# Project Phoenix:
## *The Second Coming of the Internet – Now With Security*

v1.1_FOR LIMITED RELEASE
November 1, 2010

**By:**
**Ori Eisen**
**Founder and Chief Innovation Officer**
**41st Parameter**

*© 2010, 41st Parameter, Inc. The information contained in this document is strictly confidential.*
*Any distribution, reproduction or alterations without the prior written consent of 41st Parameter, Inc. is strictly prohibited.*

*The success of the Internet ultimately rests upon consumers trusting the Internet and its safety. Cybercrime erodes this trust, and if unchecked could destroy it. At this point, while various parties are proposing changes to the regulation, governance and oversight of the Internet, it's not clear that these will be sufficient. Therefore, suggestions to consider a second Internet – I2 – while radical, must be taken seriously. If it does turn out that the best solution is to 'hit the reset button' and create a second Internet, then we need to explore the ways in which such a construct should be created.*

**Michael Barrett**
Board of Directors,
National Cyber Security Alliance Board

# Contents

## Introduction

The Internet is not ours anymore…

At the time of writing this whitepaper, late 2010, we have been running Internet 1 for about fifteen years. While the TCP/IP protocol was invented years before, the commercially viable World Wide Web took off in the mid-nineties and online fraud followed soon afterward. In March 1996, the Internet Fraud Watch report was launched with approximately 100 incidents filed each month. Then, top complaints involved pyramid schemes, magazine subscriptions, and false prizes and sweepstakes. Today online fraud is systemic, industrialized around "commercial" platforms such as Zeus, and the worldwide losses incurred total in the hundreds of billions.

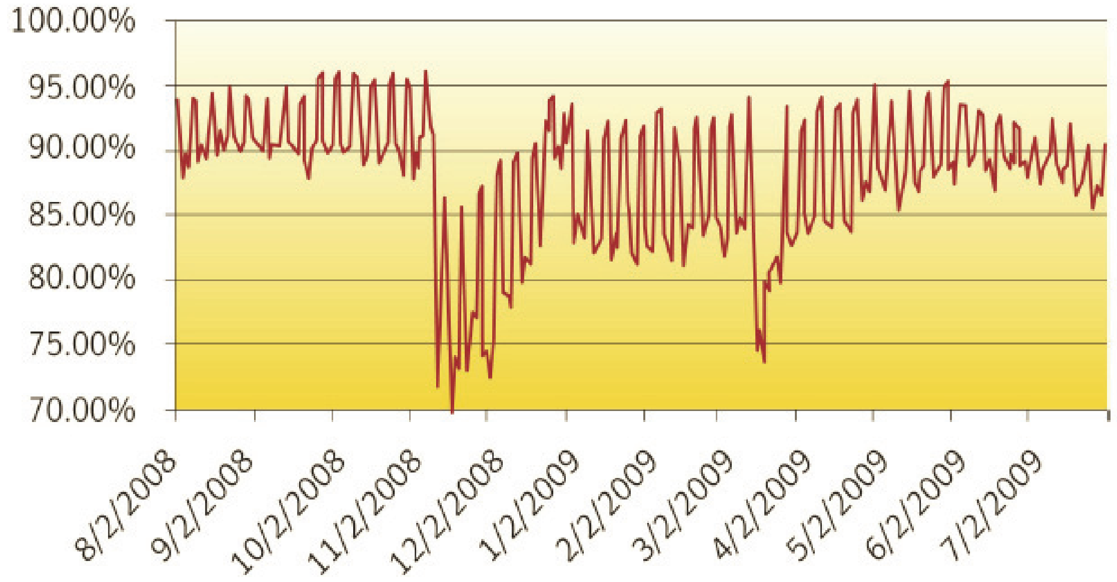
This paper is a call to action on the need for a new and parallel Internet, one that delivers the best commercially available transactional integrity. The justification is based on multiple complimentary factors that together signal the decay of Internet 1 ("I1"). I1's unsolvable security deficiencies stem from the lack of end-to-end management of:

1. Registration
2. Jurisdiction
3. Monitoring
4. Enforcement
5. Technology

### Where There is Value, There is Fraud – Always

Why do we need Project Phoenix? If you read the news, or you surf the Internet, or you have an email account – you should know why. The latest estimates from Symantec are that spam now represents close to 90% of all email traffic. The following chart says it all:

**Spam Levels:** *Malware Bearing Spam Can't Be Stopped*



*Source: Symantec*

The dramatic albeit temporary drop in spam in November 2008 was the result of law enforcement's takedown of the McColo data center in San Jose, California, the source of approximately 25% of all spam traffic.

