CMC

Center for Mobile Computing • Dartmouth College • July 2005 • cmc.cs.dartmouth.edu

CMC Launches Archive of Wireless-Network Research Data with NSF Funding

The National Science Foundation, through its Computing Research Infrastructure program, has funded a CMC research team to build a Community Resource for Archiving Wireless Data at Dartmouth (CRAWDAD). Professors David Kotz and Tristan Henderson will develop an archive of wireless network data and associated tools for collecting and processing the data, as a community resource for those involved in wireless network research and education. "This community is seriously starved for real data about real users on real networks," notes Kotz. "Our current limited collection of data is already in use at over 50 universities and research labs." On the other hand, Henderson observes that "it's really hard to collect large traces of wireless network activity, which makes many people reluctant to work with experimental data. Our new facility will dramatically increase the amount of data available, by making it easier to collect, share, and process traces of wireless network activity." The data will be freely available for research groups everywhere.

The three-year CRAWDAD project will construct a shared facility for storing large data sets collected from real wireless networks, develop common formats and tools for collecting, anonymizing, and analyzing this data, disseminate software and documentation for wireless data collection, and coordinate with other community efforts to develop network trace formats and tools. Kotz and Henderson plan to host annual workshops for those interested in using the archive or collaborating on tool development. They have already begun to work with community leaders to encourage contribution to and use of the archive. They will also encourage educators to use the tools and data in course projects and to share course modules.

By increasing the availability of data to research groups everywhere, CRAWDAD will enable new projects and enhance others in a broad range of research areas including workload characterization, location-aware services, network management, intrusion detection, quality of service, and protocol development. In every case, real data about real networks helps to better identify the real problems and to better validate proposed solutions.

For more information, visit
http://CRAWDAD.cs.dartmouth.edu.

Andrew Campbell joins Dartmouth, CMC

After several years on the faculty at Columbia University, Andrew Campbell is moving to Dartmouth College as an Associate Professor of Computer Science. Andrew brings to the CMC his long track record in mobile computing and wireless networking, and looks forward to working with CMC faculty and students on a variety of new projects.

Andrew is investigating the synthesis between the demands of highly dynamic systems (e.g., mobile and wireless systems), the need to embed better service creation engines into the network infrastructure, and the development of quantitative and scalable resource provisioning models for such environments. His work tends to connect the theoretical with the practical, architecting new networking systems that contribute to the development of the wireless Internet.

One of Andrew's current projects is Armstrong, which is focused on resilient transport and control mechanisms for sensor networks. This project is developing new technologies for wireless sensor and ad hoc networks. Andrew is perhaps best known for his work on Cellular IP, which provided an alternative approach to that found in mobile telecommunications (e.g., General Packet Radio Service) and in IP networking (Mobile IP). Cellular IP represents a new mobile host protocol that is optimized to provide access to a Mobile IP enabled Internet in support of fast-moving wireless hosts. Cellular IP incorporates a number of important cellular principles but remains firmly based on IP design principles allowing Cellular IP to scale from pico- to metropolitan-area installations.

Andrew received a prestigious NSF CAREER award in 1999, and his other research grants come from a wide variety of federal and corporate sources. Andrew has extensively served our scientific community through conference program committees and journal editorial boards. Most recently he was program co-chair for ACM MobiHoc 2005.

The CMC is pleased to have Andrew on the team.

Intel Tests Mesh Technology at Dartmouth College

A research team from Intel Labs in Hillsboro, Oregon recently deployed a 31-node WiFi mesh network in a Dartmouth residential cluster near campus. This mesh network, with an 802.11a bridge back to the core campus network, allowed the Intel researchers to test their mesh routing and configuration protocols in a realistic setting: a set of duplex homes occupied by a variety of Dartmouth staff and faculty.

