

ISTS *Bulletin*

Winter/ Spring 2008

www.ists.dartmouth.edu

Volume 5, Number 1

ISTS On the Road

ISTS researchers have been busy presenting their findings since our last newsletter. In the following dispatches, Sergey Bratus and Patrick Tsang provide trip reports on conferences at which they have presented.

In August 2007, ISTS Research Associate Sergey Bratus gave a presentation at *Defcon 15* on the packet and log data organization tools that were developed under the Kerf project. The Kerf project investigated the application of machine learning and data organization algorithms for automated log analysis, and, in particular, intrusion analysis. Its goal was to produce a new breed of algorithms that would help the analysts sift through logs in a more productive way, learning from the choices they made while browsing the data.

Defcon is a hacker convention with a long history of disclosing critical vulnerabilities in ubiquitously used technologies; arguably, it is the most famous and influential one of its kind, and we, as a community of computer users, are much safer for it. In the last few years the conference itself has become an event frequently covered by major news media organizations. Its attendance has skyrocketed to over 7,000, a good part of which are "feds" (as the conference attendees generally refer to law enforcement and other government employees), security officers and researchers of major corporations, interested academics, and other "white hats". One thing that unites the attendees is their focus on practice rather than theory, and the expectation of gaining practically applicable knowledge from every talk; as such, presenting to this group sometimes proves challenging.

In October 2007, Sergey presented a paper on attacking and securing networked embedded devices built on commodity computing architectures at the *Workshop on Embedded Systems Security*, part of the Embedded Systems Week, held in Salzburg, Austria. (This year the workshop will be held in Atlanta, GA.) The work presented

continued on page 2

Thank You David Kotz

As the New Year began, David Kotz's term as the Executive Director of the Institute for Security Technology Studies (ISTS) came to an end. Dave held the position since 2004 and was the Director of Research and Development for the Institute the year prior to his appointment as Executive Director. Over the years, Dave's commitment and dedication to all aspects of the Institute were immeasurable - he is leaving ISTS in a strong position.

Dave is already back to teaching and will continue to do so for the remainder of the academic year.

In July 2008, Dave and his family will move to India where he will begin a well-deserved twelve-month sabbatical at the Indian Institute of Science, Bangalore. While there Dave will focus his research on wireless-network measurement and modeling, expanding on his work in the MAP project at ISTS.

Dave will continue to play an active role in ISTS. He will act as principal investigator on several ISTS projects until he leaves for India and will contribute to ISTS as a faculty affiliate. Dave's efforts on the MAP and DIST projects will continue on and Dave will provide contributions to these programs even while in India.

Dave is enthusiastic about the future of ISTS. "The great thing about ISTS is that we have a strong and diverse group of interdisciplinary faculty, coupled with a rich infrastructure, bright technical staff and students, and supported by a fantastic administrative group. I look forward to working with the team to expand on ISTS's past successes and forge new directions in cyber security and trust."

We want to thank Dave for all he has done for ISTS, Dartmouth, and information security during his time as Executive Director. We wish him all the best in his future endeavors and are glad to know that while he is stepping down as the Director, he will still be working closely with us.



David Kotz

Martin N. Wybourne
Vice Provost for Research

Inside This Issue

Behavioral Fingerprinting of Wireless Devices	2
Secure Information Systems Mentoring and Training	3
Business Essentials for the Information Security Professional	4
Virtual Terrorism Response Academy (VTRA)	4
Faculty Profile	6

was partly a result of ISTS' involvement in the *Campus Security Initiative* started by Dartmouth's Peter Kiewit Computing Service's leadership, and was based on hacking a particular device that was at one point deployed throughout the Dartmouth network. A large part of the presentation described sophisticated attacks (such as various side-channel attacks) on widely deployed devices. Sergey reports that chatting with industry people who deal with automotive embedded systems was a real eye-opener: e.g., he had never thought of his car as a network -- just as prone to design compromises, and therefore, possibly, just as attackable as more familiar network types.

In February, Sergey and ISTS researchers Cory Cornelius and Dan Peebles presented their active 802.11 access point fingerprinting tool at the *Shmoocon 4* hacker conference. (The "Fingerprinting" project is detailed in the article, "Behavioral Fingerprinting of Wireless Devices".) *Shmoocon* is a relatively recent addition to the hacker convention scene, started by the "Shmoo" group of hackers, whose primary interest was in all things wireless. Once advertised, somewhat tongue-in-cheek, as "conveniently located close to all of your favorite three-letter agencies", this Washington, D.C. area event is well-attended by security researchers who work in the area.

