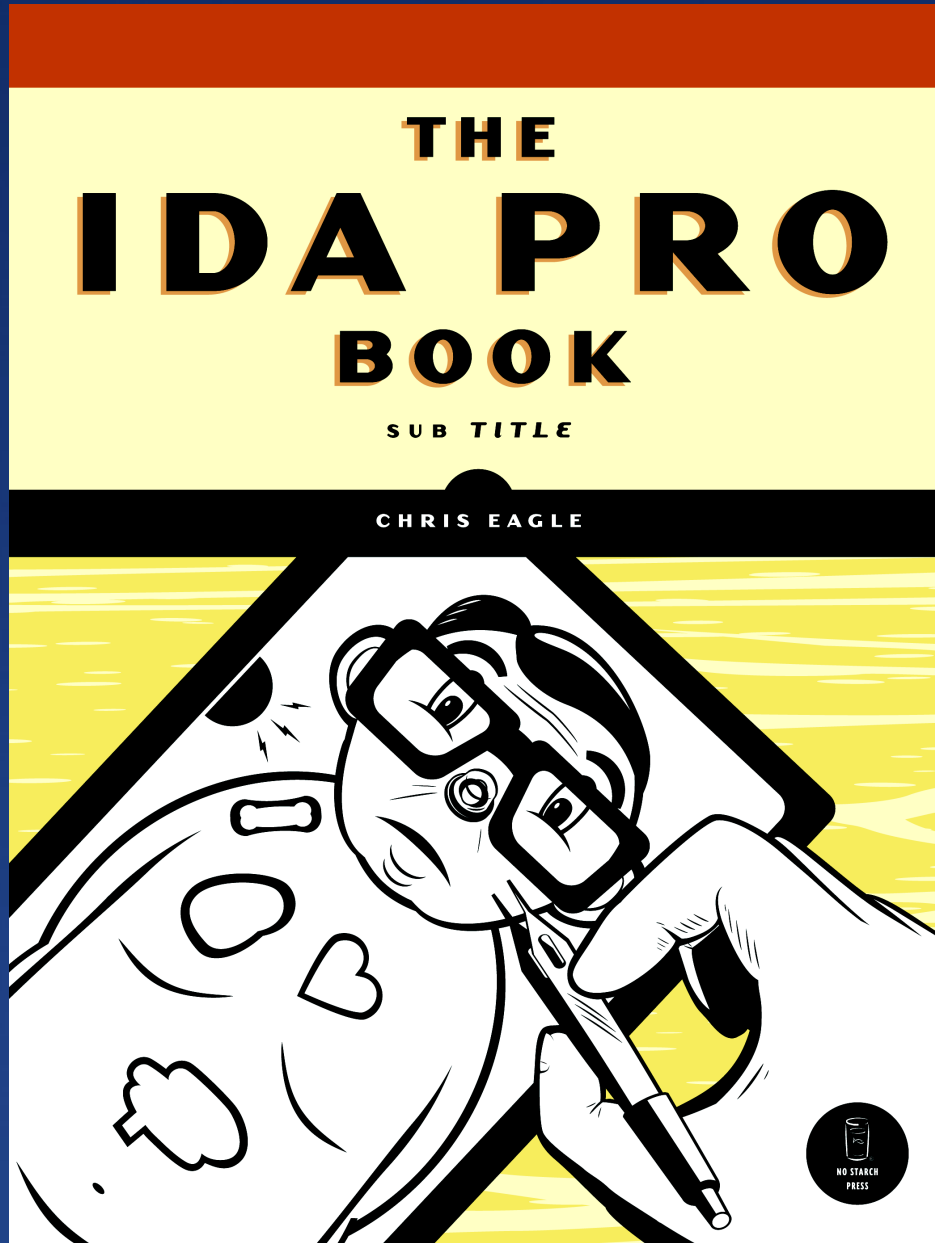




Next Generation Collaborative Reversing with Ida Pro and CollabREate

Chris Eagle and Tim Vidas
Naval Postgraduate School

Shameless Plug



Coming soon
to finer
book stores

Prepare for Demo

- Blackhat demo package
 - Compiled plugins
 - Plugin source
 - Binary for everyone to analyze
- <http://www.idabook.com/blackhat>

Why?

