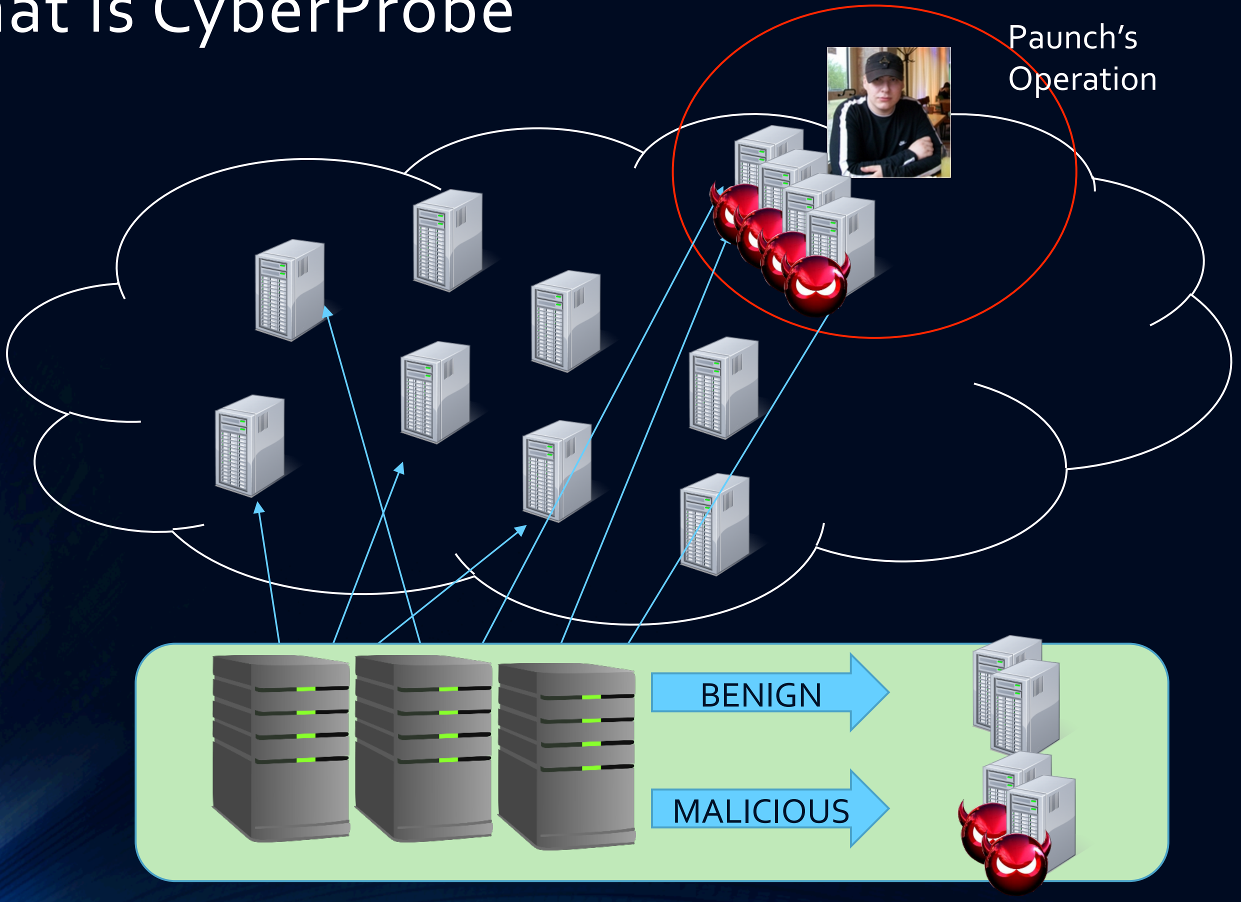
CyberProbe: Towards Internet-Scale Active Detection of Malicious Servers

A. NAPPA, Z. XU, M.Z. RAFIQUE, J.CABALLERO, G.GU
IMDEA SOFTWARE INSTITUTE
SUCCESS LAB, TEXAS A&M UNIVERISTY

Cybercriminals use geographically distributed servers to run their malicious operations

