Securing Software Ecosystem Architectures: Challenges and Opportunities

Walt Scacchi and Thomas A. Alspaugh

INSTITUTE *for* SOFTWARE RESEARCH
UNIVERSITY *of* CALIFORNIA · IRVINE

Overview

- Securing Open Architecture Command & Control Systems
- Improve security of OA software ecosystem processes
- Visually modeling (mapping) OA ecosystems
- Using architectural description language (ADL) tools and analysis techniques to model and identify OA ecosystem security vulnerabilities

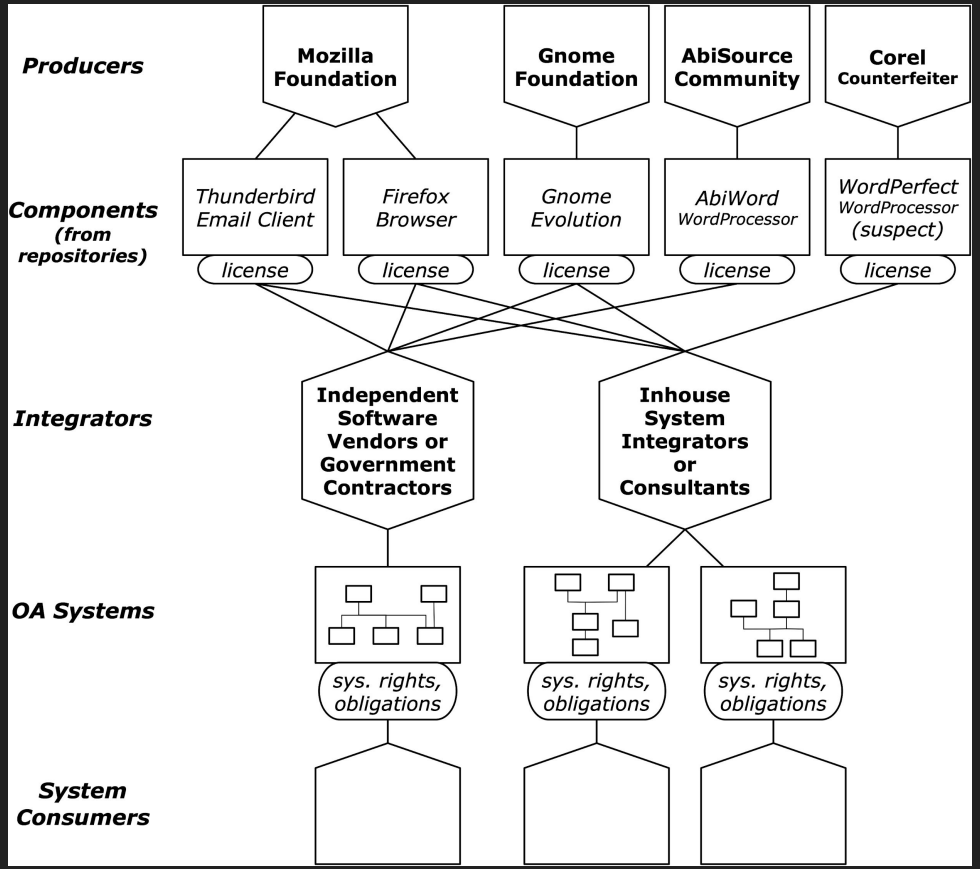
Command & Control Systems: Physical and Virtual

W. Scacchi, C.Brown, K. Neis. Exploring the Potential of Virtual Worlds for Decentralized Command and Control, *17th Intern. Command and Control Research and Technology Symposium (ICCRTS),* Paper-096, Fairfax, VA, June 2012.

