Comcast Technology Research & Development Fund

2014 Annual Report

Summary of the Fund's Operations for the 2014 Operating Year

Comcast Tech R&D Fund At a Glance: 2014 Summary

Background

Comcast created the Comcast Technology R&D Fund to identify and support important research that has the potential to advance broadband, the Internet and the global open-source community. The fund was established as a resource for researchers working on smaller and mid-sized technology projects that may not qualify for larger national grant programs.

Grants range from $3,000 for smaller projects, up to more than $100,000 for medium-term research efforts. A cross-functional team of technology and business leaders within Comcast reviews grant applications and directs funding where it is most needed, and can have the greatest potential impact. The fund enjoyed a 7-figure funding commitment from several internal groups within Comcast in 2014, and that level has been renewed for 2015.

In the second full year of the grant program, Comcast disbursed virtually the entire annual fund across a range of deserving applicants. Combined, the fund issued grants to 21 applicants in seven countries.

Objectives and Key Criteria

The fund was created to advance the Internet and open-source technology, and seeks to identify research projects that move technology forward by tackling difficult problems or pioneering new approaches. Among the factors, the fund seeks projects that:

- *Address critical cybersecurity threats*
- *Advance the deployment and adoption of IPv6*
- *Strengthen important open-source projects*

Approach

The fund offers three types of grant:

- **General Research Grants** (12 of 21 grants in 2014) – These unrestricted grants are given to support researchers at colleges and universities. They are geared toward supporting research in a range of fields relevant to the Internet and online communication.

- **Open Source Development** Grants (9 of 21 grants in 2014) – Comcast is an active participant in the global open source community. These grants are intended to support the creation and advancement of important open source projects, including those that may not have immediate business value, but which carry the potential for important technological development.

- **Targeted Research Grants** (0 of 21 grants in 2014) – Targeted research grants are set aside for research projects that may be suggested by Comcast, but which require specialized technological or academic expertise. Applicants for these grants may be organizations, academic institutions, or individuals.

2014 Highlights

Researchers we funded in 2014 included:

- *April Lorenzen of Dissect Cyber*, who received an open-source development grant to investigate a dangerous and widespread class of cybersecurity threats that exploit the Internet port (Port 53) used to deliver DNS traffic.

- *Ondrej Filip and Bedrich Kosata*, who received an open-source development grant to build open-source Internet routers for home- and small-office environments.

- *The AfterSchool Alliance*, which received a general research grant to conduct research into how Science Technology Engineering and Math (STEM) education is being incorporated into major after-school programs.

Looking Forward

Grants for the 2015 funding year have begun, and Comcast continuously reviews applications to identify new, worthy projects. For more details, or to apply visit techfund.comcast.com.

Comcast Tech R&D Fund Annual Report 2014

Grant Categories

1: GENERAL RESEARCH GRANTS
A General Research Grant provides an unrestricted award of funds to support researchers at colleges and universities. These grants are focused on supporting excellent technical or policy research in a wide variety of fields that are relevant to the Internet broadband industry. In general, applicants are encouraged to consider grants that may have a cooperative focus, whereby researchers can be matched with a Comcast engineering or policy liaison that will be involved with the research.

2: TARGETED RESEARCH GRANTS
While many Targeted Research Grant ideas may be suggested or generated by our internal teams, we may also fund specific research suggested by submitters that is also of interest to Comcast or to the Internet broadband industries. In contrast to General Research Grants, Targeted Research Grants are more narrowly tailored and typically study more specific issues. Applicants are encouraged to consider grants that may have a cooperative focus, whereby researchers can be matched with a Comcast engineering and policy liaison that will be involved with the research. Applicants for these grants may be organizations, academic institutions, or individuals.

3: TARGETED OPEN SOURCE DEVELOPMENT GRANTS
Targeted Open Source Development Grants are intended to fund new or continued development of open source software in areas of interest to Comcast or of benefit to the Internet and broadband industries. This can fund a range of development, from adding specific features to an existing open source project, to general support of an open source project in which we are interested. Applicants for these grants may be organizations, academic institutions, or individuals.

