



PassPro-techTM

simply secure.

Business Plan

University of Texas at Dallas

Ben Morrow, Stephen Dunlap

Table of Contents

- 1. Description of Proposed Idea 2
- 2. Problem Defined..... 2
- 3. Solution..... 4
 - 3.1 User Interaction..... 4
 - 3.2 Network Security 5
 - 3.3 Login Methodology..... 5
 - 3.4 Internet Threats Defeated..... 6
 - 3.5 Enterprise Security 7
 - 3.5.1 Loss or Theft of USB Device 7
 - 3.5.2 System Recovery 7
 - 3.5.3 Optional Modules for Additional Security 8
- 4. Market Defined 8
- 5. Competition and Competitive Advantage 9
 - 5.1 Mainstream Authentication Methods..... 9
 - 5.2. RSA Security..... 9
 - 5.3. SafeNet 10
 - 5.4. OpenID..... 10
 - 5.5 PassPro-tech™ Competitive Advantage 10
- 6. Product Verification and Testing 11
- 7. Business Model..... 11
- 8. Implementation Strategy 12
 - 8.1 Target Market..... 12
 - 8.2 Product Development 13
 - 8.3 Product Launch and Market Development 14
 - 8.4 Sales and Marketing 14
 - 8.5 Technical Support 16
 - 8.6 Licensing Strategy..... 17
 - 8.7 Exit Strategy..... 17
- 9. Investment Required 17
- 10. Financial Projections..... 17
- 11. Management Team and Advisory Board 18
- 12. Conclusion 20
- Appendix..... 21

1. Description of Proposed Idea

PassPro-tech™ is a unique single-sign-on password technology that offers a simple, secure way to authenticate users on multiple networks with a significantly higher level of security than competing technologies. The system is intended for applications in which multiple pre-authorized clients access and interact with one or more central server installations (banks, securities firms, universities, medical institutions, large corporations, military and government agencies, ISPs, etc.) across either the Internet or proprietary intranets.

PassPro-tech™ was invented by Dr. Jim Pritchard and has been under development since 2000. Four patents have been issued; six are pending, covering all aspects of the technology, including the multi-piece password and the transmission timing intervals (Appendix A). The PassPro-tech™ system utilizes both hardware and software components to provide secure internet authentication, while providing a robust level of protection from all kinds of malicious attacks by hackers. The entire system is transparent to the user and is as easy to use as remembering a simple username or username/password combination and pressing a button.

Extensive testing and validation by independent laboratories has certified PassPro-tech™ to be more effective than any other known method of authentication security. A prototype of PassPro-tech™ was successfully beta tested in a healthcare company for two years.

Now, with substantial intellectual property and third party verification and testing, Dr. Pritchard has partnered with two successful UT Dallas entrepreneurs, Stephen Dunlap and Ben Morrow, to commercialize the innovation.

2. Problem Defined

As the world becomes increasingly dependent on electronic communication and commerce, information security has become one of the most crucial needs in modern society. Limiting access to secure systems is essential for national defense and electronic commerce.

Nearly nine out of ten Americans (87%) store important personal data such as financial information, health records, resumes, and personal emails in files on their computers and 88% go online for sensitive activities such as banking, stock trading, or reviewing personal medical information¹. With this level of

¹ "McAfee/NSCA Cyber Security Survey." McAfee. Oct. 2007. McAfee. 3 Oct. 2008.

activity, much of which is conducted with inadequate security protection, it is no surprise that over 100 million Americans have had their personal information compromised since 2005.² There have been countless attempts to solve this problem, but none has been totally successful.

Most computer services use a standard username/password combination to grant access to the account. This approach is vulnerable to dictionary attacks where a hacker with a fast computer can “guess” the correct password. Because of this threat, many IT administrators now require passwords with numbers and special characters, different passwords for different services, and periodic password changes. Many users are forced to remember multiple passwords. Writing passwords down or storing them in a spreadsheet only increases their vulnerability. Even if a person follows all the best password practices, hackers can utilize a variety of tools and methods to gain access to a computer or sensitive data. Due to the shortcomings of current protection schemes, the average user has a significant chance of their data being compromised by at least one of the following attacks:

Table 2.1 Known Threats

<i>Snoops and Man-in-the-middle Attacks:</i>	Using special software, hackers can monitor and redirect personal transactions through routers or servers. Man-in-the-middle software (a program that enables a hacker to monitor, intercept and redirect data packets) can be acquired for just \$500, but can cause millions of dollars in damages. ³
<i>Trojan and Key-logging Programs:</i>	Malware installed on a user’s computer can record their activities, and run programs without the user noticing.
<i>Cookie Spyware:</i>	Cookies store internet browser session data so that a user can stay logged in to a website. Spyware can read and install new cookies that report private data to a third party.
<i>Phishing Sites:</i>	A user is enticed, usually through an email link, to enter login details into a site that looks reputable, but is actually a trap.
<i>Hacker-Cryptologists:</i>	Password encryption can be “cracked” by reverse engineering the algorithm and discovering the "private key".
<i>Brute Force Attacks:</i>	A computer program runs through millions of password possibilities until the correct combination is found.
<i>Denial-of-Service (DoS) & Buffer Overflow Attacks:</i>	A server is overwhelmed with requests by multiple computers driven by malicious software. This causes the server to shut down and allows the hacker to exploit a resource that would have been protected under normal operation.

² "Data Security: Get the Facts." CSIA. Jan. 2007. Cyber Security Industry Alliance. 3 Oct. 2008 <http://www.csialliance.org/publications/csia_whitepapers/CSIA_Data_Security_Get_Facts_January_2007.pdf>.

³ Knights, Miya. "Man-in-the-middle attacks on the rise." IT Pro. 6 July 2007. IT Pro. 3 Oct. 2008 <<http://www.itpro.co.uk/119212/man-in-the-middle-attacks-on-the-rise>>.

Most of the world's electronic commerce depends on encryption to protect messages, including those sent during authentication. Encryption can be broken if the hacker has the right algorithm or discovers the private key. According to a Gartner survey, retailers lost almost \$2 billion in 2006 because of people avoiding less secure website in fear of getting their credit card information stolen.⁴ Clearly, the solution to this problem is not just about protecting our personal data, but also how to relieve the drag placed on our online economy.

