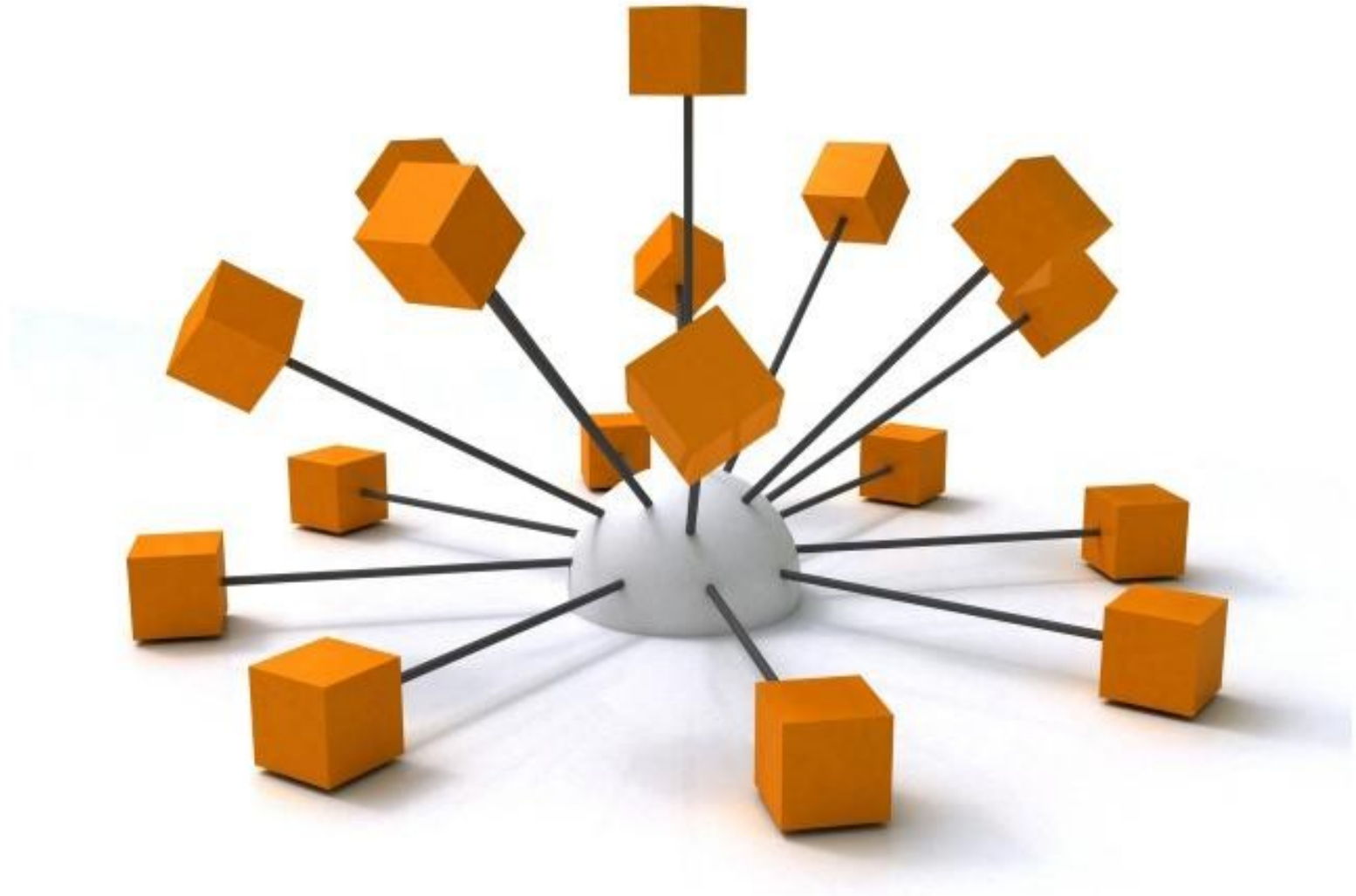
Modern Ciphernetic Ecosystems

Athanasios Kostopoulos 0x375 0x06 Nov '11



Introduction

What this presentation is about:

- Assumes little technical familiarity with the subject matter
- *Modern* (must be relevant and in-use).
- *Ciphernetic* (cryptography OR anonymity focused)
- *Ecosystems* (At least it's not “communities”(!) - just don't let RMS know about it)
- Distinct technical focus (this is not a political forum)
- Certain published attacks will be discussed

Darknet – an Academic Definition

ACM 2002 DRM Workshop

”We investigate the darknet – a collection of networks and technologies used to share digital content. The darknet is not a separate physical network but an application and protocol layer riding on existing Networks.”

