# demonsaw

Demonsaw is a new type of secure file sharing application that's secure, anonymous, free, and everywhere. It's designed to protect our anonymity and hide what we're sharing. Unlike traditional P2P networks, our IP addresses are never revealed to the world. Demonsaw is wrapped in multiple layers of user-derived cryptographic algorithms based on a new and modern security model called, Social Encryption. We can share whatever we want, with whomever we want, without fear or consequences. Safeguarding our privacy and protecting our Right to Share are the primary goals of demonsaw.

# Overview

Public-key cryptography is a proven solution for secure electronic communication over an open network without relying on a covert channel for key exchange. The use of asymmetric keys is what makes public-key cryptography possible. Founded on strong mathematics and extremely large prime numbers; public-key crypto is the de-facto standard for securing messages in the Modern Internet.

While public-key cryptography is truly awesome, it's not suited for every use. To begin with, it's a complex subject that is difficult for non tech-savvy individuals to understand. It works great in 1:1 or 1:n relationships, but difficulties begin to arise when a large group of people want to securely communicate with one another (i.e. n:m) in a dynamic environment. Exchanging public keys quickly becomes an exponential problem as more and more people are added to the group. And relying on the same key store or key store synchronization has its own problems, such as replication delays and server outages.

This presentation will demonstrate how groups of people can securely communicate without using any form of key exchange or public-key crypto. By using the contents of simple, online resources as sources of entropy, we can derive very strong encryption keys that members of a given group can use to communicate with each other. It's much easier to remember a web page than it is to remember the locations of public keys. Sometimes it takes a revolutionary idea to start a revolution.

# A Trusting Culture

- When people think about online security they think about the well-established model whereby centralized authorities mediate the flow of traffic and verify the cryptographic identities of the parties involved in every transaction.
- This model has worked well for the past 30+ years, ushering in a new era of online commerce.

# A Social Culture

- But times have changed, and we have become a social culture

- We're not just giving away insignificant details about our lives now
- Today we share so much about ourselves that who we are online reveals who we are in real life

# A Fearful Culture

- Recently we have been betrayed by governments and corporations through illegal data acquisition and security breeches
- As a result, we have become fearful and paranoid
- We have learned some difficult lessons, understanding that security models based around trust are inherently insecure

# An Empowered Culture

- We need to take responsibility for our own security - we need a new security model
- It needs to be cryptographically strong
- It needs to be decentralized: no authorities, no key stores, and no external trust
- It needs to be simple, flexible, and easy to use
- It needs to be scalable to meet the needs of the individual rather than the corporation
- We have the power to change the future

# Social Encryption

- Social Encryption is new security model designed for the individual to protect our right to privacy
- It uses 1:n webpages, documents, forum posts, or any other online resources as sources of entropy
- After specifying the online resource(s), we read in a percentage of the bytes from that online resource
    - Note that the percentage of bytes further increases the difficulty to brute-force
- It's these bytes that are the source of entropy
- We then use a key derivation function (e.g. PBKDF 1/2) to create strong symmetric encryption keys from the bytes we read in
- If multiple resources are specified we can chain the key derivations together to create even more complex key derivations
    - Cipher Block Chaining (CBC), XOR'ing the bytes, etc.
- Multiple people, each knowing the same URL(s), can derive the same encryption key by simply specifying the same web page or other online resource. Note that we never exchange any keys. Each person arrives at the same end-result because the sources of entropy are the same.
- Symmetric encryption/decryption can then occur between each personal who derived identical keys
- There is no revocation either. Simply changing which online resources are referenced (or their ordering) will be enough to completely alter the final end key, thereby creating a new secure group.

# Out-of-Band Knowledge

One might ask, "If out-of-band communication is required, then why not just exchange public keys and use a technology like PGP?"

There are 2 ways to answer this question.

1. To begin with, public-key cryptography always requires out-of-band communication. How? Either the locations and/or public keys themselves need to be exchanged between parties unless a secure key exchange algorithm (e.g. Diffie-Hellman) is used.
2. Social Encryption is not mean to replace public-key crypto, but to supplement it by providing an alternative that doesn't require any infrastructure components (no private/public keys, no key stores, no revocations, etc.). Not to mention the fact that there aren't any private keys that need to be kept private - just the sources of online entropy. There are companies/individuals who share private keys today - a terrible and insecure practice. Social Encryption solves this by using symmetric encryption instead.

