

*Introducing a Radically New and Patented  
Concept in Internet Password Protection!*

*Point to Point  
Protocol*

*Password  
Protection*

$$P \cdot P \cdot P \times P \cdot P = P^5$$

# What is $P^5$ ?

$P^5$  incorporates a new dimension to uniquely identify an Internet *password*... TIME



# Why use $P^5$ ?

$P^5$  is more secure than 128 bit encryption without the complexities of decryption.

## Why does **P<sup>5</sup>** work?

P<sup>5</sup> takes advantage of the Internet's capability to accurately maintain time intervals between messages, once a connection has been established.

## How does **P<sup>5</sup>** work?

P<sup>5</sup> paces outgoing and measures incoming timing intervals between Internet messages.

## **P<sup>5</sup>** Message Pacing

P<sup>5</sup> transmits a special Internet password sequence that precisely *paces* the outgoing time intervals between each of its messages.

## **P<sup>5</sup>** Message Measuring

P<sup>5</sup> then receives the special Internet password sequence and precisely *measures* the incoming time interval between each of its messages.

# P<sup>5</sup> Messaging Sequence

P<sup>5</sup> sends out a *sequence* of timed Internet messages formatted as a password.

# P<sup>5</sup> Password Packets

The password is sent and received as a group of messages comprised of special P<sup>5</sup> *packets*.

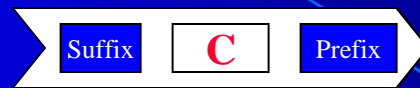
## P<sup>5</sup> Password Verification

Once the packet sequence has been completely received, P<sup>5</sup> then *compares* its measured password time intervals against the expected durations.

## P<sup>5</sup> Password Acknowledge

After the receiving computer processes the password sequence, P<sup>5</sup> then returns an Internet *acknowledgement* indicating success or failure.

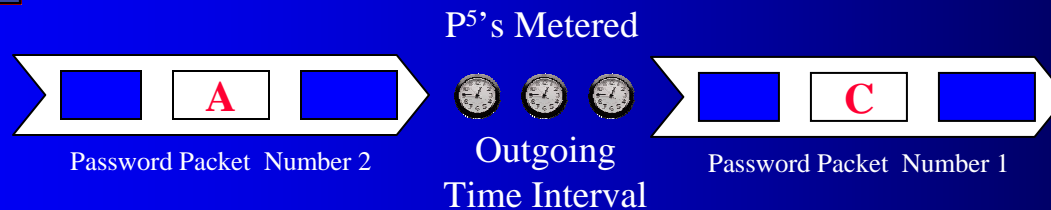
# P<sup>5</sup> Packet Format



Password Packet

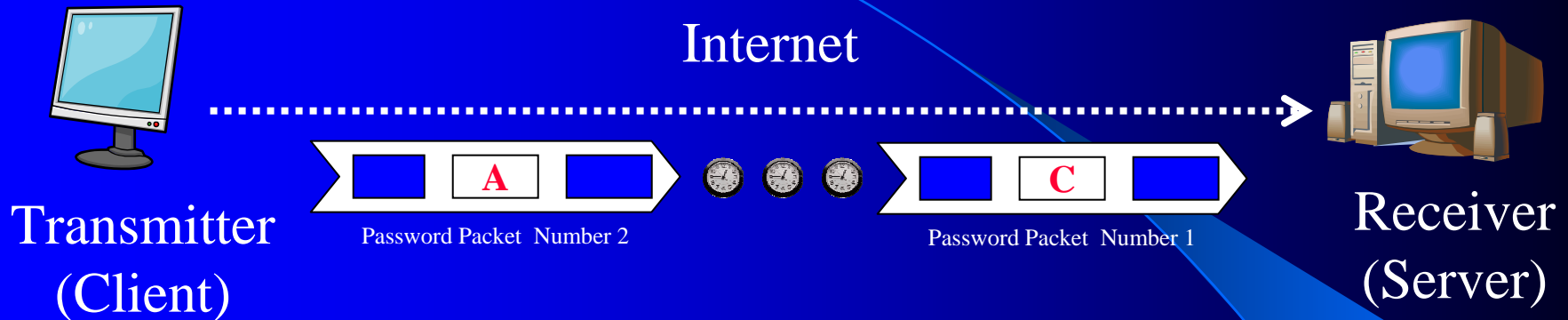
The special P<sup>5</sup> packet *format* is comprised of a prefix, suffix and a password character.

# P<sup>5</sup> Packet Timing



P<sup>5</sup> inserts predetermined outgoing *time* intervals between each P<sup>5</sup> packet.

