University of California, San Diego

Technologies and Foundations for Robust and Secure Networked Systems

Spring 2011 Newsletter

cns
Center for Networked Systems

Finding Weak Points in the Spam Economy

Despite the near-universal disdain for spam, consumer demand for a variety of goods and services allows spammers to run profitable businesses. While most people are only aware of spam as the perennially annoying clutter in their email inboxes, these messages and their dubious click-through destinations are only the exposed facets of an economic infrastructure of which few are aware and fewer still are fully knowledgeable. In order to monetize their advertisements, spam-based businesses must construct or interact with a complex system that can involve managing botnets, domain registrations, payment processing, bank accounts, fulfillment, customer service, Internet hosting, and proxy services.

Existing anti-spam initiatives have focused on addressing the most visible portions of this value chain via techniques such as e-mail filtering, URL blacklisting and Web site takedowns. However, these interventions are focused on reducing the pain for customers and not specifically on undermining the spam business model. In fact, the tens of billions of spam e-mails sent each day reflect the reality that spam remains a profitable endeavor in spite of these efforts. An alternative approach to the spam problem is to focus on the economic importance of each stage in the value chain and use this insight to drive interventions.

To this end, a team led by Center for Networked Systems researchers recently authored a paper in which they devised a methodology for the empirical study and analysis of the end-to-end resource dependencies that support the spam economy, from advertising to click-through to payment and fulfillment. As Assistant Research Scientist and lead author on the study, Kirill Levchenko (pictured above), writes in this paper, “anti-spam interventions need to be evaluated in terms of two factors: their overhead to implement and their business impact on the spam value chain.”

In their paper, jointly published by colleagues at UC San Diego, UC Berkeley and the International Computer Science Institute, the researchers first outline the spam economy pipeline, breaking down the process into three phases: advertising, click support, and realization.

Continues on page 4

LogEnhancer: Improving Software Diagnosibility

Any piece of complex software can be expected to fail given the perfect combination of programming bugs, administrative errors, and unusual system demands. Though built to be robust and tested under a number of scenarios, not every parameter of input or use can be foreseen by programmers. However, the cost of software failures in the production mode can be ruinously high in terms of lost revenue and productivity, making the minimization of failures a high priority. So, asks Computer Science and Engineering Professor Yuanyuan (YY) Zhou (pictured at left), if production failures cannot be completely eliminated through programming design, is there another way to lower the cost of recovery from the failure?

Zhou recently led a research team that tried to address this question in a paper presented at the 2011 Architectural Support for Programming Languages and Operating Systems conference. The study authors’ analysis shows that one of the greatest impediments to speedy recovery from production failures has been diagnosibility. When failures occur, programmers are often given very little information about the nature and context of the error, and so the programmers frequently spend more time trying to discover the source of a bug than they do in actually solving how to fix it.

Continues on page 3

CNS Members

CISCO Google hp invent ERICSSON NetApp ORACLE QUALCOMM

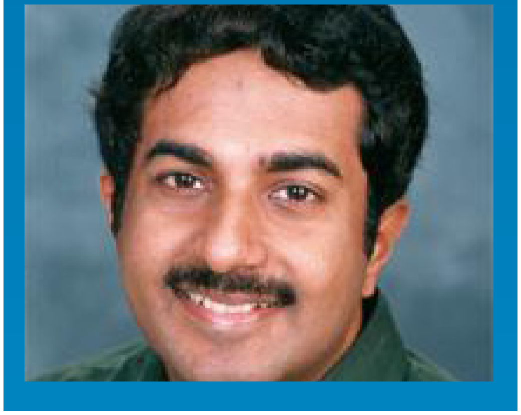
In This Issue

Google Supports Two Projects in CNS

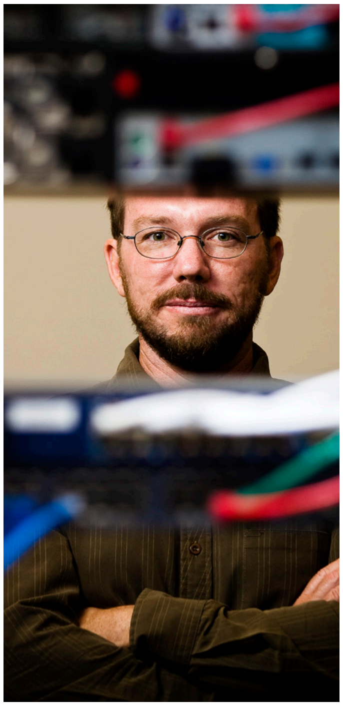
This winter Google elected to support two large projects led by CNS researchers. The first, involving Assistant Research Scientist Kirill Levchenko and CSE Professors Geoffrey M. Voelker and Stefan Savage, will support their work on "Data-driven Internet Security." The second gift supports a team comprised of Assistant Research Scientist George Porter, and ECE Professors Shaya Fainman, Joseph Ford and George Papen for their project, "Microsecond Optical Research Datacenter Interconnect Architecture."

