Backscatter

A viable tool for threat of the past and today

Barry Raveendran Greene

March 04, 2009

bgreene@senki.org

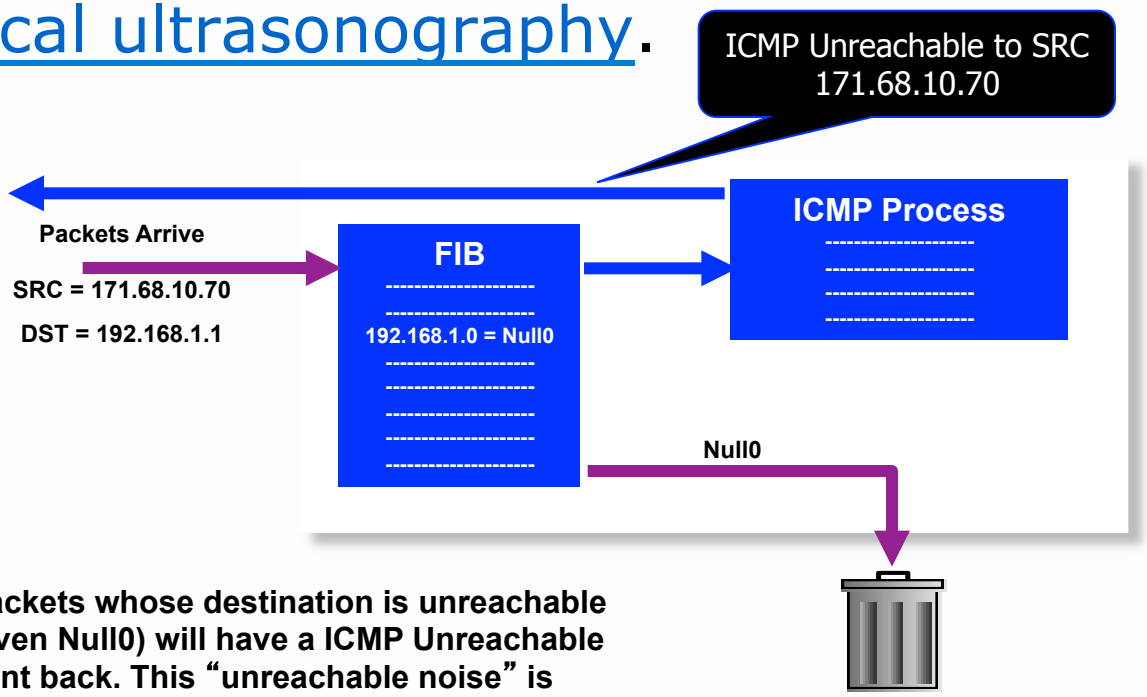
Agenda

- Backscatter: What is it?
- VzB's use with the Backscatter Traceback Technique.
- Using Backscatter for the Kamiski DNS Attack

What is *Backscatter*

What is Backscatter?

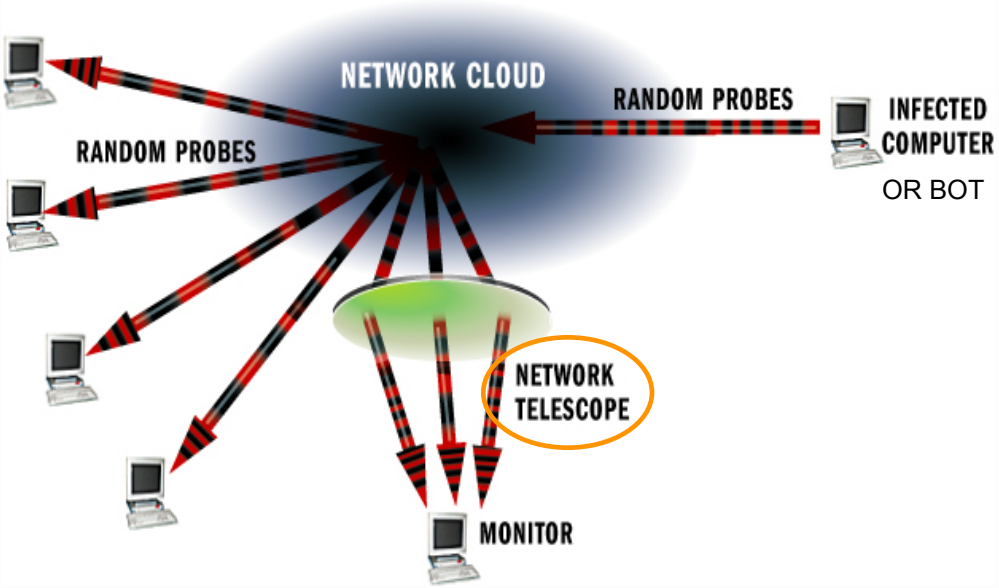
- Backscatter is the reflection of waves, particles, or signals back to the direction they came from. The term is used in astronomy and several fields of physics, as well as in photography and medical ultrasonography.



