LA-UR-17-30371
Approved for public release; distribution is unlimited.

Title: Cyber History in the DOE --The 414s

Author(s): Malin, Alex Barry

Intended for: Cyber Fire, 2017-11-16 (San Diego, California, United States)

Issued: 2017-11-13 (Draft)

Cyber History in the DOE

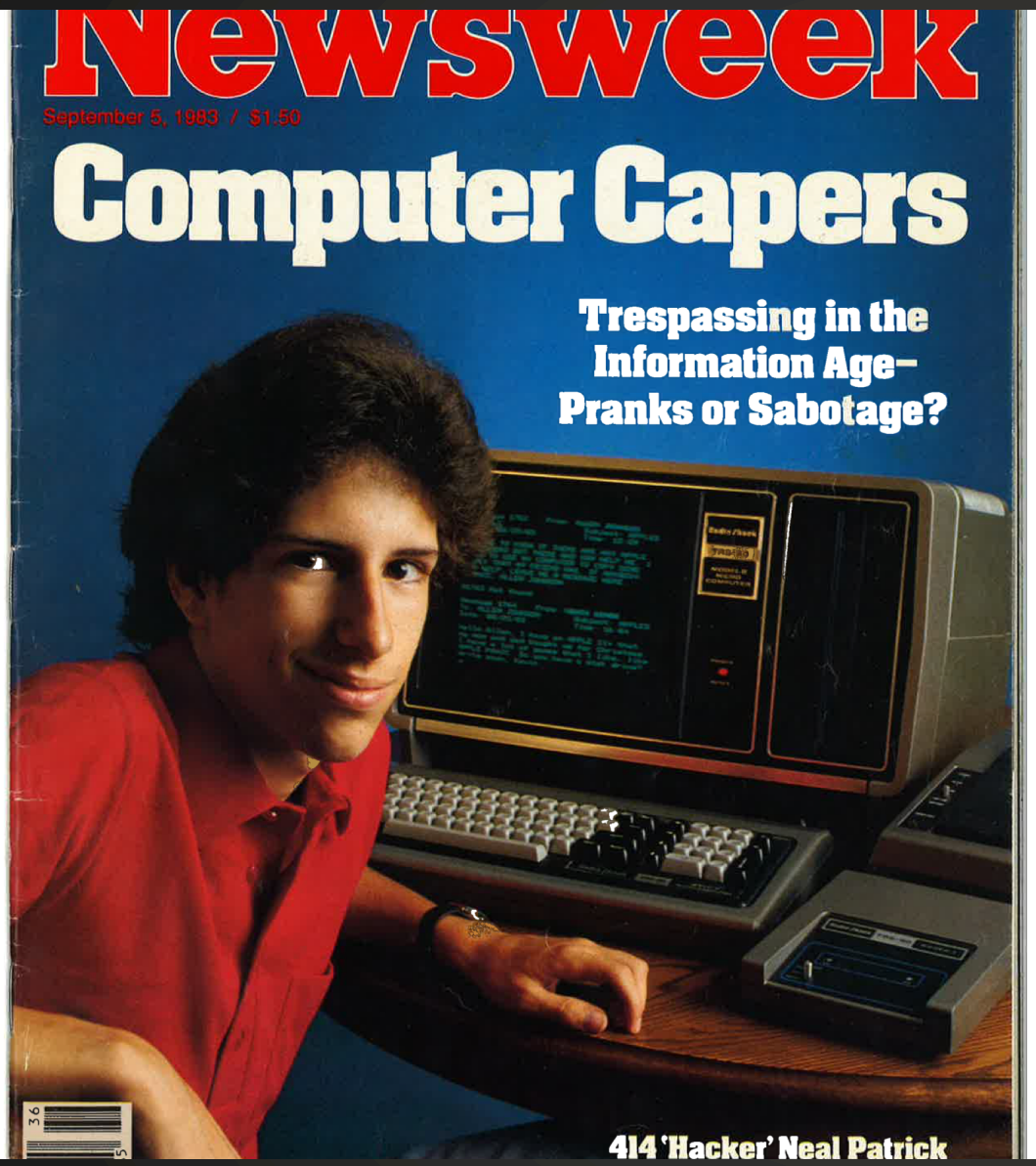
The 414s

Alex Malin

November 17, 2017

National Nuclear Security Administration

Operated by Los Alamos National Security, LLC for the U.S. Department of Energy's NNSA



- About the Cyber History Project
- Context: Insider Threats in DOE & early evolution of cyber threat
- The Milwaukee 414s aka The Boy Scouts

Rich & Important History

- **DOE Labs were targets as soon as remote access attacks were feasible**
  - Early adopters computer technology
  - Built & used early remote access technologies
  - Created early networks & connected these to many other networks
  - Repositories of valuable information related to diverse DOE missions
- **Somebody at probably every DOE Lab helped "invent" incident response and computer network defense**
  - Identify & engage these people
  - Collect and pass on their stories
  - Collect and archive records most important incidents and innovations

Incident Artifact Repository(s)

- **Neale's Incident Library / near term & long term archive**
  - Malware
  - Incident notes / case notes
  - Official reports
  - Email
  - Post mortems / white papers / lessons learned
  - Agency / auditor reports
  - Cyber history project interviews

We assume all documents protected as CUI unless formally reviewed and released.