Cisco Awards Gift to George Varghese

The Cisco University Research Program Fund recently awarded a gift in support of a project jointly headed by CSE Professor George Varghese (below) and UC Santa Barbara Professor Subhash Suri. Their project, "Fast Traffic Measurement at All Time Scales," will develop a tool to measure end-host bandwidth for data centers. It is a continuation of a prior collaboration between Varghese, Suri, and Cisco Fellow Fred Baker.



Geoffrey M. Voelker Wins Distinguished Teaching Award

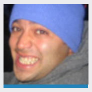


The UC San Diego Faculty Senate voted in April to give Professor Geoffrey M. Voelker a Distinguished Teaching Award, only one of five awarded across campus for the 2010-2011 academic year. Voelker, a noted systems and networking researcher in the Computer Science and Engineering department, has also long been equally respected for his innovative and energizing work as a teacher and mentor at both the undergraduate and graduate levels.

Of special note has been Voelker's senior-level software system design and implementation class, more commonly known as the "Video Game" class. For a full decade, this innovative class has been viewed by many CSE students to be the capstone experience of their undergraduate degree — and for some, as a springboard into careers in the game industry. Over the ten-week course, students break into large groups to collaborate on the design and implementation of a distributed, real-time, 3D, multiplayer computer game. The final exam, which draws a large crowd, is a public demonstration of each team's game, when volunteers from the audience face off against each other.

Graduating Students

James Anderson, advised by CSE professor Amin Vahdat, graduates in June 2011 with a Ph.D., subsequently joining Thesys Technologies.

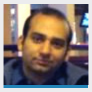


Ehsan Ardestanizadeh received his Ph.D. this past winter with a dissertation on "Feedback Communication Systems: Fundamental Limits and Control-Theoretic Approach." He joined startup ASIA. His advisor in ECE was professor Tara Javidi.

Gaurav Dhiman graduates this June in CSE, advised by Tara Javidi. His Ph.D. dissertation is on "Dynamic Workload Characterization for Energy Efficient Computing." Dhiman will join Google in Mountain View, Calif., as a software engineer.

Salih Ergut is R&D Manager of Industry Relations at Turk Telecom, after receiving his Ph.D. in winter 2011. His dissertation: "Context-Aware Computing for Wireless Networks." Ergut's advisor: Tara Javidi.

Frank Uyeda graduated in spring 2011 with a Ph.D., advised by CSE's George Varghese. His thesis: "Algorithms for Measuring and Enhancing Distribution Systems."



Hamid Bazzazz graduates this June with an M.S., advised by CSE professor Amin Vahdat. He joins Google as a software engineer.

Sambit Das has accepted a position at Cisco Systems in San Jose as a software engineer, after earning his M.S. in June 2011. His advisor was CNS director Vahdat.

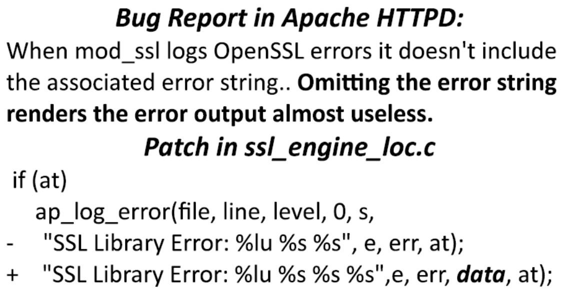
Michael Vrable, advised by CSE's Stefan Savage and Geoff Voelker, graduates in June 2011, with a dissertation on "Migrating Enterprise Storage Applications to the Cloud." Vrable joins Google's security research group as a software engineer.

LogEnhancer: Improving Software Diagnosibility

Continues from bottom page 1...

In order to cut the time and labor costs of manually inspecting the log files which are often the sole source of failure data, Zhou's research team developed a tool called LogEnhancer. LogEnhancer modifies every message in the log file so that it collects causally-related information. This information aids the programmers in their search for the code paths that are the most likely culprits for the failure. Zhou and her colleagues analyzed LogEnhancer on eight real-world applications, including Squid and Apache. They evaluated LogEnhancer by conducting experiments in a Linux environment that analyzed LogEnhancer's performance in three areas: value selection, diagnostic effectiveness, and logging overhead.

