Please pick your top 5 projects by putting numbers 1-5 in the following table

SANDMAN: Sandia Attack Modeling and Analysis framework	
Malicious activity discovery and analytics	
MiniMega	
Hosted Hardened Android	
And-lantis	
Cloud security assessment	
Mobile security assessment	
IPv6 integration into Captive Portal software	
DNSSEC test suite	
DHS S&T Competition: Voting Machine Security	
Formal Methods	
Certified Software	
H.323 Red Team	

SANDMAN: Sandia Attack Modeling and Analysis framework

Attack modeling and vulnerability analysis are crucial components of risk management in any security setting. This project is focused on developing a framework for threat modeling and analysis that automates attack graph generation and the generation and evaluation of alternative attack scenarios and mitigations. This framework will be implemented as a web interface using the Grails development platform, with attack scenario generation powered by state-of-the-art automated AI planning tools, and the cost-benefit analysis of alternative mitigations driven by a game theoretic reasoning engine. The intern's responsibilities may range from devising a graphical user interface, to developing the attack plan generation or mitigation analysis back-ends, depending on the intern's interests and background.

Desired Skills:
Java programming, ideally with experience with Grails/Ruby on rails. Previous experience in developing web applications a plus.

Looking for:
2UG at 75% time or 1UG/1HS at 100% time

Malicious activity discovery and analytics

This project involves discovery of malicious activity within large data sets of network traffic. The work will include designing and implementing schemas for distributed highly scalable databases and the use and development of MapReduce analytics. Many of these analytics involve graph algorithms developed by mathematicians, graph modeling experts, and cybersecurity subject matter experts.

Desired Skills:
Java, Hadoop MapReduce, and Accumulo

Looking for:
1UG at 50% (specifically requested)
Project not available for pick

MiniMega

Minimega is a testbed framework for emulating large scale networks of devices. It uses KVM, Qemu, and openvswitch to create arbitrary networks of devices and can scale to millions of nodes. We use minimega on our local clusters as well as DOE owned supercomputing resources.
A good public release description of the use of minimega for Android devices can be found here: http://arstechnica.com/information-technology/2012/10/megadroid-300000-androids-clustered-together-to-study-network-havoc/
Continued work this summer includes adding a distributed file I/O layer to meshage, the framework's message passing protocol, adding Nagios type functionality as a native minimega capability, and expanding the scope of minimega's capabilities to support sponsor funded mission space.

Desired Skills:
Go programming language (minimega is 100% Go) - Go is easy to learn, so if you're a good C programmer, we can teach you Go.
Knowledge or ability to quickly learn network fundamentals
Knowledge or ability to quickly learn virtualization fundamentals, KVM, Qemu
Documentation skills

Looking for:
2UG at 50%

Hosted Hardened Android
Smartphone operating systems are primarily designed for consumer use in mind. Specifically Android and iOS focus on consumer freedoms and leave enterprise Mobile Device Management (MDM) primarily to third-party solutions. While MDM solutions allow certain device and data protections to be enforced (remote wipe, enforced passcode requirements, whitelist/blacklist applications), they fall short when attempting to protect sensitive enterprise information from external compromise by an adversary. In a traditional computing environment, the enterprise incident response team can monitor network traffic and perform host-based forensics for signs of an intruder. This allows them the information they need to respond to a threat as quickly as possible. Mobile devices are portable, travel to many different locations, are intermittently connected to untrusted non-enterprise networks, and despite white/blacklist approaches, may end up running malicious software. It is very difficult to monitor these devices in real time outside of the enterprise environment, and doing so would have a negative effect on device responsiveness and battery life.
To fundamentally change the game and eliminate many of these fundamental problems with enterprise security on mobile devices, we propose shifting the Android platform and all sensitive enterprise data onto a remove server farm and using mobile devices as hardened thin clients. Moving the critical information to a central location within the enterprise makes effective corporate device management, forensics, and real-time network analysis possible. This approach also allows prevention of data loss in the case of lost or damaged devices, and access revocation for devices reported stolen.

Desired Skills:
Android experience, particularly experience with Android development, building/tweaking custom ROMS, the bootloader, and/or the rendering framework.

Hosted Android, And-lantis, and Cloud/Mobile security assessments are looking for:
3G at 50%, 4HS at 50%, and between 1-4 UG at 50%.

And-lantis

And-lantis is a 'mobile' variant of the FARM malware analysis platform. The goal of And-lantis is to add Android malware analysis to the existing Farm infrastructure. Specifically, we are interested in adding dynamic behavioral analysis, via virtualization and monitoring, to Farm. Goals for this summer include creating a representative Android x86 image to virtualize with fake sensor data, create an automated APK install/run capability for Farm to inject malware into the test image, create monitors for each of the network I/O points on Android (wifi, GSM, SMS...), and demonstrate that And-lantis can analyze and detect suspicious applications.

