



Information System Security Operation Control for High-Throughput Adaptive Resilient Transport

Providing Secure Control Plane Functionality Within The Network

Overview

The Control for High-Throughput Adaptive Resilient Transport (CHART) project directly addresses the problem of providing control plane functionality within the network. A control plane is a mechanism that connection management devices use to control and access network components and services. The need for the control plane arises from the reality that the Internet today is a best effort system that makes no guarantees on the quality of the routes, and the performance of standard protocols degrades rapidly in response to minor loss of link quality. The keys to realizing the control plane vision are the provision of a network-wide real-time weather service that is reliable, efficient, scalable, and secure, available to end hosts, and the provision of an in-network routing solution that can rapidly re-route.

Solution

The CHART Team is lead by Hewlett Packard, and the team members are McAfee® Research, now the Security Research Division of SPARTA, UC Berkeley, Princeton University, and George Mason University. The team is designing and implementing these innovations for the control plane: a backbone utilizing a routing overlay based on the Tapestry overlay infrastructure, software and hardware-based sensing to provide decentralized and end-to-end monitoring and measurement of network health, adaptive flow-based routing, adaptive and active traffic management to mitigate and manage conditions that affect network quality, and scalable. We are providing comprehensive security to keep the control plane safe from cyber attacks. All software elements of the solution run on commodity servers, therefore the cost of introducing base-level technology into an existing network is minimal. Hardware-based

sensing and a new generation of adaptive routers are optional elements for high-bandwidth (gigabit) links where software routing is of limited utility.

CHART innovations are superior to the state-of-the art in that they:

- Require minimal or no changes to client machines,
- Represent a software-based solution that requires no changes to existing routing infrastructure or protocols,
- Provide a clear path to a hardware-based solution for high-speed links that scales with the cost and speed of the link,
- Accommodate IPv6 functionality directly without change,
- Deploy readily and scale to overlay networks with tens to hundreds of thousands of subnets
- Build on the existing, working PlanetLab platform, and
- Can be gradually introduced to DoD infrastructure on a subnet-by-subnet basis.

Our contribution to the CHART Innovations is the comprehensive security architecture, which provides security at three functional levels. Security for basic communications and secure scalable high-performance multicast; Security for control plane management functions, membership, routing infrastructure, and advanced access control to internal resources; and active intrusion protection of the control plane.

Approach

The CHART approach consists of the following elements: a control plane backbone of overlay nodes that receive input from multiple sensors,

This work sponsored by DARPA through Hewlett Packard.



Control for High-Throughput Adaptive Resilient Transport

Providing Secure Control Plane Functionality Within The Network

real-time probing of network quality, and adaptation of routes.

One unique and compelling aspect is that it permits the gradual introduction of new routing technology on the network, where overlay nodes on the existing infrastructure provide immediate benefits of adaptive routing. Hardware routers serve to future-proof the solution by accommodating transmission rates of OC-48 and above. Overlay nodes also facilitate the introduction of new network applications beyond the initial use of intelligent routing. The CHART approach opens up possibilities for strategic development of next generation flow-based routers.

CHART combines a novel adaptive routing infrastructure and a distributed network-sensing infrastructure to improve end-to-end throughput across a heterogeneous and unreliable network.

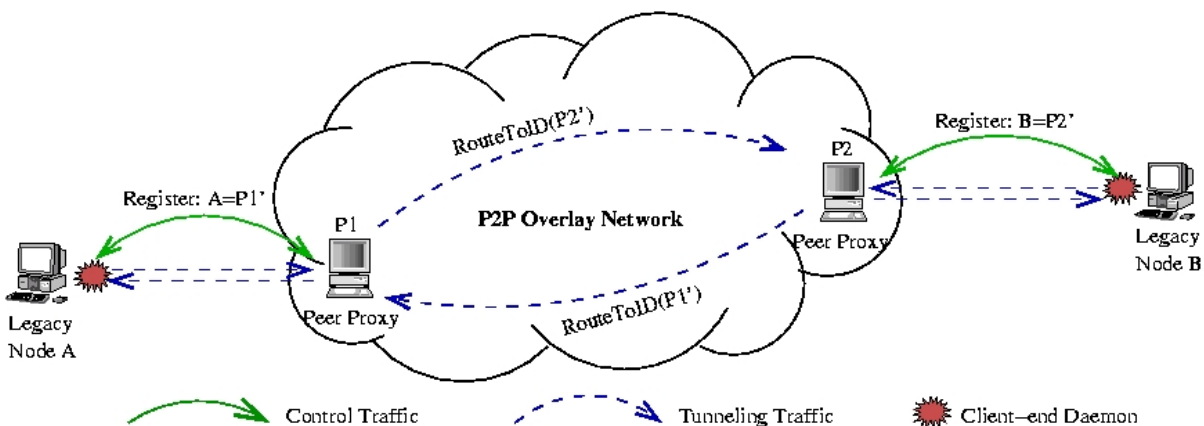
The routing infrastructure has two complementary components. The first component is a software-based routing overlay deployed on commodity computers with relatively low-bandwidth edge links, and the second component uses new, strategically deployed high-performance flow routers on high-bandwidth backbone links. Both hardware and software routers actively sense the network, and on detection of link congestion or failure, dynamically re-route traffic to preferred paths.

A common decentralized network measurement and monitoring fabric supports intelligent routing. This sensing infrastructure securely aggregates

and propagates measurements collected at both hardware and software monitors. Decentralized sensing enables enhanced traffic engineering and maintenance, and a novel fault diagnostic tool permits active 'triangulation' of link failures.

We are developing an architecture that provides a comprehensive and innovative set of security services. This includes security for basic communications and control plane management, as well as active intrusion prevention. Secure services for basic, multicast, and group communications include authentication, confidentiality, and integrity guarantees. An innovation in group communications that we are pursuing is the use of block-free group keying protocols, which have the advantage that re-keying is done without interrupting ongoing communications. We intend to provide secure communications at the level of individual packets, messages and collections of messages.

To address security for the management of the control plane, CHART provides secure membership management functions in the overlay substrate such as the credentialing and authentication of infrastructure nodes. To decrease the vulnerability associated with the compromise of a central certificate authority server, a key innovation that we propose is the use of a threshold-based distributed Certificate Authority scheme. A number of threshold (uncompromised) servers are required to generate public and private key pairs and to sign certificates.



For more information call us at 410-872-1515, send an e-mail to ISSO-research@sparta.com, or visit us on the Web at <http://www.issosparta.com/research>.