Value selection looked at how effective the LogEnhancer algorithm was in capturing variables useful for failure diagnosis. This was done by comparing the results against manual selection. Then the researchers looked at the program's diagnostic effectiveness, as measured by the usefulness of the information collected in failure diagnosis. Lastly, the team evaluated the costliness of LogEnhancer's run-time overhead.



Bug Report in Apache HTTPD:

When mod_ssl logs OpenSSL errors it doesn't include the associated error string.. **Omitting the error string renders the error output almost useless.**

Patch in ssl_engine_loc.c

```
 if (at)
    ap_log_error(file, line, level, 0, s,
-     "SSL Library Error: %lu %s %s", e, err, at);
+     "SSL Library Error: %lu %s %s %s",e, err, data, at);
```

Example of real-world patch for the purpose of enhancing log messages

Compared with historical data for real-world failures for which programmers manually inspected the log files, LogEnhancer automatically selected an average 95.1 percent of log variables responsible for application failures. As Zhou explains, "This high coverage is evidence that our design matches with the intuition of programmers in recording key values to help diagnosis… and can do at least as well as manual effort" — with little cost to run-time or increase in log size. Zhou admits that some challenges to a robust and scalable implementation of LogEnhancer remain, but believes that future developments in the tool will make this possible.

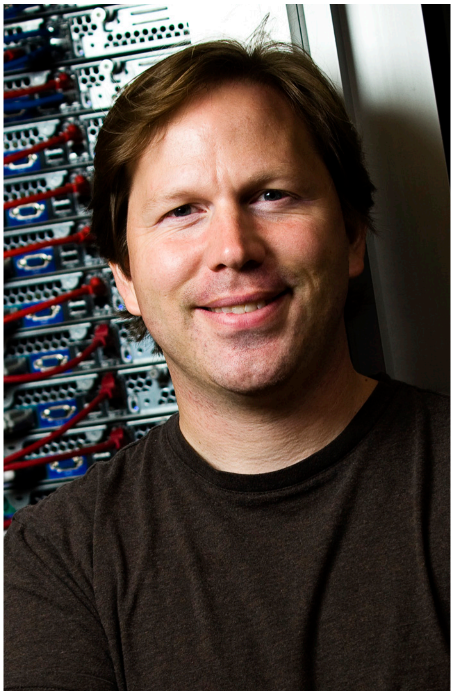
Read more at: http://opera.ucsd.edu/paper/asplos11-logenhancer.pdf

Car Security Concerns Grab National Spotlight

Having a malicious hacker remotely wrest control of your automobile even while you're driving sounds like a paranoid scenario from the latest Hollywood techno-thriller. Yet a team of researchers at CNS (led by Interim Director Stefan Savage) and the University of Washington has shown how today's highly networked vehicle systems could be compromised by third parties to make this nightmare scenario a reality. The researchers presented a report on the subject before the National Academy of Sciences' Transportation Research Board in early March. The report outlined a number of security vulnerabilities in current automotive systems. The *New York Times* quoted Savage (pictured below) as saying, "Everyone has taken this extremely seriously."

Many contemporary automobiles are manufactured with onboard cellular systems that allow them to interface with wireless networks and the Internet. Therefore, if hackers remotely access the vehicle's electronic control unit, they can gain control of the engine, locks, or braking systems.