Given that the spammers were able to quickly recover by re-hosting with different co-location providers strongly suggests that suppressing malware-carrying spam traffic is most likely a losing battle.

If one needs more reasons to know that the current Internet is serving the bad guys more than the good guys, consider the following: the LexisNexis True Cost of Fraud study reports that U.S. merchants alone are suffering in excess of $190 billion in fraud losses each year.

While these losses are alarming enough, the global loss number is much higher. More importantly, a significant percentage of the losses are well hidden in balance sheets in the form of bad debt, chargebacks, attrition, and loss of revenue opportunity as a result of consumer fear to transact or false-positives (rejected legitimate transactions), and so on…

Project Phoenix, the new and parallel Internet with transactional integrity, is becoming a necessity because the criminals' innovation outpaces the evolution of the market's defenses. We have passed the time when we can reassert total control over the existing online channel; I1 – the original Internet – will never be ours again. If the day comes when losses associated with I1 outweigh the benefits, there will be an emergency. Imagine a next generation bot attack that succeeds in inflicting financial losses so severe it impacts the EPS line of several financial institutions' income statements… in case of emergency, break glass.

A note to the reader: several early reviewers drew comparisons to the Secret Internet Protocol Router Network (SIPRNet).[1] If you are familiar with SIPRNet, then a good analogy would be that I2 is SIPRNet for civilians.

## Who Needs Project Phoenix?

For the purpose of this whitepaper, we refer to Project Phoenix, the successor generation of Internet as ("I2")[2].

Online merchants, financial institutions, airlines and other enterprises have all had to learn to deal with the security issues that are part-and-parcel of I1. Any bank with an online portal risks losses from the channel that is only as secure as the weakest link in the I1 chain.

Any online estate that is not concerned about security probably does not need I2. However, the definition of security is vague. For some, the assets requiring protection will never be monetary while for others, they are always monetary. For the purpose of this whitepaper, we define those who need security as Internet estates that move funds, cash equivalents, and highly sensitive data or intellectual property. These estates include, but are not limited to: retail banks, payment processors, brokerages, credit card issuers, online merchants, airlines, iPSPs, governments, the military, health care, higher education, insurance, social networks, law enforcement, central government banks. Exhaustive as it is, this list is far from complete.

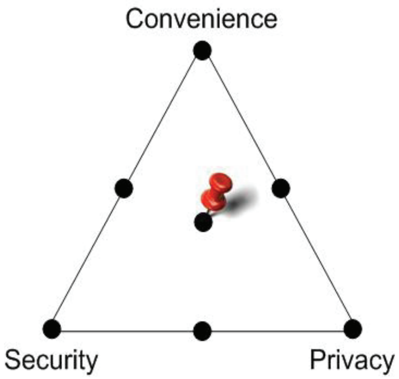
## What is the Tradeoff?

Convenience, security, and privacy are at odds. We can make a system very convenient, but it will not be secure. We can make it very secure, but it will not be convenient. And when we make it secure, regardless of convenience, it will deprive us of absolute privacy.

When you login to your bank you want them to know it is you, and only allow you to move money. How can your bank confirm your identity, without breaking the online anonymity barrier? If you want to keep your privacy, login anonymously, but for the bank to confirm it is you – something must give.

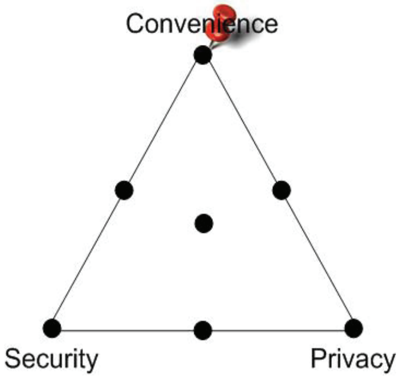
[1] *Source: http://rf-web.tamu.edu/security/Security%20Guide/S1class/Siprnet.htm*

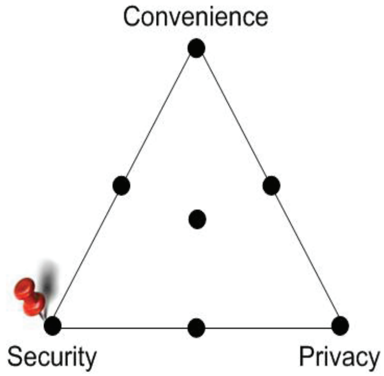
[2] *I2 in this whitepaper is not referring to Internet2, which is an academia project for new routing protocols.*



In a perfect world, convenience, security, and privacy would be balanced to achieve an acceptable level of performance in all three areas, but in a perfect world there is no crime.

