I2: THE SECOND COMING OF THE INTERNET. NOW WITH SECURITY.

BY ORI EISEN
FOUNDER, 41ST PARAMETER, A PART OF EXPERIAN

2nd EDITION. ORIGINAL PRINT DATE OCTOBER 2010

OVER THE PAST **18 MONTHS** DETAILS ON OVER **2 BILLION** CONSUMER ACCOUNTS HAVE BEEN COMPROMISED OR **STOLEN**

"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

INTRODUCTION

The Internet is not ours anymore…

At the time of writing this whitepaper, late 2010, we had been running Internet 1.0 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. According to PrivacyRights.org more than three billion records have been breached since 2005 and over two billion in 2014 alone. Today online fraud is systemic and built around "commercial" malware platforms such as Zeus. The worldwide losses incurred total in the hundreds of billions.

This paper is a call to action for a new and parallel Internet, one that delivers the promise of true security and authentication. The justification for this need is based on multiple complimentary factors that together signal the decay of Internet 1.0 ("I1"). ƒ I1's unsolvable security deficiencies stem from the lack of:

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

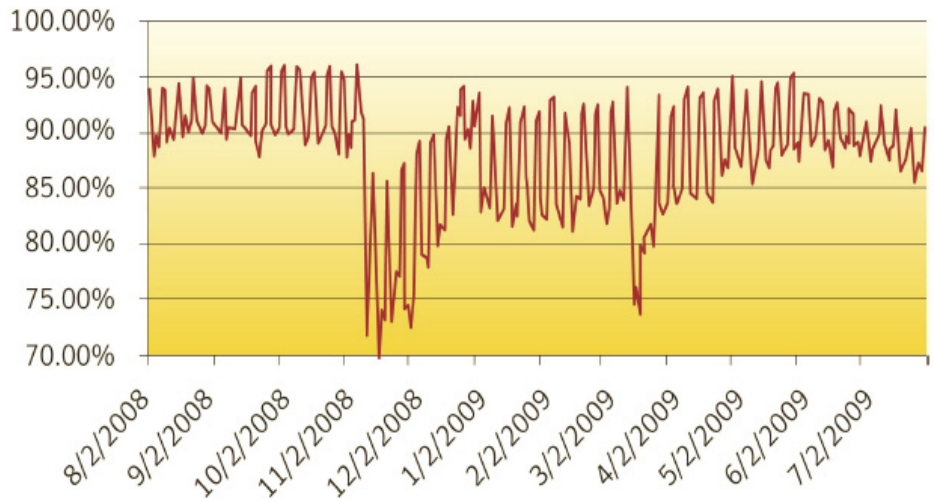
"A secure Internet in today's environment is merely an illusion. The bad guys always find a way into your network, systems, and personal information. Once they're in, it's extremely difficult to get them out. Today's security solutions aren't effective to counter the current threat landscape. As programming 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,
World's Most Famous Hacker

Where There is Value, There is Fraud – Always

Why do we need I2? 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



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 spam traffic is 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 LexisNexis True Cost of Fraud study which reports that U.S. merchants alone are suffering in excess of $190 billion in fraud losses each year.

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

I2, a new and parallel Internet with the promise of true security and authentication, is becoming a necessity because the criminals' innovation outpaces the evolution of the market's defenses. We are passed the point of reasserting total control over the existing Internet. 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 – and in case of emergency, break glass…

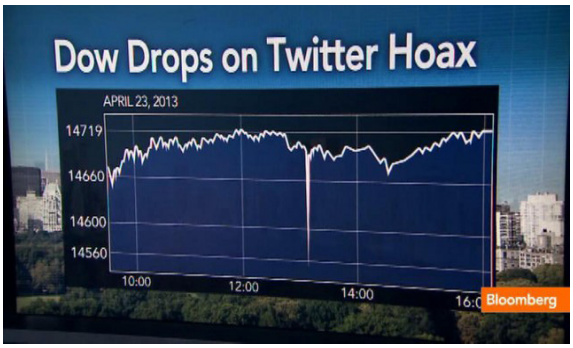
I predict an event that will be dubbed "E911" which will be the watershed moment that will make I2 seem obvious. Until then, we will continue to incur trust and financial losses as a "cost of doing business." This paper will make more sense after "E911" happens.