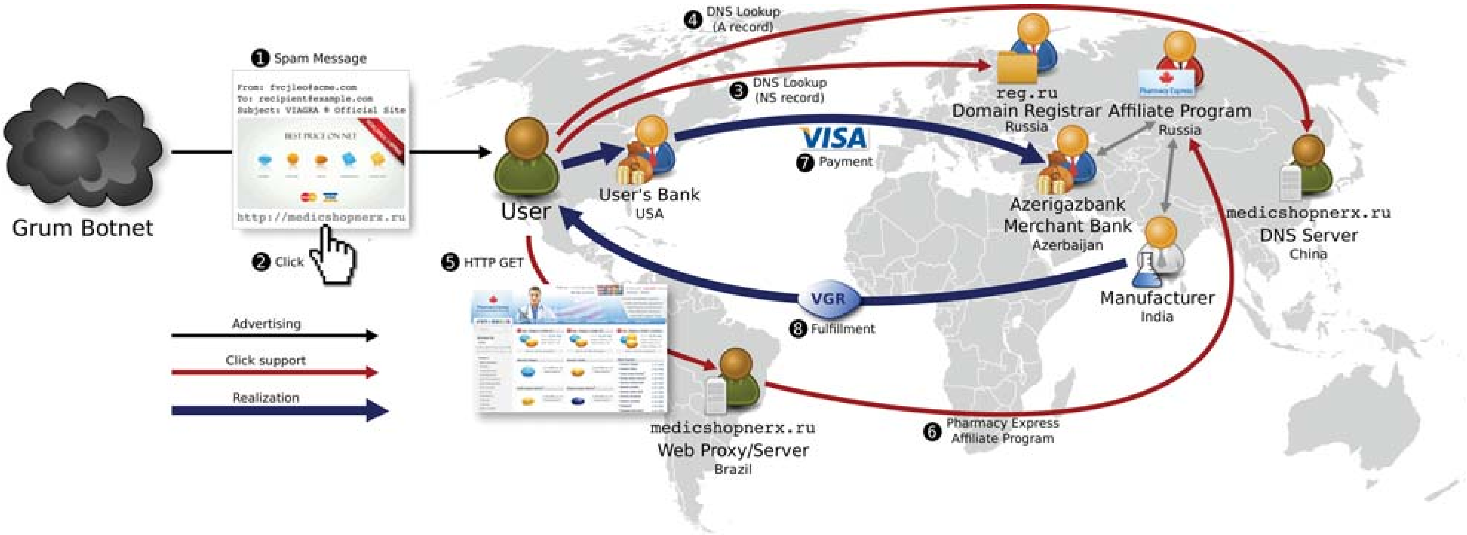
To conduct their experiments, the researchers purchased a moderately priced sedan equipped with connectivity features that are typical of what is available in the contemporary automotive market, including a Bluetooth unit. Then they infiltrated the cellular unit's authentication system and inserted malicious software into its operating system. From there, the researchers sent signals that allowed them to operate the various systems in the vehicle subject to the electronic control unit — everything from the locks to the brakes to the dashboard display. A malicious agent with access to the car's cellular unit could track the vehicle's location, unlock the door and start the vehicle, or cause the braking system not to respond to driver input.



While the study's authors cautioned that there are no known cases of hackers actually exploiting these vulnerabilities for malicious purposes, they did warn that any vulnerabilities that exist will eventually be exploited. Fortunately, the researchers report that the automotive industry has been reacting constructively to their findings and has moved to incorporate their concerns into the security design of the next generation of onboard networked systems.

To read more, visit: http://automotivemagazine.us/2011/03/10/researchers-show-how-a-cars-electronics-can-be-taken-over-remotely/ and http://www.nytimes.com/2011/03/10/business/10hack.html

Finding Weak Points in the Spam Economy



(Above) Infrastructure involved in a single URL's value chain, including advertisement, click support and realization steps

continues from page 1...

The advertising phase is the one most familiar to the public at large, and generally focuses upon using various gambits to reach the attention of potential customers and convincing them to click through to a given URL, where the advertised product may be viewed and purchased. In the contemporary online landscape, most spammers only operate as advertisers, working with affiliate programs that pay them on a commission basis for purchases. Because spam-affiliated URLs are the target of legal action, spammers usually redirect spam-enticed customers to alternate URLs and domains so that they may obfuscate the ultimate destination of the user. Additionally, the Web sites and domain resources are usually not registered by the spammer him or herself, but are purchased on the black market from an original registrar. These registered domains are supported by name and Web servers that are also often controlled by a contracted third party. Finally, the affiliate program handles the realization phase, in which the activity is monetized as the user selects an item to purchase and makes an online payment, typically via Visa or MasterCard. The goods are then shipped to the user (or provided online for virtual goods such as counterfeit software or movies).

Having profiled the infrastructure, the researchers then analyzed it for potential weaknesses and evaluated possible interventions for their effectiveness and breadth of impact. As mentioned previously, the most common forms of intervention in the past have focused on the advertising phase, where such methods as spam filters and URL blacklisting were developed. However, the continued proliferation of spam shows that these methods have only a limited efficacy. Former efforts to takedown name and Web servers have given rise to a thriving market in 'bulletproof' hosting services that resist pressure to remove sites. Affiliate programs that pay the spammers on commission can be shut down if the store owner happens to reside in an applicable legal jurisdiction, but targeting product providers has a troubled track record for success.

It is the least studied and understood portion — the financial segment — which appears to be the most vulnerable to defense against the entire system. "Without an effective mechanism to transfer consumer payments, it would be difficult to finance the rest of the spam ecosystem," explains Levchenko. This potentially simplifies the implementation of an intervention strategy, because of the high replacement cost to locate another bank to process the payment transactions.

