

# A Paradigm Shift in Remote User Authentication Systems

By **Tara Chand**  
*chand@CyberSecureInc.com*

## Introduction

The information security industry is stuck in the old paradigm of passwords, tokens and biometrics. It is ever busy refining these technologies, even when it has become abundantly clear that the information security world has changed. These technologies have severe cost, security, scale and logistical implications as well as limitations that have been well covered by the news media.

It is in the nature of a shift in paradigm that such a shift would come from someone who is not part of the establishment that has lived the old paradigm for so long. Many people may not believe or even disparage such a new paradigm, if it did not come from those they trust or revere, such as: large established companies; university scientists funded by NSF; or even an industry consortium. The new paradigm succeeds on its merits and on its ability to decidedly solve the serious problems of the old paradigm that have surfaced in the last few years and have become apparent to many in the industry.

## The New Paradigm

The new paradigm has been named NRUAS, where N stands for new. This new shift in the old paradigm is simply that this technology delivers strong authentication without passwords, security tokens and even biometrics and does so by a unique combination of existing long-held and proven security concepts. The new paradigm NRUAS has a huge impact for the better; see Figure 1.

This technology uses COCB and DTMF-PIN as the two factors of authentication. They will be described a little later here. These two factors are closely integrated with the remote person being authenticated. Since this integration delivers more than just a combination of two separate authentication factors, NRUAS is referred to as a two-factor plus strong authentication.

The uniqueness and eventual success in the marketplace of this technology lies in three attrib-

NRUAS ® A Paradigm Shift		
Current RUAS	Security Issues	NRUAS
Password  Or  Complex Password	<ul style="list-style-type: none"> <li>• Create, Memorize, Save/Write Down</li> <li>• Social Engineering - Phishing</li> <li>• Dictionary Attack, Static Passwords</li> <li>• Delivery By E - mail</li> <li>• Key Stroke Logging</li> <li>• Spyware Risk</li> </ul>	BY BEING INNOVATIVE, NRUAS DOES NOT INHERIT THESE WEAKNESSES AND LIMITATIONS OF PASSWORDS.
Password Plus Security Token	<ul style="list-style-type: none"> <li>• Logistics Of Carrying A Security Token</li> <li>• Cost Of Security Token-Based System</li> </ul>	NRUAS DOES NOT INHERIT THESE ISSUES OF SECURITY TOKENS.
Password Plus Biometrics	<ul style="list-style-type: none"> <li>• Cost And Reliability Of Biometric Sensors</li> <li>• Create And Maintain Biometric Sample Database</li> </ul>	NRUAS DOES NOT INHERIT THESE ISSUES OF BIOMETRICS.

Figure 1: NRUAS, A Two factor Plus Remote User Authentication Technology

utes: (i) what are these two-factors and how well do they integrate with a human, as a human is an integral part of the authentication process, (ii) significant cost advantage, and (iii) infinitely scalable across large customer/employee base. The cost and scalability would be the most important attributes for those who would deploy this technology.

Humans, while they all look alike, are very different. Any technology that touches them has to take that human factor into account. Hence, the new paradigm of NRUAS creates no new burdens but does away with old paradigm burdens. It eliminates having to create and memorize and use long or complex passwords, having to carry extra security devices, and supplying one's own biometrics.

## How This Technology Works

1. The person being authenticated makes a voice call (without speaking) using the existing telephone infrastructure, from

- his/her phone, any phone, cell, office, or home, to a designated phone number.
2. The NRUAS IVR server picks up the phone call and would automatically detect whether it is a cell phone, or other phone, and if the caller id is pre-registered.
3. If the caller id maps to a known cell phone, having been routed by a cell carrier, the NRUAS IVR prompts for keypad entry of a DTMF PIN.

**Note:** [DTMF PIN, while it is entered as a numeric, is communicated as a multi-frequency tone to the IVR. It is unlike the PIN entered on an ATM; that is communicated as data.]

4. If the caller id does not map to a known registered cell phone, the IVR server prompts for entry of a telephone number as an identification, and a 4-digit PIN and then advises the caller to hang up the phone. Within five seconds, IVR server

calls the caller back on a pre-stored caller id and prompts for the entry of the same numeric 4-digit PIN.

5. If the NRUAS server, by either CO or COCB and DTMF PIN, is successful in authenticating the caller, the NRUAS logic then generates a short random pass key (RPK) and voice delivers it to the caller, with a time limit during which it would work.

**Note:** [COCB refers to **Call Origination**

**Call Back**. Where the **CO** cannot be verified by NRUAS, **CB** is used in addition to **CO**. Hence this factor is called COCB.]

6. The caller on a login window uses their primary phone number as user id and uses the just received RPK as the password.
7. The business's existing authentication system identifies the caller and authenticates the caller, using the RPK and then allows access to the authorized application server. The NRUAS server then deletes the RPK after a limited time or one-time use.