Cyber History Project

- **Highlight & explore events that transformed DOE cyber security. Some examples:**
  - 1986 The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage (published 1989), by Clifford Stoll (LBL)
  - 1988 Morris Worm (Many DOE Labs)
  - 1999 Wen Ho Lee (LANL)
  - 2004 Stakkato (HPC / Many DOE Labs)
  - ACREM Incident (LANL)
  - 2008 – 2014 APT (All DOE Labs)

Cyber History Project

- **Articles, presentations and videos to collect and tell important stories**
  - Incidents
  - Computer network defense
- **Highlight historical patterns that permeate cyber security**
  - Are there lessons have we “learned” that we keep learning?
- **When future historians tell the story of the early days of the Internet, and computer incidents before the Internet, artifacts and stories archived in the Cyber History Project could prove a valuable resource**

Part 2 –The Legacy of Espionage

Theft of Nuclear Weapons Information Puts Spotlight on Insider Threat

- **Spies working for Manhattan Project voluntarily gave information to Soviet Union.**
- **August 29, 1949, Soviet Union tested its first atomic bomb**
- **Challenging to assess how much the stolen information helped the Soviets**
  - Soviet intelligence officials have often claimed critical importance
  - Little documented proof from Soviet Archives

- **Source: LANL Historian LA-UR-14-28986**

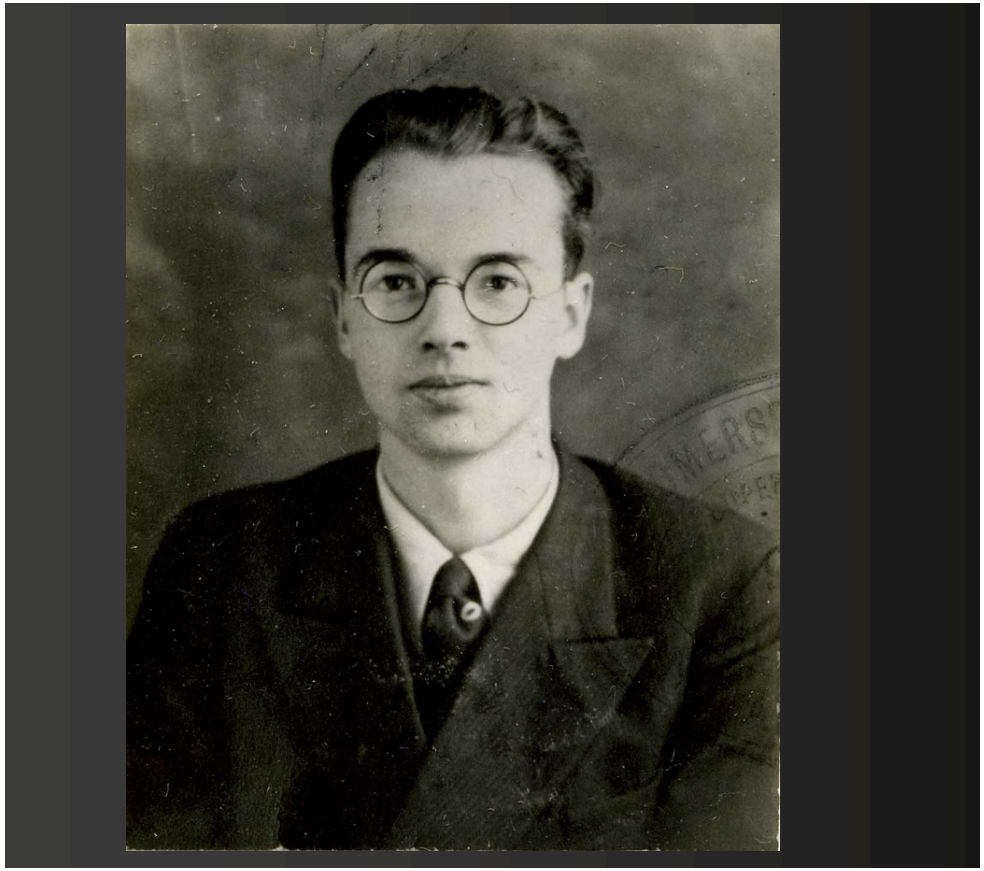
Manhattan Project Spy: Ted Hall

- **Graduated from Harvard 1944, age 18. Joined Manhattan Project at Los Alamos. Joined communist party and volunteered to spy.**
  - Code-named MLLAD, Hall was first to provide the Soviet Union with information directly from Los Alamos

