Hua Li

condorlee@hotmail.com • 408-421-9330 • Sunnyvale, CA

linkedin.com/in/hua-li-24757937

Summary

Proven software engineering lead and application security architect of large-scale complex cloud service with multi-million users across the globe.

Extensive skills on software architecture and coding, especially on automated program analysis; lead and hands on all technical and process aspects of secure development; rich experience of collaboration with cross functional teams, thousands of employees from different time zones.

Please see part 2 of this resume, a technical brief of AmberEye (the program analysis solution I created).

Skills

Development: Automated Program Analysis (Java, 6 years), Cloud service (Java/J2EE/JavaScript, 4 years), Computer Game (Windows C/C++, 5 years), Linux server (Linux C, 3 years)

Programming Languages: C/C++, Java, JavaScript, etc., can learn and code with new language in same day

Platforms: Web 10 years, Windows 5 years, Linux 3 years, Mobile(J2ME) 1 year

Application security : 10+ years, cover all technical and process aspects, include but not limited to:

- Initiate & drive SDLC process, create coding & testing guidelines, security architecture, design, threat modeling, code review, penetration testing, incident response, cross functional team collaboration, etc.
- XSS, CSRF, SSRF, SQL injection, buffer overflow, access control, etc. security risks (OWASP top 10, SANS top 25, etc.) which related to web, native, client and mobile applications
- Cryptography, TLS, PKI, etc. / PCI, GDPR, etc. security compliances & standards

Other Skills: Technical lead, cross functional team collaboration, SAST, DAST (white and black box automated security testing), system hardening, cloud & network security(Load Balancer, Firewall, ACL, etc.), program instrumentation, software architect, CI/CD, performance tuning, trouble shooting, etc.

Work Experience

Amber Technology, February 2016 - Present

It is a startup company which focuses on **AmberEye**, an automated program analysis product with one-of-its-kind technology built from scratch. The tool started as a runtime instrumentation & code analysis solution that integrated into target application, then transformed to a standalone one. The company started with 3 people, topped at 11 people (9 engineers, 1 sale, 1 operation). **AmberEye** now supports Java, C/C++/Objective C, .NET, Python, PHP, Scala, etc. languages., supports IDE plugin, CI/CD integration, as well as web portal.

Role: Founder

Responsibility: As chief architect and product manager of AmberEye, define the product workflow, modules, and features, build the overall technical architecture as well as core program an alysis algorithms. As CEO of the company, define company business, operational as well as technical roadmap, guide and lead all employees.

VMware, June 2015 - February 2016

Role: Staff security engineer

Responsibility: Lead application security work of MSBU for VMware. The BU has about 1000 software engineers, 6 application security engineers. As the technical leader / go-to-person for them for all security related challenges and problems.

RingCentral, March 2015 - June 2015

Role: Application security architect

Responsibility: Lead / hands on SDLC and technical work for RingCentral application security

Cisco, April 2011 - March 2015

Role: Application security architect

Responsibility: Technically lead Cisco WebEx product SDLC work across multiple engineering teams with 800+ engineers, located in different cities in US and China. Responsibilities include:

- Initiate, plan and drive (waterfall, agile) security guidelines, **process, and roadmap**
- Lead Cisco WebEx all **product security technical work**: security architecture, design, secure coding and code scanning, manual and automated penetration testing, security framework and solution development, vulnerability triage and solution, incident response, compliance, etc.
- Work with **cross-functional teams** (engineering, product manager, cloud service, sales, etc.), discuss and balance security and all other requirements, to ensure successful product / service delivery with well application security built in
- As the go-to-person, handle all internal and **customer** communications on WebEx product security topics

Technology: WebEx SaaS cloud includes thousands of servers across different regions of the world, with web, mobile clients, desktop clients, native servers. Thus, my work included application security of all these domains and technologies

Cisco-WebEx China, July 2007 – March 2011

Role: Team leader and security architect

Responsibility: Worked as security architect, led Cisco WebEx China product security across all engineering teams (web, client, server, mobile) to ensure WebEx product security.

The role in China was very similar to the role in United States except with the below differences:

- Did not handle U.S. side cross-functional team / customer-facing communication - my U.S. dot report boss who was an engineering director handled such communications.
- As WebEx China security team leader directly managed the team (total 7 engineers include me).

WebEx China (acquired by Cisco)**, February 2004 – June 2007**

Role: Senior Software Engineer

Responsibility: As senior member of a team and do Windows client development with Visual C++, web development with JBoss and Java, and Linux C development.

