Loss of Network Control Incidents

Joe St Sauver, Ph.D.
(joe@uoregon.edu or joe@internet2.edu)
Security Programs Manager, Internet2
Internet2 and the University of Oregon

Internet2 Fall Member Meeting
New Orleans, LA
Wednesday, Oct 15th, 2008 4:30PM

http://www.uoregon.edu/~joe/loss-of-network-control/

Disclaimer: The opinions expressed in this talk are strictly those of the author, and are not necessarily those of any other entity.

Abstract

A major western city recently found itself "locked out" from its own network for a multi-day period, allegedly as a result of actions undertaken by one of its own staff. Regardless of its cause, loss of network control for multiple days is clearly a "disaster," albeit not a traditional disaster (such as those caused by fire, extreme weather, earthquakes or other geo-environmental causes).

In discussions of this incident on the Internet2 Salsa-DR (Disaster Recovery) working group, many important implications emerged. Some of those implications include the importance of having:

(a) established procedures for password recovery/reset in the event that an administrator forgets, loses, or is otherwise unable to supply a privileged password when required;
(b) offline backups (and any passwords which may be needed to access those backups, e.g., if they've been encrypted);
(c) a well-documented and up-to-date written system configuration, in case a system needs to be re-built from scratch;
(d) procedures for handling human resource issues which may arise in conjunction with individuals working in sensitive positions;
(e) the value of periodic security audits; and
(f) the risks of running thinly staffed in key technical IT areas, among other things.

This presentation will review that incident, and discuss the lessons which we might apply to our own campus networks and systems.

I. Introduction

The Format of This Talk

- This talk has been prepared in my normal unusually-detailed format. I use that format for a number of reasons, including:
  -- doing so helps to keep me on track
  -- audience members don't need to scramble to try to take notes
  -- if there are hearing impaired members of the audience, or non-native-English speakers present, a text copy of the talk may facilitate their access to the presentation
  -- a detailed copy of the talk makes it easier for those who aren't here today to go over this talk later on
  -- detailed textual slides work better for search engines than terse, highly graphical slides
  -- hardcopy reduces problems with potential mis-quotation

  BUT I promise that won't read my slides to you!
- Because this talk is late in the conference, and many folks will be traveling soon, I also wanted to leave some time for Q&A, too

Notes Before We Get Started

- ***Goal of This Talk:*** The primary goal of this talk is **not** to engage in criticism of the City of San Francisco or the alleged perpetrator of this incident.

  My interest lies in identifying security best practices which might help others to avoid similar events.

- ***Technical Level:*** Because this is an Internet2 Member Meeting and not an Internet2 Joint Techs meeting, I've tried to keep technical material at an approachable level for a diverse audience, and I'll be providing backfill where appropriate.

- ***There Are Two Sides to Every Story:*** Throughout this talk, I'm going to try to do my best to see and tell you about both sides of the story, although there will be times where I suspect you'll notice that I find one side or the other to be more compelling.

Additional Notes Before We Get Started

- ***Presumption of Innocence:*** This presentation discusses a recent incident dating from just the summer of 2008, an incident which currently pending in the court system.

  Unless/until the courts find the accused to be guilty, the defendant should and must be presumed to be innocent.

- ***"Subpoena Repellent:"*** In preparing this presentation, I've relied solely on publicly available materials.

  I do not have direct first hand knowledge of the facts of this case, nor would I be qualified to testify as an expert witness (for either side!) in this matter.

- **So what *<u>is</u>* this "incident" we're talking about?**

II. The Incident

I Was Reluctant to Base This Talk On Any Single Description of What Occurred

- I am reminded of the 2005 remake of "Little Red Riding Hood," the movie "Hoodwinked!" which recounts an apparently simple incident from the perspective of multiple parties.

- In particular, especially for incidents involving technical material, I'm sometimes reluctant to rely solely on media accounts done by non-technical reporters. It was, however, media accounts which first brought this incident to my attention.

