Reflections on 54 Years of Mainframe Security

Barry Schrager
Founder – SHARE Security Project
Architect and Primary Author of ACF2
BSchrager@cptglobal.com
(970) 331-1143

About Me, Barry Schrager

- Formed the **SHARE Security Project** in 1972 which created the requirements for today's mainframe security systems
- In 1973, one of 20 customers invited to Poughkeepsie to review the new MVM (later renamed MVS, now z/OS) Operating System before it was announced
- Architect and primary author of ACF2
- Honored to be a Member of the Mainframe Hall of Fame
  - With Dr. Gene Amdahl, Admiral Grace Hopper and Eldon Worley

Early 1970's – What Security?

- Only security was OS Data Set Passwords
- Bit in **Data Set Control Block** (DSCB) indicated Dataset was Password Protected (Same one RACF uses for Discrete)
- From **TSO** User had to enter password
- From Batch, Operator had to enter password
  - Written on paper and given to Operator 😐
  - Or kept in a notebook on the console ☹☹
- All passwords kept in a dataset named "PASSWORD" – in clear text!
  - It was password protected ☺
- And passwords were rarely changed
- No System Integrity: this was MVT

Protecting Data @ University of Illinois Chicago

- Our faculty and grad students were being harmed – data was getting deleted or modified – by accident or on purpose (some students were doing it for fun ;-( )
- I created Resident Account: **System Entry Validation for Batch & Time Sharing (TSO)** for common identification of users
- I had Eb Klemens intercept **Allocate, Open, Scratch, Rename** to control access:

Controlled by first character of second index:

- **$:** only accessible by Userid = High Level Index
- **#:** Readable by anybody, but only owner had write and allocate/delete control
- **Anything else:** no protection at all!

Meanwhile, at SHARE

- **1972:** I was asked to form the Security Project
- **1974:** Session on visions for Data Security
  - **Eldon Worley** (original author of RACF – 1976)
    - Eldon was a developer at IBM Research who created a package: Information Management Facility (IMF)
  - **Barry Schrager** (original author of ACF2 – 1978)
  - Gentleman from **Boeing**
- **Interesting footnote:** Years later, Eldon told me there were IBMers spread around the room tasked with viewing the audience reaction to determine if there was any interest in data security from their user community.

Back Then, the World Was Different

- Mainframe MIPS for an *entire* installation were generally less than 5!
- A gigabyte of DASD storage was a lot!
  - (IBM 2314: 29 MB!)
- Computer users were usually less than 50 – a hundred was a lot!
- Everyone knew everyone
- Time Sharing (TSO) was just being deployed!
- No common method (or no method at all) of user identification for batch, transaction systems like CICS, IMS and TSO!

Early Days of Mainframe Security

- **Dataset Passwords:** Entered by the User at their TSO terminal
- Or, for batch jobs, written on a piece of paper and given to the Operator or kept in a book by the Operator and entered into the console
- Ability to limit it only for read or write access/dataset deletion

Before the Security Products

- **1970:** IBM's Installation Management Facility (IMF) deployed internally (developed by IBM Research)
- **1976:** IBM's original RACF (early version of IMF)
  - This was Eldon Worley's personal work product – Information Management Facility
  - He had been working on it since the early 1970's – it included space management, etc.
  - No generic profiles – protected one dataset at a time
- **1978:** SKK's ACF2 (Broadcom/CA-ACF2)
- **1981:** CGA's Top Secret (Broadcom/CA-Top Secret)
- **1983:** Revised RACF with Protect All and Generic Profiles

The Project Stalled (Early Meetings)

- We could not get past System Integrity and kept inter-relating it with Data Security
- System Integrity is the inability of a user to bypass the standard interfaces of the Operating System
- System Integrity is a pre-requisite to Data Security in a multi-user computer system
- Otherwise, any access controls can be bypassed

But We Did Agree on Certain Requirements

- Security System should be part of Operating System
- Identification and Authentication of Users is the first level of security
- Security should not be able to be turned off by an authorized user
- Installations should be able to run a highly secure job alongside all other jobs and users
- Selectively invoke high overhead functions like overwriting datasets with zeros on an individual resource basis
- A designated interface program, for example a specific application program, should be supported as the only way to access a specific dataset. E.g. only a few users had full access, other users had the restricted access via the designated interface program

Relief

- In 1973 IBM Announced its new VS2 Release 2 Operating System (actually, the first release of MVS)
- It had a powerful System Integrity Statement
  - Note that it did not state there are no integrity exposures, but that, they knew of none and if one was reported, they will fix it
  - “If a user can access data in a manner not subject to management control, IBM will fix it”
- Our Project could now focus on the Data Security Requirements

1974 SHARE Security Project Requirements

- Common Identification and Validation of Users
- Centralized Resource Control Facility
- Centralized Security Violation Processing
- Designated Interface Programs
- Protection by Default
  - Error of Omission
- “Algorithmic grouping” of resources and users
  - ACF2 Pattern Masking, RACF Generic Profiles
  - ACF2 UID String

Protection by Default versus Protection by Itemization

The Error of Omission

- **With Protection by Default**
  - If you forget to give someone access permission, they call you up and yell at you, you fix it, buy them a beer, and you're friends again

- **With Protection by Itemization**
  - If you forget to protect something, it's public or modified!!!