- Because Chris can't spell
- Desire for multiple people to collaborate on a project and synchronize their RE efforts.
- Sharing IDBs is problematic, slow, and doesn't allow for merging changes
- People that want to collaborate have different versions of IDA
- Ida Sync was a great start but kinda busted, and it didn't do enough anyway

Goals

- Automatically sync up to current idb state when connecting
- Allow multiple projects and provide some safety for connecting to the correct one
- Allow users to enter/exit collaboration at will
- Allow forking of projects when participants decide to try different things
- Allow some granularity on what actions each participant is allowed to perform (global/project)

Basic Idea

- Hook as many IDA actions(events) as possible
 - Example: on "create comment" send a datagram to the server
- Server
 - Mirrors the datagram to all other interested IDA sessions
 - Caches the datagram for anyone not currently connected

Asynchronous Comms

- Asynchronous comms/events not easy
 - IDA is single threaded
 - Don't start a second thread that interacts with the database!
- Windows asynchronous sockets post messages to an application's message queue
 - Handled in the GUI event loop
 - IDA Sync and IdaRub use this technique
 - Improved robustness to handle partial sends/receives
 - Complete separation of comms and GUI.

Ida'isms

- There is no pre-action hook (yet)*
 - Sometimes nice to know state before the change takes place
- Some events don't give you enough information (structure rename/delete)
 - Can't tell what old name was
- Resulted in some IDA kernel / SDK patches
 - Found one bug in notification API
 - Requested and received one change in notification API

User Interface

- CollabREate uses native API gui controls/boxes
- IDA SDK offers some user interface elements
 - Too limiting
 - No user defined drop down lists
 - No password fields

Expanding the Idea

- Once we got started a whole lot of "wouldn't this be nice" features popped up
 - Project management
 - Project forking
 - Checkpoints
 - Project migration to another collabreate server
 - Undo
 - Ability to work 'offline' then merge changes
 - Publish and subscribe permissions

Why Undo is Difficult

- IDA stores the original byte value but there is no access to the 'previous' value
- For rename operations, you are told the new name but can't recover the old name
- This could be mitigated by requiring at least two instances of IDA (inquire prior to patch) to collabREate

Why Working Offline is Difficult

- Merging changes would require conflict resolution
- If the project is used by a single participant it's not too difficult
- If the project has had no updates while the user was offline it's not too difficult
- Granular controls on the publish/subscribe model make this more difficult

CollabREate Plugin

- The plugin registers and is available for use once the initial auto-analysis has completed
- Very little state is maintained by the plugin/IDA
- IDA events cause datagrams to be packaged up and sent to the server

CollabREate Operation

- Rather than introducing new hotkey sequences, collabREate processes event notifications
 - Easy installation
 - Easy to capture all actions
 - Difficult to forget to send updates

Plugin Details

- Requires IDA Pro
 - supports 4.9, 5.0, 5.1, 5.2 & IDA freeware 4.9
- Compilation requires g++ or Visual Studio and the IDA SDK for your version of IDA
 - if using cygwin, make sure you have make, g++, etc
 - No official SDK for Freeware 4.9

Plugin Details (cont)

- The plugin can be (and is) built for specific Ida versions
- ...but the capabilities of the plugin still depends on the version of IDA you are using...
 - Some versions of IDA can publish more information than others (newer == better)

