Vsevolod Ivanov
Concordia University
seva@tumahn.net

HackerPot

10th November 2016

GENERAL REQUIREMENTS

I. Your project must have more than one level of interaction and must afford the intended modes of interaction.
II. It must be meaningful to users beyond the element of surprise.
III. It must be functional for the presentation.

OVERVIEW

A non-technical description of the themes and major elements of the project that answers the four questions at the top of the page (minimum 250 words per question)

1. *Think of a context and an environment where you would like to intervene. Where will you present your project? Who is it made for?*

   At the rate at which the technology advances, the Internet of Things might be a future that awaits us all. The low cost of the hardware makes it more accessible. The developing documentation is open to everyone with an internet connection. Anyone can become a creator with reasonable time investment. However, building something without an engineering background comes with a price. Notably, the security standards are either at the bare minimum or absent. This reality for the IoT is well reported by the vulnerabilities statistics[1]. The Internet of Things are accessible by anyone connected in its network and if no proper procedure ensuring their security were followed then, they can and they will be eventually be hacked. From this point, they can be misused in a variety of ways depending on their capabilities and possible profit for a hacker.

   Moreover, it is important to underline that the security audits are often performed by security analysts. The vulnerabilities of and IoT device are difficult to identify and even harder to visualize which makes it less accessible to the general public without particular knowledge in this domain.

[1] http://go.saas.hpe.com/fod/internet-of-things

This project aims at providing an insight into malicious activity happening in your network targeting your IoT by presenting itself as an easy bait. Once a hacker attacks it, it will notify this event using a certain output associated with a certain attack type. The latter will make these events comprehensive for users without any specific knowledge about virtual security.

The HackerPot will raise awareness about such events to encourage its users to take actions at securing their networks. It will be presented as an artificial decorative plant inspired by the Venus Flytrap plant and the HoneyPot computing concept.

2. *Think about the kind of relationship you wish to foster between your users and the artifact or installation. How can you use your project to destabilize the users and make them reflect on themselves, their environment and society?*

   I want to establish a bio-technological relation between a user and this object. The exponential human technological advancement will soon allow a user to encode data and to control biological plants[2]. By the means of this project, I want to encourage the exploration of this domain by conceptualizing a speculative, plant which interacts with network ecosphere, processes its input and outputs to a physical world with a comprehensive content for the human user. On one hand, we are using the virtual HoneyPot concept to attract hackers to this vulnerable appearing system. Then, we record their activity and we use the artificial Venus Flytrap plant’s coil to present the results to the user.

   It allows its users to sense an invisible world of internet communications accordingly to which the HackerPot reacts. Its physical reaction informs the user of a possible malveillant intruder to make the person aware of this invisible presence. From this point, it is up to the user to define a way of dealing with this issue according to the type of alert received. This is a very promising first step into the direction of protecting the user's privacy by explicitly underlining the virtual abuse of rights happening in the network.

   The Snowden leaks about mass surveillance programs such as PRISM performed by the NSA agency was quite revealing on the extend of this situation. Considering that privacy is a basic human right which every human deserves unconditionally, it is a very severe infringement.

[2] http://advances.sciencemag.org/content/1/10/e1501136.full

In fact, HackerPot is not only designed to catch a stereotyped shady hacker wearing an Anonymous mask or yet another Mr. Robot but rather it is there to catch anyone performing malicious activities on your IoT device. Whenever, it is a curious human, a bot, a worm or a coordinated attack, it will record this events in forms of logs to allow further analysis to identify what really happened.

The future versions could contain a machine learning algorithms to enable it to learn from the attacking behavior to adapt itself into this constantly evolving technological world. The latter is currently simulated by the updating of the Raspberry Pi HoneyPot framework which embeds recent detection techniques.