# P<sup>5</sup> Internet Timing

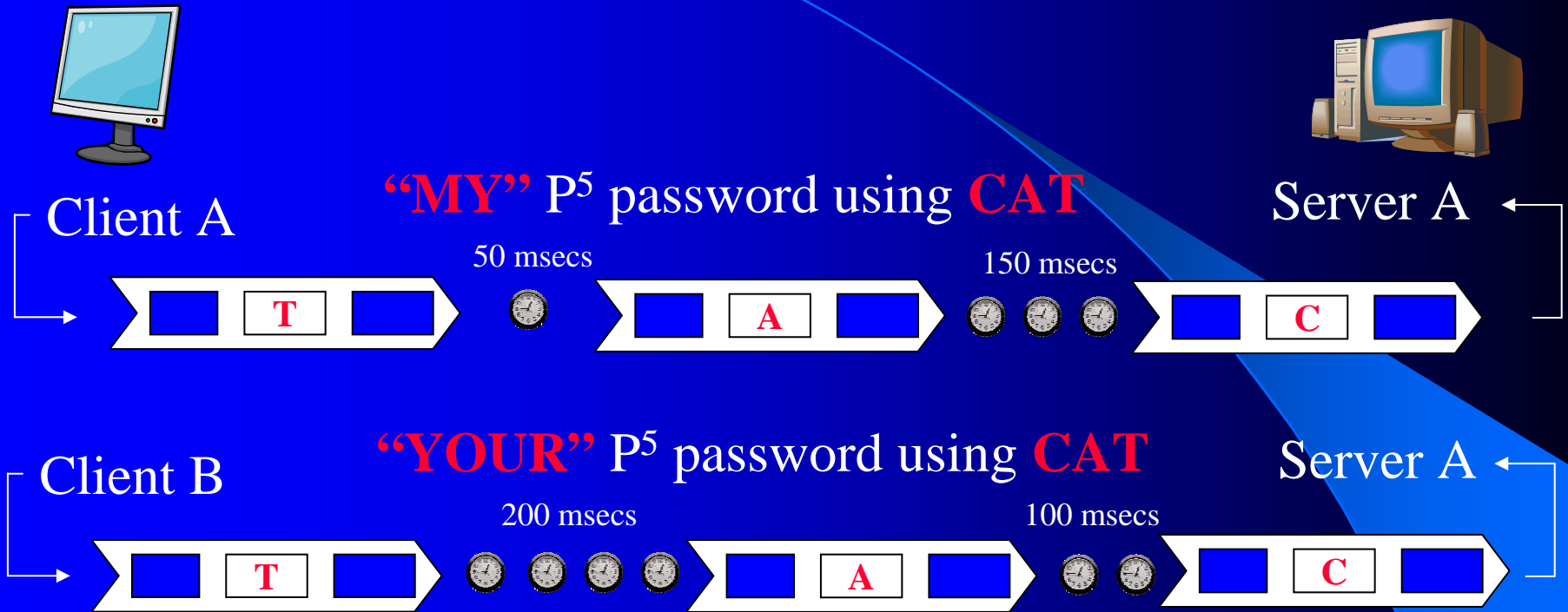


The Client paces and transmits predetermined time intervals between P<sup>5</sup> packets across the Internet.

Every time interval between P<sup>5</sup> packets is accurately preserved across the Internet.

In turn, the Server receives and accurately measures the incoming time intervals.

# P<sup>5</sup> Password Samples



The two passwords above are literally the same, however, they are unique because of their timing.

# Password Permutations

*WITHOUT* TIMING INTERVALS CONSIDERED:

Three Character Password allowing 36 different characters: A-Z, 0-9

36 characters taken 3 at a time

$$= 36 \times 35 \times 34$$

$$= 42,840 \text{ permutations}$$

Cracked in a matter of seconds by dictionary attacks.

*WITH* TIMING INTERVALS CONSIDERED:

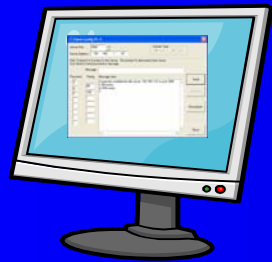
$$P^5 = 42,840 \times 1000\text{msecs} \times 1000\text{msecs}$$
$$= 42,840,000,000 \text{ permutations}$$

Would take an infinite number of attacks.

Security exponentially increases with each additional timing interval!  
One more character with timing increases the possible permutations to over 42 trillion! (DNA is one in 12 billion)

# P<sup>5</sup>

## Client & Server Computers



Salesman's  
Laptop (Client)