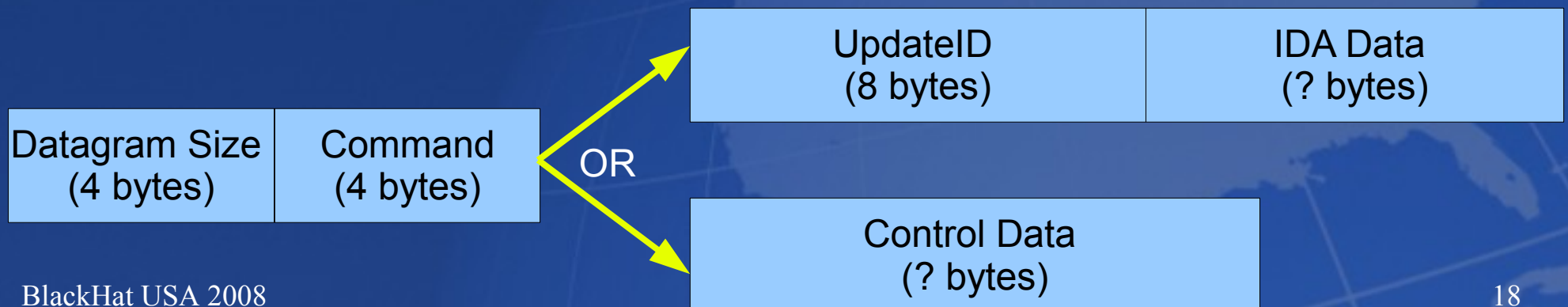
Capability by Version

IDA Version	4.9 / 4.9 FW		5.0		5.1		5.2	
	P	S	P	S	P	S	P	S
Undefine	✓	✓	✓	✓	✓	✓	✓	✓
Make code	✓	✓	✓	✓	✓	✓	✓	✓
Make data	✓	✓	✓	✓	✓	✓	✓	✓
Move seg	✓	✓	✓	✓	✓	✓	✓	✓
Name changed		✓		✓	✓	✓	✓	✓
Function added or deleted		✓		✓	✓	✓	✓	✓
Function bounds changed		✓		✓	✓	✓	✓	✓
Byte patched		✓		✓	✓	✓	✓	✓
Comment changed		✓		✓	✓	✓	✓	✓
Operand type changed		✓		✓	✓	✓	✓	✓
Enum created or changed		✓		✓	✓	✓	✓	✓
Struct created, deleted, or changed		✓		✓	✓ ¹	✓	✓ ¹	✓
Func tail added or deleted		✓		✓	✓	✓	✓	✓
Seg added, deleted, or changed		✓		✓	✓	✓	✓	✓
Flirt function identified		✓		✓		✓	✓	✓

¹ IDA 5.2 and an updated IDA 5.2 kernel is required in order for full structure updates to be properly published.

CollabREate Protocol

- Asynchronous communication
- Binary protocol
- Two command types
 - IDA update datagram (forwarded to other plugins)
 - Control messages intended only for server



CollabREate Server

- Maintains almost all the state
- Handles messages and forwards/replies accordingly
- Can be invoked in either a basic or database backed mode
- Provides an interface for managing CollabREate specific information (users, permissions, etc)

The Server

- Requires Java (tested on JDK 1.6+)
- Two modes
 - Basic
 - Simple reflector
 - No persistence
 - Database
 - JDBC interaction
 - Persistent storage
- Two components
 - Executable jar server to run in background
 - Executable jar management app

Basic Mode

- Requires no database
- Allows multiple projects per binary
 - Selectable by name
- No authentication
 - no storage mechanism for the auth info
 - related: no permissions
- Leaves no 'meta data' in the idb
- All participants must start at the same time
 - with an idb in the same state
 - no support for 'late connectors'

Database Mode

- Tested w/ postgres(8.2+) and Mysql (5.0)
- Requires jdbc driver for your database type
- Requires authentication to the server (chap/hmac - good enough ;-)
- All participants should start with a 'fresh' idb just after autoanalysis, but they can connect to the server at any time

Database Mode

- All updates posted to the project before a participant connects are sent to the participant
- Meta information is stored in the idb
 - facilitates temporarily disconnecting then reconnecting to a project
 - Allows the same 'user' to have multiple sessions
 - changes made to the database while disconnected will not be sent to the server
- Can be used for attribution