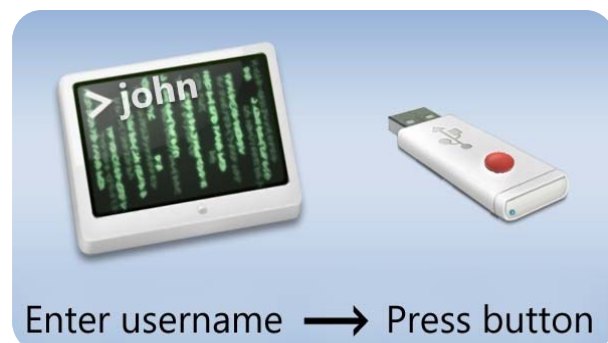
3. Solution

The PassPro-tech™ solution provides single sign-on convenience for all of a user's online banking, email, corporate applications, remote access, and stock trading applications while providing secure authentication and enhanced protection against all currently known internet authentication threats. The system incorporates both hardware and software components (resident on both the client computer and the central server) in an integrated solution that provides both a simple and unobtrusive user interface and a much higher level of security than existing solutions. The key components include:

- Software on the client computer
- Software on the host server
- A USB device unique to each user
- A simple username and/or username/password combination

3.1 User Interaction

A user simply plugs the USB device into the client computer, enters his or her username/password combination into a login dialog and presses a button on the USB device -- the rest is handled behind the scenes. No longer will users be required to remember long, cumbersome passwords, or worry about having to change them every 30 days.



⁴ Schuman, Evan. "Gartner: \$2 Billion in E-Commerce Sales Lost Because of Security Fears." Enterprise Applications. 27 Nov. 2006. eWeek. 3 Oct. 2008 <<http://www.eweek.com/c/a/Enterprise-Applications/Gartner-2-Billion-in-ECommerce-Sales-Lost-Because-of-Security-Fears/>>.

3.2 Network Security

In addition to simplifying user interaction, PassPro-tech™ defeats all of the known network-based threats detailed in Table 1 by acting as a one-time pad (OTP) equivalent. The USB device adds a physical barrier of security because its circuits are isolated from the computer until the device is activated by pressing a button or activating a validation component such as a fingerprint scanner. This prevents malicious programs from reading or accessing the data on the device while it is plugged in.

Behind the scenes, PassPro-tech™ breaks down the username into multiple data packets and sends these packets to the server in predetermined timing intervals. Even if a hacker intercepts the data packets, they will be unable to send them to the server with the correct timing intervals. Each time a user logs on, both the arrangement of the packets and the timing intervals are changed, thus creating billions of one-time-only passwords.

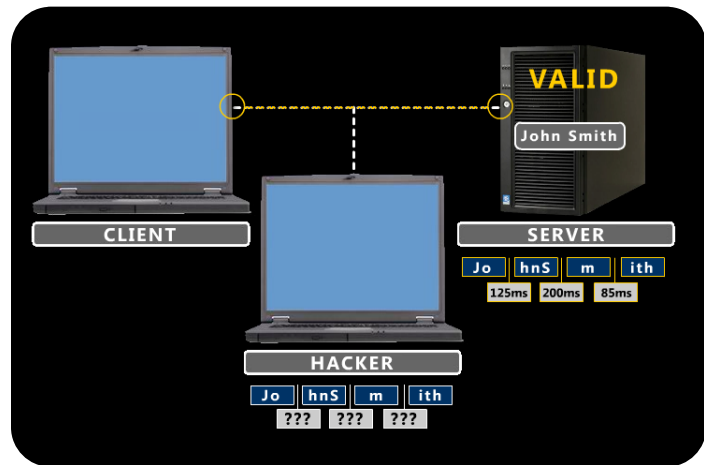
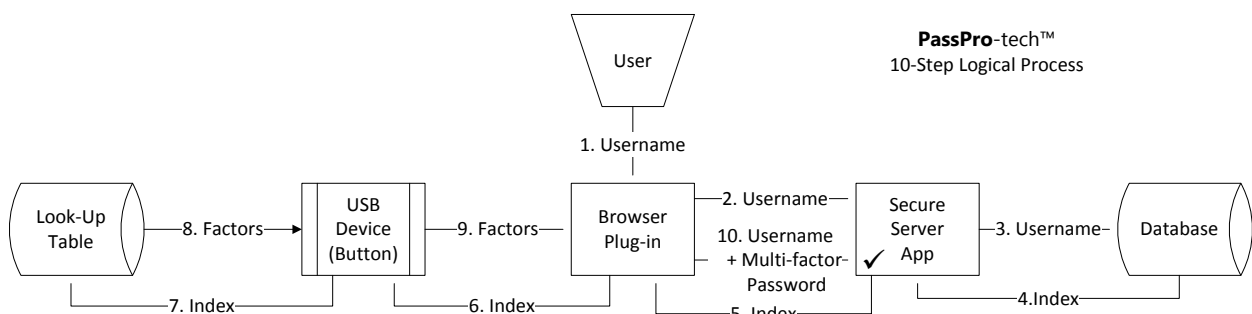


Figure 3.1 Packet-based Authentication

3.3 Login Methodology

The flow chart presented below outlines the 10-step logical process incorporated in the PassPro-tech solution.



The patented 10-step logical process allows the user to securely authenticate with the server. This methodology depicts the interaction and data flow between the user, browser plug-in (client-side

software), USB device, and the server-side software. After the username is entered (1), and the USB button pressed, the username is sent to the server (2), where it is checked for validity in the database (3). The server then requests a random line from the USB device look-up table (4-7). The USB device uses this line in the unique data table to generate a specific set of packets to be sent to the server at defined timing intervals (8). Once the server receives the packets, it verifies that the composition of the packets and timing intervals are correct (10). If the packet transmission is correct, the user is authenticated (✓).

The PassPro-tech™ system is NOT an encryption-based algorithm, vulnerable to attack by dedicated hackers. In our system, each institution will have a unique set of data tables that will be controlled by their IT staff. The first time a user connects with the institution, data tables specific to that user will be downloaded to their USB device. These data tables serve as instructions for both the arrangement of the packets and the timing intervals between them. Each time a user connects, the server will instruct the USB device to manipulate the table in some way.