Recipients

#	Recipient	Grant Type
1	April Lorenzen - Dissect Cyber	Open Source Development
2	Open Home Health & Fitness Monitor and Aggregators for the Internet of Things	General Research
3	Cooperative Association for Internet Data Analysis (CAIDA) – University of California, San Diego Supercomputing Center	General Research
4	Ruby Version Manager, Version 1.X	Open Source Development
5	Research Secure & Usable Game CAPTCHAs	General Research
6	Internet Protocol Journal Publication	General Research
7	Open Source Home Gateway Software Project at CZ.NIC	Open Source Development
8	Study on Perceptually Optimized Video Encoding for Bandwidth Reduction in Video Services	General Research
9	OpenSSL Open Source Project Support	Open Source Development
10	High Efficiency Video Codec Research - University of Texas at Arlington	Open Source Development
11	CPE Security Research - Hyperion Gray	Open Source Development
12	Open Source Development of JITSI WebRTC Videobridge	Open Source Development
13	Research Into and Open Source Development of An Improved memcached-Based In-Memory Distributed Cache - Lehigh University	General Research
14	IPv6 Routing Research - Drexel University	General Research
15	Email Interception Research - Georgetown University	General Research
16	Study on Measuring the Known-Known and Known-Unknown in Network Security	General Research
17	Study on IPv6 – Asia-Pacific Network Information Center (APNIC)	General Research
18	Support for MAAWG Participation at the Instanbul Internet Governance Forum (IGF)	General Research
19	Development of Email Cypto Test Suite	Open Source Development
20	Develop Apache HTTP Client	Open Source Development
21	Afterschool Alliance	General Research

GRANTS MADE BY GEOGRAPHY:
USA 15; Australia 1; Switzerland 1; Turkey 1; Czech Republic 1; France 1; Greece 1

Individual Grant Details and Progress Reports

What follows are descriptions of al the grantees funded by the Tech R&D Fund in the 2014 funding year, including the type of grant, the status of the research and brief synopses provided by the grantees.

April Lorenzen – Dissect Cyber

Grant type: Open Source Development
DNS Resolver Reputation and Analysis
The proposed research aims to illuminate the nature of malicious port 53 outbound traffic that currently exists in almost all networks. Port 53 legitimate use is for DNS queries and DNS queries may use either UDP or TCP. Malicious activity has found a haven here because port 53 is so commonly used for legitimate traffic, relatively little understood, and often ignored. All types of data can be passed through port 53, sometimes disguised as DNS traffic, sometimes encrypted, sometimes chunked down to UDP size limits and sometimes utilizing TCP for unlimited size. Completely standard DNS queries make a robust and rich signaling tool for criminal activities. Specialized recursive resolvers can accomplish well-known malicious business models including ad revenue generation and phishing. Malicious authoritative name servers are the first resource that every cybercrime victim connects to, where the miscreants are enjoying the extra control benefits of running their own servers.

Status / Outcome: Work In Progress

Ira Laefsky

Grant type: General Research
Open Home Health And Fitness Monitor And Aggregator For The Internet Of Things

Status / Outcome: Completed

K.Claffy and M.Luckie – Cooperative Association for Internet Data Analysis

(CAIDA) – University of California, San Diego Supercomputing Center
Grant Type: General Research
Monitoring and Visualizing Internet Outages

We propose to develop, test, and validate new tools and methods to infer congestion at AS interconnection points between high-profile transit providers, content providers, and access ISPs. Additionally, we seek to understand whether there are specific cases of congestion where other possible paths with excess capacity could support additional load. The technical challenges are to: identify the presence of congestion along a path, determine its source, and identify alternative paths. We have unique infrastructure, topology data, and measurement and analysis methods that will allow us to discover and evaluate evidence of unnecessary congestion. Understanding how the interacting incentives of different networks are reflected in performance, and the resulting impact on the rest of the Internet industry, is largely uncharted territory. Such research however carries implications for not only network technology and operations, but also broader challenges related to the evolving Internet, including technology investment, future network design, and scientific study of the Internet itself. Our independent research will inform debates in the Internet operations community, news media, and in policy circles.

Status / Outcome: Work in progress

Michal Papis

Grant type: Open Source Development
Maintenance of RVM 1.x (part time):
- adding new ruby versions,
- adding support for new systems/versions,
- implementing necessary changes for new systems,
- fixing bugs,
- working with the ruby ecosystem on improving user experience
- migrate users to RVM 2.x
- possibly maintenance of RVM 2.x if users move fast