- **Source: LANL Historian LA-UR-14-28986**
- **Photo from Wikipedia –Hall's LANL ID**

Manhattan Project Spy: Klaus Fuchs

- **Communist party member, fled Hitler's Germany. PHD from University of Bristol, 1937. Recruited for Britain's atomic bomb project. Volunteered to spy. Stole critical design information from Los Alamos**
  - Confessed to espionage, implicated his courier, Harry Gold, who implicated David Greenglass
- **Source: LANL Historian LA-UR-14-28986**
- **Photo: wikipedia.org**

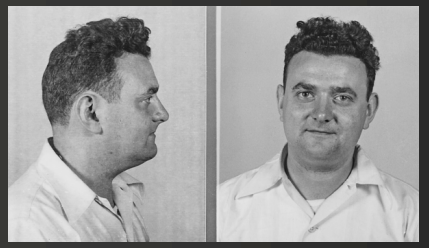


Manhattan Project Spy: David Greenglass

- **Machinist in Manhattan Project. Arrested in 1950, received reduced sentence and testified against his sister and her husband, Ethel & Julius Rosenberg**
  - Julius & Ethel Rosneburg died in the electric chair June 19, 1953
  - Greenglass recanted his testimony in 1996

Source: LANL Historian LA-UR-14-28986

Photo: wikipedia.org



History Research Questions

Manhattan Project spies! Legacy of insider threat!

- **What were the long term impacts of espionage to the practice of security and cyber security at DOE labs?**
- **When and how did DOE Labs adapt to the new threat was posed when sensitive information was processed and stored on computers? When these computers were initially assessable remotely?**
  - Were they proactive?
  - What incidents were most important? How?

Tentative Conclusions

- **Sensitivity to the insider threat impacted some early DOE lab remote access and network design**
  - Some early network pioneers at LANL grew up in Los Alamos during Manhattan Project. They baked security into design.
  - LANL deployed accounting tools in the mid 1970s
- **But that's not the entire story!**
  - Many DOE network pioneers believed it was more important to simplify and standardize than to maximize security
  - It is human nature to trust
  - Sometimes even security conscious people just want to make things work

Manhattan Project Spies & Insider Threat
A Legacy Impacting Cyber Security at DOE Labs

- **Conflicting objectives maximizing science maximizing security: arguably goes back to the earliest days of the Manhattan Project, exemplified by tensions & synergy between**
  - J. Robert Oppenheimer, Lab Director at Los Alamos
  - General Leslie R. Groves, headed the Manhattan Project for the Army Corps of Engineers

Part 3 –The 4-1-4s

Documentary film on 414s released 2015

Changes That Set Stage For 414 Incident

- New personal computing technology
- New remote access / network technology
- Social changes

DOE site network defenses in 1983 probably did not proactively account for the change in threat posed by the combination of technological and cultural changes

Commercially Availably Technology Personal Computing

- **Personal computers**
- **Modem**

Image courtesy pinterest.com

Tech Innovations

- **Remote Access**
  - Modems client / server
  - TELENET was first packet switched network available to general public
  - Arpanet
- **Pioneering networks at DOE sites**
  - First LANL production network linking multi-vendor equipment & multiple file systems in 1974 / 1975
  - DOE networks an interesting target for a curious intruder in 1980s
  - LANL deployed first security controller device 1976
    - Machine G was not behind the login control device