Internet

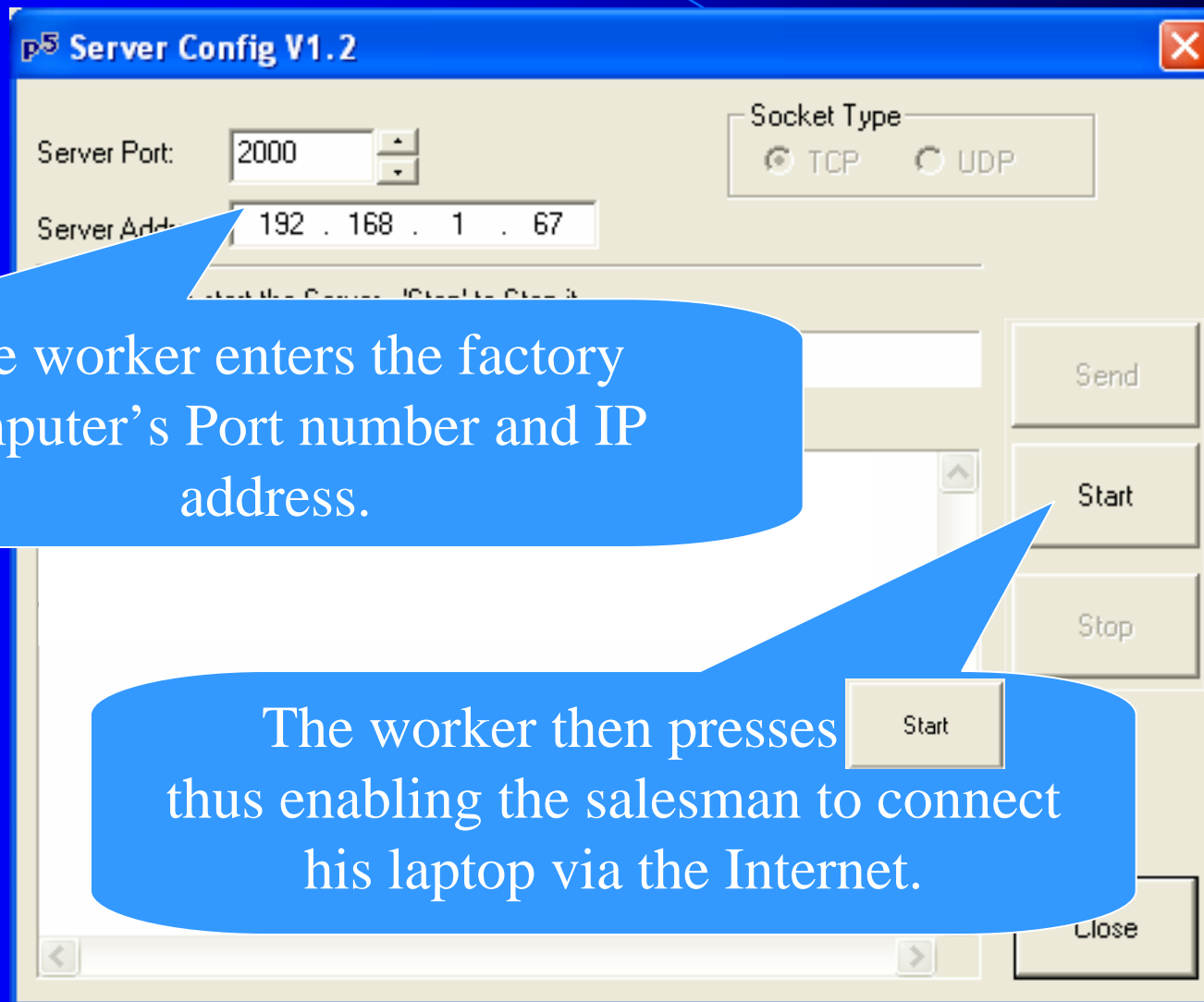


Data Base  
Computer (Server)

One scenario is an outside salesman wishing to securely access his factory's database.

# P<sup>5</sup>

## Server (At Factory)



**P<sup>5</sup> Server Config V1.2**

Server Port: 2000

Server Address: 192 . 168 . 1 . 67

Socket Type:  TCP  UDP

Send


Start

Stop

Start

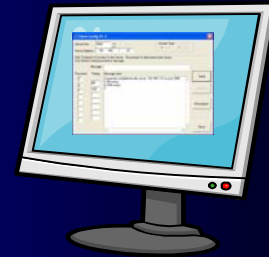
Close

The worker enters the factory computer's Port number and IP address.

The worker then presses  thus enabling the salesman to connect his laptop via the Internet.

# P<sup>5</sup>

## Client Window



**p<sup>5</sup> Client Config V1.4**

Server Port:  Socket Type:  TCP  UDP

Server Address:

Click 'Connect' to Connect to the server. 'Disconnect' to disconnect from server.  
Use Send to Send password or message.

Message:

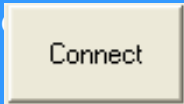
Password	Timing	Mes:
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Buttons: Send, Connect, Disconnect, Close

Connect

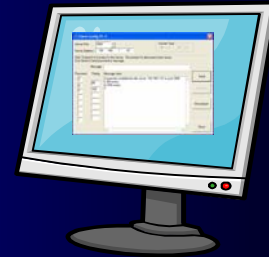
The salesman enters the factory's computer Port number and IP address.

Next the salesman presses



# P<sup>5</sup>

## Client Window



**p<sup>5</sup> Client Config V1.4**

Server Port: 2000  
Server Address: 192 . 168 . 1 . 67

Click 'Connect' to Connect to the Server. 'Disconnect' to Disconnect from the Server.  
Use Send to Send password or message.

Message:

Password	Timing	Message view:
C	85	Connection established with server: 192.168.1.67 on port 2000
A	150	
T		

Buttons: Send, Connect, Disconnect, Close

Message view: Connection established with server: 192.168.1.67 on port 2000

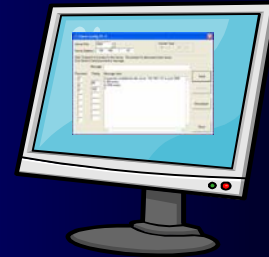
Send

The "Connection established" message is displayed here.

The salesman enters each password character followed by its respective timing interval and then presses

# P<sup>5</sup>

## Client Window



**p<sup>5</sup> Client Config V1.4**

Server Port:  Socket Type:  TCP  UDP

Server Address:

Click 'Connect' to Connect to the Server. 'Disconnect' to disconnect from server.  
Use Send to Send password or message.

Message:

Password	Timing	Message view:
<input type="checkbox"/> C	<input type="text" value="85"/>	Connection established with server: 192.168.1.67 on port 2000
<input type="checkbox"/> A	<input type="text" value="150"/>	C (85 msec)
<input type="checkbox"/> T	<input type="text"/>	A (150 msec)
<input type="checkbox"/>	<input type="text"/>	T
<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	<input type="text"/>	
<input type="checkbox"/>	<input type="text"/>	

Buttons: Send, Connect, Disconnect, Close

**The password and its measured timing interval results are returned (demo only) to the salesman in place of the usual acknowledgement.**

# P<sup>5</sup>

## Server Window



**P<sup>5</sup> Server Config V1.2**

Server Port:  Socket Type:  TCP  UDP

Server Address:

Click 'Start' to start the Server. 'Stop' to Stop it.

