finishing the story

Daniel Jackson
what actually happened

and where this lecture came from

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

Robust Defenses for Cross-Site Request Forgery
Adam Barth, Collin Jackson, and John C. Mitchell

Towards a Formal Foundation of Web Security
Devdatta Akhawe, Adam Barth, Peifung E. Lam, John C. Mitchell, and Dawn Song
what actually happened

origin policy
› proposed in research paper, 2008
› like referrer, but domain only & sent only for POSTs
› redirect bug discovered later; reviewers missed it

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

Robust Defenses for Cross-Site Request Forgery
Adam Barth, Collin Jackson, and John C. Mitchell

Towards a Formal Foundation of Web Security
Devdatta Akhawe, Adam Barth, Peifung E. Lam, John C. Mitchell, and Dawn Song
what actually happened

origin policy

› proposed in research paper, 2008
› like referrer, but domain only & sent only for POSTs
› 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

Towards a Formal Foundation of Web Security
Devdatta Akhawe, Adam Barth, Peifung E. Lam, John C. Mitchell, and Dawn Song
real model was more complex
real model was more complex

example: what origin header holds
  › our model: identity of end point
  › in reality: DNS label + protocol + port
real model was more complex

element: what origin header holds
  › our model: identity of end point
  › in reality: DNS label + protocol + port
real model was more complex

example: what origin header holds
  › our model: identity of end point
  › in reality: DNS label + protocol + port
real model was more complex

example: what origin header holds
  › our model: identity of end point
  › in reality: DNS label + protocol + port
ALLOY

MODELING SECRETS REVEALED!
MODELING SECRETS REVEALED!

Supermodel Spills All...

Model Kate Dillon is signed with Wilhelmina — one of the top agencies in the world — and has appeared in American, French, and Italian issues of Vogue. She’s also been named Mode magazine’s Model of the Year, and once graced People’s pages in their annual "50 Most Beautiful People" feature. The best part? Kate’s achieved all these things as a plus-sized beauty! Not bad for a girl who started out as a skinny model and struggled with anorexia for years... To find out more about this candid cutie, and hear her inspiring story, peep our one-on-one interview!
Alloy

developed at MIT
› since 1997
› latest version Alloy 4
› new book this fall
Alloy

developed at MIT
› since 1997
› latest version Alloy 4
› new book this fall

community site
› alloy.mit.edu
Alloy

developed at MIT
› since 1997
› latest version Alloy 4
› new book this fall

community site
› alloy.mit.edu

book site
› softwareabstractions.org
Alloy

developed at MIT
› since 1997
› latest version Alloy 4
› new book this fall

community site
› alloy.mit.edu

book site
› softwareabstractions.org

annual conference
› ABZ
alloy applications
alloy applications

in design analysis
› access control schemes
› network protocols
› web ontologies
› software architectures
› flash file systems
› electronic voting
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
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)*
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
lessons

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