3.4 Internet Threats Defeated

The robust nature of the PassPro-tech system defeats all known internet threats by employing patented (see Appendix A) hardware and software to:

1. generate a "hidden" password
2. stagger the transmission of the password
3. transmit the password over several packets
4. transmit blank packets
5. split the password transmission to multiple IP addresses to be reassembled on the company intranet (IP Address Multiplexing)

Table 3.1 Defeated Threats

<p><i>Snoops and Man-in-the-middle Attacks:</i></p>	<p>PassPro-tech™ defeats any attempt at packet injection, header modification, or IP address redirection. Intercepted packets do not contain sufficient information to derive the "actual" password nor to simulate the timing modulations used in the multi-step login process. If a transmission is interrupted, PassPro-tech™ automatically attempts to restart the sequence from the original sending client to the original receiving server.</p>
<p><i>Trojan and Key-logging Programs:</i></p>	<p>Since the password is not typed but rather constructed by the USB device, Key-loggers cannot gather sufficient information to steal the password. Since the chips in the USB device are physically disconnected from the computer until the button is pressed, and the information allowed in is very specific, a Trojan cannot read or alter the data on the device.</p>

Cookie Spyware:	Since the authentication system uses on-time-only passwords, any information gained from a cookie (internet browser cache) would no longer be valid. Additionally, any given password is associated with only one IP address, so a spyware program that transmitted data elsewhere would not be effective.
Phishing Sites:	The PassPro-tech™ system uses one-time-only passwords that are not typed; therefore a phishing site could not gather any useful login information.
Hacker-Cryptologists:	PassPro-tech™ is not a cryptographic algorithm in the traditional sense. Since we do not use encryption, but rather our patented system of multiple packets (including blank packets), timing intervals, and IP multiplexing, a cryptologist would not be able to gather sufficient information to figure out a correct multi-factor password.
Brute Force Attacks:	Testing proves that even with a simple username from the dictionary, a brute force attack will be unsuccessful. Due to the combination of timing intervals and packet splitting the combinations that are possible approach infinity.
Denial-of-Service (DoS) & Buffer Overflow Attacks:	PassPro-tech™ performs well all the way up to "wire saturation", at which point there are so many injected packets that no traffic gets through on any station. This proves that even in high network traffic and packet overload situations, the timing intervals work as intended.

(From the full report prepared by the Security Analysis and Information Assurance Laboratory as a result of extensive, real-world testing. See Section 6, Product Verification and Testing)

3.5 Enterprise Security

The system will be configured for each institution and each user with a random table generation module included in the server-side software. The IT department of the purchasing institution will be able to modify the table such that even our company won't have a backdoor into the system. This level of security is desirable for ultra-secure institutions while at the same time beneficial to the Company because PassPro-tech™ will not need to be extensively involved in the initial deployment. Ongoing support will also be limited.

3.5.1 Loss or Theft of USB Device

In the event that a USB device is lost or stolen, the system administrator, from the central server location, can block further use of the device (the same way that lost or stolen credit cards are invalidated) and issue a new USB device to the authorized user.

3.5.2 System Recovery

In the event that the server data table becomes corrupted, a new one can be generated or recalled from a backup database. If a new table is necessary, users will be prompted on the institution login screen to simply download a new table onto their USB device using the same method they did when

they signed up. This process involves holding the button on the USB device down for a few seconds and will take less than two minutes to complete.

3.5.3 Optional Modules for Additional Security

While the baseline product provides excellent network security, we will offer a number of optional USB device configurations to add additional layers of physical security depending on the needs and regulations of the institution. Additional security features such as biometrics, complex passwords, wireless key fobs, or other modifications which will secure the system from physical theft and provide more rigorous identity verification may be utilized. Many government and financial institutions are required to have biometric, multi-factor authentication as part of their network.⁵

4. Market Defined

The system is intended for applications in which multiple pre-authorized clients access and interact with one or more central server installations (banks, securities firms, universities, medical institutions, large corporations, military and government agencies, ISPs, etc.) across either the Internet or proprietary intranets. Both private industry and the government agencies, particularly the Homeland Security Department, are placing increased emphasis on information security. This market is currently yearning for a simpler, more secure way to conduct business.

Revenue for the security software and services industry, currently \$11 billion dollars, is growing at the rate of 14% annually.⁶ IT security spending by government agencies will reach \$9.6 billion by 2013.⁷ Approximately 46% (\$5 billion) of the revenue generated in this market is divided among market segments where PassPro-tech™ could be applied. These segments include identity and access management, application and transaction security, network transmissions, disk and file encryption, software protection and licensing, and entertainment monetization.

⁵ "IT Handbook InfoBase." Federal Financial Institutions Examination Council. 2008. <<http://ffiec.gov/ffiecinfbase>>

⁶ "Gartner Predicts Worldwide Security Software Revenue to Grow 11 Percent in 2008." Gartner. 22 Apr. 2008. <<http://www.gartner.com/it/page.jsp?id=653407>>.

⁷ INPUT. "Information Security Spending by the US Federal Government Will Reach \$9.6 Billion by 2013." 18 September 2008. PRWeb. 18 September 2008 <<http://www.prweb.com/releases/2008/9/prweb1348854.htm>>.

5. Competition and Competitive Advantage

Many potential competitors exist, but there is no competing solution currently on the market that defeats all the potential attacks detailed in Table 1.⁸ The mainstream method of a username/password combination is vulnerable to many network-based attacks. Three representative competitors – RSA, Safenet, and OpenID – each address some, but not all, of the potential threats. Only PassPro-tech™ protects against all of the identified threats.

Table 5.1 Competition Matrix	<i>Open Access</i>	<i>Username</i>	<i>Username + Password</i>	<i>RSA SecureID</i>	<i>Safenet iKey</i>	<i>OpenID</i>	<i>PassPro-tech™</i>
Anonymous Users		✓	✓	✓	✓	✓	✓
Password Guessing			✓	✓	✓	✓	✓
Brute Force				✓	✓	✓	✓
Phishing Sites					✓	—	✓
Single Sign-on						✓	✓
Cookie Spyware				—			✓
Trojan & Keylogging							✓
Snoops/MITM							✓
Hacker-Cryptologists							✓
				✓ = Full protection		— = Limited protection	
Ease-of-Use	*****	*****	**	*	**	**	***

5.1 Mainstream Authentication Methods

Open access, username-only, and username/password authentication methods are by far the most popular ways to authenticate users. These methods do not, however, provide adequate protection against any of the more advanced hacking tools, leaving both users and institutions vulnerable to data compromise (Table 3.1).

