DNS Record Injection Vulnerabilities in Home Routers

Kyle Schomp†, Tom Callahan†, Michael Rabinovich†, Mark Allman†‡

†Case Western Reserve University

‡International Computer Science Institute

Attacks targeting DNS resolvers

- Various attempts to poison DNS resolver caches
  - Bailiwick violations
  - Kaminsky vulnerability
- Tempting targets because they handle a large number of clients
  - One successful attack → many victims
- Mitigations for these problems
  - Bailiwick rules nearly universally applied
  - Transaction ID randomization, ephemeral port randomization, 0x20 encoding
    - 16% of resolvers use static ephemeral port – Kaminsky vulnerable

Open resolvers: a (still) growing problem

- openresolverproject.org indicates there are 27 million open resolvers on the Internet!
- Researchers found just 15 million open resolvers in 2008
- Almost doubling in last 6 years
  - (Recent downturn)
- But what are open resolvers?

Leonard, Derek, and Dmitri Loguinov. "Demystifying service discovery: implementing an internet-wide scanner." *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. ACM, 2010.

Many open resolvers are home routers

The evidence	% of Open Resolvers
RomPager embedded web server on port 80	24%
Basic HTTP auth realm header (``3068 DSL-2641R'')	24%
BPL listed by Spamhaus	51%
BPL listed by ISP	17%
DNS response from wrong port (self-NATing)	48%
Total	78%

From a sample of 1 million open resolvers

- Many open resolvers have names from the Alexa top 1,000 in cache
- Used low-end embedded device in residential location

Home routers as simple DNS forwarders

- Accept a request from a device

Device

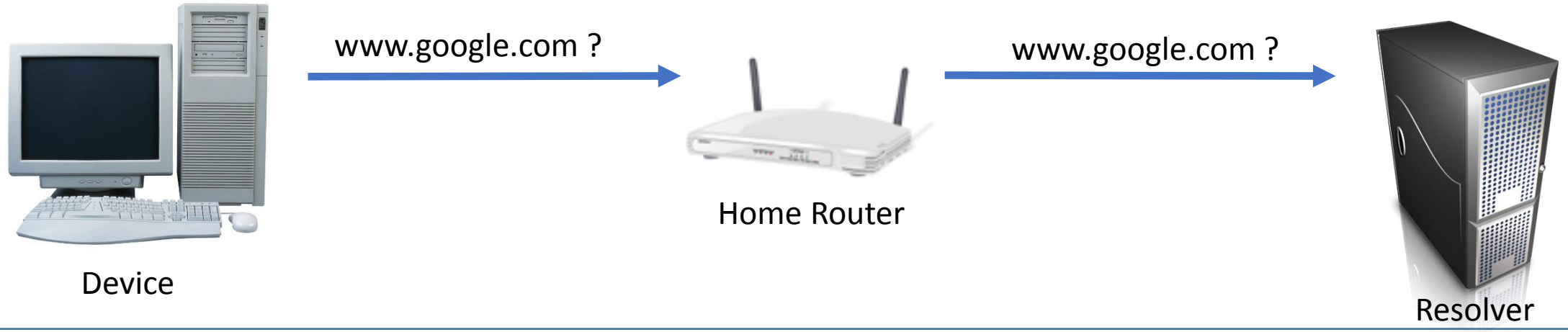
www.google.com ?

