Computer Science Colloquium

Twenty-second Series - Spring 2005

CS DEPARTMENT School of Science & Technology Sonoma State University
Prospective Students People Current Classes Catalog & Schedule Advising Facilities **EVENTS**
Clubs Jobs Other
COLLOQUIUM

Thursdays, noon to 12:50 in Salazar 2016 on the SSU Campus
Open to the Public

February 17	THE MICROPROCESSOR TEN YEARS FROM NOW: HOW DO WE HARNESS THE RAW POWER TECHNOLOGY WILL PROVIDE? Yale Patt University of Texas, Austin Processor technology is alive and well: within a few years, more than one billion transistors on each silicon die, with geometries so small that we will run these chips at frequencies in excess of 10 GHz. However, it is already the case that this increase in raw power is not being effectively utilized. In fact, the naysayers suggest that the problems will get worse, and we may as well just give up trying. In this talk, I will attempt to identify the problems and suggest ways to keep us on track to take advantage of what device technology will provide.
February 24	THE FULL FUNCTION IMS HDAM, HIDAM AND HALDB DATABASES FROM IBM Brian J. Marshall Computer Associates International, Napa What is the physical layout of IBM Hierarchical (HDAM, HIDAM and HALDB) Databases? What are the underlying methods by which the IMS DBMS stores data in these databases? What is the meaning of Segment Codes and Relative Byte Addresses? How does the IMS go about locating space for segments in the database?
March 3	HONEYD - A VIRTUAL HONEYPOT FRAMEWORK Niels Provos Google, Mountain View A honeypot is a closely monitored network decoy serving several purposes: it can distract adversaries from more valuable machines on a network, can

	provide early warning about new attack and exploitation trends, or allow in-depth examination of adversaries during and after exploitation of a honeypot. Deploying a physical honeypot is often time intensive and expensive as different operating systems require specialized hardware and every honeypot requires its own physical system. This talk presents Honeyd, a framework for virtual honeypots that simulates virtual computer systems at the network level. The simulated computer systems appear to run on unallocated network addresses. To deceive network fingerprinting tools, Honeyd simulates the networking stack of different operating systems and can provide arbitrary routing topologies and services for an arbitrary number of virtual systems. This talk discusses Honeyd's design and shows how the Honeyd framework helps in many areas of system security, e.g. detecting and disabling worms, distracting adversaries, or preventing the spread of spam email.
March 10	ANATOMY OF AN ALGORITHM Bryan Higgins Motet, Berkeley Bryan Higgins was one of the principal developers of OmniPage, the top-selling optical character recognition (OCR) program. The talk focuses on one algorithm from that program, examining how the hardware constraints of the day influenced the algorithm's design, and how changing technology and market forces influenced its evolution.
March 17	INTERACTIVE RENDERING OF PLANETARY-SCALE GEOMETRY AND TEXTURE Kenneth I. Joy University of California, Davis The real-time display of huge geometry and imagery databases involves view-dependent approximations, typically through the use of precomputed hierarchies that are selectively refined at runtime. This talk focuses on the problem of terrain visualization, in which planetary databases involving billions of elevation and color values are displayed in PC graphics hardware at high frame rates. We show how innovative data structures, new out-of-core storage organization based on space-filling curves, and optimization using graphics processors can be used to solve this problem.
April 7	BACK TO THE FUTURE: A FRAMEWORK FOR EXECUTING MALWARE SAFELY Hao Chen University of California, Davis

Malware is software with malicious intent. Besides viruses and worms, newer forms of malware have recently emerged as widespread threats to system security. These newer varieties, such as spyware and adware, are difficult to remove. Often they are bundled with more legitimate applications people want to use, which makes preventing infection difficult. State of the art defenses against malware rely predominately on signature-based detection and recovery. A major weakness of this approach is the inability to reliably detect new malware or variants of known malware. We (Hao Chen, Francis Hsu, Thomas Ristenpart, Zhendong Su) propose a novel framework for allowing users to run untrusted programs safely. We formally define what is meant by safety. Based on our formalizations, we develop a general framework for untrusted program execution that utilizes monitoring and logging to ensure safety. We will discuss our experience in implementing a prototype of the framework on Windows, the usual target of malware activity.

April 14

OUR LAST BEST CHANCE TO DEFEAT SPAMMERS, SCAMMERS, AND HACKERS

Danny Goodman
Author, Half Moon Bay

The problems associated with unwanted email, computer viruses, and outright cyber-attacks are having a substantial negative impact on productivity and personal privacy. The viability of electronic email as a reliable and desirable medium is at risk. In this talk, the author of the book "Spam Wars" will explain what is right and wrong with current legal and technological approaches to the problems, and then demonstrate how frustratingly close we are to ridding the Internet of those who take unfair advantage of everyday email users.

April 21

DYNAMICS AND ANIMATION FOR FILM, WHERE WE ARE - WHERE WE ARE GOING

John Anderson
Pixar Animation Studios, Emeryville

In the last five years physically motivated procedural animation has become an increasingly important tool for character and effects animation. The influence of these techniques has progressed from an era where dynamics based approaches were painstakingly applied to a few special shots to the point where the majority of CG character animation includes some procedural elements. We are now at a particularly exciting point in the development and application of these techniques. New technologies and faster hardware have opened the door to real-time procedural characters. These characters combine methods from dynamic simulation and multivariate statistics to provide new tools that allow animators to achieve artistic goals without losing control of the performance.

April 28

PHISHING COUNTERMEASURES

	Aaron Emigh Radix Partners "Phishing" is a form of identity theft in which deception is used to trick a user into revealing confidential information with economic value. Phishing was responsible for at least $1.2 billion in direct losses last year. Starting with a threat model based on the information flow of a phishing attack, this presentation evaluates technical countermeasures applicable at each chokepoint to detect phishing, reduce the deceptiveness of fraudulent content, provide a trusted path over the public internet and render illicitly obtained information valueless. A combination of applied cryptographic techniques has the potential to dramatically reduce the losses due to phishing and other forms of identity theft.
May 5	PROTOTYPES AND GAME DEVELOPMENT Jason Shankel Maxis/Electronic Arts, Walnut Creek Gathering requirements for game development projects is challenging. Prototypes help designers address key questions and minimize production risk. In this talk, I will present several prototyping methods and discuss their applicability to game and general software design.
May 12	SPAM AND THE LAW Ian Sweedler Deputy Attorney General, CA Dept. of Justice For almost as long as there has been unsolicited commercial email (i.e., spam), there have been attempts to combat it through legal action. Spam has been the subject of litigation based on laws of advertising, trespass, fraud and other general theories. Several states led the way with legislation specifically addressing spam, and the U.S. Congress passed a national law in 2003. To figure out where we are and where we are likely headed, it's important to understand the evolution of these laws, and the issues inherent in efforts to enforce them.