OTHER SUGGESTIONS FROM 1972-1974

- Multi Factor Identification
  - Password/Badge Reader
  - 2 Badge Readers – one used by a guard
  - Fingerprints
  - Voice Prints
  - Lip Prints ☺

- More at: www.share-sec.com/history.html

1976: IBM Announces RACF

We were thrilled, but:

- At Summer SHARE meeting details came out:
  - **No protection by default (error of omission)**
    - Protection by itemization – one dataset at a time controlled by protected bit in DSCB
  - **No algorithmic grouping**
    - ACF2 pattern masking, RACF Generic Profiles
- IBM representative to project, Bill Murray, told me that, according to the RACF development group, these were not achievable
- When IBM asked users how much data would you protect, the answer was “about 5%”

At UIC – Access Control Facility Prototype

- Pattern masking (algorithmic grouping)
- Protection by default
- I wrote the rule compiler in PL/1
- And the rule interpreter in Assembly Language
- Eb Klemens' Open, Scratch, Rename, etc. intercepts
- JES2 Modifications by Scott Krueger
- Really basic TSO Command Interface
- I gave BOF Session at March 1977 SHARE
- Several companies wanted it – none got it implemented

U of I Declined Support for a Security Product

- We previously created **J/TIP – JES2/TSO Interface Product**, which provided job submission and sysout viewing and was licensed by the University to many sites, including the IBM Development Labs
- We presented the concept of a security product to the University, but they declined to support it
- Then, Ron Murray of London Life Insurance called and offered to support the development
- My manager, Dr. Tom Brown, Director of the Computer Center, said GO FOR IT!
- So, Eb Klemens, Scott Krueger and I went to London Ontario in February 1978 to create **ACF2**

General Motors

- Presented to General Motors in January 1978
  - GM employee was head of GUIDE Security Project, so we interacted with each other
  - GM Audit very unhappy with RACF –
    - Delco Div - 3% data protection after 18 months
    - GM Research at about 4% data protection
    - Auditor – "*We don't know what percentage should be protected, but we know that 3% ain't it!!*"
  - Auditor: "When you get it working, let us know"
  - I found out later that their actual goal was to get IBM to improve RACF!
    - By showing interest in ACF2 to prod IBM
    - It was not to actually purchase ACF2

General Motors: Pontiac Motor Division

- **Genesis:** GM sought an alternative to RACF, leading to the development and successful trial of ACF2 at Pontiac.
- **The "Personal" Era:** Pontiac Security Officer Gerry Lyons knew every user and dataset. Upon seeing his first ACF2 report, he could identify "Jack upstairs" he is accessing radio inventory to optimize year-end buildouts.
- **Visibility:** Security was intuitive; access was tied directly to a clear, local business purpose.
- **The Global Shift:** ACF2 eventually installed at 135 GM sites worldwide. But, this was before the internet, so it was really good at local user groups, etc.
- **Current Reality:** Now GM is consolidated to six sites, the scale is so vast that Security Officers can no longer personally know every user, dataset, or business justification for access.

Central Intelligence Agency (CIA)

- **The Connection:** Long-time SHARE colleague Barry Lewis invited me to present in DC after joining the Department of Labor.
- **The Technical Barrier:** Initially, a presentation seemed moot because Labor used MVT, an operating system without system integrity which was introduced with MVS.
- **The "Trust Me“ Moment:** Despite the incompatibility, Barry insisted on the meeting.
- **The Reveal:** A few weeks later, Barry moved to the CIA — his time at Labor had merely been a "waiting room" while his security clearance was processed.
- **The Result:** The CIA requested to test ACF2.