In the course of the study, the researchers discovered many reasons to draw this final conclusion. First of all, the similarity between payment processing templates utilized by a wide number of spammers and the use of the same merchant banks suggests that there are relatively few affiliate programs available to process payments. Secondly, purchasers want to use trusted and protected methods to pay vendors, which means, as Levchenko explains, that "to extract value from the broadest possible customer base, stores try to support payments via the large card association networks: Visa and MasterCard." However, the use of trusted, legitimate payment methods exposes spammers and their affiliates to scrutiny of a kind that few legitimate financial institutions are willing to risk. Thus, unsurprisingly, Levchenko continues, "the sharing of payment infrastructure is substantial... [so that] of the 76 purchases for which we received transaction information, there were only 13 distinct banks acting as Visa acquirers." The data show that the number of banks willing to engage in high-risk payment transactions is quite small: over 95 percent of the transactions studied in the survey were serviced *by only three banks*.

Looking closely at the payment transactions underlines the importance of maintaining legitimacy in the eyes of credit- card companies. Visa transactions include a standardized "Merchant Category Code" that details the type of goods or services purchased by the card transaction. Though there were a couple of cases in which Visa transactions were miscoded in such a way as to suggest that the financial institution was attempting to hide the nature of the goods being purchased, the vast majority of purchases were correctly coded. Opined Levchenko: "A key reason for this may be the substantial fines imposed by Visa on acquirers when miscoded merchant accounts are discovered 'laundering' high-risk goods." This suggests strongly that even banks that are willing to deal in grey-market transactions are not willing to lie outright and so endanger their ability to process future credit-card transactions. "While there are thousands of banks, the number that are willing to knowingly process what the industry calls 'high-risk' transactions is far smaller," concluded Levchenko. Since the supply of merchant banks for spammers is low, the cost of losing a banking resource is quite high and presents few alternative resources.

Having identified the most efficient point of intervention in the spam supply chain, the research team makes two policy proposals. The first is to pressure the merchant banks to cease support and services for spammers and spam-affiliated programs. However, this approach is slow and, due to numerous legal issues, likely not to be fruitful. As a more successful alternative approach, the researchers suggest that U.S. issuing banks refuse to settle certain transactions with banks known to support spam-advertised goods and services. Though the authors foresee numerous hurdles to crafting a policy and prevention program using this latter method, they consider it to be not only feasible, but the most efficient method for interfering in the underground spam economy.

Read more:
"Study Sees Credit Cards as 'Choke Point' for Spam" in the *New York Times* at http://www.nytimes.com/2011/05/20/technology/20spam.html?hpw

California Fault Lines: Studying Failure to Prevent Failure

One of the more challenging aspects of studying emerging enterprise-level networks is developing techniques to quantify and characterize the scope of problems that are inherent to network designs and implementations. For example, uninterrupted availability is a requirement for the users of today's network-centered enterprises. However, since availability is not an intrinsic design property of a system, it is accepted that parts of networks will, at times, fail. According to Daniel Turner (pictured below), a Ph.D. student in the CSE department who led a team to address the so-called availability conundrum, the solution is that "a system must accommodate the underlying failure properties of its components." Therefore, to prevent failure, the characteristics of failure in networks (e.g., how long they last, what causes them, and how well they are masked) need to be studied.

Given the technical, social and cost barriers to capturing and analyzing data, problems that threaten even the most basic design parameters for a given system can escape close scrutiny. For example, though several measurement mechanisms have been developed to study network failures, they have proven problematic to use. Some methods are not universally available to research-motivated groups, while others can incur significant capital and operational expenses. In the absence of empirical data, researchers in this area have been using purely theoretical models, while network designers have been flying blind with regard to building to preserve availability. This motivated Turner and his group to find a way to capture availability data. "Networks," he noted, "have increasingly been identified as the leading cause of end-to-end service disruption, as they exhibit complex failure modes."

CSE Ph.D. student Daniel Turner

The result of their effort was a 'cheap and dirty' methodology for extracting data about network failures and analyzing it. In their work, the research team determined that the key was to find a network where some historical data about network failures was available and then to find a way to reconstruct failure patterns from those sources.

The researchers found an excellent study subject: five years' worth of archival data from the Corporation for Education Network Initiatives in California (CENIC), a production IP network consisting of over 200 routers serving public education and research institutions in California. By looking at router configuration files, syslog archives, and operational mailing-list announcements, the researchers derived a comprehensive failure history of the network.

For the purposes of the study, failure was defined by the research team as any event that causes a routing-state change syslog message to be recorded, and a link is considered to have failed whenever a router refuses to send traffic over it. The study confirmed and expanded upon the findings of previous studies. It showed that measures seeking to improve network stability measures can be targeted toward a small number of bad actors. The study proved that surveys of fine granularity and high utility can be conducted in a wide variety of IP networks without the implementation of expensive monitoring systems, by using existing data sources such as syslogs and operational mailing lists that are already gathered in production networks. Regarding the availability issue, the researchers discovered that the majority of failure events are due to software and hardware upgrades, while relatively few links are responsible for the majority of network failures. Turner concludes that, "This is good news because it suggests that there are a small number of 'hot spots' in the network that require attention." Additionally, since the study's findings are in line with previous investigations of other networks, it can be argued that the results of analysis are characteristic of systems in general, not merely representative of CENIC's network. There is good reason to believe, therefore, that principles about the nature of system failure derived from this study have broad applicability for future design approaches.

