PARALLEL DATA LABORATORY
CARNEGIE MELLON UNIVERSITY

THE
PDL Packet Spring Update

THE NEWSLETTER ON PARALLEL DATA SYSTEMS • SPRING 2001

http://www.pdl.cs.cmu.edu

CONSORTIUM MEMBERS

EMC Corporation
Hewlett-Packard Laboratories
Hitachi, Ltd.
IBM
Intel Corporation
LSI Logic
Lucent Technologies
Network Appliance
Panasas, Inc.
Platys Communications
Seagate Technology
Snap Appliances
Sun Microsystems
Veritas Software Corporation

I◆N◆S◆I◆D◆E

THE PDL PACKET

EDITOR
Joan Digney

CONTACT
Karen Lindenfelser
PDL Business Administrator

The Parallel Data Laboratory
Carnegie Mellon University
5000 Forbes Avenue
Pittsburgh, PA 15213-3891
VOICE 412•268•6716
FAX 412•268•3010

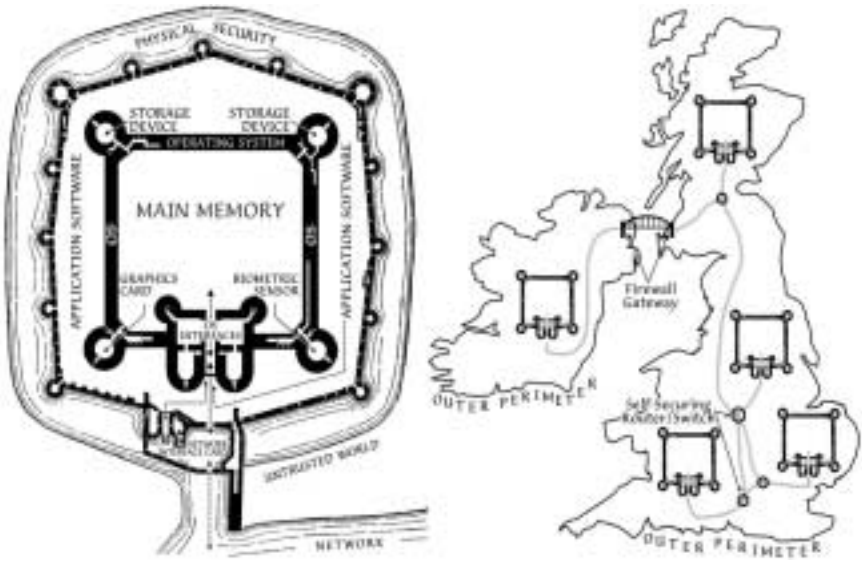
Better Security via Smarter Devices

Greg Ganger and David Nagle

Despite enormous effort and investment, it has proven nearly impossible to prevent computer security breaches. Together with our growing dependence upon on-line information and wide-area networking, this fact creates an enormous security risk to our national economic and defense infrastructures. To protect our critical information infrastructures, we need defensive strategies that can survive determined and successful attacks, allowing security managers to dynamically detect, diagnose, and recover from breaches in security perimeters.

To attack the security dilemma, the PDL has embarked on a long-term research effort to re-architect computer systems into *"Self-Securing Devices."* Funded by the Department of Defense's Critical Infrastructure Protection program for $4.7 million over 5 years, PDL draws on our expertise in Network-Attached Storage, Self-Securing Storage, PASIS, and Scalable Firewalls, to promote a security architecture where individual system components erect their own security perimeters and protect their resources (e.g., network, storage, or video feed) from intruder tampering. This "self-securing devices" architecture distributes security functionality amongst *physically distinct* components, avoiding much of the fragility and manageability inherent in today's border-based security.

... continued on pg. 5



The self-securing device architecture illustrated via the siege warfare constructs that inspired it. On the left, (a) shows a siege-ready system with layered and independent tiers of defense enabled by device-embedded security perimeters. On the right, (b) shows two small intranets of such systems, separated by firewall-guarded entry points. Also note the self-securing routers/switches connecting the machines within each intranet.

PDL NEWS

April 2001
Steve Schlosser wins Intel Fellowship
We'd like to congratulate Steve Schlosser who has been awarded an Intel fellowship. Nationally, Intel awards thirty-five Ph.D. fellowships each year, providing a cash award (tuition/fees/ stipend), an Intel CPU-based PC, an Intel Mentor, and the opportunity to conduct research or an internship at Intel.


