Network Security Today

Robin Sommer

International Computer Science Institute, &
Lawrence Berkeley National Laboratory

robin@icsi.berkeley.edu
http://www.icir.org/robin

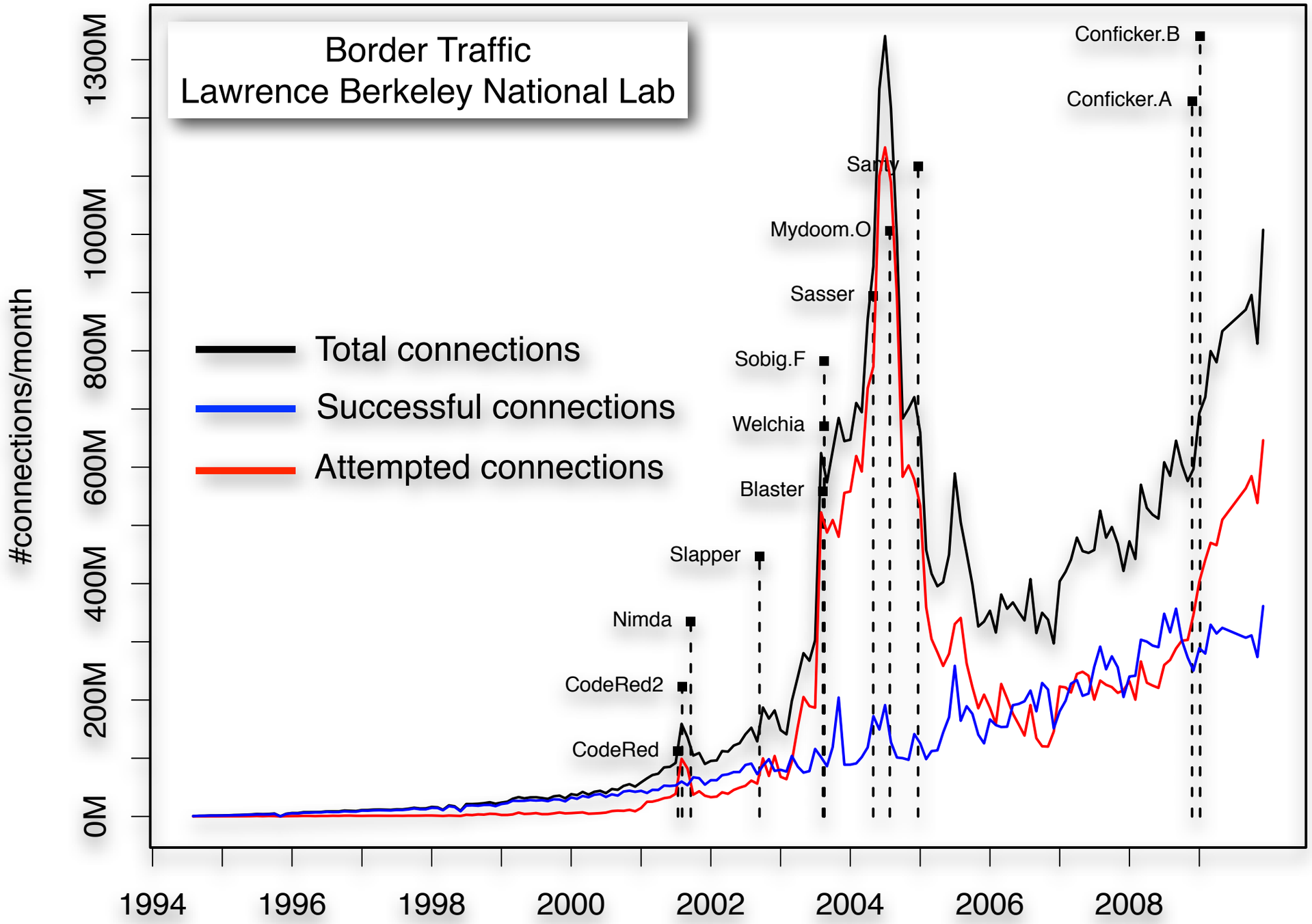
Security at the CyberBorder
February 2012, Indiana University

Outline

Part 1: Today's Network Threats.

Part 2: Defender Strategies.

The Old Days ...



Data: Lawrence Berkeley National Lab

Part 1: Today's Threats

Trend 1: Commercialization of Attacks

Trend 2: Highly Targeted Attacks

Trend 3: Insider Attacks

Trend 1: Commercialization of Attacks

Attacks aimed at making a profit.

- Selling (illegal) goods and services.
- Exfiltrate information.