Read more at: http://ccr.sigcomm.org/online/files/p315_0.pdf

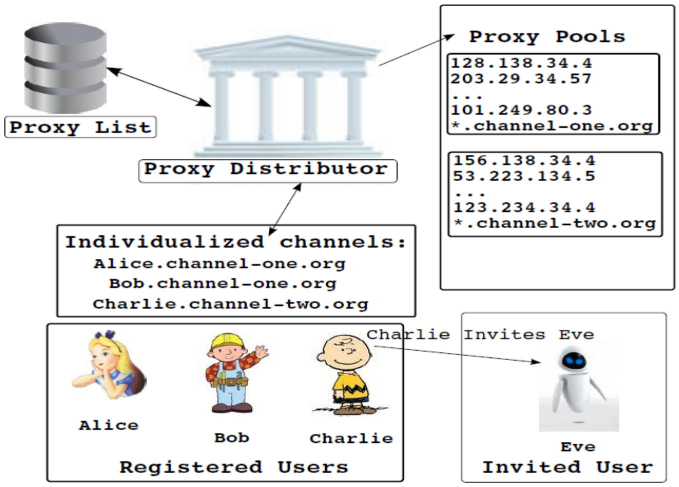
Proximax: A Revolutionary System

Ever since the Internet was first used for political expression, oppressive regimes have played an evolving cat-and-mouse game with their dissident citizens. Examples of the newest iterations of this game have been in evidence since the beginning of 2011, when the world's attention was riveted by the popular uprisings occurring throughout the Middle East. The mass movements have been revolutionary in the streets and in the ways that the protesters used the Internet and such social networking sites as Twitter and Facebook to organize themselves. Social networking tools proved so successful in mobilizing activists that the government of Egypt, in a widely decried move, cut access to those resources for several days. During the same period, the government of the People's Republic of China, fearing that the waves of unrest in the Arab world might foment trouble at home, further tightened its already strict censorship of political commentary available to Chinese users of the Internet.

To circumvent government censorship of content and social networking resources, Internet users employ external Internet proxies that support encrypted connections whose content confidentiality in turn allowed users to bypass content filtering. Because of the effectiveness of these proxies, oppressive governments have moved to monitor their use and then to block the proxies at the network level. In order to protect the identity and location of proxy servers for as long as possible from detection by the government, proxy addresses were distributed through *ad hoc* "trust networks." This gave rise to a paradox: if the protesters wanted to attract new users, they would have to advertise the proxy servers more broadly, which inevitably led to the trust networks being infiltrated — and the proxy servers were discovered and shut down. The problem for citizens seeking to express or mobilize political opposition online in authoritarian states became a network issue: how to shepherd their proxy resources in such a way as to maximize the length of time they can use a given proxy, without losing the breadth of its distribution.

This challenge, with its technical and social elements, was addressed in a recent paper by CNS Postdoctoral Researcher Damon McCoy and Research Scientist Kirill Levchenko. The problem is a difficult one, said Levchenko, "because of two conflicting goals: widely disseminating the location of the proxies to fully utilize their capacity and preventing (or at least delaying) their discovery by censors… advertising to more people means greater effectiveness, but also greater risk being blocked."

Since all proxies can be expected to be compromised eventually, focusing solely on a perfect security design for the proxy servers is an impractical goal. Therefore, the study's authors proposed framing the solution as one of finding a way to maximize a given proxy's 'yield,' where yield is defined as the number of user-hours of service provided by a set of proxies. This would require a system by which registered users and disseminators of the proxy services were evaluated so that their privileges could be revoked should they prove to be compromised. To this end, McCoy and Levchenko proposed Proximax, a proxy distribution system that creates a special set of registered users who are responsible themselves for disseminating proxy addresses throughout their private trust networks. Proximax thereby generates an effectiveness rating for each registered user by tracking how many end-users each registered user attracts to a given proxy, and by measuring how long the proxy lasts before being blocked. This effectiveness rating is used to execute more efficiently the three main tasks of the system: the distribution of proxies via the trusted networks of registered users; the management of distribution channels; and the creation of a system for the invitation of new registered users.



