Telelogin: a Two-factor Two-path Authentication Technique Using Caller ID

Haruhiko Fujii†, *Naoko Shigematsu, Hirohiko Kurokawa, and Tetsuya Nakagawa*

Abstract

This article introduces Telelogin, a two-factor two-path authentication technique for user authentication that uses caller ID (calling number notification function) in addition to user ID and password authentication over the Internet. This technique achieves highly secure personal authentication through the simple act of making a phone call.

1. Importance of stronger personal authentication

The Japan SOX Law established a few years ago requires banks and businesses to strengthen their internal controls and the security of network transactions. Banks are also taking measures against the problems of ID and password theft by phishing or spyware in response to directions from the Ministry of Finance for financial organizations to bolster the authentication process used for Internet banking.

Two-factor authentication is emerging as the mainstream approach for strengthening the security of network transactions and Internet banking. It supplements the conventional authentication by user ID and password (information supplied from the user from memory) by adding authentication by a smart card or random number table or other thing possessed by the user or biometric authentication by, for example fingerprint or blood vein pattern recognition.

However, these authentication methods have suffered from problems such as complex operation or input, requirements for special devices, and costly initial distribution and operation. Telelogin is a new two-factor authentication technique that has been attracting attention as a means of solving those problems.

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
Email: telelogin@lab.ntt.co.jp

2. Outline of Telelogin

The basic principle of this two-factor authentication is for the ID entered by a user from a terminal to be sent over the network and the telephone number sent from the caller's phone during a phone call (caller ID feature) to be registered with the service system. If this authentication is successful, the service is provided to that user (**Fig. 1**). This basic method has been patented by NTT Information Sharing Platform Laboratories.

2.1 Features of Telelogin

The special features of Telelogin are listed below.

(1) Security is high because two different routes are used—the Internet and the telephone network—and because two factors are used: the user's ID/password and the user's phone number.

(2) The additional process required for authentication is only a simple telephone call, which eliminates entry errors and is easy for the user to do.

(3) The cost of introducing new hardware is reduced by eliminating both the in-advance distribution of hardware or software, such as tokens or smart cards, electronic certification or i-appli (Java application on cell phone), and

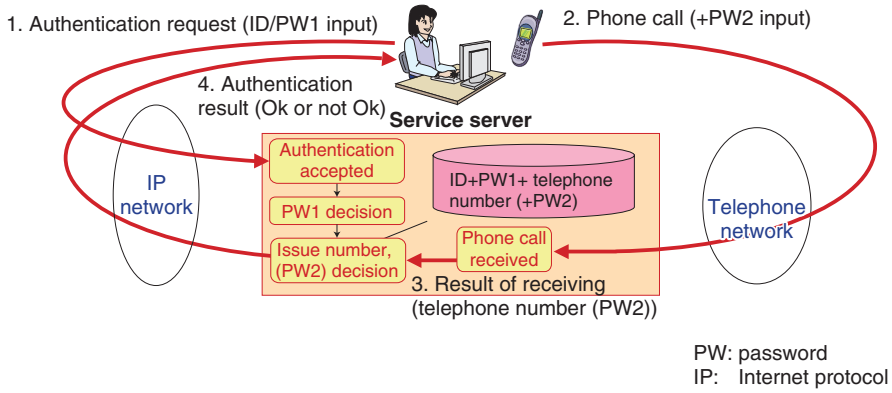

Fig. 1. Basic principle of Telelogin.

their maintenance.

(4) The crime prevention capability is high because a record of calls is kept.

(5) Various kinds of cell phones that are already in wide use can be used, so the barrier to system introduction is low.

(6) The system has wide applicability for real-world authentication such as for automatic teller machines (ATMs) as well as authentication for the Internet and remote access virtual worlds.

2.2 Proof of the calling number

The Telelogin authentication method is premised on the cell phone caller's number being genuine, and not falsified. Up to about 2005, fraudulent acts involving falsified caller ID (telephone fraud) were a problem. As measures to prevent such crimes, the Telecommunication Carriers Association formulated the Calling Number Falsification Countermeasure Guidelines in July 2005. On April 1, 2008, the Ministry of Internal Affairs and Communication put into effect the Partial Revision of the Commercial Telecommunication Facility Regulation. Following those guidelines, the various carriers implemented measures such as not forwarding the calling number for calls for which there is doubt about caller ID falsification [1].

