Financial Cryptography - Feb 13, 2007

Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer

Mohammad Mannan and Paul C. van Oorschot

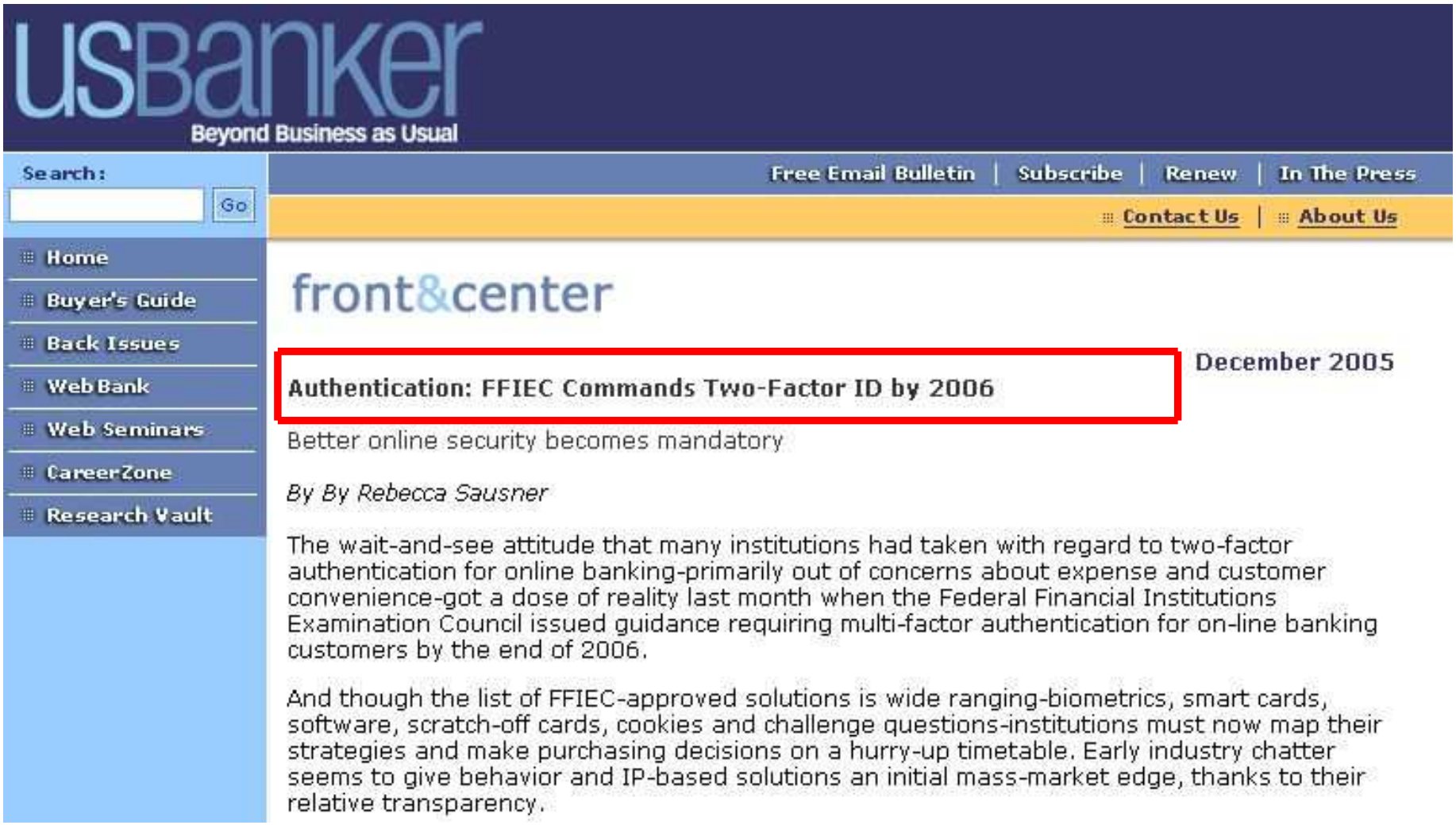
Digital Security Group

Carleton University, Canada

Web authentication in practice

1. Password-only
2. Two-factor
3. Complementary techniques, e.g.,
   - cellphone SMS
   - personal identification questions

