money for nothing, chips for free

July [edit]

- July 5 – Japan launches a probe to M d Russia as an outer space-exploring nation.
- July 17

e, 120 cou t Inte

r genocide rimes

holas II of in St

amily were

Guinea ea r Aita

). This submarine earthquake triggered a landsli

han 2,100 dead and thousands injured.

1998 Sydney water crisis involved the suspect

otosporidium and *giardia* of the water supply system of Greater Metropolitan

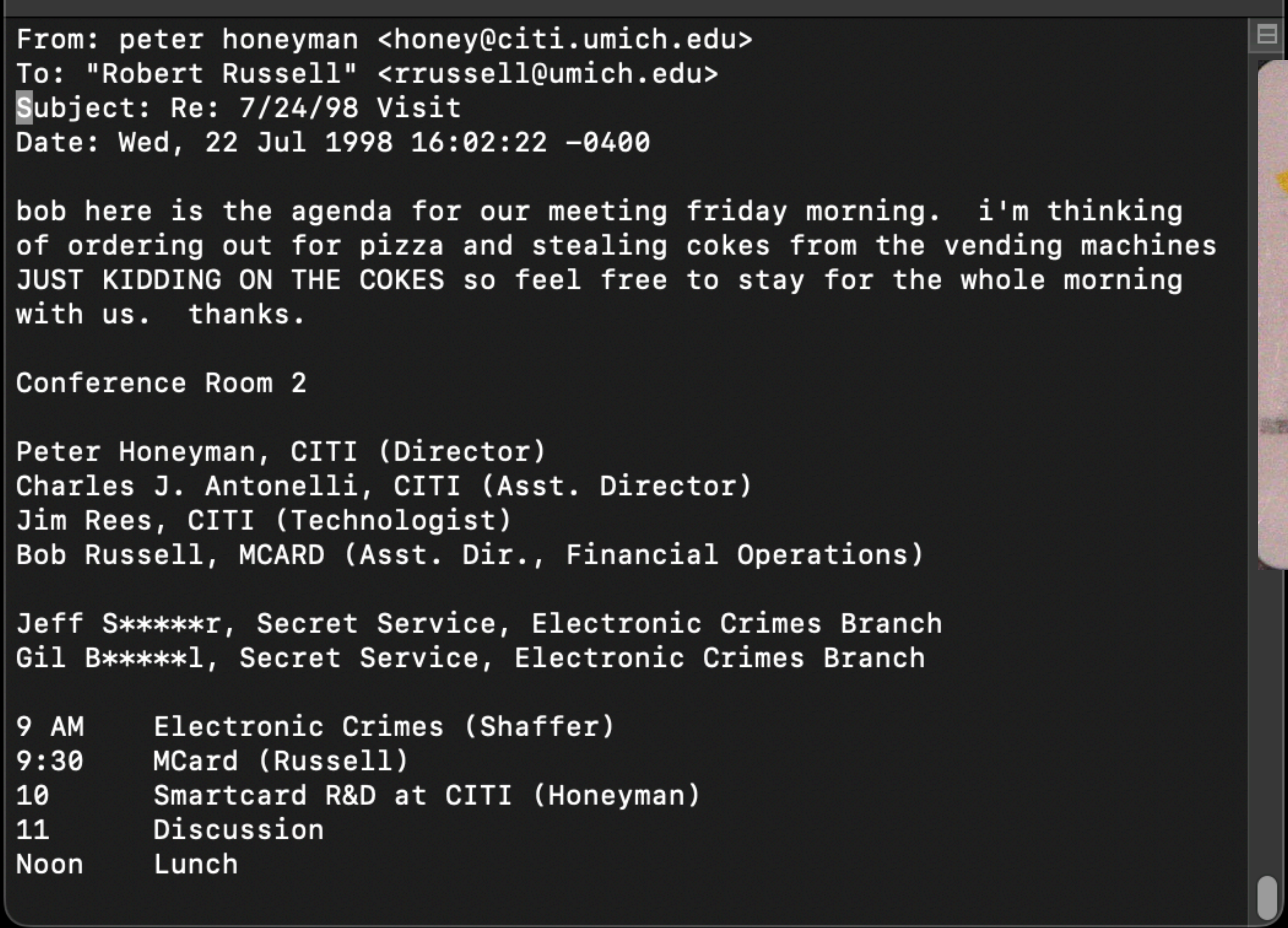
Veston Jr. enters the United States Capitol Building and opens fire, killing two

es Capitol Police, Jacob Chestnut and John Gibson.