Activist Definition

Tor: **”Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis”**

Freenet: ”Freenet is free software which lets you anonymously share files, browse and publish "freesites" (web sites accessible only through Freenet) and chat on forums, without fear of censorship.

Technical Definition I

What presented so far can be summed up as a security and privacy focused subset of *overlay networks* (usually the *unstructured* kind). But what is an overlay network ?

•Overlay networks are networks built on top of another existing network, the *underlay.* The underlay takes care of basic networking functions (primitive routing/forwarding).

• Overlay networking is a method of addressing certain shortcomings of the underlay infrastructure.

• The number of overlay (logical) hops might correspond to many underlay (physical) hops.

• Active research field, not only in security & privacy (think CDNs,VANets, etc.)

Technical Definition II

What are the essential properties of an overlay network ?

- **Support the execution of one or more distributed applications by providing infrastructure for them.**
- **Participate and support high-level routing and forwarding tasks (which usually are different than these of the underlay).**
- **Deploy across the underlay (usually the Internet) in such a way that third parties (that means YOU!) can participate in organization and operation of the overlay network.**

Reverse Sales Pitch

You really should NOT care if :

- **You do not value your privacy (Blame Canada!).**
- **You are not an activist (OWS, IR, EG etc.).**
- **You really enjoy being watched and monitored (FB, ISPs, every three letter agency out there!).**
- **You really enjoy the safety provided courtesy of your state sponsored firewall (Great Wall of China, Australia to follow ?).**
- **Cryptosystems do not tingle your fancy.**

Who knows what evil lurks within ?

General Surgeon's Warning : Within you might find the Four Horsemen of the Informational Apocalypse.

- **Atrocious Terrorists**
- **Fiendish Drug Dealers**
- **Unscrupulous Child Pornographers**
- **Blood-Curling Organized Criminals**

… and of course let 's not forget the usual suspects
- **'Wily Hackers'**
- **'Bloodthirsty Pirates'**

While you might encounter the aforementioned entities, are these limited to privacy oriented networks ?

This stuff is just for kids …

O RLY ? Have you ever heard of …

- **SWIFTNet (financial industry)**
- **SIPRNet (US DoD / US State Dept)**
- **Global Information Grid (US DoD)**
- **JWICKS (again US DoD)**
- **Loads more we do not know about (ask your friendly neighborhood DISA agent)**

The above are all examples of secure overlay networks.

Feel free to drop me a line if you have any additional information.

Common FOSS Implementations

Below is a partial list :

TOR (you must have heard of it by now).
Freenet (focused on storage).
I2P (personal preference).
GNUNet (added by popular demand ;)).

TOR : The Onion Router I

Perhaps the most famous and widely deployed anonymity network.

- **Available for Windows,OSX,GNU/Linux.**
- **Open Source (written in C).**
- **Based on the Onion Routing Concept.**
- **Focused on providing exit points towards the underlay (Internet in our case).**
  - **So cool, even Law Enforcement uses it !**
  - **Vulnerable to exit node sniffing (more on this later!)**
- **Hidden Services are available (.onion TLD) but this was not the design focus.**

What Routing ? Onion ?

Onion routing is a method of communicating anonymously using a public network.

- **“Patented” by US Navy in 1998**
- **Uses a multiple layer, onion-like analogy**
- **Basis for most privacy oriented routing protocols**
- **Centralized**
- **Source routed (static TOR circuit)**

How does it work

Very simple concept :

1) Sender determines path (circuit) to recipient quering one of many centralized resources.

2) Sender obtains all public keys for each intermediary.

3) Sender encrypts plaintext and per-intermediary routing information (myopic protocol) in each layer in reverse order.

4)Sender sends it to first intermediary, which “peels off” the layer and forwards to the next one.

Tor Hidden Services I

Hidden services are servers confined within the Tor darknet.

• The emphasis is on protecting the anonymity of the server, in addition to the client's.

•More complex process than contacting an exit node (you will see why).

•Given that Tor is somewhat centralized, this suffers from all DNS drawbacks, with a *vengeance* (how do you determine ownership within an pseudonymous network?)