The more academic part of their fingerprinting work will be presented at the *First ACM Conference of Wireless Security (WiSec '08)* in Alexandria, VA March 31 – April 2. This conference brings together researchers exploring the wide range of present and future wireless networking technologies, from the entrenched 802.11 and cellular to metropolitan, vehicular, ad hoc, satellite, underwater, and sensor networks, as well as RFID.

Finally, in April, Sergey gave an invited talk presenting the analysis tools and approaches that came out of the Kerf project and subsequent work at *Troopers08* in Munich, Germany. *Troopers08* is an international IT security practitioner conference, intended to introduce the attendees, that range from corporate officers and auditors to administrators and consultants, to in-depth knowledge about attacking and defending IT infrastructure.

At the *14th ACM Conference on Computer and Communications Security (CCS '07)* held last October in Alexandria, VA, Patrick Tsang presented the paper "*Blacklistable Anonymous Credentials: Blocking Misbehaving Users without TTPs*" he co-authored with Man Ho Au, Apu Kapadia and Sean Smith.

The presented paper introduces the *BLacklistable Anonymous Credential (BLAC)* system, the first cryptographic construction of an anonymous credential system with provable security that allows services to judge user misbehavior and blacklist misbehaving anonymous users without relying on trusted third parties that are capable of revoking the privacy of users at will. Since blacklisted users remain anonymous, misbehaviors can be judged subjectively without users fearing arbitrary deanonymization by a TTP.

Anonymous access to services such as Wikipedia and YouTube empowers users to disseminate content without the fear of persecution — a user may add political content on

Wikipedia that is forbidden by his or her government, or post a video of police brutality to YouTube. In such cases, while Wikipedia and YouTube may want to penalize users who deface webpages or post copyrighted material, it is of paramount importance for services to preserve the anonymity of their well-behaving users. By guaranteeing anonymity to *all* users, anonymous blacklisting allows services to penalize misbehavior without the risk of exposing legitimate users such as political dissenters.

In several existing credential systems, users can authenticate to services anonymously. Since anonymity can give users the license to misbehave, some variants allow the selective deanonymization (or linking) of misbehaving users upon a complaint to a trusted third party. The ability of the TTP to revoke a user's privacy at any time, however, is too strong a punishment for misbehavior. To limit the scope of deanonymization, systems such as "e-cash" have been proposed in which users are deanonymized under only certain types of well-defined misbehavior such as "double spending." While useful in some applications, it is not possible to generalize such techniques to more subjective definitions of misbehavior.

The annual *ACM Conference on Computer and Communications Security* is a leading international forum for information security researchers, practitioners, developers and users from academia, government and industry to explore cutting-edge ideas and results, as well as to exchange techniques, tools, and experiences.

Behavioral Fingerprinting of Wireless Devices

In 2007 ISTS, through a grant from the Department of Justice's Bureau of Justice Assistance, provided seed funding for a wireless device fingerprinting project. The goal of this project was to provide link-layer only tools that could determine some facts about the make, chipset and driver of a wireless station, even if it tried to masquerade as another kind of device (for example, a laptop trying to masquerade as a legitimate access point to lure unsuspecting users). While various OSI Layer 3 TCP/IP fingerprinting tools have long become the mainstay of security assessment and penetration testing, Layer 2 approaches and tools have been conspicuously lacking. The "Fingerprinting" Team set out to fill that gap.

At heart, the Team's approach is very simple: they identify a device such as an access point (AP) by engaging it in a standard frame exchange, except that the frames they send are non-standard, downright malformed, or do not make sense according to the 802.11 specifications. However, for reasons of performance or for the sake of accommodating new features that set them apart from the competition, different vendors dispensed with different "sanity checks" on incoming frames, so that their products respond to some of the non-sensical ones. The specific set characterizes their product among others with some accuracy and gives one the capability to distinguish between different chipset — driver combinations.

One important circumstance lends additional value to this capability. It appears that the authors of early 802.11 security mechanisms (such as WEP) based their design on the

“perimeter defense” or “castle vs. barbarians” threat model: APs could authenticate a client station such as a laptop by checking whether they had knowledge of a shared secret, but clients lacked a mechanism for authenticating the APs. As it turned out, the real threat was elsewhere: most high-profile attacks started with tricking clients into attempting to associate with the wrong AP, an “evil twin” of the real one. The client, usually a laptop, was then snooped upon or exploited.

Thus it was not enough to keep “barbarians” outside, it was also important to make sure that the clients could find the right “castles” (APs). Subsequent authentication protocols such as WPA2 Enterprise provided the clients with a cryptographic mechanism to authenticate an AP as belonging to a trusted set. Problem solved?

