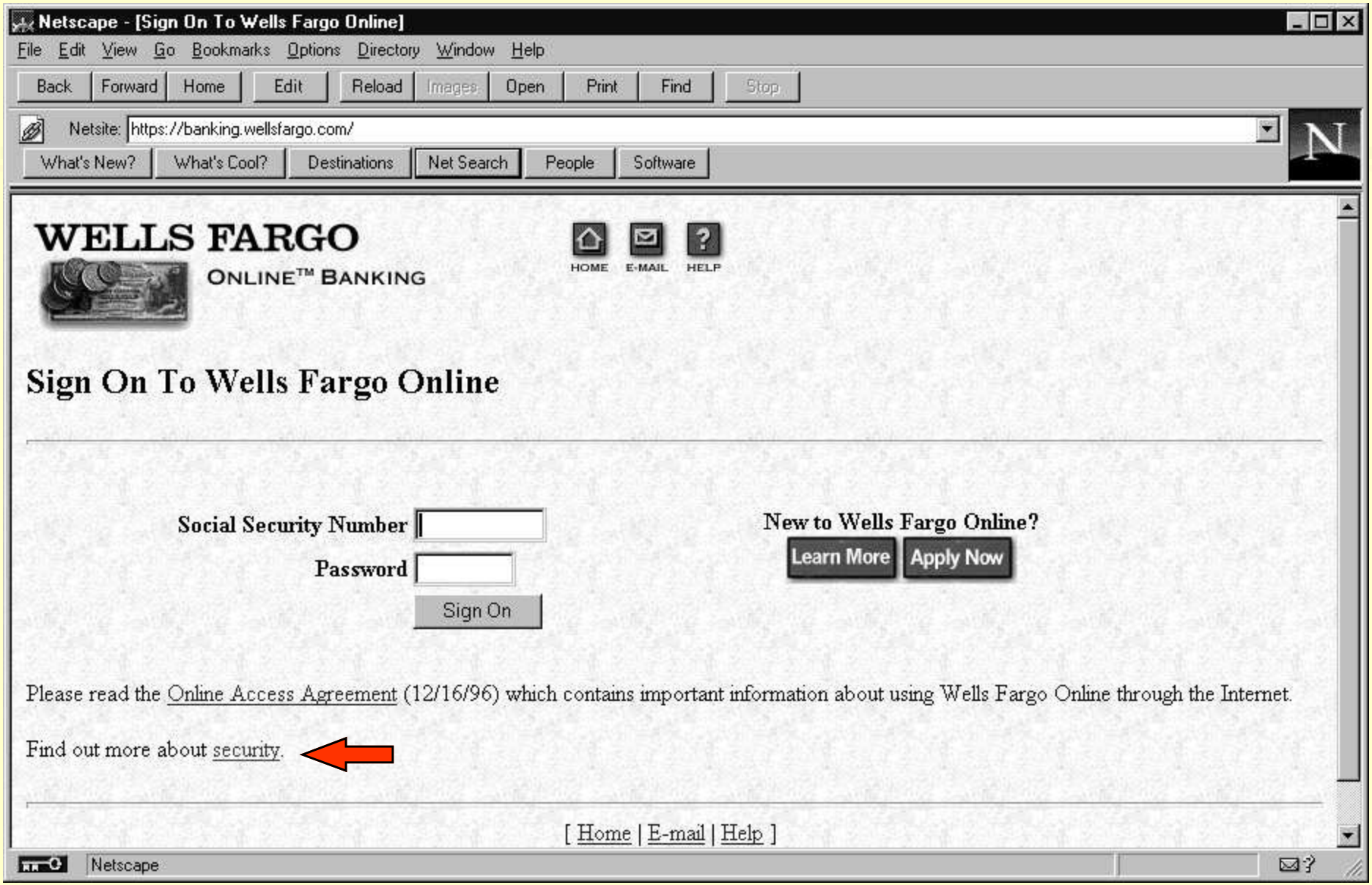