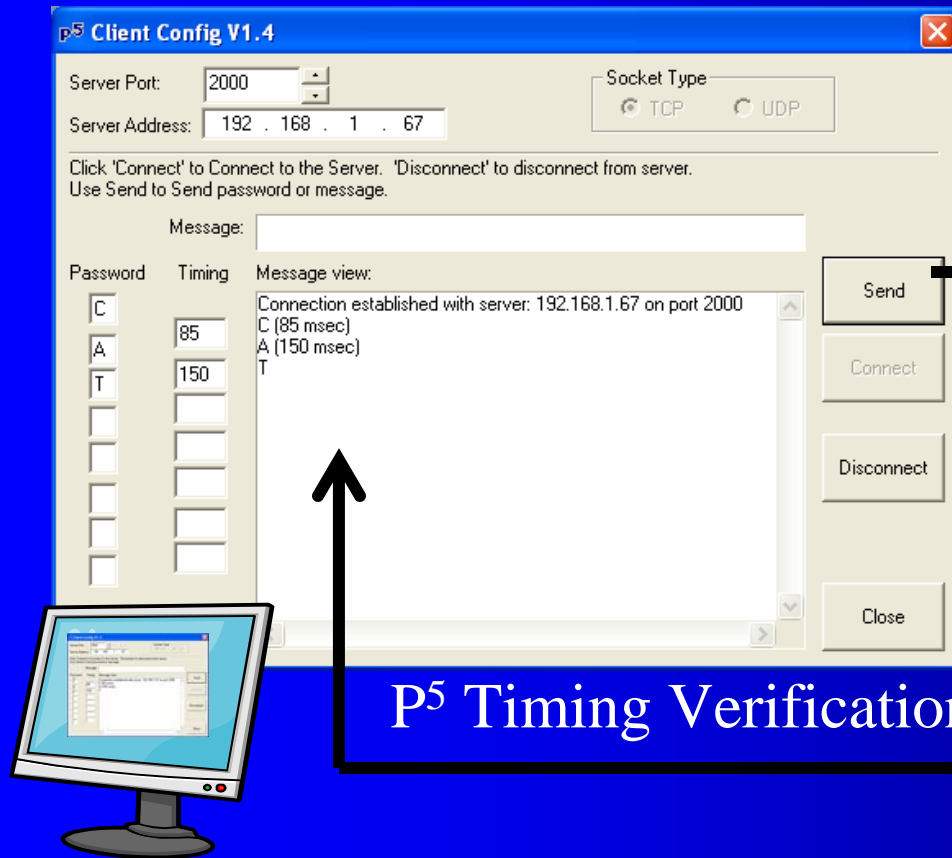
Message view:

```
Server: RMSDELL, @Address: 192.168.1.67 is running on port 2000
Connection Established
Server: RMSDELL, @Address: 192.168.1.67 is running on port 2000
C (85 msec)
A (150 msec)
T
```

The password and its measured timing interval results are displayed at the factory Server (demo only).