Home Router

Resolver

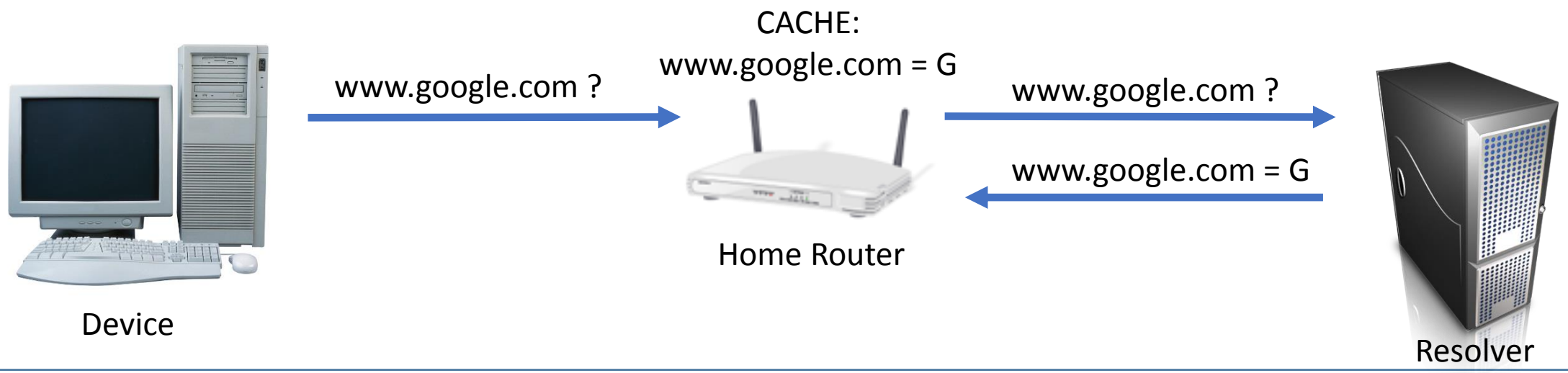
Home routers as simple DNS forwarders

- Accept a request from a device
- Forward the request to an upstream resolver



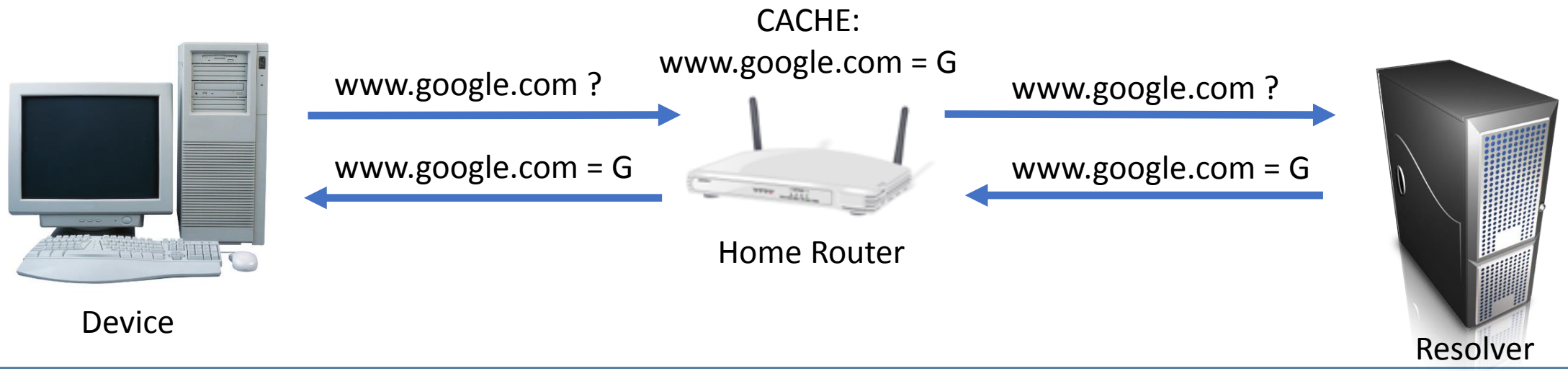
Home routers as simple DNS forwarders

- Accept a request from a device
- Forward the request to an upstream resolver
- Cache the response



Home routers as simple DNS forwarders

- Accept a request from a device
- Forward the request to an upstream resolver
- Cache the response
- Return the response to the device



What could go wrong?

- …besides home routers acting as open resolvers – not a good thing
- Serious vulnerabilities have previously been discovered in resolvers operated by major DNS providers
- Might home routers have DNS vulnerabilities as well?

Preplay vulnerability

Schomp, Kyle, and Tom Callahan, and Michael Rabinovich, and Mark Allman. “Assessing DNS vulnerability to record injection." PAM 2014.

- Many home routers simply do not validate DNS responses
  - Responses accepted from *any* source IP address / port
  - Ephemeral port number not validated
  - Transaction ID either unmodified in forwarding or not validated
- No guessing involved in the attacks at all!
- In open resolver samples, 7-9% have this vulnerability
  - Estimate 2-3 million boxes on the Internet are vulnerable

Example preplay attack

Attacker

www.victim.com ?

Home Router

Device

- Attacker sends request for domain name to poison

Example preplay attack

Attacker

www.victim.com ?

www.victim.com = A

Home Router

Device

- Attacker sends request for domain name to poison
- Attacker immediately sends a response binding to A
  - (before response from shared resolver)

Example preplay attack

Attacker

www.victim.com ?

www.victim.com = A

Home Router
CACHE:
www.victim.com = A

Device

- Attacker sends request for domain name to poison
- Attacker immediately sends a response binding to A
  - (before response from shared resolver)
- The home router inserts the binding into its cache

Example preplay attack

Attacker

www.victim.com ?