Each node is a custom case enclosing a fairly generic Linux computer and three radios (802.11b, 802.11b, and 802.11a/b/g). These nodes formed an ad hoc "mesh" network among the nodes, provided access-point service to users, with a few of the nodes using the 802.11a/b/g radio to connect the mesh to the backhaul. Intel worked with Dartmouth to install a mesh node in each duplex housing unit, then spent several months testing and experimenting with their approach. "The mesh test bed at Dartmouth allowed us to experience aspects of a real world network that could never have been exposed in our research laboratories," said one Intel researcher.

After the trial finished, the nodes were removed and half now reside in the CMC lab where they are in use for our own experiments with mesh networks and wireless measurement. The CMC is grateful to Intel for the donation of this hardware.

Graduates

Patrick Schwarz recently completed his M.S. thesis, “Building a WLAN Model”. Patrick coded a MATLAB model of an IEEE 801.11b channel for modulation and power usage studies. Patrick has returned to Helmut Schmidt University in Hamburg, Germany to complete his MS degree.

Abdelfetah Jibril recently completed his M.S. thesis, “A study of the Impact of the Medium Conditions on the Battery of Wireless Client Stations on Parts of Dartmouth College’s IEEE 802.11b Network”. Abdel studies network usage and medium statistics in order to determine transmitted power, retry and collision rates, etc. The ultimate goal is to design a network requiring lower transmitted power, thereby increasing useful battery life of portable devices. Abdel, who worked with Professor Ted Cooley, is now working for Analog Devices, Inc. in Massachusetts.

CMC News

CMC Updates by Email

You can now receive CMC news by email. Simply send email to listserv@listserv.dartmouth.edu with a message whose body says only “SUB CMC-news”, or visit the CMC web site and click on the link in the News section.

First Release of the Greenpass Code

“Greenpass”, a system for delegating access authorization rights to guest users of a restricted wireless (or wired) network, is now available for downloading. Developed by Dartmouth College’s PKI Lab, the open-source code conveniently provides a temporary key for network use. Greenpass requires only an 802.1x capable machine and a standard web browser. The code is available at http://www.dartmouth.edu/~pkilab/greenpass/.

Arnab Paul Joins the CMC

Dr. Arnab Paul recently joined the CMC as a post-doctoral research associate working with Prof. David Kotz. His broad research interests lie in mobile and distributed systems and issues arising at the intersection of robustness and security in such systems. He recently finished his PhD from the College of Computing, Georgia Tech, where he worked on various projects including distributed storage, authentication protocols for wireless systems, cluster computing and distributed programming. His current work is focused on secure and fault tolerant sensor networks, and mesh networks.

Phone, Television, and Computers Converge at Dartmouth College

In 2001, Dartmouth embarked on a computing journey that started with the deployment of an enormous one-mile square wireless network. "Convergence" has now been achieved as the College switches its cable and satellite television system to the network. "We've built an infrastructure that supports video, voice, and data," says Brad Noblet, the Director of Technical Services. "Students and faculty today want instant information and communication, no matter where they are. Convergence makes the laptop the center of your world."

Dartmouth's new video-over-the-network system is facilitated by Video Furnace, a company based in Libertyville, Ill., that specializes in encoding video for broadcast over a data network. Their system allows for live transmission of television programs without separate software like QuickTime or RealPlayer. It works across Macintosh, PC, and Linux platforms, and it works on both the wired and wireless computer networks.

The channel offering can also expand with this software, from the current 62-channel capacity to nearly a thousand. Encryption and authentication provide full protection for all video content, insuring compliance with copyrights and distribution agreements. Only people within the Dartmouth infrastructure can access this programming. "Video Furnace drastically increases our ability to offer more channels to faculty, staff, and students compared with the old analog cable television system. Plus we have the opportunity to program our own channels, so in the future we might broadcast student projects, classroom lectures or even guest speakers," says Noblet. "I think the teaching and learning applications are endless." Thomas Luxon, the Cheheyl Professor and Director of the Dartmouth Center for the Advancement of Learning (DCAL), agrees. "The new video capability is very exciting. It will certainly expand the options for students and faculty members to work together to complete assignments and think creatively about new kinds of critical assignments," he says.