2.3 Comparison with other additional authentication methods

Various additional authentication methods are compared in **Table 1**. Telelogin satisfies the requirements for security, convenience, and cost performance. It does involve call charges because a telephone call is made for each authentication, but the call time is only about one second per authentication. If a toll-free number service is used, there is no burden on the user.

3. Configuration of Telelogin functions

The Telelogin authentication function is divided into an authentication function layer for processing authentication requests from various service applications and telephone function layer for simultaneously performing the processing required to receive and answer multiple telephone calls. The configuration of the Telelogin authentication functions is illustrated in **Fig. 2**. The telephone function layer has an interactive voice response (IVR) function for receiving and answering telephone calls. It performs voice recognition processing or voiceprint authentication processing as needed in response to the user's dialing. The authentication function layer has an interface function for Active Directory, RADIUS (remote authentication dial in user service), and other existing authentication protocols. It also manages a database for IDs, passwords, and telephone numbers and sends the authentication result to the upper service provision layer according to information from the telephone function layer.

4. Telelogin application examples

Some examples of applications are login permission for Internet banking and secondary authentication for the transfer of funds for financial organizations because they use two-factor authentication [2]. If IDs and passwords have been disclosed by phishing or eavesdropping in Internet banking, the funds in the user's account might be stolen by a malicious third

Table 1. Comparison of authentication methods.

		Telelogin	One-time password	Smart card	Biometric
Security	Preventon of impersonation by an attacker	Good Difficult to falsify calling number	Good Difficult to guess	Good Difficult to duplicate	Excellent Difficult to forge
	Prevention of theft	Good Cell phone theft is easily noticed; cell phone can be disabled remotely.	Poor Theft unnoticed	Poor Difficult to notice theft	Excellent No theft
Usability	Ease of operation	Excellent Easy authentication by telephone	Poor Difficult to use by the elderly	Excellent Easy	Excellent Easy
	Use of special hardware	Good A cell phone is all that is needed	Poor Requires special token, different for each service	Fair Requires smart card for each service	Excellent No need for extra hardware
Economy	Initial cost (to strengthen authentication)	Excellent Registration of cell phone telephone number is all that is needed	Fair Requires token	Fair Requires smart card reader	Poor Requires expensive specialized hardware; difficult to install in ordinary user terminals
	Running cost (to strengthen authentication)	Fair Charge for call	Poor Expense of token maintenance and management	Fair Expense of card maintenance and management	Poor Requires maintenance and management of expensive special hardware.

