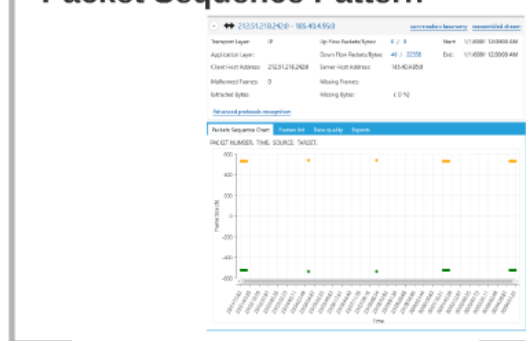
SIP Prefix Tree



Captured Alert Details



Packet Sequence Pattern



Packet Analysis

Field	Value
Length	100
Protocol	TCP
Source	10.0.0.1
Destination	10.0.0.2
Source Port	80
Destination Port	80
Sequence	1000000000
Window	65535
Flags	ACK, FIN, RST, SYN
Checksum	0x12345678
Options	None

Fraud Attack 5

Visualization 6

Conclusion 7

SIP Fraud Attack

- Gateway should not allow forwarding calls to PSTN without proper authentication.
- Many gateways have very poor security measures (if any at all)
 - A call to PSTN via the gateway require to guess a correct prefix.

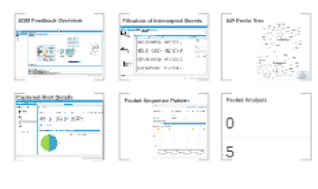
Attack Scheme



Netfox Detective



Visualization



Conclusion

- We can monitor **100 Gbps**.
- Detection uses *extended flow records*
- Presented system provides:
 - *flow records*
 - *full packet capture* of detected IP
 - *history*: beginning of each flow of detected IP - **Time Machine**

20
1996-2016
CESNET

Thank you!
Any questions?
@liberouter
<https://www.liberouter.org>

This presentation

Acknowledgment

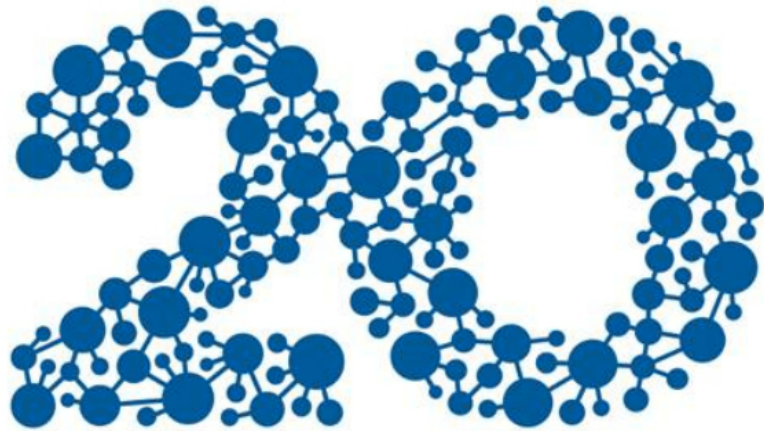
- Tomas Cejka
- Zdenek Rosa
- Tomas Jansky
- Viktor Pus

My contact

Jan Pluskal

Conclusion

- We can monitor **100 Gbps**.
- Detection uses *extended flow records*
- Presented system provides:
 - *flow records*
 - *full packet capture* of detected IP
 - *history*: beginning of each flow of detected IP - **Time Machine**



1996–2016

CESNET

© 2016 CESNET, s.r.o.
Všechna práva vyhrazena.
Tento dokument je chráněn autorským právem.
Žádná část tohoto dokumentu nesmí být reprodukována, šířena, rozesílána nebo publikována bez předchozího písemného souhlasu CESNET, s.r.o.
CESNET, s.r.o. je registrovaná společnost s ručením omezeným v ČR.
IČO: 25227123, DIČ: CZ25227123
Sídlo: Březnická 7, 160 00 Praha 6, Česká republika
Telefon: +420 224 312 222, Fax: +420 224 312 223
E-mail: info@cesnet.cz, www.cesnet.cz

Thank you! Any questions?

@liberouter 

<https://www.liberouter.org>

This presentation



Acknowledgment

- Tomas Cejka
- Zdenek Rosa
- Tomas Jansky
- Viktor Pus

https://prezi.com/rbwm_9todtb7

My contact



Jan Pluskal

Bibliography

- **Benáček, P., Blažek, R.B., Čejka, T., Kubátová, H.:** "*Change-Point Detection Method on 100 Gb/s Ethernet Interface*", ACM/IEEE Symposium on Architectures for Networking and Communications Systems 2014 (ANCS2014), Marina del Rey, CA, USA, 2014
- **Čejka, T., Kekely, L., Benáček, P., Blažek, R.B., Kubátová, H.:** "*FPGA Accelerated Change-Point Detection Method for 100 Gb/s Networks*", Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS), 2014 (will be published in Oct. 2014)
- **Čejka, T., Rosa, Z., Kubátová, H.:** "*Stream-wise Detection of Surreptitious Traffic over DNS*", 19th IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (IEEE CAMAD 2014), Athens, Greece, 2014 (will be published in Dec. 2014)
- Lots of Google indexed images has been used for this presentation...credit goes to their creators!