SÉCURITÉ.ORG

Building an Early Warning System in a Service Provider Network

Nicolas FISCHBACH
Senior Manager, IP Engineering/Security - COLT Telecom
nico@securite.org - http://www.securite.org/nico/

version 1.1

COLT

we make business straight.forward

Agenda

- » **What are ISPs / NSPs looking for ?**
- » **Honeynet-like sensors**
  - > Routers as honeypots
  - > DDoS detection with honeybots
  - > Traffic diversion to honeyfarms
- » **Other information sources**
  - > System data
  - > Security data
  - > Network data
- » **Early Warning System**
  - > Putting all the information bits together
- » **Conclusion**

DDoS, Worms and the Underground

- **MEECES – an acronym for**
  - Money
  - Ego
  - Entertainment
  - Cause
  - Entrance into social groups
  - Status

- **Max Kilger (Honeynet Project)**
  - Applies to the underground/”hacker”/blackhat community
  - INTEL agencies’ MICE (Money, Ideology, Compromise, Ego)

DDoS, Worms and the Underground

» What have we seen up to now

- > Cause/Hacktivism:
  - Web site defacement
  - DDoS (SCO, WU/MSFT, etc)
- > Ego/Status:
  - “I have more (network) power than you”
  - “I’m not going to loose that item in <online game>”
- > Entertainment
  - “Hey look, I just DoSed <favorite IRC user/website>”
- > Entrance into a social group
  - “Wanna trade this botnet ?”

DDoS, Worms and the Underground

- **What have we seen up to now**
  - Money:
    - BGP speaking routers
    - SPAM, botnets, open proxies, etc.
    - C/C numbers incl. personal information, eBay accounts, etc.
- **Where are we today ? Real money**
  - "Pay or get DDoSed"
  - Worms for SPAM
  - Organized crime using "real world" proven ways of making money on the Internet
  - Targets: online business, mainly gaming/gambling/betting sites nowadays

DDoS, Worms and the Underground

» **Where are we today**

- > “Loosing” a botnet isn’t a tragedy
- > Mass-acquisition tools are mandatory
- > Protect your property (host and communication channel)
  - - Control channel over IRC/P2P/not so common protocols/IPv6 (anonymous)
  - - Secure the host to avoid multiple zombies/agents
- > Not for fun on free time anymore (people with network and DoS filtering technology/techniques skills)
- > The skills, knowledge, organization and hierarchy are not different/worse in the “blackhat” world... anything but not the chaotic world we all expect