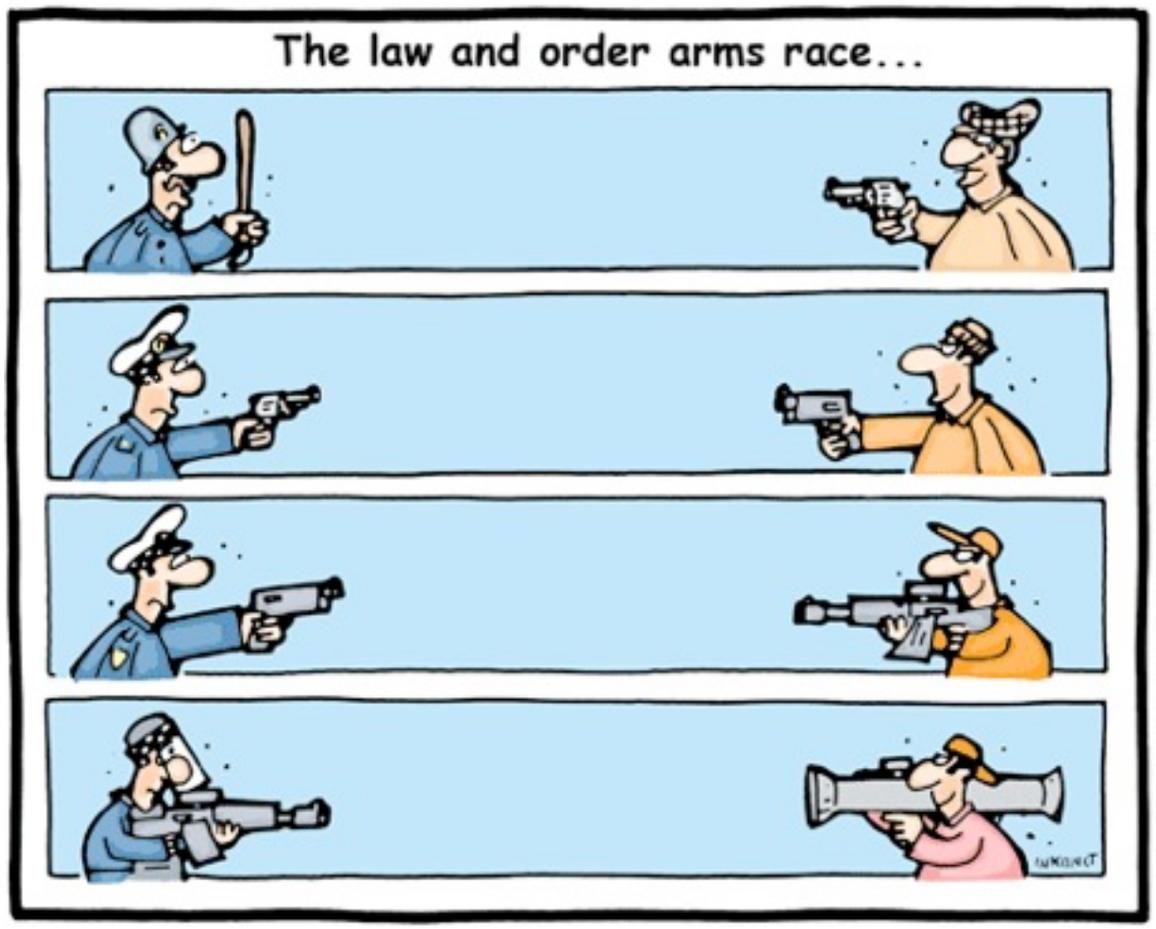
Thriving underground economy.

- Empowered by virtually endless supply of “bots”.
- Everything is on sale (“crime-as-a-service”).

“Pay Per Install” Services

Crime Economics

Accelerated arms race.
Innovative, fast moving attackers.



Bear race.
If attack pays, it's good enough.

Trend 2: Highly Targeted Attacks

High-skill / high-resource attacks.

- Targeting **you.**
- Extremely hard to defend against.
- Attribution virtually impossible.

Typical Instances

- “Advanced Persistent Threats”.
- Activist hacking.

Targeted Attacks: APTs

Open Letter to RSA Customers

Arthur W. Coviello, J

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA. We took a variety of aggressive measures against the threat to protect our business and our customers, including further hardening of our IT infrastructure. We also immediately began an extensive investigation of the attack and are working closely with the appropriate authorities.

egory
ealed
n
RSA's

Source: RSA

Advanced Persistent Threat (APT). MANDIANT defines the APT as a group of sophisticated, determined and coordinated attackers that have been systematically compromising U.S. government and commercial computer networks for years. The vast majority of

Source: MANDIANT

Targeted Attacks: APTs (2)

EXPLOITATION LIFE CYCLE

STEP 1 Reconnaissance

STEP 2 Initial Intrusion into the Network

STEP 3 Establish a Backdoor into the Network

STEP 4 Obtain User Credentials

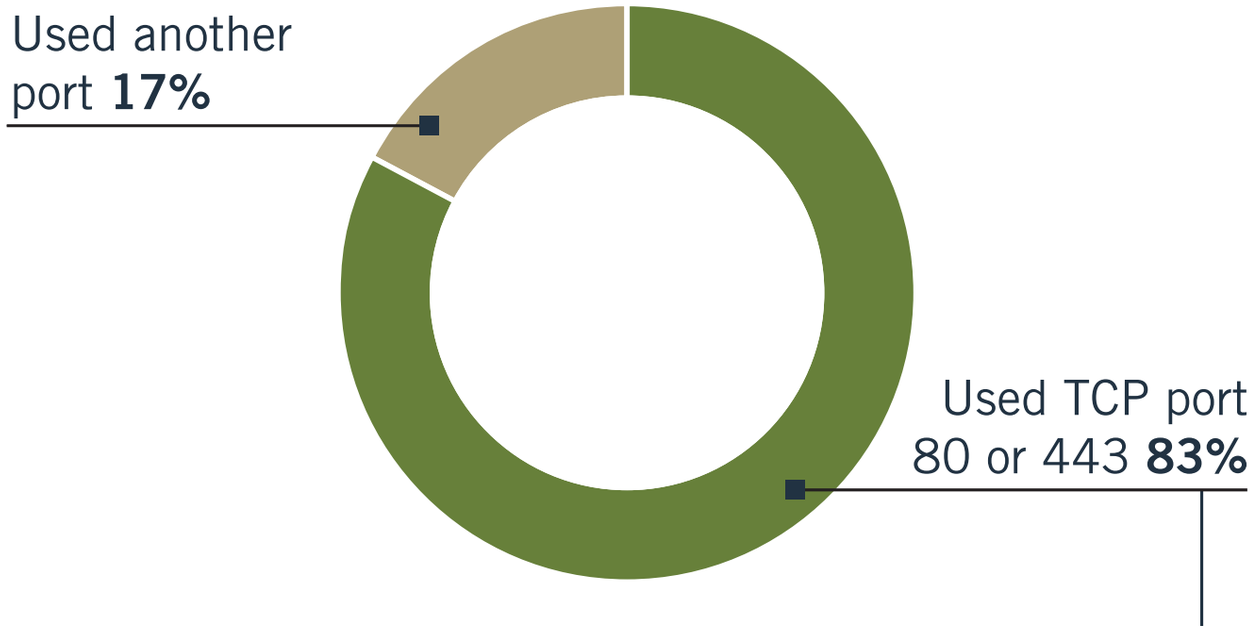
STEP 5 Install Various Utilities

STEP 6 Privilege Escalation / Lateral Movement / Data Exfiltration

STEP 7 Maintain Persistence

APT MALWARE COMMUNICATION

100% of APT backdoors made only outbound connections



In no instance was any APT malware written or configured to listen for inbound connections.