- Exploit servers -> Malware distribution
- Payment servers -> Monetization
- Redirectors -> Anonymity
- C&C servers -> Control botnets
- P2P bots (server functionality)

What is CyberProbe



Existing detection techniques: Passive

- Honeypots
- Spamtraps

- **LIMITATIONS**

  - Slow

  - Incomplete (i.e., limited view)

Existing detection techniques: Active

- Run malware samples
- Honeyclient farms (i.e. Google Safebrowsing)

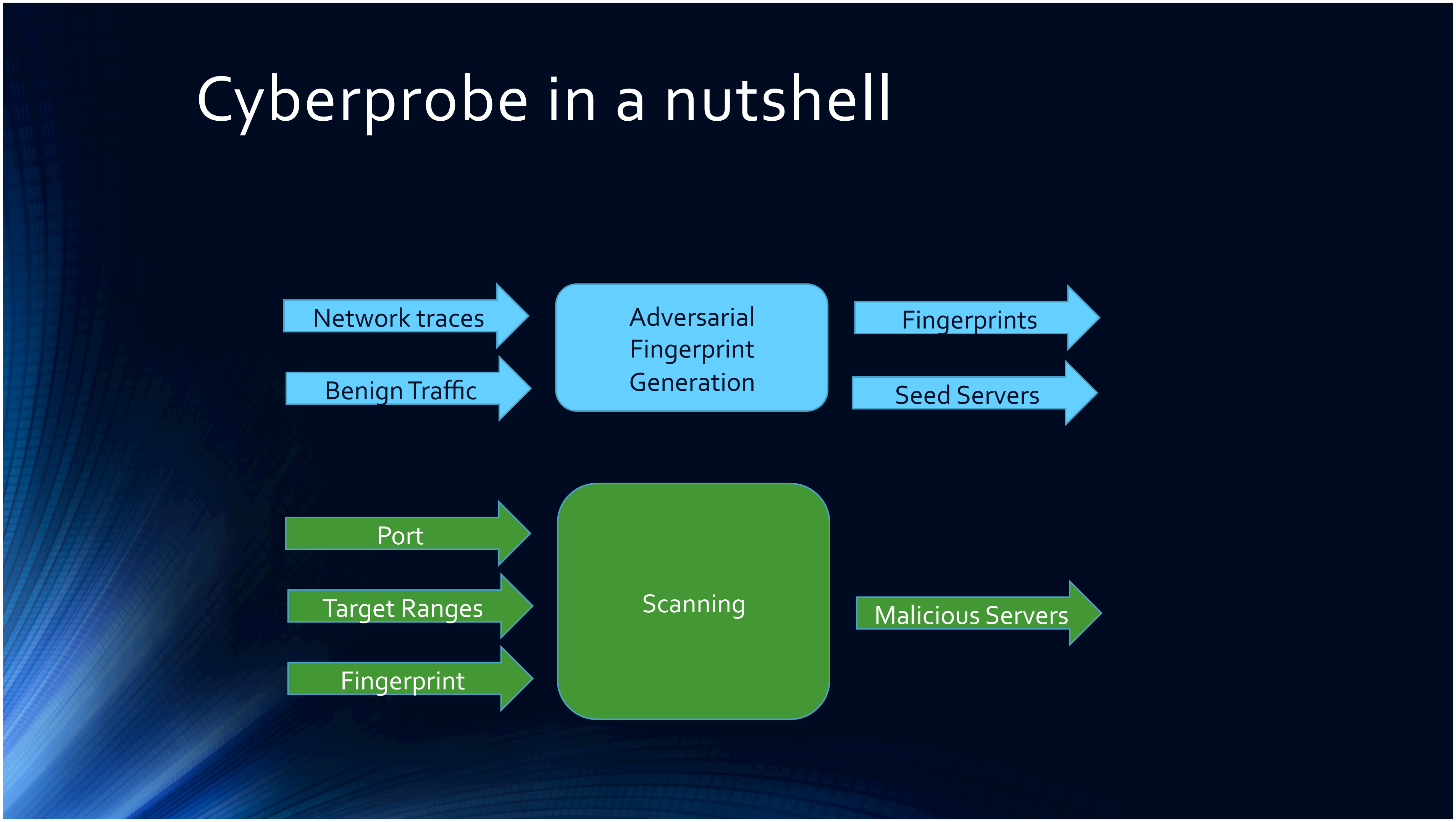
- **LIMITATIONS**

  - Expensive

  - Incomplete (i.e., Safebrowsing focuses on exploit servers)

