software studio

finishing the story

Daniel Jackson

changing tracking for redirects

when response is redirect

- why not mark origin as redirecting server?
- because attacker could use open-redirects

what's an open redirect?

- apps often use redirects with URLs as query params

  eg: http://mysite.com?d=mysite.com&p=login
- developer may have forgotten to check URLs

  eg: can issue http://mysite.com?d=attacker.com

so what to do?

- can track a set of origins; add redirector to the set

what actually happened

and where this lecture came from

origin policy

- proposed in paper by Adam Barth from Google (2008)
- redirect bug discovered later; reviewers missed it

alloy model of web security

- confirmed bug in their own origin policy
- analyzed 4 others (referrer, HTML5, WebAuth, CORS)
- found unknown vulnerabilities in 3!

http://seclab.stanford.edu/websec/

Robust Defenses for Cross-Site Request Forgery
Adam Barth, Collin Jackson, and John C. Mitchell
15th ACM Conference on Computer and Communications Security, 2008

http://tools.ietf.org/html/rfc6454

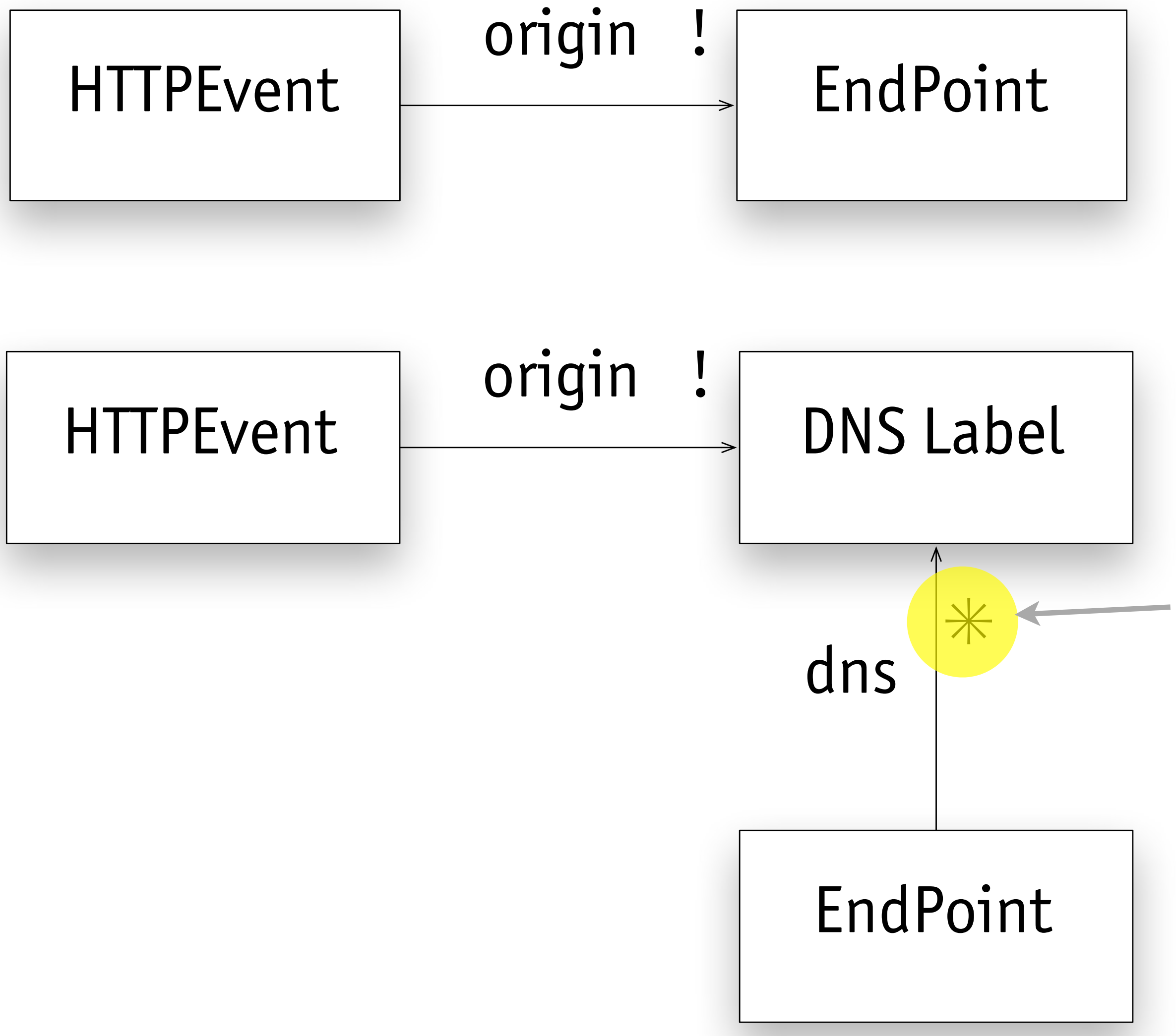
Towards a Formal Foundation of Web Security
Devdatta Akhawe, Adam Barth, Peifung E. Lam, John C. Mitchell, and Dawn Song
23rd IEEE Computer Security Foundations Symposium, 2010

