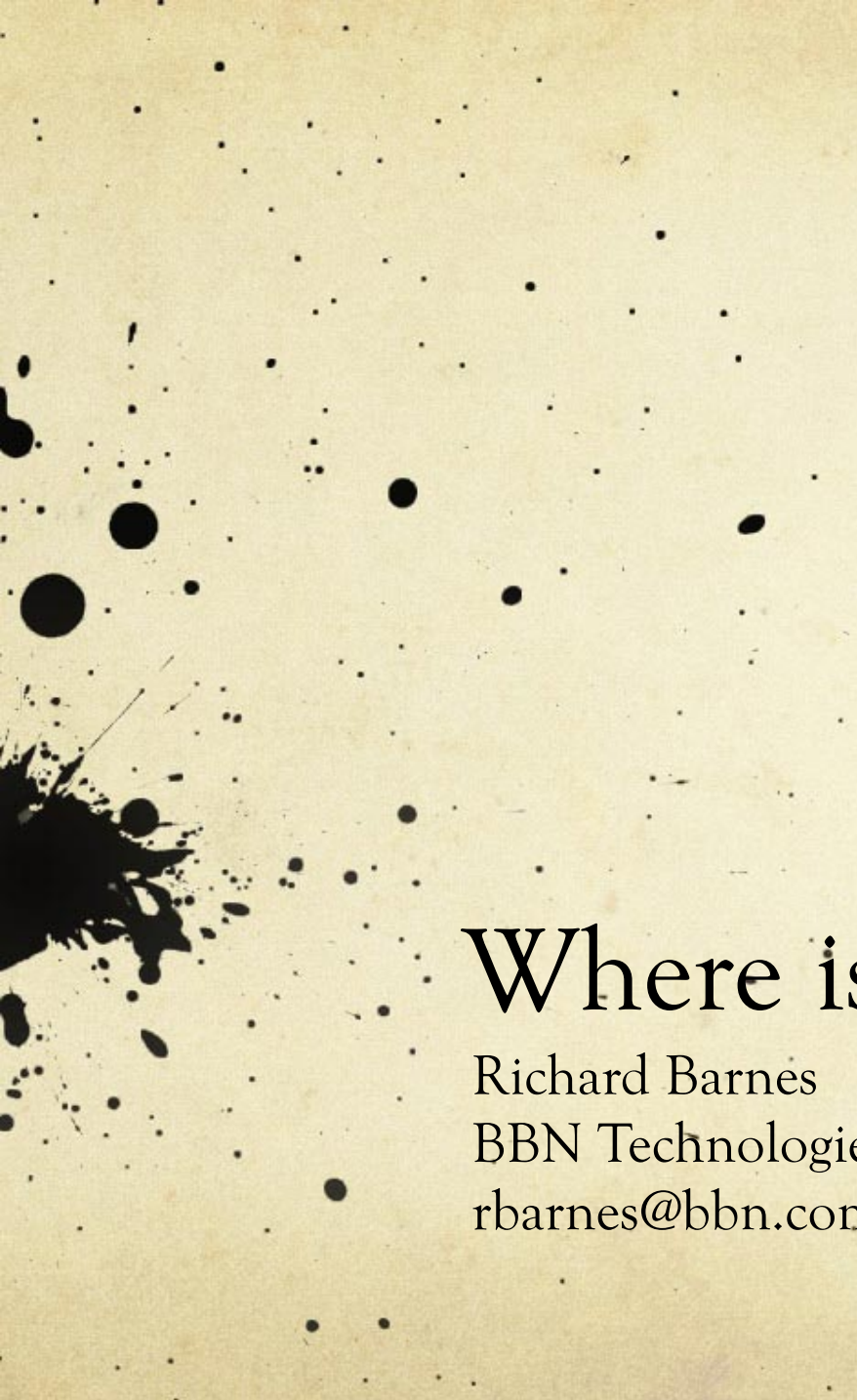


Where is the IPv6 network?

Richard Barnes
BBN Technologies
rbarnes@bbn.com

IPv6 is Big

- Supposing we view a /48 as functionally similar to a /24...
  - IPv4: 12,577,420 /24s advertised ($\sim 2^{23.6}$)
  - IPv6: 3,523,931,041 /48s advertised ($\sim 2^{31.7}$)
    - ... and that's with the current level of IPv6 deployment
    - ... and really, /48s get subdivided too
- Prefixes in BGP cover huge swaths of addresses
- How do we understand the network?
  - How "**big**" is an AS?
  - What parts of the address space are **actually in use**?