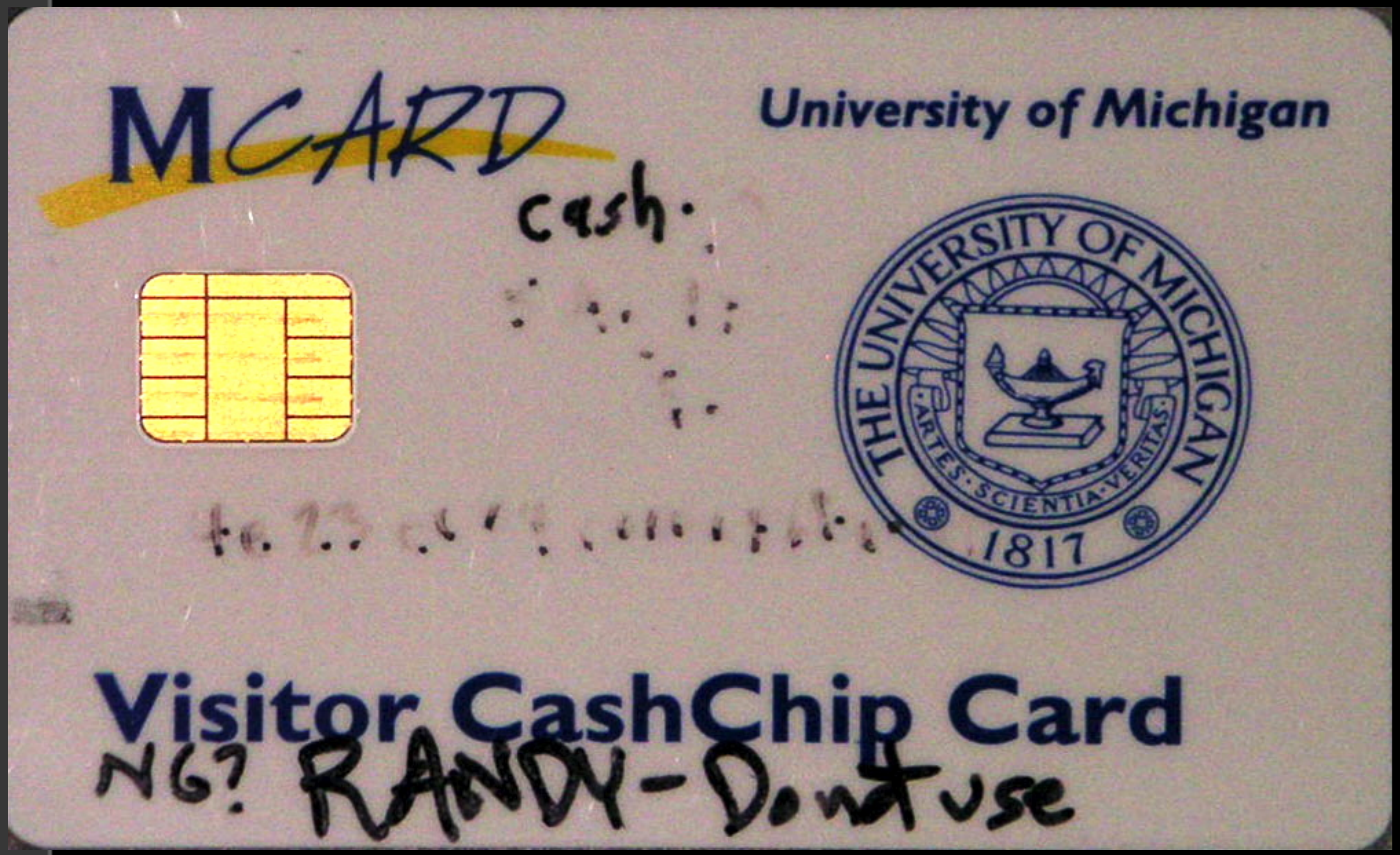
THE NETHERLANDS
1998
9

8

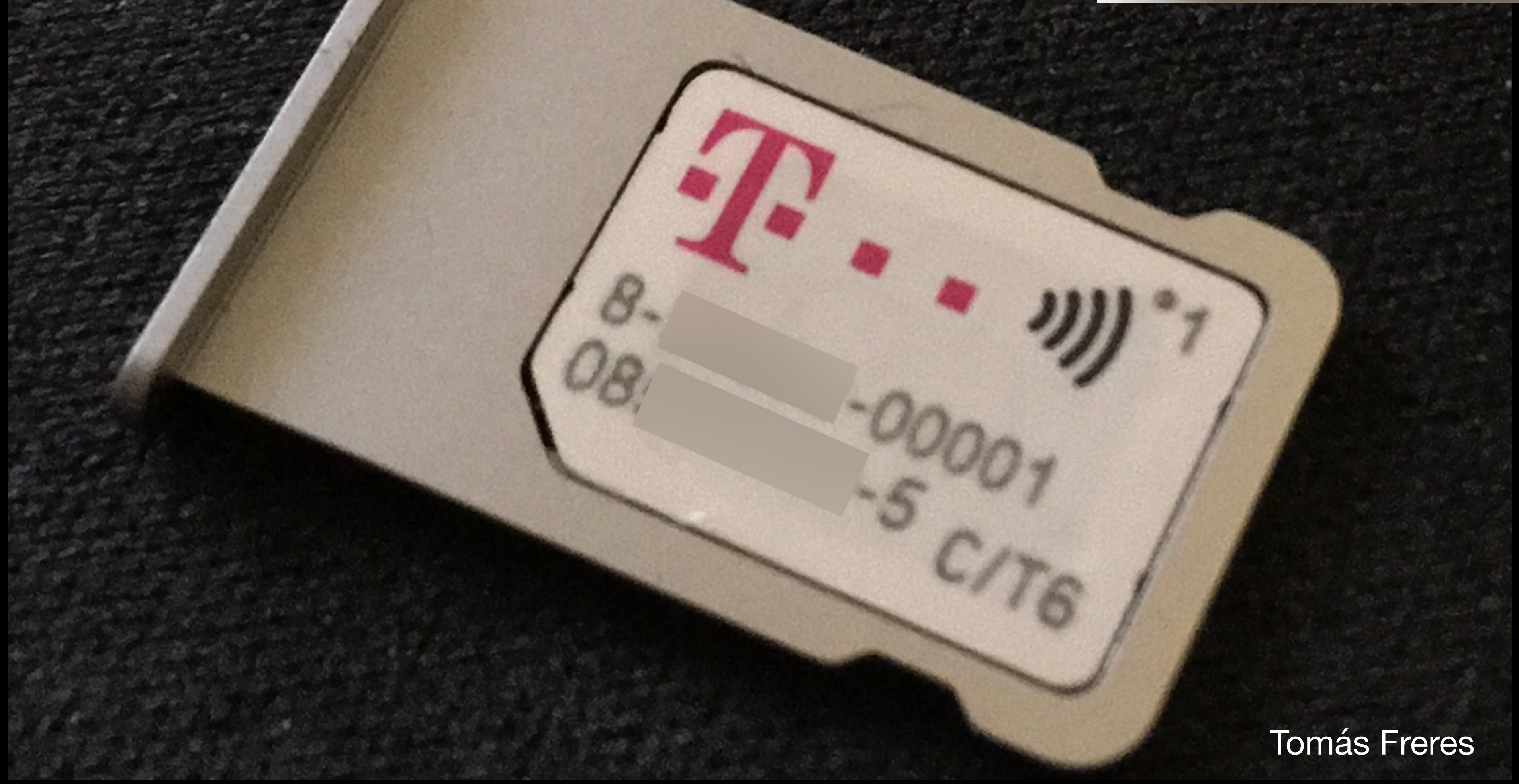
MARSEILLE
FILM
1
8
3
11
6
9
5
16
2
4
7

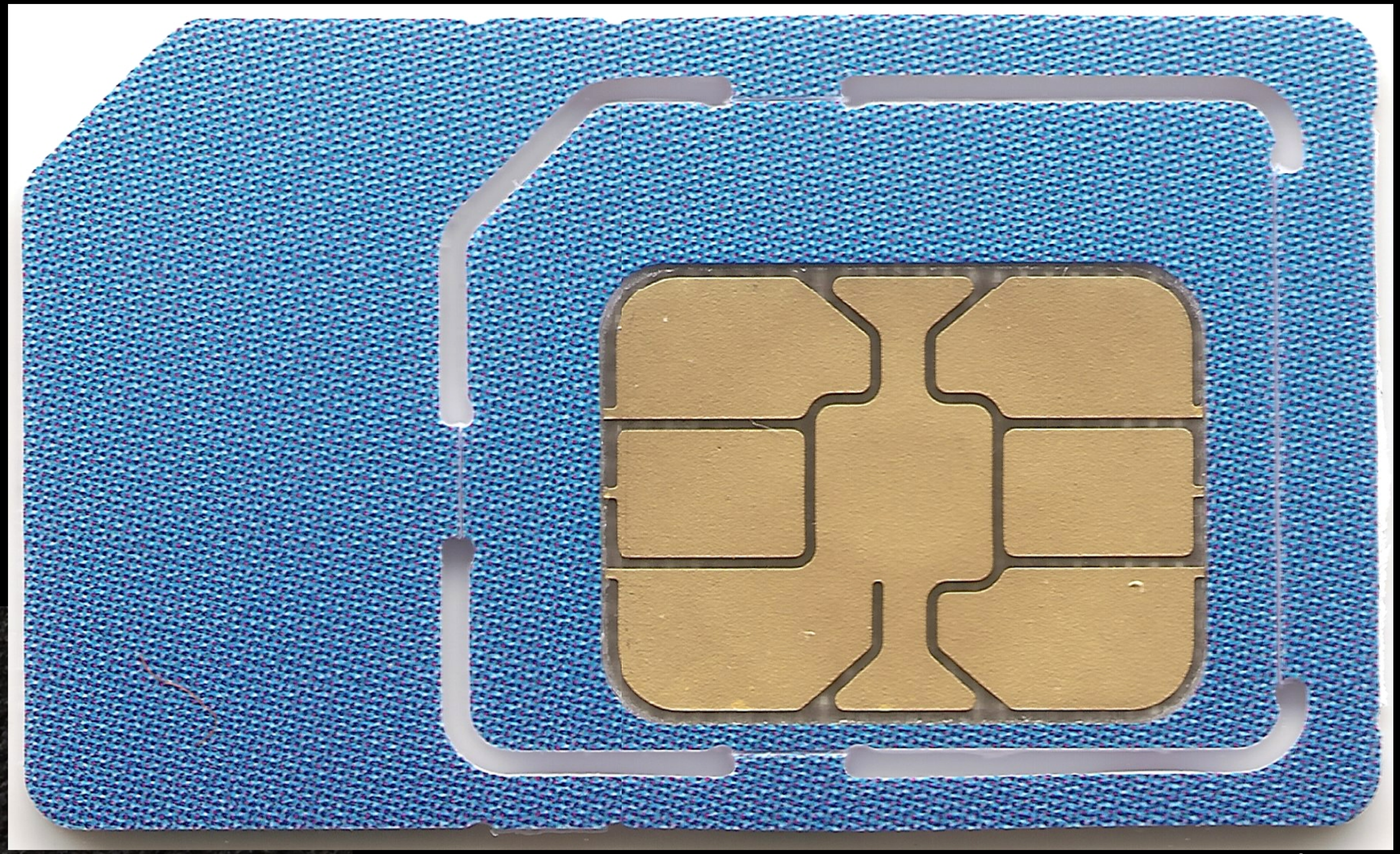


```
From: peter honeyman <honey@citi.umich.edu>
To: "Robert Russell" <rrussell@umich.edu>
Subject: Re: 7/24/98 Visit
Date: Wed, 22 Jul 1998 16:02:22 -0400

bob here is the agenda for our meeting friday morning.  i'm thinking
of ordering out for pizza and stealing cokes from the vending machines
JUST KIDDING ON THE COKES so feel free to stay for the whole morning
with us.  thanks.

Conference Room 2

Peter Honeyman, CITI (Director)
Charles J. Antonelli, CITI (Asst. Director)
Jim Rees, CITI (Technologist)
Bob Russell, MCARD (Asst. Dir., Financial Operations)

Jeff S*****r, Secret Service, Electronic Crimes Branch
Gil B*****l, Secret Service, Electronic Crimes Branch

9 AM    Electronic Crimes (Shaffer)
9:30    MCard (Russell)
10      Smartcard R&D at CITI (Honeyman)
11      Discussion
Noon    Lunch
```

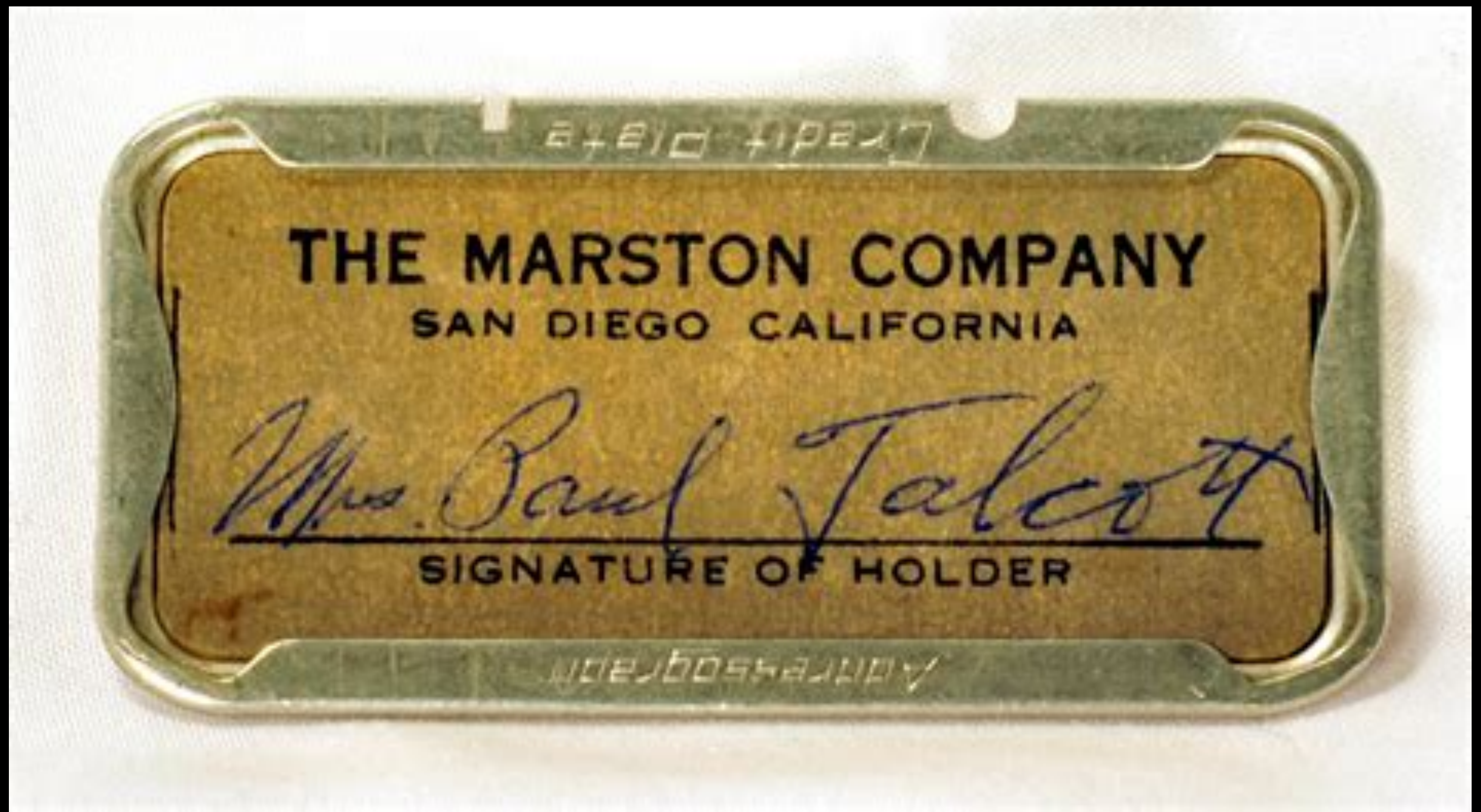


a brief history of smart cards


Tomás Freres


Telefónica O_2

187659


Credit Plate
THE MARSTON COMPANY
SAN DIEGO CALIFORNIA
Mrs Paul Talcott
SIGNATURE OF HOLDER
Addressograph