Release Schedule

■ Plugin

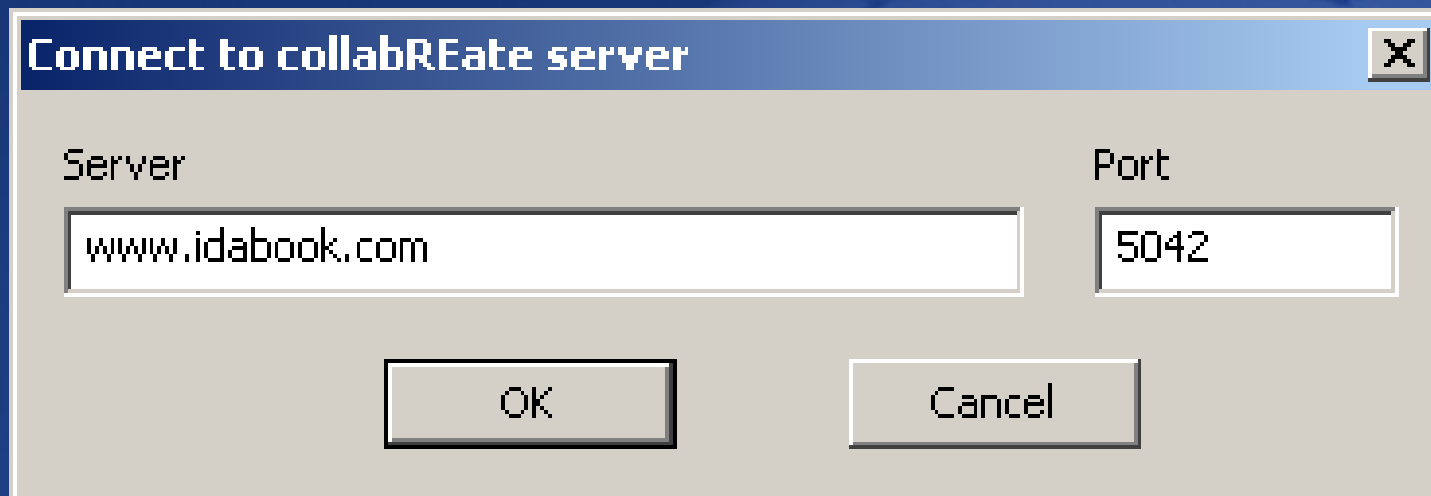
- Source and binaries are available now:
- <http://www.idabook.com/collabreate>

■ Server

- Will be available after Defcon (Monday)
- Source / java jar available **idabook.com**
- Ready to go VMWare appliance on vmware.com/appliances/
 - FC9, java installed, database setup, etc