Source: MANDIANT

Targeted Attacks: Activist Hacking

Source: Wikipedia

Defender Strategies

Challenges

Varying threat models.

No ring rules them all.

Semantic complexity.

The action is really at the application-layer.

Volume and variability.

Network traffic is an enormous haystack.

Legal and ethical frameworks.

Not everything you can do, you may.

Defender Strategies

Creating visibility.

Instrument the network comprehensively.

Analyze semantics.

Not bytes.

Share intelligence.

“The good guys share, too!”

Active response.

Blacklist, or whitelist, what you know.

Creating Visibility with Bro

```
> bro -i en0
[ ... wait ...]
> cat conn.log
```

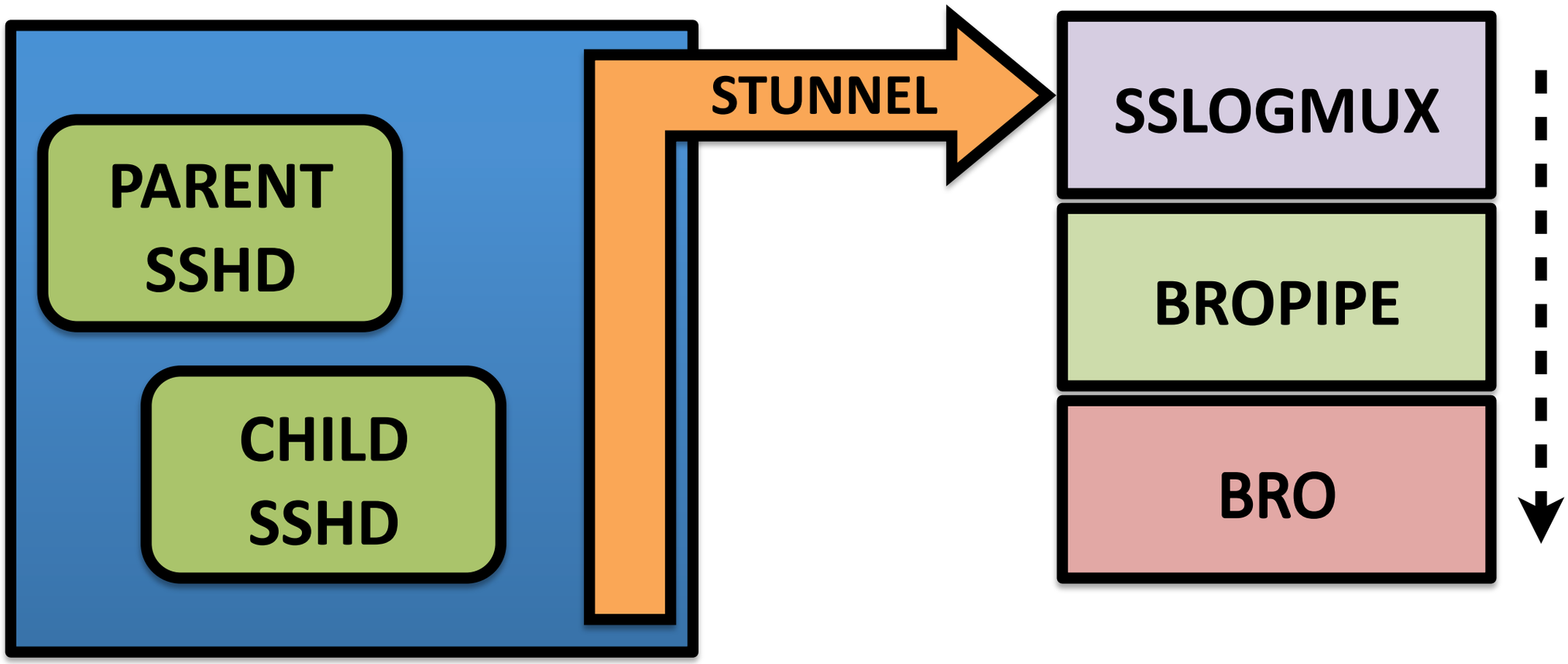
```
#fields ts          id.orig_h         id.orig_p  id.resp_h         id.resp_p proto  service  duration
1144876741.1198  192.150.186.169 53115      82.94.237.218   80        tcp    http     16.14929
1144876612.6063  192.150.186.169 53090      198.189.255.82  80        tcp    http     4.437460
```

```
[...] host                uri                      status_code  user_agent [...]
      docs.python.org     /lib/lib.css             200          Mozilla/5.0
      docs.python.org     /icons/previous.png      304          Mozilla/5.0
      docs.python.org     /lib/lib.html            200          Mozilla/5.0
      docs.python.org     /icons/up.png            304          Mozilla/5.0
      docs.python.org     /icons/next.png          304          Mozilla/5.0
      docs.python.org     /icons/contents.png      304          Mozilla/5.0
      docs.python.org     /icons/modules.png       304          Mozilla/5.0
      docs.python.org     /icons/index.png         304          Mozilla/5.0
       www.google.com     /                        200          Mozilla/5.0
```

```
1144876742.3338  192.150.186.169  53116      docs.python.org  /icons/index.png  304  Mozilla/5.0
1144876745.6144  192.150.186.169  53117       www.google.com  /                 200  Mozilla/5.0
```