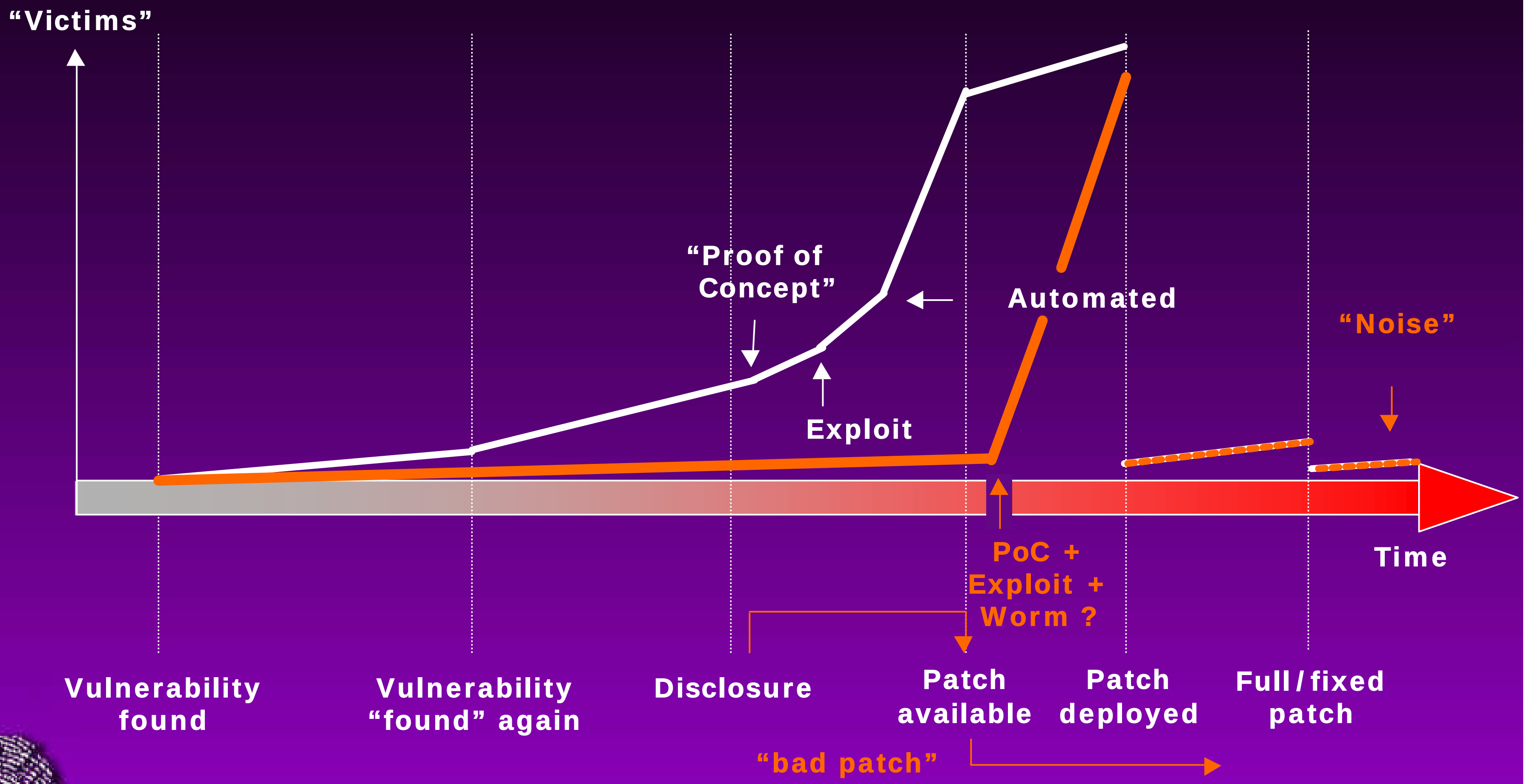
DDoS, Worms and the Underground

» Where are we today

- > A few hundred/thousand dollars/euros is a yearly salary in poor countries
- > AP and SA are the main sources, not (just) .ro anymore
- > Usually good education, leaving in a country with a high number of unemployed people
- > Most of the communications are in-band (Internet), out-of-band is limited to “hacker” meetings or local phone calls
- > Do you have the resources to analyze TBs a day of IRC logs coming from compromised hosts/honeypots (in x different languages) ?

DDoS, Worms and the Underground

» A vulnerability's life cycle: worm or not ?



> Key: is the exploit "generic" ? [Messenger vs LSASS]

What are ISPs/NSPs looking for ?

» **An EWS in a large network**

> Detect
  - DDoS attacks
  - (Unknown) worms
  - SPAM
  - Covert channels
  - Hacked system
  - Open proxies
  - Scans

> Detect it early!

> Cover a large network
  - Distributed approach, bandwidth/PPS requirements and system performance

> Easy to detect/fingerprint ?

What are ISPs/NSPs looking for ?