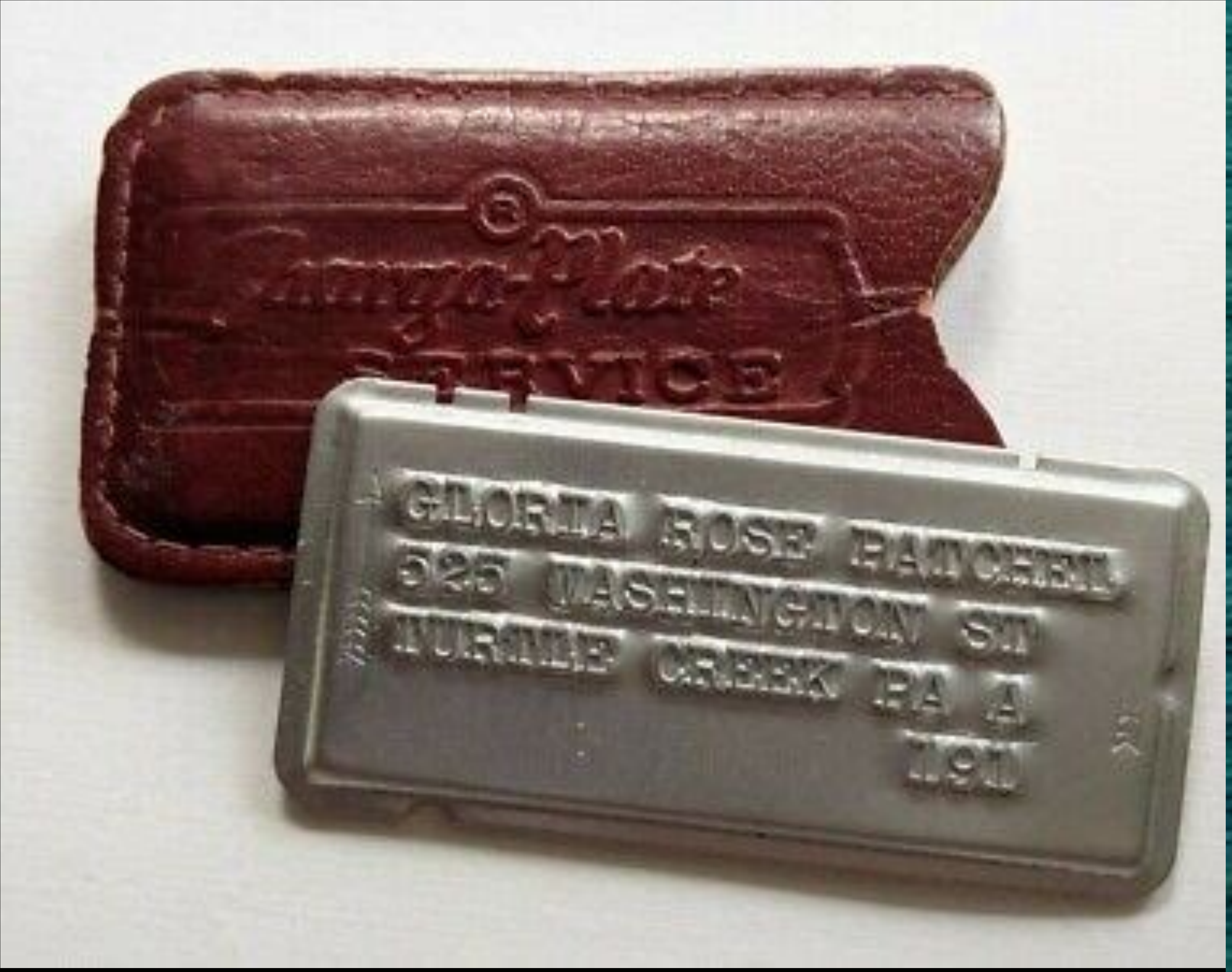
ABRAHAM
18465-C
STRAUS INC

121433
RHCo

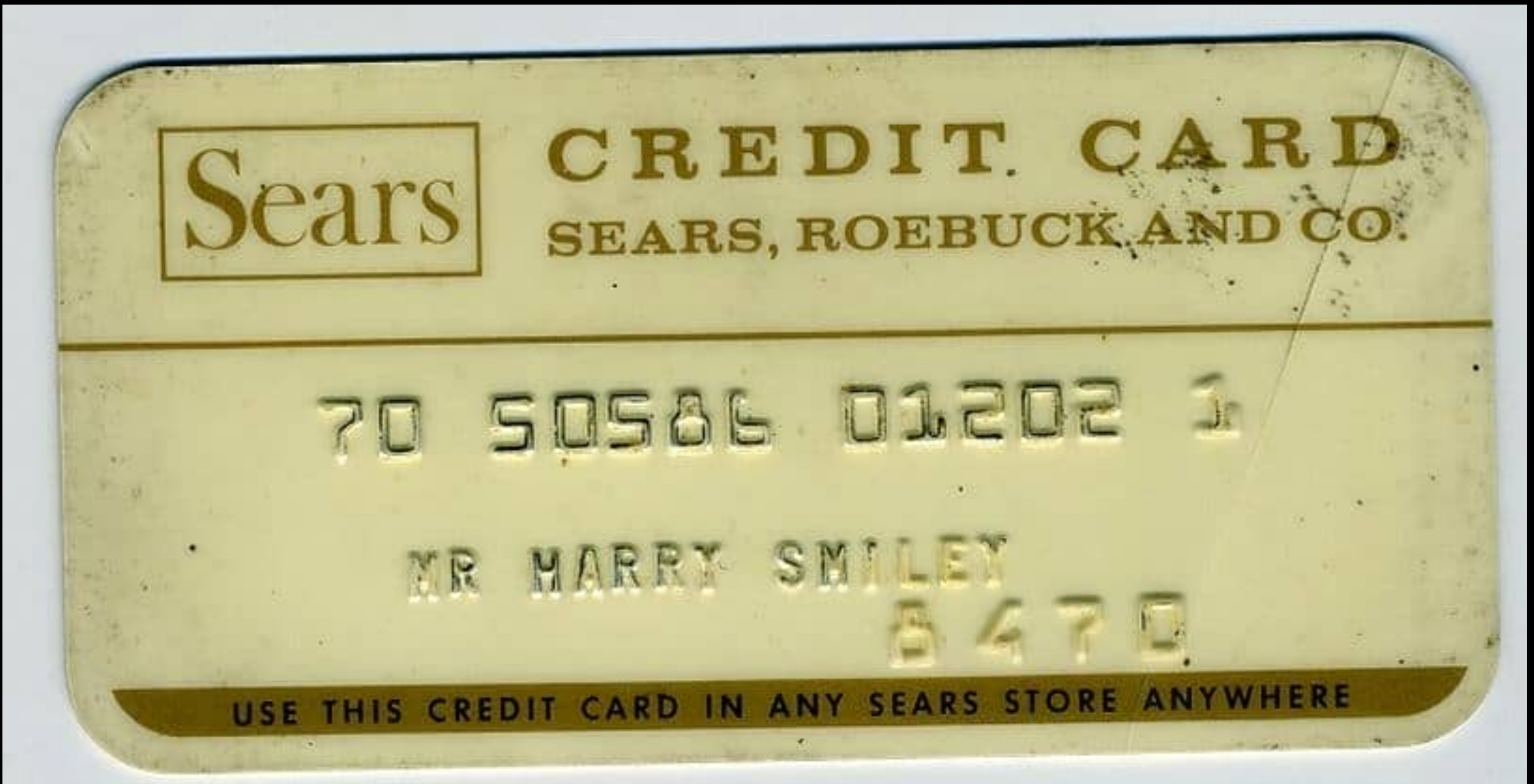
61254

39332
RHCo

A&S
7439-B

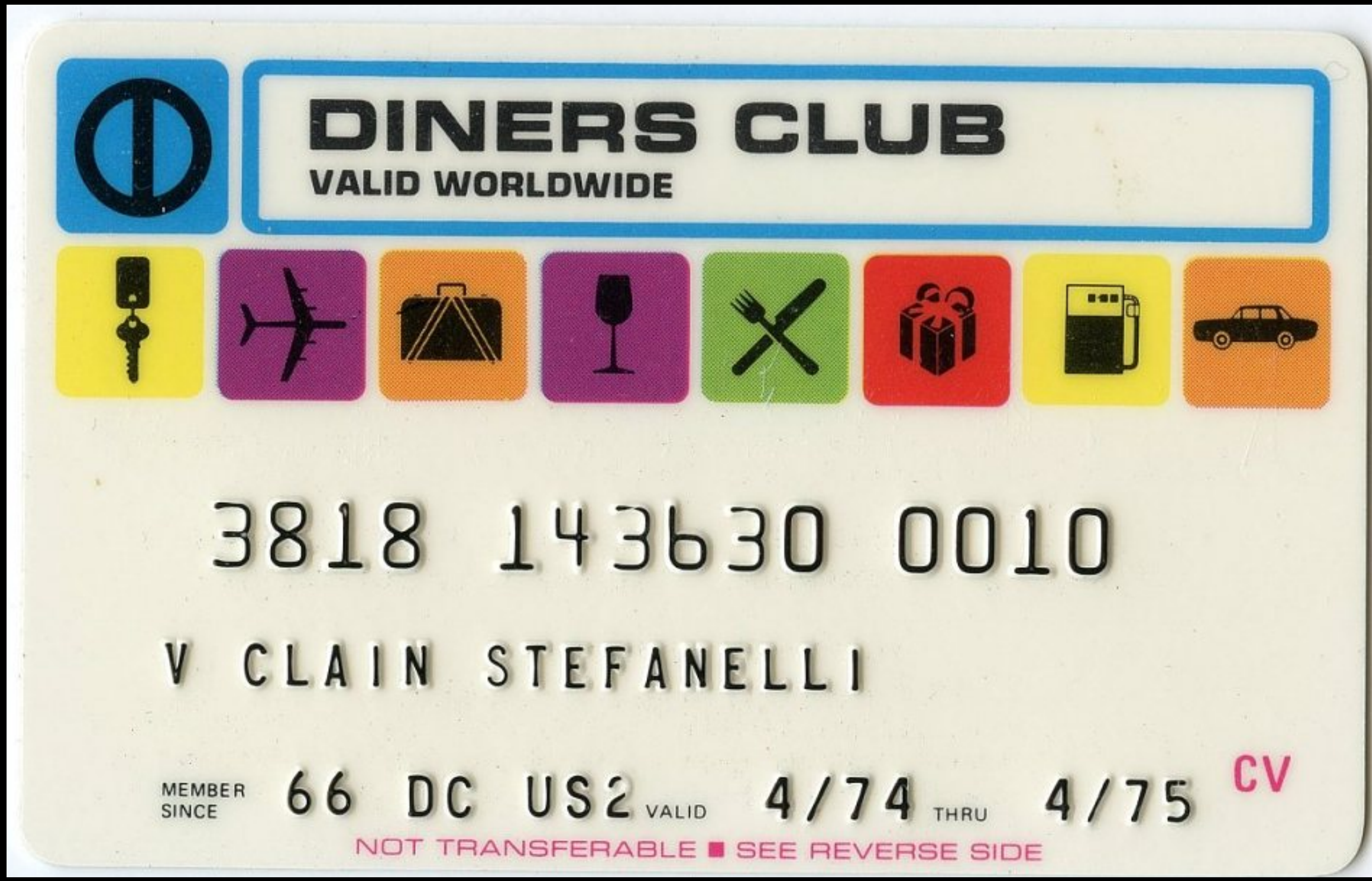

Charga-Plate
SERVICE
GLORIA ROSE PATCHEL
525 WASHINGTON ST
MYRTLE CREEK PA A
1191

Charga-Plate
Associates
Charga-Plate
Associates
MRS RALPH A WILKINS
2 PARK LANE
S WALPOLE MASS
1026-089 2
www.timepassagesnostalgia.com


Sears
CREDIT CARD
SEARS, ROEBUCK AND CO.
70 50586 01202 1
MR HARRY SMILEY
6470
USE THIS CREDIT CARD IN ANY SEARS STORE ANYWHERE

CHARGA-PLATE
GROUP
MRS IRA B ZASLOFF
79 REMSEN ST
BROOKLYN 2 NY A

AMERICAN EXPRESS
PAYS FOR TRAVEL AND ENTERTAINMENT WORLDWIDE
007 035 157 2 200AX
MEMBER SINCE 61
06/70
V CLAIN STEFANELLI
NOT TRANSFERABLE
SEE REVERSE SIDE


DINERS CLUB
VALID WORLDWIDE
3818 143630 0010
V CLAIN STEFANELLI
MEMBER SINCE 66 DC US2 VALID 4/74 THRU 4/75
CV
NOT TRANSFERABLE ■ SEE REVERSE SIDE

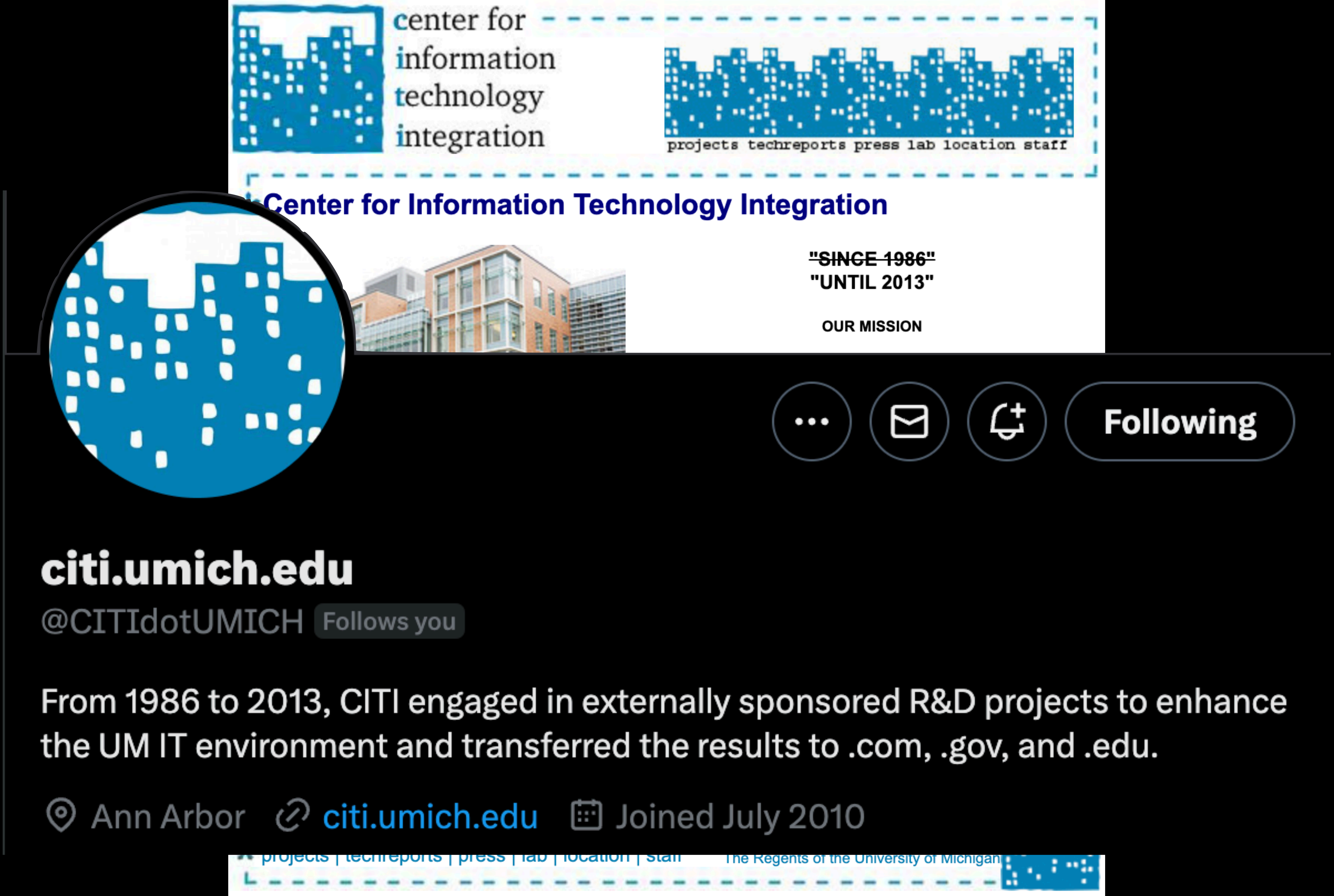
VISA
MasterCard

BANKAMERICARD
VISA
4101 123 456 188
GOOD THRU LAST DAY OF
00/00 BWG
PAT YOUNG

Mondex
Electr
BANK OF AMERICA
PETER HONE
SPECIAL EDITION
RELOADABLE
VISA
Cash

ERICSSON
SH888
MOTOROLA
NOKIA
Meny
verizon
LG

smart card r&d



center for
information
technology
integration

projects techreports press lab location staff

Center for Information Technology Integration

~~"SINCE 1986"~~
"UNTIL 2013"

OUR MISSION

citi.umich.edu

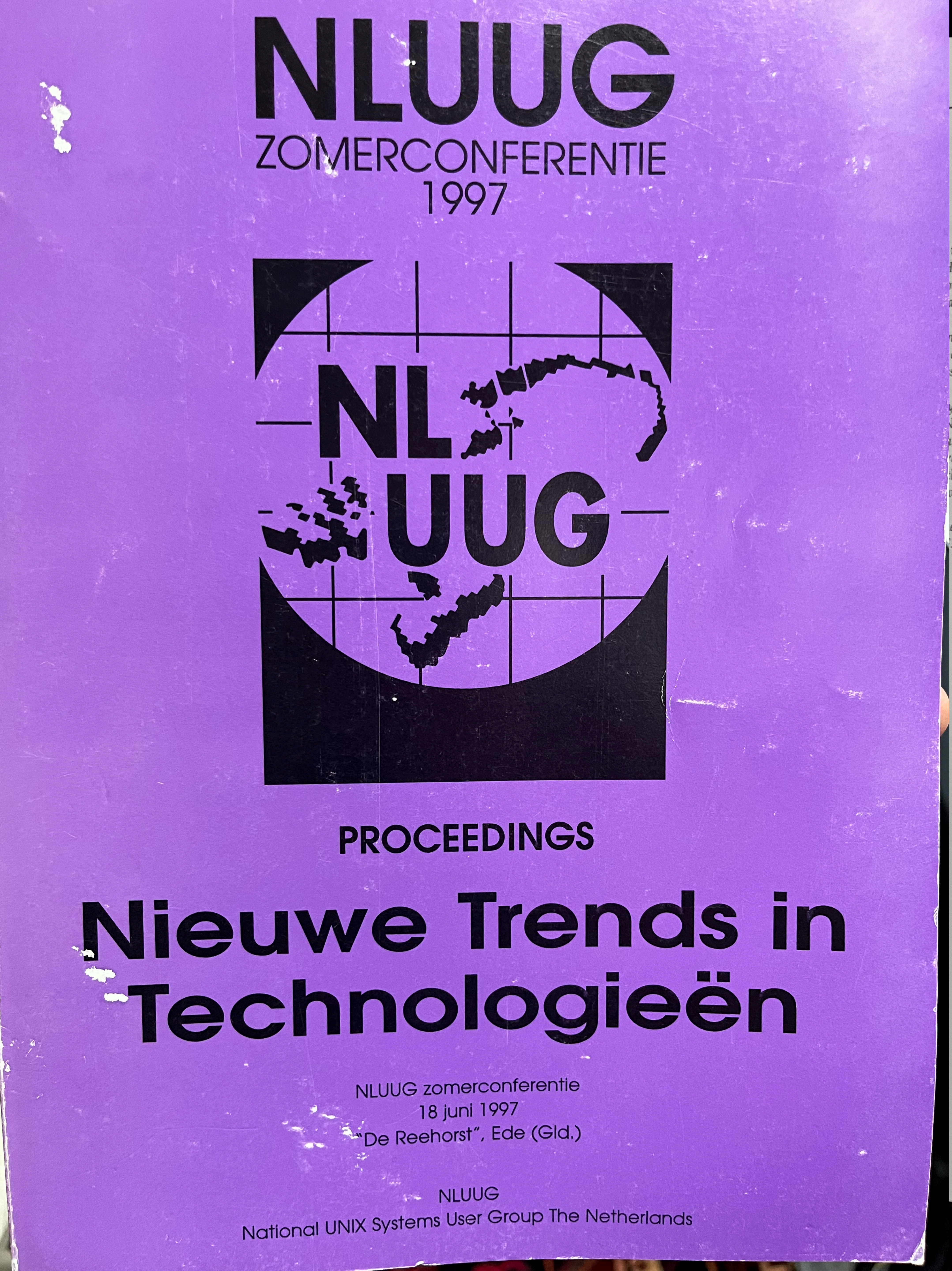
@CITIdotUMICH Follows you

From 1986 to 2013, CITI engaged in externally sponsored R&D projects to enhance the UM IT environment and transferred the results to .com, .gov, and .edu.