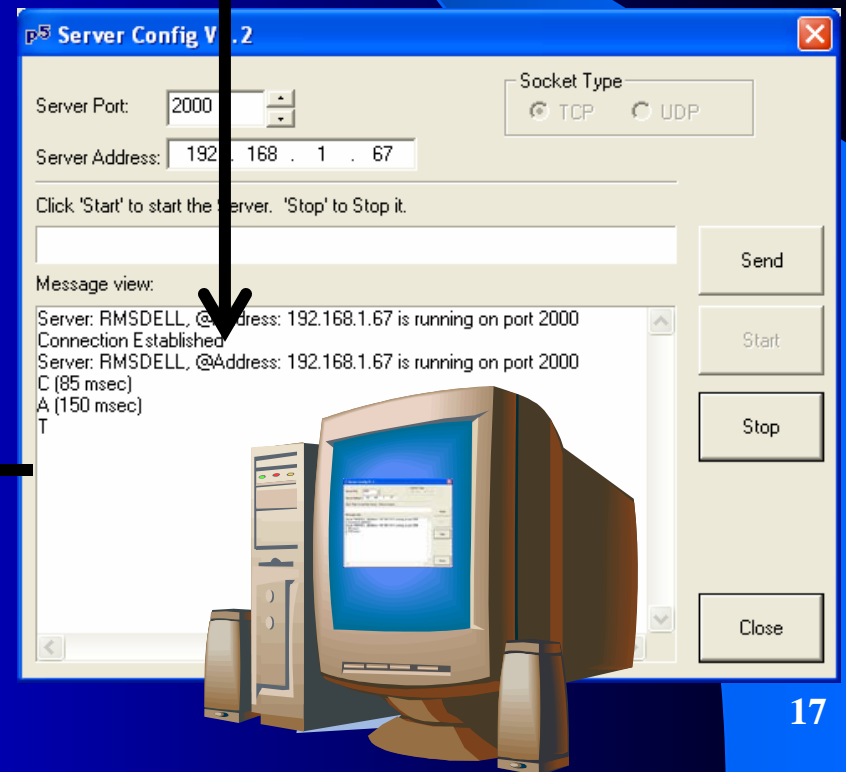
# P<sup>5</sup>

## Client & Server Windows



P<sup>5</sup> Timing Verification

Sending P<sup>5</sup>



# P<sup>5</sup> History

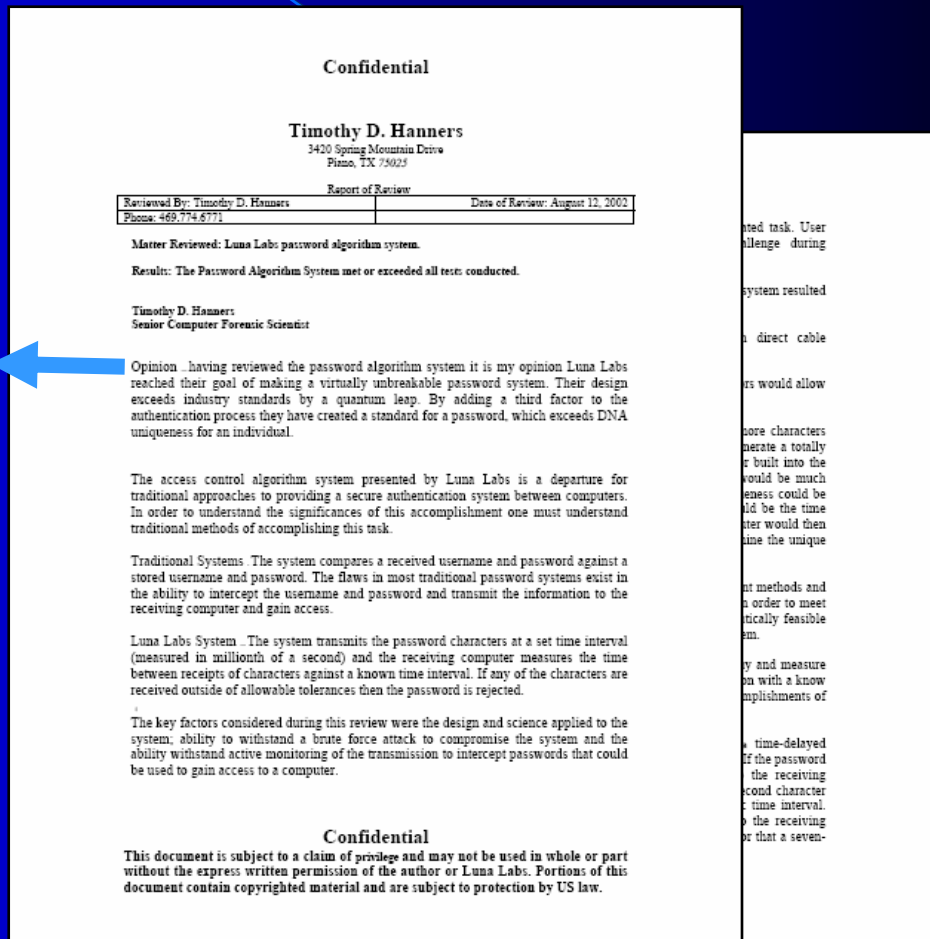
- The patent application for the password algorithm was filed in February 2001.
- Later in 2001, password software was written to demonstrate the feasibility of the password timing concept between two directly linked PCs.
- In 2002, the password software was evaluated by a banking computer analyst. His area of expertise is in secure monetary transfers. The essence of his report is shown on slide 20.
- Later that year, the password program was tested by Electronic Data Systems (EDS) and a favorable report was issued by their engineers as shown on slide 21.

# P<sup>5</sup> History (continued)

- Continuing development during 2004 and 2005 demonstrated that the concept would indeed work across the Internet.
- Patent #7,043,640 was issued for the P<sup>5</sup> password algorithm in May 2006. See file “UnitedStatesPatent\_7043640.pdf”.
- Over the years P<sup>5</sup> has evolved from a rudimentary PC to PC serial cable communication demonstration running under DOS to a sophisticated TCP/IP Windows application running over the Internet.
- The feasibility of this password program has been demonstrated over the Internet and the product is ready to be groomed for market.

# Computer Analyst's Letter

“Luna Labs reached their goal of making a virtually unbreakable password system. Their design exceeds industry standards by a quantum leap. By adding a third factor to the authentication process they have created a standard for a password, which exceeds DNA uniqueness for an individual.”

