Semester Project Proposal

Orie Steele, Simon Sidhom, Tom Parisi, Ken Bodzak

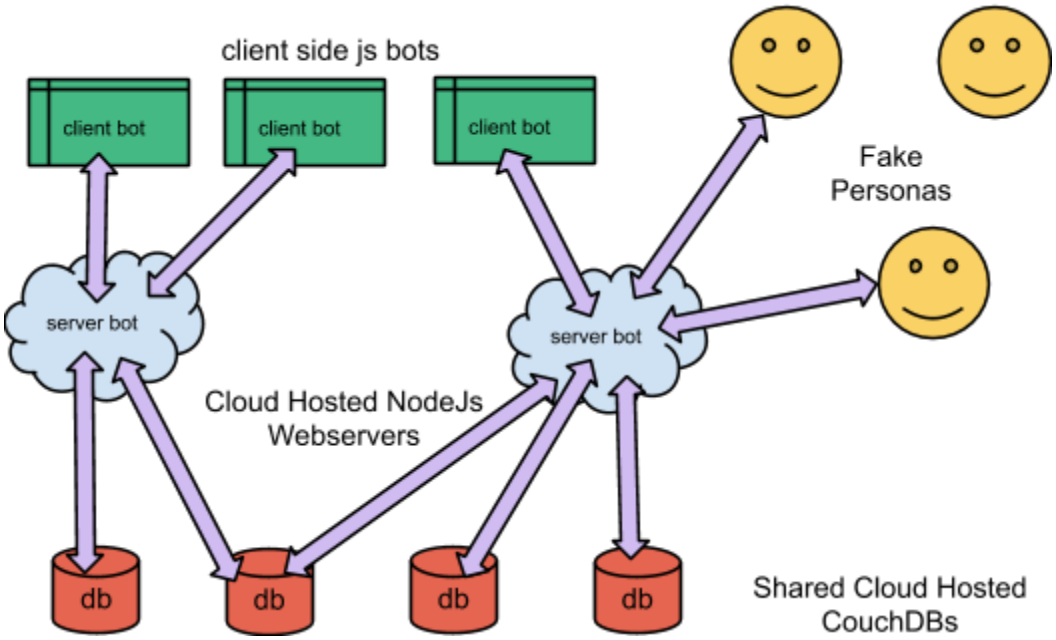
1 Project summary

We propose to build a javascript implementation of a voluntary botnet for management of an online persona management system. We hope to explore techniques for C&C, data warehousing, client side ajax injection and worker scheduling within a computationally limited framework. Our goal is to build the nodes in NodeJS with CouchDB for data persistence and warehousing. We hope to implement a hybrid structure similar to the one described in :

An Advanced Hybrid Peer-to-Peer Botnet
http://www.usenix.org/event/hotbots07/tech/full_papers/wang/wang.pdf

We hope to explore the system described as: Operation Metal Gear (http://anonnews.org/?p=press&a=item&i=752)

This system is apparently a tool for managing many fake online profiles for the purposes of entity manipulation and correlation through social media. This type of system sits at the crossroads between psychology, security, and pattern recognition. It could potentially be applied to influence large numbers of real world individuals, and as such represents a serious threat to critical systems both technological and social. In order to ensure the effectiveness of such a tool, the system must be able to influence public opinion by maintaining and controlling fake online persona's without being detected.



2 Motivation for the project

The recent revolutions world wide coupled with the accelerating role of social networks in coordinating peaceful protests make social network manipulation a prime target for adversaries both domestic and foreign. The prevalence of free cloud based services offers an opportunity to build scalable distributed web applications for close to zero cost. A pure javascript implementation allows for simplicity and ease of adoption as a platform for research and development including easy integration with RESTful web services and public API's. According to the article posted above and links within the article, this is an active area of research among organizations which are serious about security.

3 Approach

Each node of the botnet will be a web server written in NodeJS with an interface to a CouchDB database. We hope to keep the coupling between server and database loose. We plan to explore the benefits of sharing a remote RESTfully accessed database and facilitating client side javascript worker scheduling. The bot net will access social network profiles, social news sites and other public data sources, retrieve public data and then re-post modified data and occasionally messages coming directly from command and control. We will also explore the possibility of created automated fake persons with predetermined agendas. We hope to analyze the influence of injected information has on existing social networks, and attempt to track its progress through the network in order to determine optimal injection points and types.

4 Expected outcomes/deliverables

We hope to build an extensible platform for coordinating sock-puppet botnets. We plan to report on the security risks and benefits of pure javascript implementation in addition to possible real world extensions of the platform, both malicious and non malicious. Because the project may be to large for the scope of this class, we plan on building a community and framework for future development in addition to a relevant research section for topics which we may not be able ti implement or cover during the semester.

5 Division of labor

Coding will be done in a team programming style. We will at least design the program together in the same room and then split up the modules.

There will be many opportunities for relevant research which may or may not be implementable in the time frame provided. We plan to track relevant topics, and provide channel for crowd sourced contribution to the project.

6 Timeline

We plan do develop this project agile style, everything all at once, here are some estimates on the overall time to be spent on each component.

System Specification (About 1 Week)

Platform Development (3-4 Weeeks)

Algorithm Design and Analysis (mostly literature review) (2-3 Weeks)

Documentation Community involvement and future work (1-2 Weeks)