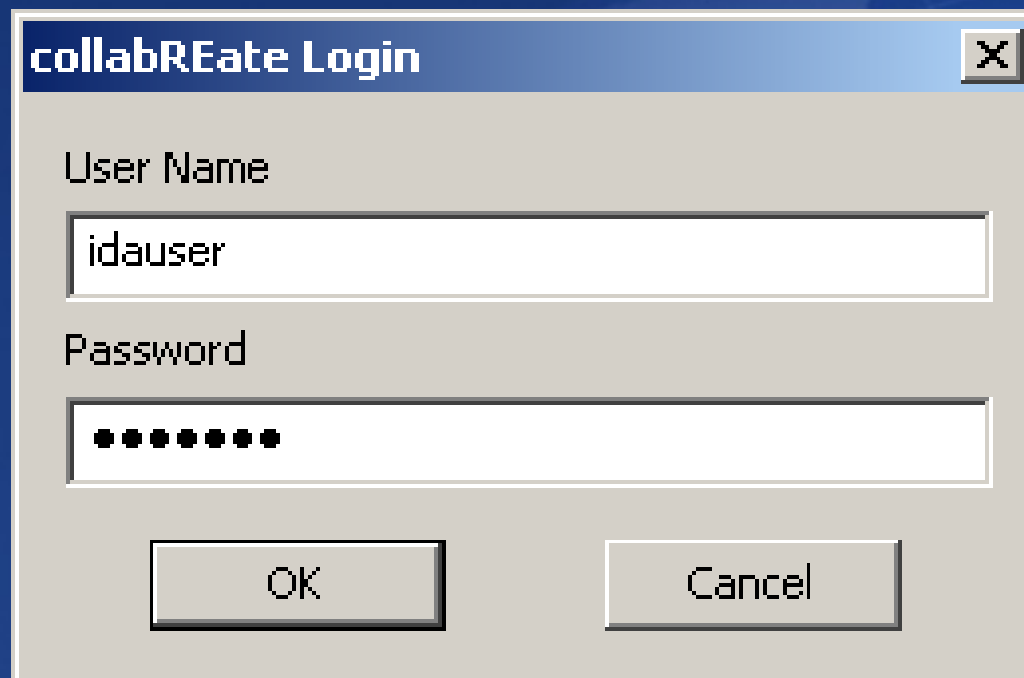
Overview

- After opening a database, activate plugin
 - Default hotkey is Alt-F6



Authenticate

- Provide user name and password
 - MD5 of input file is also sent to server
 - Users are managed by the server administrator



The image shows a Windows-style dialog box titled "collabREate Login". It has a standard title bar with a close button (X) in the top right corner. The dialog contains two text input fields. The first field is labeled "User Name" and contains the text "idauser". The second field is labeled "Password" and contains ten black dots, indicating a masked password. At the bottom of the dialog, there are two buttons: "OK" on the left and "Cancel" on the right.