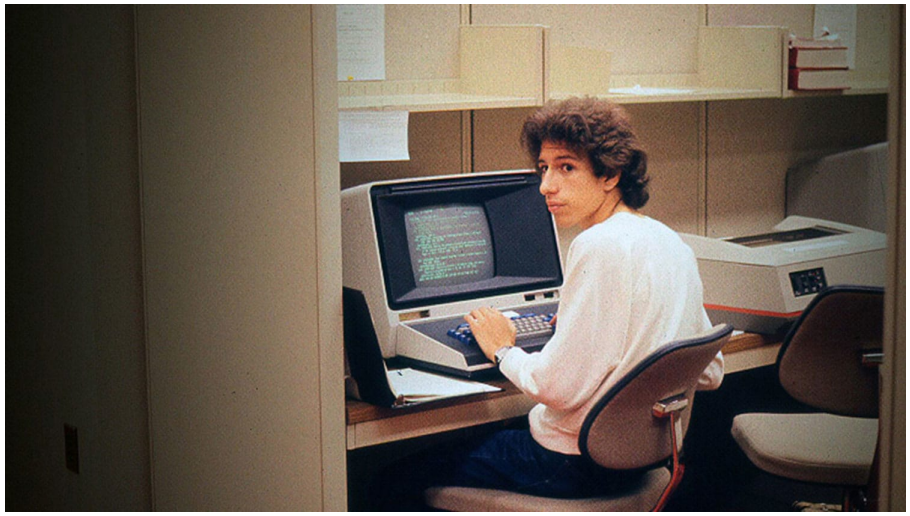
- **Source: (*https://en.wikipedia.org/wiki/Telenet)***
- **Source: Interview Cathy Stallings (LANL)**
- **Source: "The Route Less Taken" by Nicholas Lewis LA-UR-16-20103**

Cultural Change

- **Proliferation of computer clubs**
  - Bulletin boards to exchange electronic messages and information (including “how to” hack)
- **Morality of unauthorized access “hacking” was ambiguous in 1983**
- **1983 film WarGames glamorized hacking**
- **The 414s became the public face of the teen “whiz kid” in summer 1983**

414s Met at Explorer Scout Troup Computer Club Sponsored by IBM

- Their computer club met at Milwaukee IBM office
- They played with computers at school, in Explorer Scouts, at stores like Radio Shack, and at home
- Came up with name “4-1-4s” at a local park, noticing gang signatures



Source:http://www.cnn.com/2015/03/11/tech/computer-hacker-essay-414s/ Timothy Winslow

414s Began Playing Games … Evolved … Ended up Breaking into Mainframes

- **414s communicated via local, public electronic bulletin boards**
- **Accessed private, long distance bulletin boards**
  - Looking for games, curiosity
- **Free long distance telephone calls.**
  - Call “collect,” bill calls to other people’s accounts
  - Valid access numbers for free long distance calls
- **May 1983 414s started breaking into mainframes**
- **414s later said they thought they weren’t doing anything wrong, so long as they didn’t do damage**

- **Source: https://www.washingtonpost.com/archive/politics/1983/08/30/young-computer-bandits-byte-off-more-than-they-could-chew/f407e5df-6eaf-4f9b-8b38-04304960d2d9/**

414s Ideas & Inspiration 1983 Movie “War Games” Technique: “WarGames Dialing”

War Games Official Trailer

The “Incident” of the 414s: The LANL Story

- **The film WarGames was released in May 1983.**
- **The first (known) remote access incident at LANL was May 1983**
- **The 414s broke into LANL in June 1983**

Activity: As you listen to this story, identify aspects of 414 intrusion response that seem familiar to incident responders today

Machine G

- **LANL system manager detected intrusion when he dialed into Machine G from home, noticed an interactive login as user NETPRIV, a privileged account**
- **Kept an eye on things while LANL security manager contacted TELENET security office, hoping to to trace call.**
  - Modem dial traced to phone # in 414 area code –Wisconsin
- **Once call successfully traced, engaged intruder in electronic mail interaction, which was logged**

The “Network Map Maker”

- **Via electronic mail, Intruder said:**
  - “We were spelunking in your electronic caves and trying to see how long this could go on before being noticed.”
  - “If you would like a full report about your security problems please contact us.”
  - “Although our entry was unauthorized it was not malicious. We simply wanted to check the security of your system.
- **Via electronic mail, System Manager informed intruder**
  - Call had been traced
  - Intruder had accessed a federal facility
- **Intruder & System Manager spoke next day over phone**

The Phone Call

- **Intruder explained how he had accessed computers on LANL network.**
- **Said he intended no harm, only exploring topology of network**
- **Remarked that it was most complex network he had seen and was preparing a sketch on paper**
  - The initial LANL report was titled: “The Case of The Network Map Maker”
- **Intruder requested account to further communicate security ideas**
  - Network manager turned down suggestion
  - Invited intruder to send a written report,
  - Cautioned him he might be wise to consult an attorney.
- **System manager never learned the name of the intruder**

414s Identified –National News

- LANL reported to FBI
- Per wikipedia/414, another site also identified Wisconsin teens
- Teen "wiz kids" were hyped by national news media throughout the summer of 1983
- Nuclear Weapons facility prominent in TV / print headlines
- Press release from LANL & response to media questions
- "We really got beat up over it," per LANL system administrator

Teens' Computer Equipment Seized

by United Press International

FBI agents on a nationwide hunt for equipment used to crack military and business computer systems raided the homes of teenage electronics whizzes in six states, reportedly turning up software gangs led by youths known as "The Cracker" and "The Wizard."