PalmScape, July 2002 – December 2003

Role: Co-Founder, Technical Lead

Responsibility: As co-founder and technical lead of a startup company lead the development of games and applications running on mobile devices

SoftStar(Beijing), July 2000 – July 2002

Role: Technical Lead

Responsibility: Hired as the leader of a computer game development team for SoftStar, one of the best computer game companies in China (like Blizzard entertainment in the world), working on a multi-player, real time strategy game (like StarCraft) development on Windows platform with Visual C++. Created key technologies for the game - native full graphical UI and game display, physical simulation, game world, AI, video, audio, etc.

Sun-USTC, July 1999 – July 2000

Role: Software Engineer

Responsibility: Worked as a software engineer, developed web and native applications on Windows and Linux platform with Visual C++, HTML, JavaScript, Linux C.

Education

September 1995 – July 1999: Bachelor of Computer Science, Anhui State University, China.

I was acknowledged as the best developer and called "the doctor" by my classmates. Whenever their programs had any weird bugs, they came to me for diagnose and I generally helped them in minutes.

During the summer vacation after my 1st grade, I developed a full video computer game - I did everything - the game design, graphic, sound effects, music digital processing, 8K lines of source code, and talks to video and audio hardware directly, the whole game from scratch.

My classmates played this game and loved it. It was year 1996 in China - almost no commercial computer game vendor, no web site or book tells you "How to develop a computer game".

I was coding almost every day during the college. I developed a lot of small tools and computer games during college time and became a "senior engineer" even before graduation.

Industry Event

Presented at OWASP China 2009 with topic "A couple of things about XSS".

After that more of our security team members presented in at OWASP China / OWASP Asia conferences with my encourage and guidance.

Static Code Analysis

The challenges of SAST and how AmberEye tackle them

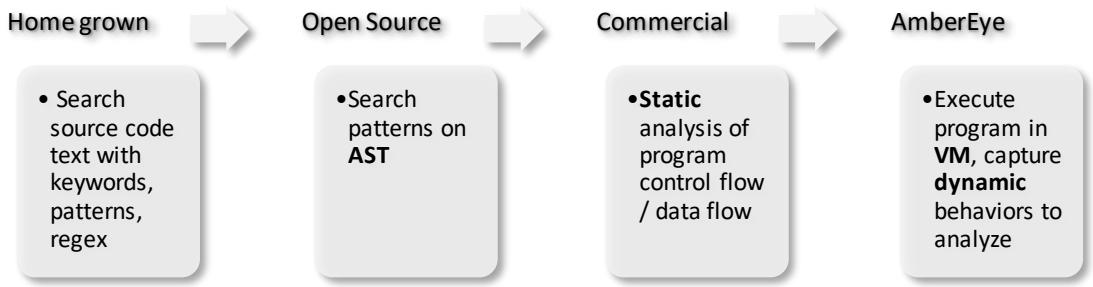
Background

To the industry, human level accuracy of SAST(static code analysis) is a mission impossible in any foreseeable future. Its difficulty is close to, if not as hard as AGI(Artificial General Intelligence). But on the other hand, there are quite a few of solutions out there, including commercial products as well as open-source tools. That's kind of like what happens in the artificial intelligence domain - there are many solutions, although no full solution yet.