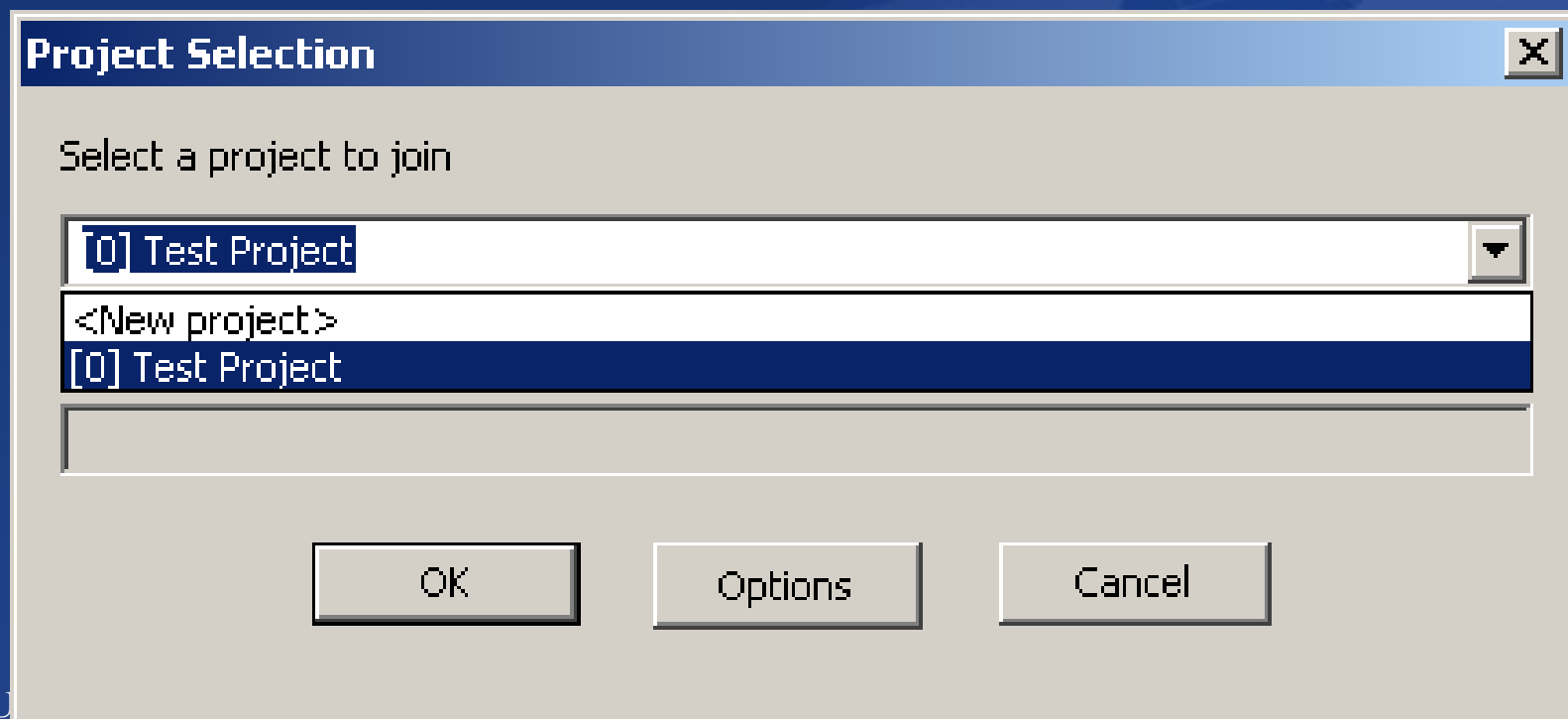
Join a Project

- Two cases

- If you were previously joined to a project you are automatically rejoined to that project
- If you have never joined a project the server sends a list of all projects based on the same binary you have opened (MD5 comparison)

Project Selection/Creation

- Choose from compatible projects
 - Based on MD5
- Set desired permissions



Specifying Permissions

- Choose what you want to publish or subscribe to
- For new projects dictates what others can do



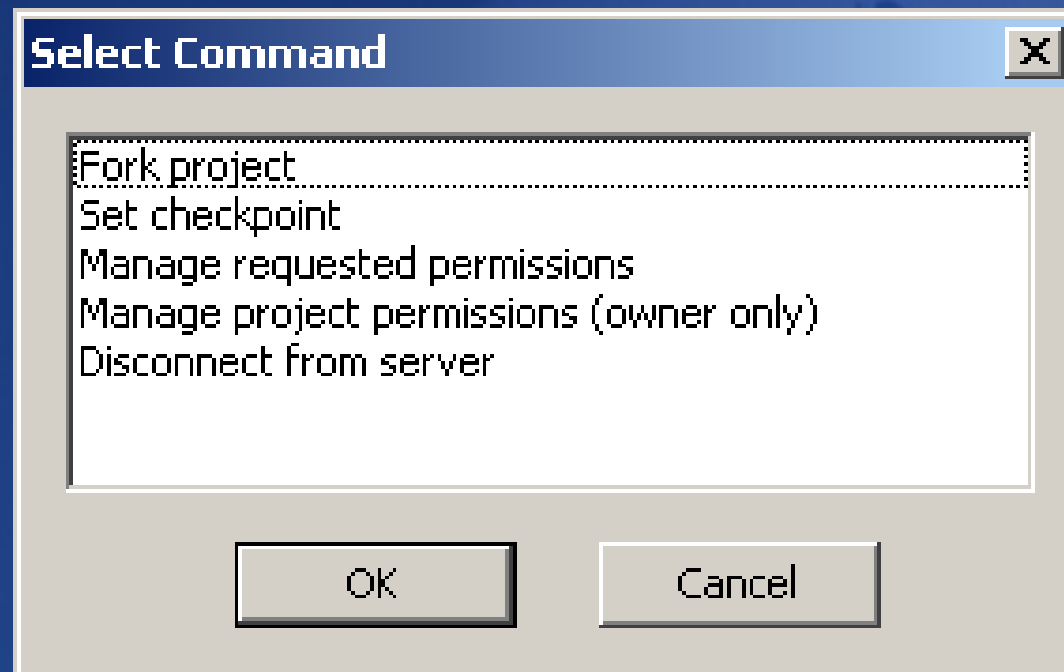
The screenshot shows a dialog box titled "Project Options" with a close button (X) in the top right corner. The dialog contains a list of options, each with two checkboxes: "Pub" and "Sub". All checkboxes are checked. Below the list are four buttons: "Subscribe All", "Subscribe Only", "OK", and "Cancel".