5.2. RSA Security

RSA Security requires a complex method to enter multiple passwords. In their system a user is required to carry a keychain device that displays a 6-digit number which rotates every minute. Users

⁸ Please see Table 2, Section 3.4 for a discussion of how PassPro-tech successfully defeats each of the identified threats.

must type their username, password, and the 6-digit number each time they log on. Due to the success of this technology RSA has gained significant market share in corporate networks.

The effectiveness of RSA's SecureID system is limited due to both security vulnerabilities and weak human factors. This system is susceptible to key logging and phishing attacks. With the user's information stolen, these automated programs could gain access to a user's account within milliseconds, clearly within the 1-minute window. In addition, the number-generating algorithm can be copied thus giving an attacker the ability to predict future rotating numbers and spoofing the login. Users find this method cumbersome since they must fill out three fields and often have to wait until the rotating number changes in order to make sure they submit the form on time. Last, the keychain display can be difficult to read due to its size and contrast. These user inconveniences add up to many hours of lost productivity.

5.3. SafeNet

SafeNet attempts to "one up" RSA by offering a USB device that plugs into a user's computer rather than a keychain display. SafeNet also offers users another layer of protection with a fingerprint reader on the USB device. While this approach is more user friendly, it does not significantly improve protection. It reduces vulnerability to phishing and key-logging attacks, but SafeNet's iKey is still susceptible to man-in-the-middle and "spoofing" attacks. Since the iKey authentication never changes, the exposure time for attacks is virtually unlimited.

5.4. OpenID

OpenID offers the ability to sign on to multiple websites with one username and relies on a third party to verify the user's account. For example, a Yahoo! Mail account can be used log on to other websites. This is the least secure of the competitors analyzed because of its vulnerability to man-in-the-middle, key logging, and phishing attacks. It is also dependent on a third party to be accessible and honest throughout the authentication process.

5.5 PassPro-tech™ Competitive Advantage

PassPro-tech™ is superior to competitive alternatives in the information security market because it: (1) offers a unique combination of physical and logical barriers that prevent hackers and snoopers from

intercepting data, thus (2) defeating all currently identified security threats, while (3) providing unparalleled ease-of-use (See Table 3.1, Section 3.4 for details).

6. Product Verification and Testing

The effectiveness of the PassPro-tech solution has been independently verified by the Security Analysis and Information Assurance Laboratory (SAIAL) at The University of Texas at Dallas, which also performs testing for the NSA, EPA, DoD, and the Department of Homeland Security. Eight separate tests were run over a six week period in a variety of environments and configurations. The SAIAL found PassPro-tech to be “powerful and in many ways unbreakable,” as it defeated each internet authentication attack they threw at it. The PassPro-tech™ system was also successfully beta-tested for two years at National EDI Systems Corp., a company that transmits electronic health insurance claims between doctors’ offices and insurance companies in more than 40 states. PassPro-tech™ met all HIPAA security requirements; no significant problems were encountered.

7. Business Model

PassPro-tech™ will use a subscription-based business model, with an initial charge for both hardware and software and an ongoing license and maintenance fee, based on the number of users. For smaller clients, PassPro-tech™ will be offered for an initial price of \$18 per user for the server software and \$15 per user for the client software, with a \$25 cost for the USB device and \$3 for maintenance, or a total of \$61 per user. Larger clients will receive discounts of up to 60% on the software and USB device, reducing the initial cost per user to as little as \$26 per user, as detailed in the table below.

Table 7.1 Tiered Pricing Model	Tier One	Tier Two	Tier Three	Tier Four
Users	0-5000	5001-10000	>10000	>100000
Discount		25%	40%	60%
Server Software/User	\$18.00	\$13.50	\$10.80	\$7.20
Client Software/User	\$15.00	\$11.25	\$9.00	\$6.00
USB Device	\$25.00	\$18.75	\$15.00	\$10.00
Annual License & Maintenance/User	\$3.00	\$3.00	\$3.00	\$3.00

Annual license and maintenance fees of \$3 per user will also be charged. For this price a company would have access to updates and replacements as well as technical support. For a mid-sized (100-employee) company, the total cost of \$6,700 would provide protection for three years. This tiered

pricing model is competitively priced within the industry and will encourage mass adoption of the PassPro-tech™ product, while providing superior security and convenience.

As market penetration increases, users who already possess a PassPro-tech™ USB device will be able to log on to multiple server sites with their original device, further reducing the initial cost for issuing companies.

PassPro-tech™ will benefit from an ongoing stream of residual income from the maintenance plan, device replacements, and system upgrades. Our projections assume that, over time, a certain percentage of customers will upgrade to USB devices offering higher levels of security. For example, a fingerprint reader on the USB device or software that requires a more complex username/password combination would allow for additional identity verification. Finally, new potential customers are entering the market each year, as the software security market continues to grow at a rate of 14% annually. We plan to attract many of those new customers and expand our market to international regions.

8. Implementation Strategy

8.1 Target Market

PassPro-tech™ has been designed for applications in which multiple pre-authorized clients access and interact with one or more central server installations (banks, securities firms, universities, medical institutions, large corporations, military and government agencies, ISPs, etc.) across either the Internet or proprietary intranets. Although individual users will realize considerable benefit from the single-sign-on features and the elimination of the need for multiple and complex passwords, our target customer will be the enterprise that controls the server installation and has a strong interest in protecting both individual users and enterprise networks and databases from unauthorized access or intrusion.