Ann Arbor citi.umich.edu Joined July 2010

projects | techreports | press | lab | location | staff

The Regents of the University of Michigan



NLUUG

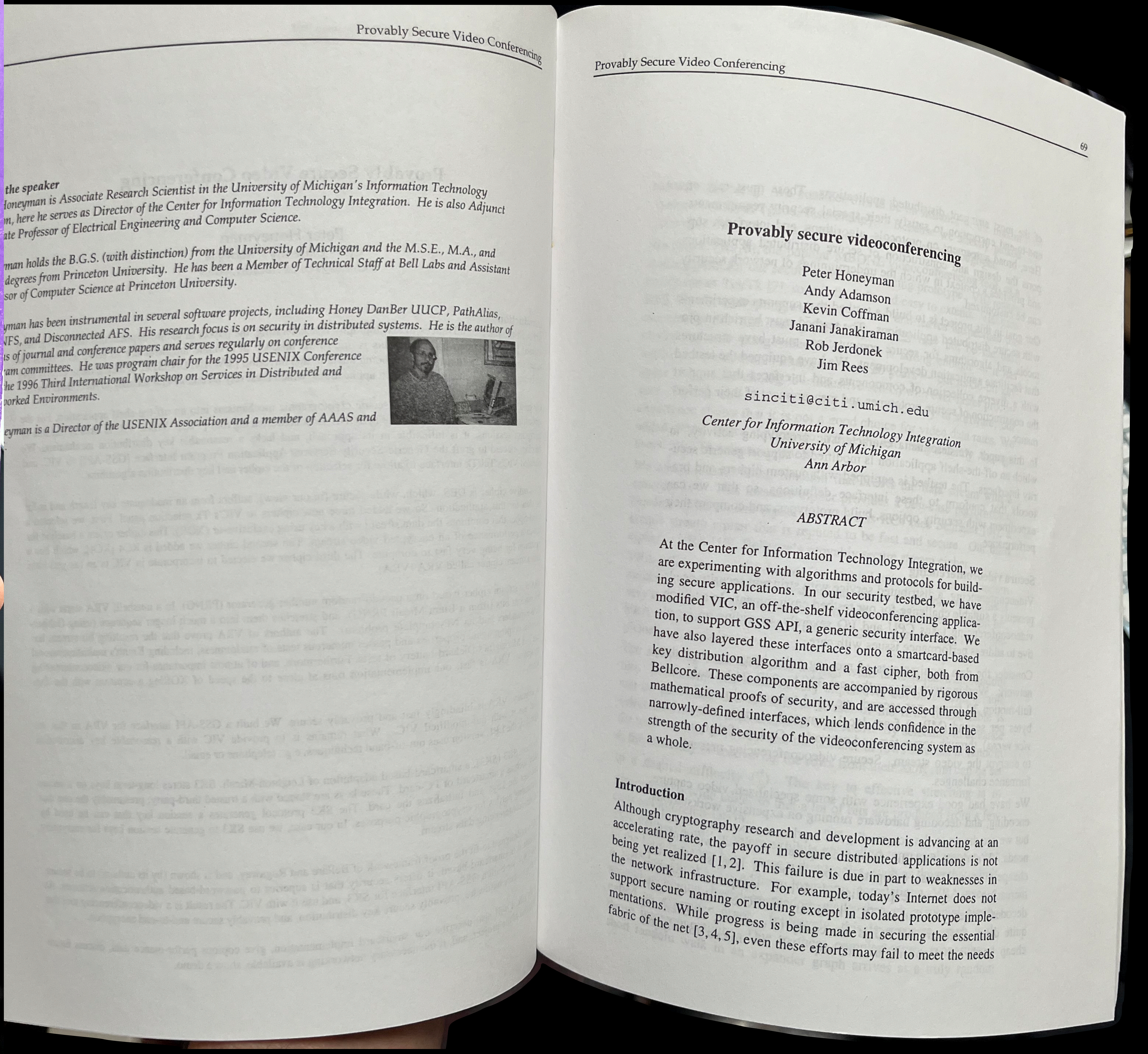
ZOMERCONFERENTIE
1997

PROCEEDINGS

Nieuwe Trends in Technologieën

NLUUG zomerconferentie
18 juni 1997
"De Reehorst", Ede (Gld.)

NLUUG
National UNIX Systems User Group The Netherlands



the speaker

Honeyman is Associate Research Scientist in the University of Michigan's Information Technology
on, here he serves as Director of the Center for Information Technology Integration. He is also Adjunct
ate Professor of Electrical Engineering and Computer Science.

man holds the B.G.S. (with distinction) from the University of Michigan and the M.S.E., M.A., and
degrees from Princeton University. He has been a Member of Technical Staff at Bell Labs and Assistant
sor of Computer Science at Princeton University.

yman has been instrumental in several software projects, including Honey DanBer UUCP, PathAlias,
NFS, and Disconnected AFS. His research focus is on security in distributed systems. He is the author of
s of journal and conference papers and serves regularly on conference
am committees. He was program chair for the 1995 USENIX Conference
he 1996 Third International Workshop on Services in Distributed and
orked Environments.

eyman is a Director of the USENIX Association and a member of AAAS and

Provably secure videoconferencing

Peter Honeyman
Andy Adamson
Kevin Coffman
Janani Janakiraman
Rob Jerdonek
Jim Rees

sinciti@citi.umich.edu

Center for Information Technology Integration
University of Michigan
Ann Arbor

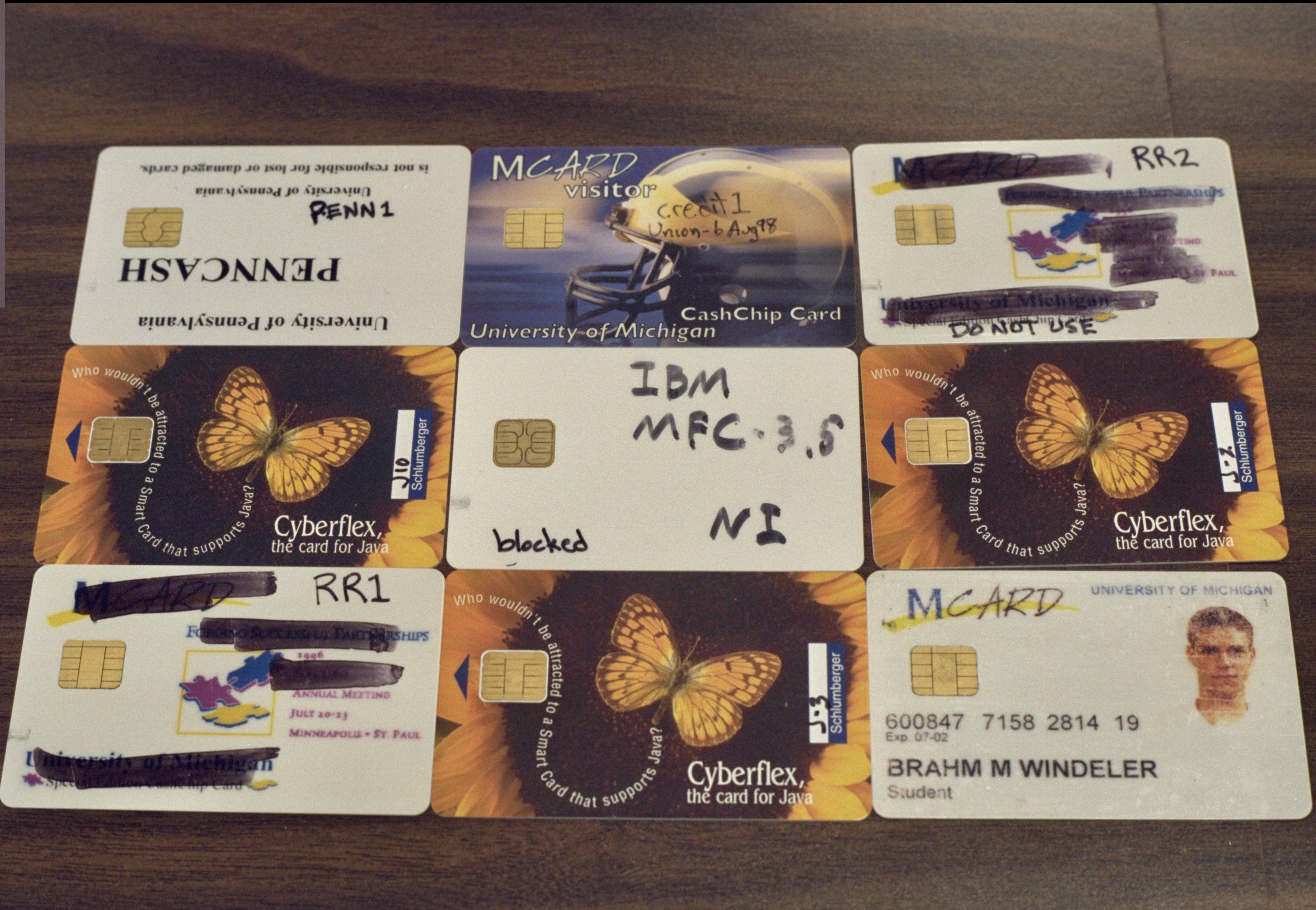
ABSTRACT

At the Center for Information Technology Integration, we are experimenting with algorithms and protocols for building secure applications. In our security testbed, we have modified VIC, an off-the-shelf videoconferencing application, to support GSS API, a generic security interface. We have also layered these interfaces onto a smartcard-based key distribution algorithm and a fast cipher, both from Bellcore. These components are accompanied by rigorous mathematical proofs of security, and are accessed through narrowly-defined interfaces, which lends confidence in the strength of the security of the videoconferencing system as a whole.

Introduction

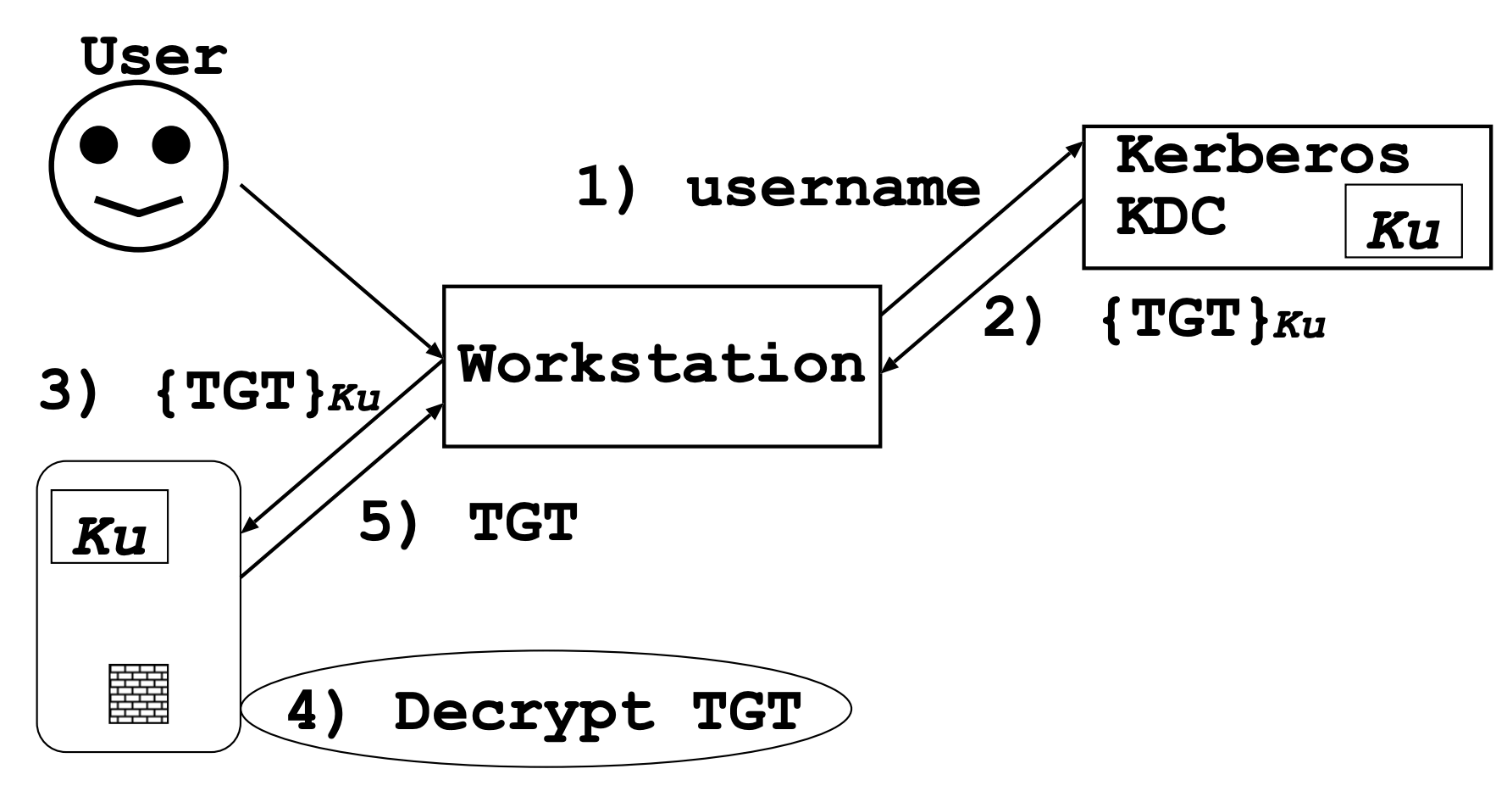
Although cryptography research and development is advancing at an accelerating rate, the payoff in secure distributed applications is not being yet realized [1, 2]. This failure is due in part to weaknesses in the network infrastructure. For example, today's Internet does not support secure naming or routing except in isolated prototype implementations. While progress is being made in securing the essential fabric of the net [3, 4, 5], even these efforts may fail to meet the needs

Look for the for tasty, Balanced Choice snacks!