Contributions

- Novel active probing approach for Internet-scale detection of malicious servers
- Novel adversarial fingerprint generation technique
- Implement approach into CyberProbe
- Use CyberProbe for 24 localized and Internet-wide scans
  - Identifies 151 malicious servers
  - 75% of the servers unknown to databases of malicious activity (e.g., VirusTotal, UrlQuery)
  - Identifies provider locality property



Cyberprobe in a nutshell

Network traces

Benign Traffic

Adversarial Fingerprint Generation

Fingerprints

Seed Servers

Port

Target Ranges

Fingerprint

Scanning

Malicious Servers

Fingerprints

- **A fingerprint for each operation & server type**
- **A fingerprint comprises:**
  - **A probe construction function → Packet**
  - **A classification function → Snort signature**

Clickpayz1

Probe: GET /td?aid=e9xmkgg5h6&said=26427

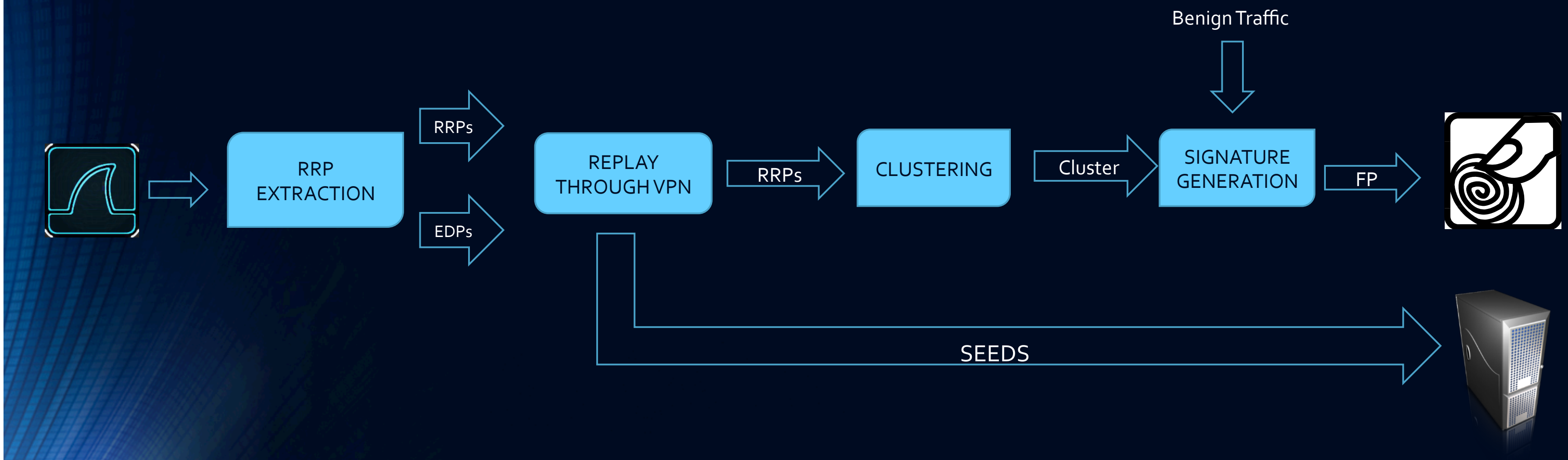
Signature:

content: "302"; http_stat_code;
content: "\r\n\r\nLoading…"