Network Measurement

- Passive measurement is not so helpful
  - BGP hides most of the interesting information
  - NetFlow would help, but only within a limited scope
- How about active measurements?
  - Ping, traceroute, etc.
  - How do you choose where you send traces?
    - Current SOTA: Random per BGP prefix

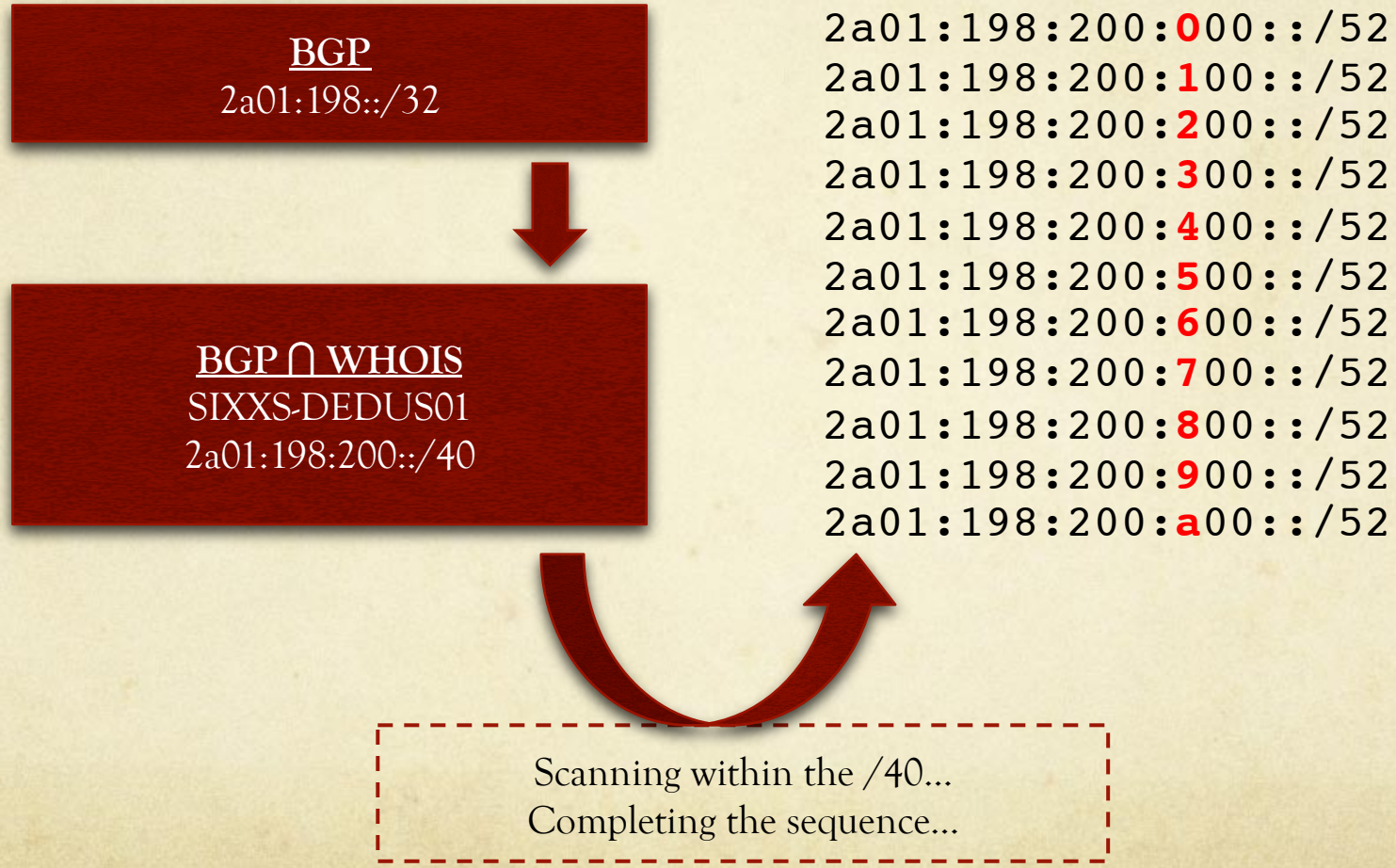
Going beyond BGP

- To tell two networks apart in measurements, we need to trace to a target in each of them
- Finding networks via pure random scanning within BGP-announced prefixes doesn't scale
- Start with BGP, add more information
  - 4 bits of randomness
  - Registration information (WHOIS)
  - Information gathered in earlier scans

