COMPUTER SECURITY HISTORY WORKSHOP

11-12 July 2014

Charles Babbage Institute
University of Minnesota

8:00 Breakfast
8:30 Welcome & Introductions
8:45 CBI project overview
9:20 break
9:30 Session 1
tinyurl.com/cbi-cshw

WELCOME & INTRODUCTIONS

1.5 days: 13+1 papers (in volume)

- 1 Conceptual Foundations (J. Epstein)

- 2 Industry Foundations (T. Benzel)

- 3 Law & Privacy (C. Landwehr)

- 4 Identity & Anonymity (R. Bace)

➡️revise for *IEEE Annals Hist. Comp.*

WELCOME & INTRODUCTIONS

program notes

- Aspray & Cortada *split into* Aspray (2C oral) + Cortada (2D written)

- Saturday: 20-min cavern tour (1:00) 45-min cavern tour (2:15)

- NSF.TC 1116862 'Building Infrastructure for Computer Security History'

-

WELCOME & INTRODUCTIONS

workshop sessions

- present in <u>20</u> mins

- discuss for <u>15</u> mins

- change speakers in ~<u>3</u> mins (slides/PDF before to Tom or laptop)

WELCOME & INTRODUCTIONS

who is who . . . ?

- Donn Parker (<u>you</u> should <u>do</u> this!)
- Tom Misa (CBI director)
- Jeff Yost (CBI assoc. director)
- Katie Charlet (CBI admin)
- R. Arvid Nelsen (CBI <u>archivist</u>: lunch)
- NSF-TC (Landwehr + Epstein)

WELCOME & INTRODUCTIONS

where to go for …?

- breakfast, coffee, lunch = here AL 120
- dinner = Campus Club 4th floor Coffman (East Bank across river)
- restrooms = AL *opposite* side
- wi-fi = 'UofM Guest'
- CBI = AL 211

WELCOME & INTRODUCTIONS

candid discussion among 'strangers'?

•different backgrounds, communities, concepts, perspectives (OK!)

•watch jargon + acronyms

•ask (expect) clarifying questions

•please 'mix' at meals

WELCOME & INTRODUCTIONS

origins of CBI

- Erwin Tomash (MN+CA) f. 1978
- computer history needs place: document + oral histories + research
- U Minnesota 'Digital State' 1980
- Arthur Norberg (1981--2005)

WELCOME & INTRODUCTIONS

CBI today

- support: College + ULibraries + HST + ERA chair + fundraising + grants*
- 4 staff + students + GSRA + 2x SRF
- 400 oral histories (+600 FastLane)
- 200 archival collections [Sat. tours]
- infrastructure for computer history

CBI builds infrastructure

- ... companies, sci instrument, ARPA-IPTO, software, FastLane

- oral histories (20K/yr ▶ /month)
cbi.umn.edu/oh

- documents, reports, letters, notebook (inside view: why+how?)
cbi.umn.edu/collections/archmss.html

CBI's Computer Security dox

- Donn Parker purl.umn.edu/40845
- Willis Ware purl.umn.edu/41431
- Walter Anderson (GAO)
- Carl Hammer (DPMA, ACM)
- SHARE, Inc (security sessions)
- IBM Data Security Manuals
- David Cavanagh (Sun Life + I-4)

CBI's Computer Security OH

- James Bidzos (2004)
- Martin Hellman (2004)
- Donn Parker (2003)
- Willis Ware (2003)
- Peter Patton (2000)
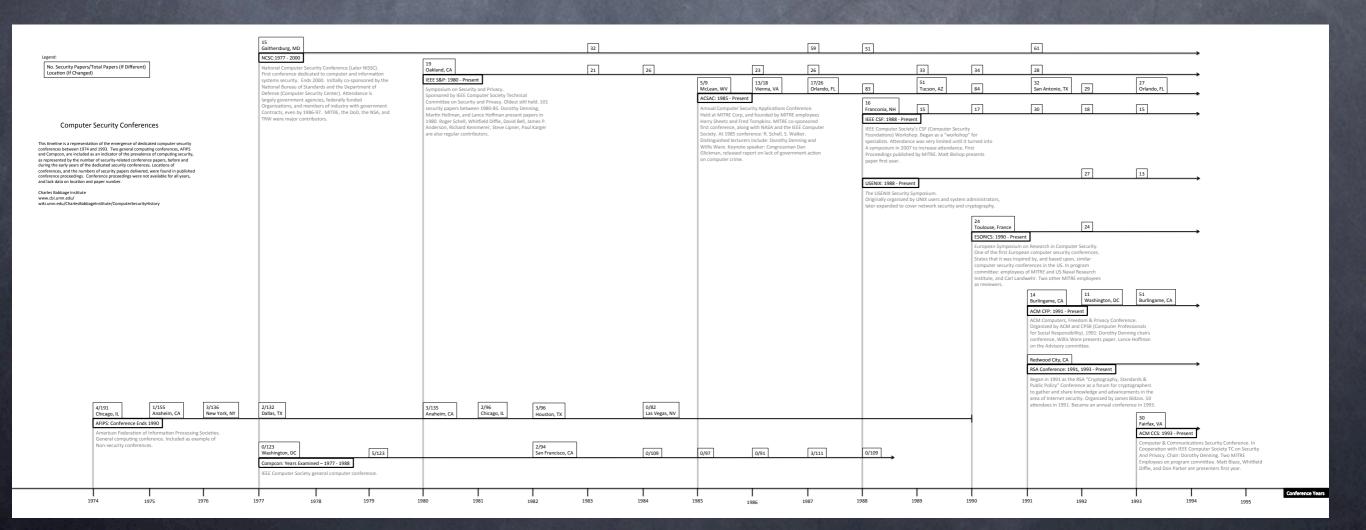
Computer Security project goals