Steve Schlosser

Steve's research focuses on MEMS-based storage's design and application. This non-volatile storage technology merges magnetic recording material and thousands of recording heads to provide storage capacity of 1-10 GB of data in an area under 1 cm^2 in size with access times of less than a millisecond and streaming bandwidths of over 50 MB per second. Further, because MEMS-based storage is built using photolithographic IC processes similar to standard CMOS, MEMS-based storage has per-byte costs significantly lower than DRAM and access times an order of magnitude faster than conventional disks.

March, 2001
Mor Harchol-Balter Receives Anna McCandless Chair
Mor Harchol-Balter, assistant professor of computer science, has been awarded the Anna McCandless Chair, a three-year term career development professorship that provides funding for travel and sabbaticals, including partial costs of academic-year teaching and research and programs. Jim Morris, dean of the School of Computer Science, said, "Mor arrived here, hit the ground running and has already launched an exciting program of research and education in computer system performance."

A graduate of the University of California at Berkeley, Harchol-Balter received her doctorate in 1996. Manuel Blum, professor of computer science and Turing Award winner, was the committee chair of her thesis entitled "Network Analysis Without Exponentiality Assumptions." Currently, her research interests include performance analysis and computer systems design, particularly distributed systems. Her research applications include Web servers, distributed Web servers, distributed supercomputing servers, networks of workstations, and communication networks. Harchol-Balter teaches performance analysis and computer networks and also advises three Ph.D. students. A prolific researcher, she is the author of numerous papers published in various journals and conference proceedings.

The Anna McCandless Chair is sponsored by the estate of Anna Loomis McCandless. McCandless was a 1919 graduate of Margaret Morrison Carnegie College and was known for her persistence and determination. A native of Pittsburgh, McCandless worked for a private investor and then Fidelity Trust Co. after graduating from Carnegie Tech. She was the first female member of the Board of Trustees in 1967 and was named a life trustee in 1973. She was the longest serving female trustee, having served on the board for 29 years. In 1963, McCandless received Carnegie Mellon's Alumni Service Award.


Mor Harchol-Balter

… continued on pg. 4

RECENT PUBLICATIONS: ABSTRACTS

http://www.pdl.cs.cmu.edu/publications/publications.html

Enabling Dynamic Security Management of via Device-Embedded Security

Ganger & Nagle

Carnegie Mellon University Technical Report CMU-CS-00-174, December 2000.

This report contains the technical content of a recent funding proposal. In it, we propose a new approach to network security in which each individual device erects its own security perimeter and defends its own critical resources. Together with conventional border defenses (e.g., firewalls and OS kernels), such *self-securing devices* provide a flexible infrastructure for dynamic prevention, detection, diagnosis, isolation, and repair of successful breaches in borders and device security perimeters.

Managing network security is difficult in current systems, because a small number of border protections are used to protect a large number of resources. We plan to explore the fundamental principles and practical costs/benefits of embedding security functionality into infrastructural devices, such as network interface cards (NICs), network-attached storage (NAS) devices, video surveillance equipment, and network switches and routers. The report offers several examples of how different devices might be extended with embedded security functionality and outlines some challenge of

… continued on pg. 3

RECENT PUBLICATIONS

… continued from pg. 2

designing and managing self-securing devices.

Track-Aligned Extents: Matching Access Patterns to Disk Drive Characteristics

Schindler, Griffin, Lumb & Ganger

Carnegie Mellon University Technical Report CMU-CS-01-119. April, 2001.

Track-aligned extents (traxtents) utilize disk-specific knowledge to match access patterns to the strengths of modern disks. By allocating and accessing related data on disk track boundaries, a system can avoid most rotational latency and track crossing overheads. Avoiding these overheads can increase disk access efficiency by up to 50% for mid-sized requests (100-500 KB). This paper describes traxtents, algorithms for detecting track boundaries, and the use of traxtents in file systems and video servers. For large file workloads, a modified version of FreeBSD's FFS implementation reduces application run times by 20% compared to the original version. A video server using traxtent-based requests can support 56% more concurrent streams at the same startup latency and buffer space. For LFS, 44% lower overall write cost for track-sized segments can be achieved.

PASTENSE: a Fast Start-up Algorithm for Scalable Video Libraries

Harizopoulos & Gibson

Carnegie Mellon University Technical Report CMU-CS-01-105, March, 2001.