Status / Outcome: Work in progress

Nitesh Saxena – University of Alabama Birmingham

Grant Type: General Research
Research Secure And Usable Game Captchas
Almost every online service relies upon captchas to thwart various forms of online attacks. Unfortunately, existing captcha solutions (e.g.,

those based on distorted characters embedded within an image) suffer from significant usability and security problems. They are often very difficult to solve by legitimate users, and constantly broken via automated attacks (computer programs that solve the captchas) and low-cost human-solver relay attacks (e.g., paid humans that solve the captchas on behalf of the attacker). More alarmingly, the usability degradation can be so severe on many occasions that users feel frustrated and give up using the services that deploy captchas. Consequently, companies lose customers and suffer economic losses. In this project, we break new grounds by exploring the next generation of captchas – ones based on simple computer games. Game captchas may address the aforementioned problems with existing captchas and make captcha-solving a fun activity for users. Specifically, we will focus on a broad class of game captchas -- called Dynamic Cognitive Game (DCG) captchas -- which challenge the user to perform a game-like cognitive task interacting with a series of dynamic images. We will formalize, design and implement different variations of these captchas, and systematically dissect them across: (1) automated attacks, (2) human-solver relay attacks, and (3) usability.
As an end result, this research will attempt to develop DCG captchas that are both secure (with respect to automated as well as relay attacks) and user-friendly (easy, fun and engaging for users rather than being annoying).

Status / Outcome: Completed

Ole Jacobsen

Grant Type: General Research
Internet Protocol Journal
Support for the re-launch of the Internet Protocol Journal

Status / Outcome: Completed

Ondrej Filip, Bedrich Kosata

Grant type: Open Source Development
Open Source Home Gateway project at NIC.CZ
The project aims to develop open-source hardware and an operating system with

application software to create an open, secure, auto-updating and feature rich SOHO router. The project has already started and this request is for ongoing funding.

The aim of the project is to create a truly open - both hardware and software - SOHO router. In 2014, the main focus will be on further development of the operating system into a generic secure and feature rich operating system for routers with DNSSEC, IPv6 and QoS being the main focus points. We plan to improve and extend our NETCONF configuration interface to support advanced functionality, such as settings dependencies, fine-grained access management, etc. In hardware, we plan to build on our current model of router Turris and fine-tune it.

Status / Outcome: Development complete, routers delivered to Comcast for evaluation

Hari Kalva – Florida Atlantic University

Grant Type: General Research
Study On Perceptually Optimized Video Encoding For Bandwidth Reduction In Video Services
Description: The amount of video produced and consumed is growing at an exponential rate and is taking up an increasingly large amount of computing and communication resources. We believe, to have an immediate impact on the bandwidth used by video services, we need bandwidth reduction methods that work with existing codecs.

Video processing tasks such as compression, search, and analysis depend on what users see in videos. Psycho-visual studies have shown that perceptual and cognitive factors affect what users see when they watch video. The main goal of this research is to identify perceptual phenomena that predicts what users are likely not able to see when they watch video and exploit that knowledge to improve video compression. This project proposes to study a promising perceptual phenomenon known as temporal masking and develop effective methods to exploit this phenomena for visually lossless video compression. With this approach we can encode video with the same visual quality as optimized AVC/H.264 video (e.g., AVC/H.264 at 1 Mbps) while reducing the video bitrate.

(cont.)

Preliminary results show that we can achieve up to 14% bitrate reduction on top of optimized AVC/H.264 encoding. The proposed research is expected to result in substantial additional compression gains. With video representing increasingly large percentage of Internet traffic, these seemingly modest improvements in compression will quickly add up to substantial bandwidth savings at Internet scales. A big advantage of this approach is that the proposed approach is independent of compression algorithms and can be applied over existing video delivery infrastructure by just updating the encoders. Expected research output and publication *

The outcomes of this project are:

- 1. A study of temporal masking for visually lossless compression
- 2. Algorithms and tools for visually lossless video coding based on temporal masking
- 3. A comparative analysis and subjective quality evaluation of proposed visually lossless coding methods
- 4. Prototype based on X.264 demonstrating the bitrate savings achieved on top of optimized AVC/H.264
- 5. Performance evaluation of gains over MPEG-2 and HEVC encoded video.