FBI agents launched raids from New York to California this week and seized thousands of dollars of equipment. Sources said the investigation focuses on offenses including illegal use of electronic message services, tapping of defense information and destruction of stored data.

The Detroit Free Press quoted a source close to the investigation who said damage caused by a Detroit group of computer enthusiasts was estimated "between $500,000 and $1 million" and "dozens and dozens of systems were involved. Systems were damaged everywhere, coast to coast."

"It's a matter of deliberate, calculated sabotage," the source said. "The main slant of the investigation is anything defense-related."

In Irvine, Calif., agents seized equipment Tuesday at the homes of David Hill, 17; Wayne Correia, 17; Gary Knutson, 15; and his brother, Gregg, 14.

"We never would or never did try to harm any kind of system or steal any kind of information," a shaken Hill said at a news conference yesterday. "We were just playing around in there."

The Irvine youths blamed a mysterious teen whiz called "The Cracker" for teaching them how to tap a commercial network that charges users.

Correia said seven agents raided his home, with one FBI man breaking through his second-story bedroom window, flashing his badge and saying, "Hold it right there, that computer is mine."

Detroit newspapers and TV news stations reported the FBI raided at least 12 homes in six states. The raids were reportedly conducted in Irvine, Detroit, Tuscon, Ariz., Oklahoma City, Okla., New York and Virginia.

AP photo

Wayne Correia sits in bedroom where FBI confiscated his computer equipment.

Plugging Security Holes

- **Changed TELENET service –no longer accept "collect" calls.**
  - Pre-paid calls require additional login & password
  - This cost an extra $100/month
- **Changed default account passwords**
- **Changed user passwords on compromised machines**
- **Removed "Guest" accounts from modem interfaces**
- **New policy requiring security approval prior to major changes**
- **Engaged vendors to discuss improvements to VMS system and installation procedures**

Sources That Tell the LANL Story

- **Investigation notes & reports**
- **Announcements for meetings between system managers and security managers**
- **Memoranda formally notified DOE and FBI**
- **Press release & notes on answering questions from press**
- **Memoranda to DOE sites about news reports & cyber concerns**
- **Memoranda from LANL Director to Lab employees**
  - Possibly first instance at LANL of policy by memo

Special thanks to Cheryl Gomez & Becky Rutherford for preserving these source materials

Memoranda to Managers at other DOE Labs Shares Lessons Learned

- “The recent incident reported by the national media of an unauthorized access of (LANL) computer system by a group of youths from Milwaukee has brought to our attention some things of which all of us in the (DOE) should be both aware and concerned.”
- LANL detected intruders, reported incident to DOE & FBI, which led to identity of suspects
- Hacking Culture
  - War Games movie & new CBS TV series “Whiz Kids”
  - Main character of War Games has “become a real part of our society”
  - Hackers use computer bulleting boards to share how to information
- Lessons learned –deficiencies corrected
  - Incident was caused by “careless systems management.”
  - Importance of “conscientious systems management”

Cyber History

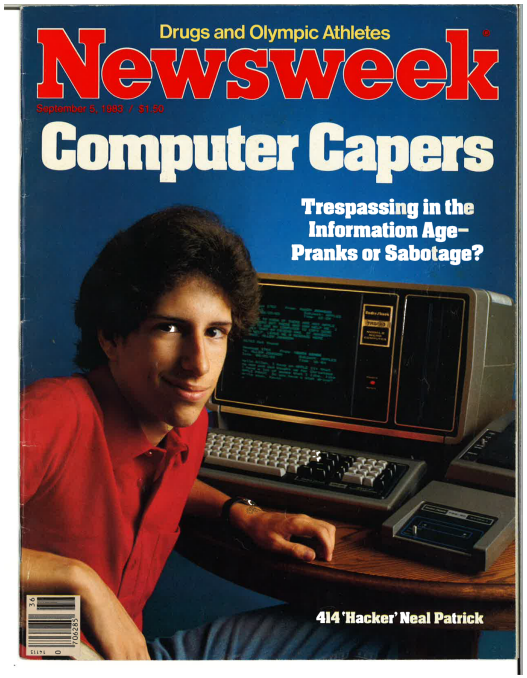
Identify aspects of the Network Map Maker / 414 incident that sound familiar today?

How unique was network Map Maker / 414 Incident?

- **Technology evolution led to vulnerabilities that weren't accounted for in network defense**
- **Governance issues & new policy**
- **System management & configuration weaknesses**
  - Careless system management
- **Scramble to plug holes**
- **Impacted reputation**

Neal Patrick Became Spokesperson For 4-1-4s

- Print & TV & radio interviews
- Covered by major newspapers and magazines
- Phenomena of teen hacker became part of national conversation summer 1983
- Testified before U.S. House of Representatives 9/26/83
  - Asked when he realized that what he did may have been wrong, Patrick said, “Once the FBI knocked at my door.”