University of Pennsylvania
is not responsible for lost or damaged cards.
PENN1
PENNCASH
University of Pennsylvania
MCARD
visitor
credit1
Union-6 Aug 98
CashChip Card
University of Michigan
RR2
DO NOT USE
Who wouldn't be attracted to a Smart Card that supports Java?
J10
Schlumberger
Cyberflex,
the card for Java
IBM
MFC-3.5
blocked
NI
Who wouldn't be attracted to a Smart Card that supports Java?
Schlumberger
Cyberflex,
the card for Java
RR1
Annual Meeting
July 20-23
Minneapolis • St. Paul
Who wouldn't be attracted to a Smart Card that supports Java?
J3
Schlumberger
Cyberflex,
the card for Java
MCARD
UNIVERSITY OF MICHIGAN
600847 7158 2814 19
Exp. 07-02
BRAHM M WINDELER
Student

Smartcard Integration with Kerberos V5

Naomaru Itoi and Peter Honeyman
Center for Information Technology Integration
University of Michigan
Ann Arbor
itoi@eecs.umich.edu, honey@citi.umich.edu



SCFS: A UNIX Filesystem for Smartcards

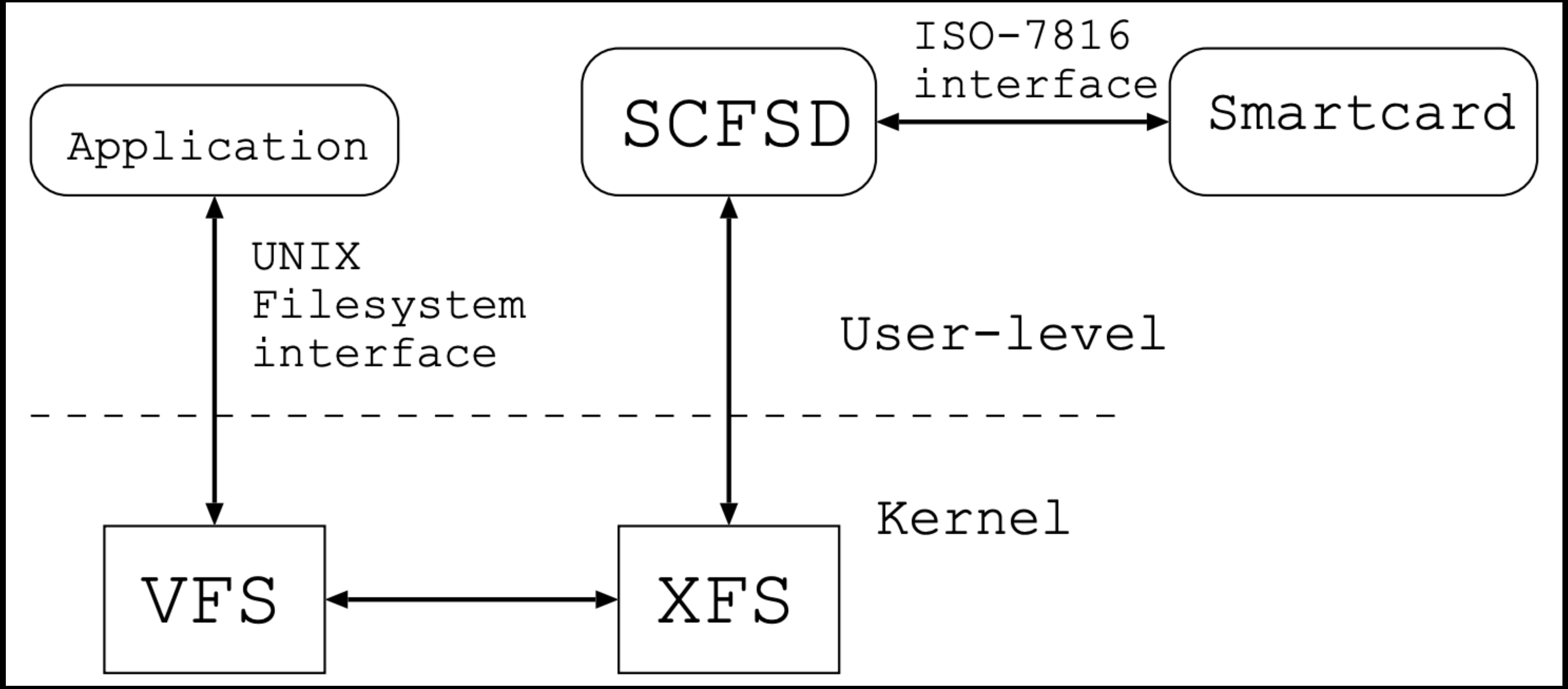
Naomaru Itoi, Peter Honeyman, and Jim Rees

Center for Information Technology Integration

University of Michigan

Ann Arbor

itoi@eecs.umich.edu, honey@citi.umich.edu, rees@umich.edu



Application

SCFSD

ISO-7816 interface

Smartcard

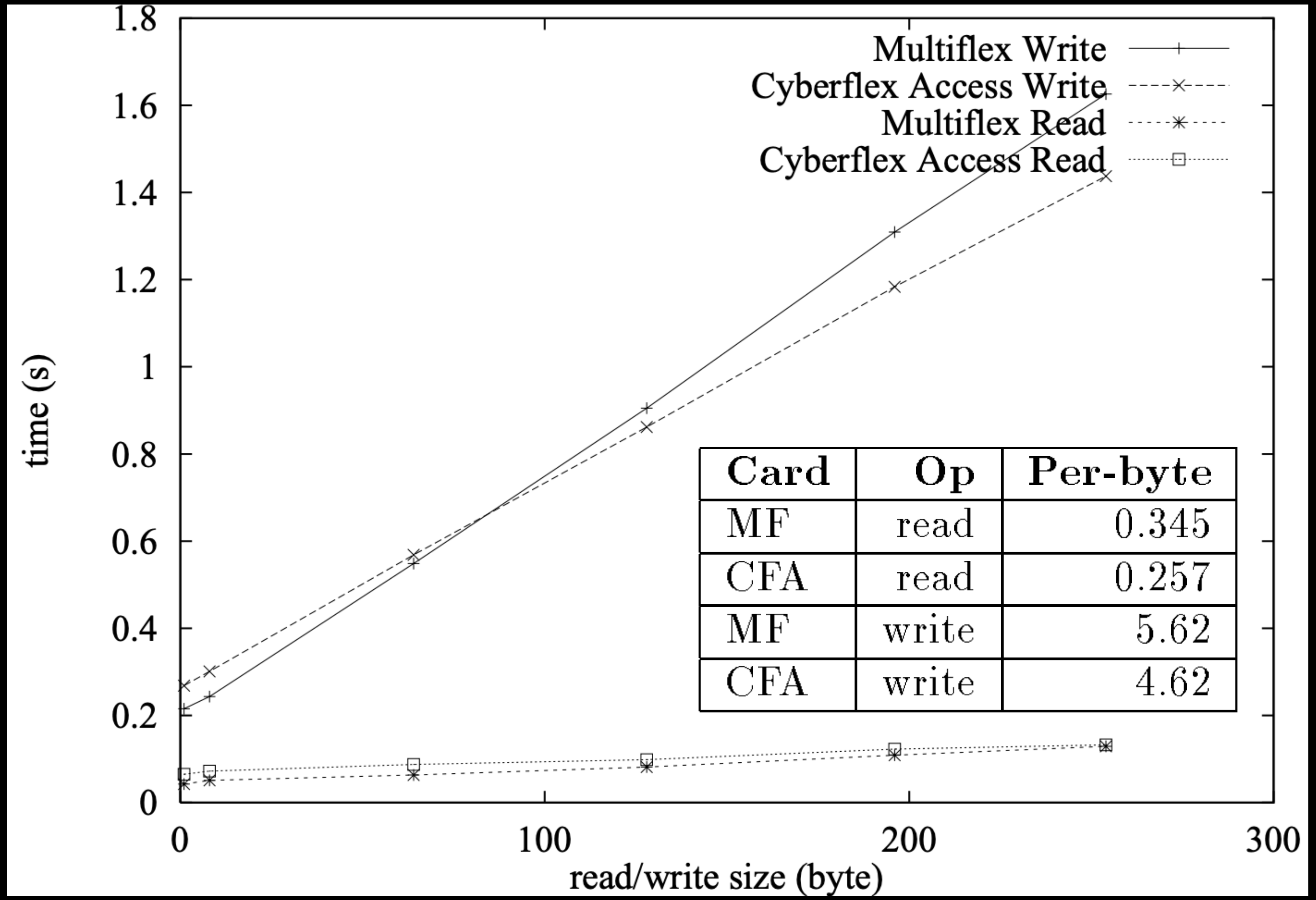
UNIX Filesystem interface

User-level

Kernel

VFS

XFS



Card	Op	Per-byte
MF	read	0.345
CFA	read	0.257
MF	write	5.62
CFA	write	4.62

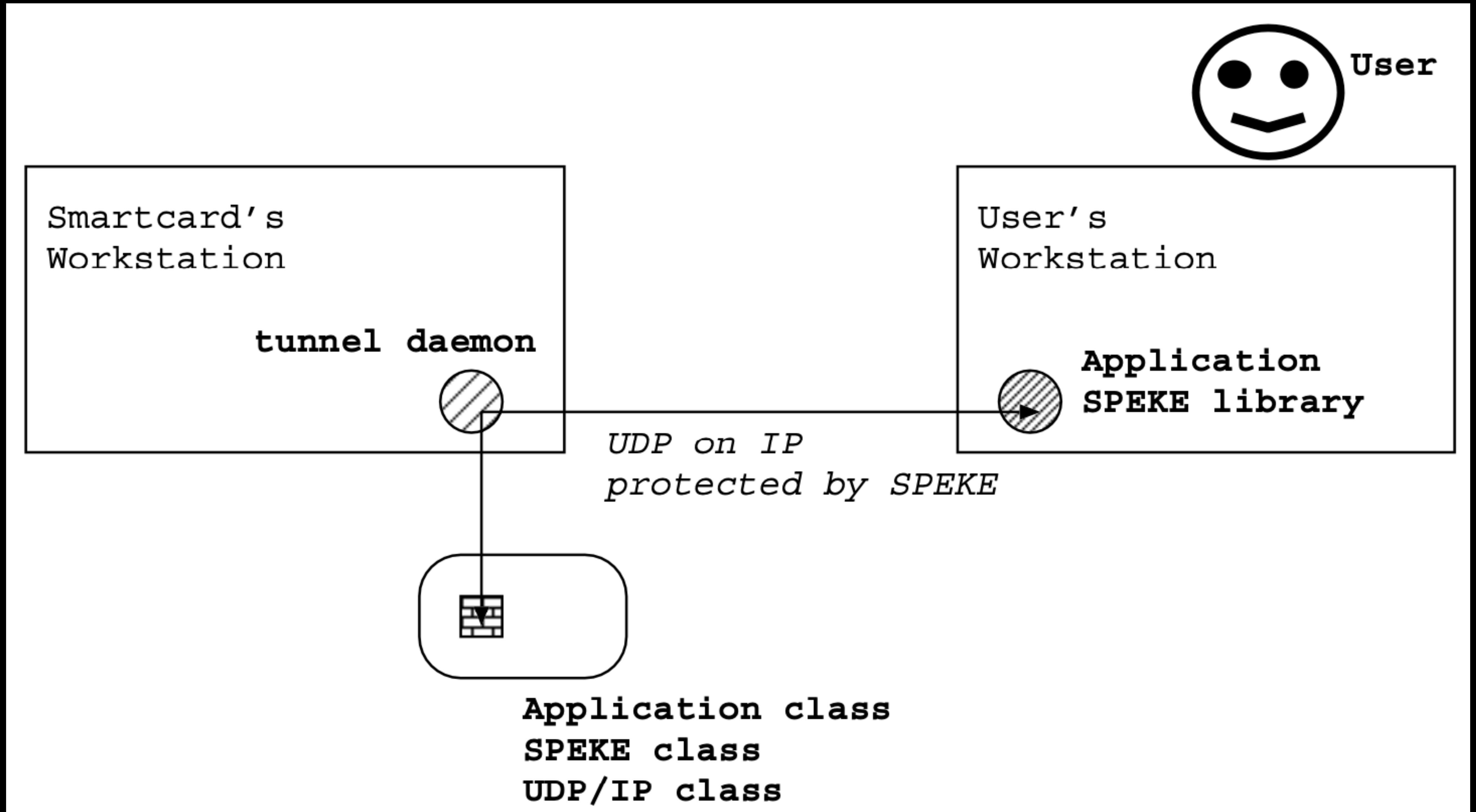
aglo
@
HEIMDAL.CITI.UMICH.EDU
TODOS
ARGOS MINI

Microsoft Windows Smart Card Toolkit
Cyberflex the card for Java
Who wouldn't be attracted to a Smart Card that supports Java?
Schlumberger
TODOS
ARGOS MINI
DataKey
MODEL 330
PKI Smart Card
CITIBANK
ENT USER NAME ATEST >
12345ENT

