Crowdsourced Security at the Government Level: It Takes a Nation (of Hackers)

Jay Kaplan
CEO/Cofounder
Synack
@JayKaplan
Synack

“leverages the best combination of crowdsourcing researchers and leveraging technology to discover security vulnerabilities in our customers’ web apps, mobile apps, IoT devices and infrastructure endpoints”
Crowdsourcing: It’s Everywhere ...
Crowdsourcing: It’s Everywhere
Why?

- Diversity of ideas
- Access to talent and expertise
- Scalability
- Incentive-driven motivation
Idea Generation & Corporate Innovation

OUT OF IDEAS?

G-WIN
Worldwide Innovation Network

GE OPEN INNOVATION

Challenge.gov
Government Challenges, Your Solutions
Idea Generation & Corporate Innovation

G·WIN
Worldwide Innovation Network

GE OPEN INNOVATION

Challenge.gov
Government Challenges, Your Solutions
Government Agencies Leveraging Crowdsourcing

DoD  NSA  NIH  HHS  EPA  NIST  FDA  NASA  …to name a few
Some challenge.gov examples

- Robocall Challenge (FTC, 2012)
  - Objective: Block illegal robocalls
  - Prize: $50,000
- Astronaut Glove Challenge (NASA, 2010)
  - Objective: Design an improved, flexible glove for use by NASA’s astronauts
  - Prize: $450,000 ($250,000 for first place)
- Wendy Schmidt Oil Cleanup X Challenge (NOAA, Dept of Interior)
  - Objective: Create highly efficient method of cleaning up oil spills from the ocean surface
  - Prize: $1.4M ($1M for first place)
What about Cyber Security?

- Over 70% of security professionals believe the cybersecurity skills shortage does “direct & measurable” damage to the organization.
- Over 1 Million cybersecurity jobs remain unfilled (1.5 Million by 2019).
- Over 93% of organizations take just minutes to compromise.
- Over 75% of organizations report at least one breach/year (that they know about...).
The Government wants to respond...

Obama Advises Trump To Train 100,000 Hackers

The Obama Administration has recommended that incoming President Donald Trump execute a comprehensive cybersecurity strategy, including the training of 100,000 white hats.

Action Item 4.1.1: The next President should initiate a national cybersecurity workforce program to train 100,000 new cybersecurity practitioners by 2020. (SHORT TERM)
But it’s not that easy

“Recruiting and retaining Army civilian cyber talent is challenging.” -Lt. Gen Edward Cardon, frmr. Commander, Army Cyber Command

“We are about halfway through the overall build, in terms of manning for the cyber mission.” -Lt. Col. Valerie Henderson, Pentagon
Yet the attacks continue

“The cyber threat is real...Cyber threats are increasing in frequency, scale, sophistication and severity of impact” - James Clapper, (now former) Director of National Intelligence. Clapper declared to Congress last year that cybersecurity is the top threat our nation faces, even more so than terrorism.
The gap is widening

A Widening Gap: Federal Cyber Incidents vs. Federal Cyber Budget

Federal Cyber Threat Curve
Federal Cyber Investment

Bringing a Knife to a Gun Fight (Essentially)

- Out-gunned
- Out-numbered
- Out-maneuvered
Would the government ever consider crowdsourcing hackers to help fill this gap?
Enterprise Organizations Are Doing It

Hundreds, if not thousands of programs today

>80% of programs are private

PUBLIC

Google
Bounty

Yahoo!

Microsoft

Uber

PRIVATE/
INVITE-ONLY

Apple

News
Apple is launching an invite-only bug bounty program
It's one of the last major tech companies to start paying for exploits
by Yael Golan | @YaelGolan | Aug 4, 2016, 11:30pm EDT

LinkedIn

News
LinkedIn says private bug bounty program works for it better
Bug Bounty: How it Works

Bug Bounty programs pay external security researchers a bounty for finding vulnerabilities in a company’s IT assets.

1. Crowd of bug bounty participants/hackers
2. Submit vulnerabilities through web platform or security@ inbox
3. Internal and/or external security team(s) reviews submissions
4. Valid bugs Passed onto remediation/dev team

Bounty Payment/Administration team rewards the hackers.
Historical Adoption of Bug Bounty Programs

- Netscape started one of the first “Bugs Bounty” back in 1995, big gap in time until further adoption
- 2010 saw adoption by Google, fellow tech giants soon followed
- Early programs were open self-managed bug bounty programs
- Massive transition toward the private/invite-only model