Packets whose destination is unreachable (even Null0) will have a ICMP Unreachable sent back. This "unreachable noise" is backscatter.

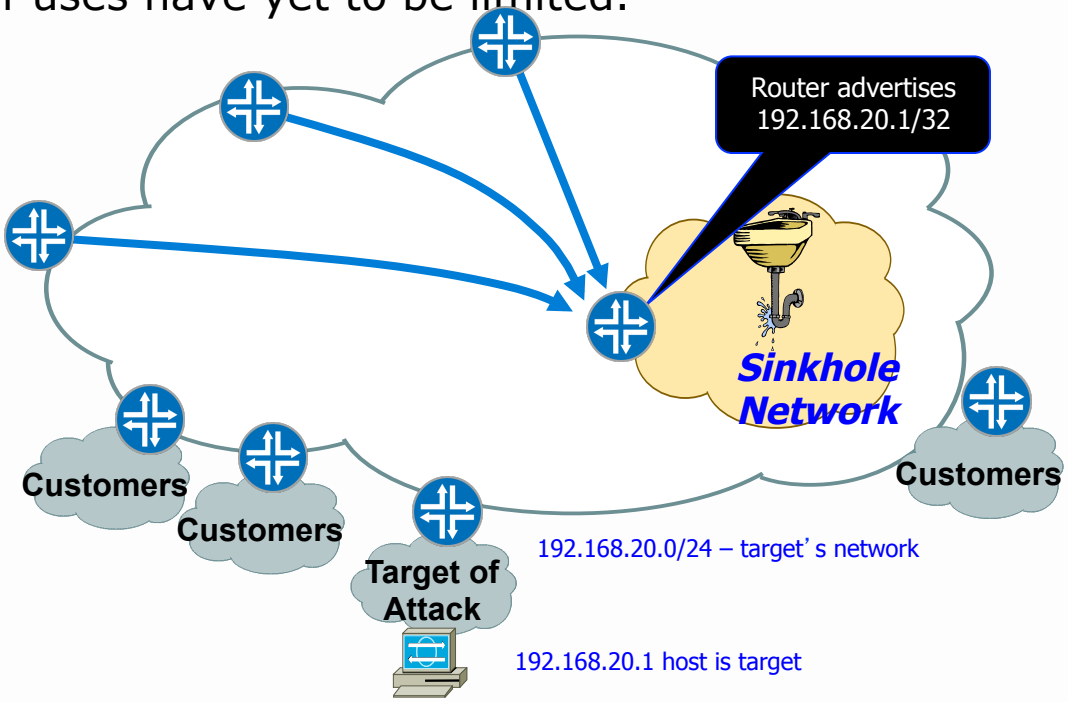
What is Backscatter?

- Backscatter (or background radiation) will collect from a variety of traffic:
  - Scans on the Network
  - TCP Response Traffic (SYN+ACK from a spoof)
  - Man in the Middle Attempts



Sinkhole Routers/Networks

- A Sink Hole Network is a section of an SP's network designed to withstand a direct DOS/DDOS attack and perform a wide variety of security task.
- It builds on the strengths of an SP – routing traffic – allowing an SP to use its strength to watch for attacks, classify them, and mitigate threats to their network.
- Sink Hole networks are a low cost, flexible, and broad security tool whose range of uses have yet to be limited.