Striping video clip data over many physical resources (typically disk drives) balances video server load with less data replication. Current striped video delivery algorithms can have high start-up latency if the load is high. We propose a new, fast start-up algorithm, PASTENSE. This algorithm minimizes start-up latency by using aggressive prefetching to exploit disk idle time, and using available RAM to dynamically optimize the newly requested video's schedule. Our proposed method (a) does not require changes in the existing striped data placement (b) it never performs worse than alternate designs and (c) it achieves significant benefits: up to 9 times faster start-up times under high loads.

Selecting the Right Data Distribution Scheme for a Survivable Storage System

Wylie, Bakkaloglu, Pandurangan, Bigrigg, Oguz, Tew, Williams, Ganger, Khosla

Carnegie Mellon University Technical Report CMU-CS-01-120. April, 2001.

Survivable storage system design has become a popular research topic. This paper tackles the difficult problem of reasoning about the engineering trade-offs inherent in data distribution scheme selection. The choice of an encoding algorithm and its parameters positions a system at a particular point in a complex trade-off space among performance, availability, and security. We demonstrate that no choice is right for all systems, and we present an approach

… continued on pg. 4

NEW PDL FACULTY

Anastassia Ailamaki

Anastassia Ailamaki received her Ph.D. from the Computer Sciences Dept. of the University of Wisconsin-Madison in Nov. 2000. Her thesis, titled "Architecture-Conscious Database Systems," states that the key to drastically improving database management system (DBMS) performance is to study the time breakdown of its hardware execution footprint. Proving this is done by examining commercial DBMSs, and looking for similar behavior trends on prototype DBMSs. The hardware bottlenecks provide insight for developing architecture-conscious DBMSs.

Anastassia's research focuses on DBMSs and their interaction with computer architecture using innovative interdisciplinary methods to improve DBMS performance by studying the hardware behavior of modern commercial systems. Currently, she is working to design indexing data structures and data/instruction placement algorithms to achieve optimal cache and memory bandwidth utilization. On multiprocessor platforms, her work focuses on cache coherence protocols as they influence DBMS behavior. Her long-term goal is to explore the interaction between database systems and other related areas in order to improve performance (compilers, networks) and expand functionality (artificial intelligence, user interfaces). She is also interested in making application logic a first class citizen in database systems, and has demonstrated that active DBMS functionality can be used to fully support scientific workflows modeling soil science and biochemistry experiments. She is also interested in developing client-server database systems that exploit new data representation standards, such as XML.

… continued on pg. 6

RECENT PUBLICATIONS

… continued from pg. 4

to codifying and visualizing this trade-off space. Using this approach, we explore the sensitivity of the space to system characteristics, workload, and desired levels of security and availability.

System Design Considerations for MEMS Actuated Magnetic-Probe Based Mass Storage

Carley, Ganger, Guillou & Nagle

IEEE Transactions on Magnetics, January 2001.

This paper presents common system design considerations imposed on magnetic storage devices that employ MEMS devices for positioning of a magnetic probe device over a magnetic media. The paper demonstrates that active servo control of the probe tip to media separation can be achieved with sub-nanometer accuracy. It also demonstrates that reasonable-size capacitive sensors can resolve probe tip motions with a noise floor of roughly 22 picometers, allowing them to be used as position sensors in magnetic force microscope (MFM) readout approaches. In addition, this paper demonstrates that although MEMS media actuators can achieve scanning ranges of ∓ 50 μm, the mass of the media sled imposes important access time and data rate constraints on such MEMS-actuated mass storage devices.

My Cache or Yours? Making Storage More Exclusive

Wong, Ganger & Wilkes

Carnegie Mellon University Technical Report CMU-CS-00-157, November 2000.

Modern high-end disk arrays typically have several gigabytes of cache RAM. Unfortunately, most array caches employ management policies in which the same data blocks are cached at both the client and array levels of the cache hierarchy - that is, they are inclusive. As a result, the aggregate cache behaves as if it was only as big as the larger of the client and array caches, instead of as large as the sum of the two.

This paper explores the potential benefits of exclusive caches, in which data blocks are either in the client or array cache, but never in both. Exclusivity helps to create the effect of a single, large unified cache. We propose an operation called DEMOTE for transferring data ejected from the client cache to the array cache, and explore its effectiveness in increasing cache exclusivity using simulation studies. We quantify the benefits of DEMOTE, the overhead it adds, and the effects of combining it with different cache replacement policies across a variety of workloads. The results show that we can obtain useful speedups for both synthetic and real-life workloads.