+ HUNDREDS of other organizations

Netscape

Google

Facebook

PayPal

Microsoft

LinkedIn

Apple
## Benefits of Bug Bounties

### Advantages of Bug Bounty Programs

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Adversarial/Hacker Perspective</strong></td>
<td>External hackers provide visibility into what adversaries truly see</td>
</tr>
<tr>
<td><strong>Incentive-based Testing</strong></td>
<td>Bounty rewards drive testing activity. No valid bug reports, no rewards</td>
</tr>
<tr>
<td><strong>Scalable</strong></td>
<td>Grow pen testing and red teams with hundreds/thousands of hackers</td>
</tr>
<tr>
<td><strong>Diverse &amp; Adaptive</strong></td>
<td>Not limited in diversity, instead fueled by a multitude of hacker vantage points</td>
</tr>
<tr>
<td><strong>Continuous</strong></td>
<td>Not limited in time &amp; scope, instead can provide continuous testing coverage</td>
</tr>
</tbody>
</table>
So Let’s Look back to RSAC 2016

At RSA, Defense chief Carter unveils feds first 'bug bounty'
It works!

Registered eligible participants: 1,410
Total reports received: 1,189
Total valid reports: 138
Total time it took to receive first vulnerability report: 13 minutes
The results

“Through this pilot, we’ve found a cost-effective way to support what our dedicated people do every day to defend our systems and networks — and we’ve done it securely and effectively. And the results exceeded our expectations.”
Time for Expansion
Crowdsourcing is a modern business practice that, as of 2010, the Federal government has employed to obtain needed services, ideas, or content by soliciting contributions from a large group of people rather than from traditional employees or suppliers. Crowdsourcing incentivizes innovation in solving mission-centric problems. Remaining ahead of present and emerging cyber threats is a significant responsibility in any environment. For DoD the responsibility is amplified as the repercussions associated with security failure are severe.

3. PURPOSE & OBJECTIVE

With the assistance of the private sector, the Government intends to use existing commercial crowdsourcing expertise and best practices, tailored for the Government’s use, to support the DoD in the application of the crowdsourcing methodology to enhance its information security. In support of this objective, the DoD intends to partner with a commercial firm that has extensive experience with administering crowdsourced vulnerability discovery and disclosure activities as a service. Under the resulting task order, the firm will host DoD bug bounties and/or other crowdsourced security activities on behalf of the DoD.
FA1 vs. FA2: Scope

**FA1**

4. SCOPE

For this first challenge, the Office of the Secretary of Defense intends to conduct crowdsourced vulnerability discovery and disclosure services against several websites and their subdomains, owned by one of the Military Departments that has both internal and external components. The website has static content and dynamic fields with Human Resource data in the backend (as well as other interactive customer engagement features (i.e., chat, user accounts). The challenge will...

“intends to conduct crowdsourced vulnerability discovery & disclosure services against several websites and their subdomain, owned by one of the Military Departments... has static content and dynamic field with HR data in the backend.

**FA2**

4. SCOPE

The first FA2 Task Order will be to conduct private crowdsourced vulnerability discovery and disclosure activities against the source code and operational instantiation of one or more modules in a DoD file transfer capability. (Although the solution includes dozens of distinct components, the scope of the first task order would include 1) approximately 200,000-500,000 lines of DoD contractor developed and maintained code owned by DoD, and 2) a live internal DoD application, accessible via the DoD Intranet. It is expected that DoD code will be hosted in the contractor’s platform, accessible only through DoD-specified authentication methods, and...

“...conduct private crowdsourced vulnerability discovery & disclosure activities against the source code and operational instantiation of one or more modules in a DoD file transfer capability... includes dozens of distinct components, scope would include 1.) ~200-500k lines of DoD contractor developed and maintained code owned by DoD and 2.) live internal DoD application accessible via the DoD intranet
FA1

as other interactive customer engagement features (i.e., chat, user accounts). **The challenge will be opened to all U.S. persons but limited to 400 registrants, preferably recruited based upon expertise by the contractor.** Additional details about the specific domain will be provided to the IDIQ FA1 awardee upon task order award.

FA2

available only to vetted researchers, triage personnel, and approved asset-owner personnel. The contractor will develop rules of engagement for conducting all testing activities.

Both the proprietary code and software are sensitive Government assets. Therefore, the FA2 contractor will be required to maintain a private community of skilled and trusted researchers, diverse in skillset, and able to conduct both deep binary hacking, web-based attacks, reverse engineering, and network and system exploitation. **The challenge phase itself will last three (3) weeks, and the total period of performance of the task order will not exceed four (4) months.**

“Both the proprietary code and software are sensitive Government assets. Therefore, the FA2 contractor will be required to maintain a private community of skilled and trusted researchers, diverse in skillset, and able to conduct both deep binary hacking, web-based attacks, reverse engineering, and network and system exploitation...