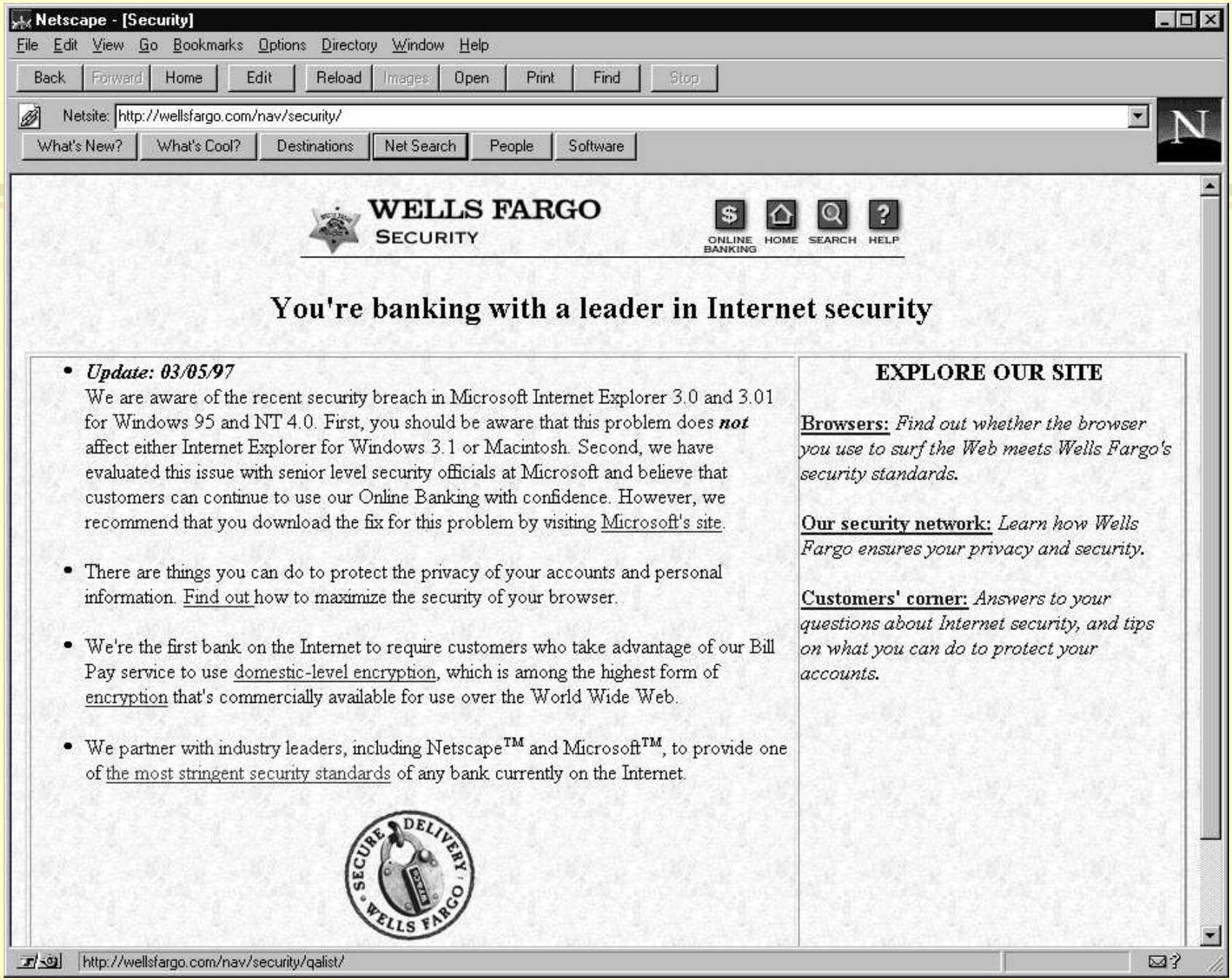
Security Protocols