Status / Outcome: Work in progress

OpenSSL Foundation

Grant Type: Open Source Development
OpenSSL Development Process Support
Support for the work of the OpenSSL foundation to enhance development process

Status / Outcome: Completed

University of Texas at Arlington

Grant type: Open Source Development
High Efficiency Video Codec research
High Efficiency Video Coding (HEVC) is a new video coding standard created by the JCT-VC group within ISO/IEC and ITU-T. An increasing variety of services, the growing popularity of HD video, and the formats going beyond HD (e.g., 4K × 2K or 8K × 4K resolution) are creating even

stronger needs for compression capabilities superior to AVC's. Now mobile devices and tablet personal computers will also need to receive and display HD video. HEVC has been designed to address essentially all existing applications of previous standards and to particularly focus on two key issues: increased video resolution and the increased use of parallel processing architectures. The syntax of HEVC is generic, and its design elements could also be attractive for other application domains that have not been used by the previous standards. HEVC is targeted to provide the same quality as H.264 at about half the bit-rate and will replace soon its predecessor in multimedia consumer applications. This increasing efficiency has supported the evolution of multimedia applications towards higher spatial and temporal resolution formats (e.g. HD) and the arising of more complex applications, such as 3D video. Digital Signal Processor (DSP) technology allows the implementation of very flexible video decoders at relative low cost and low power consumption. Previously, the optimization techniques of MPEG-2, H.264 and HEVC video decoders based on DSP technology were implemented with excellent results. Here, the main concentration is on implementation of HEVC video decoder based on multicore digital signal processor in order to decode higher resolution. In a previous work, an implementation based on HM9.0 reference software was presented, but in this work, HM13.0 latest reference software will be used.

Status / Outcome: Work in progress

Hyperion Gray

Grant type: Open Source Development
CPE Security research
We propose researching whether it is viable to develop an automated software solution that can be run on virtually any home router to scan the device against a predefined security baseline and automatically change any noncompliant configurations to the compliant setting. There are, however, many challenges that must be overcome in order to develop a vendor-agnostic and automated solution, such as the proprietary nature of home router operating systems and the complexity and variety of configuration items and settings within each, just to name a few. If we can develop such a solution, then the average home

user – or their ISP – could be empowered to secure their home router with nothing more than a mouse click, which would truly revolutionize home network security. Our proposed solution is distinct from current router lock-down solutions in that we are proposing a *vendor-agnostic* solution that is *generalized and extensible*; current solutions tend to be vendor-specific and version-specific, meaning that each one must be developed individually for each model and version. Furthermore, our proposed research leading up to the development of a solution prototype would make significant contributions to the broader security community, in contrast to existing or planned proprietary solutions.

Status / Outcome: Work in progress

Emil Ivov

Grant type: Open Source Development
Open Source Development of JITSI WebRTC Videobridge
Jitsi Videobridge is a new open communications project that enables scalable, high-quality video conferences and is designed to be used for WebRTC. Currently, it already supports a number of popular use-cases including multi-party web conferences. We would like to add some important features that would make it even more versatile and useful to expand how WebRTC can be used as an application platform. These are Video Recording, Post processing capability, and a JSON / REST API. This would be released as open source code.

Status / Outcome: Work in progress

Michael Spear – Lehigh University

Grant Type: General Research
Research into and Open Source Development of an Improved memcached based In-Memory Distributed Cache
In large-scale internet services, an in-memory cache provides a shortcut that allows compute nodes to quickly acquire data without interacting with a large and slow network storage. However, it is possible that interaction with the in-memory cache can be a bottleneck. In conversations with John McCann and Sree Kotay, we learned of one such problem, where large packets of

data are requested from memcached servers, modified slightly, and then sent back to memcached servers. During periods of high network traffic, two transfers of large packets can create a bottleneck. This research will invent new mechanisms that enable computation, in the form of pre-compiled shared libraries or dynamically generated scripts, to be run at the memcached server. By sending computation to the data, the overheads of transmission can be reduced dramatically, lowering overall system load and reducing bandwidth requirements during periods of high demand. This research will also produce novel mechanisms for deciding when to migrate computation. Evaluation will be performed on traces of Comcast workloads, with a goal of ultimately using the software in a production environment at Comcast.

Status / Outcome: Work in progress

Gaurav Naik – Drexel University

Grant Type: General Research
IPv6 Routing Research
Today's networks are developed with numerous assumptions about their typical operating regions consisting of patterns of usage, the network conditions and their underlying support infrastructure. These assumptions lead to a fairly static choice of routes that may perform adequately within regions of anticipated operation but fail drastically under unexpected network conditions or unanticipated uses. This team proposes to demonstrate IPv6 segment routing (SR) and SFC to illustrate how data, video or otherwise, can be more efficiently delivered over routed links in SDN and non-SDN networks. These links may not necessarily represent the shortest paths but instead the most efficient (or best) paths for the content to be delivered.