Unfortunately, many 802.11 drivers that implement their devices’ link layer functionality and are therefore necessary to support the mutual cryptographic authentication, were shown to be vulnerable to malicious frames, giving the attacker remote code execution, and thus full kernel-level control! This is not surprising, considering the complexity of the 802.11 link layer, designed to accommodate many features envisioned by various vendors, some of which never materialized, but still has protocol elements reserved for them. Succinctly put, “complexity kills”.

Thus, despite solid cryptographic solutions, a rather odd chicken-and-egg problem persists: it is best to avoid communicating with an untrusted AP, but such trust can only be established through communication. Since in the initial phases of such communications it is trivial for an attacker to spoof APs that a client is looking for, we end up with a conundrum.

The Team’s fingerprinting tool provides some help in such situations: if it recognizes an “evil twin” is based on a different vendor’s architecture, it can alert the user of this fact. Fingerprinting can be used as a “secret handshake” to help validate the AP, prior to any other more complex (and thus more risky) exchanges. Naturally, a range of more traditional fingerprinting uses is possible: reconnaissance, finding unauthorized APs, and so on.

See more about the Fingerprinting Project Team in the “ISTS On the Road” section.

Secure Information Systems Mentoring and Training

As part of its core educational mission, ISTS is sponsoring a program to help foster expertise in information security at small colleges and liberal arts institutions throughout the Northeast and New England. The SISMAT (Secure Information Systems Mentoring and Training) program seeks to help train undergraduates in a variety of areas, including network security tools, basic cryptography concepts, and secure protocols. SISMAT combines intense hands-on training, a paid internship, and independent research support for students who will be college juniors or seniors during the 2008-2009 school year.

SISMAT is recruiting computer science students with an in-

terest and aptitude for security-related thinking and problem solving. The ability to work well with others, think creatively, absorb a variety of information in a short amount of time, and a desire to practically apply that knowledge are all more important than a student’s GPA, although academic qualifications are also a factor in program admission. SISMAT especially seeks students from populations traditionally underrepresented in computer science, including women and minorities.

As the demand from industry, government, and other sectors for skilled information technology and computer science graduates grows, a critical part of that demand is for knowledgeable, competent security specialists who understand the interplay between security and complex systems. One of the primary purposes of SISMAT is to identify motivated and talented undergraduates and inculcate them with an appreciation for the issues involved in monitoring networks and managing the interplay of cryptosystems. Dartmouth and ISTS have particular expertise in these two areas, which helps distinguish SISMAT from other security “crash courses.”

The selected undergraduates will be invited to participate in the SISMAT training course, a two-week seminar to be held at Dartmouth from June 16 to June 27. The seminar will incorporate both lecture-style meetings, guest speakers, and extensive lab work meant to give participants hands-on experience with the tools used in the real world. After the seminar, students will then undertake an internship in information security using the techniques they have learned at Dartmouth.

SISMAT also aims to help students and their faculty mentors grow the systems security and cryptography curriculum at their home institution. To this end, students will undertake a mentored research project in security in the Fall semester following their internship. These mentored research projects are an ideal way to develop the curriculum for a security topics course that the faculty member wants to lead.

SISMAT is in its inaugural, pilot year. SISMAT will help educate a new generation of security professionals to meet the needs of commercial, governmental, and non-profit organizations, as well as facilitate the improvement of security education throughout the region. The program’s focus (Public Key Infrastructures and trusted systems) reflects areas of expertise that these organizations currently desire in security interns or new employees.

We are excited about the possibilities and relationships this type of program can help nurture, and its potential to enhance Dartmouth’s reputation as a center for excellence in practical information security. If you are a student interested in applying to the program, a professor interested in taking on a mentoring role, or an organization interested in hosting a SISMAT intern, please see our website (<http://www.cs.dartmouth.edu/~sismat/>) for more information or contact us at sismat@cs.dartmouth.edu.



Business Essentials for the Information Security Professional

Tuck's Center for Digital Strategies and Tuck Executive Education at Dartmouth have developed a new program entitled "Business Essentials for the Information Security Professional," which will be held on May 12-16, 2008 at the Tuck School of Business at Dartmouth College. This program, sponsored in part by ISTS through a grant from the Department of Homeland Security's National Cyber Security Division (NCSD), is designed for chief information security officers (CISOs) and their direct reports seeking to enhance their fundamental business skills and knowledge, to complement their technical expertise and to communicate more effectively with other strategic business leaders in the company.