Our target customer is legitimately concerned about data security on their servers due to news headlines, privacy lawsuits, and federal regulations. These businesses recognize the risk of poor network security and the importance of protecting their corporate information and customers' and employees' records. In addition to these general requirements, we have identified the unique security needs of four particular market segments:

- **Small and Medium-Sized Enterprises (SMEs):** in addition to protecting their enterprise networks, these companies frequently need to authenticate transactions with larger organizations while sending payroll, insurance, or other sensitive information.
- **Regulated corporations (including banks, healthcare and educational institutions):** in addition to protecting their enterprise networks, these need to standardize authentication for multiple network-based applications across a large and frequently changing user base. Most of these organizations are subject to extensive regulatory requirements related to privacy laws.
- **Unregulated corporations (manufacturing, distribution, transportation and similar businesses):** in addition to protecting their enterprise networks, these need to standardize authentication for multiple network-based applications across a large and frequently changing user base.
- **Governments:** in addition to protecting their global networks, these need to standardize authentication for multiple network-based applications across a large user base. In addition, they frequently need to provide higher levels of security for various classified and financially sensitive communications.

8.2 Product Development

The PassPro-tech™ product includes both hardware and software components. Prototypes of the USB device have been designed by the founders, assembled by a contract electronics manufacturing company (Appendix B), and used in the validation and testing cited in Section 6. Software development is currently underway, utilizing two experienced security software developers, David Russo and Peter E. Koenig, under contract to the company. The following product development requirements remain to be completed prior to product launch:

- 1) Creating a production design for our USB plug-in device to make it rugged, tamper-proof, and cost-effective;
- 2) Enlisting a qualified manufacturer for the device;
- 3) Completing software development to make our system compatible with all Internet browsers on the client side and with different network protocols and software on the server side;
- 4) Creating user manuals and other system documentation;
- 5) Training (or outsourcing) a customer-support team; and
- 6) Ensuring that our system meets all governmental and industry standards, including:
 - a) *ROHS*: Hazardous material standard for chip manufacturing
 - b) *OMB M-06-16*: security standard that we exceed by using a 4-factor authentication system

It is anticipated that these activities will proceed in parallel and be accomplished within 12 months of funding.

8.3 Product Launch and Market Development

A three-phase product launch and market development plan will be implemented over a five-year period commencing approximately one year after funding (following completion of the product development activities). This phased approach will provide for meaningful and attainable benchmarks along the road to success.

Table 8.1. Phased Implementation Approach

<p><i>Phase 1:</i> First Customers</p>	<p>Our initial marketing efforts will focus on the regulated corporations (banks, healthcare and educational institutions) and selected government agencies because they are subject to extensive regulatory oversight and are vulnerable to privacy lawsuits. These customers will help us develop our reputation and gain additional credibility in the marketplace.</p> <p>General Criteria: Years 1-2, \$4.5M Revenue, 25 Customers, break-even</p>
<p><i>Phase 2:</i> Mass Production</p>	<p>In Phase 2, we will broaden our focus to include SMEs and unregulated corporate entities. In order to address this broader market, we will add Independent Sales Organizations (ISOs) to supplement our internal team. These ISOs will be a commission-based sales force. Many will have pre-established relationships with IT departments in these companies. As awareness of PassPro-tech™ grows, increased volume will justify mass production and economies of scale and scope will come into play. At this point we should be eligible for government contracts and would begin to generate significant revenue.</p> <p>General Criteria: Years 3-4, \$50M Revenue, 200+ Customers</p>
<p><i>Phase 3:</i> Licensing</p>	<p>In Phase 3, as PassPro-tech™ becomes an industry standard, we expect that other companies will want to incorporate our technology into their products. This will yield additional income in the form of royalties from our patented processes. When our product becomes the industry standard for authentication security, we will be in a good position to exit via acquisition or an initial public offering.</p> <p>General Criteria: Year 5+, industry standard, exit</p>

8.4 Sales and Marketing

Phase 1 will focus on initial market penetration and creating awareness of the PassPro-tech™ solution in the marketplace. Our sales and marketing efforts will be implemented by the founders and our internal sales and marketing team.

Our initial target customers will be the regulated corporations (banks, healthcare and educational institutions) which are subject to stringent security requirements mandated by multiple regulations. Our value proposition will focus on: (1) enhanced network security; (2) reduced risk of regulatory or legal

sanctions; and (3) ease-of-use for their customers and employees. We anticipate that these institutions will purchase PassPro-tech™ to install on their servers and provide their employees and/or customers with the USB devices for secure access. We currently have interest from institutions and organizations such as UT Dallas, NYU, Hewlett-Packard, Ericsson and the Department of Defense.

We will supplement our direct sales efforts with a marketing communications campaign designed to increase awareness of the PassPro-tech™ solution. We plan to gain publicity through strategic articles, blogs, and a strong internet presence and create a strong word-of-mouth campaign by attending and speaking at trade shows, industry vertical conferences, etc. We will also seek to get press coverage from cyber security publications such as *Government Security Magazine* and the *Journal of Homeland Security*.

Once we've established a connection with a target institution, either by word-of-mouth or by direct sales efforts, we will target both IT departments and operating management (the former to address the technology aspects and the latter to address the risk/reward tradeoffs). We estimate that the sales cycle from first contact to implementation will be 4 to 6 months in larger institutions, We also realize that larger entities often have a budget cycle, especially within the government, so the timing of the proposal will be important.

The objective in Phase 1 will be to establish approximately 25 customers, including a number of high-profile accounts that will provide credible references for the expanded sales and marketing efforts in subsequent phases. Our first few customers will receive discounts on the system as we enter the market. We will also have an affiliate program where referrals are rewarded with a percentage of the contract. This will both increase awareness and increase adoption of our system through word-of-mouth. The affiliate program will add to the leads our internal sales team generates.

In Phase 2, we will expand our sales and marketing efforts through the use of Independent Sales Organizations (ISOs) or VARs to extend the reach of our marketing capabilities nationwide and broaden our focus to include unregulated corporations and SMEs.

We will select the ISOs on the basis of their established relationships with key accounts in our targeted market segments. We have identified 28 potential ISOs, each of whom could generate in excess of \$10,000 in monthly revenue during the first 12 months of operations, accounting for approximately 50% of our gross revenues . This sales force will develop a nationwide awareness for our

product while generating enough demand for mass production. We anticipate that these organizations will be able to leverage existing relationships within the customers' IT departments to quickly ramp up our sales efforts.

A strategic partnership with a company like Computer Associates or other IT management and consulting firms could potentially bring in a large number of customers, and will be pursued. Since we have the most secure, patented product in the network security market, we think this would be a beneficial endeavor for both the consultant and our company.