- For example…

"S.F. officials locked out of computer network"

- ***A disgruntled city computer engineer has virtually commandeered San Francisco's new multimillion-dollar computer network, altering it to deny access to top administrators even as he sits in jail on $5 million bail, authorities said Monday.***

  Terry Childs, a 43-year-old computer network administrator who lives in Pittsburg [California], has been charged with four counts of computer tampering and is scheduled to be arraigned today.

  Prosecutors say Childs, who works in the Department of Technology at a base salary of just over $126,000, tampered with the city's new FiberWAN (Wide Area Network), where ***records such as officials' e-mails, city payroll files, confidential law enforcement documents and jail inmates' bookings are stored.***

  Childs created a password that granted him exclusive access to the system, authorities said. He initially gave pass codes to police, but they didn't work. When pressed, Childs refused to divulge the real code even when threatened with arrest, they said.

  He was taken into custody Sunday. City officials said late Monday that they had made some headway into cracking his pass codes and regaining access to the system.
  [article continues]
  Source: www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/14/BAOS11P1M5.DTL
  [emphasis added]

An Alternative to Media Reports: Court Filings

- Copies of many court filings relating to this case are available from Paul Venezia's blog site at InfoWorld at http://weblog.infoworld.com/venezia/archives/017979.html including:

  -- The affidavit by the investigating officer for an arrest warrant

  -- The prosecutor's complaint against Childs

  -- The defense attorney's motion to reduce bail

  -- The prosecutor's motion in opposition to a reduction in bail

- Those primary sources provide important information which will help you understand the details of this incident.
- Everyone interested in this topic should take the time to read those legal documents.

An Anonymous City of San Francisco "Insider"'s Take on the Incident

- There is still one other perspective that's also worth reviewing, and that is the anonymous account of someone who is apparently a knowledgeable network insider at the City of San Francisco, and who shared their unique perspective with Paul Venezia. See "Why San Francisco's network admin went rogue," http://www.infoworld.com/article/08/07/18/30FE-sf-network-lockout_1.html (URL wrapped due to length) It would have been better if that source had been willing to identify him or herself, but sometimes that simply isn't realistic.
- I also looked for official City of San Francisco Committee on Information Technology meeting minutes, and found http://www.sfgov.org/site/coit_meeting.asp?id=57950 but while there are agendas dating as recently as October 9th, the most recent meeting minutes available date July 8th, 2008

A Network Lockout: An Odd Sort of “Disaster”

- Regardless of what account of the incident you read, you quickly find yourself confronting the fact that the city of San Francisco incident is clearly a “disaster,” albeit an unusual one.
- No, it wasn’t a fire or hurricane or earthquake, but it was every bit as much of a disaster for the City of San Francisco:
  -- the city experienced the sort of catastrophe that at least some non-technical managers fear most, losing control over assets allegedly because of the actions of a trusted technical insider
  -- they also suffered substantial national negative publicity, and
  -- they spent a lot of money that they probably hadn't planned to spend
- While this is an odd sort of "disaster," Internet2's Salsa Disaster Recovery working group considers all types of disasters, including odd ones, so here we are together today.

This Incident Could Have Been a Lot Worse

- As bad as it was, it could have been a lot worse.

- As far we can tell based on publicly available accounts:

  -- The network didn't go down; it continued to run during the incident, including continuing to deliver mission critical functionality for services such as public safety

  -- The city's network's hardware and software wasn't damaged

  -- Personally identifiable data wasn't publicly disclosed, nor was data modified without authorization

  -- Staff members weren't harmed, etc.

The Incident Was Expensive

- See, for example: http://www.infoworld.com/article/08/09/10/San_Francisco_hunts_for_mystery_device_on_city_network_1.html

  That article stated that the city has already paid $182,000 to Cisco contractors and $15,000 in overtime related to the incident, and has set aside an additional $800,000 to cover further future costs associated with the incident.