Proximax system components

For an example of how the effectiveness rating can be used to implement these tasks, Proximax determines whether a given user's request to invite others to join a network channel should be sent. Each time new invitations are suggested to the system, a reputation-based analysis is performed on the registered user and on all of the current users previously invited by that user. The relationship of each user to his or her current registered invitees forms a tree system that is evaluated both for its rate of utilization and for the longevity of its proxies. Once a user in a subtree acquires a low reputation, the entire tree loses its privileges, thus helping to maintain the overall well-being of the trusted network. "To our knowledge," says McCoy, "this is the first system to build a proxy distribution system that automatically adjusts the resources allocated to each channel and groups registered users together in shared pools of proxies based on similar blocking risk rates."

Despite the practicality and high usability of its design, Proximax can be further optimized, according to the study's authors. Of particular concern is how to deal with specific countermeasures on the part of governments seeking to infiltrate protected proxy systems. For example, a malicious actor could infiltrate a network and inflate his or her performance rating so that a greater number of system resources would be allocated to that actor, effectively rendering these resources as useless as they might be if they were shut down, but without alerting Proximax that the system was compromised. Another problem is that the design of Proximax assumes the integrity of the root administrative group: if an agent infiltrates the core user group and gains full access to all the proxies, then Proximax's measurement techniques will not be able to measure and detect this accurately. McCoy and Levchenko plan a future implementation of Proximax as a feature of a Tor anonymous proxy system that might include technical solutions to the above challenges in addition to several other possible optimizations.

More: http://cseweb.ucsd.edu/~dlmccoy/papers/mccoy2011fc.pc

(History) Sniffing Out Rotten Practices on the Web

Most Internet users take it for granted that their web browsing history is untraceable by third parties who lack access to their physical machines. However, the reality is that vulnerabilities in widely employed JavaScript web applications have created opportunities for third parties to track covertly information about an individual's online activities. While these vulnerabilities and the attacks that could be launched to exploit them have been proposed and discussed in the security research literature for some time, CSE Professor Hovav Shacham explains that "little is actually known about them in the wild." Shacham, along with a research team comprised of Ph.D. student Dongseok Jang and Professors Ranjit Jhala and Sorin Lerner, conducted an empirical study that proves that many popular Web sites can, and in fact do, use covert techniques to compromise users' privacy and to track their browsing behavior. Specifically, the researchers were interested in estimating how many and what kinds of Web sites might be extracting information from their visitors, and how careful these sites might be to obfuscate their behavior.

The investigators studied a general class of vulnerabilities they refer to as "privacy-violating information flows," which include: *stealing cookies* (using information stored on a page's cookie to transmit data about the Web user to a third party); *location hijacking* (when dynamically loaded code on a safe site navigates the viewer to a malicious site from which a phishing attack or full machine compromise can be launched); and *behavior tracking* (tracking how a user clicks on, scrolls over, highlights and keyboards while viewing a page). One example of these flows, history sniffing (where a malicious site can determine whether a user has visited a specific site in the past), can be conducted through the exploitation of a Web browser feature that lets users know when they have visited a link by changing its display color. Web site owners can insert history-sniffing code into their pages in order to check if their visitors have also gone to their competitors' Web sites or they can pass collected data to third-party advertisers who use the information to build profiles on Web users.

"A survey of 50,000 of the web's most visited websites by the team from UC San Diego found 485 sites using this method to get at browser histories, 63 were copying the data it reveals and 46 were found to be 'hijacking' a user's history."

-BBC News, 2/12/2010

CSE Professor Hovav Shacham

To undertake the survey, the research group designed an information flow policy language that allowed them to detect different kinds of privacy-violating flows in JavaScript code. This language permitted the group to identify sites within code where taints might be inserted or prohibited. "For example," said Jang, "to specify a cookie-stealing flow, we inject a 'secret' taint into the cookie, and block that taint from flowing into variables controlled by third parties." Then they implemented the information flow engine into the Google Chrome browser, so that it could monitor the four privacy-violating flows to be studied.

The study itself was conducted by applying the policy language in the modified Chrome browser to the front pages of the Alexa global top 50,000 websites. Whenever the browser reported the transference of some kind of information related to the privacy-violating information flows of interest, the investigators followed up to confirm. In the case of history sniffing, the researchers discovered 46 web sites where this occurred, including one site that is ranked in the Alexa top 100. And while 46 sites out of 50,000 may not seem like many, the investigators caution that these were only those sites where history-sniffing behavior could be confirmed. Seven times as many sites surveyed exhibited behavior the researchers considered suspicious, but that could have been checking visitors' web habits through means even more difficult to detect. One confounding factor might be measures taken to obfuscate their history-sniffing implementations. The team found that the JavaScript used to implement the history sniffing was often dynamically generated by the Web page, making it difficult to discern if history sniffing is occurring if one simply looks at the Web page's static code, and thus implying that the site's owners intended to hide their actions from outside observers.