I1 was driven towards convenience, as the ".com" meant "commercial" and it needed to be convenient and "fun" to stimulate mass adoption.





I2 must be driven towards security first and foremost, with privacy and convenience as a secondary priority.

### Why Can't We Patch-Up I1?

We can…we did…we are…we will. However, at the core of the Internet protocol, inside the TCP/IP stack, security was never a requirement…. Or was it?

Speaking with Vinton Cerf, the "Father Of The Internet", it became apparent that security took a back seat to getting the nascent system to work at all:

> *Classified projects were undertaken early in the Internet's design and implemented by appropriate organizations, but because the designs incorporated technology which was then classified, they could not be released for use by the general Internet community. Since that time, the widespread adoption of the Internet and the development of publicly available security technologies has set the stage for renewed efforts to refine the existing implementations of the Internet including consideration of significant departures from the present design to potential new ones.*

**Vinton Cerf, PhD**
Co-Designer of the TCP/IP Protocols and the Architecture of the Internet

The issues we face begin in the real world, where fake identification documents and certified copies of birth certificates are for sale to anyone willing to pay. This is a problem beyond the scope of I2; nonetheless, we can make I2 as secure as the diplomatic passport and visa scheme.

On I1, anyone can impersonate you and create new synthetic identities. It is a fact, and any solution needs to take that into account.

We are constantly wrapping I1 with more layers, more fraud prevention, IDS, firewalls, anti-malware, anti-virus solutions – only to fall victim to the next vulnerability. For I2 to be secure and have integrity, we need to register users in the physical world first and only then allow them to become digital citizens, or *Netizens of I2*.

> *A secure Internet in today's environment is merely an illusion. The bad guys always find a way into your network, systems, and personal information. Once they're in, it's extremely difficult to get them out. Today's security solutions aren't effective to counter the current threat landscape. As programming languages evolved, we're still deploying SSL and firewall solutions to protect our business. It's time to think out of the box and build a secure network like I2 that can put trust back into doing business over the Internet.*
>
> **Kevin Mitnick,**
> Information Security Consultant

## The I2 Business Model

While all countries are traversed using roads built by the government, in many places there are also toll roads. Why would anyone pay to use a toll road if there is a free motorway? The assumption is that toll roads are "better" – less congested, fewer accidents, cleaner, better maintained – and it is the driver's discretion to use them. The same case should be made for I2.

I1, the current Internet, will stay as is, likely forever. However, those who need security in their business will be willing to pay to ride I2's secure rails. The same thing happened in the Wild West when people began hiring a secure stagecoach to move their money.

Especially with the current court cases[3] questioning banks' liability when transactions go wrong, it is only a matter of time before I1 will carry an unprofitable level of risk.

Thus, when I2 becomes a viable option, a bank can tell its customers:

> *"If you want to transact on the World Wide Web (I1) and enjoy its convenience, you will not be able to repudiate the transaction. However, to secure the transaction, guarantee the funds and enjoy zero-liability, you need to use I2."*

Granted, given the low losses provided by the well-funded and well-maintained I2, a bank would be willing to pay the "toll" for this private toll road - at least for high risk transactions.

## Funding, Launching and Maintaining I2

To build I2 into a steady state that includes maintenance will require a substantial investment. The venture capital community, financial institutions, and governments are likely candidates for parties willing to invest in I2 to secure their business processes, create a business advantage and potentially participate in the financial returns generated.

To get I2 launched will require a fraction of the total investment, and it could be built in a matter of a few years.

[3] *See Lopez v Bank of America in References for additional information.*

## The Five Tenets of I2

The following five tenets must be observed if I2 is to be both secure and commercially viable:

1. Registration
2. Jurisdiction
3. Monitoring
4. Enforcement
5. Technology

### *Registration*

One of the reasons I1 is so broken is because it is so open. There is little to no validation upon login to the network or opening an account with a company within the network (email, bank, social network etc.) Anyone can pretend to be anyone else. Because I1 is driven by convenience instead of security, there is reluctance among competitors to be the first to make any process less convenient. Even when clear security measures are available, companies still prioritize market share, industry performance metrics and/or customer satisfaction over security decisions. If a consumer can get the same utility with less effort from your competitor, the path of least resistance will prevail.

I2 should be driven by security first, and everything else second. Thus, the registration process must be as ironclad as possible. We all know that to travel cross-border, we need a passport. We all know how to go about getting a passport - the fees and processes involved. By following the same principles for I2, we will require in-person registration.