BGP ∩ WHOIS

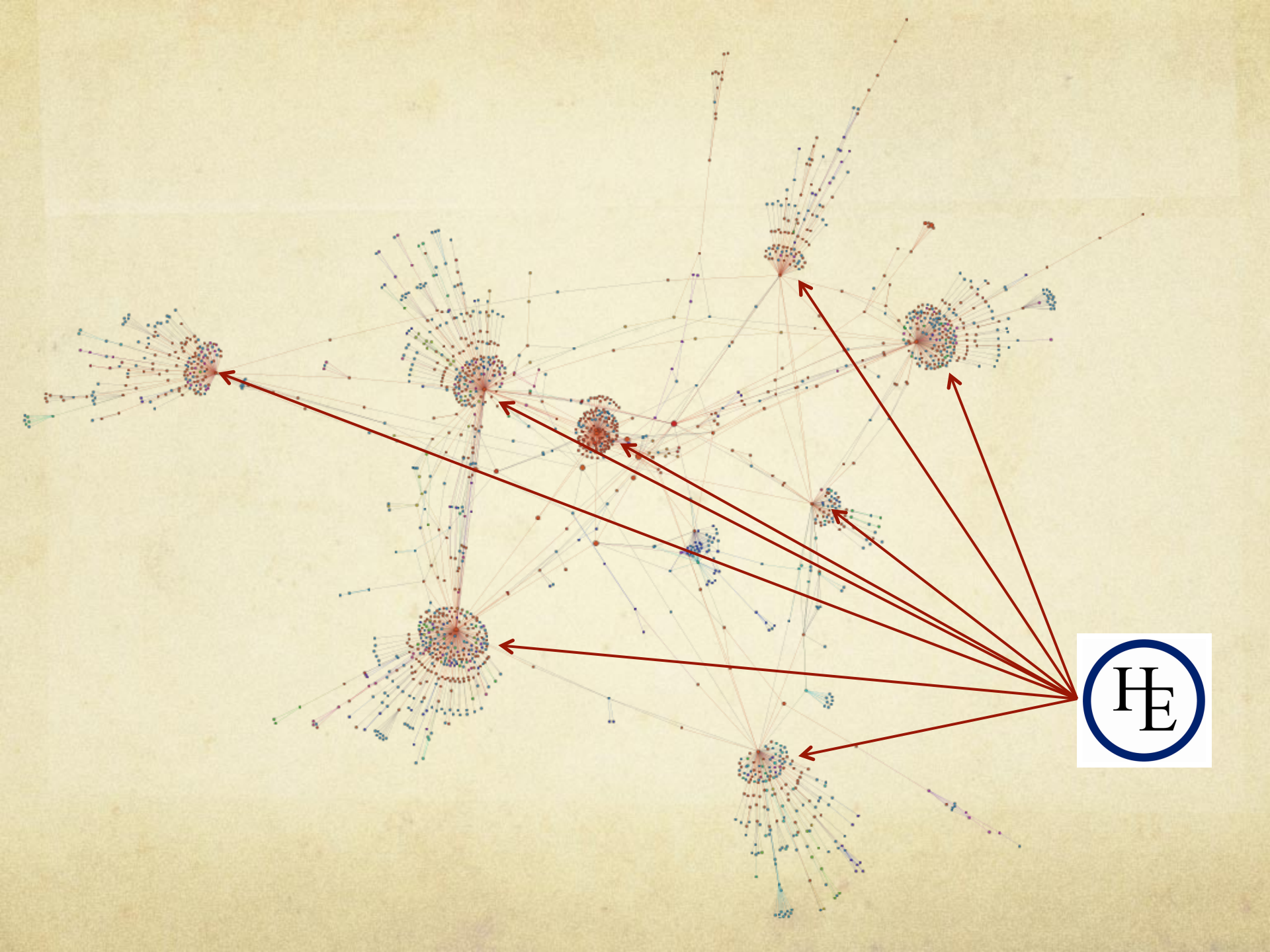
Prefix		Network	BGP	Gain
2a02:f8:7:1a::/64	IT	AISA-NET-1	/32	32
2a01:4f8:141:22::/64	DE	FORMER-03-GMBH	/32	32
2406:4800::/64	SG	DOCOMOinterTouch-HQ-V6	/40	24
2405:2000:ff10::/56	IN	CHN-CXR-TATAC	/32	24
2607:f6f0:100::/56	US	EQUINIX-EDMA-V6-CORP-01	/40	16
2001:42c8:ffd0:100::/56	ZA	CAPETOWN-KLT-TATA	/32	24