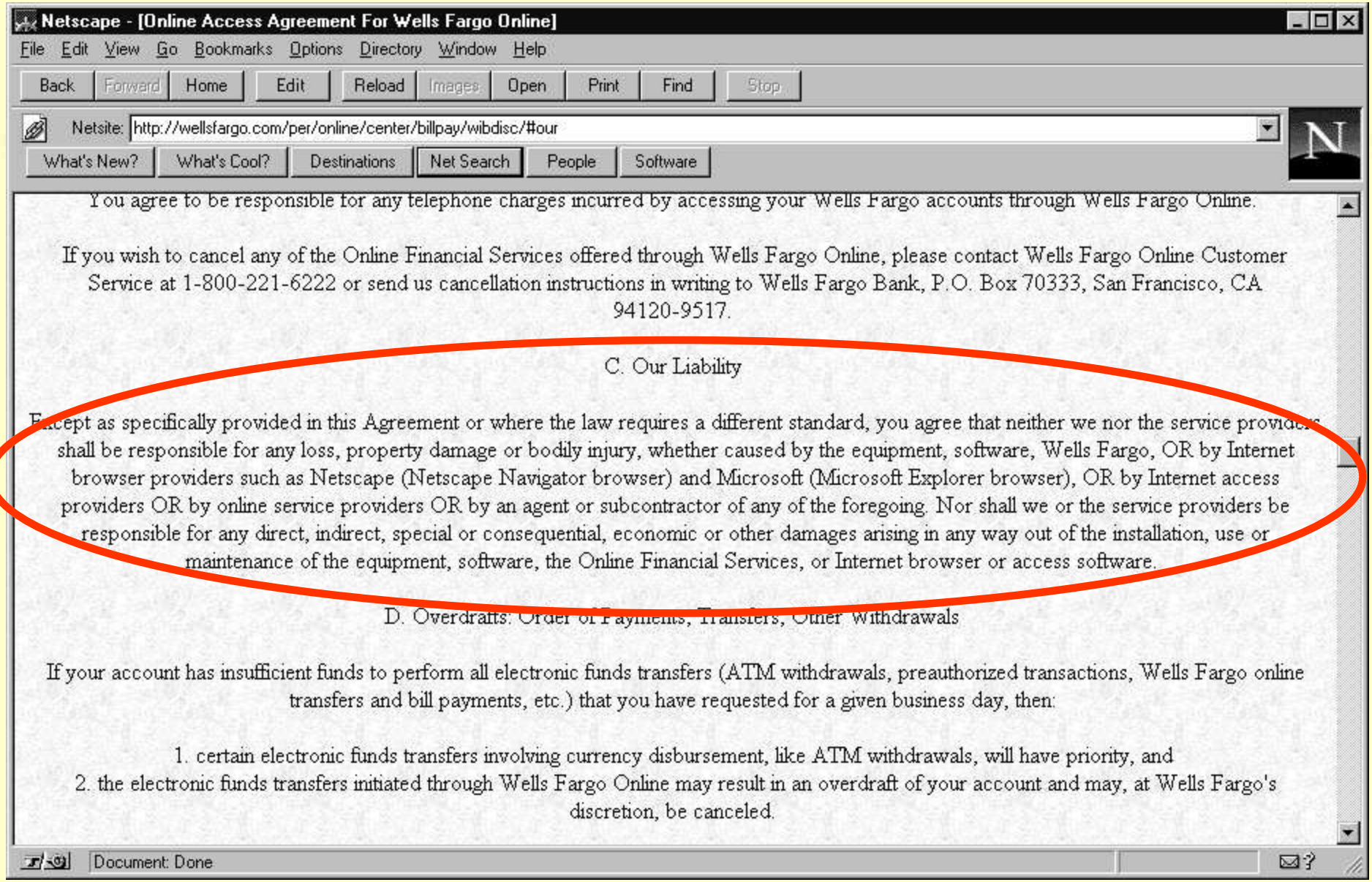
John C. Mitchell
Stanford University

Acknowledgments

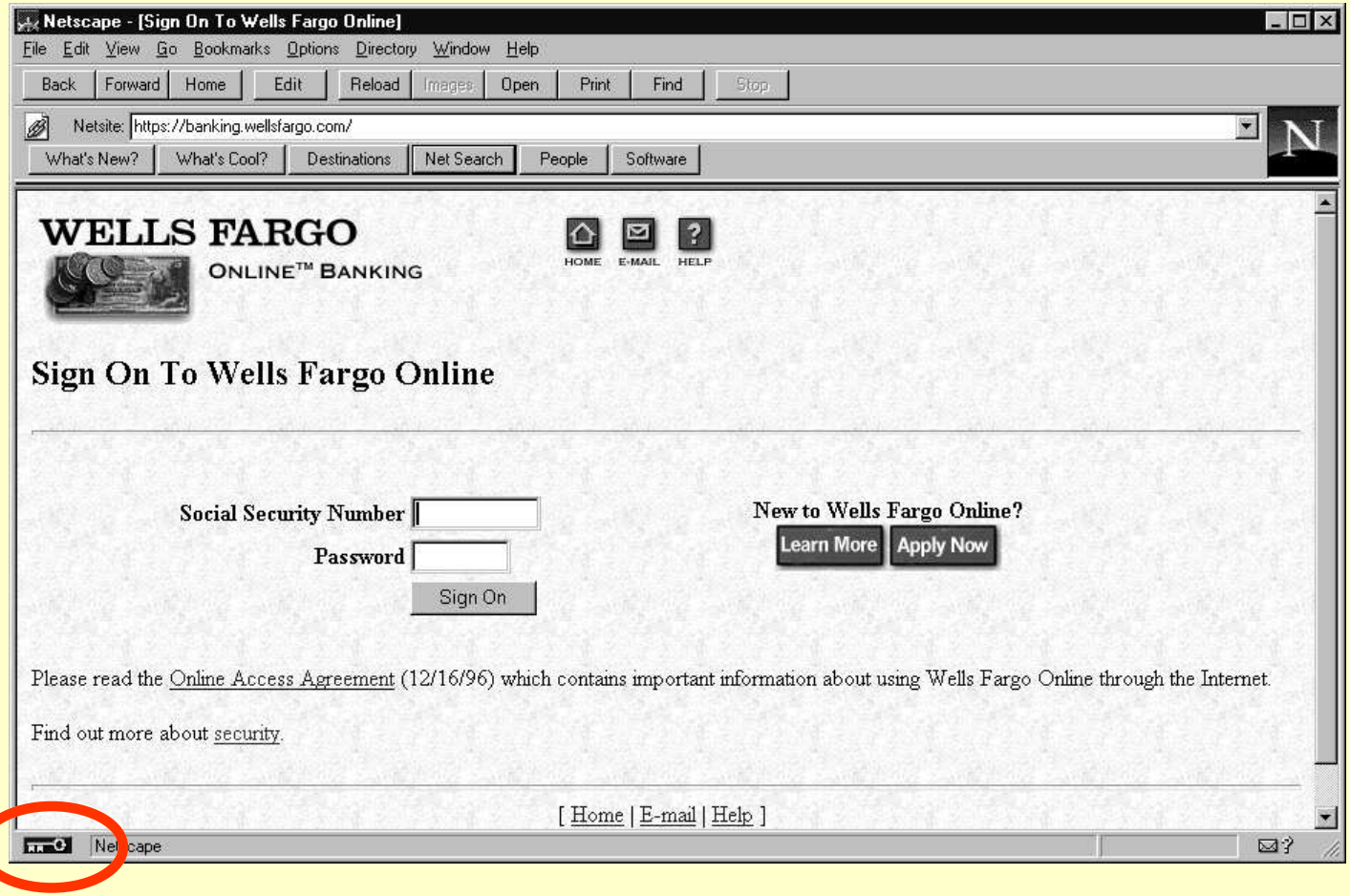
David Dill, Cynthia Dwork (IBM), Stephen Freund, Li Gong (Sun), Francois Guimbretiere, *Mark Mitchell*, John Rushby (SRI), Jens Skakkebaek, Vitaly Shmatikov, *Ulrich Stern*