Hearings Fall 1983 –House Committee on Science & Technology

- **Neal Patrick was the first witness**
- **2nd witness was Jim McClary, Division Leader, LANL**
- **According to a 1984 article in IEEE Security & Privacy, by David Bailey (LANL), leading off hearings with a Computer enthusiast" and "victim" led to a "circus" atmosphere**
  - Approximately 20 TV news cameras
  - Clicks of still cameras so loud sometimes witnesses could not be heard

Hearings Fall 1983 –House Committee on Science & Technology

- **David Bailey (LANL) reported**
  - Lack of clarity about ethics of unauthorized remote access by “hackers” who had no malicious intent
  - Members of congress discussed need for new legislation to establish that hacking was a crime, but they had difficulty defining computer crime
  - As the hearings progressed, concerns about state sponsored hacking
  - Only one witness identified concern about organized criminal hacking; this wasn’t on their radar

- Source: IEEE Security & Privacy “Attacks on Computers: Congressional Hearings & Pending Legislation” David Bailey 1984

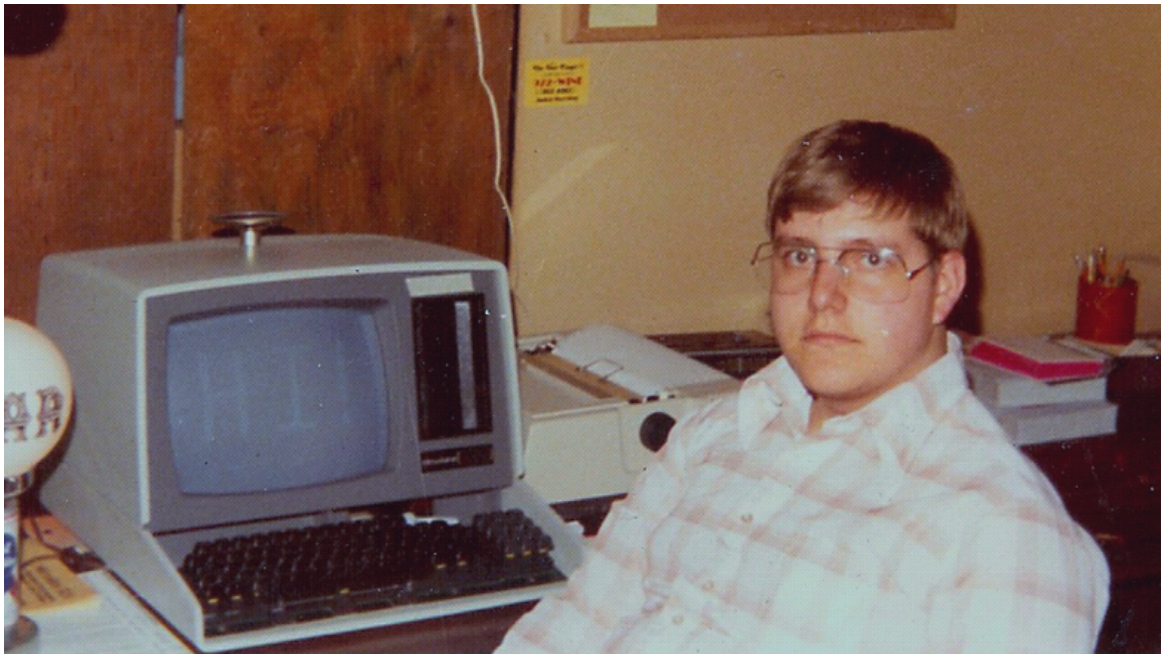
Two 4-1-4s Convicted

- **Gerald Wondra & Timothy Winslow pleaded guilty misdemeanor charges, convicted of breaking law against making obscene/harassing phone calls**
  - There were no federal laws against computer crime
- **In an interview published in 1984, Assistant US Attorney Eric Klum said it was the first computer crime prosecution in which motive was not financial gain**
- **Sentenced to 2 years probation, $500 fine**
  - Prohibited from using a modem until probation over

- Source: NYT article “Two Who Raided Computers Pleading Guilty” 1984/03/17

I hacked into a nuclear facility in the 80s. You're welcome

Source: http://www.cnn.com/2015/03/11/tech/computer-hacker-essay-414s Timothy Winslow



In an interview published 30 years later, Winslow said he was proud that 414s set stage for new computer laws and better security practices

"In a way, what we did as a group made for safer computing today."