If I2 will require brand new infrastructure to register users, it will take decades to fund and build. Thus, to economically optimize for security and mass adoption, I2 registration must mimic the diplomatic visa or passport issuance process. An early example might be the Postal Bank operated by Israel Post. The IPOST service debuted as an online payment site for bill payment, but a later phase will "provide every citizen of Israel with a unique, secure email box through which they will be able to receive and send communications from and to all government offices and agencies.

If we think the diplomatic visa or passport process is as broken as I1, we should not embark on I2. Otherwise, we should agree the I2 registration process will be orders of magnitude more secure.

### *Jurisdiction*

The Internet has always been available to any citizen of any nation. However, I1 has no jurisdiction and no real power when it comes to enforcement of rules of conduct -- I2 will be different.
Any nation or organization wanting to participate in I2 will need to sign a Commercial Agreement specifying the terms and conditions under which it will be granted access privileges. All transactions on I2 will be subject to its jurisdiction; controlled by an I2 governing body structured much like other consortia efforts.

In the case that an organization wants to gain direct access to I2 in advance or independent of its host nation, it can. However, this means that this organization will lose its membership should it exceed the abuse thresholds set by I2 bylaws.

## *Monitoring*

There are reports that monitor abuse by a country on I1. However, there is little to no recourse for curtailing abuse.

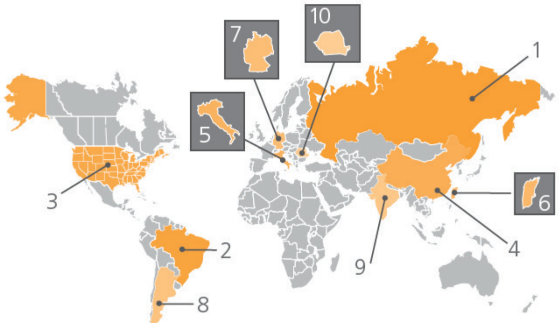


*Figure 1: Attack Traffic, Top Originating Countries*

|  | Country | % Traffic | Q2 09% |
|---|---|---|---|
| 1 | Russia | 13% | 1.2% |
| 2 | Brazil | 8.6% | 2.3% |
| 3 | United States | 6.9% | 15% |
| 4 | China | 6.5% | 31% |
| 5 | Italy | 5.4% | 1.2% |
| 6 | Taiwan | 5.1% | 2.3% |
| 7 | Germany | 4.8% | 1.9% |
| 8 | Argentina | 3.6% | 0.8% |
| 9 | India | 3.4% | 0.9% |
| 10 | Romania | 3.2% | 0.6% |
| – | Other | 39% | 31% |

*Source: Akamai, State of the Internet, Third Quarter 2009*

I2's governing body will monitor attack traffic from each originating country or organization against an acceptable abuse threshold. This process should mirror the card schemes such as Visa, Mastercard, American Express and Discover which monitor merchants and processors to keep abuse in check.

For example, in I2, should a country or organization exceed the abuse threshold, the Agreement will mandate actions to be taken to address the rogue activity. This may include, but is not limited to, extradition of the culprits and/or prosecution within the country where the attack originated. I2 members will be disconnected should they exceed the established abuse threshold, violate Agreement terms, or be voted off the system for cause. I2 is a private network and membership should not be assumed - it is a privilege, not a right.

No system functions flawlessly on its own, so I2 must be proactively monitored. Monitoring all stages of I2's users' lifecycle will be critical for its security and stability. The users' lifecycle business processes to be monitored include: registrations, logins, account takeovers and and transactions, relevant to I2 DNS and/or businesses utilizing I2.

Once a user receives credentials for I2, they will need to login to the network for the first time. I2's authentication will then bind the I2 account to its user and device(s).

Since the charter of I2 includes continuous reporting, monitoring and enforcement of its network, "pipe-cleaning" will occur as a natural byproduct of operation, ensuring minimum abuse.

The monitoring will be done ala NORAD -- a center for monitoring and intelligence will operate the network and oversee security 24 x 7. For incident response and management, there will be a NOC (Network Operations Center) and a SOC (Security Operations Center) and a ROC (Risk Operations Center).

*Source: NORAD*

Because I2 has an emphasis on abuse detection, risk-management and fraud control, a risk operations center must also be established. While the NOC is responsible for network stability, availability and performance, and the SOC is responsible for intrusion detection and prevention, the ROC is responsible for integrity of I2 members from the first login onwards. Monitoring business processes from the perspective of member institutions, the ROC will monitor I2 logins to the network itself, protecting by proxy all estates inside 12. Over time, a logical extension to monitoring I2 network logins might be to leverage the embedded security of I2 to also monitor member transactions such as account opening or account takeover.