real model was more complex

example: what origin header holds

› our model: identity of end point

› in reality: DNS label + protocol + port

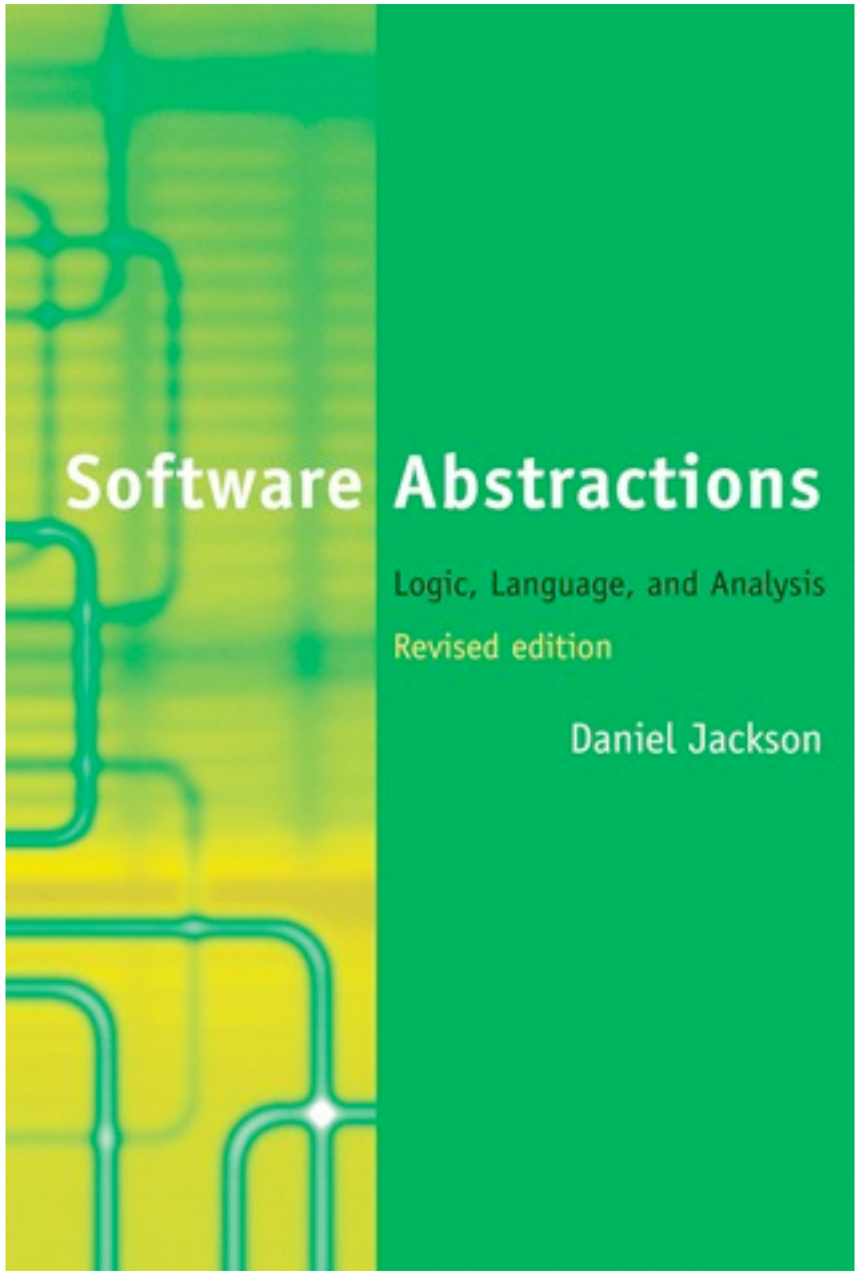


our model

more realistic model

DNS rebinding!