Tor Hidden Services II

Assuming that an .onion has introduced itself to the ecosystem, here's the simplified version :

1)Client queries the directory server about .onion

2) DS redirects client to the *intro point* (negotiated during server joining phase)

3)Client finds a *rendezvous point* and establishes a pseudonym

4)The client forwards key exhange information and *rendezvous point* to the *intro point.*

***5)* Hidden Server established its own circuit with the *rendezvous point*, indicating client's pseudonym**

6)Key negotiation is finalized and service can now start.

(it can even get more indirect!)

FreeNet I

Freenet can be regarded as a *distributed, anonymous* data store.

- **Free Software (Windows/OSX/GNU/Linux).**
- **Significant Research Work Behind It.**
- **Storage Oriented, as opposed to Message oriented.**
- **Users contribute both bandwidth and encrypted storage space (plausible deniability).**
- **Content is kept on a popularity basis (unpopular content is deleted in order to make space for more popular content).**
- **Content published can survive long after the original publisher is gone.**
- **More decentralized that Tor.**

I2P Introduction

I2P is a more security focused implementation of the concepts described so far. Some key facts :

- **Started 2003, forked from Freenet.**
- **Still WiP (0.8.10) but quite usuable.**
- **FOSS software.**
- **Primarily written in Java (thank $DEITY for JIT).**
- **Focus is on operations within the I2P ecosystem.**
- **Packet switched, as opposed to “static” circuits.**
- **A somewhat “paranoid” overlay network.**
- **No centralized resources per-se (which can be good and bad).**

A picture is worth ...

Simplified I2P overlay :

Streaming	Datagrams
I2CP	
Garlic encryption	
Tunnel messages	
NTCP	SSU
TCP	UDP
IP	

Tunnels ? Why not another vegetable ?

I2P is based on unidirectionaly, short-lived tunnels.

- **2-parties required 4 tunnels (but how does it scale?).**
- **Tunnels are either client or exploratory.**
- ***Exploratory*: created constantly, tested within a defined set of parameters. Good ones are promoted to client tunnels.**
- ***Client* : Does what it says on the tin.**
- **Default lifetime is *10 minutes*. Might expire earlier if network degradation occurs.**
- **Tunnel hop length varies (the more you have the more safer you can be but the more delay you will get).**

I hate vampires ...

Garlic routing is an extension of onion routing.

- **Routing-wise, they are identical.**
- **Message-wise, a *garlic* can contain multiple messages.**
- ***Garlics* contain additional routing directives (a time delay element can be introduced to hinder timing attacks).**
- ***Garlics* travel through short-lived, unidirectional *tunnels.***

There is light at the end of ...

I2P uses cryptographically *unique* endpoints.

- **An endpoint is analogous to IPv4 Host:port tuple.**
- **An endpoint can be *mobile.***
- **A destination is composed of : 1024bit DSA for signing, 2048bit El-Gamal for encryption and assorted certificate information.**
- ***IMPOSSIBLE* to remember for average humans, thus using shortened mnemonics (think /etc/hosts on steroids), cryptographical uniqueness is lost.**

So far, so good …

So far, a quick tour of pseudonymous unstructured overlays has painted a rather positive image. Is this always the case ? Is security binary ?

To continue with the ecosystem analogy, in every ecosystem there are predators, sometimes migrating to different ecosystems altogether (thing French shrimps!)

This is *NOT* an exhaustive list of attacks.

Exit point sniffing

Not part of threat model but ...

- **Exit nodes sniff content exiting the darknet.**
- **Dan Egerstad a few years back got a slew of interesting data and made it to Slashdot.**
- **Moxie Marlinspike used SSLStrip in his Tor exit node (nice guy, eh?)**
- **Some guy, some place said *"The choice of using Tor equates having a choice between your ISP sniffing your traffic or having a random exit node sniffing your traffic"* - exaggeration but invalid ?**

Timing/Traffic Analysis

If an adversary controls a portion of the darknet, can correlate traffic between origin and destination and use it to determine who is talking with whom (a form of traffic analysis).

- **Impractical but still within the realm of possibility.**
- **Each time a static circuit is abnormally terminated, retransmission of the messages gives these attacks an increased chance.**
- **I2P contains the facilities to mitigate these attacks by introducing a delay element to each garlic, as well as by bundling multiple messages together.**

Multiverse attacks

Overlay nodes simultaneously exist on the underlay as well.

Irongeek correlated underlay data (e.g. Apache banners) with overlay node data and was able to deduce node identities.

A little common sense (and proper configuration) goes a long way.

Endpoint/Content Attacks

How can you be sure that the endpoint you are connected to is the proper one and not a mimicry ?