Hans Brechbühl and Eric Johnson

"Many security professionals find their security initiatives hindered because of their inability to communicate effectively within their firms," says Hans Brechbühl, executive director of the Center for Digital Strategies and the program's faculty director. "Simply understanding the technology and the technical risks is often not enough to generate action. Security executives must understand how the issues tie in across the enterprise to help them communicate information security risk in a way that the rest of the business will hear and understand its importance."

Developed in part through the Center for Digital Strategies' research and through workshops with leading CISOs from Global 1000 firms, this program will convey business concepts and skills that will help the information security professional to better understand how business leaders think, to appreciate organizational dynamics, to build an information security strategy, and to create a business case for security investments. The program will feature expert faculty from the Tuck School of Business, including Paul Argenti, Pino Audia, Sydney Finkelstein, Stephen Powell, and Kent Womack, and a curriculum tailored to the needs of today's information security professional. Over the course of the four days, executives will be engaged in the following topic areas: "Strategic Thinking and Planning;" "Leadership, Change, and Organizations;" "Communications, Power, and Influence;" "Risk, Investment, and Decision-Making;" and "Program/Project Management and Governance." These topics will be presented through a variety of methods, including short lecture presentations, case discussions, interactive projects, and individual and small group exercises.

"While this program will certainly have a significant impact on the practice of security management," said Eric John-

son, director of the Center for Digital Strategies, "we also believe it will represent leading-edge education and be a powerful way to bring top information security professionals into the research process at Dartmouth—bringing theory and practice of information security closer together."

For more information about this program, contact Jennifer Childs, Program Manager for the Center for Digital Strategies, at 603-646-0899, or visit the program website at www.tuck.dartmouth.edu/besp.

Virtual Terrorism Response Academy (VTRA)

In January 2007, Dartmouth College's Interactive Media Laboratory (IML) released a training program designed to teach fire, EMS, and law-enforcement personnel how to respond to WMD incidents. In the 16 months since its release, the program has been adopted and implemented across the United States.

The program is called "Ops-Plus for WMD Hazmat," and it is the first course in the Virtual Terrorism Response Academy (VTRA). "Ops-Plus" uses video-game-style tactical simulations to reinforce lessons from top EMS, fire, police, and FBI instructors.

"We blend video of real humans who are expert hazmat trainers into the gaming environment," said IML Director Joseph V. Henderson, MD. He brings to the project more than 23 years of experience creating interactive training for medical and military audiences. "It's not just glorified PowerPoint. It's accessible and effective. Even if you've never played a video game, you can learn from 'Ops-Plus,' and you can easily use this over and over again to keep your skills sharp."

The course begins in the simulated Hazmat Learning Lab, then proceeds to fully-interactive, simulated emergency situations. During the program, the trainee uses accurately-modeled instruments, answers various WMD-related questions, and makes tactical decisions. In the debriefing section, an expert trainer explains the impact of the trainee's decisions during the simulations.

"The trainee faces a series of increasingly-challenging tactical situations," said Henderson. "The choices the trainee makes drive realistic scenarios that would involve life-and-death consequences during real incidents."

For example, the trainee must determine what personal protective gear and special instruments to use for scenarios involving a suspected "dirty bomb" lab, including equipment that detects and measures radiation. The scenarios encourage trainees to consider the time of day, the temperature, and weather conditions, all of which can influence real hazmat operations.

The VTRA program helps address what Henderson said is a national problem of public-safety personnel being issued equipment and instruments they aren't fully trained to use. The program may be used individually or by instructor-led groups, either as preparatory/refreshers instruction or as a complement to live training.



"We had dozens of local, state, and federal responders help us develop and test VTRA, and it has been really well received," Henderson said. "Fire, police and EMS agencies and academies nationwide have adopted 'Ops-Plus' for preparatory and refresher training. It's already being used statewide in New York, Connecticut and Pennsylvania, and it has been approved for statewide use in California."

IML, which is part of the Dartmouth Medical School, specializes in combining technology with innovative instructional design. The lab also develops interactive simulations to train medical and military audiences. IML created VTRA with support from ISTS.

"IML has done a wonderful job using emerging technology to address the issue of emergency preparedness," said David Kotz, former director of ISTS and a professor of computer science. "By developing software that's effective and easy to use, Joe Henderson's group has created a resource that will be beneficial for many, many first responders and their communities."

Individual copies of "Ops-Plus" are \$35 and can be purchased through the non-profit National Fire Protection Association. For more information about IML and VTRA see <http://iml.dartmouth.edu/vtra/>

Faculty Profile



Recently, Professor Stephen Taylor of the Thayer School of Engineering returned to Dartmouth and ISTS after a four-year assignment with the Defense Advanced Research Projects Agency (DARPA). While with DARPA, he served as a Program Manager in the Strategic Technology Office. In this profile, Professor Taylor discusses his time at DARPA, the differences

between government and academia, and his future research interests, among other things.