This perfect triad of NOC, SOC, and ROC will be joined at the hip, complete each other, and act in unison to protect I2.

| NOC Responsibilities | SOC Responsibilities | ROC Responsibilities |
|---|---|---|
| Firewalls | IDS | Risk and Correlation Engines |
| DNSSEC | SEM | Link Analysis |
| Provisioning | Authentication | Statistical Distributions |
|  | SSL / TLS | Risk-based Authentication |
|  | Remediation | Forensic Investigations |
|  |  | Anomaly Detection |

## *Enforcement*

Monitoring is pointless without follow-up, management and ultimately enforcement.

I1 is a free-for-all system where there are repercussions only once you inflict a very high threshold of pain on the system. This fosters a network in which criminals operate freely, knowing the chances of prosecution and punishment are miniscule.

Frank Abagnale, one of the world's most respected authorities on the subjects of forgery, embezzlement and secure documents, describes the conviction rate of white-collar crimes as such:

> *All these crimes are about risk and reward. Criminals look at identity theft and say only 1 in 700 criminals gets convicted. And they look at check forgery and know that for every 1,400 forgers arrested, only about 123 are convicted and about 26 go to jail. So the rewards are great and the risks are very slim, and that's just one of the reasons it is very popular.*
>
> **Frank Abagnale,**
> Author, "Catch Me if You Can" and
> Secure Document Consultant

I2 will be a private network with a zero-abuse policy. I2 members must adhere to the I2 SLA and respond quickly to requests for investigation and/or immediate shutdown of offending accounts or nodes. By design, this will prevent some entities from even applying for I2 membership. Some may not have diplomatic relationships with the developed world or have no desire to adhere to the strict enforcement policy. While disconnection is a last resort – it will be exercised, keeping abuse to a minimum.

I2 will be globally distributed. Therefore, we should expect that someone from a non-I2 country or organization may attempt to infiltrate I2. The I2 member responsible for the breach will bear the responsibility for investigation and mitigation of the breach.

### *Technology*

This is going to be the most challenging aspect, and is saved for last for a reason. Most technologists reading this far are no doubt curious to read about the new technology I2 will require. Note: Now is a good time to take an arrow out of your quiver, and take aim…

Most of what's new is actually…*old*.

Appendix A could serve as the strawman RFC document for exploratory discussions around the development of I2. Another topic to be decided is which organizations and individuals would be invited to participate and why. The best way to describe it is "back to basics" without cutting any security corners this time around. This includes overt and covert risk monitoring throughout I2.

There will be many ideas on how to actually achieve this. The purpose of this whitepaper is to identify what needs to be done and present high-level concepts versus specific solutions. As technology evolves so will I2, yet, the intent must be kept intact.

A user-flow in I2 can be summarized in the following 7 steps and is depicted in the diagram below.

1. Install the I2 Client Software (may be optional over time)
2. Login to I2 using three factors of authentication
3. Encryption of keystrokes between the keyboard, OS and I2 Client Software
4. Receive fresh, per-session malware and virus-free I2 VM
5. I2 VM will have dynamic visual cues to assure users they are in the I2 Domain
6. I2-Compliant Browser in the I2 VM will serve I2-compliant sites
7. Generation and issuance of I2 session receipt