Clearly, privacy vulnerabilities that were previously considered theoretical have now been proven to be a real feature of Web browsing. "Our study shows that popular Web 2.0 applications like mashups, aggregators, and sophisticated ad targeting are rife with different kinds of privacy-violating flows," concludes Shacham. "Hence there is a pressing need to devise flexible, precise, and efficient defenses against them."

Shacham's team intends to conduct further studies that are both larger in scale and that will address a broader variety of privacy-information flows. They also want to look at the occurrence of security attacks like phishing and request forgery. Once the scale and detail of the current state of privacy violation on the Web has been measured, the hope is to transform the framework of the modified browser that they developed to detect and to observe privacy violating information flows into a robust client-side protective mechanism that will restore surfing anonymity to web browsers.

Read more: "An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications" at
http://cseweb.ucsd.edu/~hovav/papers/jjls10.html

Developing Protocols for Congestion

Wireless networks are comprised of radio nodes organized in a mesh topology so that all devices within the wireless coverage area can communicate in the network and can continue to operate even if a specific node goes down. One subtype of wireless network first designed in the 1970s as a DARPA project, the wireless *ad hoc* network, has a number of specific uses. This kind of network is called "*ad hoc*" because it lacks a centralized, preexisting infrastructure such as the dedicated routers or access points of more standard wired and wireless networks. The lack of dedicated routers means that each node within the network participates in forwarding data for other nodes. The minimal need for configuration, potential for rapid deployment, and lack of reliance on central nodes make *ad hoc* networks preferable for use in emergency response, disaster management, military conflicts, and surveillance.

However, as the demand for wireless grows, the probability is that wireless networks will approach or exceed their carrying capacity, resulting in congestion and delays. The concern over congestion is particularly urgent in wireless *ad hoc* networks, where nodes must relay each other's packets. In an attempt to forestall the problem of network congestion, a research team led by Electrical Engineering PhD student Abhijeet Bhorkar, collaborating with ECE Professor Tara Javidi and CSE Professor Alex C. Snoeren, has proposed the use of a congestion-aware routing algorithm they have dubbed the Congestion Diversity Protocol (CDP). "CDP is a distance vector protocol that routes packets through neighbors with the least estimated remaining delivery time at each hop," explains Bhorkar.

In their project, the research team investigated two performance measurements: end-to-end delay and delivery ratio. End-to-end delay is the amount of total delay seen when traveling from one origination point to a final destination in a network. The delivery ratio is the ratio of packets delivered at the destination to the packets. The implementation was evaluated in an indoor wireless testbed and their results were significant, says Bhorkar. "For constant bitrate traffic loads that are less than the capacity of the network, congestion diversity routing reduces delay, decreases packet drop rate, and increases throughput in comparison" to other previously developed routing algorithms. In some special cases, the CDP performed 50 times better than other current or proposed congestion-reducing protocol candidates.

Read more at: *http://circuit.ucsd.edu/~tjavidi/Abhijeet/Infocom2011.pdf*

Get Connected

Stay up-to-date about upcoming CNS events, including lectures and Research Reviews, by signing up for the CNS Events RSS feed. To do so, visit the CNS website at

http://cns.ucsd.edu

and click on the link "CNS Events RSS Feed."

Upcoming Events

August 3 and 4, 2011
CNS Summer Research Review
Conference Rooms Jacobs Hall, UC San Diego Campus in La Jolla, Calif.

The CNS Summer Research Review will feature keynotes and talks by members of our industry affiliates; grant proposals for the 2011-2013 CNS Research Grant Program; progress reports about projects on current grants; a graduate student research poster session and reception; and numerous opportunities for informal interactions among member companies and CNS faculty, researchers and graduate students.

Attendance at the Summer 2011 Research Review is limited to industry sponsors and invited guests.
For more information, please contact Kathy Krane at *kkrane@ucsd.edu* or call 858-822-5964.

Mission and Objectives of CNS

Calit2 UCSD Jacobs School of Engineering

The mission of CNS is to develop key technologies and frameworks for networked systems. By combining our research talents and strengths in partnership with industrial leaders, CNS achieves critical mass and relevant focus, accelerating research progress and creating key technologies, frameworks and systems understanding for robust, secure networked systems and innovative new applications. CNS also works to educate the next generation of top students with a perspective on industry-relevant research and to train students on how to continue their leadership throughout their careers. This is accomplished by bringing together leading faculty, students, and companies to investigate the most challenging, interesting and important problems in computer networks.

If you are interested in joining the Center, please contact Director Amin Vahdat at vahdat@cs.ucsd.edu.