www.victim.com = A

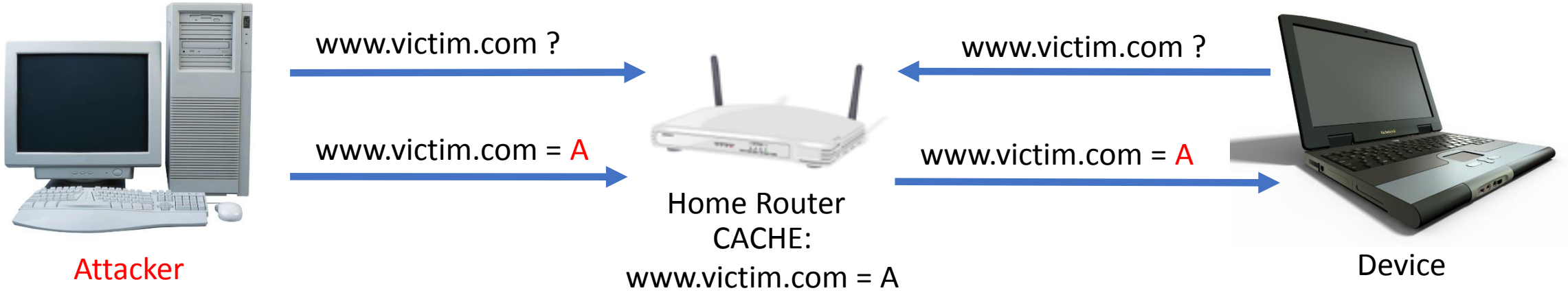
Home Router
CACHE:
www.victim.com = A

www.victim.com ?

Device

- Attacker sends request for domain name to poison
- Attacker immediately sends a response binding to A
  - (before response from shared resolver)
- The home router inserts the binding into its cache
- Client device subsequently requests domain name

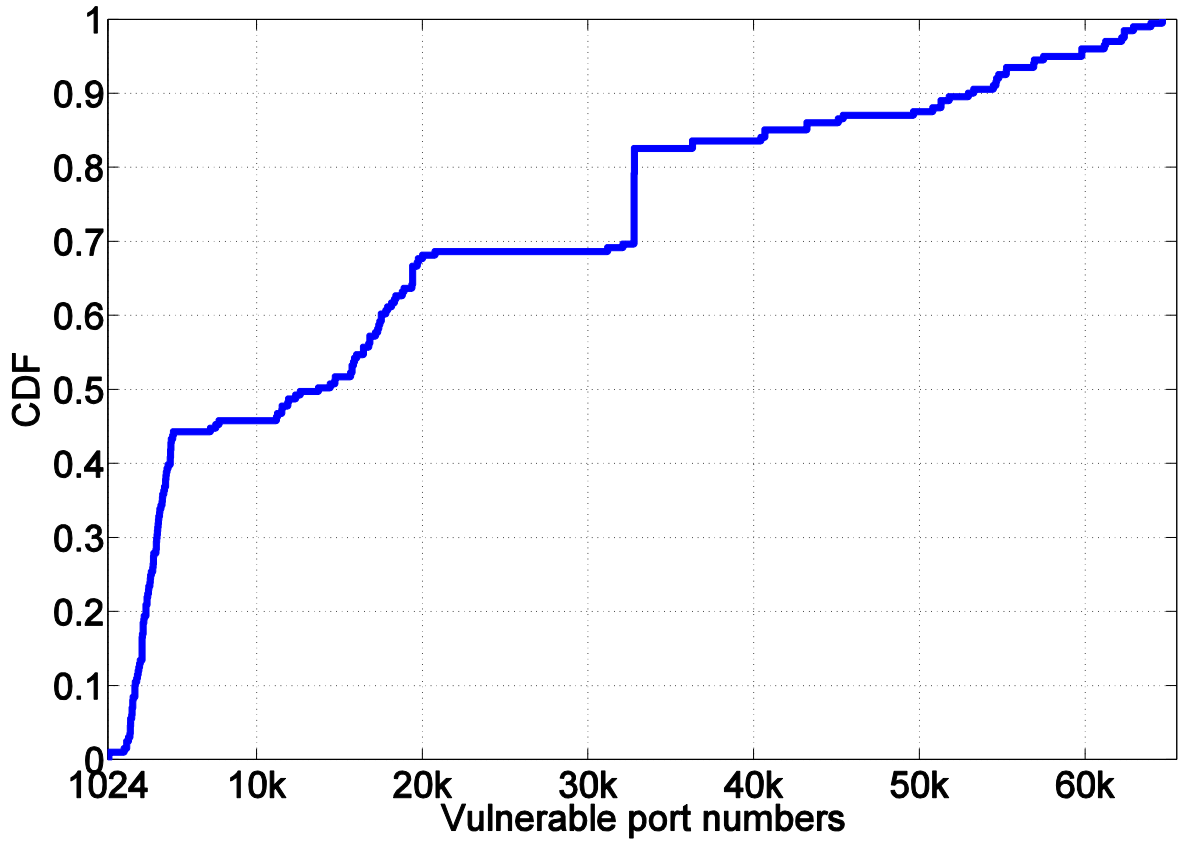
Example preplay attack



- Attacker sends request for domain name to poison
- Attacker immediately sends a response binding to A
  - (before response from shared resolver)
- The home router inserts the binding into its cache
- Client device subsequently requests domain name
- Receives poison

But there's more…

- Preplay vulnerability doesn't require any guessing
- Another 7-10% of home routers are only protected by a variable port number
- Guessing the correct port number from [0,65535] is hard
- But the selected port number may not be random



Why poison home router caches?