Computer Crime Law

- **6 bills were introduced in 98th Congress dealing with computer crime**
- **Counterfeit Access Device and Abuse Act 1984**
  - First computer crime law
  - Only 1 prosecution
- **The Computer Fraud and Abuse Act of 1986**
  - Amended in 1989, 1994, 1996, 2001, USA Patriot Act, 2002, 2008 by the Identity Theft Enforcement and Restitution Act

- Source: https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_(CFAA)
- Source: https://en.wikipedia.org/wiki/The_414s
- Source: https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

Final Comments

- **A bit more about the Cyber History Project**

Homework Assignment, Part 1!

DOE Labs were some of the places where incident response, and network defense, were invented.

- **What were the earliest intrusions at your sites? Anybody else hit by 414s? Extra credit for incidents before 1983!**
- **Find out who has kept case notes, memorabilia, artifacts, wants to pass on stories**
- **Who were the people at your site who invented incident handling and network defense? Help them preserve this history!**
  - Already retired?
  - Soon to retire?

Homework Assignment, Part 2!

- **What were the most significant incidents at your site**
  - Things incident responders & managers did right
  - What mistakes did they learn from?
- **Does anybody collect and archive cyber artifacts? If not, start now before history is lost**

Homework Assignment, Part 3!
Lessons Learned From (More) Recent Events

- **The APT incidents from around 2008 – 2014 were among most important in DOE & US Gov history. What lessons learned may apply to APT actors that pose a threat today? And in the next 2 or 3 years?**
  - If you participated, share stories and lessons learned with new managers and new colleagues.
  - If you are new, talk to people who remember this (recent) history to learn from their mistakes and successes.

Living History

- **DOE Labs continue to make important contributions and innovations, adding to the legacy for leadership in network defense and intrusion response.**
- **You have a history**
- **You're making history**

Homework Extra Credit!