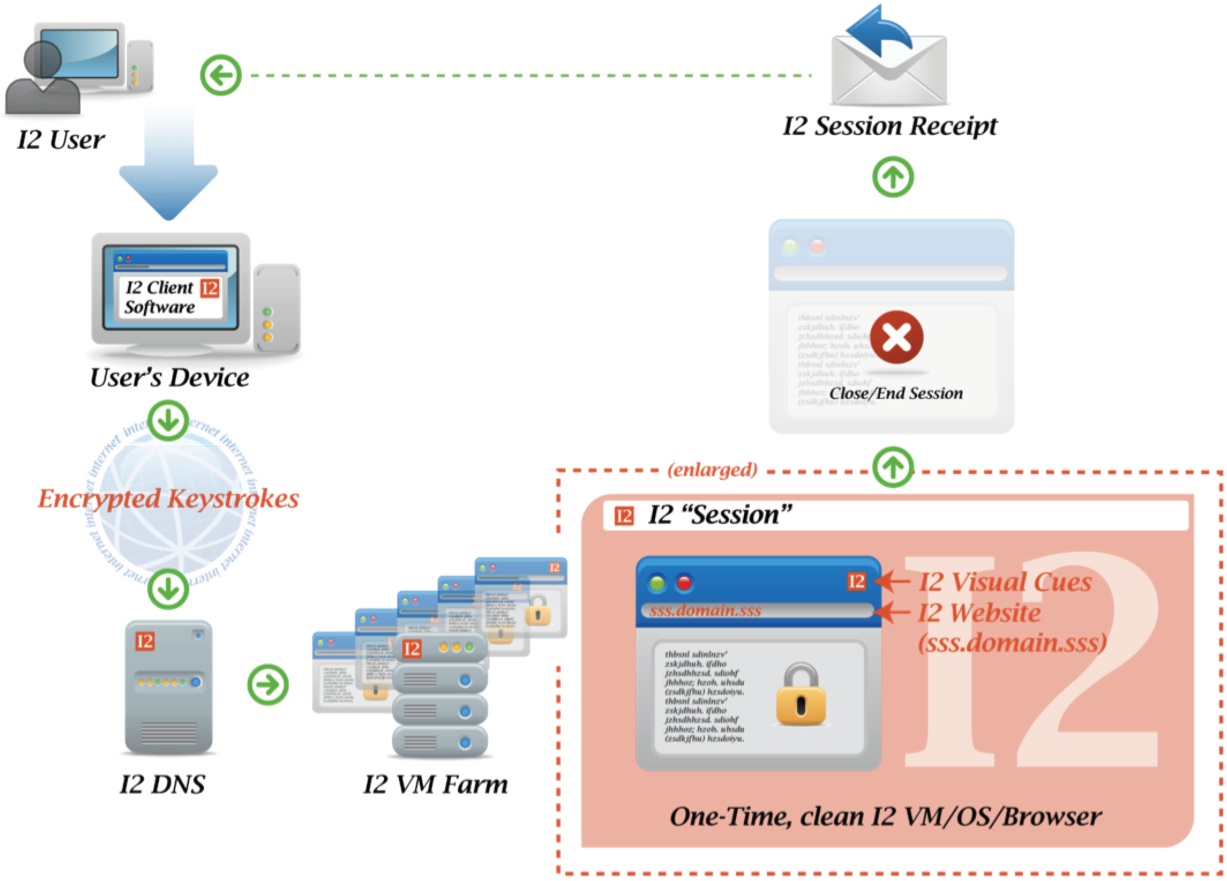


**Figure 1 – I2 Topology**

| | |
|---|---|
| **Users Device(s)** | Any device or computer: PC, MAC, Mobile, Game Console, Tablet, iPod, iPad etc… |
| **I2 Client Software** | Distributed during in-person registration or delivered via courier to a verified address |
| **I2 DNS** | The primary I2 DNS servers pointing a user to an I2 VM Farm, which provide the one-time VMs |
| **I2 VM Farm** | A cluster of I2 servers that provide one-time VMs for I2 users |
| **I2 Session** | A session conducted on an I2 VM which lasts until the user logs out |
| **I2 Website** | A website available only to an I2 server farm. It has a beginning and end domain extensions that cannot be misconstrued to be an I1 website, e.g., sss://sss.domain.sss |
| **I2 Dynamic Visual Cues** | I2 websites will have dynamic visual cues to let users know they are in a safe zone |
| **I2 Session Receipt** | After each I2 session a user will get an I2 session receipt |

## Summary

In order to address security and policy on all fronts, the I2 solution will have the following features:

### Registration

- Credentials will be tied to a user and a physical and verifiable street address.
- An in-person process, similar to the issuance of a passport or opening of a new bank account.

### Jurisdiction

- Any organization seeking I2 membership will sign the Commercial Agreement containing terms and conditions.
- The Agreement will cover the allowable abuse threshold in order to maintain membership.
- The Agreement will cover the process of disconnection from and reinstatement to the I2 network.
- The I2 domain will have jurisdiction, so prosecution of criminal activities on I2 will become viable for business, law enforcement and the I2 governing body.

### Monitoring

*A triad of centers will monitor I2:*

- NOC – Network Operations Center
- SOC – Security Operations Center
- ROC – Risk Operations Center

### Enforcement

- I2's governing body will be able to enforce the laws within its jurisdiction and disconnect and prosecute offending parties.

### Technology

- Client Software that Emulates a Dumb Terminal
- Three Factors of Authentication
- Encrypted and Time-Encoded Keystrokes
- One-time I2 VMs and One-time OS
- I2-Compliant Browser
- Dynamic Visual Cues
- I2 Session Receipt

***Please see Appendix A for Technology section, including I2 Solutions and Components Flow.***

# Appendix A – Technology

## *I2 Solution and Components Flow*

This section expands on the seven essential elements underpinning I2 that were highlighted under Technology in the main body of this paper.

### Client Software that Emulates a Dumb Terminal

I2 Client Software will be distributed in-person during registration or delivered via courier to a verified address. The software will point the device to a secure I2 DNS, and secure the keystrokes all the way from the keyboard, to the OS to I2.