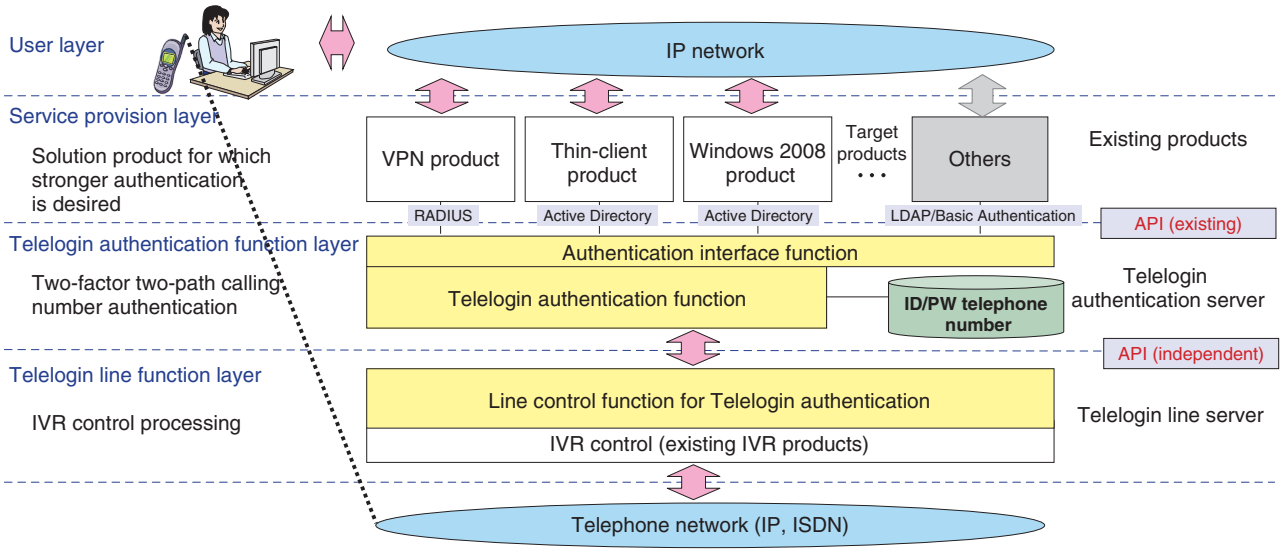

Fig. 2. Configuration of Telelogin authentication functions.

party. Telelogin protects user funds by strengthening the security of authentication. The Telelogin operation for user login in Internet banking is illustrated in **Fig. 3**.

Another application example is login authentication in measures used to strengthen control within corporations (thin client systems, remote access gateways, etc.). Such solutions were originally designed

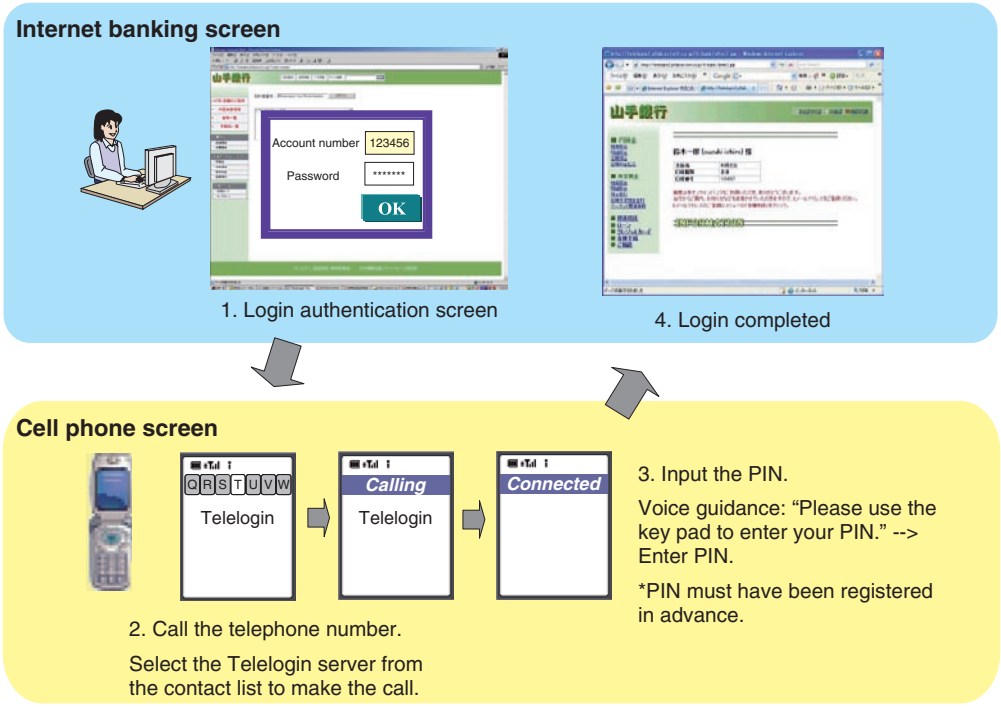

Fig. 3. Internet banking login authentication application example.

to prevent the theft of important software or data from personal computers and other such devices used outside the company for remote access to servers and computers within the company rather than for storing software or important information in the devices used outside the company.

Even with these solutions, however, there is still a risk of data leaks through the theft of IDs and passwords. The risk can be reduced by using Telelogin to strengthen authentication. The Telelogin operation for user login from a thin client is illustrated in **Fig. 4**.

5. Service models

Broadly speaking, we can consider two types of Telelogin service models: the network service model (for application service providers (ASPs)) and the system integration model.