PDL NEWS

… continued from pg. 2

March, 2001

Garth Goodson Receives IBM Research Fellowship

Garth Goodson is the recipient of a Research Fellowship from IBM. The fellowship, eligible for renewal, covers Garth's tuition for the year and includes a stipend of $15,000. Garth plans to spend some time with the storage research group at IBM Almaden in the next year.

Garth is a Ph.D. student in ECE and has recently been working on Self-Securing Storage Systems (S4 for short). Self-securing storage prevents intruders from undetectably tampering with or permanently deleting stored data by internally auditing all requests and keeping all versions of all data for a window of

Garth Goodson

time, regardless of commands received from potentially-compromised host operating systems. Within this window, valuable information exists for intrusion diagnosis and recovery. Garth is also currently a teaching assistant for 18-546: Introduction to Storage Systems.

February, 2001

3 Professors Receive Research Grants from Dept. of Defense

The U.S. Department of Defense has awarded grants to three Carnegie Mellon faculty members, including Greg Ganger, Assistant Professor of Electrical and Computer Engineering, for their national defense research efforts. The grants were three of 20 awards totaling $9.3 million. The average award is $875,000 per year for three years.

Ganger and co-PI David Nagle have planned a project for the Air Force Office of Sponsored Research focusing on "Enabling Dynamic Security Management of Networked Systems via Device-Embedded Security." Please see the article on page 1 and the Carnegie Mellon Technical Report CMU-CS-00-174, available at http://www.pdl.cs.cmu.edu/Publications/ for further information.

… continued from pg. 1

Specifically, this "self-securing devices" architecture addresses three fundamental difficulties by: (1) simplifying each security perimeter (e.g., consider NIC or disk interfaces), (2) reducing the power that an intruder gains from compromising just one of the perimeters, and (3) distributing security enforcement checks among the many components of the system.

Current security mechanisms are based largely on singular border protections. This roughly corresponds to defense practices during Roman times, when defenders erected walls around their camps and homes to provide protective cover during attacks. Once inside the walls, however, attackers faced few obstacles to gaining access to all parts of the enclosed area. Likewise, a cracker who successfully compromises a firewall or OS has complete access to the resources protected by these border defenses. Of course, border defenses were a large improvement over open camps, but they proved difficult to maintain against determined attackers – border protections can be worn down over time and defenders of large encampments are often spread thin at the outer wall.

As the size and sophistication of attacking forces grew, so did the sophistication of defensive structures. The most impressive such structures, constructed to withstand determined sieges in medieval times, used multiple tiers of defenses. Further, tiers were not strictly hierarchical in nature – rather, some structures could be defended independently of others. This major advancement in defense capabilities provided defenders with significant flexibility in defense strategy, the ability to observe attacker activities, and the ability to force attackers to deal with multiple independent defensive forces.

Applying the same ideas to computer and network security, border protections (i.e., firewalls and host OSs) can be augmented with security perimeters erected at many points within the borders. Enabled by low-cost computation (e.g., embedded processors, ASICs), security functionality can be embedded in most device microcontrollers, yielding "better security via smarter devices." We refer to devices with embedded security functionality as *self-securing devices* (see figure on page 1).

Self-securing devices can significantly increase network security and manageability, enabling capabilities that are difficult or impossible to implement in current systems. For example, independent device-embedded security perimeters guarantee that a penetrated boundary does not compromise the entire system. Uncompromised components continue their security functions even when other system components are compromised. Further, when attackers penetrate one boundary and then attempt to penetrate another, uncompromised components can observe and react to the intruder's attack; from behind their intact security perimeters, they can send alerts to the security administrator, actively quarantine or immobilize the attacker, and wall-off or migrate critical data and resources. Pragmatically, each self-securing device's security perimeter is simpler because of specialization, which should make correct implementations more likely. Further, distributing security checks among many devices reduces their performance impact and allows more checks to be made.

By augmenting conventional border protections with self-securing devices, this new security architecture promises substantial increases in both network security and security manageability. As with medieval fortresses, well-defended systems conforming to this architecture could survive protracted sieges by organized attackers.