3. *Think about the notion of empowerment. Is your artifact really helping or challenging its users in any way or is it just another psychological prosthesis?*

   This project encourages the exploration of a digital world by using a very simple HackerPot interface to observe the dynamics of malicious network activities. In fact, the road to the user's appropriation of this device can be resumed as such:

   Awareness → Action → Control → Empowerment

   The HackerPot goal is to inform a user of malicious activities in the network that may be unleashed on any other of your IoT devices. Furthermore, it stores the logs (records) of those events and it can be extended to implement your current IoT devices if their source code is available. Stepping back from all these possibilities into the *Awareness* part, we can directly see how the physical HackerPot object can make the user aware of its happening by the use of different physical responses. Then, the user can either shut down to ignore a "notification" of a certain type of attack or leave it to accumulate them into a visual representation of the most popular attacks.

   $$\text{attacks} \equiv \text{notifications}$$

   This means that attacks of a certain type are proportional to the number of notifications a user will receive allowing him to see its dynamics.

   $$\text{constant} * (\text{number of notifications}) = \text{output intensity}$$

   Then, there could be a correlation between attacks from the same category and as an example, the output intensity. In case, the notifications aesthetics are more pleasant with a flickering lights of a certain speed, their quantity could be proportional to the speed of the light's flickering.

4. *Think about something meaningful. What are you trying to tell us with your project?*

This project aims to explore the merging between the virtual and the physical world by introducing a crucial security concept in a playful manner. Security is often neglected and a very common argument serving as a justification to avoiding learning about it :

“There will be always a zero-day”

Also known as day zero, it’s a timestamp when a new undisclosed software security vulnerability is announced to the public. It is an endless day for any security head that have to find a patch or workaround for the impacted software components as soon as possible.

Taking this argument as a justification for avoiding securing your software systems would be as good as letting the door of your house unlocked by stating that someone will always find a way to go inside. Of course, when we talk about our physical world suddenly we realize that we have double standards with the virtual one. One of the reasons of this would be due to a more concrete feeling of the impact. However, when someone is emptying our bank accounts, stealing our personal data or using many hacked slaves machines to perform highly demanding electrical tasks, we always rely on this higher entity referred to as a system. We live in this system and it protects us which comforts us and it makes us careless about the virtual security. Nevertheless, as the complexity and magnitude of the virtual world keep expanding, we realize how hard it would be to control every possible vulnerable machines with a small federation of “systems”.[3]

In the same direction, a very common technique in pentesting[4] on a highly secured enterprise is to use something called social engineering. What happens is that instead of trying to find virtual vulnerability you socially trick its employees without any security-wise training in order to physically go inside one of its buildings and to hook an usb with a virus into a computer or even the server room. Thus, bypassing all of the complex and highly secured external structure.

To both of these previous situations, there is one main weak point namely, the poor employee without any security-wise training…

[3] https://youtu.be/ZdhyM5jHu0s

[4] https://en.wikipedia.org/wiki/Penetration_test

This project addresses this weakness components by presenting the security aspect in a playful manner. It is informative but most importantly educational because it stimulates a response from the user according to humanly unseen malicious activity in the network. Not only it will reduce the delay in response to an incident but perhaps, a HackerPot will serve as a skeleton for introducing educational IoT security that will allow a user to respond to these type isolated events itself without relying on any external systems.

STORYBOARD

Describe your project's levels of interaction through a storyboard

Interactions:

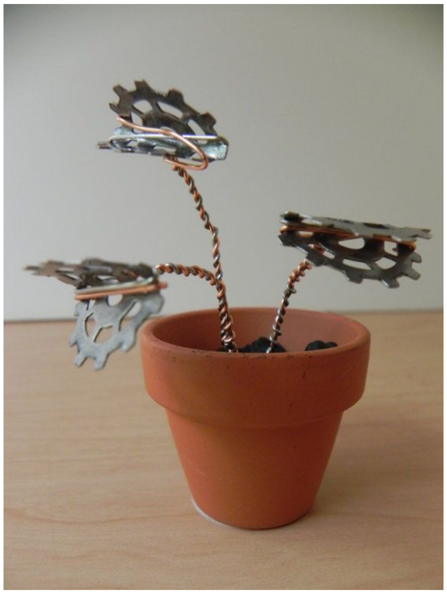
1. HackerPot ⟵⟶ Network ⟵⟶ Hacker
2. User ⟵⟶ Physical gesture ⟵⟶ HackerPot

Technical:

- Each branch with a leave is for a type of an attack
- Color reacts as the number of attacks increases
- Progressive bending of leaves if a hacker is catched (depending on time)