Alex Malin

High Performance Computing Division

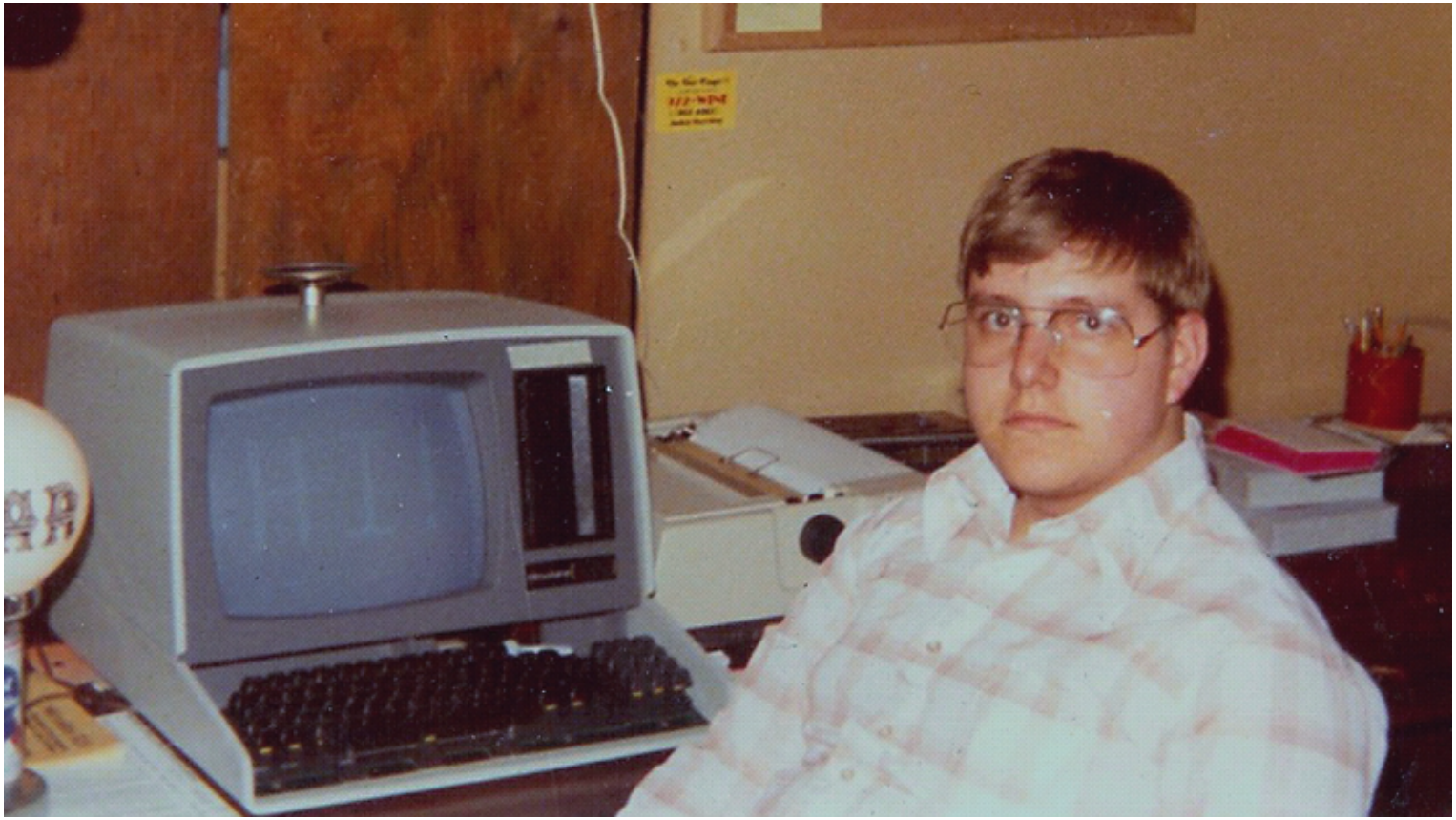
cyberhistory@lanl.gov

505-665-1797

If you're interested in cyber history contact us!

I hacked into a nuclear facility in the 80s. You're welcome

Source: http://www.cnn.com/2015/03/11/tech/computer-hacker-essay-414s Timothy Winslow



Additional Slides

Documents that Tell the LANL Story

- Incident notes describing compromise of “Machine G”
- Electronic mail between intruder and user who detected intruder
- Logs of intruder connecting from Machine G to other LANL computers
- The Case of the Network Map Maker –Report from Security Manager
- Intrusion timeline & details
- Aug 18 Letter from GTE Telenet Communications Corporation to LANL report on Host Port Utilization
- Aug 18 Incident Summary & Lessons Learned: Memo to DOE sites
- Techniques used by Milwaukee Youths to Access LANL computers
- Actions Taken or Planned by LANL to Prevent Reoccurrence
- Aug 11 LANL Press Release

Documents that Tell the LANL Story

- **July 15 Memo announcing meeting to discuss intrusion between security managers and system managers**
- **Aug. 11 Q&A for Public Affairs**
- **Aug. 17 Memo from DOE/Abq formally notifying FBI**
- **Aug. 26 Memo on Security of Laboratory Open Computing Systems to lab workers from Lab Director**

Technological Innovations: Networking & Remote Access

- **Computers from different vendors couldn't communicate**
- **You physically brought a deck to a computer facility**
  - Operators ran the card deck & printed output
- **1974/1975 –The first production network at LANL linking multi-vendor equipment & multiple file systems**
  - Keyboard Concentrator Computer (KCC) –Login terminal via modem
  - Computer Based Terminal (CBT) –Read in card deck remotely
    - Submit jobs from across the Lab without driving over
    - Output back through CBT to printer

- **Source: Interview Cathy Stallings (LANL)**
- **Source: "The Route Less Taken" by Nicholas Lewis LA-UR-16-20103**

How Did “Network Map Maker” Break In?

- **TELENET service installed about a year**
  - Machine G was connected to TELENET service
  - NETPRIV account 4 character password same as DEC manual
- **Intruder migrated from “G” to several other VAX computers**
  - Command yielded passwords for all DECNET (privileged) accounts.
  - Intruder created new system account, ran a program, deleted it after execution
  - Lots of file access activity
- **One extended session lasting 38 hours**

New Technology: Networking & Remote Access

- **LANL workers built networking hardware & software from protocol up**
- **Deployed Network Security Controller in 1976**
  - Connected 3 network partitions
  - Restricted file and resource access based on passwords
  - Recorded user logins and machine logged onto
  - Logged output to teletype in computer room
  - After X bad logins, blacklisted from logging in
    - Seems to imply computer security focus on preventing and detecting the Insider Threat

- **Source: Interview Cathy Stallings (LANL)**
- **Source: "The Route Less Taken" by Nicholas Lewis LA-UR-16-20103**

LANL Investigates and Reports Incident

- **Memoranda formally notified DOE and FBI**
- **Memoranda to DOE sites about news reports & cyber concerns**
  - Report on techniques used by “Milwaukee Youths” to access the LANL Computer System
- **Memoranda from LANL Lab manager to Lab employees**
  - Possibly first instance at LANL of policy by memo
- **Meetings**
- **Case notes & internal reports**

Documentary Film Released 2015

"THE 414s tells the story of the first widely recognized computer hackers, a group of Milwaukee teenagers who gained notoriety in 1983 when they broke into dozens of high-profile computer systems, including the Los Alamos National Laboratory, a classified nuclear weapons research facility."

Source: http://www.imdb.com