... will be “closed” by invite only ... passed criminal background checks. For this FA2 task order, **Gov’t expects researcher quality over quantity.**
FA1 vs. FA2: Task Execution & Platform Capabilities

FA1

This requirement falls under the domain of Functional Area 1 (FA1) of the DoD Crowdsourced Vulnerability Discovery & Disclosure Services IDIQ Contract and involves enabling researchers to conduct remote, over the Internet crowdsourced vulnerability discovery and disclosure services against several Internet-accessible public-facing websites. The contractor’s platform will be the mechanism for:

• Participants to apply to participate in the challenge and to submit vulnerability reports;
• All communication between the contractor and participants;
• The contractor to triage the reports and submit to the Government remediation team; and
• The Government remediation team to communicate and coordinate with the contractor’s triage team.

...platform mechanism for:

• Participants to apply/participate & submit vuln reports
• Communication between contractor & participants
• Contractor to triage reports & submit to Gov’t. remediation teams
• Gov’t remediation team to communicate & coordinate with contractor’s triage team

FA2

• Providing comprehensive vulnerability report triaging, validation, and prioritization within 48 hours of submission, and reporting to the DoD Remediation Teams to ensure it can patch the vulnerability as soon as possible;
• Providing the secure portal through which all testing occurs with full packet capture capabilities to enable continuous monitoring and auditability;
• Researchers to submit all vulnerability reports;
• Participants to apply to participate in the challenge and to submit vulnerability reports;
• Conducting all management and coordination with researcher community and project management and coordination with DoD Remediation Teams;
• Coordinating the disclosure of vulnerabilities affecting third party organizations/vendors.

...platform mechanism for:

• Comprehensive vuln report triaging, validation, prioritization & reporting to DoD w/in 48 hrs
• Secure Portal through which all testing occurs with full packet capture —> continuous monitoring & auditability
• Participants apply (vetting) and submit full reports
• Conduct all mgmt. & coordination with researcher community and project mgmt. & coordination w/ DoD remediation teams
Government Acquisition Processes...
Defense Digital Service moved at Silicon Valley Speed

Agile Acquisition!

DoD Expansion —> Two-pronged effort (Review)

<table>
<thead>
<tr>
<th>Functional Area 1: Public Facing Domains</th>
<th>Functional Area 2: Sensitive IT Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participants</td>
<td>Open to all US persons</td>
</tr>
<tr>
<td>Process</td>
<td>Triage of all vulnerabilities</td>
</tr>
<tr>
<td>Technology</td>
<td>Vulnerability Management System</td>
</tr>
</tbody>
</table>
Bug Bounty vs. Hack the Pentagon

For the first time in DoD history, the Pentagon invited a crowd of ethical hackers to test one of their sensitive systems.

1. US & allies’ most advanced researchers are vetted and invited to participate via the contractor platform.

2. Replicated target in a cyber range. All researcher activity routed through a secure gateway and trackable IP addresses.

3. Critical vulns start flowing in! Contractor triages and prioritizes all submissions.

4. Real-time adversarial intelligence is passed onto DoD remediation teams and SECDEF Mattis.

Contractor rewards hackers with bounties for each vuln submitted!
Hack the Pentagon Mentality Shift

Hack the Pentagon has become increasingly progressive in its targets...

- Hacking a DoD Marketing Site
- Launching a Crowdsourced Security Policy
- Hacking an Army Recruiting Website
- DoD Vulnerability Disclosure Policy
- Hacking Internal Sensitive Assets
- Hack the Pentagon: Critical Assets
Recent Success

Hack the Pentagon: Critical Systems
For the first time, the DoD invited a crowd of hackers to test one of their complex, sensitive systems.

Some of the results:

- **80** Top Researchers
- **<24 hours** to find first critical vulnerabilities
- **>$30,000** payout for a vulnerability

Thanks to all of the incredibly talented hackers who worked with us to improve the security of the @DeptofDefense and our country! Success.
Adoption of Crowdsourced Security

Gartner predicts 5 to 10 years to mainstream market adoption ...

Synack and IRS join forces for private bug bounty program

The IRS has awarded a $2 million sole-source contract to a crowdsourced security company to penetration test its computer networks using a global network of vetted white-hat hackers.
What's next?

Platforms?

Mission Control Systems?

Databases?

Critical Infrastructure?
Why Wait? How Can You Get Started Today?

Decide how much risk you’re willing to take on, paired with your overall objectives

...a few things to consider

1. “Nice to have” vs. Key Component/Replacement of Security Testing
2. Public vs. Private/Invite-Only
3. Self-Run vs. Hosted vs. Fully-Managed
4. Requirements & Controls
5. Budget, Value & ROI
Why Wait? How Can You Get Started Today?

What You’ll Need

1. Clear Scope & Rules of Engagement (ROE)
2. Clearly documented submission guidelines & process flow for researchers
3. Clear bounty/swag/acknowledgement expectations
4. Dedicated triage, response, and award personnel
5. Plans to integrate valid bugs into remediation workflows

But there are companies here to help…
That said, will we be asking about your crowdsourced network of hackers next year, not your Ubers?
Thank You