» **An EWS in a large network**

> Lots of data

> Information sources

- Honey* sensors
- Systems and Applications
- Security devices
- Network

» **Quick 101**

- BGP
- MPLS
- Netflow
- DDoS
- Honeypot

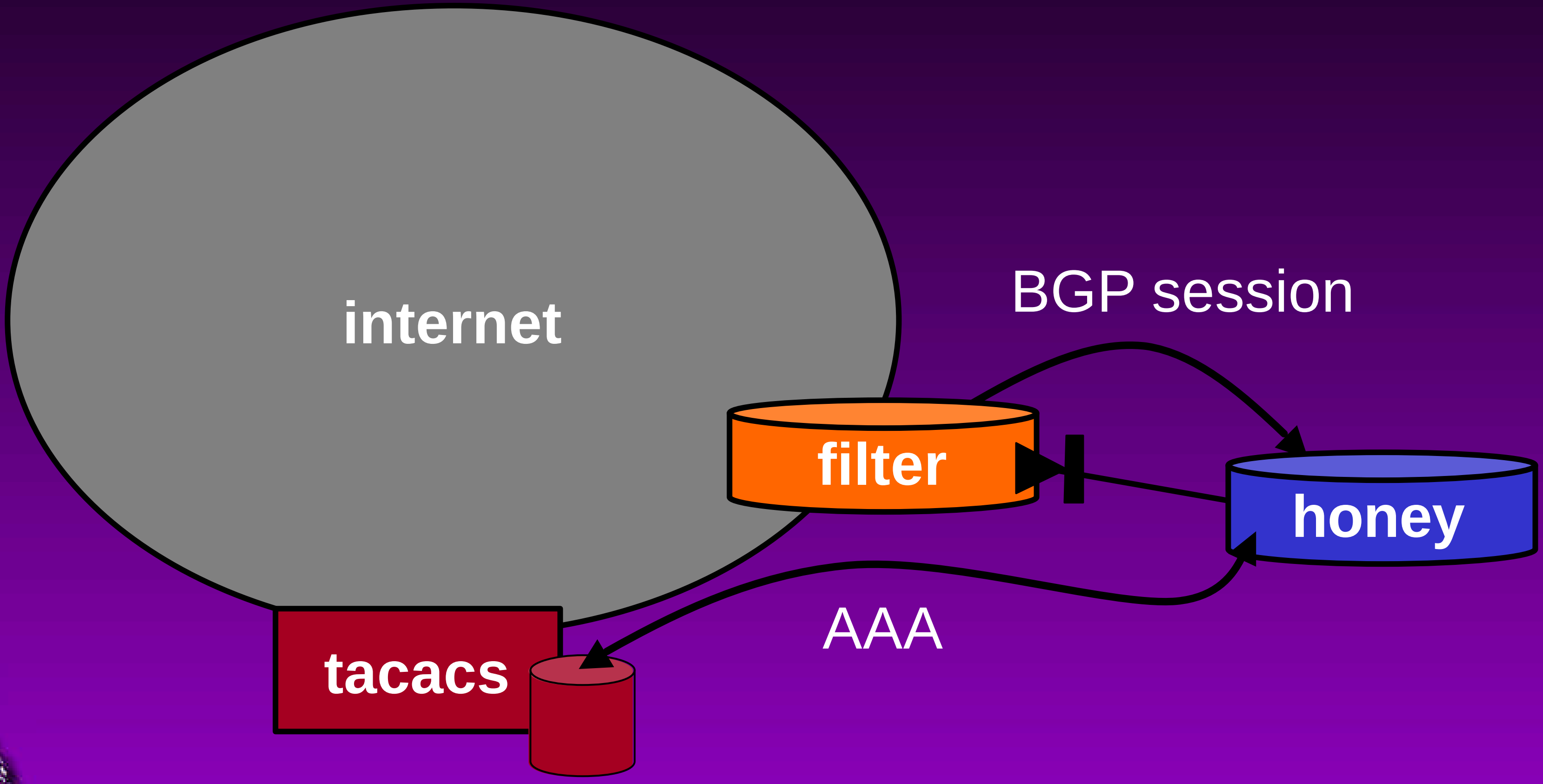
Honeyrouters

» **Routers as honeypots**

- > BGP speaking routers
- > Traded in the underground: more value than eBay accounts or valid CC numbers
  - - Makes them good targets
- > Password policy issue
  - - Are miscreant just scanning for open telnet/SSH or “brute force” the login and try out commands ?
- > BGP route injection: DDoS attack or SPAM ?

Honeyrouters

» Network architecture



Honeyrouters

- » **Using honeyd**
  - > Cisco CLI/telnet script
  - > SNMP script
- » **Using an UNIX+Zebra**
  - > Cisco-like CLI
- » **Using a Cisco router**
  - > Real BGP feed
    - - "read-only" BGP session
  - > Real "fake" account
    - - AAA and TACACS+
  - > Real network connectivity
    - - IP filtering and rate-limiting