The Video Furnace deployment follows the 2004 migration from the traditional phone system to VoIP, or voice-over Internet protocol. According to Noblet, there are valuable cost savings by merging the three systems. He says that concentrating on one enhanced network avoided upgrading and maintaining three disparate networks and it resulted in a two-thirds savings. Both Luxon and Noblet are anxious to see the new and probably unusual applications that this new technology will bring about, and CMC researchers look forward to studying the effect of this traffic on the wireless network and the way that it changes network usage.

Dartmouth Upgrades WiFi Network with Aruba

Dartmouth College is replacing and expanding its pioneering campus-wide WiFi network. By year's end, most of the original 550 Cisco 802.11b access points will have been replaced by approximately 1,500 access points from Aruba Networks. These new 802.11a/b/g access points support all three WiFi technologies in a "wireless switch" architecture. The large number of access points provides the density required for the shorter-range and higher-bandwidth 802.11a, which is designed to support voice and video.

Indeed, "we've built a converged network," said Director of Technical Services Brad Noblet. "What that means is that we now use one network infrastructure to effect communications for data, voice, and video; all three services are now available on both the wireless and wired portions of the network." Last summer Dartmouth replaced all faculty and staff desk telephones with Cisco voice-over-IP (VoIP) telephone handsets, and supports the use of wireless VoIP handsets from Cisco and Vocera. This spring, Dartmouth launched a new video-over-IP service from VideoFurnace, which will eventually replace the cable TV network on campus (see above article for more details). Up to 62 cable TV channels are currently available on the wired network, and up to four are available to 802.11a users anywhere on campus.

For more information about the Dartmouth wireless network, follow the News link on the CMC homepage.

New Research Papers

Complete Text at http://cmc.cs.dartmouth.edu/papers

Kwang-Hyun Baek and Sean W. Smith. *Preventing Theft of Quality of Service on Open Platforms.* Technical Report TR2005-539, Dartmouth College, Computer Science, Hanover, NH, May 2005.

As multiple types of traffic converge onto one network (frequently wireless), enterprises face a tradeoff between effectiveness and security. Some types of traffic, such as voice-over-IP (VoIP), require certain quality of service (QoS) guarantees to be effective. The end client platform is in the best position to know which packets deserve this special handling. In many environments (such as universities), end users relish having control over their own machines. However, if end users administer their own machines, nothing stops dishonest ones from marking undeserving traffic for high QoS. How can an enterprise ensure that only appropriate traffic receives high QoS, while also allowing end users to retain control over their own machines? In this paper, we present the design and prototype of a solution, using SELinux, TCPA/TCG hardware, Diffserv, 802.1x, and EAP-TLS.

Kwang-Hyun Baek, Sean W. Smith, and David Kotz. *A survey of WPA and 802.11i RSN authentication protocols.* Technical Report TR2004-524, Dept. of Computer Science, Dartmouth College, Hanover, NH, November 2004.

In the new standards for WLAN security, many choices exist for the authentication process. In this paper, we list eight desired properties of WLAN authentication protocols, survey eight recent authentication protocols, and analyze the protocols according to the desired properties.

JS.W. Smith. *Trusted Computing Platforms: Design and Applications.* Springer, 2004.

Mobile computing requires greater use of surrounding "local" infrastructure that may now be controlled by another party, and consequently be less trustworthy. This book is a grand survey of hardware techniques in this space.

David Blinn, Tristan Henderson, and David Kotz. *Analysis of a Wi-Fi hotspot network.* In Proceedings of the International Workshop on Wireless Traffic Measurements and Modeling (WiTMeMo '05), pages 1-6, June 2005.

Wireless hotspot networks have become increasingly popular in recent years as a means of providing Internet access in public areas such as restaurants and airports. In this paper we present the first study of such a hotspot network. We examine five weeks of SNMP traces from the Verizon Wi-Fi HotSpot network in Manhattan. We find that far more cards associated to the network than logged into it. Most clients used the network infrequently and visited few APs. AP utilization was uneven and the network displayed some unusual patterns in traffic load. Some characteristics were similar to those previously observed in studies of campus WLANs.