Attack on major DNS resolver

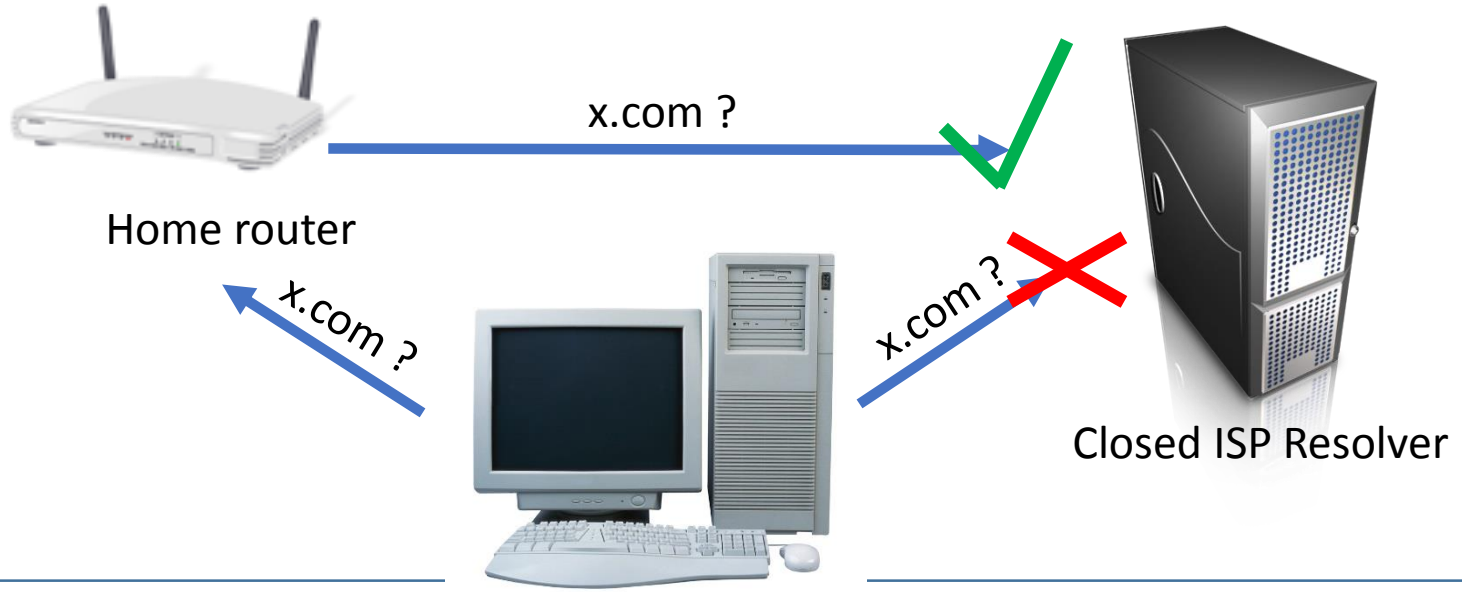
- Complex attack
- Affects potentially thousands
- Detectable via IDS
- Poison whole domains

Attack on home router

- Trivial to launch
- Single household affected
- No one’s watching
- Poison single query string

Home routers putting us at risk

- Record injection not the only reason home routers are dangerous
- Reflection / DNS amplification attacks because they are open
- Indirect attacks on closed portions of the resolver infrastructure



What can we do about this?

- Home router software doesn’t get updated
  - Wait a few years for hardware update
  - Future models could have an automatic update feature
  - Vendors can push security updates
- UDP/53 blocking to residential IP address ranges
  - Nearly all home routers only accept DNS requests on port 53
    - Blocking would be effective
  - *Some* use port 53 as the ephemeral port
    - Care must be taken not to block their legitimate traffic
    - Make exceptions for popular public DNS resolvers (i.e., 8.8.8.8)
  - Might block other legitimate client traffic

CASE WESTERN RESERVE UNIVERSITY EST. 1826

INTERNATIONAL COMPUTER SCIENCE INSTITUTE

Thank you! Questions?

Kyle Schomp – kgs7@case.edu