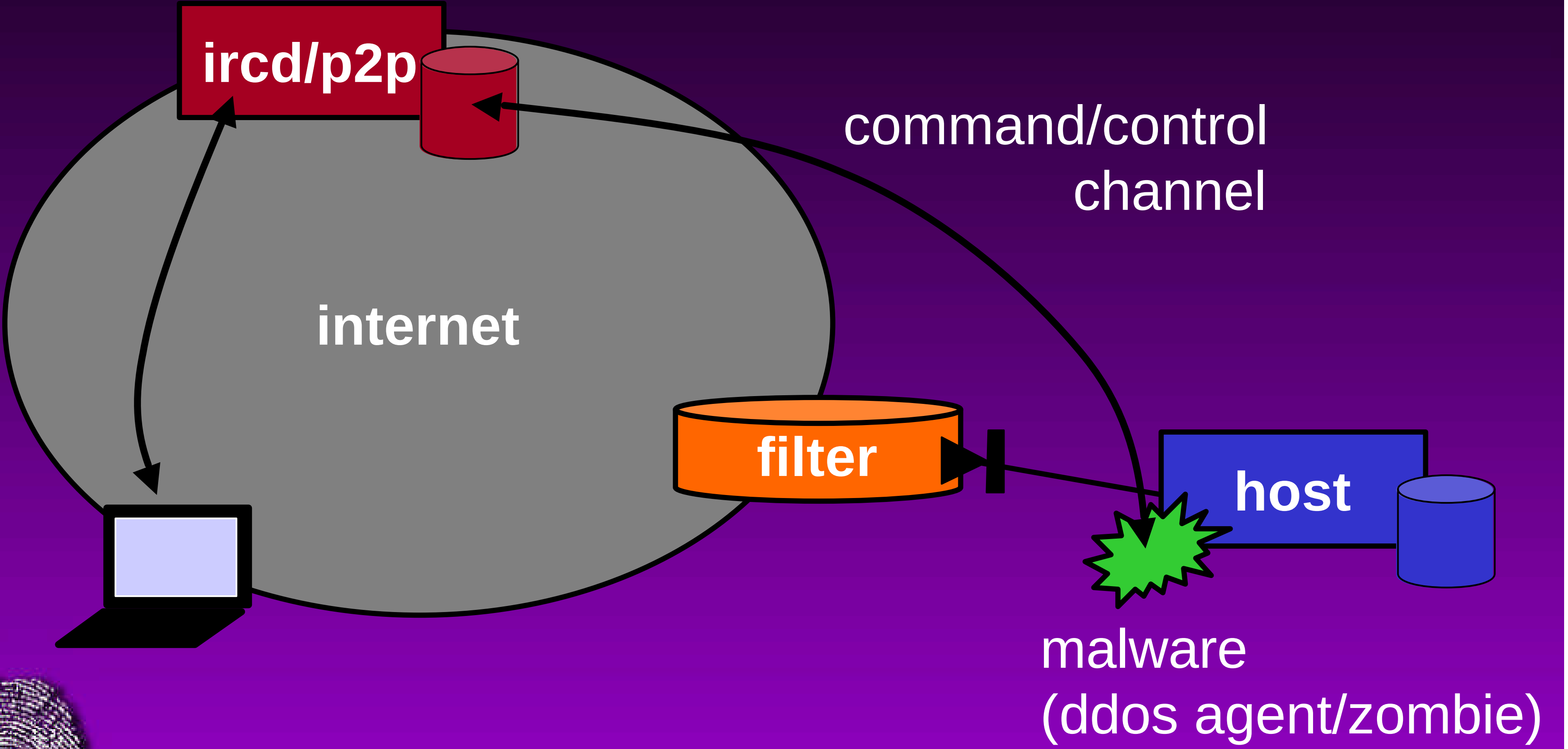
Honeybots

» **DDoS attack detection with honeybots / honeyzombies**

- > DDoS attack detection
  - Netflow, ACLs, SNMP, etc.
- > “Other SPs” DDoS detection
  - Backscatter data
  - Honeybots
    - . 0) Infected host post-mortem/forensics
    - . 1) Run bots and DDoS agents/zombies in a sandbox
    - . 2) Watch IRC, P2P, control channel communications