Netscape - [Sign On To Wells Fargo Online]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Netsite: https://banking.wellsfargo.com/
What's New? What's Cool? Destinations Net Search People Software
WELLS FARGO
ONLINE™ BANKING
HOME E-MAIL HELP
Sign On To Wells Fargo Online
Social Security Number
Password
Sign On
New to Wells Fargo Online?
Learn More Apply Now
Please read the Online Access Agreement (12/16/96) which contains important information about using Wells Fargo Online through the Internet.
Find out more about security.
[Home | E-mail | Help]
Netscape


Netscape - [Security]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Netsite: http://wellsfargo.com/nav/security/
What's New? What's Cool? Destinations Net Search People Software
WELLS FARGO
SECURITY
ONLINE BANKING
HOME
SEARCH
HELP
You're banking with a leader in Internet security
Update: 03/05/97
We are aware of the recent security breach in Microsoft Internet Explorer 3.0 and 3.01 for Windows 95 and NT 4.0. First, you should be aware that this problem does not affect either Internet Explorer for Windows 3.1 or Macintosh. Second, we have evaluated this issue with senior level security officials at Microsoft and believe that customers can continue to use our Online Banking with confidence. However, we recommend that you download the fix for this problem by visiting Microsoft's site.
There are things you can do to protect the privacy of your accounts and personal information. Find out how to maximize the security of your browser.
We're the first bank on the Internet to require customers who take advantage of our Bill Pay service to use domestic-level encryption, which is among the highest form of encryption that's commercially available for use over the World Wide Web.
We partner with industry leaders, including Netscape™ and Microsoft™, to provide one of the most stringent security standards of any bank currently on the Internet.
SECURE DELIVERY
WELLS FARGO
EXPLORE OUR SITE
Browsers: Find out whether the browser you use to surf the Web meets Wells Fargo's security standards.
Our security network: Learn how Wells Fargo ensures your privacy and security.
Customers' corner: Answers to your questions about Internet security, and tips on what you can do to protect your accounts.
http://wellsfargo.com/nav/security/qalist/


Netscape - [Online Access Agreement For Wells Fargo Online]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Edit Reload Images Open Print Find Stop
Netsite: http://wellsfargo.com/per/online/center/billpay/wibdisc/#our
What's New? What's Cool? Destinations Net Search People Software
You agree to be responsible for any telephone charges incurred by accessing your Wells Fargo accounts through Wells Fargo Online.
If you wish to cancel any of the Online Financial Services offered through Wells Fargo Online, please contact Wells Fargo Online Customer Service at 1-800-221-6222 or send us cancellation instructions in writing to Wells Fargo Bank, P.O. Box 70333, San Francisco, CA 94120-9517.
C. Our Liability
Except as specifically provided in this Agreement or where the law requires a different standard, you agree that neither we nor the service providers shall be responsible for any loss, property damage or bodily injury, whether caused by the equipment, software, Wells Fargo, OR by Internet browser providers such as Netscape (Netscape Navigator browser) and Microsoft (Microsoft Explorer browser), OR by Internet access providers OR by online service providers OR by an agent or subcontractor of any of the foregoing. Nor shall we or the service providers be responsible for any direct, indirect, special or consequential, economic or other damages arising in any way out of the installation, use or maintenance of the equipment, software, the Online Financial Services, or Internet browser or access software.
D. Overdrafts; Order of Payments, Transfers, Other Withdrawals
If your account has insufficient funds to perform all electronic funds transfers (ATM withdrawals, preauthorized transactions, Wells Fargo online transfers and bill payments, etc.) that you have requested for a given business day, then:
1. certain electronic funds transfers involving currency disbursement, like ATM withdrawals, will have priority, and
2. the electronic funds transfers initiated through Wells Fargo Online may result in an overdraft of your account and may, at Wells Fargo's discretion, be canceled.
Document: Done