- **Tor is vulnerable to these attacks.**
- **Freenet is vulnerable to spamming attacks as well (Remember kids ! Consensus can be a bad thing!)**
- **I2P uses strong crypto but human mnemonics are NOT immune to it.**

Software overlay attacks

All overlay providers discussed so far are software itself.

- **Software contains vulnerabilities.**
- **Have you seen the recent Tor CVEs ?**
- **Are you sure your Darknet implementation has undergone extensive security review ?**
- **How about the underlying Operating System ?**

Application-layer attacks

Assume that the strong cryptography used is solid (which is the case for most adversaries). What do you attack ?

- **Client-side leaks (yes, they can propagate within the darknet, after all the overlay is just a specialized infrastructure provider).**
- **Malware attacks.**
- **Trojanized cryptographic providers (in tandem with malware).**

Forensic analysis

Again, the overlay providers are executed within the confines of the Operating System (host-wise) and the underlay (network-wise).

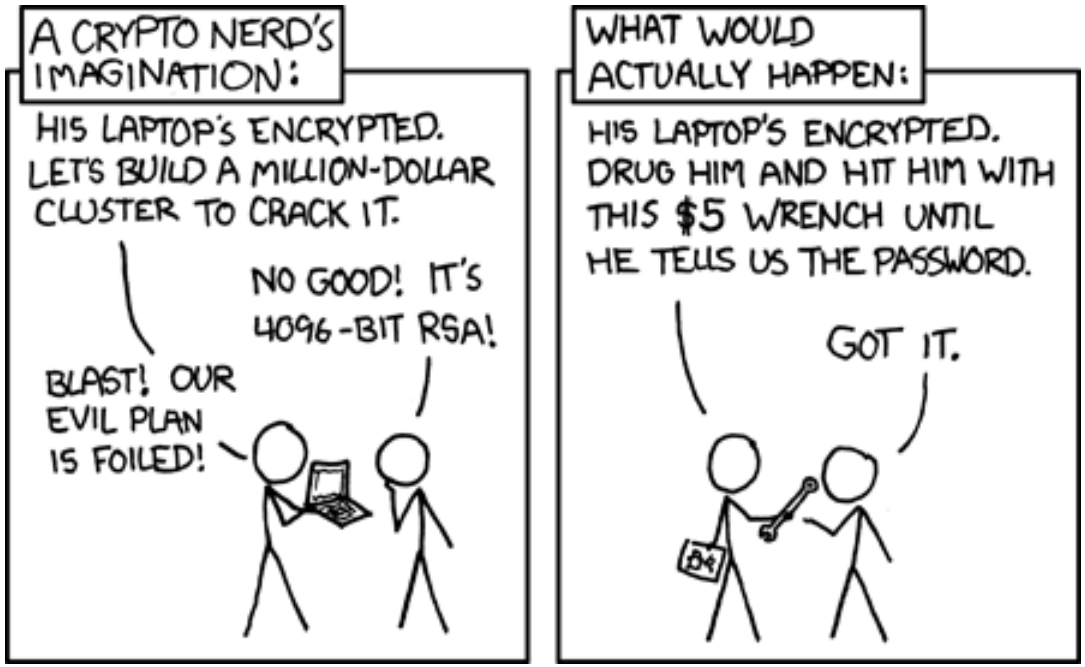
- **Encrypt early, encrypt often.**
- **Virtualization can be your friend.**
- **It's 11pm, do you know where your swap is ?**
- **Never trust a browser.**
- **Sometimes, just the simple fact that you are using a "darknet" is more than enough to put you in a world of hurt.**

Ask me after the presentation for some setup ideas.

The HUMINT factor

Even the best cryptography cannot protect you against social engineering. What was Fox Mulder's (weak!) password again ?

Also, let's not forget :



Your Darknet needs YOU !

Some ways *you* can contribute :

- **Raise awareness.**
- **Use it (and please share some bandwidth).**
- **Add content to it (lack of commercial interest).**
- **Good ol' financial support.**
- **Code something for it.**
- **Most of the solutions presented are FOSS so feel free to give a helping hand.**
- **Security Review (you can never have enough).**

Questions ?
Ideas ?

Thank you !

I can talk about this all day (and it's going to be a long day!).

Constructive feedback is more than welcome !

Drop me a line lixtetrax@grhack.net
Follow me at twitter

Shout outs :
argp, huku, fotisl, rest of GRHack
I2P team for their magnificent work
The crazy Swedes (you know who you are)