Sequence Completion



Testing Methodology

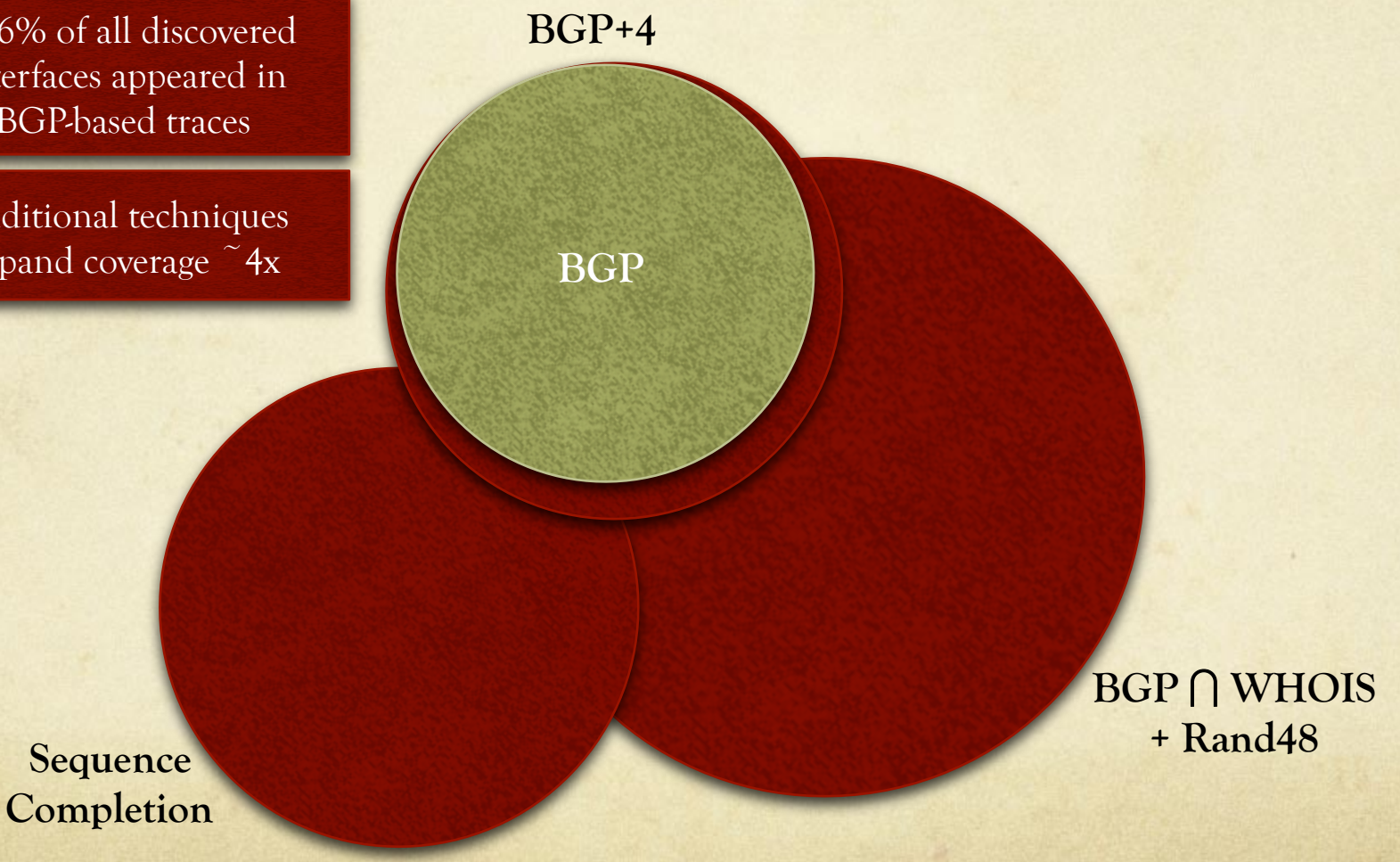
- 5 nodes from commercial VPS services
- ICMP Paris traceroutes to selected targets