Adversarial Fingerprint Generation: Goals

- **Minimize traffic**
- **Generate inconspicuous probes**

Adversarial Fingerprint Generation: Architecture



Benign Traffic

RRP EXTRACTION

RRPs

EDPs

REPLAY THROUGH VPN

RRPs

CLUSTERING

Cluster

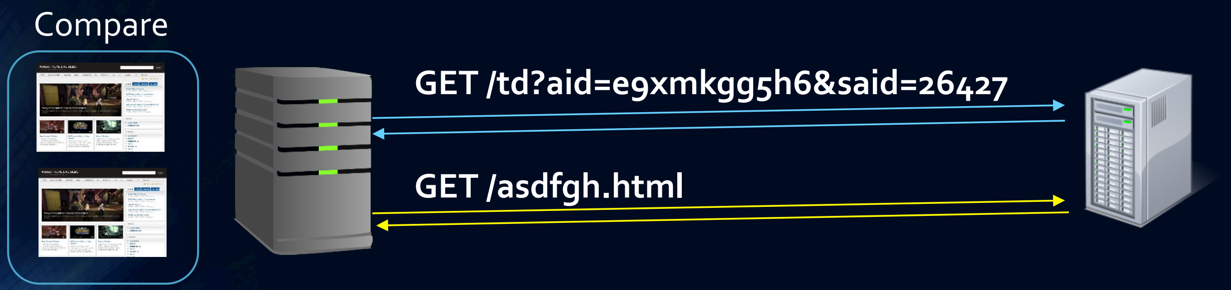
SIGNATURE GENERATION

FP

SEEDS

Generation details

- Replay
  - VPN for: anonymity, IP diversity and for new states
  - Check result against random resource from the server