Secure Browser Interaction



Basic Concepts

- Encryption scheme:

  encrypt(plaintext,key) decrypt(cyphertext,key^{-1})

- Secret vs. public key
  - Public key: publishing key does not reveal key $^{-1}$
  - Secret key: more efficient; can have key = key $^{-1}$
- Hash function

  map long text to short hash key; ideally, no collision
- Signature scheme

  public key^{-1} and private key provide “authentication”

Establishing Secure Communication

- Parties use protocol to
  - choose encryption scheme, e.g.
    - 40-bit international encryption with 2^{40} keys
    - 120-bit domestic encryption with 2^{120} keys
    - choose among versions of specific scheme
  - agree on shared secret key
    - Secret key more efficient than public key
    - Minimize reuse of hard-to-establish public key

Secure Socket Layer (*SSL*)

- Three goals
  - Negotiate specific encryption scheme
    - Possible “version attack”
  - Authenticate client and server
    - Appeal to “signature authority”
  - Use public key to transmit secret key

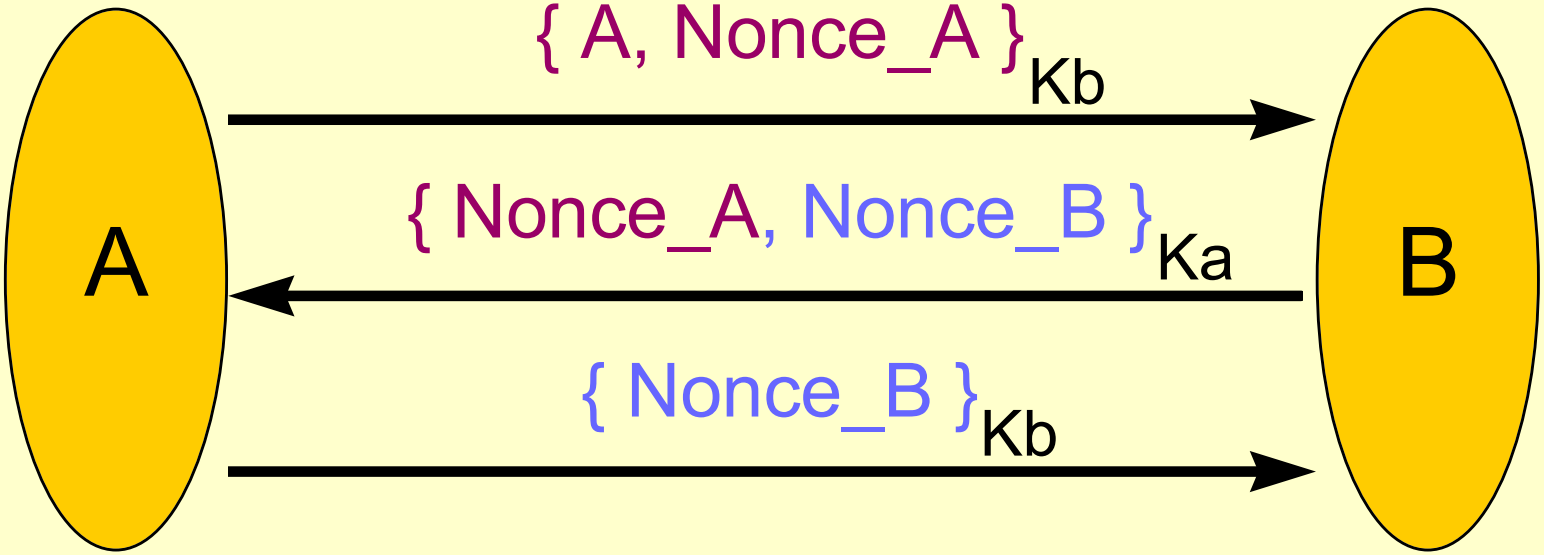
Several underlying primitives: public key, signature scheme, hash function, private key