- conduct 30 OH [▶ Jeff]

- knowledge-networking wiki

- publish scholarship [▶ Jeff]

- create security-history community

Computer Security wiki

- wiki.umn.edu/CBI_ComputerSecurity/
- Current activities, Who is who
- open: completed interviews
- People (174); Programs (16); Publications* (29); Systems* (24); Events (30)

Computer Security timeline

- wiki.umn.edu/CBI_ComputerSecurity/PubTimeline

- security conferences 1974-93

Computer Security Conferences

This timeline is a representation of the emergence of dedicated computer security conferences between 1974 and 1993. Two general computing conferences, AFIPS and Compcon, are included as an indicator of the prevalence of computing security, as represented by the number of security-related conference papers, before and during the early years of the dedicated security conferences. Locations of conferences, and the numbers of security papers delivered, were found in published conference proceedings. Conference proceedings were not available for all years, and lack data on location and paper number.

Charles Babbage Institute
www.cbi.umn.edu/
wiki.umn.edu/CharlesBabbageInstitute/ComputerSecurityHistory

Legend:
No. Security Papers/Total Papers (If Different)
Location (If Changed)

15 — Gaithersburg, MD — NCSC:1977 - 2000
National Computer Security Conference (Later NISSC). First conference dedicated to computer and information systems security. Ends 2000. Initially co-sponsored by the National Bureau of Standards and the Department of Defense (Computer Security Center). Attendance is largely government agencies, federally funded Organizations, and members of industry with government Contracts, even by 1986-97. MITRE, the DoD, the NSA, and TRW were major contributors.

19 — Oakland, CA — IEEE S&P: 1980 - Present
Symposium on Security and Privacy. Sponsored by IEEE Computer Society Technical Committee on Security and Privacy. Oldest still held. 101 security papers between 1980-85. Dorothy Denning, Martin Hellman, and Lance Hoffman present papers in 1980. Roger Schell, Whitfield Diffie, David Bell, James P. Anderson, Richard Kemmerer, Steve Lipner, Paul Karger are also regular contributors.

ACSAC: 1985 - Present
Annual Computer Security Applications Conference. Held at MITRE Corp, and founded by MITRE employees Harry Sheetz and Fred Tompkins. MITRE co-sponsored first conference, along with NASA and the IEEE Computer Society. At 1985 conference: R. Schell, S. Walker. Distinguished lecturers include: Dorothy Denning and Willis Ware. Keynote speaker: Congressman Dan Glickman, released report on lack of government action on computer crime.

16 — Franconia, NH — IEEE CSF: 1988 - Present
IEEE Computer Society's CSF (Computer Security Foundations) Workshop. Began as a "workshop" for specialists. Attendance was very limited until it turned into A symposium in 2007 to increase attendance. First Proceedings published by MITRE. Matt Bishop presents paper first year.

USENIX: 1988 - Present
The USENIX Security Symposium. Originally organized by UNIX users and system administrators, later expanded to cover network security and cryptography.

24 — Toulouse, France — ESORICS: 1990 - Present
European Symposium on Research in Computer Security. One of the first European computer security conferences. States that it was inspired by, and based upon, similar computer security conferences in the US. In program committee: employees of MITRE and US Naval Research Institute, and Carl Landwehr. Two other MITRE employees as reviewers.

14 — Burlingame, CA / 11 — Washington, DC / 51 — Burlingame, CA — ACM CFP: 1991 - Present
ACM Computers, Freedom & Privacy Conference. Organized by ACM and CPSR (Computer Professionals for Social Responsibility). 1991: Dorothy Denning chairs conference, Willis Ware presents paper. Lance Hoffman on the Advisory committee.