Secure Internet Smartcards

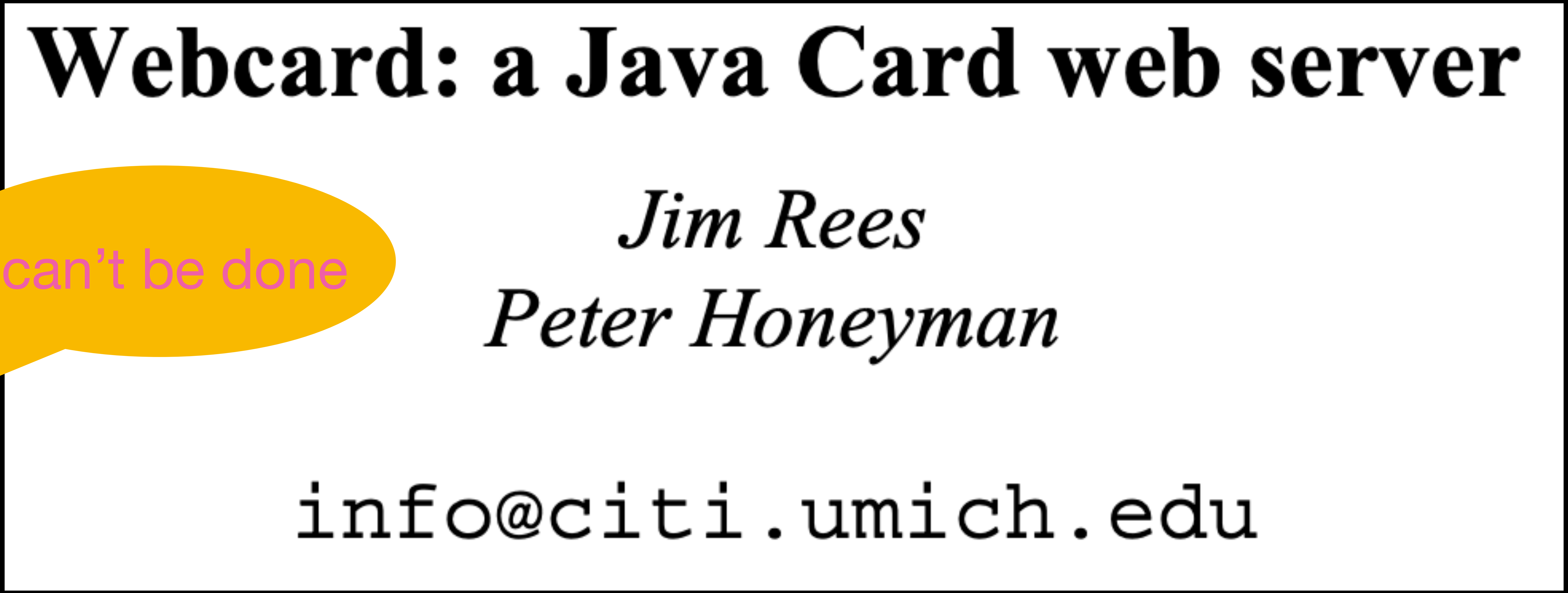
Naomaru Itoi, Tomoko Fukuzawa, and Peter Honeyman

Program in Smartcard Technology
Center for Information Technology Integration
University of Michigan
Ann Arbor
http://www.citi.umich.edu/projects/smartcard/



time (s)	events
0.00	kinit start
0.02	SPEKE connect start
0.03	Host send SPEKE1 (connect request)
0.03	Host send SPEKE2 (Q_A)
2.07	Host recv SPEKE1 (Q_B)
3.56	Host recv SPEKE2 (connect ok)
3.56	get_key_num start
5.88	get_key_num finish
5.88	decrypt ticket start
9.93	decrypt ticket finish
9.93	decrypt ticket start
12.80	decrypt ticket finish
12.80	kinit end

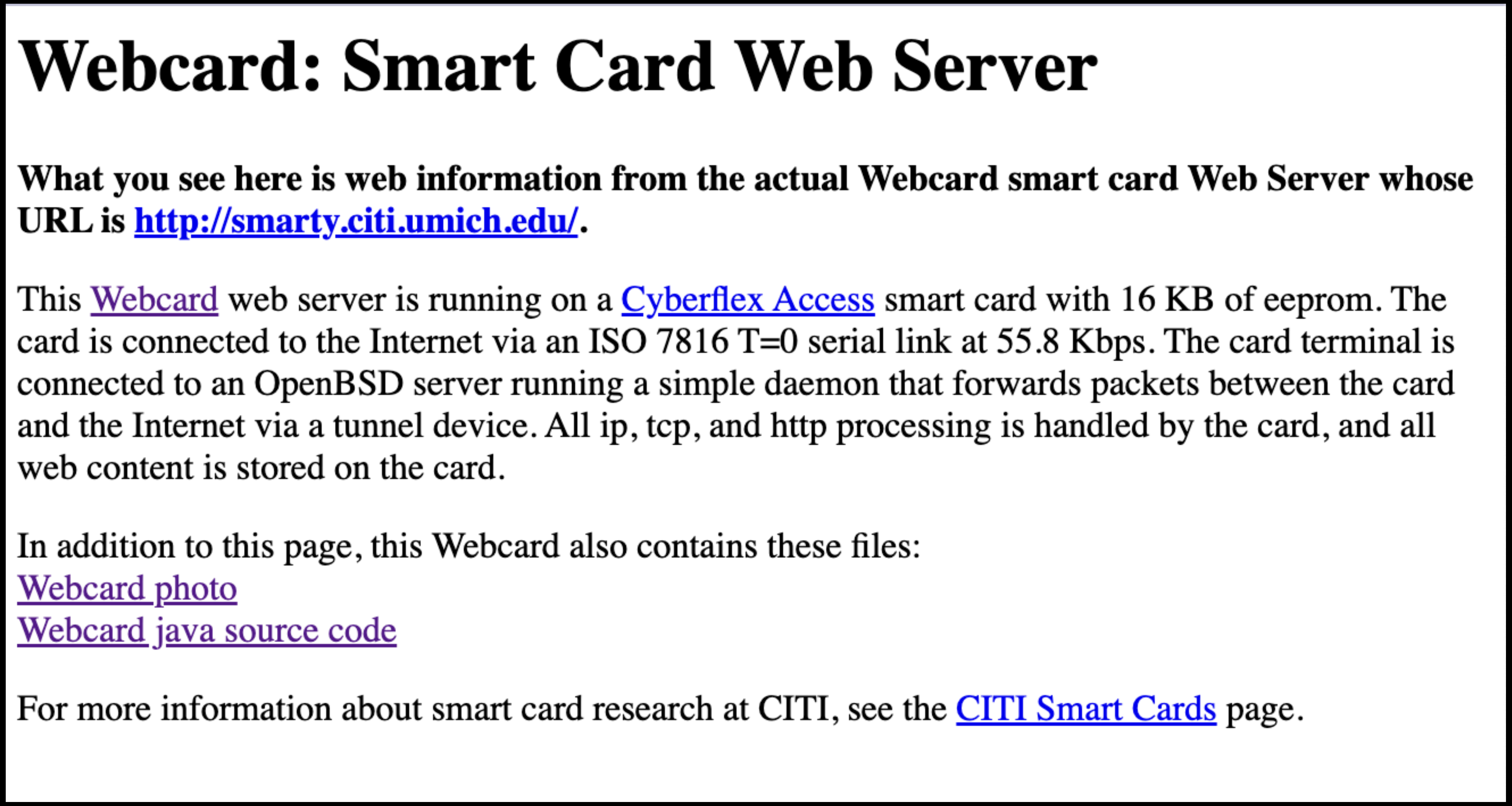
it can’t be done



Webcard: a Java Card web server

Jim Rees
Peter Honeyman

info@citi.umich.edu



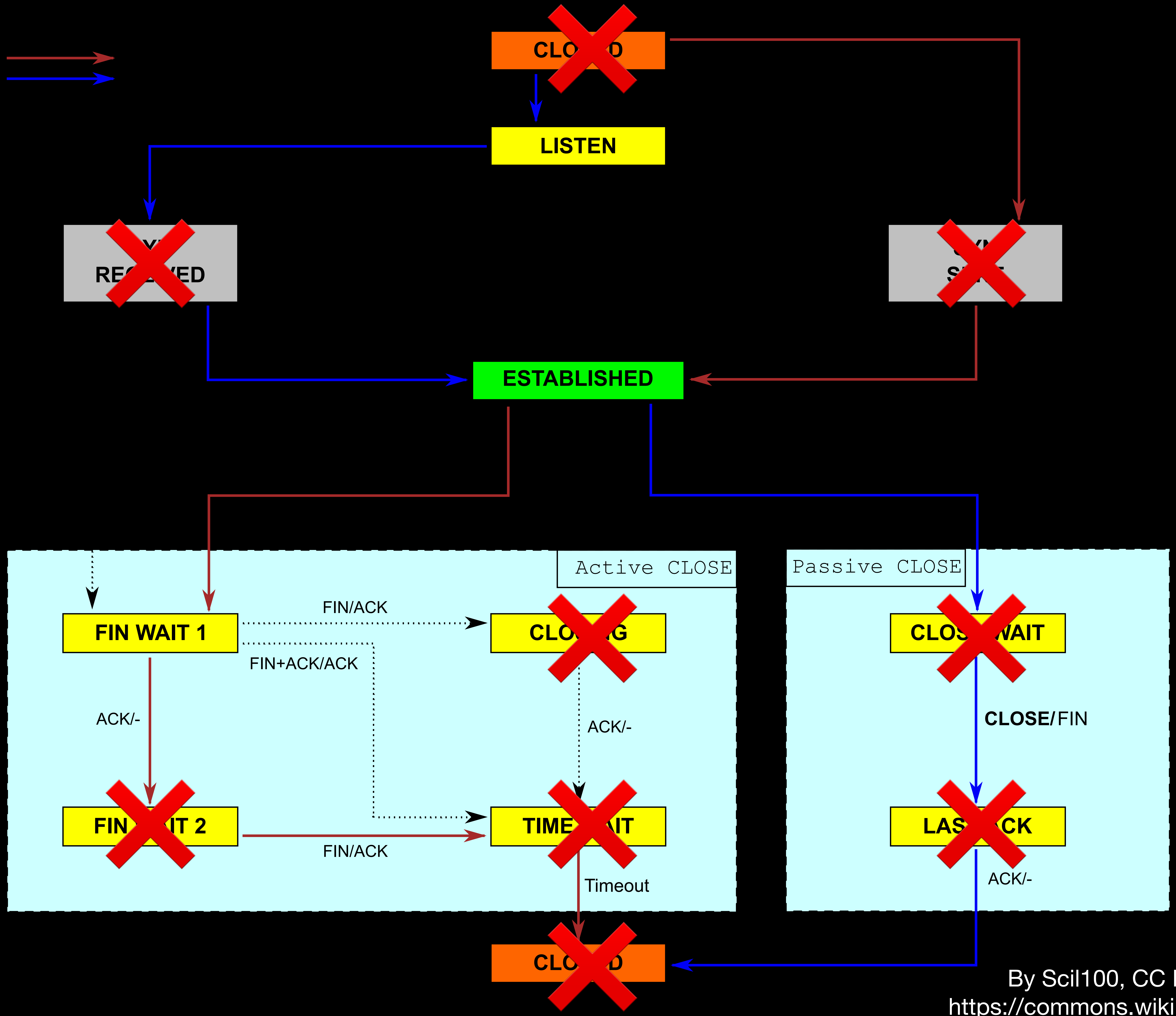
Webcard: Smart Card Web Server

What you see here is web information from the actual Webcard smart card Web Server whose URL is http://smarty.citi.umich.edu/.

This Webcard web server is running on a Cyberflex Access smart card with 16 KB of eeprom. The card is connected to the Internet via an ISO 7816 T=0 serial link at 55.8 Kbps. The card terminal is connected to an OpenBSD server running a simple daemon that forwards packets between the card and the Internet via a tunnel device. All ip, tcp, and http processing is handled by the card, and all web content is stored on the card.