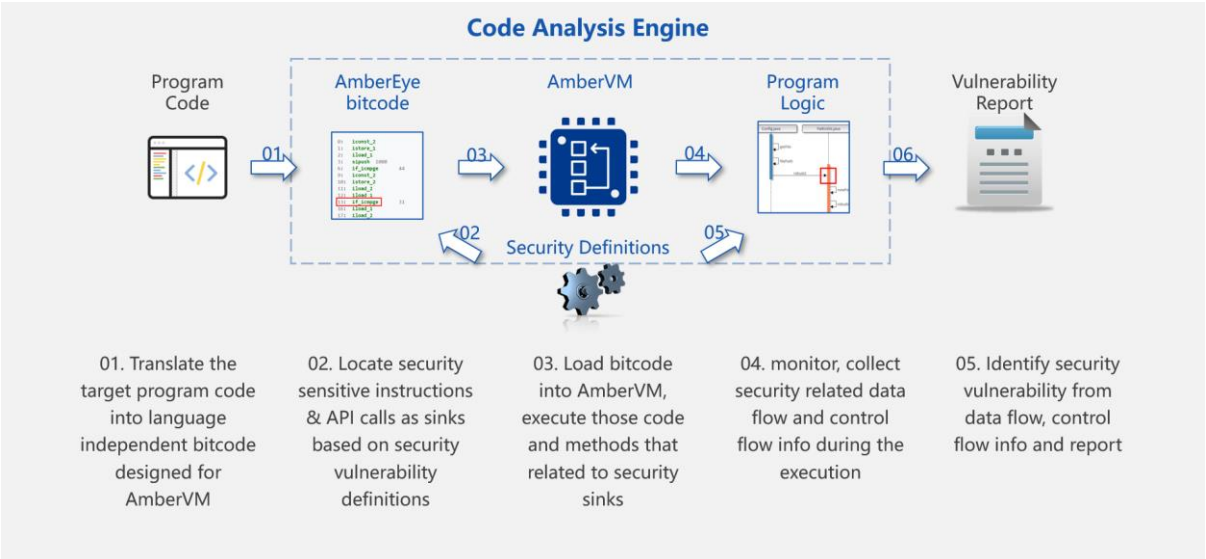
The fact is, the creators as well as the users of SAST(and AI) solutions, mostly are engineers, understand that although SAST tools have a lot of limitations, there are still useful to a certain degree, so these limitations are considered as "acceptable".

With these facts in mind, we created AmberEye, a unique code analysis solution which does not accept, but break most of these limitations.

Code analysis solutions and technologies



The basic workflow of AmberEye



How code analysis challenges are tackled

<table>
<tr><th rowspan="2">The challenges</th><th colspan="2">Answer from Industry Solutions</th><th colspan="2">Answer from AmberEye</th></tr>
<tr><th>Strategy</th><th>Result</th><th>Strategy</th><th>Status</th></tr>
<tr><td>1. The dynamic, complex nature of computer program logics and runtime behavior</td><td>Abstract and analyze dynamic behavior as static data structure like AST, CFG, SSA, lattice, first-order logic, etc.</td><td>Works for simpler program logics</td><td>A dedicated virtual machine is crafted to run the code like real. Dynamic behaviors are well captured for analyze</td><td>Feature ready (see note)</td></tr>
<tr><td>2.1 “if” to control execution flow:
if (!isAdmin) …;</td><td>Better products integrate SAT / SMT to validate execution path</td><td>Invalid execution path caused false positives pruned</td><td rowspan="2">Identify security validation logics of “if” to eliminate false positive effectively, also pruning invalid execution paths</td><td>Feature ready</td></tr>
<tr><td>2.2 “if” for security validation:
if (c >= ‘a’ && c <= ‘z’) s += c;
if (emaiRegex.matches(e)) …;</td><td>Usually ignores such complex but common security validation logics</td><td>False positive / negative tolerated</td><td>Feature ready</td></tr>
<tr><td>3. Function pointer / virtual method / dynamic typing / etc.</td><td>Assume all possible functions called</td><td>False positive / negative tolerated</td><td>Dynamic tracking of function pointer, “this”, or “Object” to secure the exact data type and method to be invoked</td><td>Feature ready</td></tr>
<tr><td>4. Dynamic array(map) access
v = request.getString(“value”);
elems[index] = v;</td><td>Assume all members of the array is tainted by v</td><td>False positive / negative tolerated</td><td>Build runtime array storage model to track exact taint propagation paths</td><td>Code ready</td></tr>
<tr><td>5.1 Loop - taint propagation</td><td colspan="2" rowspan="2">A common solution is to find “loop invariants”, which is an fuzzy / unreliable process</td><td rowspan="2">Virtually run the loop to identify taint propagation paths as well as loop statistics (invariants)</td><td>Feature ready</td></tr>
<tr><td>5.2 Loop - loop statistics</td><td>Code ready</td></tr>
<tr><td>6. 3rd party framework and API integration</td><td colspan="2">Support it, but could be inconvenient and inaccurate because of the discrepancy between static data structure and dynamic logic of APIs</td><td>Support code level, script-based configuration, to integrate into AmberVM execution flow precisely</td><td>Feature ready</td></tr>
<tr><td>etc.</td><td colspan="2"></td><td></td><td></td></tr>
</table>

Note

- **Feature ready** - the feature code finished, unit and integration tested. Works well as part of the product. It may have problems on certain combinations / corner cases over the variety programs in the wild, which shall be treated as bugs / enhancement and usually can be addressed quickly.
- **Code ready** - the feature has technical design as well as code finished but need debug and test before formal release.