Zack Butler and Daniela Rus. *Event-based control for mobile sensors.* IEEE Pervasive Computing, 2(4):34-42, Oct-Dec 2003.

In many sensor networks, considerably more units are available than necessary for simple coverage of the space. Augmenting sensor networks with motion can exploit this surplus to enhance sensing while also improving the network's lifetime and reliability. Sensor mobility allows better coverage in areas where events occur frequently. Another use of mobility comes about if the specific area of interest (within a larger area) is unknown during deployment. We've developed distributed algorithms for mobile-sensor networks to physically react to changes or events in their environment or in the network itself. Distribution supports scalability and robustness during sensing and communication failures. We present two classes of motion-control algorithms that let sensors converge on arbitrary event distributions. These algorithms trade off the amount of required computation and memory with the accuracy of the sensor positions. We also present three algorithms that let sensor networks maintain coverage of their environment. These algorithms work alongside either type of motion-control algorithm such that the sensors can follow the control law unless they must stop to ensure coverage.

Guanling Chen, Kazuhiro Minami, and David Kotz. *Naming and discovery in mobile systems.* In Rajeev Shorey, Chan Mun Choon, A. Ananda, and Ooi Wei Tsang, editors, Mobile, Wireless and Sensor Networks, John Wiley, 2005. Accepted for publication.

Middleware supporting mobile applications must provide naming and discovery functionalities to enable anytime and anywhere service access. In this chapter, we survey existing service-discovery standards, identify four challenges for naming and discovery in a mobile environment, and provide a detailed discussion of the approaches that can be used to address each of these challenges.

Guanling Chen and David Kotz. *Policy-driven data dissemination for context-aware applications.* In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, pages 283-289, Kauai, Hawaii, March 2005. Short paper.

Context-aware pervasive-computing applications require continuous monitoring of their physical and computational environment to make appropriate adaptation decisions in time. The data streams produced by sensors, however, may overflow the queues on the dissemination path. Traditional flow-control and congestion-control policies either drop data or force the sender to pause. When the data sender is sensing the physical environment, however, a pause is equivalent to dropping data. Instead of arbitrarily dropping data that may contain important events, we present a policy-driven data dissemination service named PACK, based on an overlay-based infrastructure for efficient multicast delivery. PACK enforces application-specified policies that define how to discard or summarize data flows wherever queues overflow on the data path, notably at the mobile hosts where applications often reside. A key contribution of our approach is to uniformly apply the data-stream ``packing'' abstraction to queue overflow caused by network congestion, slow receivers, and temporary disconnection. We present experimental results and a detailed application study of the PACK service.

Tristan Henderson, Denise Anthony, and David Kotz. *Measuring wireless network usage with the experience sampling method.* In Proceedings of the First Workshop on Wireless Network Measurements (WiNMee), April 2005.

Measuring wireless local area networks has proven useful for characterizing, modeling and provisioning these networks. These measurements are typically taken passively from a vantage point on the network itself. Client devices, or users, are never actively queried. These measurements can indicate what is happening on the network, but it can be difficult to infer why a particular behavior is occurring. In this paper we use the Experience Sampling Method (ESM) to study wireless network users. We monitored 29 users remotely for one week, and signaled them to fill out a questionnaire whenever interesting wireless behavior was observed. We find ESM to be a useful method for collecting data about wireless network usage that cannot be provided by network monitoring, and we present a list of recommendations for network researchers who wish to conduct an ESM study.

Tristan Henderson and David Kotz. *Measuring wireless LANs.* In Rajeev Shorey et al., editor, Mobile, Wireless and Sensor Networks: Technology Applications and Future Directions. John Wiley & Sons, New York, NY, 2005. Accepted for publication.