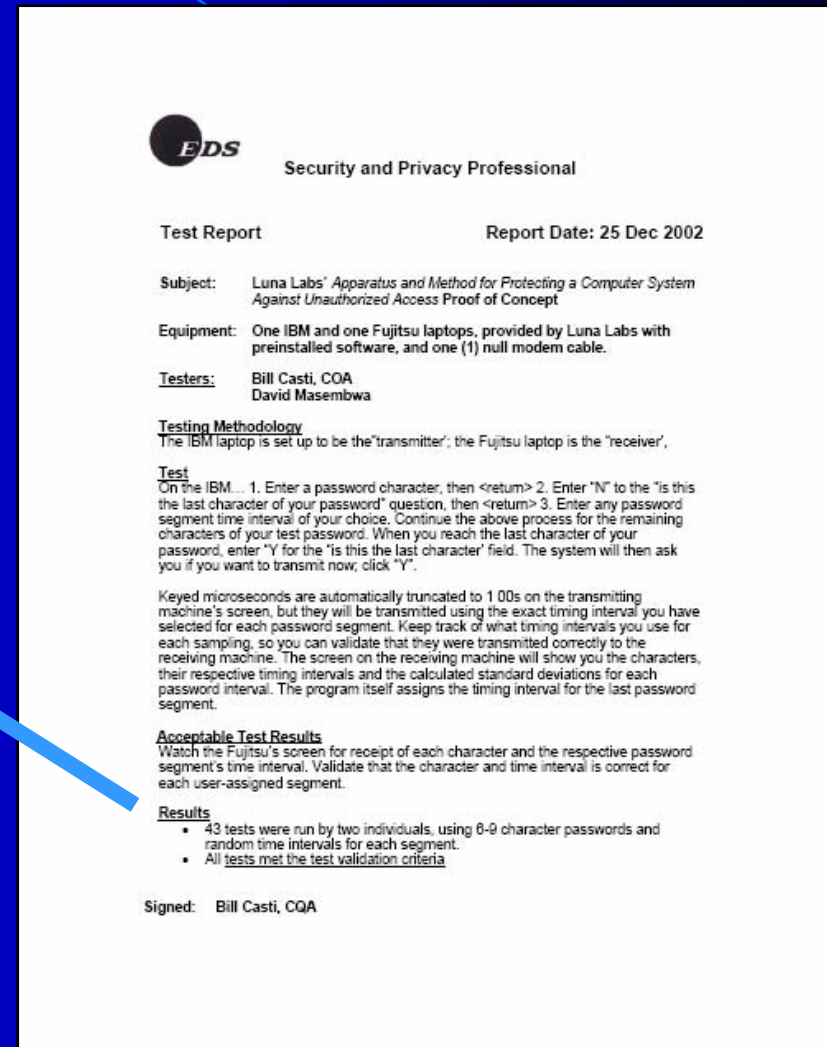


# EDS Letter

## Results

43 tests were run by two individuals, using 6-9 character passwords and random time intervals for each segment.

All tests met the test validation criteria



**EDS** Security and Privacy Professional

**Test Report** Report Date: 25 Dec 2002

**Subject:** Luna Labs' Apparatus and Method for Protecting a Computer System Against Unauthorized Access Proof of Concept

**Equipment:** One IBM and one Fujitsu laptops, provided by Luna Labs with preinstalled software, and one (1) null modem cable.

**Testers:** Bill Casti, COA  
David Masembwa

**Testing Methodology**  
The IBM laptop is set up to be the "transmitter"; the Fujitsu laptop is the "receiver".

**Test**  
On the IBM... 1. Enter a password character, then <return> 2. Enter "N" to the "is this the last character of your password" question, then <return> 3. Enter any password segment time interval of your choice. Continue the above process for the remaining characters of your test password. When you reach the last character of your password, enter "Y" for the "is this the last character" field. The system will then ask you if you want to transmit now; click "Y".

Keyed microseconds are automatically truncated to 1 00s on the transmitting machine's screen, but they will be transmitted using the exact timing interval you have selected for each password segment. Keep track of what timing intervals you use for each sampling, so you can validate that they were transmitted correctly to the receiving machine. The screen on the receiving machine will show you the characters, their respective timing intervals and the calculated standard deviations for each password interval. The program itself assigns the timing interval for the last password segment.

**Acceptable Test Results**  
Watch the Fujitsu's screen for receipt of each character and the respective password segment's time interval. Validate that the character and time interval is correct for each user-assigned segment.

**Results**

- 43 tests were run by two individuals, using 6-9 character passwords and random time intervals for each segment.
- All tests met the test validation criteria

Signed: Bill Casti, COA

# Microsoft's View on Passwords

"Any password that we can expect people to remember can be bruteforced," said Bruce Schneier, chief technology officer for Counterpane Internet Security and author of several books on security.

[print version] Password imperfect | CNET News.com Page 3 of 3

security. For the most part, two-factor authentication just adds cost, said Charles Fitzgerald, Microsoft's general manager of platform strategies.

"The move we made was driven by a security perspective, not an operational-cost perspective," he said.

In its internal push, Microsoft is piloting its own technology: it's using .Net-enabled smart cards provided by Axalto, formerly known as Schlumberger. That puts .Net, Microsoft's software platform for running software on any device, back into competition with Sun Microsystems' JavaCard software for smart cards.

The smart-card push comes after Microsoft has made a few missteps in the identity management arena. Its pint-size Windows CE for Smart Cards operating system failed to attract developers. On top of that, its Passport service, a foray into online consumer identity management, [did not win over enough service providers](#) to become useful.

Fears about e-commerce fraud are adding momentum to the smart-card drive. The password issue is a lurking iceberg, and e-commerce sites, financial institutions and other large companies have only seen the tip of it, said Prakash Ramamurthy, vice president of products and technology for Oblix, a maker of identity management systems. Consumers and employees have multiple accounts holding personal information, and an attacker only has to find the one with the weakest security.

"Identity is one thing that is being duplicated," Ramamurthy said. "And when you have that information more than once, you have a security hole."

For the moment, Microsoft's plugging of that hole in its internal systems is not being carried over to its technology for consumers. People with password worries will have to wait and see whether the company puts any provisions in place in its software.

"Enterprises are more willing to invest to solve the problems," Microsoft platform strategist Fitzgerald said. "On the consumer side, I am not saying that we are doing nothing in that space, but the things that we have talked about over the last few weeks have little to do with consumers."

[Copyright](#) ©1995-2006 CNET Networks, Inc. All rights reserved.