Secure Socket Layer (*SSL)*

- Three steps in protocol
  - Client requests connection with server
  - Server responds, sends public key
  - Client sends encrypted private session key, hash of messages to avoid tampering

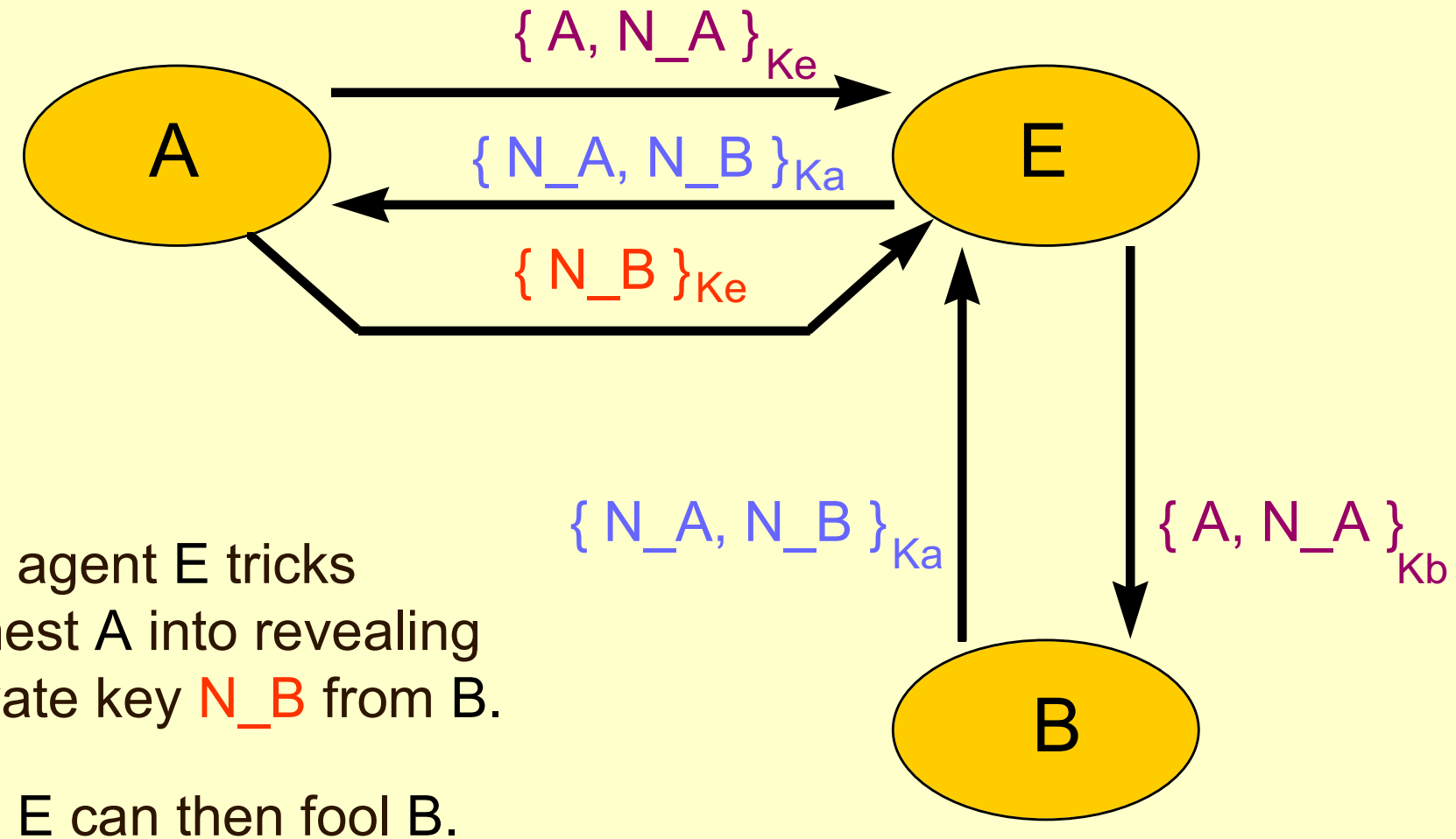
Illustrate basic concept, difficulties using Needham-Schroeder key exchange