Wireless local area networks have become increasingly popular in recent years, and are now commonplace in many venues, including academic and corporate campuses, residences, and “hotspots” in public areas. It is important to understand how these wireless LANs are used, both for deploying networks, and for the development of future wireless networking protocols and applications.

In this chapter we discuss the measurement and analysis of the popular 802.11 family of wireless LANs. We describe the tools, metrics and techniques that are used to measure wirelss LANs. The results of existing measurement studies are surveyed. We illustrate some of the problems that are specific to measuring wireless LANs, and outline some challenges for collecting future wireless traces.

New Research Papers (Continued)

A. Iliev and S.W. Smith. *Private information storage with logarithmic-space secure hardware.* In Information Security Management, Education, and Privacy. and Proceedings of i-NetSec 04: 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems, pages 201-216. Kluwer, 2004.

In Private Information Retrieval (PIR), a user obtains one of N records from a server, without the server learning what record was requested.

In Proceedings of i-NetSEc, the Third Working Conference on Privacy and Anonymity in Networked and Distributed Systems. This task is very similar to the one undertaken by the older Oblivious RAMs work, and indeed the latest PPIR work uses techniques developed for Oblivious RAMs. Previous PPIR work had two limitations: the internal space required was still O (N lg N) bits, and records could only be read privately, not written.

In this paper, we present a design and experimental results that overcome these limitations. We reduce the internal memory to O(\lg N) by basing the pseudorandom permutation on a Luby-Rackoff style block cipher, and by redesigning the oblivious shuffle to reduce space requirements and avoid unnecessary work. This redesign yields both a time and a space savings. These changes expand the system's applicability to larger datasets and domains such as private file storage.

These results have been implemented for the IBM 4758 secure coprocessor platform, and are available for download

Minkyong Kim and David Kotz. *Classifying the mobility of users and the popularity of access points.* In Thomas Strang and Claudia Linnhoff-Popien, editors, Proceedings of the International Workshop on Location- and Context-Awareness (LoCA), volume 3479 of Lecture Notes in Computer Science, pages 198-209, Germany, May 2005. Springer-Verlag.

There is increasing interest in location-aware systems and applications. It is important for any designer of such systems and applications to understand the nature of user and device mobility. Furthermore, an understanding of the effect of user mobility on access points (APs) is also important for designing, deploying, and managing wireless networks. Although various studies of wireless networks have provided insights into different network environments and user groups, it is often hard to apply these findings to other situations, or to derive useful abstract models.

In this paper, we present a general methodology for extracting mobility information from wireless network traces, and for classifying mobile users and APs. We used the Fourier transform to convert time-dependent location information to the frequency domain, then chose the two strongest periods and used them as parameters to a classification system based on Bayesian theory. To classify mobile users, we computed diameter (the maximum distance between any two APs visited by a user during a fixed time period) and observed how this quantity changes or repeats over time. We found that user mobility had a strong period of one day, but there was also a large group of users that had either a much smaller or much bigger primary period. Both primary and secondary periods had important roles in determining classes of mobile users. Users with one day as their primary period and a smaller secondary period were most prevalent; we expect that they were mostly students taking regular classes. To classify APs, we counted the number of users visited each AP. The primary period did not play a critical role because it was equal to one day for most of the APs; the secondary period was the determining parameter. APs with one day as their primary period and one week as their secondary period were most prevalent. By plotting the classes of APs on our campus map, we discovered that this periodic behavior of APs seemed to be independent of their geographical locations, but may depend on the relative locations of nearby APs. Ultimately, we hope that our study can help the design of location-aware services by providing a base for user mobility models that reflect the movements of real users.

Minkyong Kim and David Kotz. *Modeling users' mobility among WiFi access points.* In Proceedings of the International Workshop on Wireless Traffic Measurements and Modeling (WiTMeMo '05), March 2005.

