Project Proposal

Aaron Greenberg, Allie Duncan, Cypress Frankenfeld, Geoff Pleiss

Our goal is to better understand cyber security by implementing our own worm. Ideally, this worm will be for mobile devices, since mobile cyber security is a new field. This worm will contain a payload to demonstrate that it has infected a device, and potentially will install a backdoor to root the device. Through this project, we aim to understand malware propagation, firewalls, and network security.

Techniques:
After researching mobile device security and computer worms, we will utilize software design principles to outline the structure and function of the program we intend to create. With the planning complete, we will implement the program, ideally using C. To ensure that the computer worm functions as intended, we will perform some type of sandboxed verification.

Minimum Deliverable:
The minimum deliverable will be a worm that spreads across devices (computers or mobile phones). It will be able to replicate itself and spread to other devices (possible via email, network, etc.), and will carry a simple payload.

Maximum Deliverable:
The maximum deliverable will be a worm that spreads across *mobile* devices. It will create a backdoor in the device that will give a remote user root access to execute programs. Ideally, this worm will be spread in a discrete mobile-specific manner (e.g. via bluetooth).

Starting up:
Our first step is to begin researching the design and implementation of computer worms. We need a foundation of knowledge to be able to understand how we want to create a worm for mobile devices. We will also need to research security of mobile devices to figure out how to discover vulnerabilities that can be targeted by the worm we build.

The main challenges we foresee are:

- Finding a vulnerability on a mobile device that we can exploit to gain root permissions
    - We have contacted Mark Chang (our resident mobile expert) to enlist help in finding this.
    - It may be easier to find exploits in older OSs, which have more known problems.
- Spreading a worm safely without it contaminating devices other than our own
    - To make sure that we are not running a risk of unintentionally infecting devices, we will need to enlist the help of Allen or IT in setting up a safe working environment.