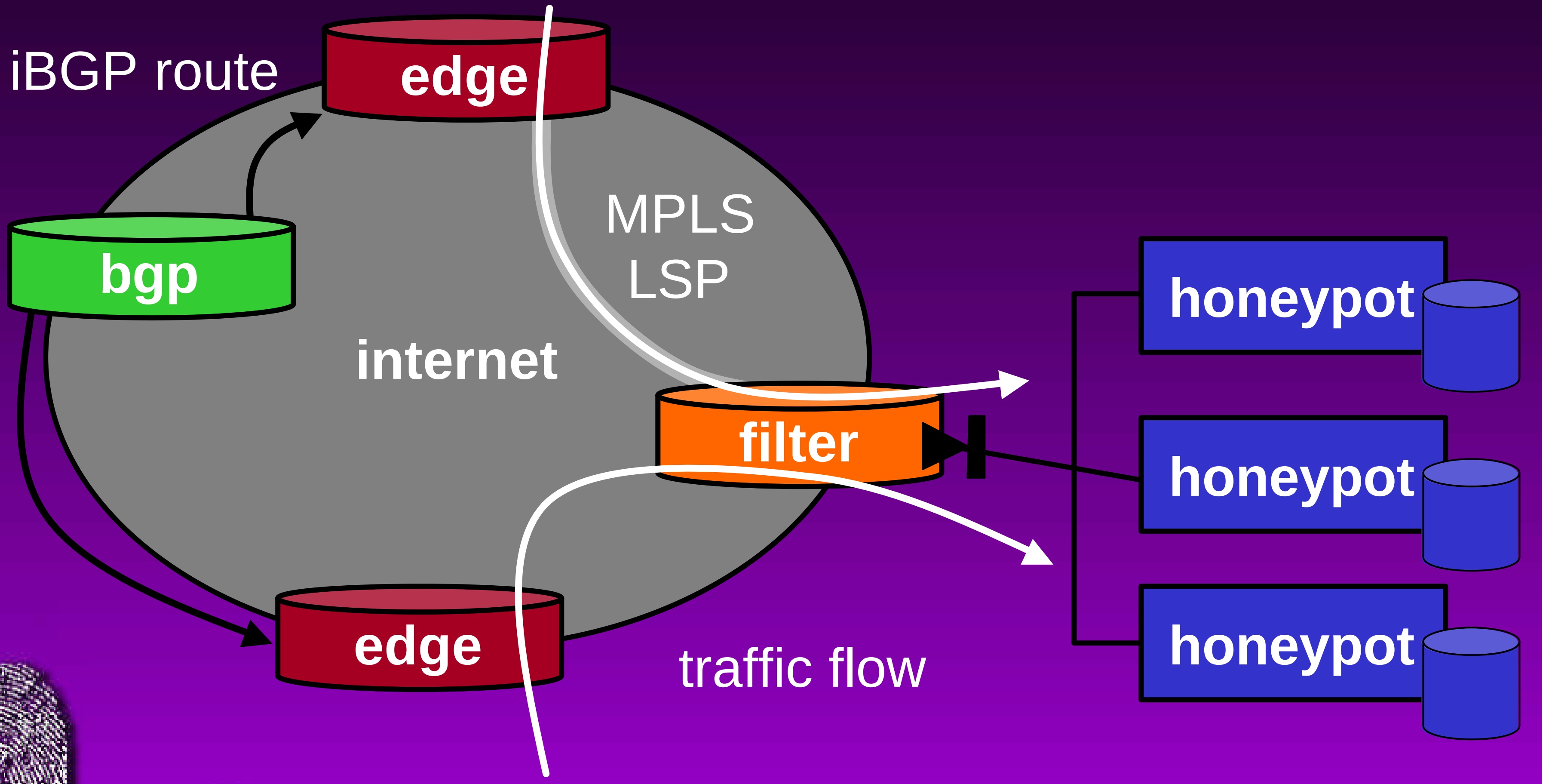
Honeybots

» **Network Architecture**



Honeyfarms

» **Traffic diversion to honeypots**



Honeyfarms

- **Traffic diversion to honeypots**
  - Easy traffic rerouting
  - May be “invisible”
  - Limitations
    - RTT/TTL may change
    - Overhead (L2TP and especially GRE/IPIP)
  - Use low-interaction honeypots
    - Basic TCP/UDP listeners, no “real” active response
    - honeyd
  - Avoid high-interaction (unless you have time and resources)
  - Established sessions
    - p0f v2: learn what the source may run on

System Data

» **System information sources**

- > Exposed services
  - - SMTP (mail server/relay): virus@MM
  - - DNS (authoritative/caching): Zonelabs/TAT14
  - - HTTP (portal/cache)
- > System logs

System Data

» **What not to do (at least not as an SP)**

> Use honeypots/fake open relays to detect and fight SPAM

- Risk of ending up in RBLs

> Use open proxies to detect surfing, phising, etc.

> Use honeypots/honeybots to bite back and clean up attacking systems: “Active Defense”

- Legal issues
- Not customers and even if they are... AUP ?
- Usually causes more harm than good!

> But an interesting approach inside an IT network

- Automated network “management”
- Perimeter is defined

Security Data

- » **Security information sources**
  - > Firewalls
  - > xIDS
  - > Anti-virus
  - > Security logs

Network Data

» **Network information sources**

- > Routers
  - ACLs
  - uRPF and interface counters
  - Requires a mix of scripts and SNMP polling
- > Traffic
  - Netflow
    - "Header" (src/dst IP, src/dst port, protocol, ingress interface, ToS but exports TCP flags, ASN, etc) and inbound only
  - Full traffic dump (RMON/SPAN/RTE/tap) in specific locations (hosting center upstreams, DSL/dial aggregation, etc)
  - "Dark" IP space
  - Sinkholes