Modeling movements of users is important for simulating wireless networks, but current models often do not reflect real movements. Using real mobility traces, we can build a mobility model that reflects reality. In building a mobility model, it is important to note that while the number of handheld wireless devices is constantly increasing, laptops are still the majority in most cases. As a laptop is often disconnected from the network while a user is moving, it is not feasible to extract the exact path of the user from network messages. Thus, instead of modeling individual user's movements, we model movements in terms of the influx and outflux of users between access points (APs). We first counted the hourly visits to APs in the syslog messages recorded at APs. We found that the hourly number of visits has a periodic repetition of 24 hours. Based on this observation, we aggregated the visits of multiple days into a single day. We then clustered APs based on the different peak hour of visits. We found that this approach of clustering is effective; we ended up with four distinct clusters and a cluster of stable APs. We then computed the average arrival rate and the distribution of the daily arrivals for each cluster. Using a standard method (such as \emphthinning) for generating non-homogeneous Poisson processes, synthetic traces can be generated from our model.

David Kotz and Kobby Essien. *Analysis of a campus-wide wireless network.* Wireless Networks, 11:115-133, 2005.

Understanding usage patterns in wireless local-area networks (WLANs) is critical for those who develop, deploy, and manage WLAN technology, as well as those who develop systems and application software for wireless networks. This paper presents results from the largest and most comprehensive trace of network activity in a large, production wireless LAN. For eleven weeks we traced the activity of nearly two thousand users drawn from a general campus population, using a campus-wide network of 476 access points spread over 161 buildings at Dartmouth College. Our study expands on those done by Tang and Baker, with a significantly larger and broader population.

We found that residential traffic dominated all other traffic, particularly in residences populated by newer students; students are increasingly choosing a wireless laptop as their primary computer. Although web protocols were the single largest component of traffic volume, network backup and file sharing contributed an unexpectedly large amount to the traffic. Although there was some roaming within a network session, we were surprised by the number of situations in which cards roamed excessively, unable to settle on one access point. Cross-subnet roams were an especial problem, because they broke IP connections, indicating the need for solutions that avoid or accommodate such roams.

Qun Li and Daniela Rus. *Global clock synchronization in sensor networks.* In Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE Computer Society Press, May 2004.

Global synchronization is crucial to many sensor netowrk applications that require precise mapping of the collected sensor data with the time of the events, for example in tracking and surveillance. It also plays an important role in energy conservation in MAC layer protocols. This paper discusses three methods to achieve global synchronization in a sensor network: a node-based approach, a hierarchical cluster-based method, and a fully localized diffusion-based method. We also give the synchronous and asynchronous implementations of the diffusion-based protocols.

Kazuhiro Minami and David Kotz. *Secure context-sensitive authorization.* Journal of Pervasive and Mobile Computing, 1(1):123-156, March 2005.

There is a recent trend toward rule-based authorization systems to achieve flexible security policies. Also, new sensing technologies in pervasive computing make it possible to define context-sensitive rules, such as ``allow database access only to staff who are currently located in the main office.'' However, these rules, or the facts that are needed to verify authority, often involve sensitive context information. This paper presents a secure context-sensitive authorization system that protects confidential information in facts or rules. Furthermore, our system allows multiple hosts in a distributed environment to perform the evaluation of an authorization query in a collaborative way; we do not need a universally trusted central host that maintains all the context information. The core of our approach is to decompose a proof for making an authorization decision into a set of sub-proofs produced on multiple different hosts, while preserving the integrity and confidentiality policies of the mutually untrusted principals operating these hosts. We prove the correct-

New Research Papers (Continued)

Jason Liu, Yougu Yuan, David M. Nicol, Robert S. Gray, Calvin C. Newport, David Kotz, and Luiz Felipe Perrone. *Validation of wireless models using direct-execution simulation of ad-hoc routing protocols.* Simulation: Transactions of The Society for Modeling and Simulation International, January 2005. Accepted for publication in the ``Best of PADS 2004'' special issue.