**Note:** Steps 1 to 7 may typically take 15 seconds.

### Important Things to Note:

- a. The RPK has the attributes of being Ultra short and Ultra fast, as it is usually a 4-digit alphanumeric that is good for 15 seconds. However, NRUAS enables the RPK to be customized to the needs of its users and the system they are logging in by customizing the length of RPK, the time it is good for (minutes, hours or days) and from which remote person's phones COCB factor can work.
- b. The phone used in this technology is not a security device in the sense of the security token, as no formulas are executing within it. Hence losing a phone is not like losing a security token. Cell phone companies generate the cell phone caller id, not the phone itself, by mapping the SIM or device MAC to an account number and its status and then to the caller id.
- c. Phones, and specifically cell phones, are the most widely used infrastructure. In digital phones, the control information and voice channel are encrypted and are not subject to cloning or eavesdropping.
- d. The DTMF PIN is a 4- to 6-digit numeric and even though it acts as a something-you-know factor, it is unlike a traditional password. Multiple incorrect entries of DTMF-PIN, as few as 2 or 3, disable the

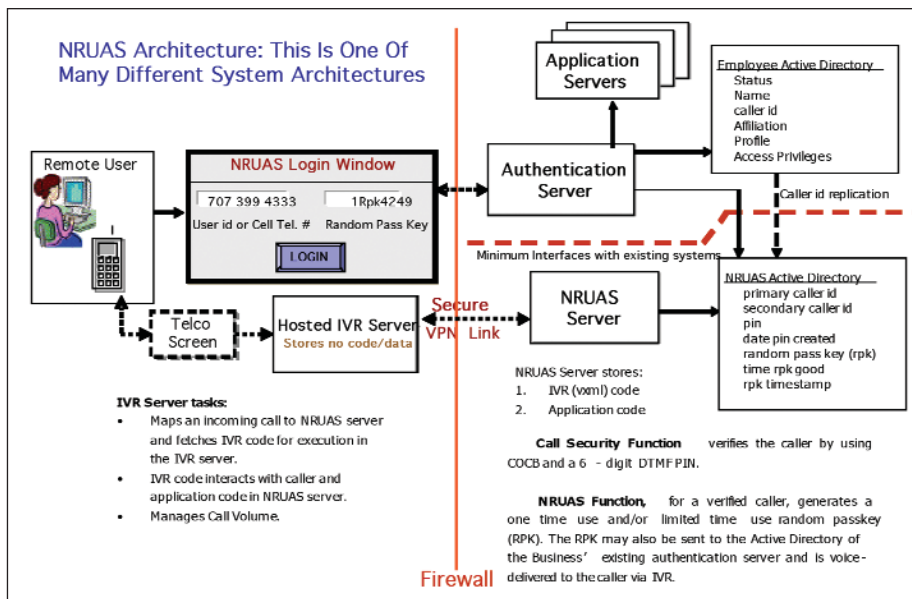


Figure 2: NRUAS Implementation Architecture

login, requiring system administration intervention.

- e. Some users may prefer RPK delivery by short messaging system (SMS). However, SMS uses a data packet store and forward network like an Internet and may be subject to hacking. Hence NRUAS prefers a real time voice delivery to ensure a remote person is in the loop. Each authenticated call generates a new RPK and can be obtained anytime from anywhere.
- f. This technology relieves the human as well as the business's existing authentication/application server from creating, remembering, keeping safeguarding, resetting a password, and complexity and logistics of a token or smart cards-based second factor.

### Deployment Architecture


The deployment architecture embodies systems engineering and security principles such as, separation of systems, compartmentalization of data, and need to know. See Figure 2.

This technology uses and depends on the Interactive Voice Response (IVR) systems. IVR is a highly reliable, versatile and mature technology that is in widespread use by many in the industry. The use of IVR is growing rapidly in the banking and other industries for access to Web applications and the ability to pull data from large databases. There are many standard platforms that can handle large call volume of very short durations such as those that are used by this technology.

The architecture is such that the server does not touch or use any employee or customer data. IVR server does not store any code or data. NRUAS can be incrementally deployed to work within existing systems with virtually zero training costs. It uses the most widely used existing login user interface. Telco Screen, implemented in the Telco, prevents DoS attacks on the IVR server.

### Conclusion

NRUAS, the paradigm shift in remote user authentication, delivers strong authentication without passwords, security tokens and even biometrics and does so by a unique combination of existing long-held and proven security concepts. It uses COCB and DTMF-PIN as the two factors of authentication. These two factors are closely integrated with the remote person being authenticated, and thus make it a two-factor plus strong authentication.

This technology has three distinct and valuable attributes of: (i) the two factors integrate with a human, as human is an integral part of the authentication process, (ii) significant cost advantage, (iii) infinitely scalable across large customer/employee base. These attributes make the NRUAS flexible, robust, secure and economical technology and architecture to deploy. 

*Tara Chand is President of Cyber Secure, creating innovative information security and identity theft solutions.*

Note: NRUAS, COCB, DTMF-PIN, RPK, Ultra short, Ultra fast, and Telco Screen are service marks of Cyber Secure Inc.