Mandating two-factor authentication



usbanker
Beyond Business as Usual

Search: Go

Free Email Bulletin | Subscribe | Renew | In The Press

Contact Us | About Us

- Home
- Buyer's Guide
- Back Issues
- Web Bank
- Web Seminars
- CareerZone
- Research Vault

front&center

December 2005

Authentication: FFIEC Commands Two-Factor ID by 2006

Better online security becomes mandatory

By By Rebecca Sausner

The wait-and-see attitude that many institutions had taken with regard to two-factor authentication for online banking-primarily out of concerns about expense and customer convenience-got a dose of reality last month when the Federal Financial Institutions Examination Council issued guidance requiring multi-factor authentication for on-line banking customers by the end of 2006.

And though the list of FFIEC-approved solutions is wide ranging-biometrics, smart cards, software, scratch-off cards, cookies and challenge questions-institutions must now map their strategies and make purchasing decisions on a hurry-up timetable. Early industry chatter seems to give behavior and IP-based solutions an initial mass-market edge, thanks to their relative transparency.

Failure of two-factor authentication

NETCRAFT

Webserver Search

What's that site running?...

Search

Example: .google.com
Example: www.netcraft.com

Netcraft Services

News

- Subscribe to Netcraft News

Security Services

- Anti-Phishing Toolbar
- Phishing Site Feed
- Bank Fraud Detection
- Phishing Site Countermeasures
- Audited by Netcraft
- Open Redirect Detection
- Web Application Security Testing
- Web Application Security Course

Internet Data Mining

- Hosting Provider Switching Analysis
- Hosting Provider Server Count

« Previous | Up | Next »

Fraudsters Attack Two-Factor Authentication

An ongoing phishing attack against Citibank is using man-in-the-middle tactics against two-factor authentication to gain access to online banking accounts.

The second authentication factor used by Citibank is provided by a security token – a physical item possessed by an account holder – which generates a one-time password that remains valid for approximately one minute. One-time passwords are useless to an attacker if they are captured via keylogging trojans, as they will not work immediately after the victim has used them, nor will the attacker be able to gain access to the victim's account at a later date.

However, by tricking a victim into entering these items of data into a form, the attacker's site can automatically relay the authentication credentials to the real Citibank site instantly. Effectively, this allows the attacker to successfully log in on behalf of the victim.

Problems of web authentication

1. Most machines are untrustworthy
2. How to use an online service in the presence of:
    - keyloggers and rootkits
    - phishing, pharming, and DNS poisoning
    - session hijacking

Users are losing trust on the web.

Outline

- Mobile Password Authentication (MP-Auth)
- Attacks against MP-Auth
- Implementation
- Comparison of web authentication techniques
- Concluding remarks