Computer simulation has been used extensively as an effective tool in the design and evaluation of systems. One should not, however, underestimate the importance of validation-the process of ensuring whether a simulation model is an appropriate representation of the real-world system. Validation of wireless network simulations, particularly wireless ad-hoc routing protocol simulations, is difficult because not only must the implementation of the simulated protocol be validated against its design specifications, but also the wireless model must capture important characteristics of the wireless environment. In this paper, we present our approach of using direct-execution simulation to validate wireless models against real outdoor experiments. In particular, we conducted an outdoor trial run of four ad-hoc routing algorithms running on thirty-three 802.11-enabled laptops moving randomly in an athletic field. This paper documents a common testbed that supports direct execution of a set of ad-hoc routing protocol implementations in a wireless network simulator. The testbed reads traces collected from a real experiment, and uses them to drive direct-execution implementations of the routing protocols. Doing so we are able to reproduce the same network condition as in a real experiment. By comparing routing behavior measured in the real experiment with behavior computed by the simulation, we are able to validate the models of radio behavior upon which protocol behavior depends. We conclude that, contrary to popular belief, it is possible to have fairly accurate results using a simple wireless model. We observed, however, that the routing behavior is quite sensitive to one of this model's parameters. The implication is that one should i) use a more complex wireless model that explicitly models point-to-point path loss, ii) use measurements from an environment typical of the one of interest, or iii) study behavior over a range of environments to identify the sensitivities of the protocol's performance under different network conditions.

J. Marchesini, S.W. Smith, O. Wild, J. Stabiner, and A. Barsamian. *Open-source applications of tcpa hardware.* In 20th Annual Computer Security Applications Conference. IEEE Computer Society, December 2004.

How can Alice trust computation occurring at Bob's computer? Since it exists and is becoming ubiquitous, the current-generation TCPA/TCG hardware might enable a solution. When we started investigating this technology, the specification of the TCG software stack was not publicly available, and an implementation is still not; so, we designed and built an open-source platform based on Linux and commercially available TCPA/TCG hardware which would allow us to address the problem of trusting computation. Within the limits of TCPA/TCG hardware security, our solution balances what Alice needs to do to make trust judgments against what Bob needs to do to keep his system running.

Furthermore, we describe how we use our platform to harden three sample open-source applications: Apache SSL Web servers, OpenCA certification authorities, and (with SELinux) compartmented attestation to balance privacy with DRM.

To our knowledge, our project remains the only open-source TCPA/TCG platform in existence, and is also enabling trusted computing applications developed by our user community (enforcer.sourceforge.net reports over 1100 sourcecode downloads so far).

Kazuhiro Minami and David Kotz. *Secure context-sensitive authorization.* In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications (PerCom), pages 257-268, Kauai, Hawaii, March 2005.

There is a recent trend toward rule-based authorization systems to achieve flexible security policies. Also, new sensing technologies in pervasive computing make it possible to define context-sensitive rules, such as ``allow database access only to staff who are currently located in the main office.'' However, these rules, or the facts that are needed to verify authority, often involve sensitive context information. This paper presents a secure context-sensitive authorization system that protects confidential information in facts or rules. Furthermore, our system allows multiple hosts in a distributed environment to perform the evaluation of an authorization query in a collaborative way; we do not need a universally trusted central host that maintains all the context information. The core of our approach is to decompose a proof for making an authorization decision into a set of sub-proofs produced on multiple different hosts, while preserving the integrity and confidentiality policies of the mutually untrusted principals operating these hosts.

Jihwang Yeo, Moustafa Youssef, Tristan Henderson, and Ashok Agrawala. *An accurate technique for measuring the wireless side of wireless networks.* In Proceedings of the International Workshop on Wireless Traffic Measurements and Modeling, Seattle, WA, USA, pages 13-18, June 2005. USENIX.