Alloy



Software Abstractions: Logic, Language, and Analysis, by Daniel Jackson, published by The MIT Press. Used with permission.

developed at MIT

- latest version Alloy 4
- 2d edition of book (2012)

community site

- http://alloy.mit.edu

book site

- http://softwareabstractions.org

annual conference

- ABZ

alloy applications

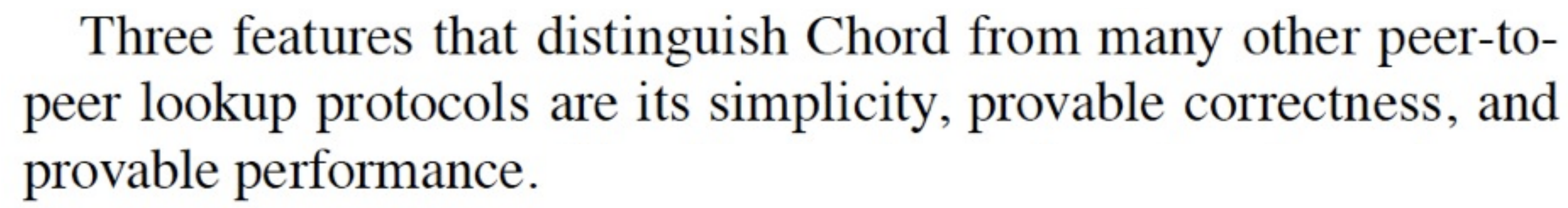
in design analysis

- access control schemes
- network protocols
- web ontologies
- software architectures
- flash file systems
- electronic voting

in configuration

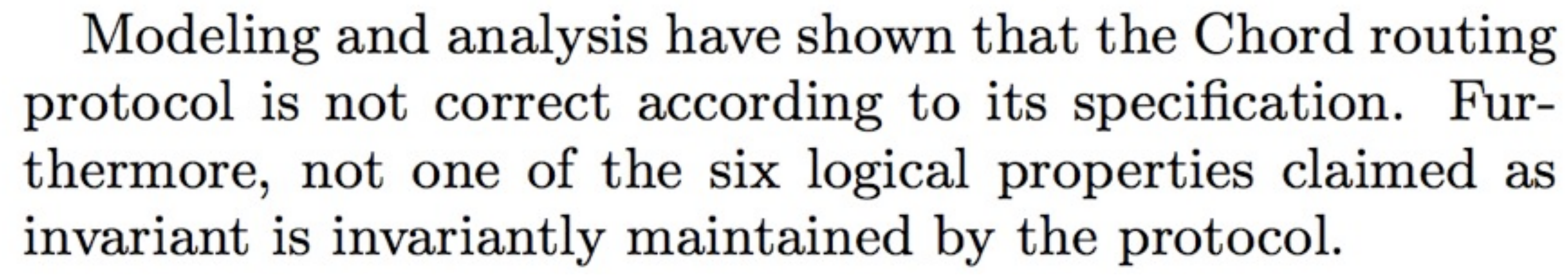
- network settings
- data structure repair
- Facebook security settings
- test case generation

a typical Alloy story



Three features that distinguish Chord from many other peer-to-peer lookup protocols are its simplicity, provable correctness, and provable performance.

Ion Stoica et al. Chord: A Scalable Peer to Peer Lookup Service for Internet Applications, SIGCOMM 2001 (also TON, 2003)



Modeling and analysis have shown that the Chord routing protocol is not correct according to its specification. Furthermore, not one of the six logical properties claimed as invariant is invariantly maintained by the protocol.

Pamela Zave. Invariant-Based Verification of Routing Protocols: The Case of Chord, 2009

lessons

- security is hard!
- better to use trusted platform than DIY
- testing & review not enough
- modeling is high bang/$

6.170 Software Studio
Spring 2013