Backscatter Traceback

Backscatter Traceback

- Created by Chris Morrow and Brian Gemberling @ UUNET as a means of finding the entry point of a spoofed DOS/DDOS.
  - http://www.secsup.org/Tracking/
- Combines the Sink Hole router, Backscatter Effects of Spoofed DOS/DDOS attacks, and remote triggered Black Hole Filtering to create a traceback system that provides a result within 10 minutes.
- Breakthrough in the ability to work DDOS incidents on the Internet.
- "Leadership through Example" which resuscitated techniques like dRTBH and Sink Holes – which are the mainstay tools in today's network defense.

NANOG 23 Tutorial

- Tutorial: ISP Security - Real World Techniques II
- Abstract: The Internet is a battleground, with ISP's and their customers right in the middle of the line of fire. What ISPs need to protect themselves are tools and techniques that work in the line of fire, i.e., tools that fight DoS attacks and provide something other than a busy signal on the customer service line. This tutorial will walk ISPs through the five stages of working an attack: preparation, identification, classification, traceback, and reaction. Focus will be placed on techniques that work - with specific vendor features left for other sessions. All the techniques have been validated and proven to be operationally deployable and workable under conditions of network stress. The key objective is to empower other ISPs to deploy these vendor-independent techniques, which will provide a foundation for inter-NOC cooperation to trace back the attacks to their source.
- http://www.nanog.org/meetings/nanog23/abstracts.php?pt=OTQwJm5hbm9nMjM=&nm=nanog23