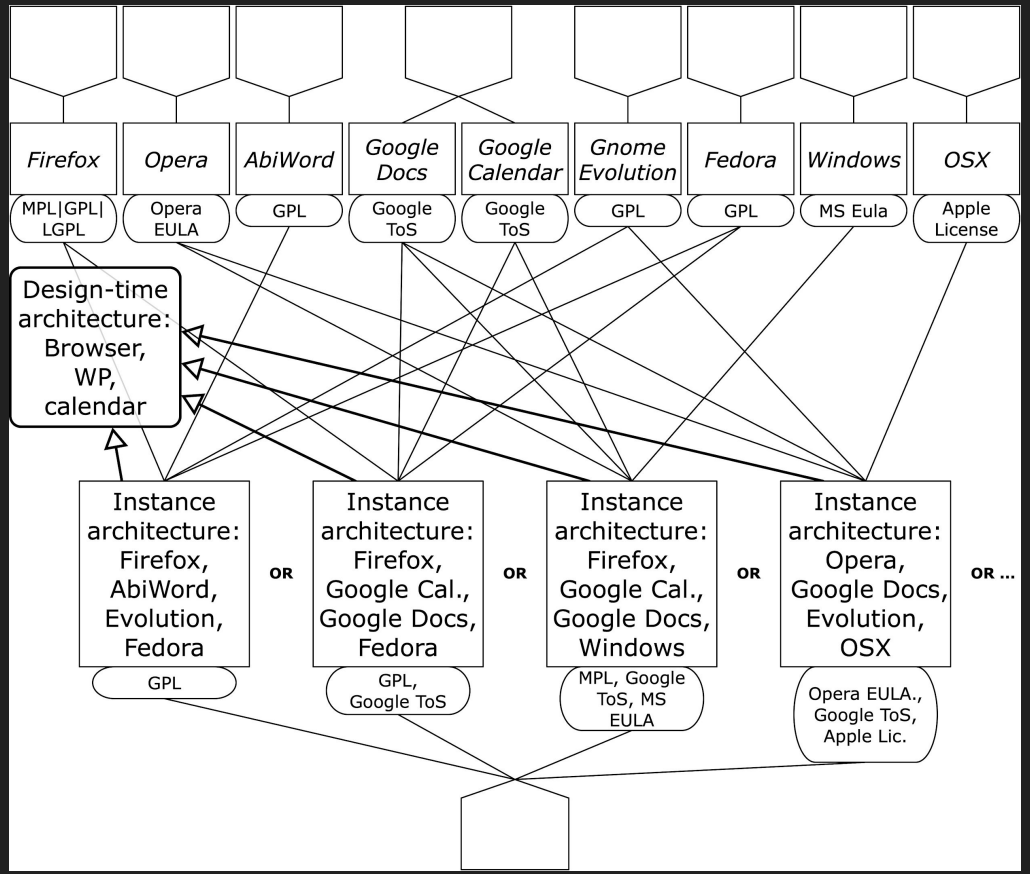
Table 1. Software supply chain security threats and defenses, organized by supply chain process.

Software supply chain processes	Common ecosystem security problems for each process	Example threats to the supply chain[1]	Software supply chain security defenses[1,12,13]	Further defenses enabled by explicit OA[1,2]	Challenges in progressing to the next software supply chain process[1,12,13]
Component sourcing	Untrusted or corrupt software producers	Counterfeit repositories for sourced components[7]	Independent validation of components and interconnections	Validation of provenance in component supply chains	Independent validation of components sourced from unknown providers
Continuous integration and release[1,2]	Infected or corrupt component producers	Counterfeit components in commercial products[7]	Component provenance tracking and analysis	Re-creation of multiversion builds to validate software product integrity	Collecting and passing on provenances, taggants, and other information for evaluation
Delivery and deployment[1,2]	False flag download sites, bait-and-switch downloads	Counterfeit software with false certificates[6]	Installation of components into security encapsulations	Maps of installed software configurations to guide defenses	Producing and delivering trustable, verifiable packages
Continuous evolution[11,12]	Outdated component versions with known vulnerabilities	Update mechanism hijacked to enable remote control and data exfiltration[5]	All of the defenses listed	Repositories listed, deployment of multiversion releases	Maintaining security, trust, provenance, and other requirements as ecosystem and configurations evolve