Who Needs I2?

Online merchants, financial institutions, airlines, governments, critical infrastructure, social media accounts of high influence (White House, AP, NYT, WSJ, Cent Com) who deal with the insecurity of I1.

Online estates that are not concerned about security probably do not need I2. However, the definition of security is vague. For some, the assets requiring protection are not monetary, while for others they are always monetary. For the purpose of this whitepaper, the definition of those who need security is Internet estates that move funds, cash equivalents, and highly sensitive data and intellectual property. These estates include, but are not limited to: banks, payment processors, brokerage-dealers, credit card issuers, online merchants, airlines, iPSPs, governments, military, health care, higher education, insurance, social networks, law enforcement, central government banks. Exhaustive as it is, this list is far from complete.

When the AP Twitter account was hacked and one tweet was sent: What do you think happened to the stock market?

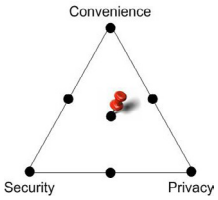


The hacker who posted this tweet could easily have short sold their stock and profited from the insecurity if I1.

What is the Trade-off?

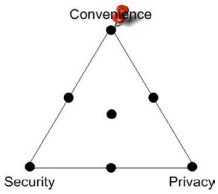
Convenience, security, and privacy are at odds. We can make a system very convenient, it will not be secure.

We can make it very secure, yet, it will not be convenient.



And when we make it secure, regardless of convenience, it will deprive us of absolute privacy.

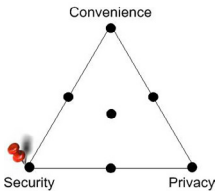
When you login to your bank you want them to know it is you, and only allow you to move money. How can your bank confirm your identity, without breaking the online anonymity barrier? If you want to keep your privacy (login anonymously) and you want the bank to confirm it is you – something must give.



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

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

I2 must start with security first and foremost, with privacy and convenience as secondary priorities.



Why Can't We Patch Up I1?

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

After speaking with Vinton Cerf, the "Father Of The Internet", it became apparent that security took a backseat 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 begins 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 obtaining a genuine government-issued ID such as a passport.

On I1, anyone can impersonate you and create new synthetic identities. It is our new reality, and any solution needs to take that into account. To quote Kevin Mitnick, former hacker turned security expert: "The milk is already spilled and the data is out there."

In fact, when I went to search for Kevin Mitnick's Facebook page, I was greeted with more than 20 profiles claiming to be him, having his picture and personal information – how do you know which is the real Kevin Mitnick? How do you know if any of the profiles are his?

We are constantly wrapping I1 with more security layers, more fraud prevention layers, 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.

The I2 Business Model

All countries use roads built by the government, and in many places there are also toll roads. Why would anyone pay to use a toll road if there is a free road? The assumption is that toll roads are "better" – less congested, cleaner, have fewer accidents, and are better maintained. It is the driver's discretion to use them and they are not mandatory. 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. Companies like American Express and Wells Fargo started this very way. Folks had a choice to move their own goods and money through the Wild West, or pay for someone who specialized in doing so and guaranteed the delivery. Today's World Wide Web is yesterday's Wild, Wild West…

Especially with the current court cases 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 and not use the free motorway - at least for high risk / high value 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. It will secure their current business processes, create a business advantage and potentially share the value 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. The good news is that many technologies from I1 can be salvaged, and we don't need to start from "scratch." One way to imagine I2 is a VPN (Virtual Private Network) on top of I1, which serves as a private club. This VPN will use the best security available and be a proxy for I1. Thus, if you are trying to login to your bank on I1, a request can be made to I2 to authenticate you. After you pass the rigorous process, a message back to the bank will authenticate that it is you on the other end with 99.999% certainty. 100% certainty is never attainable as you could be forced to login under duress.