Wireless monitoring (WM) is a passive approach for capturing wireless-side traffic with rich MAC/PHY layer information. WM can suffer, however, from low capture performance, i.e., high measurement loss, due to the unreliable wireless medium. In this paper, we experimentally show that WM can perform reliable and accurate measurements on wireless traffic, in actual, non-ideal channel conditions. We demonstrate how to increase capture performance by merging traces from multiple monitoring devices. This merging enables WM to capture over 99% of the IP layer traffic and over 97% of the MAC/PHY frames in a controlled experiment. Our results indicate that WM enables reliable analysis of the collected traces, and should encourage the wireless research community to use this technique for a wide variety of research areas, such as traffic analysis, user mobility and handoff analysis, and MAC/PHY anomaly detection.

To hear about new CMC papers as soon as they're posted, subscribe to the CMC-Papers mailing list. Simply send email to listserv@listserv.dartmouth.edu with a message whose body says only "SUB CMC-papers", or visit the CMC web site and click on the link in the Papers section.

About the CMC

The goal of the Center for Mobile Computing at Dartmouth College is to realize the potential for ubiquitous mobile devices and wireless communications to improve the way we live, the way we work, and the way we learn.

We have the opportunity to leverage Dartmouth's campus-wide wireless network, its group of experienced researchers, its residential campus with an innovative and creative student culture, its long tradition of pervasive deployment of cutting-edge technology and of technology in the classroom, and its local institutes for Security Technology (ISTS) and Information Infrastructure Protection (I3P). This combination makes Dartmouth College a unique environment for understanding the future, in which mobile computing becomes ubiquitous on university campuses, corporate campuses, and the consumer world.

The CMC is comprised of researchers from the Departments of Computer Science and Sociology and from the Thayer School of Engineering, including faculty, post-doctoral researchers, M.E. and Ph.D. students, and undergraduate students, and of staff from Dartmouth's Computing Services department. Participating faculty members have extensive experience in wireless networks, sensor networks, mobile agents, parallel and distributed computing, operating systems, information retrieval, robotics, signal processing, and sociology.

The Center's projects receive funding from the CMC industrial Partners, and federal funding from the Department of Homeland Security (through ISTS), the Defense Advanced Research Projects Agency (DARPA), the Office of Naval Research, and the National Science Foundation.

Center research facilities include campus-wide wired and wireless networks as well as a heterogeneous collection of computing systems. In effect, Dartmouth College is an extensive testbed with several thousand networked computers and active users.

Partnership

We invite corporations to become Partners of the CMC. Partners have early access to advanced research that can lead to next-generation products and services. At the same time, the CMC benefits from a better understanding of the needs and direction of industry, helping to keep research relevant and driven by application needs.

Contact us if you are interested in being a partner at cmc@cs.dartmouth.edu

Benefits:

- Access to CMC students, making connections that may lead to future employment
- Access to CMC faculty
- Early access to prototypes
- Access to CMC labs and facilities, when appropriate.

Ultimately, each partnership leads to a host of benefits and to a relationship that can be customized to the needs and interests of the partner.

Current Partners

NTT DoCoMo

DoCoMo USA Labs

Current Sponsors

U.S. Department of Homeland Security

NSF

Cisco Systems

intel

CMC Faculty and Staff

http://cmc.cs.dartmouth.edu/people/

Professor Denise Anthony, Department of Sociology

Professor Andrew Campbell, Department of Computer Science

Professor Ted Cooley, Thayer School of Engineering

Professor George Cybenko, Thayer School of Engineering

Adjunct Professor Bob Gray, Department of Computer Science

Research Professor Tristan Henderson, Department of Computer Science

Professor David Kotz, Department of Computer Science

Research Professor Sue McGrath, Thayer School of Engineering

Adjunct Professor Daniela Rus, Department of Computer Science

Professor Sean Smith, Department of Computer Science

Brad Noblet,
Director of Technical Services,
Peter Kiewit Computing Services

Ron Peterson,
Senior Programmer,
Department of Computer Science

CONTACTS

General information, partnership inquiries, and subscription changes: *cmc@cs.dartmouth.edu*

All Dartmouth people mentioned in this newsletter can be reached at:
firstname.lastname@dartmouth.edu