Desired Skills:
Knowledge or ability to quickly learn network fundamentals
Knowledge or ability to quickly learn virtualization fundamentals, KVM, Qemu
Documentation skills

Hosted Android, And-lantis, and Cloud/Mobile security assessments are looking for:
3G at 50%, 4HS at 50%, and between 1-4 UG at 50%.

Cloud security assessment

In this project, security assessment of one or more of the open source cloud solutions such as Openstack, Cloudstack, and/or Eucalyptus will be done.
Vulnerability assessment and penetration tests on Compute, Storage, and Networking resources will be conducted.

Hosted Android, And-lantis, and Cloud/Mobile security assessments are looking for:
3G at 50%, 4HS at 50%, and between 1-4 UG at 50%.

Mobile security assessment

Security assessment of one or more of the popular mobile platforms such as Android, iOS, and/or Windows Phone will be done.
Vulnerability assessment and penetration tests on hardware, software, and network environment of mobile platforms will be conducted.

Hosted Android, And-lantis, and Cloud/Mobile security assessments are looking for:
3G at 50%, 4HS at 50%, and between 1-4 UG at 50%.

IPv6 integration into Captive Portal software

Internet Protocol version 6 (IPv6) is the next-generation network protocol, now being deployed across the Internet in enterprises, Internet Service Providers, tier-one backbone networks, and other environments. As deployment increases, hosts and applications must support IPv6 and dual-stack IPv4/IPv6 functionality. This project involves integrating IPv6 support into a captive portal implementation used for granting Internet access.

Desired Skills:
Previous work with networking, firewalls, open source software, and Web development, including AJAX.

Looking for:
1G at 50% or 2UG at 50%

DNSSEC test suite

The Domain Name System Security Extensions (DNSSEC) add authentication to the Domain Name System (DNS). Adoption is slow, due in part to the complexity involved with deployment and maintenance. Sandia has been involved with global monitoring and analysis of DNSSEC deployment, using DNSViz. This project involves building a DNSSEC testbed with deliberately misconfigured DNS services and a framework and API for testing against them, such that they can serve as a resource for regression testing for DNSViz and other validating/testing tools.

Desired Skills:
The project will require work with networking, DNS, firewalls, virtual machines, open source software, and API development.

Looking for:
1UG at 50%

DHS S&T Competition: Voting Machine Security

Important note: This project will only be available to interns who arrive on or before May 20 and leave on or after August 5.
a. Overall Project Description: A voting machine's operation seems deceptively simple: it needs to input a list of candidates, as well as a sequence of votes, and output the final tally for each candidate, as well as the resulting winner. Remarkably, however, even with this relatively simple functionality, building secure electronic voting machines has proved elusive. This project involves competitive design of a voting system by two Sandia teams, with each team subsequently red teaming the other's design.
b. Summer 2013 Intern Objectives: A team from the CCD in Sandia, CA and a separate team from the CCD in Sandia, NM will engage in a multi-phase competition to design and implement a solution, then aggressively test the solution offered by the other team.

Desired Skills:
Secure design and programming
Penetration testing

Looking for:
1G, 2UG at 50%

Formal Methods

Composition of components with formal guarantees that manifest themselves as global invariants for any program composition.

Desired Skills:
Familiarity with interactive theorem provers.

Looking for:
1G at 100% (specifically requested)
Project not available for pick

Certified Software

Formal verification of software and/or hardware components is typically applied at the end of the development cycle, to check for inconsistencies and errors. For the important case of cyber-physical systems, formal methods are rarely applied at all. Powerful formal techniques may be applied, however, if formal methods are used from the start of development -- such techniques would allow us to design components that are provably correct by construction. Cyber-physical components, in particular, could benefit from this approach. In this project, we will be extending the capabilities of existing theorem provers and model checkers to enable development of provably correct cyber-physical systems. This will be accomplished by adapting these provers to solving problems unique to the cyber-physical domain, integrating provers into Sandia's existing development workflows, and making certain kinds of advanced proof techniques more tractable.

Desired Skills:
Formal methods, theorem provers (especially Coq), physical systems modeling

Looking for:
1G at 100% (specifically requested)
Project not available for pick

H.323 Red Team

Sandia Videoconferencing is a Center of Excellence for NNSA and leads in the identification and mitigation of cyber security in videoconferencing hardware/software. This project focuses on the

hardware and software to securely traverse Sandia's firewall's with H.323 traffic (Videoconferencing over IP). There are four phases to the project. Phase one is the mockup of the infrastructure to mimic firewalls and a DMZ including bridging, gatekeepers, and firewall traversal servers. Phase 2 of the project is to characterize traffic through the firewalls and identify all ports, loads and traffic patterns. Phase 3 involves locking down the traversal servers to comply with H.460 compliant traversal and characterizing the traffic. Phase 4 involves red teaming the solution – looking for and identifying vulnerabilities.

Desired Skills:
Background in IP networks; experience with transport of real-time multimedia on IP; knowledge of firewall policies and implementation; knowledge of vulnerabilities/risks and mitigations of H.323 multimedia traffic. If lacking in these areas, we will mentor you to bring you up to speed.

Looking for:
2G at 50%