Firewall Testing

Dr. E. Eugene Schultz, Prof. Sonia Fahmy, Florian Kerschbaum, Manu Pathak, Hao Wu, Mike Frantzen, Eric Hlutke, Seny Kamara

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.

Motivation

- Current firewall testing based only on known vulnerabilities
- Firewall models lack detailed descriptions
- No prediction about potential vulnerabilities

Model

- Based on a data flow model
- Details firewall functionality
- Flexible to model different implementations
- Provides basis for analysis and prediction

Vulnerability Classification

- Analysis of known vulnerabilities
- Categorization into software vulnerabilities: Ivan Krsul’s Ph.D. thesis
- Mapping to data flow model

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.

Vulnerability Categories

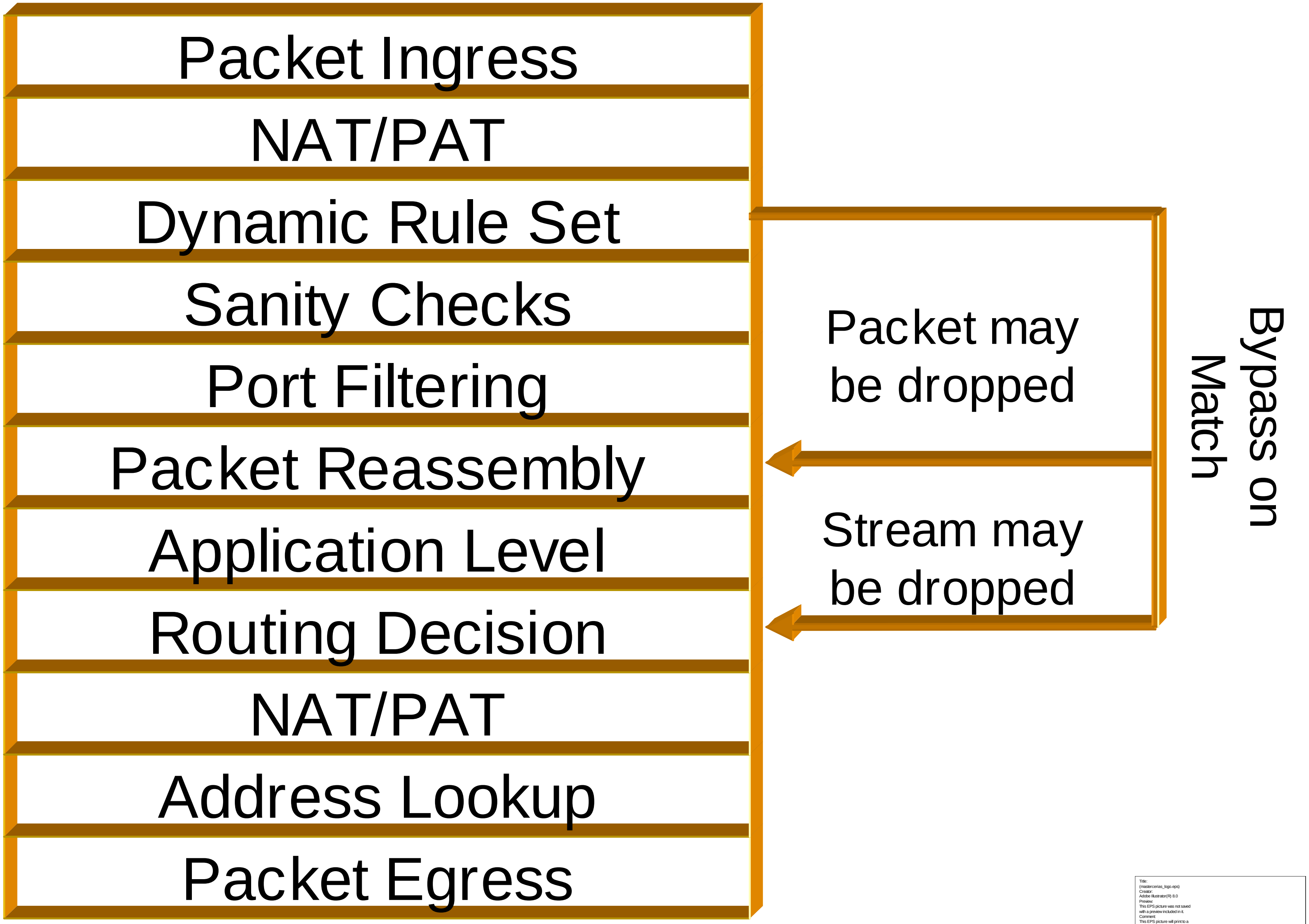
- memavail: Assumes that enough memory is available
- netdata: Assumes that network data is valid and bounded
- reassembly: Assumes that reassembly does not change data
- insufverif: Assumes that a set of verifications is sufficient
- trustnetobj: Assumes that network data can be trusted
- criticalsect: Assumes protection of critical section is sufficient

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.

Future Work

- continue vulnerability classification
- predict vulnerabilities based on analysis
- test predicted vulnerabilities
- improve firewall model for possible attacks

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.



Packet Ingress

NAT/PAT

Dynamic Rule Set

Sanity Checks

Port Filtering

Packet Reassembly

Application Level

Routing Decision

NAT/PAT

Address Lookup

Packet Egress

Packet may
be dropped

Stream may
be dropped

Bypass on
Match

Title:
(mastercerias_logo.eps)
Creator:
Adobe Illustrator(R) 8.0
Preview:
This EPS picture was not saved
with a preview included in it.
Comment:
This EPS picture will print to a
PostScript printer, but not to
other types of printers.

Data Model Software Flaw	NAT/PAT	Dynamic Rule Set	Sanity Checks	Port Filtering	Packet Reassembly	Application Level
memavail		FW-1 ACK Saturation				
netdata					PIX Frag. DOS	FW-1 Script Tag
reassembly				Fragmented SYN		FTP PASV
insufverif			Raptor ICMP			
trustnetobj				Int. address forwarded		
criticalsect	FW-1 NAT					