Creating Visibility: Encryption

"Auditing SSHD"



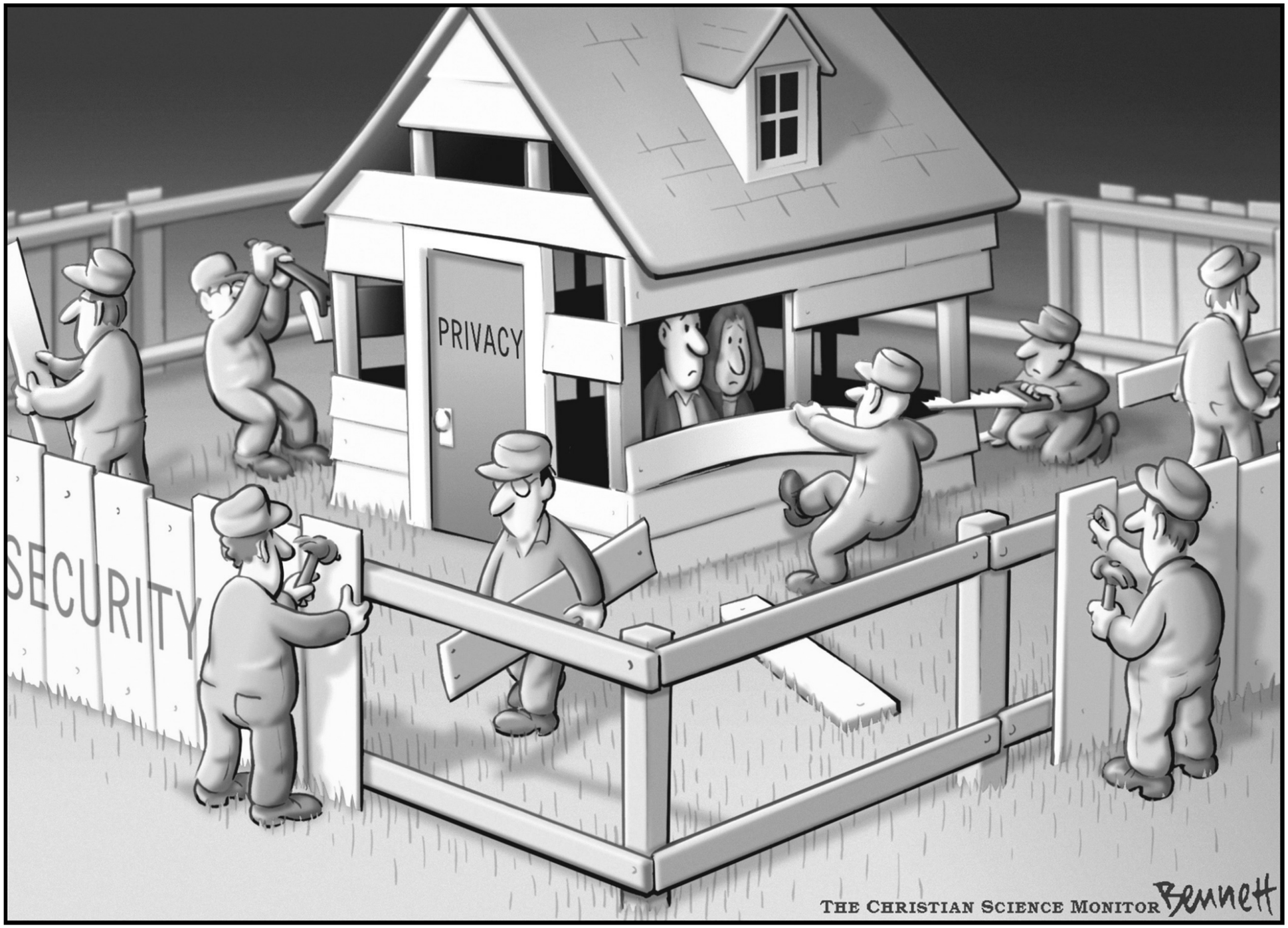
Source: Scott Campbell / NERSC

NERSC Computer Use Policies Form

Monitoring and Privacy

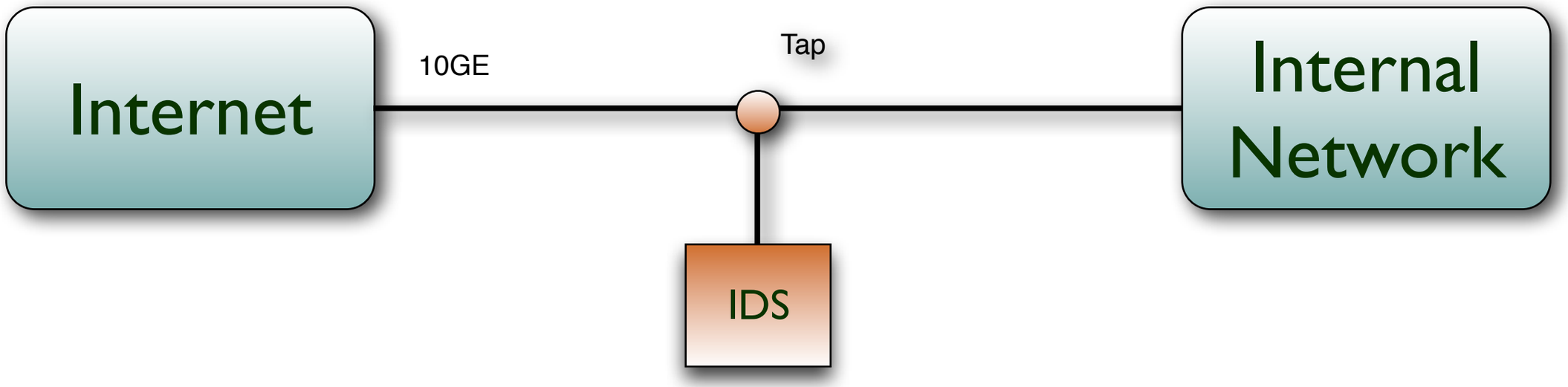
Users have no explicit or implicit expectation of privacy. NERSC retains the right to monitor the content of all activities on NERSC systems and networks and access any computer files without prior knowledge or consent of users, senders or recipients. NERSC may retain copies of any network traffic, computer files or messages indefinitely without prior knowledge or consent.