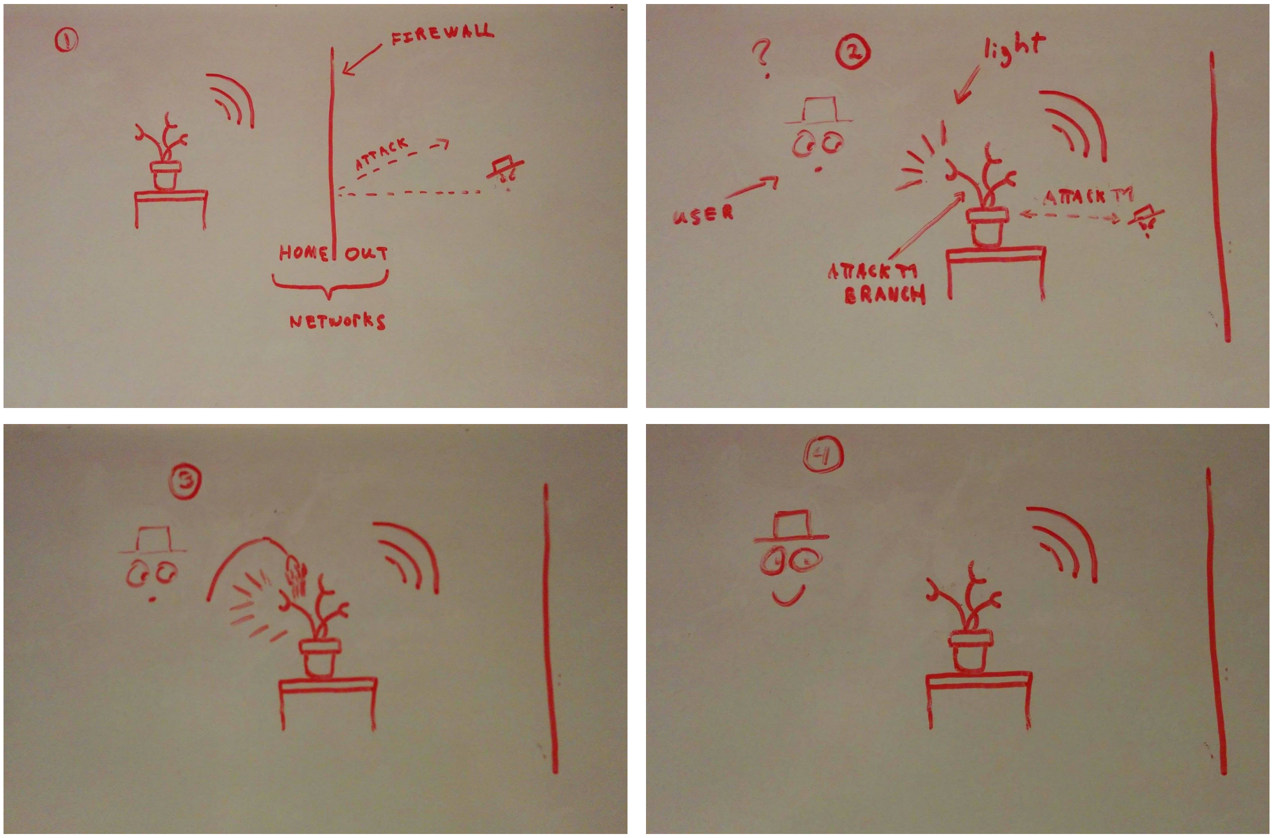
Inspiration:

- NightwindStudios Sculpture on Etsy[5]



[5] https://www.etsy.com/ca/listing/198123362/steampunk-venus-flytrap-wire-sculpture?ref=market

Storyboard:



Note : the progressive bending of leaves on a hacker catch was not included due to uncertainty of its implementation.

SIMILAR PROJECTS

Research and give a brief summary (minimum 250 words each) of at least three similar projects).