What did you find most rewarding about your work at DARPA?
I have been supported by DARPA, in one way or another, for over 25 years – so being able to give back to my country, at a time of national crisis, was a real honor and a privilege for me.

What did you find most challenging?
I had to think about technical problems on a national scale, communicate my ideas crisply, develop an entire technology base, and then build relationships that get new capabilities transitioned into the military – it's a completely different view of science at that level and scale.

What are the main differences you found between working in the government and working in academic communities?
Scale is the main one – I worked on problems that a single research group could not hope to solve. Secondly, the notion of

going up the learning curve just isn't there – everyone is already up the learning curve and running full speed ahead. Finally stability, students have to be supported for 3 to 5 years in order to complete a Ph.D. – a typical DARPA program lives and dies by the progress it makes every quarter.

What are your teaching and research plans now that you are back at Dartmouth?

On the teaching side, I think we should build a kit-plane – like the Lancair Legacy – let students populate it with all sorts of novel and outrageous sensors – then hook it up through satellite communications and perform real-time sensing. There are all sorts of things that students can learn from this kind of real-world teaching project that you just don't get from a book and a classroom. On the research side, I'm excited about distributed sensing for biomedical and military applications — I think there are new opportunities afforded by multi-core blades in these areas.

How did you decide to become an engineer?

I built model aircraft as a kid – there wasn't much else I could do – I had asthma and, before fast acting inhalers, asthmatics were stuck in bed gasping for air most of the time. I left school as soon as I could and moved away from home so that I could get into an aeronautical apprenticeship – I just wanted to be near planes – it has been a lifelong passion.

What advice would you offer to someone contemplating going into your field?

Learn math and build stuff. You need to know both discrete and continuous math so that you can communicate with people in other disciplines – even if you don't understand everything they say all the time. Build stuff because it's fun and fun is what carries you through the hard times in a career – it's not a job, it's a way of life.

Of what professional accomplishment are you most proud?

The DARPA Directors Award, that I won last year, stands out for me on a very personal level — primarily because of the high regard I have for the my peer group on the national stage and the hard work that it took to earn. To be accorded this signal honor, before the top technical leaders of our country, was a very humbling and emotional experience.

Recent and Upcoming Speakers

April 21, 2008

Donna Dodson
National Institute of Standards and Technology
(NIST)

May 12, 2008

Landon Cox
Assistant Professor, Duke University

May 27, 2008

Jeffrey Stanton
Associate Dean for Research & Doctoral Programs;
Associate Professor, Syracuse University

6211 Sudikoff Laboratory
Hanover, NH 03755

Phone: (603) 646-0700

Fax: (603) 646-1672

Email: info@ists.dartmouth.edu

www.ists.dartmouth.edu

Welcome



Ajit Appari, Ph.D.
Research Fellow, Glassmeyer/ McNamee Center for Digital Strategies, Tuck School of Business, Dartmouth College

Ajit is a Postdoctoral Research Fellow at the Center for Digital Strategies at Tuck. His research, broadly speaking, focuses on risk measurement and risk management of information technology investments. Currently, he is working on the Center's research projects entitled "Information Risk in Data-Oriented Enterprises" and "Business Rationale for Cyber Security."



Michael Locasto, Ph.D.
ISTS Fellow
Department of Computer Science, Dartmouth College

Michael joins ISTS as a postdoctoral Research Fellow working with Professors Sean Smith on the SISMAT project and David Kotz on the MAP project.

Michael is interested in exploring methods for applying machine intelligence to a variety of

security mechanisms. In particular, he has researched ways to make intrusion defense systems automatic, correct, and adaptive.



Tanzeem Choudhury, Ph.D.
Department of Computer Science, Dartmouth College

Tanzeem Choudhury is an Assistant Professor in the Computer Science Department at Dartmouth and an affiliate faculty member at the University of Washington. She comes to Dartmouth from Intel Research Seattle.

Tanzeem develops machine learning techniques for systems that can reason about human activities, interactions, and social networks in everyday environments. She co-organized a multidisciplinary workshop on Modeling Social Dynamics, sponsored by the National Science Foundation (NSF), and is leading an NSF-funded research effort that unites sensing and communications tools employed by ubiquitous computing with machine learning techniques, in order to study unobtrusively large populations of interacting humans over extended periods of time. An affiliated faculty member of ISTS, Tanzeem is leading the Discovery of Trends in Activity-Aware Computing Environments project.