The Security Fence



Cartoon Courtesy Clay Bennett / The Christian Science Monitor

Analyzing Semantics

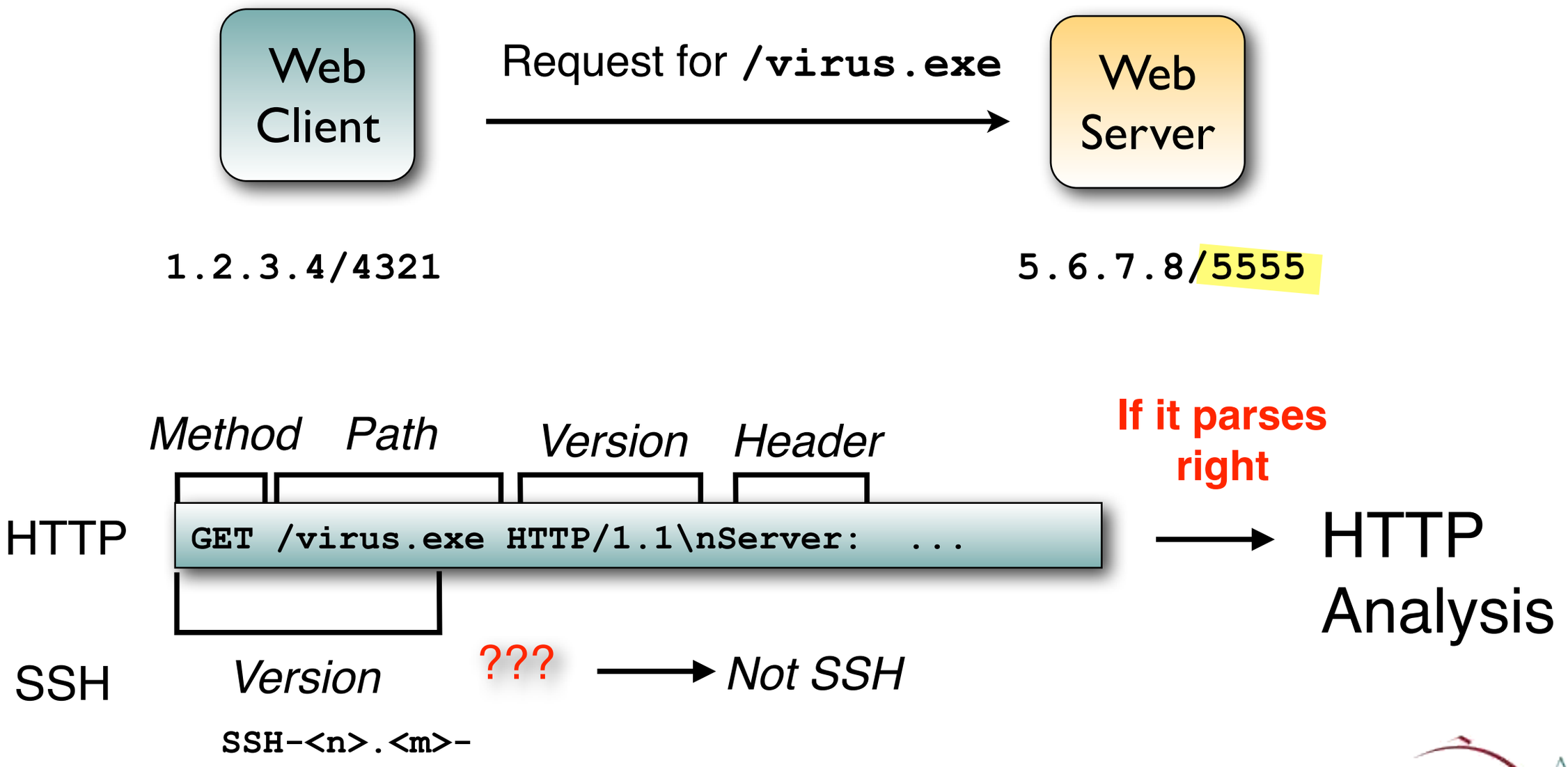


Example: Finding downloads of known malware.

1. Find and parse all Web traffic.
2. Find and extract binaries.
3. Compute hash and compare with database.
4. Report, and potentially kill, if found.