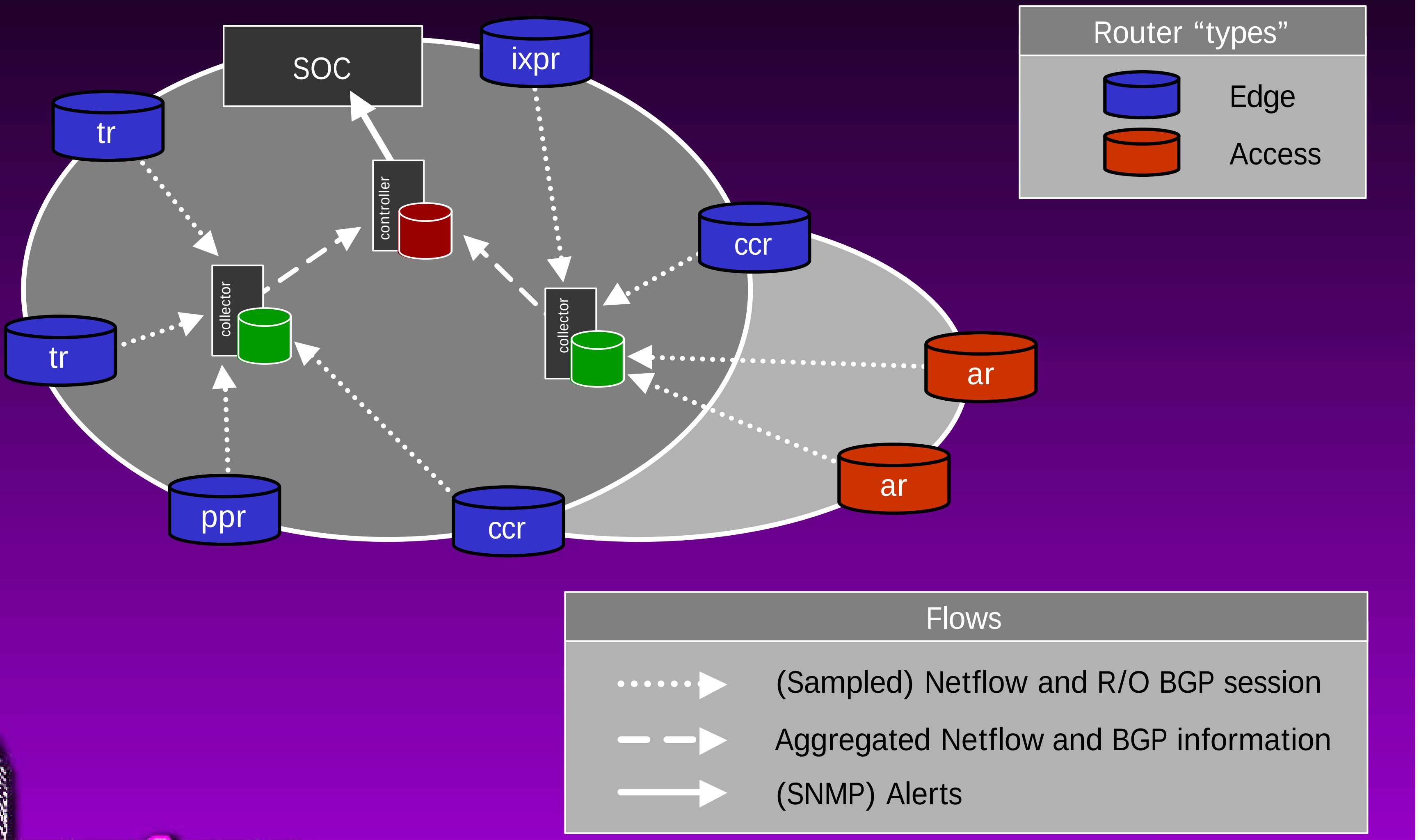
Network Data

» **Network information sources**

- > Routing
  - BGP updates
  - Route-server
  - Projects
    - RIPE RIS
    - Netlantis