- Contains the PPT, PDF, and Real Broadcast of the Tutorial

Backscatter Today: Kaminski DNS Poison Attack

Chain of Victimization

Target

Users

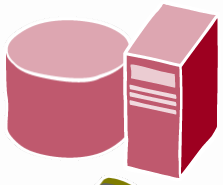
Means to a Target

Recursive DNS Resolver

Operator

Target

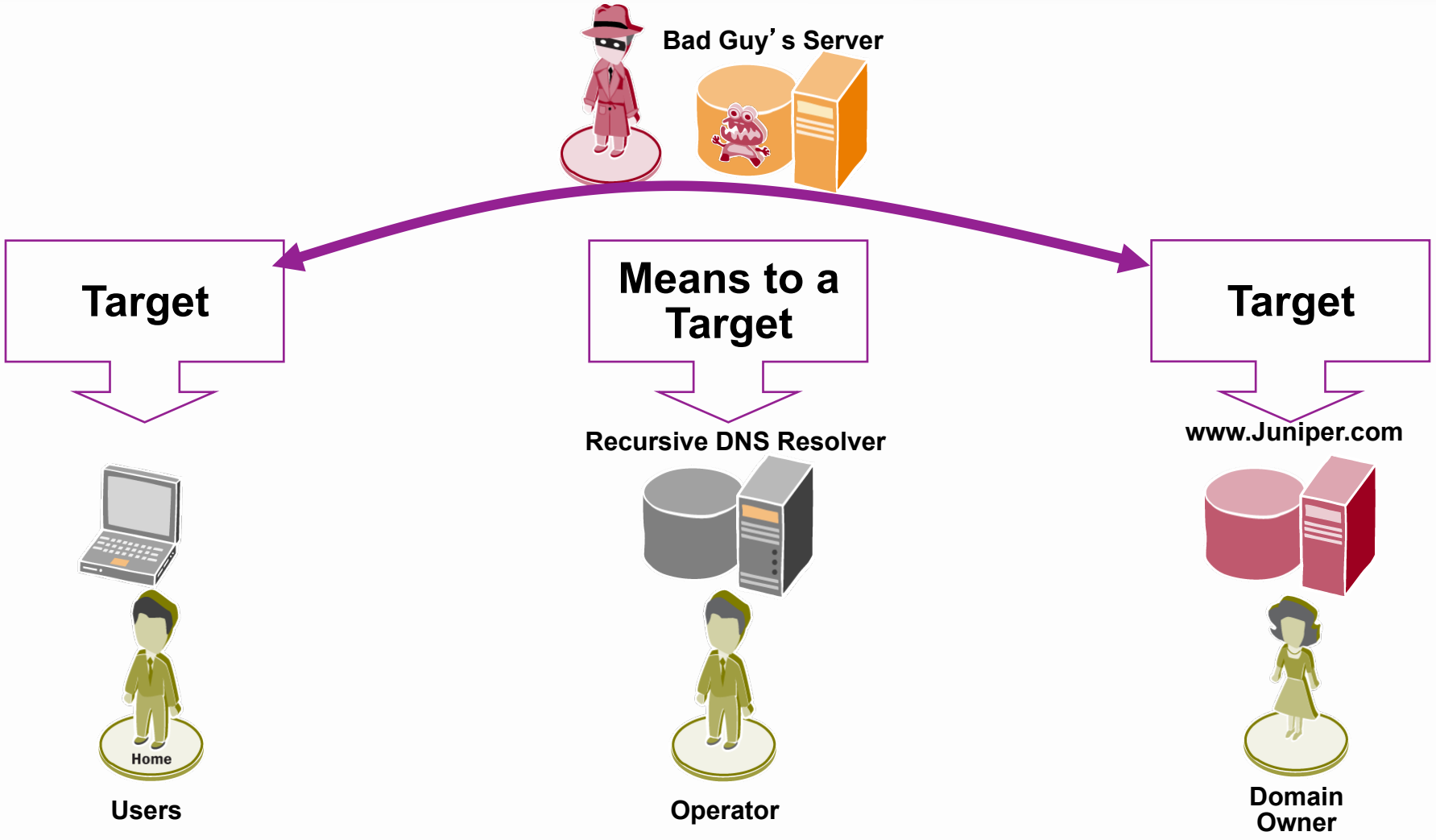