Training and compensation will be important. These individuals will attend a weekend "boot camp" about our product as well as receive literature and marketing materials. They will be compensated with a competitive commission to ensure they sell our product instead of a similar type of product from a competitor or substitute.

Our internal team will continue to focus on penetrating larger accounts, with particular emphasis on regulated institutional and government accounts, either alone or in partnership with the ISO sales teams. Eventually, we plan to aggressively pursue new commercial and military applications in areas beyond simple user sign-on services. Our technology can prevent cloned subscriptions in cellular networks and TV services. With PassPro-tech™ a new variety of physical locks can be developed for high security locations such as shipping ports and restricted areas. PassPro-tech™ can also secure voice and data transmissions on satellite communications.

Network externalities will eventually come into play. Selling the system to smaller companies will be much quicker -- especially if one of the companies they communicate with on a regular basis has already adopted the system. For example, landing one health insurance company could enable us to sell to all of the doctors' offices associated with that company.

8.5 Technical Support

PassPro-tech will provide technical support and detailed manuals for our products. We will provide 24/7 telephone support provided by a reputable technical support organization. We anticipate that our ongoing costs for technical support will be relatively low. Based on our beta test experience, it is rare that technical support is needed after the initial installation. At our beta-test company, a single IT company employee installed the PassPro-tech™ system with only minimal assistance. No technical

support has been needed during our 2-year test. We also expect that some customers, with highly sensitive data, will only allow their own employees access their secure networks and servers. This will further reduce our involvement in the implementation and support of the system, saving us additional costs.

8.6 Licensing Strategy

The PassPro-tech™ system can be integrated into other hardware components. The USB device can be combined with the keyboard on a desktop, laptop, or mobile device and the software can come pre-installed on personal computers and authentication servers. We will actively pursue companies like Cisco, Dell, and Apple to integrate and license our technology. Another option for a strategic partnership would be the integration of the PassPro-tech™ software into a pre-existing software package. Intuit is an excellent candidate to use our system for their personal finance software -- Quicken and QuickBooks.

8.7 Exit Strategy

By the end of our five year implementation phase, we anticipate that the PassPro-tech™ will have become recognized as an industry standard. At this point, we anticipate that companies like VeriSign, HP, IBM, and RSA would be interested parties because of their ongoing involvement in enterprise-level networks security. An initial public offering is another potential exit strategy. This will raise funds for market expansion and will allow our venture investors to exit with a substantial return.

9. Investment Required

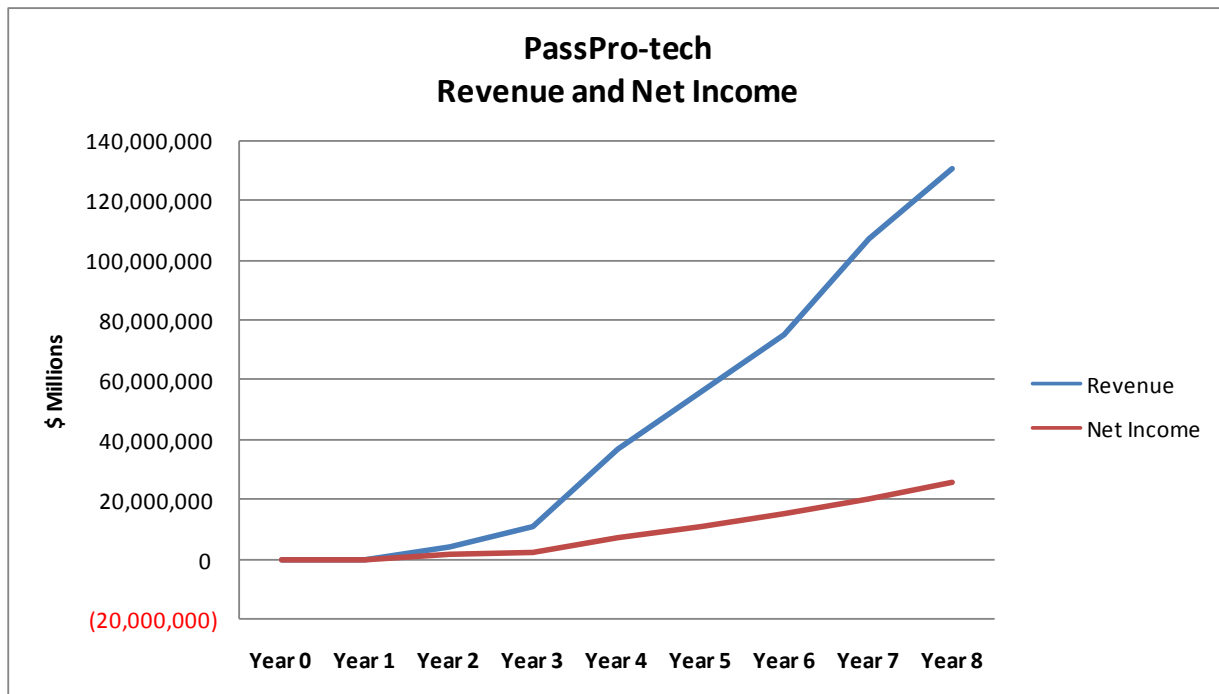
A modest amount of start-up funding will be necessary to commercialize our product and meet initial sales goals. To achieve our objectives, PassPro-tech™ is seeking \$1,000,000 in seed money for Phase 1. The initial investment will be utilized for sales and marketing expense (\$300,000); product development (\$300,000) and working capital (\$200,000) with an anticipated cash balance of approximately \$200,000 when we reach break-even in the fourth quarter of the second full year of operations.

10. Financial Projections

We anticipate limited revenues during the first year of operations, with sales commencing during the fourth quarter after funding. Phase 1 will be completed during the second year with total revenues

of \$4.3 million. We anticipate that we will achieve break-even during the fourth quarter of the second year, generating sufficient profits to fund the expansion of our operations in Phase 2, including the recruitment and hiring of additional full-time staff, and supporting marketing, interoperability testing, and mass production of the PassPro-tech™ system from that point forward.

By the end of the fifth year, we expect the company to have revenues in excess of \$56 million and net income in excess of \$10 million. The chart below summarizes our projected financial performance; details are provided in Appendix C.



