Project ideas

Please fill in your name, email address, and general idea you'd like to explore for your final project.

Michael McCanna <acrefoot@mit.edu>, Duncan Townsend <duncent@mit.edu>: Implementing a deniable steganographic filesystem (possibly in a FUSE module). The medium for the stenography is MP3 files, or possibly certain video files (for larger filesystems).

Ben Bitdiddle <benbit@mit.edu>: Helping Android users track what permissions each application exercises over time.

Paul Medlock-Walton <paulmw@mit.edu>: Add security to communications between mobile phones and the server when playing a geo-location multiplayer game using TaleBlazer. http://education.mit.edu/projects/taleblazer (Need 1 more person, server and mobile code both in JavaScript)

Ilia Lebedev <ilibedev@mit.edu>: I would like to Implement dynamic permissions in android: in addition to asking the user to approve permissions during installation, high-risk permissions must be prompted when the application generates an intent. The user can chose to deny or approve the intent, and to optionally remember his decision for current session, for current version of the app, or forever. This approach to access control may or may not require that the intent be handled in a safe way, even if denied, if the application blocks and waits for a response. If time permits, I would also like to explore fine-grained network access policies in Android. I believe it may be possible to construct a demo in google's emulator, or even on a dev phone.

Emily Stark <emystark@mit.edu>, Meelap Shah <meelap@mit.edu>: We plan to build a tool to convert existing web apps into a form that provides data confidentiality guarantees to clients. Our tool will take as input server side code and partition it into two pieces; one piece will remain on the server and the other will be pushed to the client. Data fields containing sensitive client data will be encrypted on the client so that nothing is revealed to the server. The code will be partitioned so that the piece that remains on the server can operate on ciphertext. This will maintain the application's functionality while providing the confidentiality guarantees we desire.

Isaac Gutekunst <igutek@mit.ed>, Jelle van den Hooff <jelle@mit.edu>: We would like to create an application framework that performs tainting of all data, and allows controlled inter-application communication. The framework may allow the concept of a secure clipboard that allows pasting between certain privileged applications. For example, copying from a list of quiz solutions, and a pasting into a new quiz would be allowed, but copying answers into a quiz would not.

Ryan Lopopo <lopopo@mit.edu>, Edgar Salazar <esalazar@mit.edu>, William Ung <willgu@mit.edu>: We would like to allow users to revoke a subset of dangerous android permissions on a per app basis. We will wrap applications in their own sandboxes and interpose on their intents, possibly redirecting them to dummy services.

Josh Hodosh <jo21979@mit.edu>, Philip Marquardt <pm22824@mit.edu>, Michael Specter <mi22536@mit.edu>, Frank Moda <cr21205@mit.edu>: Examine the security of NFC in Android mobile phones with respect to the digital wallet. Exploit any potential vulnerabilities and offer mitigation techniques.

Adin Schmahmann <adin@mit.edu>: I'd like to work on creating a GUI for defining dependencies to help with specifying security considerations. However, if anyone would be interested in creating a version of UserFS, but using capabilities, or finding a way to properly sandbox a web browser binary let me know.

Katherine Fang <katfang@mit.edu>, Yuzhi Zheng <yuzhi@mit.edu>, Deb Hanus <dhanus@mit.edu>, Elizabeth Hawkins <elhawk@mit.edu>: Examining the security of Google's Chromebook laptops.

Eva Rose <evarose@mit.edu>: To allow safe mobile code-exchange between Android components, for example, to permit sending callback code fragments that avoid unnecessary, actual callbacks.

Matthew Falk <mfalk@mit.edu>, Ryan Terbush <rterbush@mit.edu>, Arkady Blaykher <rkadyb@mit.edu>: Exploiting human physiology to enhance security of otherwise trivially guessed passwords by adding timing analysis to password inputs.

Mark Zhang <mzhang@mit.edu> (Jet) Sizhi Zhou <zhou2011@mit.edu>: Implement a predicate encryption file system, which will allow a master to give parties different file permissions with only one encryption key. Looking to implement on a service such as DropBox, using Python.

Madars Virza <madars@mit.edu>: I would like to add a polymorphic backend to LLVM, which could be used to generate deeply watermarked code. Alternatively I would like to work on the PKI problem by implementing additional kinds of notaries for Convergence like SSL Observatory-based notary (currently there is only a perspectives-type notary).

Mikhail Kazdagli <kazdagli@mit.edu>: I'd like to use IntelPIN's binary instrumentation to implement emulation mechanism for unmodified binaries. This feature should allow to analyze dynamic behavior of x86 code, and if it reveals suspicious behavior, this security system should block its execution.

Chris Calabrese <cbreezy@mit.edu>: Possibly working with the Android operating system and writing/analyzing some cool exploits to take advantage of the security model and any implementation flaws in a particular version of the software.

Joe Colosimo <colosimo@>: Hardware side-channel attacks. I'm interested in looking at some basic cryptography libraries for Atmel AVR microcontrollers and potentially exploiting them through side-channel attacks. Existing papers point to these kinds of vulnerabilities as being very real and very measurable. Between measuring timing (which is usually very precise with microcontrollers) and current (which can help mitigate preventions to timing attacks through spincoiling), data should be extractable from the controller. This has applications in embedded devices that have secret keys inside them.

Stefan Gimmillaro <stefang@mit.edu>: Interested in exploring PHP/MYSQL vulnerabilities; creation automatic testing of php websites to search for common exploits. Also interested in p2p data encryption.