The CIA Conversation

- **The Follow-up:** One month after testing began, Barry Lewis shared a mix of "good and bad" news.
- **The IBM Vulnerability:** A flaw was discovered that belonged to IBM but could have been blocked by ACF2.
- **A Different Priority:** When I offered to fix it, Barry declined, joking that they might need to use the vulnerability for "hacking" themselves (this was 1979!).
- **Strategic Success:** Despite the flaw, the CIA purchased ACF2 and recommended it to 100 of their associates and subcontractors.
- **The Catch:** When asked for contact information to follow up on these leads, the response was "I can’t do that! You will just get calls“

SHARE ACF2 User Experience Session

- Are you going to purchase a security product from IBM or from these three guys? ☺
- In 1979 or 1980 – ACF2 User Experience Session
  - Linda Vetter of General Motors
  - Barry Lewis of the Central Intelligence Agency
- We could not use them as references, but, we could give out copies of their presentation ;-)

ACF2 Success Funded

- The first VM security product – ACF2/VM
  - Charlie Kao Product Architect
- The first Operating System Audit Product
  - Examine/MVS, aka CA-Examine, CA-Auditor
  - Martin King Product Architect

Success

- SKK Sold to UCCEL at end of 1986
- 2700 Installations Worldwide
  - Including the CIA, NSA, Britain's MI5, Federal Reserve System, FDIC, Senate, Office of the President, entire Australian Government, etc.
- 60% Market Share against IBM's RACF & CA's Top Secret
- Offices in London, Sydney, Brussels, Hong Kong and Chicago
- UCCEL acquired by CA in 1987
- CA acquired by Broadcom in 2018

But the world is different today

- Users –
  - Then a few dozen, and max a hundred or two
  - Now thousands
- The Security/Operations staff knew the users & data
  - Gerry Lyons of Pontiac Motor Division – looking at his first ACF2 dataset logging/violation report
    - That's Jack upstairs
    - That dataset contains the radio inventory
    - He's optimizing the model year build-out
      - You can't put an expensive radio in a cheap car
      - Or a cheap radio in an expensive car
    - Gerry knew all the users and all the corporate data and the business reason for the access

Now, Today's World of Mainframe Security

- Organizations only have a few datacenters, each servicing thousands of users
- Security Officers and Security Administrators do not know all the data and all the users and do not make access decisions for user access on their own
- There is an approval process for the Data Owners and User Managers to request these access permissions be implemented

But …

- Some employees have been around for decades
- And changed roles, got promoted, etc.
- Access permissions have changed over time
- Been given permissions based upon temporary projects, etc.
- But have all the old access permissions been removed?
- Is it a risk that some of them still carry some of their old access permissions?

Exposures of NPI – Non Public Information

Lax security controls – e.g. “Open Access” –
- Complacency – “our mainframe is secure”
- ACF2 UID(*) and RACF ID(*) and UACC(READ)
- Lack of real understanding about data security

Copies of production data
- Best of intentions – testing, etc. – not protected as well as production – not masked for privacy

Unprotected derivative data
- Reports & Database query results
- Backups

Common attack vector is obtaining “insider” credentials – lax controls and unprotected copies are really dangerous

Access permissions must be reviewed

- Where is the sensitive data stored? Who knows? What about copies?
  - I once was part of a development team for a product -- Datasniff
- Who has permission to view or update my department's sensitive data?
- What data do my employees have view or modify access for?
- As they change roles, employees sometimes accumulate access permissions over time

Access Analysis Reports

- When I was at EKC in the late1990's, I developed the following ACF2 reports (now from Vanguard):
  - Dataowner Dataset Reports – who has what access to my data?
  - Dataowner Resource Reports – who can execute my sensitive transactions?
  - Userowner Dataset Reports – what data can my employees access?
  - Userowner Resource Reports – what transactions can my employees execute?
- ACF2 provided reports, ACFRPTRX and ACFRPTXR, now provide this analysis
- zSecure provides similar reports for RACF
- Users accumulate additional access over time, but, the accumulated access, if not regularly reviewed, presents an exposure
- Access permissions must be periodically reviewed both from the data owner point of view and the user manager point of view

Vulnerability Issues

- Is the code delivered by IBM and ISV's secure?
  - Does each vendor make a "Statement of Integrity"?
- Do the installation-added SVC's and Exits have any integrity vulnerabilities in them?
- What about installation-added SVCs which deliberately alter the state of the caller? Are there any?
  - One of my Audit Findings -- The systems programming manager at a large firm called it secure because it was "password protected"– required "AUTH" in register 0 😐
- Can sensitive information be "ex-filtrated" via downloading the dataset to a PC or e-mailing from the mainframe?

Thank You

Questions & Comments?

Learn more about SHARE Security Project history:
SHARE_Security_and_Data_Management_Project__Data_Security_Requirements__1974.pdf
Great paper by Julie Ann Williams / New Era Software
Contact Barry Schrager: BSchrager@cptglobal.com
(970) 331-1143