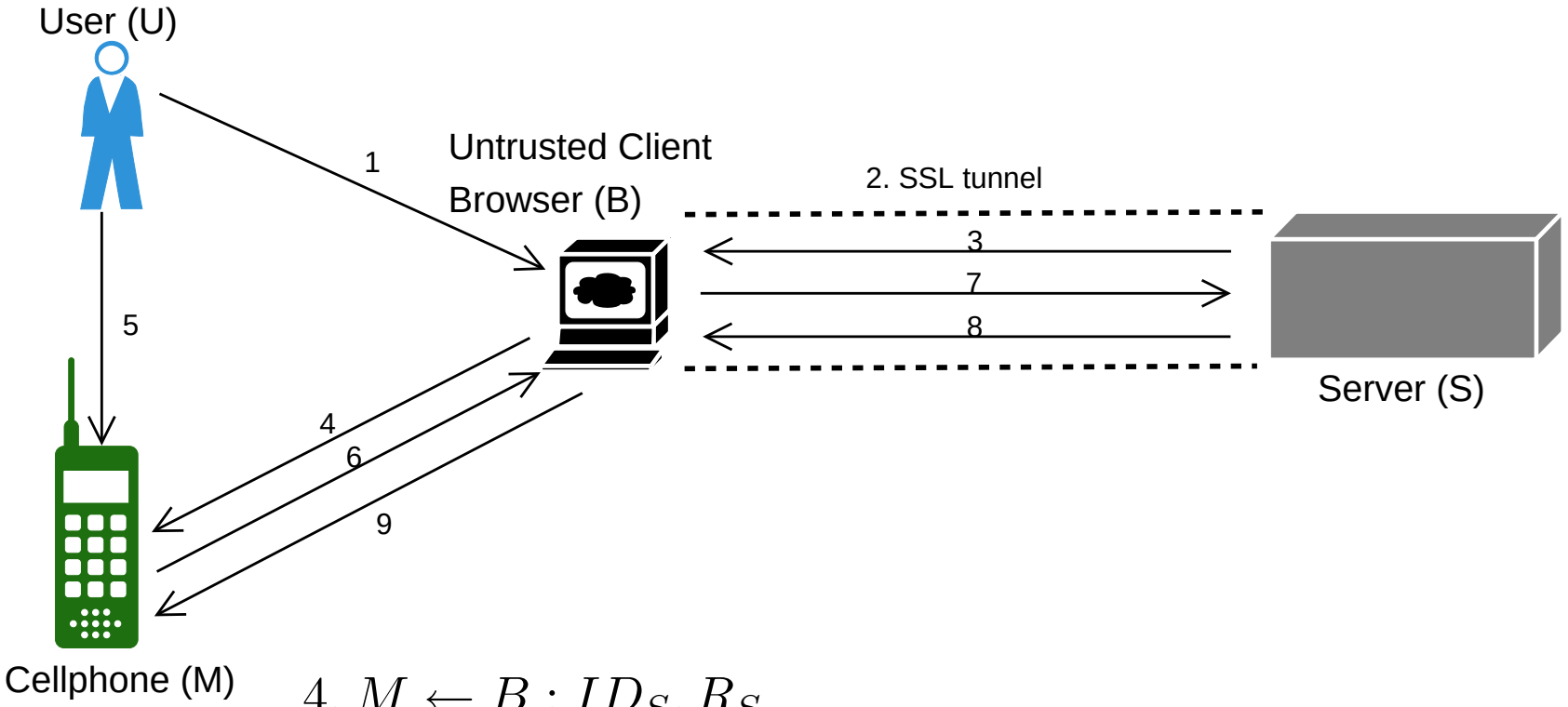
Defences provided by MP-Auth

1. Keyloggers: **separate** long-term password input from host machines
2. Phishing: **encrypt** a password with the target website's public key
3. Session hijacking: enable transaction **confirmation**

Overview of MP-Auth

1. User U loads her bank's (S) public key to her cellphone M
2. U goes to the bank's website using a browser B
3. U inputs her password P to M
4. M encrypts P using S's public key, and sends the result to B
5. B forwards the encrypted P to S, and S replies with success or fail