Pro: No connection to PC needed.  
Con: Device could be forgotten or stolen; requires user to input the mathematically generated sequence; only good for computer and network access.  
**Biometric reader**  
What: Technology based on a human trait that can be used to identify a person, most often a fingerprint.  
Pro: Biometrics cannot be forgotten or stolen; can be used for building and network access.  
Con: Expensive to deploy; recognition problems can occur.  
Source: CNET News.com

What: A matchbox-size device that generates a sequence of numbers acting as a one-time password.

http://news.com.com/2102-7355\_3-5475264.html?tag=st\_util\_print 8/6/2006

http://news.com.com/2102-7355\_3-5475264.html?tag=st\_util\_print 8/6/2006

# ARC Network Security White Paper

“The traditional barriers to adding network security technology to embedded systems have been performance bottlenecks due to computationally-intensive cryptography algorithms and significant memory requirements.”

**ARC Provides Network Security Solutions for Embedded Applications**  
www.ARC.com

Nearly all of data...  
extremely well be...  
explosion in the m...  
and TCP/IP. These...

To companies pro...  
efficiency by gatti...  
such networked a...  
network, publicize...

With an increas...  
occurring over the...  
ity. The traditi...  
book. The due to...  
barriers are now...  
Adoption is being...  
to perform cryptog...

**TCP/IP Secto**  
The three major se...  
means that the ser...  
means that no one...  
received has not...

Although TCP/IP...  
contributed to the...  
order to handle a...  
Consequently, pe...  
anyone who has I...  
IP networks for su...

**IPSec and SSL**

Several protocols address the security vulnerabilities of TCP/IP. The two most common are IP Security (IPSec) and Secure Socket Layer (SSL). These protocols use complex algorithms for encryption and authentication, including Data Encryption Standard (DES), Advanced Encryption Standard (AES), Message Digest (MD5) and Secure Hashing Algorithm (SHA). These algorithms are used to protect data integrity and confidentiality using encryption techniques, and to establish and ensure the identity of the data's originator using authentication techniques.

IPSec and SSL both address the network security issues of confidentiality, authentication, and integrity. However, they do so in slightly different ways because they operate at different layers of the protocol stack.

**IPSec vs SSL**

```
graph TD
    subgraph SSL_Stack [SSL]
        S1[SSL]
        T1[TCP/UDP]
        I1[IP]
        E1[Ethernet]
        S1 <--> T1
        T1 <--> I1
        I1 <--> E1
    end
    subgraph IPSec_Stack [IPSec/IKE]
        T2[TCP/UDP]
        I2[IP]
        E2[Ethernet]
        T2 <--> I2
        I2 <--> E2
    end
    I2 <--> IKE[IPSec/IKE]
```

SSL operates at the transport layer of a TCP/IP stack, above the TCP and UDP layers, and just below the application layer. IPSec operates at a much lower part of the stack in the network layer.

IPSec is used for configurable and highly controlled secure access to a private network. It can work with any TCP/IP application above the IP layer, including web, e-mail, and file transfer applications, as well as terminal services, IP telephony, and other client-server applications. SSL, on the other hand, is used for secure web access to a publicly available website. Because it operates at the transport layer, a limited number of applications can be used with SSL, mainly web, e-mail, and file-transfer applications. Other applications that use SSL are often accessed with a customized web browser-based front-end. Currently, only IPSec supports User Datagram Protocol (UDP)-based applications, such as audio and video streaming. There is no standard method for securing UDP communication with SSL.

SSL and IPSec offer similar types of encryption and authentication. In terms of overall security, IPSec can be considered more secure than SSL for a number of reasons. Because IPSec requires specially-configured software on both the client and server side, it offers more security than an SSL solution, which could permit access from unknown users.

© 2004 ARC International -2- Network Security white paper

# P<sup>5</sup> Patent Abstract

## USPTO PATENT FULL-TEXT AND IMAGE DATABASE

[Home](#)[Quick](#)[Advanced](#)[Pat Num](#)[Help](#)[Bottom](#)[View Cart](#)[Add to Cart](#)[Images](#)

(1 of 1)

United States Patent

7,043,640

Pritchard, et al.

May 9, 2006

Apparatus and method for protecting a computer system

### Abstract

There is disclosed an apparatus and method for protecting a computer system by providing an improved password to prevent unauthorized access to the computer system. The apparatus of the present invention generally comprises a password controller capable of comparing a received password attempt with a stored password. The stored password of the present invention comprises a time envelope that comprises at least one password segment comprising: 1) an entry event, 2) a predetermined time interval following the entry event, and 3) a terminating signal to mark the end of the password segment. Access to the computer system is authorized when password segments of a password attempt match the corresponding password segments of the stored password. The stored password of the present invention generally comprises groups of computer readable characters separated by time intervals of variable length. A time delay is added to each response to a password attempt in order to conceal the length of the time intervals within the stored password.

Inventors: **Pritchard; James B.** (Fairview, TX); **Calcote; Clyde R.** (Richardson, TX)

Appl. No.: **783049**

Filed: **February 14, 2001**

# P<sup>5</sup> Summary

- Requires less computer processing and memory overhead than encryption/decryption schemes.
- Renders password character “sniffer” programs useless.
- Password timing intervals may be changed dynamically upon each successful computer link-up over the Internet. (Supports rolling timing intervals)
- Increased security with each additional character and time interval added.
- The power of high speed or multiple computer attacks is reduced to zero if the timing criteria is not met. *Hackers will not have the patience necessary to break in even though they understand the essence of the algorithm (ie. 42 trillion tries).*

# P<sup>5</sup>

## Summary (continued)

- No key fob or additional hardware is required.
- Works on small to large LANs as well as the Internet.
- Ideal for embedded microprocessor applications with limited memory and slower processing speeds.
- Lower processing overhead enables frequent verifications during computer Internet transactions.
- Immune to computer dictionary and phishing attacks.