Discovered Interfaces

26.6% of all discovered interfaces appeared in BGP-based traces

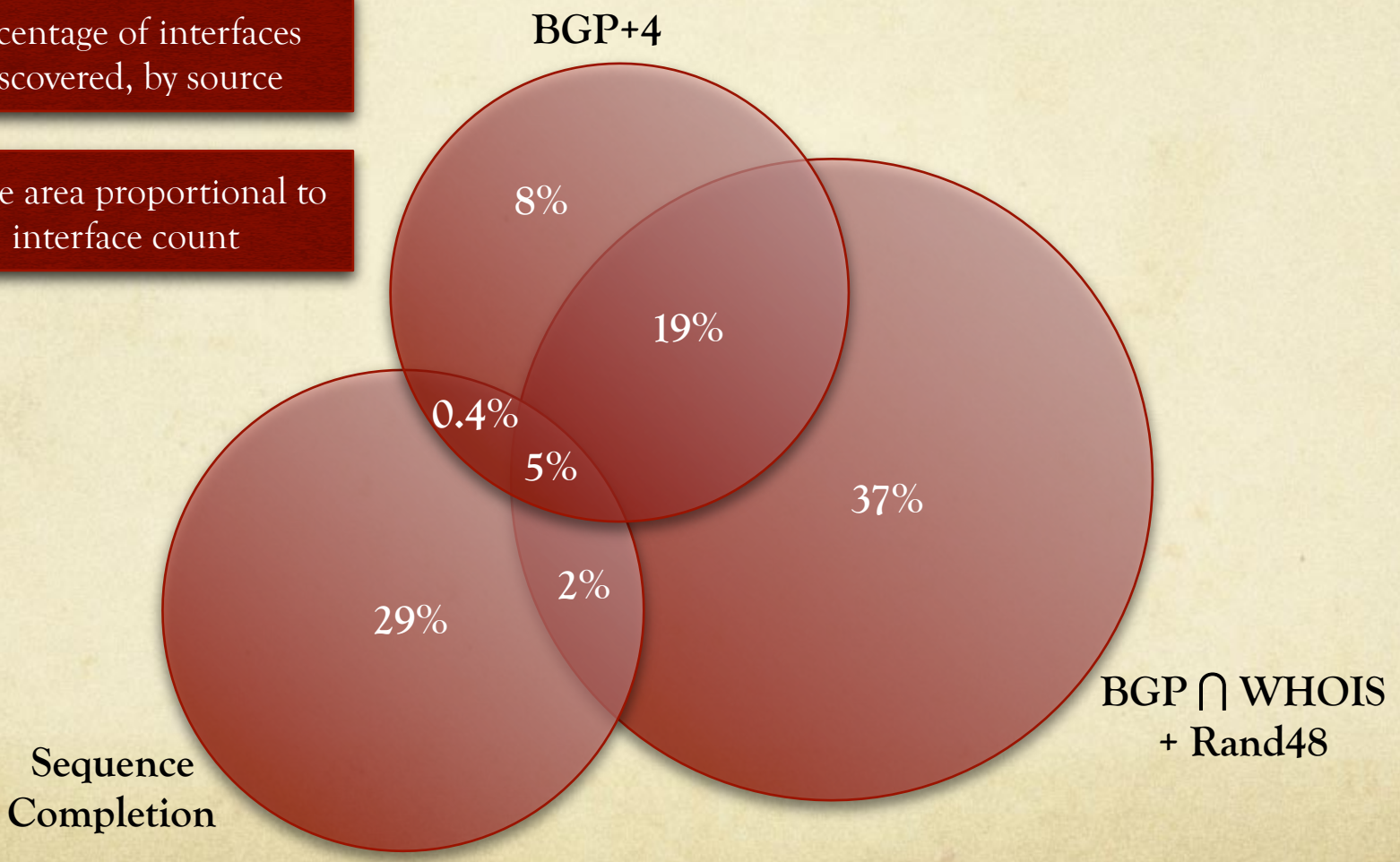
Additional techniques expand coverage ~4x



Discovered Interfaces

Percentage of interfaces discovered, by source

Circle area proportional to interface count



Thanks!

Richard Barnes
rbarnes@bbn.com