Port-independent Application Analysis

Bro's Dynamic Protocol Detection



Identifying HTTP Servers

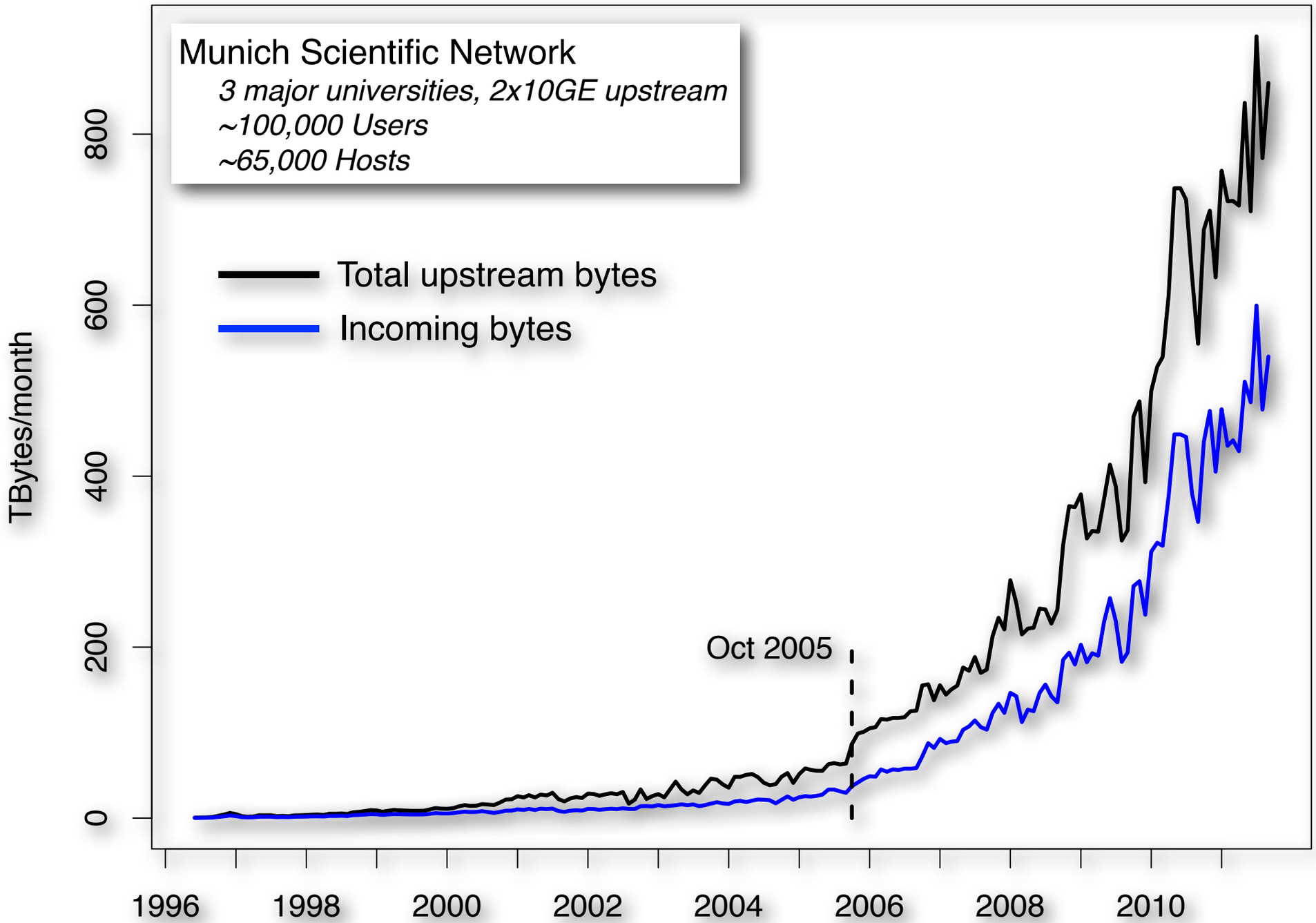
Server Addresses

a198-189-255-200.deploy.akamaitechnolgies.com
a198-189-255-216.deploy.akamaitechnolgies.com
a198-189-255-217.deploy.akamaitechnolgies.com
a198-189-255-230.deploy.akamaitechnolgies.com
a198-189-255-225.deploy.akamaitechnolgies.com
a198-189-255-206.deploy.akamaitechnolgies.com
a198-189-255-201.deploy.akamaitechnolgies.com
a198-189-255-223.deploy.akamaitechnolgies.com
72.21.91.19
a198-189-255-208.deploy.akamaitechnolgies.com
a198-189-255-207.deploy.akamaitechnolgies.com
nuq04s07-in-f27.1e100.net
a184-28-157-55.deploy.akamaitechnologies.com
a198-189-255-224.deploy.akamaitechnolgies.com
a198-189-255-209.deploy.akamaitechnolgies.com
a198-189-255-222.deploy.akamaitechnolgies.com
a198-189-255-214.deploy.akamaitechnolgies.com
nuq04s06-in-f27.1e100.net
upload-lb.pmtpa.wikimedia.org
nuq04s08-in-f27.1e100.net

HTTP Host Headers

ad.doubleclick.net
ad.yieldmanager.com
b.scorecardresearch.com
clients1.google.com
googleads.g.doubleclick.net
graphics8.nytimes.com
l.yimg.com
liveupdate.symanteclive update.com
mt0.google.com
pixel.quantserve.com
platform.twitter.com
profile.ak.fbcdn.net
s0.2mdn.net
safebrowsing-cache.google.com
static.ak.fbcdn.net
swcdn.apple.com
upload.wikimedia.org
www.facebook.com
www.google-analytics.com
www.google.com