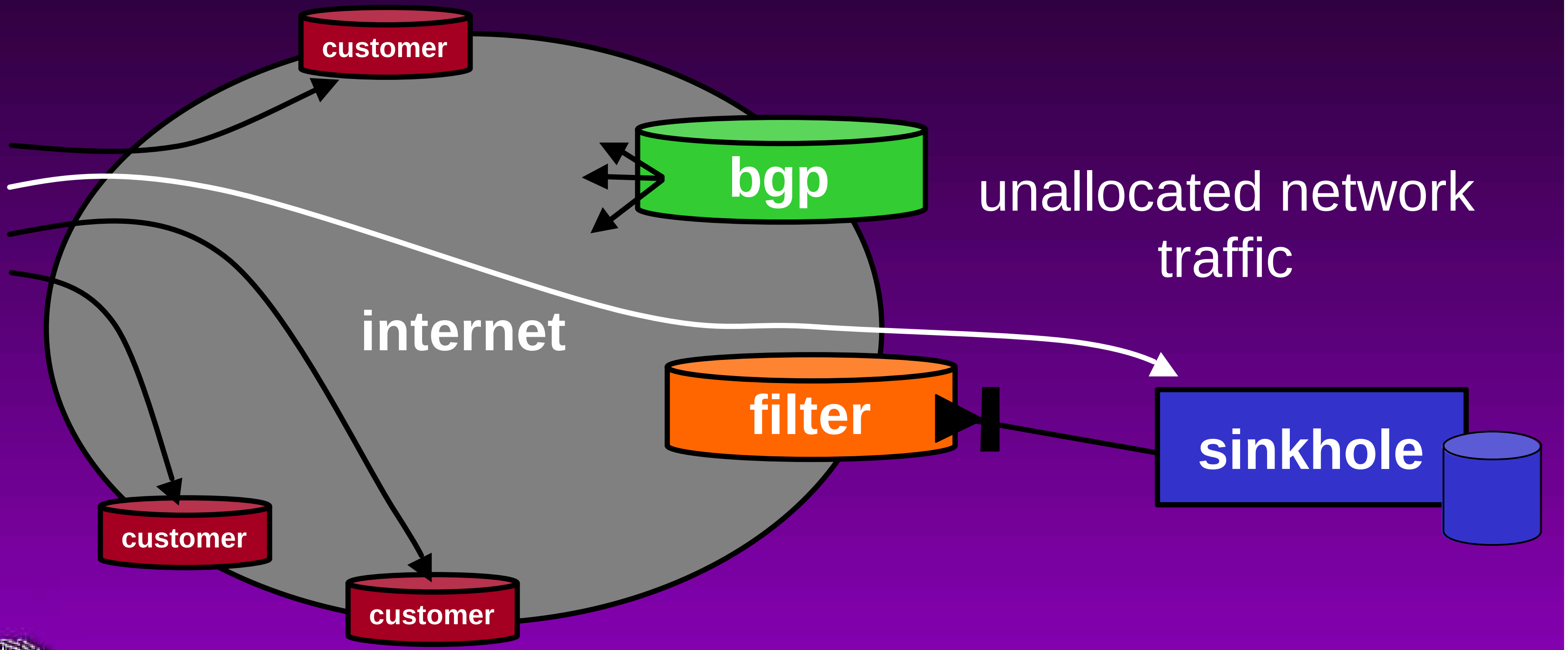
Netflow and BGP

» Network Architecture



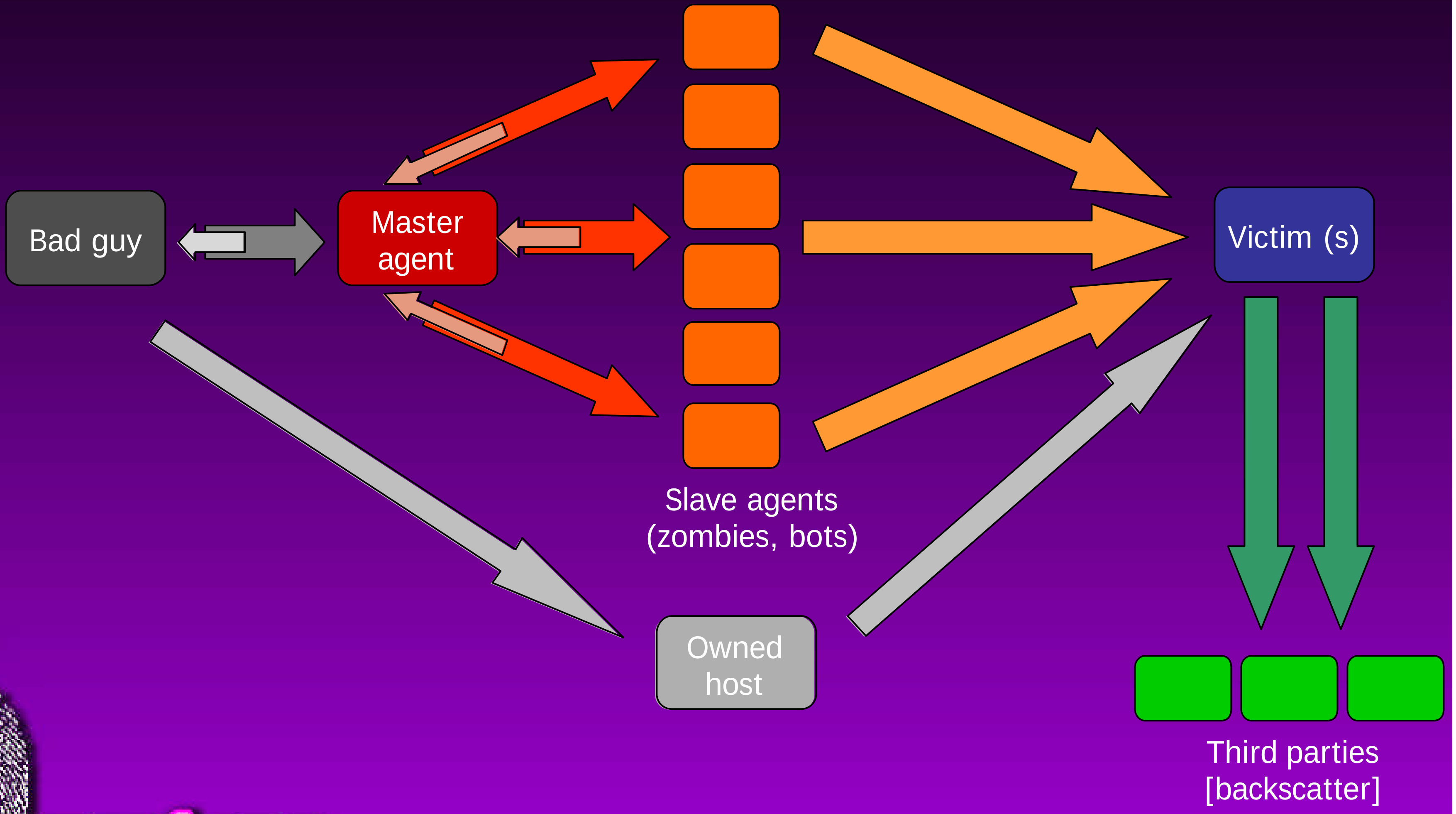
Dark IP space/Sinkholes

» Network Architecture



Dark IP space/Sinkholes

» **Collecting backscatter data**



Dark IP space/Sinkholes

- **Setup**
  - BGP speaking router
    - Route-reflector
    - Full iBGP mesh
  - Announce PA/PI allocations
  - Non-allocated/unused prefixes routed to the sinkhole/darkIP monitor
  - More-specific route followed for allocated (customer space)
  - Dynamic (add/remove)
    - Take the prefixes’ history into account
      - Ceased customers
      - Allocation method (dial/DSL): lots of short term noise
  - Central or distributed/regional deployment ?
    - IP Anycast

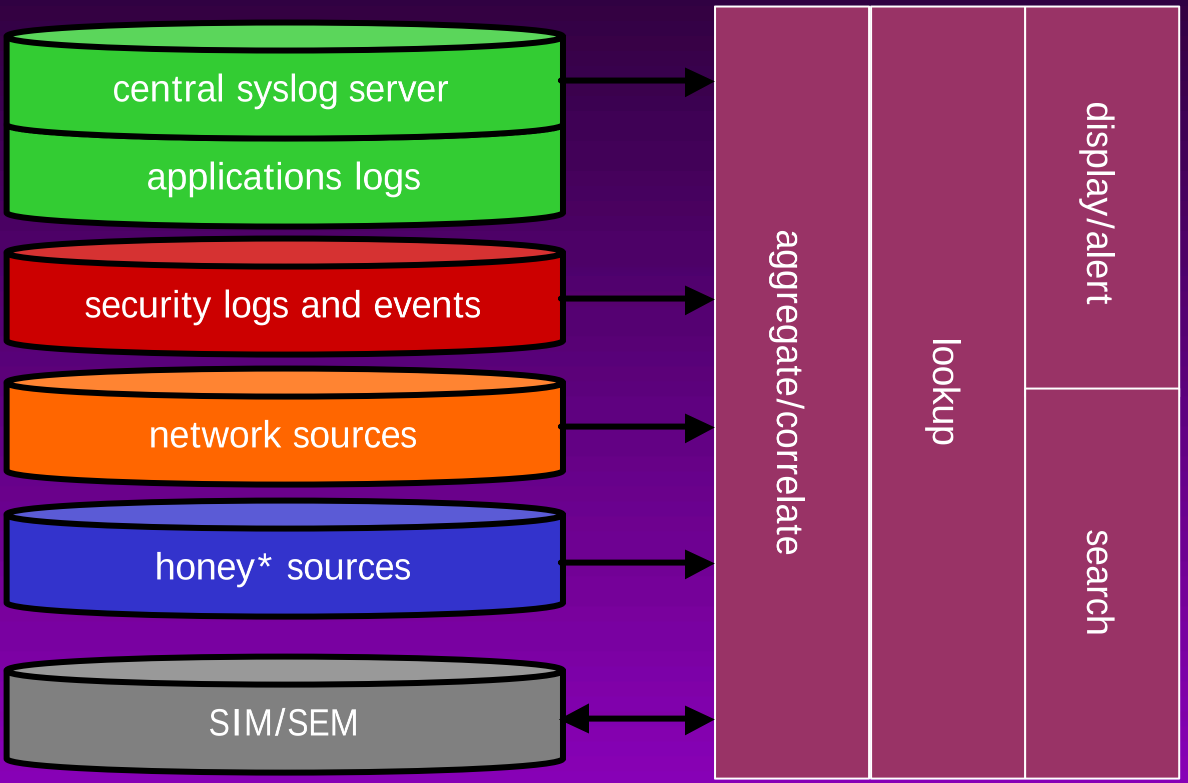
Dark IP space/Sinkholes

- **Data analysis**
  - > What kind of information will you get ?
  - > How to identify backscatter from other (rogue) traffic

Early Warning System

» **EWS**

> Share/reuse data with/from your SOC (SIM/SEM)



Early Warning System

- » **EWS**
  - > Which data have value ?
    - - High value
    - - Low value
  - > Use the human eye to catch anomalies
  - > Challenge: how to display and visualize data
- » **Can be deployed and useful inside an IT network**
- » **Don’t put your network at risk by deploying these sensors**

Conclusion

- » **Conclusion**
- » **See also**
  - > Backbone and Infrastructure Security Presentations
    - http://www.securite.org/presentations/secip/
  - > (Distributed) Denial of Service Presentations
    - http://www.securite.org/presentations/ddos/
- » **Q&A**
- » **Thanks**
  - > Lolo, Phil, Marc, Lance, Jose and Toby

Image: www.shawnsclipart.com/funkycomputercrowd.html