The network service model provides Telelogin authentication to customers as an ASP service included in the calling charges. As shown in **Fig. 5(a)**, a Telelogin authentication server and a Telelogin line server are placed in the ASP center and managed by the ASP. The Telelogin line server receives the customer's call via a toll-free number or other means for which the receiver bears the call charges and detects the calling number. The Telelogin authentication server uses the caller's number it receives from the Telelogin line server to perform the authentication. The thin client server or other service server that requires Telelogin authentication is installed in the customer's environment and connected to the ASP center via a line (e.g., a leased line or virtual private network (VPN)). The sharing of facilities with other customers makes the initial investment and operating cost lower.

The system integration model is for customers who want to embed Telelogin authentication in their own environment. As shown in **Fig. 5(b)**, in addition to the service server, the Telelogin authentication server, the Telelogin line server, and the telephone line that receives the Telelogin authentication telephone are all in the customer's own environment, so there is no sharing of facilities with other customers. The model can be selected according to each customer's service requirements, so a flexible response to customer needs is possible.

6. Future plans

We will proceed with the production of Telelogin products by NTT Group companies. Then, the NTT Group companies plan to expand to commercial thin-client systems and remote access gateway products

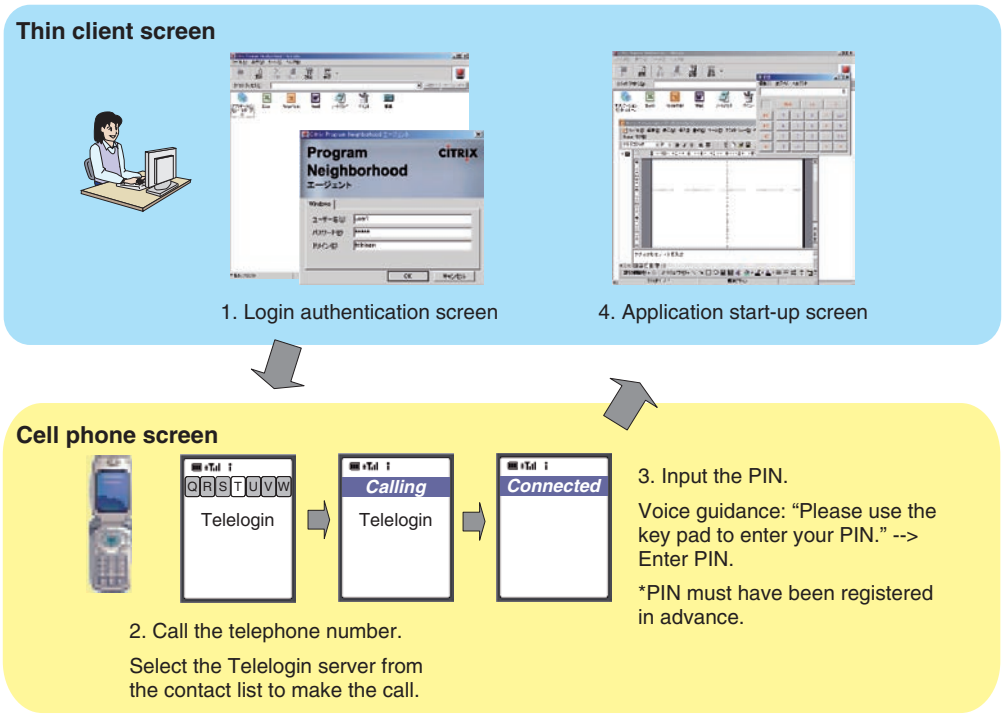

Fig. 4. Thin client login authentication application example.