THE FIVE TENANTS 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

In-Person 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 (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 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 passport process is as broken as I1, we should not embark on I2. Otherwise, we should agree the I2 registration process would be orders of magnitude more secure than we have today.

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 organization.

Any person or organization can gain access to I2, yet may lose its membership should it exceed the abuse thresholds set by I2 bylaws.

Monitoring

Today, there are reports that monitor abuse by country. However, there is little-to-no recourse for curtailing abuse.

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 fraud and abuse levels in check.

Should a user exceed the abuse threshold, their membership agreement will be revoked. I2 users will be disconnected should they exceed the established abuse threshold, violate their membership 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 monitoring will include: registrations, logins, account takeovers and transactions.

Once a user registers in-person they will receive 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, device/s and physical token.

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%

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) a SOC (Security Operations Center) and a ROC (Risk Operations Center.)

What is a ROC?

Because I2 has an emphasis on abuse detection, risk-management and fraud control, a Risk Operations Center (ROC) must 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 the integrity of I2 members' transactions from the first login onwards. ROC will monitor I2 activities to the network itself, regardless if they passed authentication or not. When a user login to their bank on I1, the bank can invoke a request to authenticate the user. I2 will invoke the user via a mobile app to provide high-fidelity authentication (HFA). I2 will send a secure message to the bank that their user is indeed on the other end. Then, the user can continue their session with their bank on I1 with the standard risks associated.

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

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

Enforcement

Monitoring is pointless without follow-up, incident 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 chance of prosecution and punishment is minuscule.

One of the world's most respected authority 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**
>
> Security expert and New York Time's Best Selling Author of 'Catch Me If You Can'

I2 is a private network with no tolerance for abuse. I2 members must adhere to the I2 SLA or risk shutdown of thier account. I2 will be globally distributed. Therefore, we should expect that non-I2-users might attempt to infiltrate I2. Furthermore, I2 will come to symbolize the bastion of hope for security, a "Online Fort Knox" of sorts – and will by design paint a target on itself.

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.

While not a panacea, the proposal summarized below and discussed in greater detail in Appendix A is worthy of an initial RFC document. The best way to describe it is "back to basics" without cutting any security corners this time around. This includes overt and covert risk measures 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.

1. Visit an office (post office or bank) or ask for a meeting at your home/office
2. Identify yourself in-person with government issued ID, preferably a passport
3. Install the I2 Client Software and get a physical token
4. Bing your identity in-person to the physical token

This process binds the user to the account in-person, and removes the option to masquerade as many identities. In order to get I2 digital credentials, you first need physical credentials and to be present.

After this initial registration, a user can add/edit their additional devices and cards without further in-person visits. If any of the devices, cards, reader are lost or stolen, they should be reported – and I2 can revoke their validity.

This setup will stop most attempts to become someone else. It is better to give a physical token that is unassailable than use biometrics. Should the data of the biometrics ever gets breached, the user can not simply change their biometrics.

Authentication with Four Factors…No Less

In 2005 and 2011, 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?

Something a person knows—commonly a password or PIN. If the user enters 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.

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 qualifies as meeting the guidelines. This led to solutions that only added another element to the authentication scheme versus truly adding another factor.

In I2, we must use ALL THREE factors during authentication versus utilizing additional elements within the SAME factor.

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

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.
- In-person process, similar to the issuance of a passport or opening of a new bank account. The user will be asked to provide government issued identifying document preferably a passport.
- I2 will provide authentication equivalent of NIST level 4 and above. (http://www.itl.nist.gov/lab/bulletns/bltnaug04.htm)

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 will be handled by the company that bears the risk. Since the charter of I2 includes continuous reporting, monitoring and enforcement of its network, "pipe-cleaning" will occur as a natural byproduct of operational monitoring.

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 disconnect offending members.

Technology

- Client Software
- Physical token delivered in-person
- Four Factors of Authentication

"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

CONTACT INFORMATION

602 206 6052 direct
ori.eisen@gmail.com email