MP-Auth steps



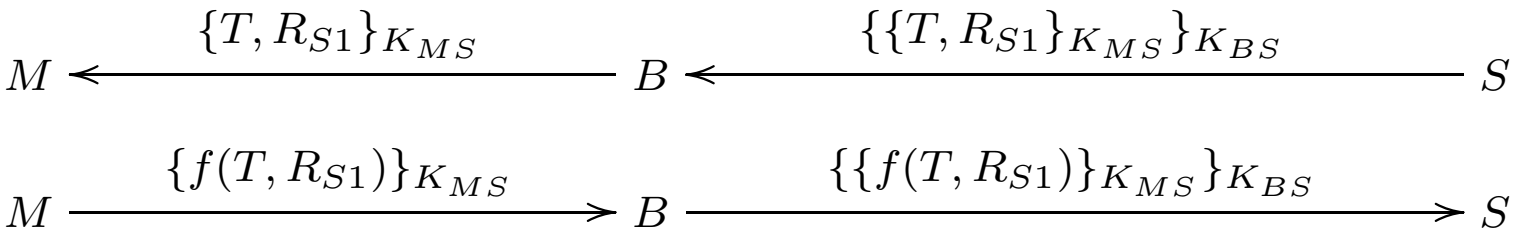
$$4.\ M \leftarrow B : ID_S, R_S$$

$$6.\ M \rightarrow B : \{R_M\}_{E_S}, \{f(R_S), ID_U, P\}_{K_{MS}}$$

$$9.\ M \leftarrow B : \{f(R_M)\}_{K_{MS}}$$

here, $K_{MS} = f(R_S, R_M)$

MP-Auth: transaction confirmation



- T: "Pay $\$25$ to Verizon", R_{S1} is nonce, K_{BS} is an SSL key
- Do we need to confirm **all** transactions?
  - maybe not

MP-Auth security

- Formal proofs: ✗
- BAN-like overview: ✓
- AVISPA protocol analysis tool: ✓

  `http://www.scs.carleton.ca/~mmannan/mpauth/`

Attacks against MP-Auth

1. Malware on a personal device
2. Common-password attack (re-used across websites)
    - PwdHash [7] might help
3. Social engineering
    - “Please enter your password on the browser”

Addressing malware on a personal device

1. Digitally signed software update
2. Limited functionality devices
    - better than hardware tokens?
3. TCG's Mobile Phone Work Group (MPWG)
4. virtualized Trusted Platform Module (vTPM [8])

MP-Auth implementation

1. Prototype: web server, Firefox extension, desktop client, Java MIDlet
2. No modifications to the web server or browser code
3. Usable performance
   - MP-Auth login is almost **eight times slower** than SSL login, but still **less than a second**
   - entering a userid and password takes much longer time

Comparing MP-Auth with existing literature

	Protection against			Requirement			
	Session-hijacking	Phishing	Key-logging	Trusted proxy	On-device secret	Trusted PC OS	Malware-free mobile
MP-Auth	✓	✓	✓				✗
Phoolproof [6]		✓	✓		✗		✗
BitE [4]			✓		✗	✗	✗
SpyBlock [2]	✓	✓	✓		—	✗	
Three-party [5]	—	—	✓		✗		✗
Camera-based [1]	✓	✓	✓	✗	✗		✗
Web-Auth [9]		✓	✓	✗	✗		✗
Guardian [3]			✓		✗		✗

Concluding remarks

1. Exploit malware-free personal device to improve web security
2. Why not browse from the cellphone?
    - does not solve phishing, DNS hijacking
3. MP-Auth is **not** foolproof – needs usability testing
    - users must be careful when confirming a transaction
4. MP-Auth may reduce impact of:
    - phishing, keylogging, and session hijacking

References

[1] Clarke et al. The untrusted computer problem and camera-based authentication. In *Pervasive Computing*, volume 2414 of *LNCS*, 2002.

[2] C. Jackson, D. Boneh, and J. Mitchell. Spyware resistant web authentication using virtual machines. Online manuscript. `http://crypto.stanford.edu/spyblock`.

[3] N. B. Margolin, M. K. Wright, and B. N. Levine. Guardian: A framework for privacy control in untrusted environments, June 2004. Tech Report 04-37 (U. Mass., Amherst).

[4] J. M. McCune, A. Perrig, and M. K. Reiter. Bump in the Ether: A framework for securing sensitive user input. In *USENIX Annual Technical Conference*, 2006.

[5] A. Oprea, D. Balfanz, G. Durfee, and D. Smetters. Securing a remote terminal application with a mobile trusted device. In *ACSAC*, 2004.

[6] B. Parno, C. Kuo, and A. Perrig. Phoolproof phishing prevention. In *Financial Cryptography*, volume 4107 of *LNCS*, 2006.

[7] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. Stronger password authentication using browser extensions. In *USENIX Security*, 2005.

[8] R. C. Stefan Berger, K. A. Goldman, R. Perez, R. Sailer, and L. van Doorn. vTPM: Virtualizing the trusted platform module. In *USENIX Security*, 2006.

[9] M. Wu, S. Garfinkel, and R. Miller. Secure web authentication with mobile phones. In *DIMACS Workshop on Usable Privacy and Security Systems*, July 2004.