Based on our financial projections, we anticipate a return in excess of 74% on the initial investment of \$1,000,000 by the end of the fifth year of revenue.

11. Management Team and Advisory Board

Dr. Jim Pritchard, a Dallas-based dentist, began developing the PassPro-tech concept in the early 2000's when he realized that the methodology for sending patients' health records to insurance companies was unsecure.

Two MBA students from UT Dallas, working with Dr. Pritchard, have formed the company, now with significant intellectual property and a beta-tested product, and are preparing the technology for commercialization. As founders of multiple start-up companies, **Stephen Dunlap** and **Ben Morrow** have

experience in the sales, marketing, computer networking, and software development industries, and have the chemistry and diversity required for success.

Stephen Dunlap graduated Summa Cum Laude with his Business Administration degree in spring 2008, and is currently seeking his Masters of Business Administration (MBA). Stephen has served as CEO of two-startup companies, Nexxus Marketing Group LLC where he managed a profitable residential real estate restoration and development firm and GreenGrid Corporation where he developed new technology for electrical storage in vehicles, and creating GreenGrid as a platform to springboard product development and raise capital. Stephen is involved in the Entrepreneurship Club, Beta Gamma Sigma (Management Honor Society) and Golden Key Honor Society. Mr. Dunlap has also won the 2008 Texas Business Hall of Fame Scholarship and President's Education Award.

Ben Morrow received a Bachelor of Science degree in Business Administration and a Bachelor of Arts degree in Arts and Technology. He also completed the University's rigorous pre-med curriculum. He has co-founded three companies - Morrow Lawncare, ViVX design, and GreenGrid. In the 12-member Global Investment Club he participates in growth stock trading decisions for a portfolio larger than \$200,000. As a student, Morrow was involved in the Honors Program, the Dean's Council, and the Entrepreneurship Club. As an Orientation Team Mentor he helped acclimate hundreds of new students to campus. He also had the honor to be the sole student speaker at the undergraduate commencement ceremony and has studied business and culture abroad in China and India.

PassPro-tech has developed a diversified advisory board with expertise in electrical engineering, computer communications, corporate and intellectual property law, and venture development.

- **Steven W. Smith** was a successful manager at General Electric's Aerospace Business Group for seven years, when he left to attend law school at the University of Texas School Of Law. Smith has 16 years of experience as a patent and trademark attorney, during which time he established and ran his own successful law firm and served as an officer of the Dallas Bar Association.
- **Perry Baty**, currently COO of National EDI, has 27+ years of experience in computer technology sales and product implementation, and has consulted with Fortune 500 corporations regarding their IT infrastructures.
- **Peter E. Koenig** has 23 years experience in software and hardware development. Peter was the software development manager at InterVoice, when he founded Domain Technologies, a designer of digital signal processor (DSP) design firm. He sold the company in early 2008 to VeriSilicon.

- **Douglas Carlson** is the Executive Director of Communications and Computing Services at New York University. Doug is responsible for the operation and evolution of NYU's international communications, computing and network security infrastructure. Prior to joining NYU, he managed and supported large-scale communications and computing services at several academic, corporate and research facilities.
- **David Rex** is a partner at Jackson Walker, where he specializes in assisting entrepreneurs and emerging companies from formation to exit. Mr. Rex has extensive expertise in private merger, acquisition and divestiture transactions, including business analysis, due diligence, negotiation of definitive agreements, financing, and research and resolution of related complex legal issues.

12. Conclusion

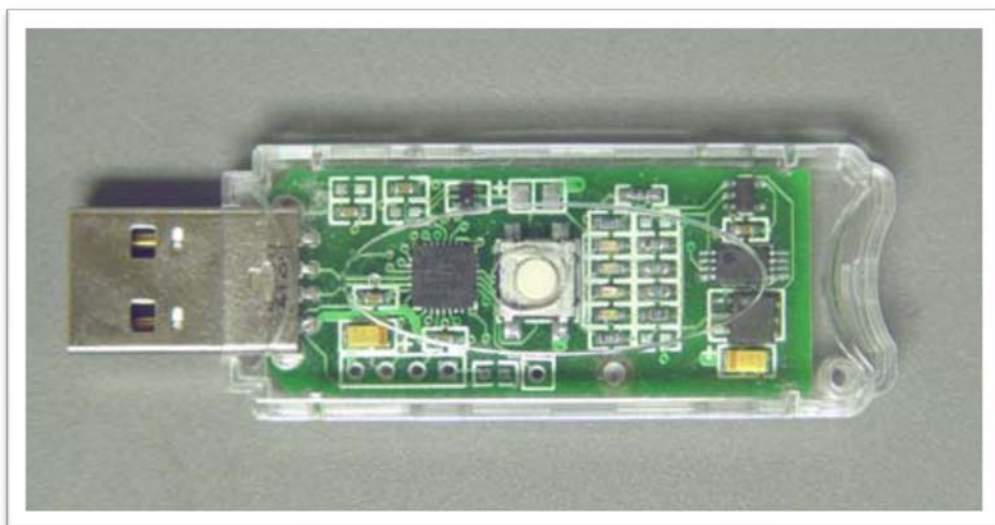
Nine out of ten Americans have their personal information at risk every day. PassPro-tech™ eliminates this risk by offering powerful protection that secures and simplifies the online experience.

PassPro-tech™ -- *simply secure.*

Appendix

Application No./ Publication No.	Filing Date	Subject Matter
09/783,049	02/14/2001	Time-Based Password Technology
09/847,757	05/02/2001	Virus Trap Computer
11/020,780 2006/0136993	12/22/2004	Blank Packet Password
11/061,223 CIP of 09/783,049 2005/0149762	02/18/2005	Time-Based Password Technology With Rolling Codes
11/149,818 CIP of 11/020,780 2006/0136740	06/10/2005	Server Index Value to Client Lookup Table
11/268,204 CIP of 11/061,223 2006/0070125	11/07/2005	Client Plug-in Device
11/607,764 CIP of 11/061,223 2007/0150743	12/01/2006	Address Division Multiplexing
In progress	02/13/2007	Secure Financial Transactions
In progress	07/10/2008	Cellular Network Access
In progress	07/10/2008	Logon Dialog and Single Sign-On
<i>Issued (Blue), Pending (Black)</i>		