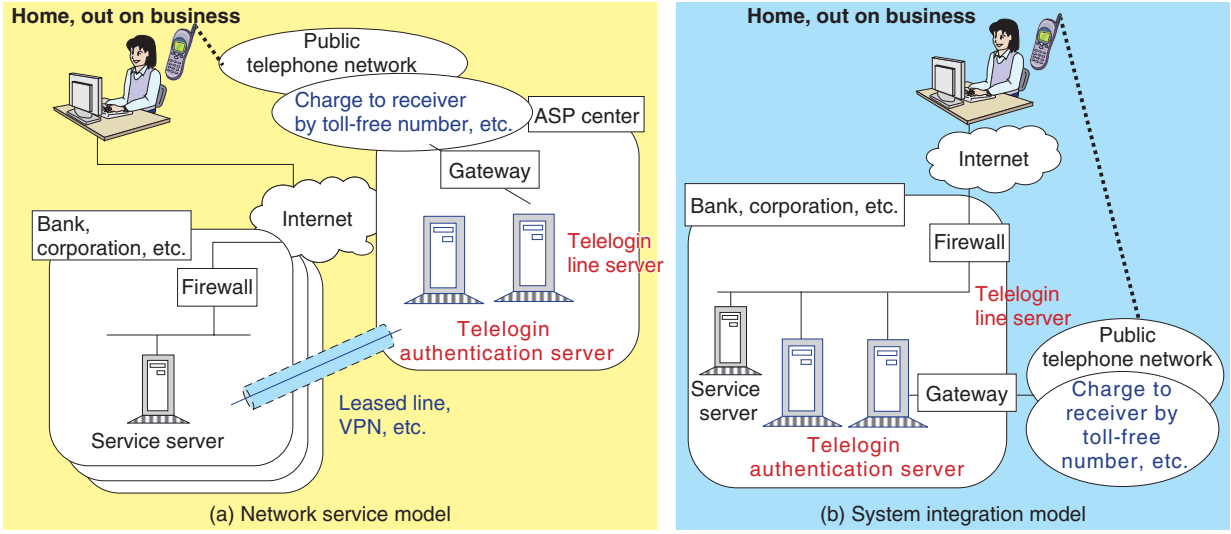

Fig. 5. Service model example.

such as a SSL-VPN (SSL: secure sockets layer), single sign-on products, and voiceprint authentication products. The NTT business companies also plan to provide a Telelogin authentication service for enterprises that combines a toll-free number and VPN connection as a network service.

We expect the Telelogin authentication technique to continue to expand in systems of universities, where a high percentage of students have cell phones and the frequency of access from outside is high, in local government systems, which require a high degree of convenience, and in systems provided by banks, which are seeking new authentication methods.

References

[1] http://www.tca.or.jp/japan/news/050701.html (in Japanese).

[2] H. Fujii, K. Hata, and T. Nakagawa, "Requirements for the Telelogin System," Regional Financial Organization IT Conference Report, "Trends in Financial Business using Cell Phones," Center for Financial Industry Information Systems, pp. 26–27, 2006 (in Japanese).

Haruhiko Fujii
Software Architecture Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.S. degrees in electrical engineering from Waseda University, Tokyo, in 1997 and 1999, respectively. He joined NTT Information Sharing Platform Laboratories in 1999.

Naoko Shigematsu
Research Engineer, Software Architecture Project, NTT Information Sharing Platform Laboratories.

She received the B.S. and M.S. degrees in geophysics from Tohoku University, Miyagi, in 1993 and 1995, respectively. She joined NTT Telecommunication Networks Laboratories in 1995. She moved to NTT East R&D Center in 1999. She moved to NTT Information Sharing Platform Laboratories in 2000. She has been engaged in R&D of ATM network operation systems and storage area networks for them.

Hirohiko Kurokawa
Senior Research Engineer, Software Architecture Project, NTT Information Sharing Platform Laboratories.

He received the B.S. degree in mathematics from Fukui University, Fukui, in 1981. He joined Nippon Telegraph and Telephone Public Corporation (now NTT) in 1981. From 2000 to 2002, he was engaged in R&D of smart card management systems. He is currently working on multifactor authentication systems.

Tetsuya Nakagawa
Senior Research Engineer, Supervisor, Software Architecture Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.S. degrees in electrical engineering from Waseda University, Tokyo, in 1986 and 1988, respectively. He joined NTT Transmission System Laboratories in 1988. He has been engaged in the development of Internet service provider and Internet portal services and in the planning of R&D strategy in the field of information sharing platforms. He moved to his present post in 2005.