Needham-Schroeder Key Exchange



Result: A and B share two private numbers not known to any observer without Ka^{-1}, Kb^{-1}

Anomaly in Needham-Schroeder



Evil agent E tricks honest A into revealing private key N_B from B.

Evil E can then fool B.

Analyzing Security Protocols

- Think long and hard
- BAN Logic
- Logic-based tools
- Exhaustive state-enumeration tools

Murφ [Dill et al.]

- Describe finite-state system
  - *Startstate* declaration
  - Transition rules
  - Correctness conditions
- Scalable: choose system size parameters
- Automatic exhaustive testing

  space limit: hash table to avoid repeated states

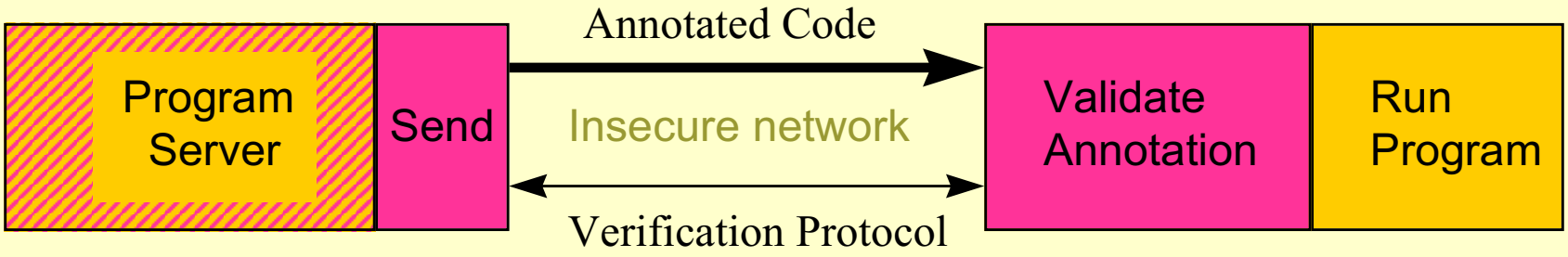
Murφ for security protocols

- Formulate protocol
- Add adversary
  - Control over "network" (shared variables)
  - Possible actions
    - Intercept any message
    - Remember parts of messages
    - Generate new messages, using observed data and initial knowledge (e.g. public keys)
- Identify correctness conditions

Murφ Results [1997]

- Analyze common protocols
  - Needham-Schroeder
  - Kerberos
    - Found bug in documented algorithm
    - one client, two servers
  - TMN cellular phone protocol
    - Found all known bugs automatically
    - Model algebraic properties of encryption function
- Work in progress: SSL protocol

Network Software Distribution



- Annotate programs with critical information
- Receiver checks annotations
  - on arrival, possibly by dialog with sender
  - during execution, possibly probabilistically
- Minimize exposure to severe risks

Other Security Work in Department

- Cheriton, Greenwald, et al.
  - Stanford University Research Firewall (SURF):
  - trade off information transfer vs information security
- Luckham, Meldal, et al.
  - modeling the MISSI security policies in Rapide
- Roscheisen (Digital Libraries)
  - Contract-based Rights Management
- Wiederhold
  - Trusted Interoperation of Healthcare Information (TIHI)
- Others?