# P<sup>5</sup> Security Applications

- Credit card verification terminals,
- Home banking transactions,
- Point of sale terminals,
- Utility (Electric, Gas, Water, ...) networks,
- Factory automation networks,
- Embedded applications,
- RFID communication, Smart cards,
- Military radio, phone and satellite communications.

# Virus Trap Patent Award

- During the P<sup>5</sup> password development, an additional security device called a “Virus Trap Computer” was conceived.
- A patent for this device was applied for in May of 2001.
- Subsequently, patent #6,931,552 was issued in August 2005.
- The final two slides depict the abstract and diagram for the Virus Trap Computer.
- The Virus Trap Computer is easily implemented as a PCMCIA card for a laptop or as a PCI card for a desktop computer.
- 41 Patent Claims see “UnitedStatesPatent\_6931552.pdf” file.

# Virus Trap Abstract

## USPTO PATENT FULL-TEXT AND IMAGE DATABASE

[Home](#)[Quick](#)[Advanced](#)[Pat Num](#)[Help](#)[Bottom](#)[View Cart](#)[Add to Cart](#)[Images](#)

(1 of 1)

United States Patent

6,931,552

Pritchard, et al.

August 16, 2005

**Apparatus and method for protecting a computer system against computer viruses and unauthorized access**

### **Abstract**

There is disclosed an apparatus and method for protecting a first computer system against an intrusion such as a computer virus or an unauthorized access. The apparatus comprises a second computer system that is coupled to the first computer system in a manner that permits the second computer system to receive all computer communications that are directed to the first computer system. The second computer system detects an intrusion before the intrusion reaches the first computer system. The second computer system deletes the intrusion by deleting the operating system and all other data on the second computer system. After the compromised operating system and data have been erased, a clean version of the operating system and data is supplied to the second computer system from a restoration controller within the second computer system, or from the first computer system, or from a backup copy of the clean version of the data.

Inventors: **Pritchard; James B.** (Fairview, TX); **Calcote; Clyde R.** (Richardson, TX)

Appl. No.: **09/847,757**

Filed: **May 2, 2001**

# Virus Trap Diagram

US 6,931,552 B2

APPARATUS AND METHOD FOR PROTECTING A COMPUTER SYSTEM AGAINST COMPUTER VIRUSES AND UNAUTHORIZED ACCESS

James B. Pritchard, 660 Meandering Way, Fairview, Tex. 75069 (US); and Clyde R. Calcote, 1009 Serenade La., Richardson, Tex. 75081 (US)

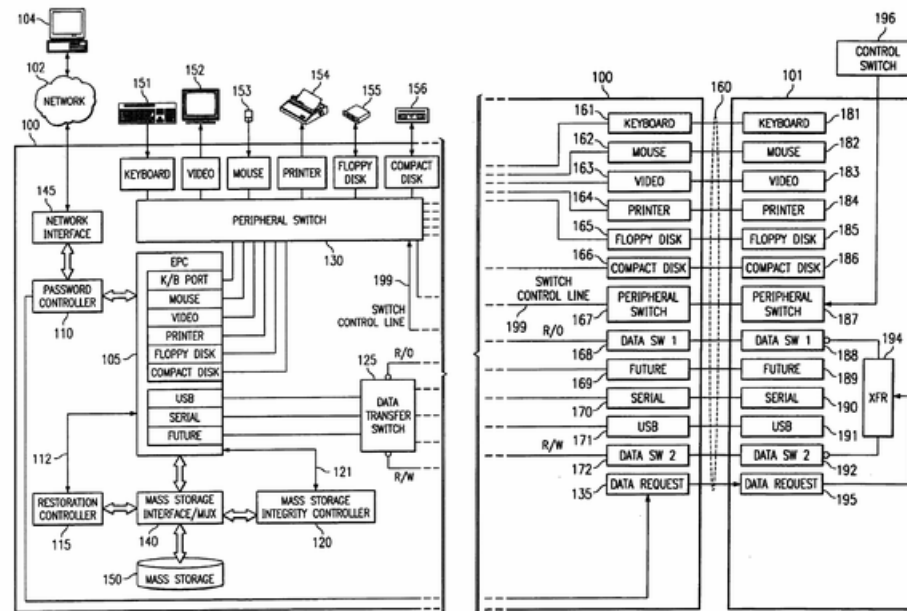
Filed on May 02, 2001, as Appl. No. 9/847,757.

Prior Publication US 2002/0166067 A1, Nov. 07, 2002

Int. Cl.<sup>7</sup>H04L 9/00

U.S. Cl. 713—201

41 Claims



28. A virus trap for protecting an associated host computer from a computer virus received from an external source, said virus trap comprising:
- a mass storage device for storing data and application programs;
  - an embedded processor for controlling the virus trap and running the application programs;
  - a password controller for receiving and verifying a first-level password from the external source;
  - means, responsive to a positive verification of the first-level password, for receiving communications from the external source and supplying the communications to the embedded processor;
  - an integrity controller for monitoring the data and application programs to detect unauthorized read or write operations; and
  - a restoration controller, responsive to a detection of an unauthorized read or write operation, for taking corrective action to erase corrupted data and/or applications associated with the detected unauthorized read or write operation, and to restore the erased data and/or applications with uncorrupted data and/or applications.