Status / Outcome: Work in progress

Eric Burger – Security & Software Engineering Research Center (S2ERC) - Georgetown University

Grant Type: General Research
Email interception project
Description: The proposal is a measurement study

of email interception. Since the content (and metadata) of intercepted emails can be trivially read, convention wisdom tells us that confidential information should never be sent via unencrypted emails. The proposed project explores whether such advice is actually prudent. We aim to answer the question "how often are emails actually intercepted on the Internet?" To determine the regularity of which interception occurs, we will transmit (false) emails whose content would be attractive to potential eavesdroppers, but are sent only between our own email accounts. In particular, our fake emails will contain URLs that purportedly contain sensitive information about mortgages, bank accounts, passwords, and shared files. The emails will be sent between geographically distributed email servers located through the globe, with embedded URLs that resolve to web servers under our control. Since the emails are sent only between our servers and are addressed to fictitious email accounts, any visit to one of the embedded URLs must be due to the (illegal) interception of our email.

Status / Outcome: Completed, poster session proposed

Manos Antonakakis Ph.D – Georgia Institute of Technology

Grant Type: General Research
Study on measuring the known-known and known-unknown in network security
Description: Development of a basic unit of measurement for defining the cyber security status of a network. The research proposal aims to assess the security level of Comcast's network and the impacts to the level stemming from advancements in botnets communication mechanisms. The methodology entails comparing known/unknown and benign/malicious domains against Comcast's passive DNS data to generate a standardized measurement unit. The research is relevant because it will advise us as to the percent of malware/botnet traffic we are currently detecting using various security services (or not detecting). This in turn will help us tune our techniques, invest or divest from certain technologies and ultimately help us keep our customers informed about security and privacy threats.

Status / Outcome: Completed

Geoff Huston – APNIC

Grant Type: General Research
IPv6 Study
Description: Asia Pacific Network Information Centre (APNIC) is one of the five regional Internet registries. APNIC provides number resource allocation and registration services that support the global operation of the Internet. It is a not-for-profit, membership-based organization whose members include Internet Service Providers, National Internet Registries, and similar organizations. In addition to the many services that APNIC offers to the members in its regions, APNIC is world renowned for its efforts advancing, developing, and deploying Internet measurements, including those specific to IPv6 and DNSSEC. Their measurement platform, described below in greater detail, analyzes the deployment of IPv6 around the globe including adoption of IPv6 across the Comcast network. This proposal is proposed under the Comcast Tech Fund category: Measurement and Analysis. Preliminary measurement of Comcast by APNIC has already provided interesting and useful insight into various aspects of Comcast's IPv6 deployment including the types of IPv6 technologies that are being used by Comcast customers. This project will help advance the following: It will provide greater detail regarding where various transition technologies (tunnels like Teredo and 6to4) are being used within the Comcast network. It will provide an interface that Comcast can leverage to encourage customers to disable technologies like 6to4, targeting these specific users. It will also gather additional data to explore performance differences between IPv4 and IPv6 and assist with long-term deployment strategies.

Status / Outcome: Work in progress

Messaging, Malware and Mobile Anti Abuse Working Group

Grant Type: General Research
Description: Support for MAAWG attendance at the IGF in Istanbul to participate in ISOC organised Best Practice forum on Spam.

Status/Outcome: Completed

(cont.)

Jonathan Grier

Grant type: Open Source Development
Development of email crypto test suite
We aim to develop, with Comcast's support, an open source development and testing platform that will help developers adopt these standards, and validate their email system for security, open standards, and compatibility. We aim to spur adoption of secure email by the entire community: no matter how they use email, people worldwide will all be able to securely communicate with each other, without forging, without phishing, and without privacy violations, all using the same secure, open standards based security.

Status / Outcome: Completed

Oleg Kalnichevski

Grant Type: Open Source Development
Apache Android Development
Description: Develop an Android optimized version of Apache HttpClient based on the latest official release that: 1) retains full backward API compatibility with the Google internal fork while upgrading implementation classes to the latest release of the official version, 2) provides full API with the stock version of Apache HttpClient, 3) makes selective use of Android specific features that are not available in the context of Java Standard Edition, and 4) avoids creating a fork of the main code line. Users and developers of the Android platform would benefit from having a better, more feature full implementation of Apache HttpClient available for Android. It would also serve to keep Android platform more open and diverse.

Status / Outcome: Completed

AfterSchool Alliance

Grant Type: General Research
Description: The Afterschool Alliance is planning to release a Special Report on STEM in Afterschool, an additional report drawn from the data of America After 3 PM, the largest household survey on afterschool.

Status/Outcome: Work in Progress

COMCAST
techfund.comcast.com