www.example.com



Domain Owner

Focus of the Industry

Threat to Juniper



The Attack Vector Results in Backscatter

Spoof
ns.example.com

Recursive DNS Resolver

ns.example.com

Users

Operator

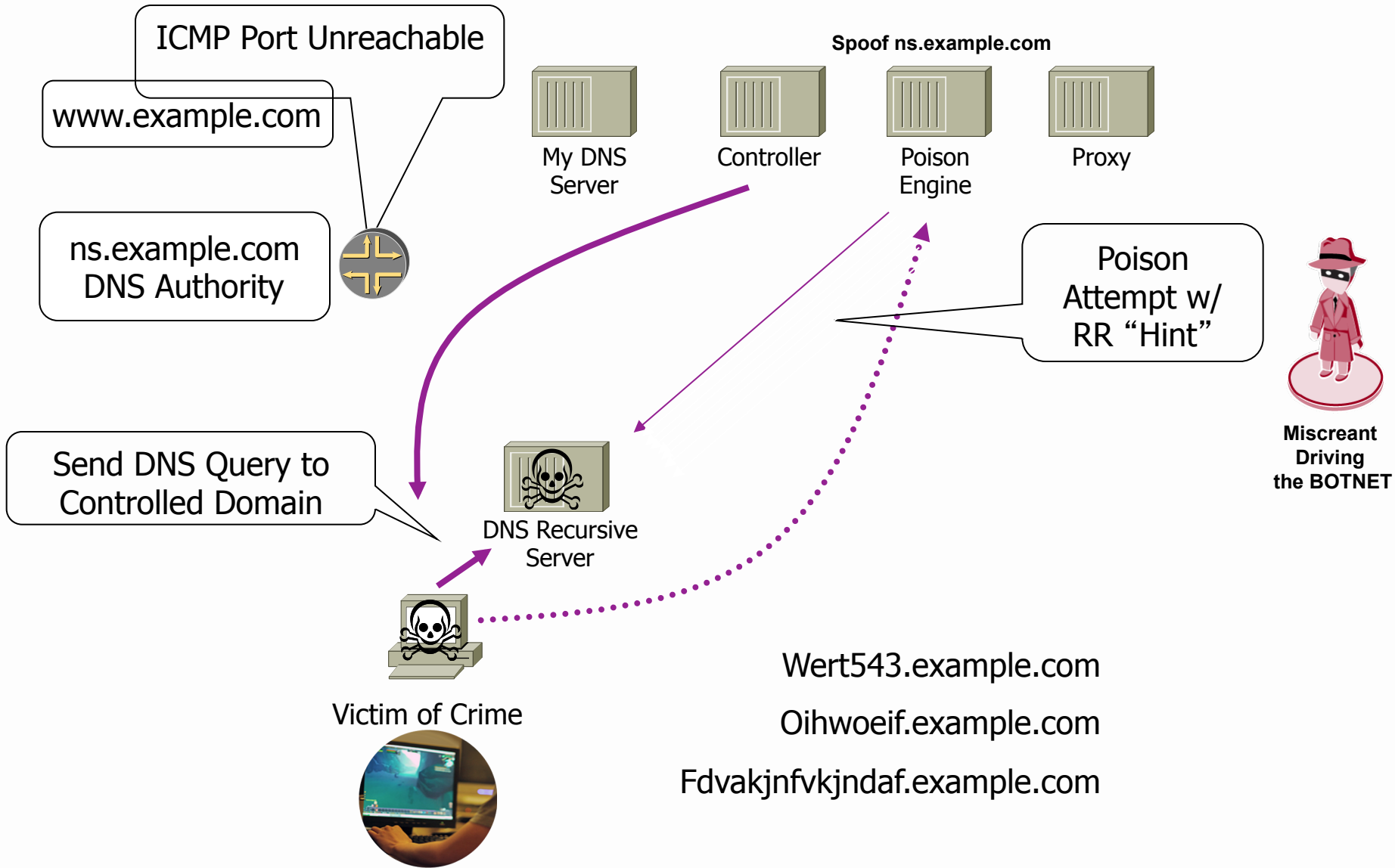
ICMP Port Unreachables arrive at ns.example.com