Compare

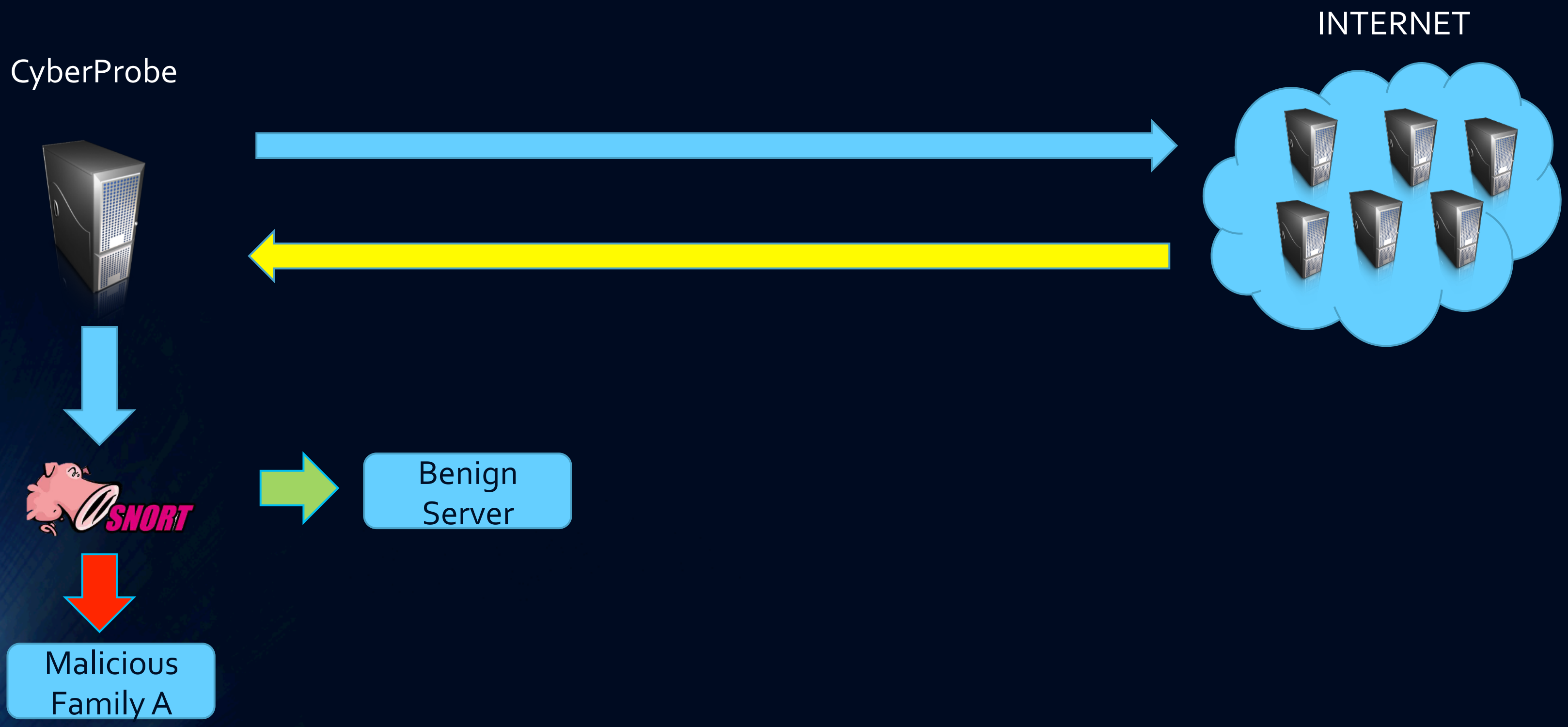
GET /td?aid=e9xmkgg5h6&said=26427

GET /asdfgh.html

Scanning

- 3 scanners:
  - Horizontal → SYN scan
  - AppTCP scanner (sends app-level probe)
  - UDP scanner
- 3 scan ranges:
  - Localized-reduced
  - Localized-extended
  - Internet-wide
- Signature matching uses Snort

AppTCP and UDP scanners



Scanning summary

TCP

- TCP horizontal scanner (fast, polite)
- TCP sniffer (reliable to get responses to our probes)
- AppTCP scanner (Asynchronous + Snort)

UDP

- UDP scanner (fast, polite) + Snort

Ethical Considerations

To scan as politely as possible we:

- Rate-limit scanners
- Set up forward and backward DNS entries for scanners
- Set up a webpage in the scanners to explain our experiment
- Remove from whitelist provider’s ranges that request so
- Manually check fingerprints

Adversarial fingerprint generation results

Type	Source	Families	Pcaps	RRPs	RRPs Replayer	Seeds	Fingerprints
Malware	VirusShare	152	918	1,639	193	19	18
Malware	MALICIA	9	1,059	764	602	2	2
Honeyclient	MALICIA	6	1,400	42,160	9,497	5	2
Honeyclient	UrlQuery	1	4	11	11	1	1

AppTCP Scan Results

- 151 total servers scans
- Virustotal k % of the servers
- UrlQuery 1
- MalwareDo xVault 1%

4x Better Coverage

Servers Operations

Operation	Fingerprints	Seeds	Servers	Prov.	Provider Loc.
bestav	3	4	23	7	3.3
bh2-adobe	1	1	13	7	1.8
bh2-ngen	1	1	2	2	1.0
blackrev	1	1	2	2	1.0
clickpayz	2	2	51	6	8.5
doubleighty	1	1	18	9	2.0
kovter	2	2	9	4	2.2
ironsource	1	1	7	4	1.7
optinstaller	1	1	18	4	2.0
soft196	1	1	8	4	2.0
TOTAL	**14**	**15**	**151**	**47**	**3.2(avg.)**

Observations

Provider Locality:

Once a relationship has been established with a provider it is very likely that more than one malicious server will be setup with this provider

P2P bots Scan Results

Type	Start-Date	Port	Fingerprint	Targets	SC	Rate	Time	Found
R	2013-03-19	UDP/16471	zeroaccess	40,448	1	10	1.2h	55 **(0.13%)**
I	2013-05-03	UDP/16471	zeroaccess	2,6B	4	50,000	3.6h	7,884 **(0.0003%)**

Related Work

Scanning:

- Leonard et al. IMC ‘10
- Heninger et al. Usenix Security ’12
- Zmap

Fingerprinting:

- FiG
- PeerPress

Signature Generation:

- Honeycomb, Autograph, EarlyBird, Polygraph, Hamsa
- Botzilla, Perdisci et al., Firma

Conclusion

- Novel active probing approach for Internet-scale detection of malicious servers
- Novel adversarial fingerprint generation technique
- Implement approach into CyberProbe
- Use CyberProbe for 24 localized and Internet-wide scans
  - Identifies 151 malicious servers
  - 75% of the servers unknown to databases of malicious activity (e.g., VirusTotal, UrlQuery)
  - Identifies provider locality property

Thanks!

Future Work

- Scanner IP diversity
- Completeness
- Shared hosting (i.e. CDN)
- Complex protocol semantics