The main structural changes will ensure that I2's core remains secure, while "dumbing-down" the end nodes. To do this we bring back the notion of keyboards that only send instructions to a server (aka dumb terminals, such as the VT-100 and IBM 3270). This will concentrate the security problem at the server, allowing security efforts to focus on the core system.

This is not proposing to replace current physical keyboards, rather to enhance the software design so malware will not be able to intercept, mimic or tamper with the instructions.

SSL/TLS protocol does a good job encrypting text in transit. The latest malware such as Zeus captures keystrokes even before SSL/TLS encryption. The I2 Client Software will encrypt keystrokes so only an I2 server can decrypt them. Thus, we have essentially "dumbed-down" the client-side of the equation. The intent is for the physical keyboard to remain the same and for the OS to send the keys to the I2 Client Software, and for the I2 Client Software to encrypt it before transmitting onwards.

Furthermore, the encryption will employ a tamper-evident feature, to prevent keystroke replay. By encrypting the traffic, even if intercepted it will be useless to an attacker.

If the I2 Client Software cannot provide this functionality, another solution must be devised.

### Three Factors of Authentication...No Less

In 2005, the FFIEC (Federal Financial Institutions Examination Council) issued guidance for financial institutions regarding two-factor authentication.

The gist of the guidance is:

> *"Multifactor authentication utilizes two or more factors to verify customer identity. Authentication methodologies based upon multiple factors can be more difficult to compromise and should be considered for high-risk situations."*

### *What are the Factors of Authentication?*

In 2005, the FFIEC (Federal Financial Institutions Examination Council) issued guidance for financial institutions regarding two-factor authentication.

- *Something a person knows*—commonly a password or PIN. If the user types in the correct password or PIN, access is granted.

- *Something a person has*—most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.

- *Something a person is*—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.

### *Three Factor Authentication is NOT Three Elements of the Same Factor*

The most common misinterpretation of the FFIEC guidance remains that adding "more elements" of one of the factors (i.e. knowledge-based authentication in addition to password) qualifies as meeting the guidelines. This led to solutions that only added another element to the authentication scheme versus actually adding another factor.

In I2, we must use ALL THREE factors during authentication and NOT utilize additional elements within the same factor.

Multiple vendors and solutions will be certified for I2 and a user can chose between them.

## *Encryption*

I2 will need encryption one step beyond SSL/TLS. Not only is encryption needed between a node and a host, it must also be added from the keyboard through the OS and the I2 Client Software.

Messages between the "dumb terminal" and the I2 host will be first encrypted by the I2 Client and the OS, and then encrypted again by SSL/TLS for transmission. Assuming all keystrokes will be generated inside this framework, the risk of keyloggers and Man-In-The-Middle attacks is greatly diminished.

While there are different alternatives to avoid keyloggers, such as dynamic visual keyboards used with a pointing device, the risk of video capture remains. However, video capture will not pose a threat, as it will not help decrypt the I2 Client Software. We should recognize that keylogging has been a major contributor to the insecurity of I1, and has yet to be completely addressed.

Lastly, on the topic of credential-sniffing and replay attacks, there are some safeguards to be added. One can argue that as long as the malware can observe the encrypted keystrokes, all the criminals need to do is replay it to gain access. In this example, the criminals don't know what the password is, as it is encrypted; yet they still have the necessary credential… or do they?

In risk management and fraud detection we need to know if a message is authentic regardless of its content. Thus, if we add the timestamp, down to the millisecond, to each keystroke, it will make them tamper-evident. In other words, even if malware was to capture the time-encoded and encrypted keystrokes, they will not be valid on the I2 system ever again.

Further, observing this transmission again will alert the ROC to a potential breach triggering the appropriate actions to be taken.

### One-Time I2 VMs and One-Time I2 OS

In the Washington Post's blog, "Security Fix", Brian Krebs raised the idea of booting a device from a "Live CD" with a clean copy of a Linux OS.

> *Their conclusion? While there are multiple layers that [sic] of protection that businesses and banks could put in place, the cheapest and most foolproof solution is to use a read-only, bootable operating system, such as Knoppix, or Ubuntu.*
>
> **Brian Krebs,**
> "Security Fix Blog"
> *Washington Post*

Taking the idea one step further will allow I2 users to connect to a virtual machine with a clean OS and therefore malware and virus-free. After the session ends, this VM will be obliterated; preventing any malware that may have been placed on it from harming either the user's computer or I2.