In addition to this page, this Webcard also contains these files:
Webcard photo
Webcard java source code

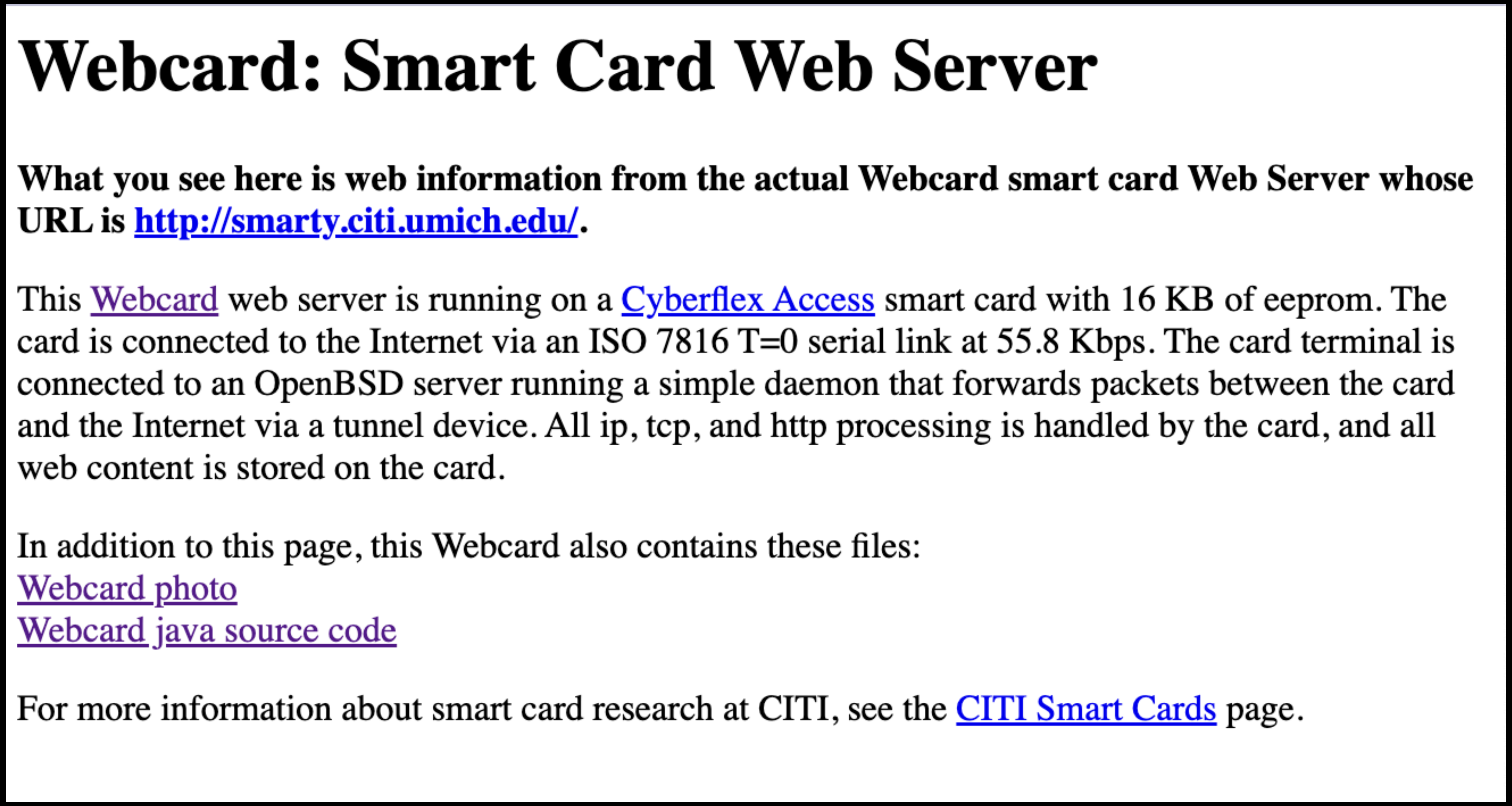
For more information about smart card research at CITI, see the CITI Smart Cards page.


CLO D
LISTEN
RE ED
S
ESTABLISHED
Active CLOSE
Passive CLOSE
FIN WAIT 1
FIN/ACK
CLO G
FIN+ACK/ACK
CLOS WAIT
ACK/-
ACK/-
CLOSE/FIN
FIN IT 2
FIN/ACK
TIME IT
LAS CK
Timeout
ACK/-
CLO D

Webcard: a Java Card web server

Jim Rees
Peter Honeyman

info@citi.umich.edu



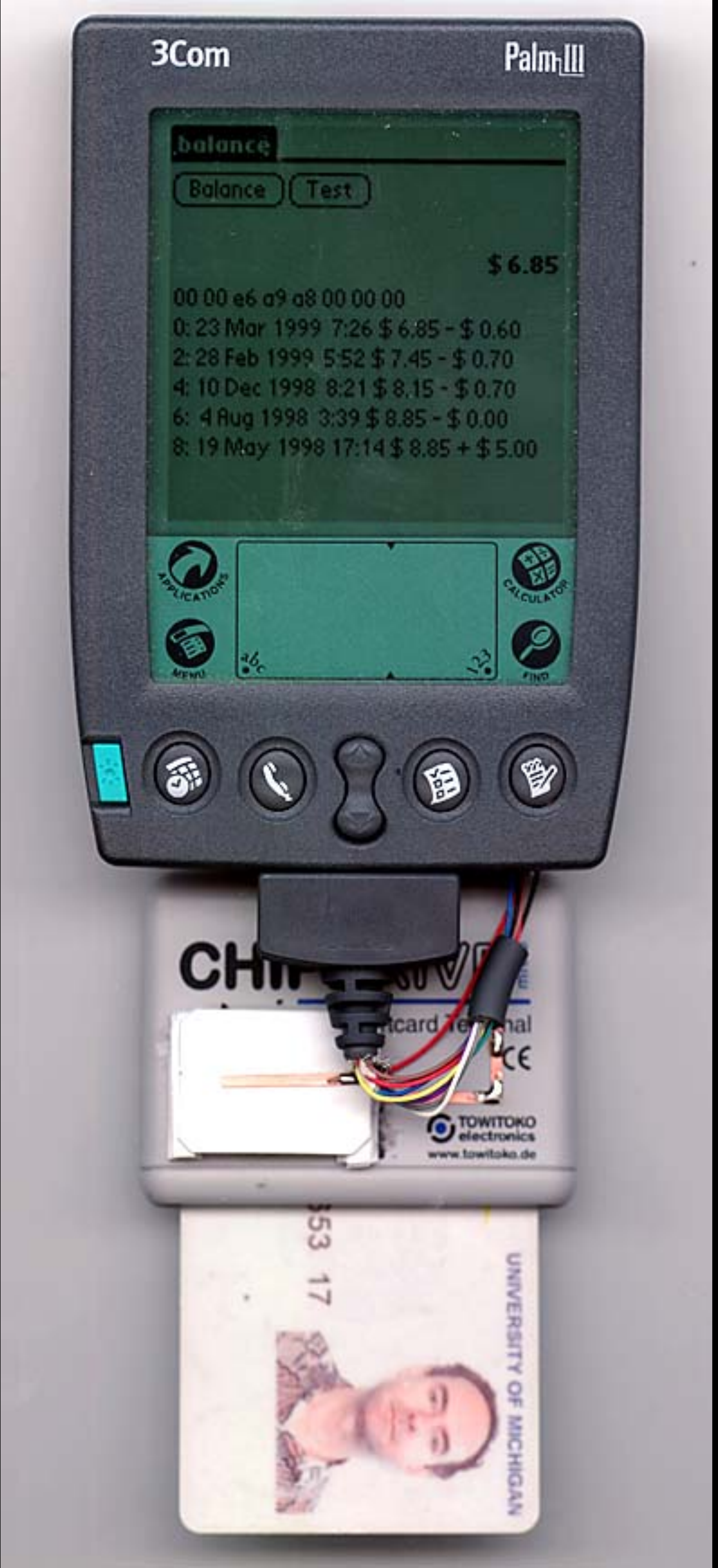
Webcard: Smart Card Web Server

What you see here is web information from the actual Webcard smart card Web Server whose URL is http://smarty.citi.umich.edu/.

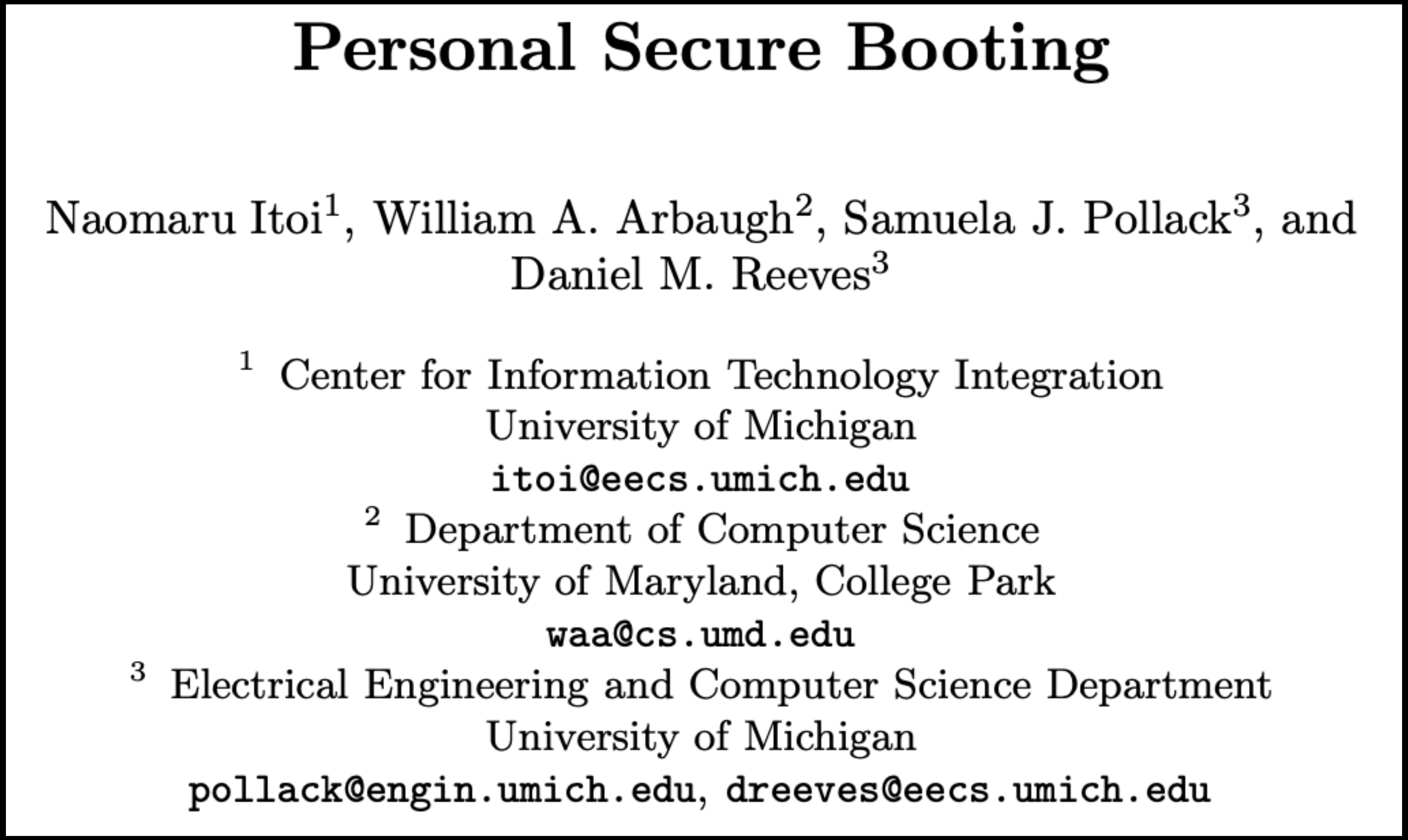
This Webcard web server is running on a Cyberflex Access smart card with 16 KB of eeprom. The card is connected to the Internet via an ISO 7816 T=0 serial link at 55.8 Kbps. The card terminal is connected to an OpenBSD server running a simple daemon that forwards packets between the card and the Internet via a tunnel device. All ip, tcp, and http processing is handled by the card, and all web content is stored on the card.

In addition to this page, this Webcard also contains these files:
Webcard photo
Webcard java source code

For more information about smart card research at CITI, see the CITI Smart Cards page.



```
balance
Balance  Test
                                   $ 6.85
00 00 e6 a9 a8 00 00 00
0: 23 Mar 1999 7:26 $ 6.85 - $ 0.60
2: 28 Feb 1999 5:52 $ 7.45 - $ 0.70
4: 10 Dec 1998 8:21 $ 8.15 - $ 0.70
6:  4 Aug 1998 3:39 $ 8.85 - $ 0.00
8: 19 May 1998 17:14 $ 8.85 + $ 5.00
```

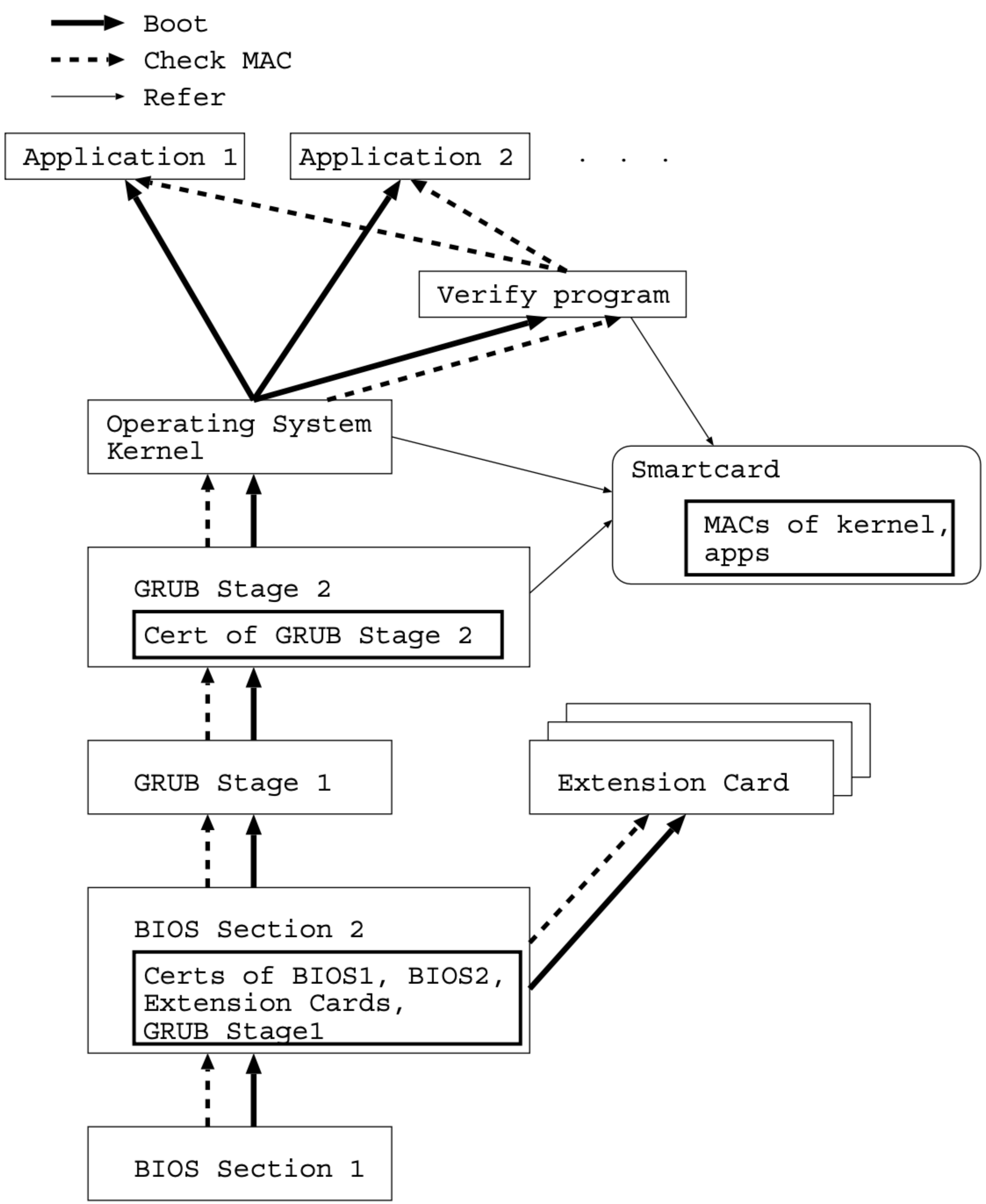


Personal Secure Booting

Naomaru Itoi[1], William A. Arbaugh[2], Samuela J. Pollack[3], and Daniel M. Reeves[3]