3. Complex Social Encryption might require some out-of-band communication (as does public-key crypto), as in the case of multiple web pages with varying percentages of the bytes used for key derivation. Even in this case, there are no infrastructure components that have to be setup, such as public keys. One huge benefit of Social Encryption is that there are no private keys that need to be kept safe.
4. Simple Social Encryption doesn't usually require out-of-band communication.
    a. Why? Because the type of information that's needed to access the source of entropy is something as simple as a web page address.
    b. And, Social Encryption can usually safely make the assumption that most of the secure groups that individuals want to interact with already have a pre-establish shared knowledge base.
    c. For example, I know where my Mother works. Her company has a web page. She and I both know this. This is all that's needed for us to use Social Encryption to derive the same cryptographically strong key.
    d. If we want to increase the cryptographic strength of our key derivations (i.e. possibly prevent an outsider from guessing her work website), we can use her birthday, March 17 60, as the percentage of bytes we will use for key derivation (17.6%). Or an even simpler solution is to use the URL of an image buried in her company's website, perhaps the image of her receiving an award for performance last year.

# Why Not Just Use Strong Crypto?

One might ask, "Once you are willing to go so far to achieve this, you can simply use existing strong crypto to do it anyway?"

Sure, one can always use strong crypto, with private/public keys, key stores, and the requirement to keep the private key secured. And many applications take this approach. But up to this time, strong crypto hasn't really been easily accessible to the average, non-tech savvy individual without some sort of infrastructure in place. Most people don't understand "private" or "public" keys. But they understand a webpage or an image on Facebook/Instagram. The ability to empower individuals to secure their own private messages and information exchanges without a traditional cryptographic infrastructure is a new and emerging market. In a world where our privacy rights are continuing to dwindle, we need to empower the individual to be accountable for their own security. That's what Social Encryption is all about.

# The Benefits of Social Encryption

The benefits of a security model like Social Encryption are huge. Here is a quick synopsis of some of the key benefits:

- No centralized authority
    - No infrastructure components
    - No private keys to lose
    - No public keys to host
    - No need to worry about key revocation
    - No need to worry about which online key store to use or whether it synchronizes with other key stores in a timely fashion, etc.
- Leveraging webpages or other online resources as sources of entropy
    - There is entropy all around us
    - Billions of sites, web pages, and images located in cyberspace
- Adding multiple online resources increases cryptographic strength
    - 1:N resources
    - The more layers we add, the more computationally infeasible (i.e. impossible over the span of a single lifetime) it becomes to brute-force the key(s)
- It's easy to remember a webpage, not easy to remember public key servers, ports, etc.
    - Many of these web sites are already committed to our long-term memories, e.g. reddit.com, cnn.com, demonsaw.com, etc.
    - Everybody has URL's in common
    - Most of the people we interact with share some common sites

- No Revocation
  - No need for setting up a revocation process/plan
  - Just change the ordering of the URLs, add/remove a URL and the end-result cryptographic keys change
  - Change the percentage of entropy use and the same thing happens
- It's important to note that there is always shared knowledge, even with public-key cryptography
  - Contextual, or shared knowledge, is required with Social Encryption is, but it can be pre-knowledge and therefore no out-of-band communication is needed
  - Instead of knowing he location of a public key, we remember a URL
  - This URL can with an html page, an image, an online document, or anything accessible online

# Summary

In the past, the ability to securely communicate and share data was a difficult problem. It either required a huge security infrastructure with authorities and key stores, or an exchange of keys via many different secure message exchange protocols (e.g. Diffie-Hellman). These past solutions had many problems, including the lack of scalability, difficulty, and reliance on other components, protocols or technologies to make everything possible.

Social Encryption is a new security model that takes into consideration our vast amount of shared knowledge. It uses this as a form of entropy by which cryptographic keys are generated. No new knowledge is required. Both small and large groups of people can use Social Encryption is to securely communicate and exchange data, either at home or in hostile and oppressive environments. It's by our shared knowledge that we are able to protect ourselves so well.

**Eijah**