Device-Embedded Security Examples

Network Interface Cards (NICs): The role of NICs in computer systems is to move packets between the system's components and the network. Thus, the natural security extension is to enforce security policies on packets forwarded in each direction. Like a firewall, a self-securing NIC does this by examining packet headers and simply not forwarding unacceptable packets into or out of the computer system. A self-securing NIC can also act as a machine-specific gateway proxy, achieving the corresponding protections without scalability or identification problems; by performing such functions at each system's NIC, one avoids the bottleneck imposed by current centralized approaches.

Storage Devices: The role of storage devices in computer systems is to persistently store data. Thus, the natural security extension is to protect stored data from attackers, preventing undetectable tampering and permanent deletion. A self-securing storage device does this by managing storage space from behind its security perimeter, keeping an audit log of all requests, and keeping previous versions of data modified by attackers. Since a storage device cannot distinguish compromised user accounts from legitimate users, the latter requires keeping all versions of all data. Finite capacities will limit how long such comprehensive versioning can be maintained, but 100% per year storage capacity growth will allow modern disks to keep several weeks of all versions. If intrusion detection mechanisms reveal an intrusion within this multi-week *detection window*, security

… continued on pg. 6

BETTER SECURITY VIA SMARTER DEVICES, CONT'D

… continued from pg. 5

administrators will have this valuable audit and version information for diagnosis and recovery.

Biometric Sensors: The role of biometric sensors in computer systems is to provide input to biometric-enhanced authentication processes, which promise to distinguish between users based on measurements of their physical features. Thus, the natural security extension is to ensure the authenticity of the information provided to these processes. A self-securing sensor can do this by timestamping and digitally signing its sensor information. Such evidence of when and where readings were taken is critical to secure use of biometric information because, unlike passwords, biometrics are not secrets. For example, anyone can lift fingerprints from a laptop with the right tools or download facial images from a web page. Thus, the evidence is needed to prevent straightforward forgery and replay attacks. Powerful self-securing sensors may also be able to increase security and privacy by performing the identity verification step from within their security perimeter and only exposing the results (with the evidence). By embedding mechanisms for demonstrating authenticity and timeliness inside sensor devices, one can verify sensor information (even over a network) even when intruders gain the ability to offer their own "sensor" data.

Graphical Displays: The role of graphical displays in computer systems is to visually present information to users. Thus, a natural security extension would be to ensure that critical information is displayed. A self-securing display could do this by allowing high-privilege entities to display data that cannot be overwritten or blocked by less-privileged entities. So, for example, a security administrator could display a warning message when there is a problem in the system (e.g., a suspected trojan horse or a new e-mail virus that must not be opened). By embedding this screen control inside the display device, one gains the ability to ensure information visibility even when an intruder gains control over the window manager.

Routers and Switches: The role of routers and switches in a network environment is to forward packets from one link to an appropriate next link. Thus, one natural security extension for such devices is to provide firewall and proxy functionality; many current routers provide exactly this. Some routers/switches also enhance security by isolating separate virtual LANs (VLANs). More dynamic defensive actions could provide even more defensive flexibility and strength. For example, the ability to dynamically change VLAN configurations would give security administrators the ability to create protected command and control channels in times of crisis or to quarantine areas suspected of compromise. When under attack, self-securing routers/switches could also initiate transparent replication of data services, greatly reducing the impact of denial-of-service attacks. Further, essential data sites could be replicated on-the-fly to "safe locations" (e.g., write-once storage devices) or immediately isolated via VLANs to ensure security.

For more information on the Self-Securing Devices project, visit our web pages at www.pdl.cs.cmu.edu and see the first publication abstract listed in this issue of the PDL Packet.

NEW PDL FACULTY

… continued from pg. 3

Srinivasan Seshan

Srinivasan Seshan joined CMU's SCS faculty in August 2000. He received his Ph.D. from the Computer Science Division of the University of California at Berkeley. There, Srini was part of the Daedalus, Infopad, and RAID groups. Before coming to CMU, Srini was a Research Staff Member in the Networking and Security Department the IBM Thomas J. Watson Research Center.

Srini's interests are in network software for computer systems. He is currently working on new network protocols and services to support ubiquitous computing applications and wide-area distributed network applications. In the past, he has worked on improvements to the TCP protocol, firewall design, performance prediction for Internet transfers, mobile computing, transport for wireless networks, routing for mobile systems, fast protocol stack implementations and RAID system design. Srini is also interested in many other areas in distributed computing and communication systems.