[1] Center for Information Technology Integration
University of Michigan
itoi@eecs.umich.edu
[2] Department of Computer Science
University of Maryland, College Park
waa@cs.umd.edu
[3] Electrical Engineering and Computer Science Department
University of Michigan
pollack@engin.umich.edu, dreeves@eecs.umich.edu

[W]e have developed a system called sAEGIS, which embraces a smartcard as personal secure storage for computer component hashes, and uses the hashes in a secure booting process to ensure the integrity of the computer components.



tasty, Balanced Choice snacks!
Get less than 30% calories from fat
Look for the for tasty, Balanced Choice snacks!
COLD
DRINK

a vending machine protocol

1. vending machine checks that the purse has sufficient funds
2. cardholder makes and receives a selection
3. vending machine updates the purse

Message to MCard	MCard response
RESET	I’m awake!
How much $$$ in the purse?	$18.23
Last entry in transaction log?	$18.23
Authenticate me: give me a nonce	Here is a nonce
Nonce encrypted with shared key	Vending machine is authentic
Reserve $1.25 in the transaction log	OK

phase 1: before the selection

1.25
A
1
B
2
C
3
D
4
E
5
MCARD
Value $ 18.23
Make a Selection
Insert MCARD Only
Insert
Here

Message to MCard	MCard response
Give me a nonce	Here is a nonce
Debit $1.10 from the purse, authenticated with encrypted nonce	👍🏽
Another nonce-based authentication	Thou art truly an authentic vending machine
Log the $1.10 transaction	👍🏽

phase 2: after the selection

0 grams
Trans Fat
Lay's
BRAND
Classic
Potato Chips

why?

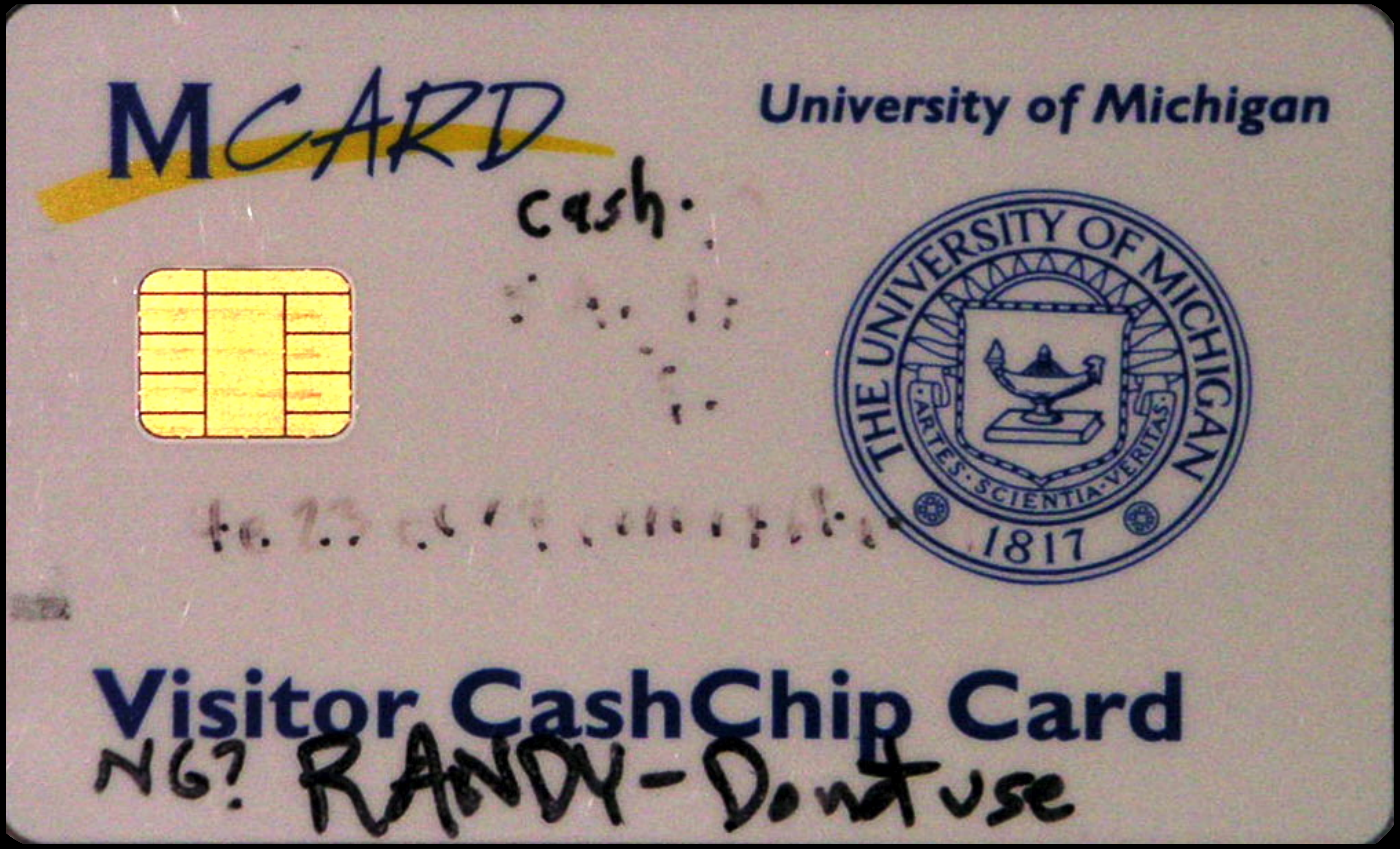
candidate protocol

1. Mutually authenticate
2. Check purse value
3. Customer makes selection
4. Update the purse
5. Deliver the selection
6. Eject card

ACCEPTS $1 BILLS
INSERT BILL HERE
SENSATIONS
McCOY'S
FLAME GRILLED STEAK
KitKat
Old Dutch

MCARD
return
DELL
Butterfinger
100 GRAND
ROLD GOLD

responsible disclosure



Message to MCard	MCard response
RESET	I’m awake!
How much $$$ in the purse?	$18.23
Last entry in transaction log?	$18.23, like I said
Authenticate me: give me a nonce	Here is a nonce
Nonce encrypted with shared key	Vending machine is authentic
Reserve $1.25 in the transaction log	OK

Phase 1: before the selection

$100 F
SILVER TRADING COMPANY, LLC
WWW.SILVERTRADING.NET

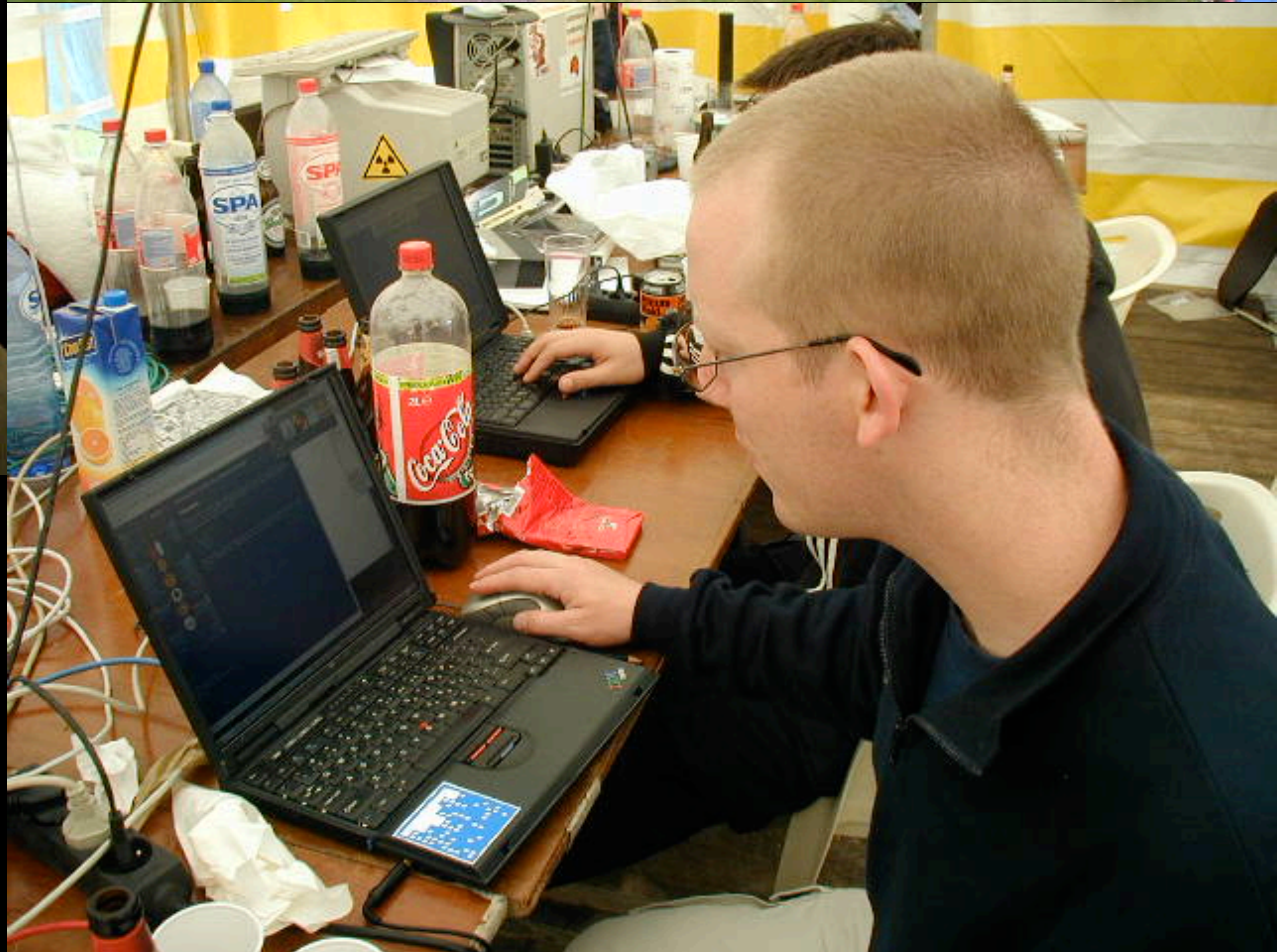
we spent it all

- Itoi, N., Honeyman, P. Pluggable authentication modules for Windows NT. *2nd USENIX Windows NT Symposium* (Seattle, 1998).
- Itoi, N., Honeyman, P. Practical security systems with smartcards. *IEEE 7th Workshop on Hot Topics in Operating Systems* (Rio Rico, 1999).
- Itoi, N., Honeyman, P. Smartcard integration with Kerberos v5. *USENIX Workshop on Smartcard Technology* (Chicago, 1999).
- Itoi, N., Honeyman, P., Rees, J. SCFS: a UNIX filesystem for smartcards. *USENIX Workshop on Smartcard Technology* (Chicago, 1999).
- Itoi, N., Fukuzawa, T., Honeyman, P. Secure Internet Smartcards. *1st International JavaCard Workshop* (Cannes, 2000).
- Rees, J., Honeyman, P. WebCard: a Java Card web server. *IFIP TC8/WG8.8 4th Working Conference on Smart Card Research and Advanced Applications* (Bristol, 2000).
- Itoi, N., Arbaugh, W.A., Pollack, S.J., Reeves, D.M. Personal Secure Booting. *6th Australasian Conference on Information Security and Privacy* (Sydney, 2001).
- Itoi, N. *Integrating Secure Hardware into Modern Security Systems: Authentication, Secure Storage, and Secure Bootstrap*. Doctoral dissertation, University of Michigan, 2001.

CHAOS
COMMUNICATION
CAMP

OpenBSD
OPENBSD
OpenBSD
OpenBSD
OpenSSH

XS4ALL


SPA
Coca-Cola

aftermath

acknowledgements

- CITI
  - Jim Rees
  - Naomaru Itoi
  - Brahm Windeler
- Bellcore
  - Avi Rubin
- Schlumberger
  - Scott Guthery
  - Tim Jurgenson
  - Bertrand du Castel

dodging the feds

thank you

5/
5/28/02
5/29/02
5/28/02
5/28/02
5/26/02
5/28/02
5/26/02
5/29/02
5/26/
5/26/02
5/28/02
5/29/02
ALEX
6/1
WYTSE
5/28/02
ROP
6/1/02
JOS
VISSER
5/ /02

SANE
Ruby Lounge
Wrangler