Furthermore, each time a user logs into I2, a fresh, clean copy of the VM will be instantiated. This will allow any security vulnerabilities to be fixed in one place, without requiring millions of updates – enabling for the first time centralized continuous remediation.

With the combination of a dumb terminal and a clean copy of the OS, I2 will perpetually maintain its pristine condition for each new session. The security of I2 will no longer depend on users purchasing AV and malware solutions, paying and renewing subscriptions, or downloading and installing the latest updates. Anti-malware protection must be distributed via a centralized perpetual remediation operation in conjunction with the NOC.

Optionally, the software distributed to I2 users could reside either on a USB memory stick or a CD to ensure a clean connection to I2's fresh instance. It is important to remember that not all users will be able to use a USB memory stick or a CD, thus I2 will not be reliant on it.

By using the I2 Client Software to send encrypted messages over SSL/TLS to a clean I2 VM, which then connects to the I2 network – we get closer to maximum security online.

### *I2-Compliant Browsers*

I2 Client Software on your computer leads you to the clean I2 VM, which has an I2-Complaint browser. The main requirement of the I2-Compliant browser is to block the copying of I2 websites, thus helping curb mimicry as the precursor to online crime. The intent is to optimize for security first and foremost.

Without the website source code, it will be far more difficult to create a phishing site within or outside I2. The source code will only remain on I2.

I2-Compliant browsers can be provided by the main browser publishers. Certain functionality common to current browsers will be disabled, including Save As, View Source and other functions that enable copying and saving I2 websites. This can be achieved by disabling (greying-out) functions from the mainstream GA versions. Thus, any browser could potentially be I2-Compliant as long as it meets the requirements. In order to be certified as an I2-Compliant browser, the browser's source code may be subject to review by the I2 governing body.

### *Dynamic Visual Cues*

Through dynamic visual cues, users will have a high level of certainty that they have arrived at I2.

Today, a criminal can mimic any I1 website by copying the source code and placing it elsewhere. Thus, I2 needs to prevent this and provide users dynamic visual cues confirming they are in a safe zone using I2-Compliant browsers and websites.

Furthermore, while this will not completely solve the problem, the high-level concept is to generate a dynamic visual cue, bound to an I2 VM session plus the user and the current time, so it cannot easily be mass-replicated.

We should adopt methods used to curb counterfeit paper printing, such as elaborate designs and add a dynamic element, which changes per user-session and incorporates the current time.

### *I2 Session Receipt*

A session receipt will be sent to the user after each session concludes. The session receipt will confirm usage and also serve as an alert to unauthorized uses. One option is for an out-of-band notification and another would be to show activity in I2 at the next login. The session receipt will have at a minimum the account number (partially masked), session number (partially masked), date and time of login, logout and session duration.

Additionally, users could opt-in to limit the day, time, device, IP Address or MAC Address that can access their I2 account.

> *“In 1999, very few thought that the threat of viruses could keep pace with the growth of the Internet, and almost nobody had heard about what is today commonly known as phishing. A few years later, both of these threats emerged and evolved, as organized crime understood their potential and poured in. We have fought a fierce and often losing battle ever since. What is worse, the threat to mobile computing is now what the Internet threat was in 1999 and with the limitations of battery power and I/O capabilities on handsets, we may not be able to keep up as well against on this front. The mounting threat is what has caused experts to endorse a new Internet, designed with security in focus. This is what is referred to as I2.”*
>
> **Markus Jakobsson**
> Principal Scientist at Palo Alto Research Center

## References

- ***March 18, 2010. DarkReading:*** *http://darkreading.com/security/attacks/showArticle.jhtml?articleID=224000047*
- ***March 19, 2010. IDG News Service:*** *http://www.computerworld.com/s/article/9173778/To_fight_scammers_Russia_cracks_down_on_.ru_domain*
- ***March 22, 2010. The Register***: *http://www.theregister.co.uk/2010/03/22/microsoft_live_captcha_bypass/*
- ***How Frank Abagnale Would Swindle You***: *http://www.usnews.com/money/blogs/the-collar/2008/05/19/how-frank-abagnale-would-swindle-you*
- ***Transport Layer Security***: *http://en.wikipedia.org/wiki/Transport_Layer_Security*
- ***Avoid Windows Malware: Bank on a Live CD***: *http://voices.washingtonpost.com/securityfix/2009/10/avoid_windows_malware_bank_on.html*
- ***Lopez v. Bank of America***: *http://www.americanbanker.com/usb_issues/115_4/-246231-1.html*
- ***Authentication*** : *http://en.wikipedia.org/wiki/Authentication*
- ***Ubuntu***: *http://blogs.computerworld.com/15815/can_ubuntu_save_online_banking*