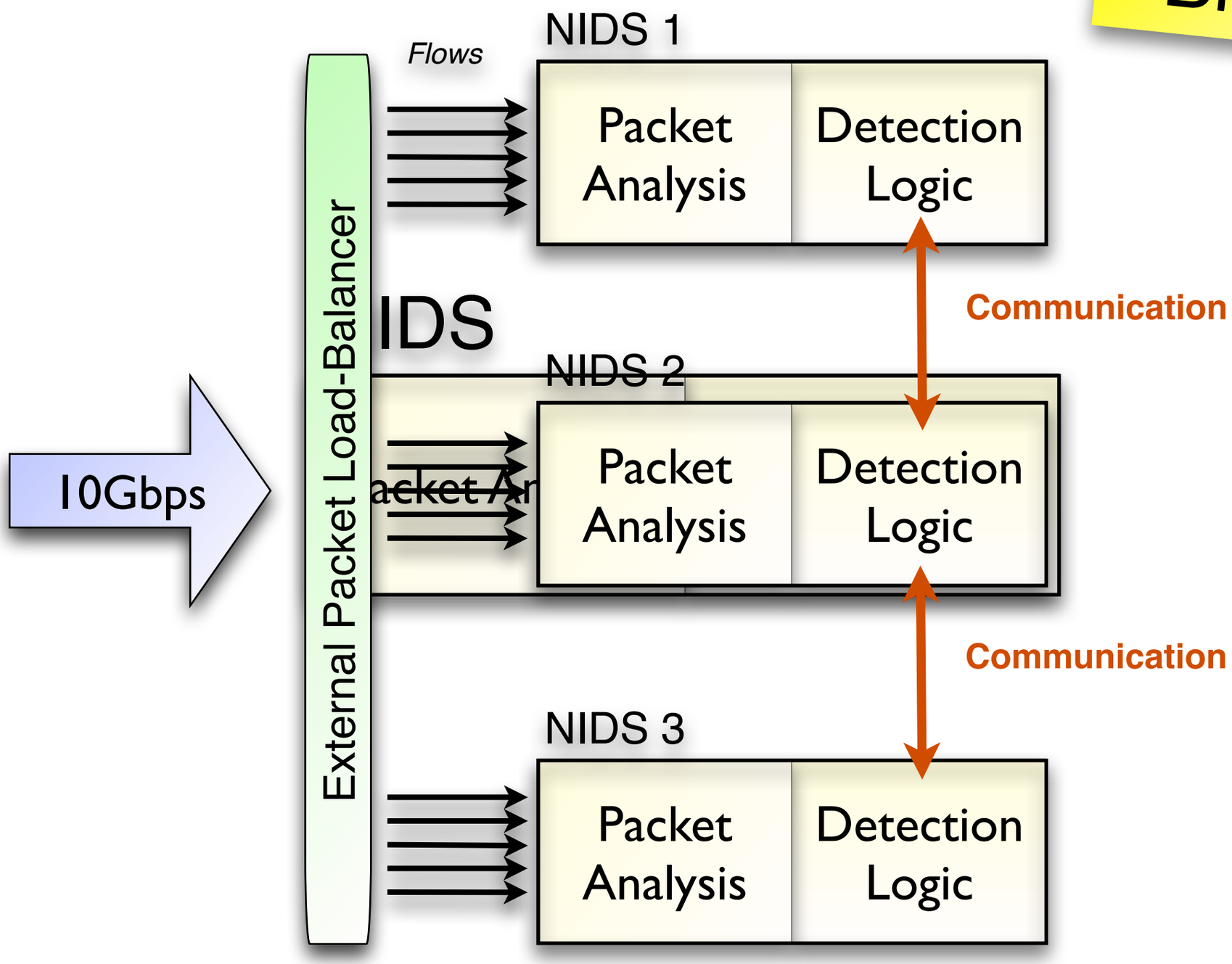
Performance Challenges



Data: Leibniz-Rechenzentrum, München

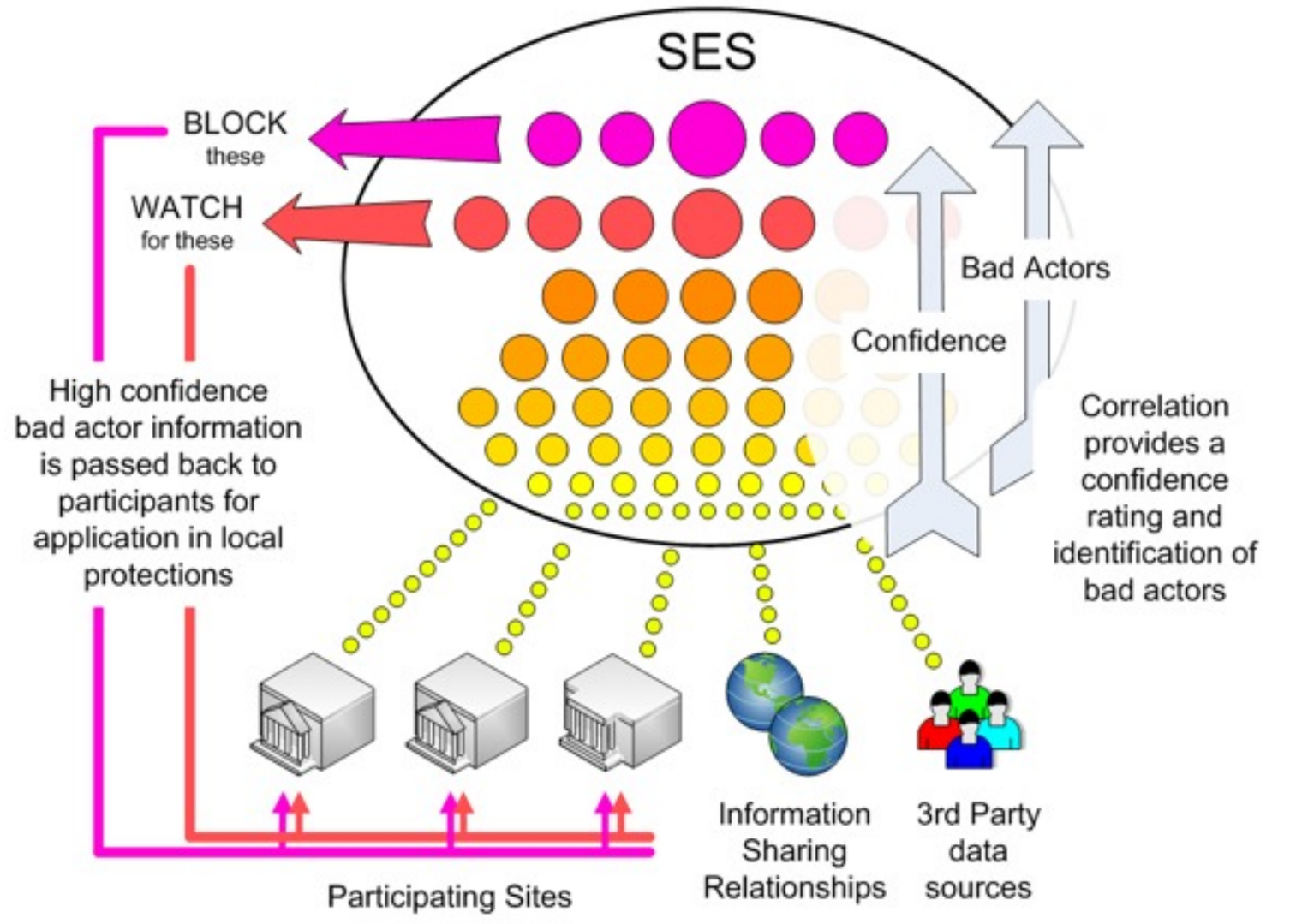
Load-balancing Architecture

"Bro Cluster"



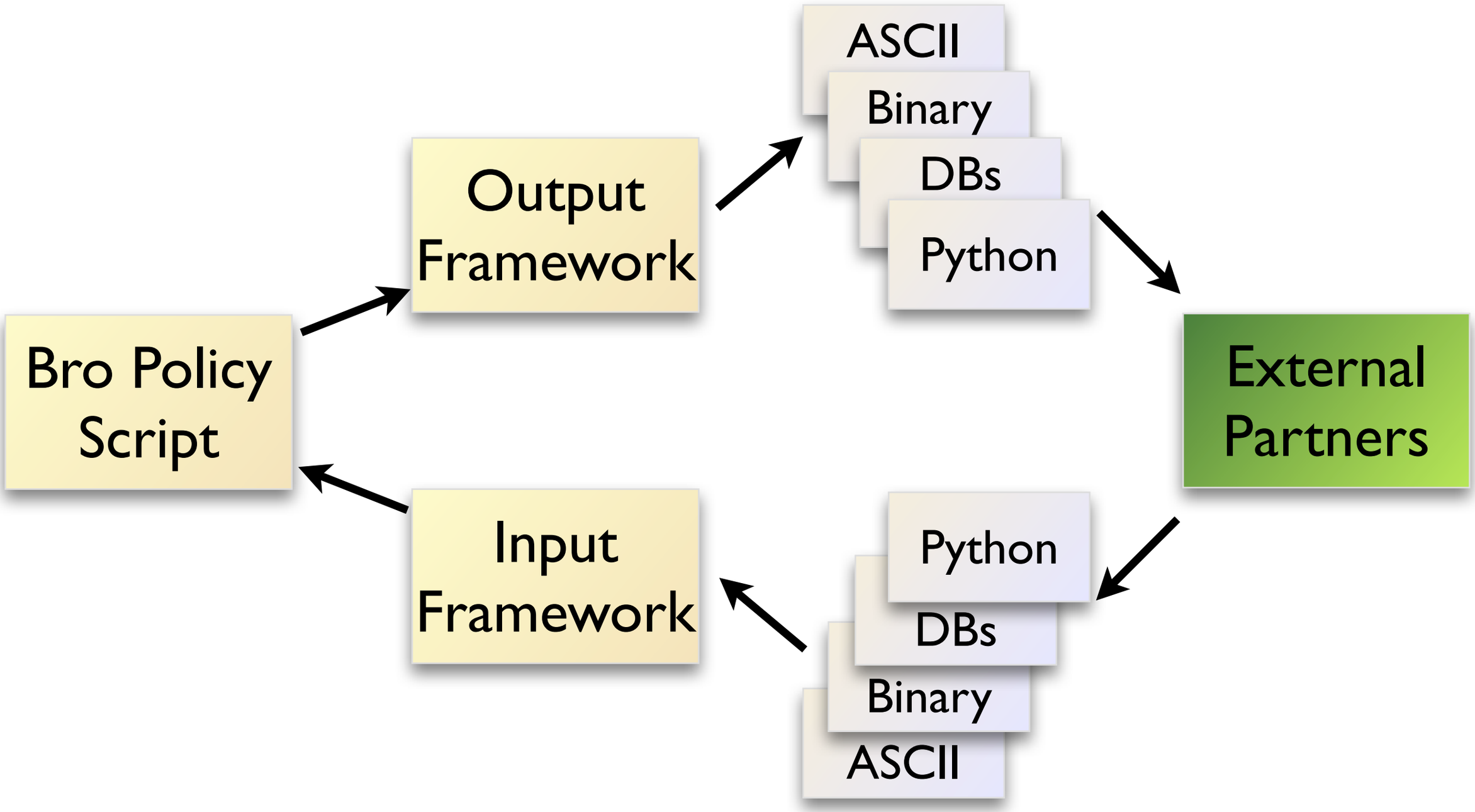
Sharing Intelligence

REN-ISAC's Security Event System



Source: REN-ISACs

Real-time Intelligence with Bro



Active Response

Interface to the network layer.

- Kill sessions.
- Block hosts (local, remote).
- Block applications (static, dynamically).

The Extreme: White-list activity.

- Destinations, applications, services.
- Technically challenging, need full proxy.

Conclusion

Today's Threats

- Commercialization of Attacks
- Highly Targeted Attacks
- Insider Attacks

Defender Strategies

- Creating visibility.
- Analyze semantics.
- Share intelligence.
- Active response.

Understand semantics, put activity into broader context, react, and share your knowledge.

Thanks for your attention.

Robin Sommer

International Computer Science Institute, &
Lawrence Berkeley National Laboratory

robin@icsi.berkeley.edu
http://www.icir.org/robin

Security at the CyberBorder
February 2012, Indiana University