Notes : The HoneyPot computing concept is mainly virtual. This is mainly due to the fact that it is designed for the security oriented individuals. Therefore, I did not find any complete IoT HoneyPot device. By using intensive computing power, it is possible to emulate many virtual hosts in the network using only one physical device. Often an old computer or even directly the computer of a person can be used to simulate a large variety of physical devices on the network. This doesn't stop us at seeing how useful these case studies are into understanding the possible interactiveness by imagining its possible physical representation.

For the physical part related to the Venus Flytrap plant, I found an alternative method of creative a stimulus of a material using soft tissues in robotics. However, this may be hard to create due to time constraints.

I. Toaster[6]

An interesting case of study happened when Andrew McGill decided to simulate a primitive toaster connected to the network. He achieved this by using a server that appeared as a toaster to the network users. This device was presented with a basic terminal access control panel. The credentials were picked from the most commonly used ones.

The main purpose was to get some statistics on the malicious activities happening in a quite looking network. He connected this "toaster" to the network at 13:12 and since the online activity seemed very calm, Andrew expected to wait few days or weeks to get some results. However, he got the very first hacking attempts at 13h53. It was interesting to see that the human or bot was trying to use this toaster's model for the credentials before going with the most commonly used password and succeeding its attack.

He didn't expect it to be so popular and it makes us realize how many unnoticable attacks can be ongoing without our knowledge due to lack of tracking resources. It is very amusing to imagine a real physical IoT toaster simulating a toasting action after each successful exploit.

[6] http://boingboing.net/2016/10/28/insecure-internet-connected.html

II. Raspberry Pi Honeypot[7]

This is quick overview of how a networking individual can create a HoneyPot to analyse basic security traffic. He explains that the main advantage of using a Raspberry Pi over an Arduino is that it allows a user to install an Operative System such as GNU / Linux. In turn, this system contains security packages containing all of the major tools needed for a creating of HoneyPot such as a package called Dionaea. From there, you can make it even simpler and avoid writing your own scripts from scratch for all of the use cases by using a framework build on top these tools. An example of such framework would be MHN (Modern Honey Network) that has everything build inside and on top of that it is constantly updated by the latest techniques due to its Open Source nature. Therefore, one of the only parts a person setting up a project using fully the HoneyPot concept would be to configure this framework for its needs on top of an GNU / Linux Operative System.

After which, one could write a little script notifying when some event is triggered to some external software listening for those.

III. Flytrap inspired robot[8]

The purpose of this research was to create an artificial Venus Flytrap insectivorous plant by deciphering its bio-mechanics. The dynamics of this plant are as follows : when an insect passes in the leaf of the plant, this leaf will suddenly bend and close on top of the insect and imprison it for nutrition purposes.

In hard robotics, the joints of the leaf can be implemented using mechanics adapted for rigid bodies. For instance, the actuation of the artificial leaf to catch an insect would be implemented using motors, sensors and a controller. In turn, this will allow only a discrete number of degrees of freedom.

Whereas, one could have a continuous number of degrees of freedom in soft robotics. It would be achieved by creating a tissue like material that will bend according to externally controlled actuation agents.

A quite simple looking mechanism turns out to be a very complex and intriguing one that approaches the robotics in a non-traditional way using hard robotics.

[7] https://www.rs-online.com/designspark/raspberry-pi-honeypot-helps-you-to-improve-your-network-s-security

[8] http://biorobotics.snu.ac.kr/wp-content/uploads/2014/05/2014_BIOBIO_Flytrap-robot.pdf

One aspect which this study highlighted to me is that this soft robotics motions are similar to the way our joins are bendings after an actuation agents are stimulated by our nervous stimuli.

For the HackerPot, it could be a very interesting and elegant way to create a smooth and gradual motion of bending the leaf to illustrate the newly trapped prey. After which, the leaf could come back to its original opened shape by representing the food digesting with a certain delay of time before reopening.

CONCLUSION

Write a paragraph on how/why your project will be different and more interesting in comparison to the projects you researched.

As stated previously, the HoneyPot computing concept is mainly virtual whereas the Venus Flytrap plant is purely biological. Therefore, I think that my project is very interesting because it creates a unique artistic binding between the virtual computing and the biological plant concept to form a bio-technological IoT HackerPot artifact inspired by the similar projects in each of its composite domains.