Domain Owner

Actions

- Monitor ICMP Port Unreachable Backscatter on all our DNS Authority Server.
  - JUNOS Filter to syslog and SNMP Trap
  - STRM/jFlow on the routers
- Get ICMP Port Unreachable Backscatter alert from all our DNS Contracted Partners.

Backscatter – ICMP Port Unreachable



ICMP Unreachable & DNS

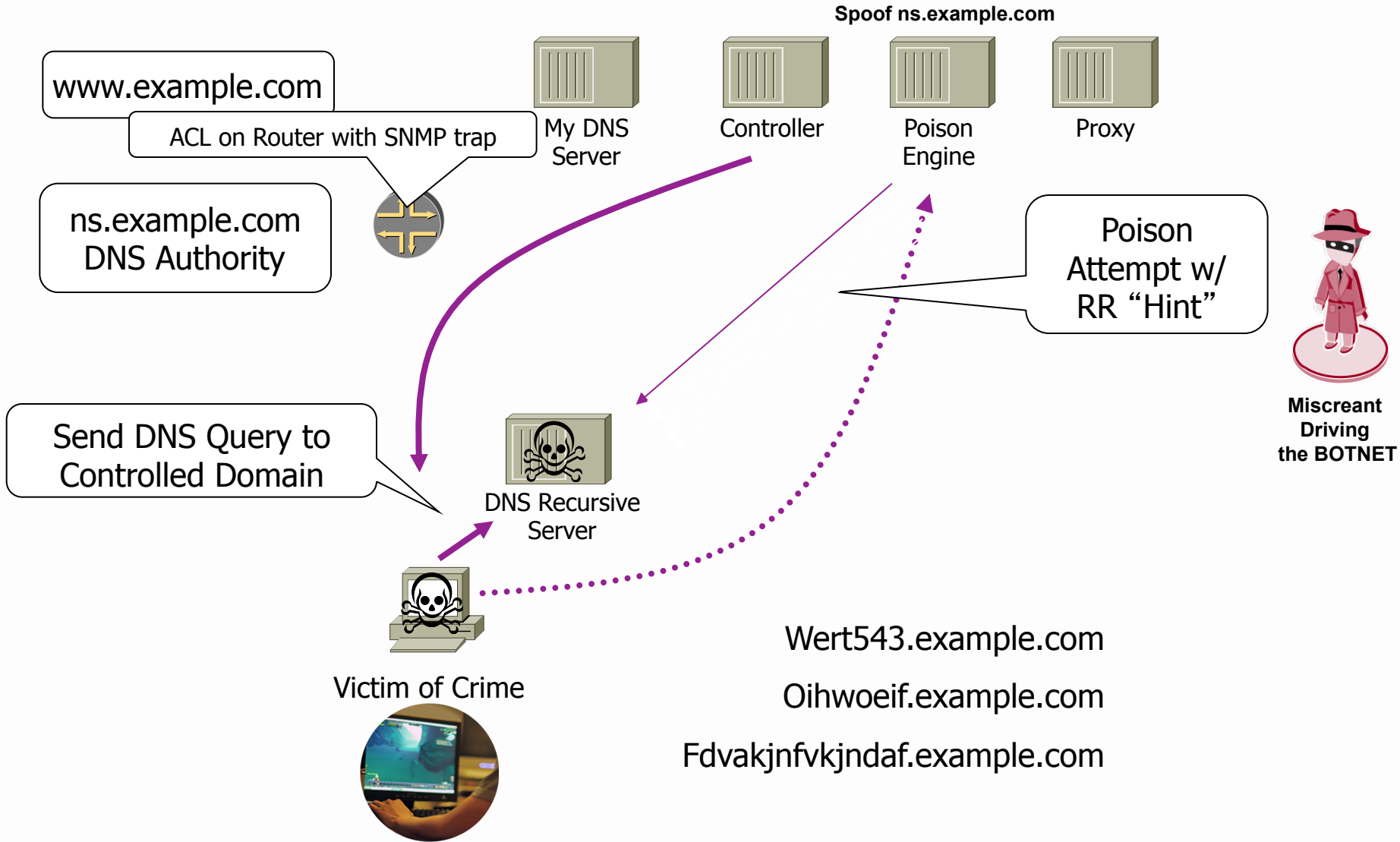
- ICMP Unreachable – specific port unreachable – are not normal packets which arrive at:
  - DNS Masters
  - DNS Slaves
  - DNS Split-Horizon Authoritative Servers
- Live Observation
  - Lauching the attack results packets arriving on closed ports of the recursive DNS Server.
  - This send ICMP Port Unreachable to the source packet – which is the DNS Authority being spoofed.

ICMP Port Unreachable

- This will tell you that someone somewhere is poising somewhere so that they can be a man in the middle between you and your customer!

- How to monitor:
  - Classification ACLs (match ingress on ICMP port unreachable)
  - Netflow
  - IDP
  - NetScreen (any matches on ICMP Unreachable

ACLs – How?