Appendix A. Patent Table



Appendix B. Prototype USB device

PRICING MODEL				
	Tier One	Tier Two	Tier Three	Tier Four
Users	0-5000	5001-10000	>10000	>100000
		25%	40%	60%
Server Software/User	\$18.00	\$13.50	\$10.80	\$7.20
Client Software/User	\$15.00	\$11.25	\$9.00	\$6.00
USB Device	\$25.00	\$18.75	\$15.00	\$10.00
Maintenance/User/Year	\$3.00	\$3.00	\$3.00	\$3.00

Appendix C. Pricing Model

Cost/Account Size								
Users	100	500	1,000	5,000	10,000	50,000	100,000	500,000
Server Software/User	\$1,800	\$9,000	\$18,000	\$67,500	\$135,000	\$540,000	\$720,000	\$3,600,000
Client Software/User	\$1,500	\$7,500	\$15,000	\$56,250	\$112,500	\$450,000	\$600,000	\$3,000,000
USB Device	\$2,500	\$12,500	\$25,000	\$93,750	\$187,500	\$750,000	\$1,000,000	\$5,000,000
Maintenance/User/Year	\$300	\$1,500	\$3,000	\$15,000	\$30,000	\$150,000	\$300,000	\$1,500,000
Total Startup Cost	\$6,100	\$30,500	\$61,000	\$232,500	\$465,000	\$1,890,000	\$2,620,000	\$13,100,000
Startup Cost/User	\$61	\$61	\$61	\$47	\$47	\$38	\$26	\$26
Maintenance Renewal/Year								
Annual Cost - Years 2+	\$300	\$1,500	\$3,000	\$15,000	\$30,000	\$150,000	\$300,000	\$1,500,000
Annual Cost/User	\$3	\$3	\$3	\$3	\$3	\$3	\$3	\$3

Appendix D. Cost for Various Numbers of Users

REVENUE MODEL							
		Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
Revenue Model							
Tier One Customers		0	5	15	50	100	200
Tier Two Customers		0	0	7	12	20	40
Tier Three Customers		0	0	1	3	10	20
Tier Four Customers		0	0	0	1	5	10
		0	5	23	66	135	270
Users	Average Users						
Tier One Customers	500	0	2,500	7,500	25,000	50,000	100,000
Tier Two Customers	7500	0	0	52,500	90,000	150,000	300,000
Tier Three Customers	40000	0	0	40,000	120,000	400,000	800,000
Tier Four Customers	200000	0	0	0	200,000	1,000,000	2,000,000
		0	2,500	100,000	435,000	1,600,000	3,200,000
New Users/Year	Average Users						
Tier One Customers	500		2,500	5,000	17,500	25,000	50,000
Tier Two Customers	7500		0	52,500	37,500	60,000	150,000
Tier Three Customers	40000		0	40,000	80,000	280,000	400,000
Tier Four Customers	200000		0	0	200,000	800,000	1,000,000
			2,500	97,500	335,000	1,165,000	1,600,000
Maintenance Only Users			0	2,500	100,000	435,000	1,600,000

Appendix E. Revenue Model

INCOME STATEMENT							
	Revenue	Year 0	Year 1	Year 2	Year 3	Year 4	Year 5
Revenue	Per User						
Tier One Customers	\$61	0	152,500	305,000	1,067,500	1,525,000	3,050,000
Tier Two Customers	\$47	0	0	2,441,250	1,743,750	2,790,000	6,975,000
Tier Three Customers	\$38	0	0	1,512,000	3,024,000	10,584,000	15,120,000
Tier Four Customers	\$26	0	0	0	5,240,000	20,960,000	26,200,000
Maintenance Revenue/User	\$3	0	0	7,500	300,000	1,305,000	4,800,000
Total Revenue		0	152,500	4,265,750	11,375,250	37,164,000	56,145,000
Cost of Sales							
USB Devices	\$6	0	15,000	585,000	2,010,000	6,990,000	9,600,000
Software Duplication/Packaging	\$35	0	175	805	2,310	4,725	9,450
Install Support - Fixed	\$10,000	0	50,000	230,000	660,000	1,350,000	2,700,000
Install Support per User	\$2	0	5,000	195,000	670,000	2,330,000	3,200,000
Ongoing Support	\$2	0	3,750	150,000	652,500	2,400,000	4,800,000
Total Cost of Sales		0	73,925	1,160,805	3,994,810	13,074,725	20,309,450
Gross Profit		0	78,575	3,104,945	7,380,440	24,089,275	35,835,550
Margin %			51.5%	72.8%	64.9%	64.8%	63.8%
Operating Expense							
Selling Expense (Install Revenue)	20%	150,000	152,500	851,650	2,215,050	7,171,800	10,269,000
Product Development/Maintenance	10%	150,000	152,500	425,825	1,107,525	3,585,900	5,134,500
General & Administrative Expense	7%	50,000	106,750	298,078	775,268	2,510,130	3,594,150
		350,000	411,750	1,575,553	4,097,843	13,267,830	18,997,650
Operating Income		(350,000)	(333,175)	1,529,393	3,282,598	10,821,445	16,837,900
Provision for Income Tax	35%	0	0	(296,176)	(1,148,909)	(3,787,506)	(5,893,265)
Net Income		(350,000)	(333,175)	1,233,216	2,133,688	7,033,939	10,944,635
Percent of Revenue		0.0%	-218.5%	28.9%	18.8%	18.9%	19.5%

Appendix F. Income Statement

Expense Assumptions

Cost of Sales

- 1) USB devices will cost \$6 to manufacture
- 2) Software duplication and packaging will cost \$35 per customer
- 3) Initial install will cost an average of \$10,000 per customer
- 4) Install support per user will be \$2
- 5) Ongoing support per user will be \$2/year

Operating Expenses

- 1) Selling Expense will be 20% of install revenue
 - a) Commissions will account for half of this expense (10% of install revenue)
- 2) Product development and maintenance will cost 10% of install revenue
- 3) General and administrative expenses will be 7% of install revenue

Appendix H. Expense Assumptions

Revenue Assumptions

- a) Accounts receivables will be 45 days
- b) Inventory will be 75 days cost sales outstanding

Current assets will be 2%

Appendix I. Revenue Assumptions