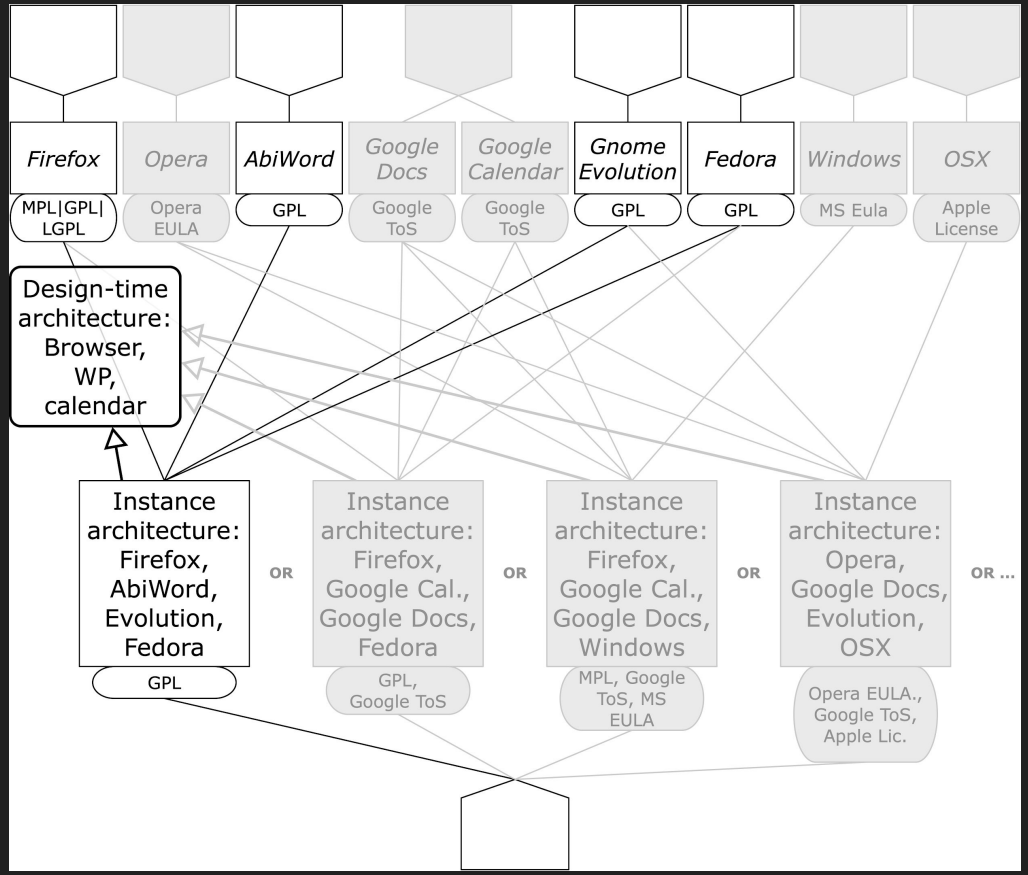
Software Ecosystem Supply Network



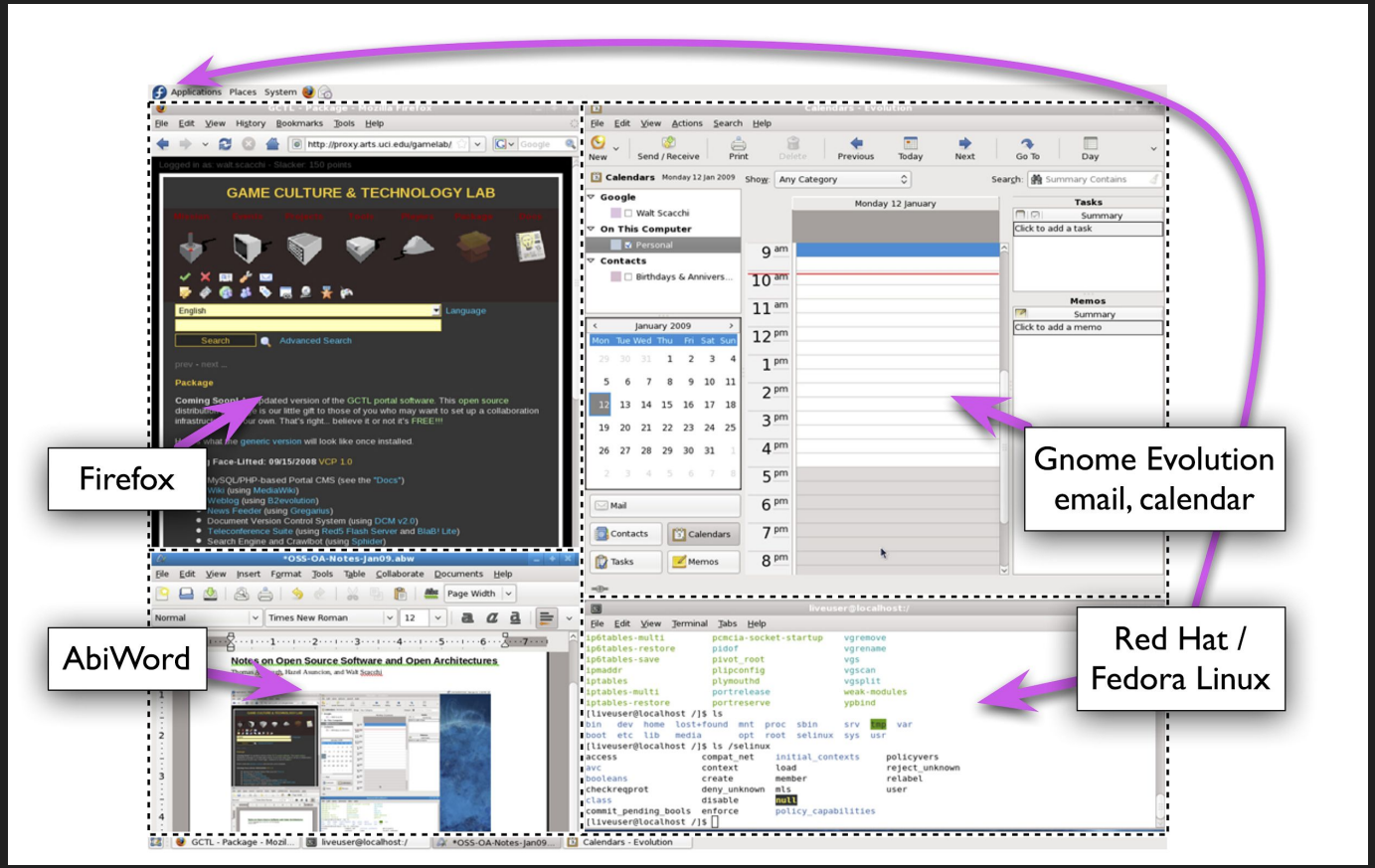
OA Ecosystem Product Line Supply Chains



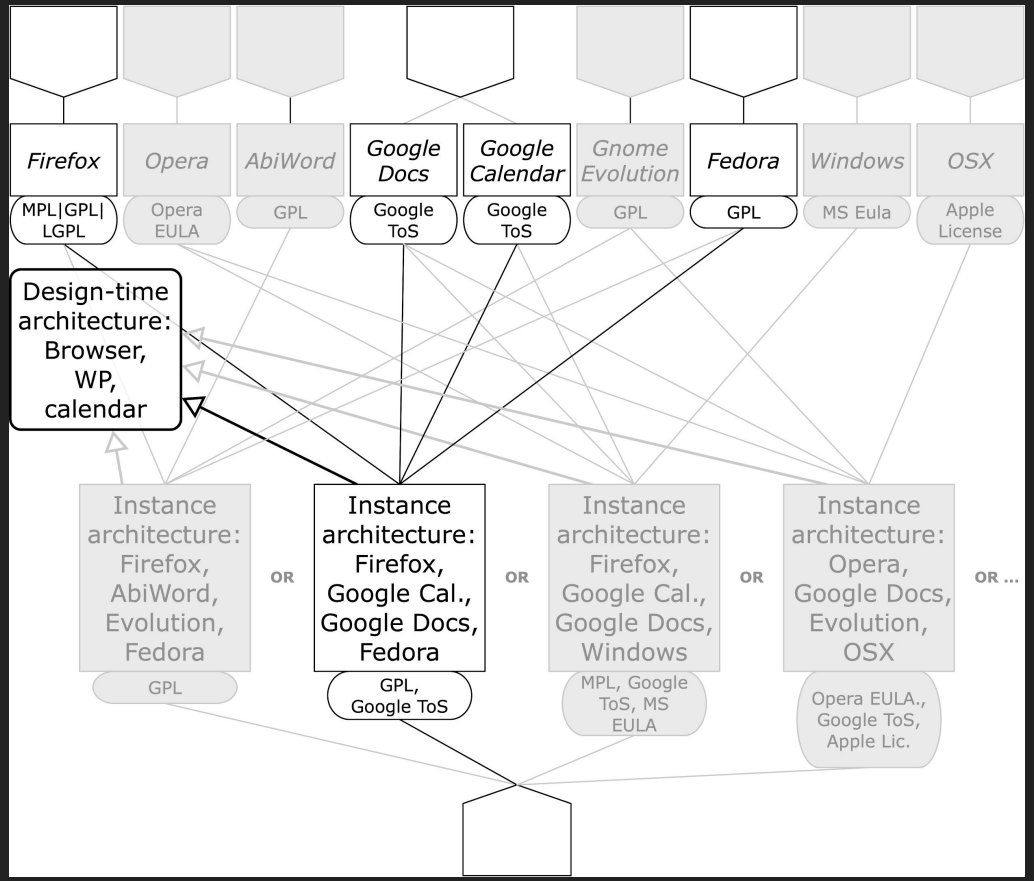
An OA Ecosystem Product Supply Chain

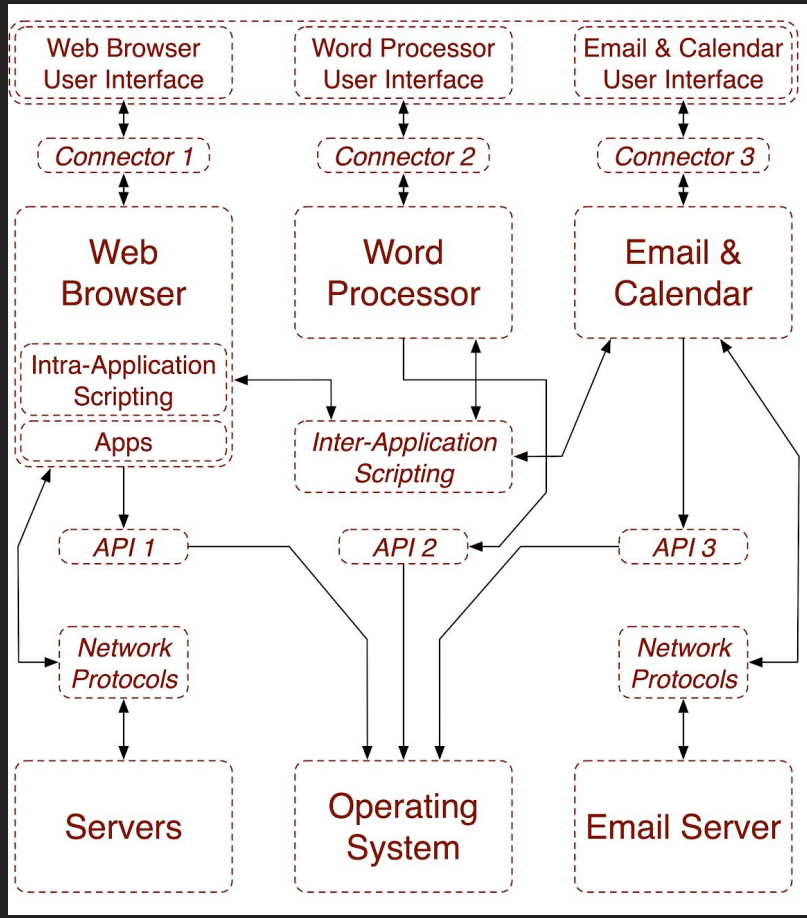


OA Ecosystem Instance Configuration