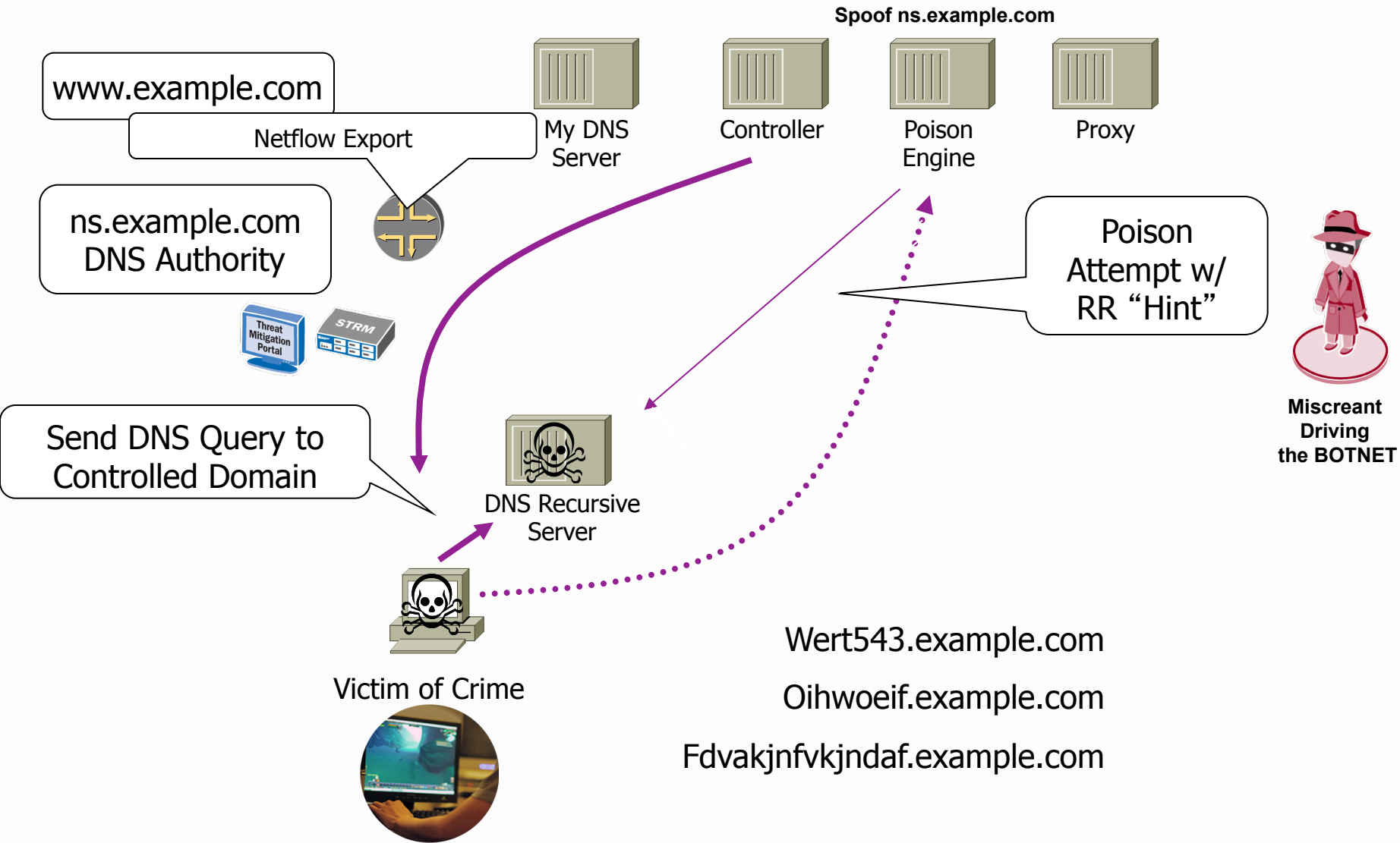

Spoof ns.example.com
www.example.com
ACL on Router with SNMP trap
My DNS Server
Controller
Poison Engine
Proxy
ns.example.com DNS Authority
Poison Attempt w/ RR "Hint"
Miscreant Driving the BOTNET
Send DNS Query to Controlled Domain
DNS Recursive Server
Victim of Crime
Wert543.example.com
Oihwoeif.example.com
Fdvakjnfvkjndaf.example.com

JUNOS Example

- JUNOS can syslog and a syslog watcher could then alert the operator. The example below also adds a counter and discards (rather than rejects) the packets.

```
ps@phillip> show configuration firewall
family inet {
     filter discard-icmp-unreachables {
         term discard-traffic {
             from {
                 protocol icmp;
                 icmp-code port-unreachable;
             }
             then {
                 count icmp-port-unreachables;
                 syslog;
                 discard;
             }
         }
         term explicit-accept {
             then accept;
         }
     }
}
```

Netflow


Spoof ns.example.com
www.example.com
Netflow Export
My DNS Server
Controller
Poison Engine
Proxy
ns.example.com DNS Authority
Threat Mitigation Portal
STRM
Poison Attempt w/ RR "Hint"
Miscreant Driving the BOTNET
Send DNS Query to Controlled Domain
DNS Recursive Server
Victim of Crime
Wert543.example.com
Oihwoeif.example.com
Fdvakjnfvkjndaf.example.com