Redwood City, CA — RSA Conference: 1991, 1993 - Present
Began in 1991 as the RSA "Cryptography, Standards & Public Policy" Conference as a forum for cryptographers to gather and share knowledge and advancements in the area of Internet security. Organized by James Bidzos. 50 attendees in 1991. Became an annual conference in 1993.

4/191 — Chicago, IL / 1/155 — Anaheim, CA / 3/136 — New York, NY / 2/132 — Dallas, TX / 3/135 — Anaheim, CA / 2/96 — Chicago, IL / 3/96 — Houston, TX / 0/82 — Las Vegas, NV — AFIPS: Conference Ends 1990
American Federation of Information Processing Societies. General computing conference. Included as example of Non-security conferences.

0/123 — Washington, DC / 2/94 — San Francisco, CA — Compcon: Years Examined ~ 1977 - 1988
IEEE Computer Society general computer conference.

30 — Fairfax, VA — ACM CCS: 1993 - Present
Computer & Communications Security Conference. In Cooperation with IEEE Computer Society TC on Security And Privacy. Chair: Dorothy Denning. Two MITRE Employees on program committee. Matt Blaze, Whitfield Diffie, and Don Parker are presenters first year.

Conference Years

1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995

Computer Security Multics

- wiki.umn.edu/CBI_ComputerSecurity/SystemsMultics

- Multics: origins, security, 'object'

- collect fragments [3600 words]

- Yost 2 weeks at MIT Archives (MAC Saltzer + Corbató papers)

- aim to publish 'complete story'

- tinyurl.com/cbi-cshw

Charles Babbage Institute–"Building an Infrastructure for Computer Security History"
The Oral History Component (and related presentation/publication efforts)
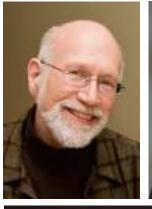NSF Sponsored Project # 1116862

Oral Histories

- CBI—more than 3 decades of leadership in IT oral histories

This project (to date):

- 24 of 30 conducted
- 20 available
- 1,712 transcript pp.

Methodology:

Extensive targeted research; 2-4 hr. Interviews; transcription; interviewer and interviewee editing; published online on searchable database

Roger Schell
Barry Schrager
Rebecca Bace
Steve Lipner
David Bell
Tom Van Vleck
Steve Walker
Eldon Worley
Peter Denning
Dorothy Denning
Peter Neumann
Susan Nycum
Teresa Lunt

Matthew Bishop
Karl Levitt
Daniel Edwards
Seymour Goodman
William Murray
Robert Johnston
Eugene Spafford
Marv Schaefer
Carl Landwehr
John McLean
Richard Kemmerer

How have we decided who to interview

- Seminal/pioneering contributors to the computer security field in the 1960s-1980s (focus pre-Web era)

- Expert advice from our advisory committee

    (Bace, Bishop, Johnston, Katzke, Lipner, Murray, Odlyzko, Parker, and Spafford)—list of roughly 120 key pioneers.

- Clusters—to gain insight and multiple perspectives, and achieve a degree of depth on targeted themes to create research opportunities for ourselves and others

Some of Our Themes/Clusters

- **High Assurance/TCSEC**— (Schell, Lipner, Bell, Walker, D. Denning, Neumann, Edwards, Schaefer, Landwehr, McLean, Kemmerer)

- **Multics** (Neumann, Van Vleck, P. Denning, Lipner, Schell)

- **Intrusion Detection** (Bace, D. Denning, Lunt, Neumann, Bishop, Spafford, Levitt, Kemmerer)

- **Research Program Leadership** (Schell, Walker, Bace, Lunt, Landwehr, Levitt)

- **Industry** (Shrager, Worley, Murray, Johnston, Walker, Bell, Van Vleck, Lipner, Schell)

- **Education** (P. Denning, D. Denning, Bishop, Levitt, Spafford, Kemmerer)

2014 Presentations from Project Research

Yost   Business History Conference (computer security and corporate responsibility)-Presented in March

CBI Workshop (industry origins)-July

Business History Society of Japan (cooperative organizations—IBM Share and CSI)-Sept.

SHOT (IDES/NIDES)-Nov.

Lewis SHOT (US Computer Scientists Trip Reports on USSR in late 1950s and 1960s)-Nov.

Publication Plans/Efforts Underway

- Two special issues approved by editorial board of *IEEE Annals of the History of Computing* for CBI Workshop papers—Misa and Yost (co-guest editors).

- N. Lewis "Cybernetics and the Death of Stalinism: Soviet Computing Through the Eyes of Western Experts." (two part article)—submitted to *IEEE Annals*

- J. Yost, "The March of IDES: A History of the Intrusion Detection Expert System."—draft manuscript completed

- T. Misa, J. Yost, and N. Lewis—Plans for Multics security article (based on Corbato and Saltzer Papers at MIT Archives, OHs)