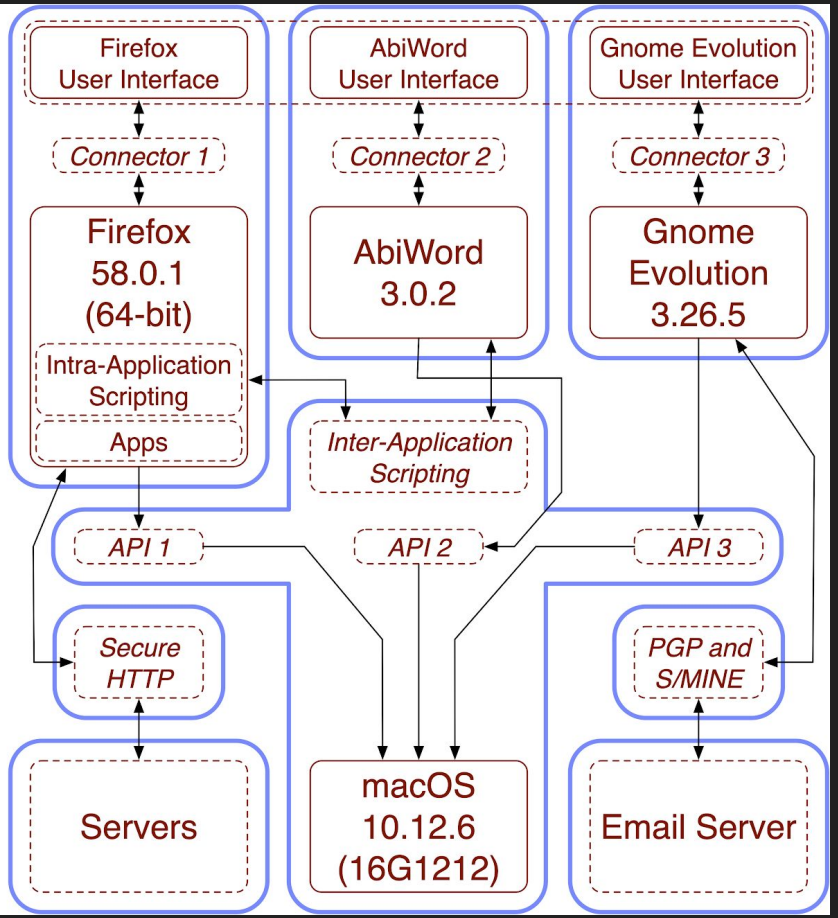


Alternative OA Ecosystem Product Supply Chain



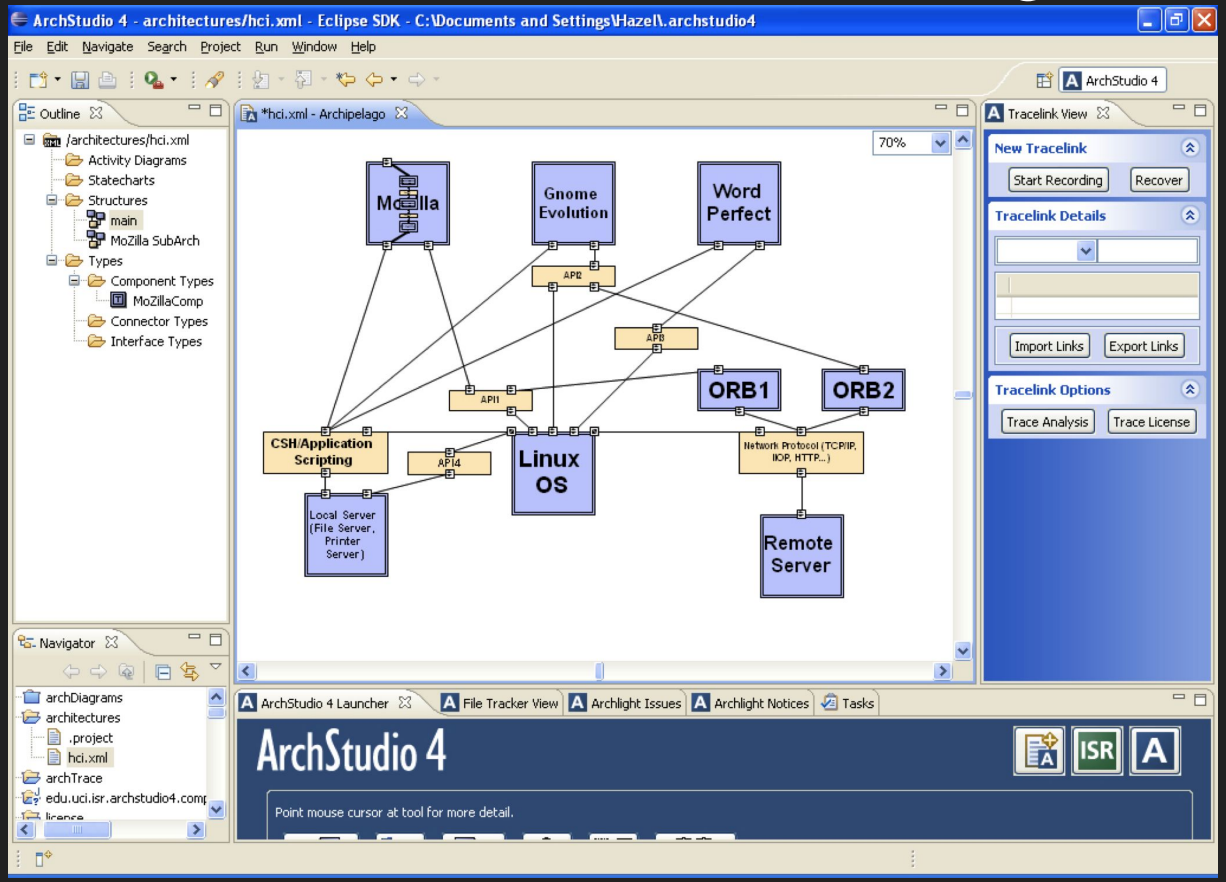


Abstract OA Ecosystem Map



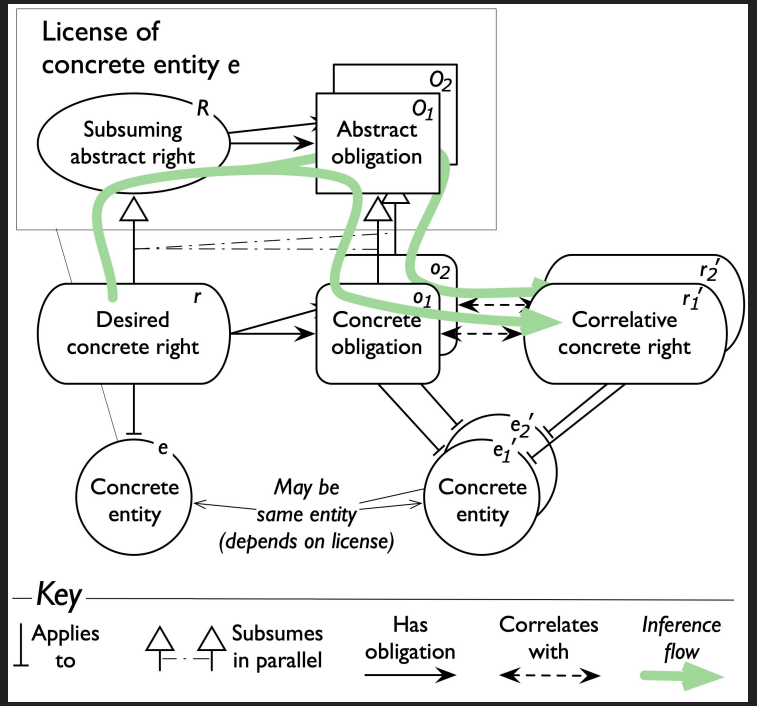
Concrete OA Configuration Map

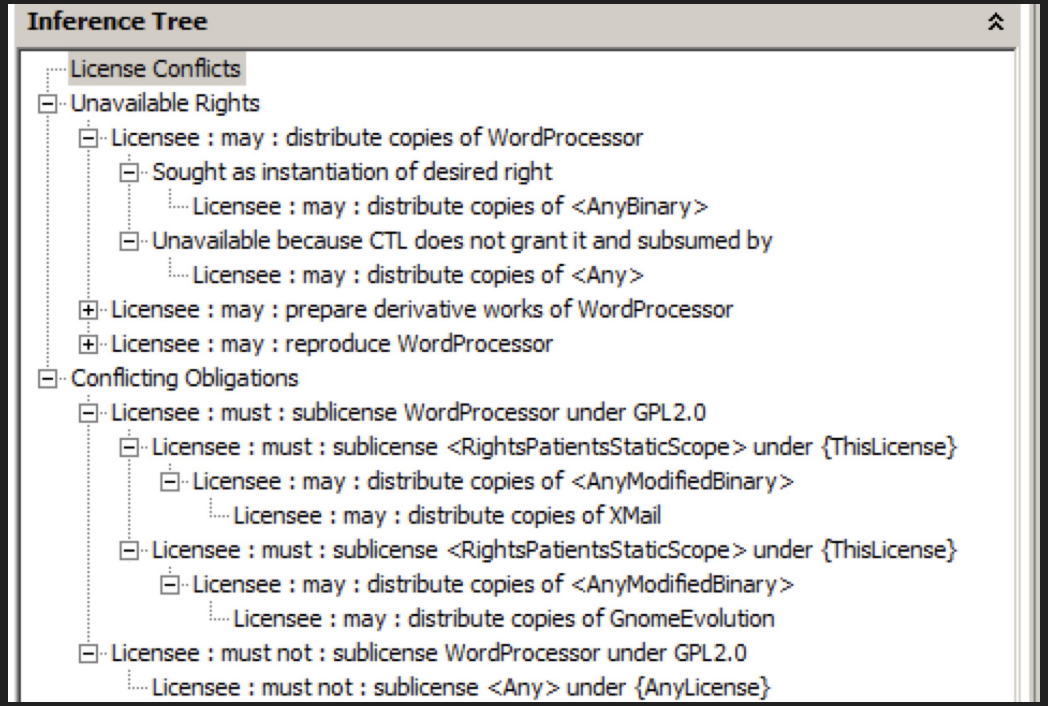
ArchStudio 4 OA Modeling



R. N. Taylor, N. Medvidovic, and E. M. Dashofy, *Software Architecture: Foundations, Theory, and Practice*, Hoboken, NJ: Wiley, 2009.

ADL-based IP / Security License Analysis Capability





T.A. Alspaugh and W. Scacchi. Licensing Security, *Proc. Fifth Intern. Workshop on Requirements Engineering and Law*, 25-28, September 2012. Also see, T.A. Alspaugh, H. Asuncion, and W. Scacchi, Presenting Software License Conflicts through Argumentation, *Proc. 22nd Intern. Conf. Software Engineering and Knowledge Engineering* (SEKE2011), 509-514, Miami, FL, July 2011.

Conclusions

- Open Architecture and software ecosystem maps are **useful to identify where and when security vulnerabilities occur**
- OA ecosystem maps serve as **reference models**
- **OA maps**: abstract or concrete (detailed)
- OA **maps reveal where and how system configurations are potentially modified during each supply chain process**
- Use **Architectural Description Languages** (ADLs) to specify, visually map, analyze, and update software architectures

Acknowledgements

This research was supported by grants N00244-16-1-0004 and N00244-16-1- 0053 from the Acquisition Research Program at the Naval Postgraduate School, Monterey, California. No endorsement implied.