Options	Pub	Sub
Undefine	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Make Code	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Make Data	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Segments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Renames	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Functions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Byte Patch	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Comments	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Otypes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enums	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Structs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Flirt	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Thunk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IDP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Buttons:

Additional Commands

- Rather than introduce several new hotkeys, collabREate overloads its activation key
- When already active, the hotkey provides access to additional functionality



Demo

- Basic mode
- Database mode
 - Binary versions and source are available at <http://www.idabook.com/blackhat>
 - Put the collabreate.plw for your version of IDA into your “plugins” directory BEFORE opening IDA
 - Open IDA (use demo.exe found in blackhat.tgz)
 - Hit **Alt-F6** to start collabREate
 - Username: blackhat
 - Password: Really? (no really it *IS* “Really?”)

Other interesting uses

- Install plugin X or script Y on one collabREating copy of IDA
- The effects of X or Y are mirrored to other collabREators (installation not required)
 - Nobody blindly executes precompiled binaries do they?
 - Has anyone actually built IDAPython or IDARub?
 - Why make everyone on the team experience the pain?
- Assumes that X or Y cause IDA to generate events that collabREate recognizes

Other Interesting Uses

■ Learning environment

- Projects can essentially be setup as “read only”
 - This amounts to full subscribe and no publish permissions on the server
- This way the project owner can push in-class IDB updates to students with no fear of a student messing up any database but their own.
- Students can still navigate, open subviews, etc while updates are occurring

Future Work

- New API will allow even more events to be hooked
- Pre-hook events will facilitate an UNDO feature
- Better permission interface
- Merge algorithm for offline changes (maybe)
- Project migration across servers

Questions?

- Anyone? Bueller?
- Let us know how CollabREate works for you!
- Contact info:
 - Chris Eagle, cseagle <at> gmail
 - Tim Vidas, tvidas <at> gmail

References

- Ida sync
 - http://pedram.redhive.com/code/ida_plugins/ida_sync/
- Ifak's forum entry on about 4/28
 - <http://www.hex-rays.com/forum/viewtopic.php?f=8&t=2055> (reg req'd)
- JDBC
 - <http://jdbc.postgresql.org>
 - <http://www.mysql.com/products/connector/j/>
- CHAP RFC 1994
- HMAC RFC 2104

FAQ

- Q: Since you must open the binary and allow IDA to complete the auto-analysis prior to connecting to the CollabREate server, won't different versions of IDA (and thus different versions of auto-analysis) result in a slightly different disassembly?
- Q: How do you guarantee that the databases all start in the same state prior to receiving CollabREate updates?

FAQ

- A: you could force IDA to not do any analysis upon open, then start the plugin, then force a re-analysis...and hope that all of the analysis actions have events in IDA, AND hope that collabREate recognizes all the events....
- but in practice, the auto analysis' from different versions are “close enough” to being the same “most of the time” for effective collabREation
(no, we don't have any stats to back this up)

- Feel free to inform us of your experiences

FAQ

- Q: how did you make a plugin for the freeware?
- A: made my own freeware specific SDK – no it's not available to the public.
- Also see http://www.woodmann.com/collaborative/tools/index.php/IDA_Free_4.9_SDK_Library_Patch (YMMV)

FAQ

- Q: Does / can the plugin control the focus in IDA? (eg can attached plugins automatically scroll)
- A: No. For one, this would have limited usefulness for CollabREation, second IDA doesn't really provide access to these kinds of events.