- This is a substantial amount of money to spend in tight economic times, even when it is being spent by a major city in conjunction with a major networking project.

Let's Also Not Miss That This Incident Has Been A Personal "Disaster" for the Defendant

- The defendant has been jailed and would need to post $5,000,000 bail in order to be released pending his trial.
- If eventually convicted of his alleged offenses, he faces up to seven years in prison.
- I'd be surprised if a civil suit doesn't follow the criminal trial.
- Its hard to believe that the defendant will have much of a professional future with the City of San Francisco after an incident of this magnitude, regardless of whether he's convicted.
- This is all very regrettable given the fact that by all accounts the defendant was a very talented network engineer.
- **So how was this even technically possible? How could one person allegedly obtain total control over an entire city's backbone network? I believe it came down to a strong starting position plus a series of unexpected "gotchas."**

III. “Gotchas” and the City of San Francisco FiberWAN Network's Passwords

A Strong Starting Position

- When it comes to **taking** control of a major network, it helps if the owner begins by **giving** control of it to you.

- In this case, the alleged perpetrator was the person in charge of the city's network, and as such he had:

  -- total access
  -- an intimate knowledge of the network (after all, he'd built it)
  -- a high level of technical expertise (he's a CCIE, one of less than 20,000 or so CCIEs worldwide), and
  -- he apparently had limited managerial oversight.

- That's a pretty darn strong starting position. Now combine that with an interesting set of "gotchas…"

Gotcha #1: One (and Only One) Administrator With Full Access

- When you first read about that sort of incident (or at least when I first read about it), my first thought was **"Surely more than one person had privileged access to the City of San Francisco's routers and other network devices?"**

- It only took a minute for me to recognize that there was always the unsettling possibility that someone with privileged access might have changed the enable password to some new value known only to himself, but in reading the court filings it was clear that no, Childs was, ***and was known by the city to be***, the only one with full administrative access to the city's network.

- That should have set off alarm bells -- at least it sure did for me.

The “It's-A-One-Engineer-Shop” Problem

- In my opinion having only one network engineer with full administrative access to your network is a very bad idea because it represents a potentially profound “single point of failure:”

  -- Would you be okay having your network run on “autopilot” while your one network engineer is out sick or on vacation?

  -- What would you do if your one network engineer gets “pancaked” by a bus when he or she steps out for lunch?

  -- What if he or she got a better career opportunity and left?

  -- What if he or she simply "flipped out" one day?

- Granted, network engineers are expensive and in short supply, but the work they do on any non-trivial-size network is too critical to “make do” with just one.

More Generally: The Insider Threat

- **"San Francisco Case Shows Vulnerability Of Data Networks"** http://www.washingtonpost.com/wp-dyn/content/article/2008/08/10/AR2008081001802.html [URL wrapped; emphasis added]

"[…] Terry Childs, 43, was arrested July 13 at his suburban home, where **police found $10,000 in cash, diagrams of the city-county computer network, a co-worker's access card, a loaded 9mm magazine and several loose .45-caliber rounds. Under the user name Maggot617**, he hijacked the system and refused to turn over passwords for the network, which superiors belatedly discovered only he controlled. […]

"I don't want to make it sound hopeless," but "when I go around and give talks, **it seems like people don't really understand their risk of being the victim of insider sabotage**," said Dawn Cappelli, a specialist in insider threats with CERT, the Carnegie Mellon Software Engineering Institute's Computer Emergency Response Team […]"

I Think Many People *Do* Get The Insider Threat

- *"The 2008 (ISC)^2 Global Information Security Workforce Study, conducted by Frost & Sullivan, found that* ***51% of IT executives and security professionals consider internal employees "the biggest threat" to security.*** *And an Information Security magazine survey this year found a full* ***70% of respondents concerned about detecting and shutting down internal attacks.***"

  http://searchcio-midmarket.techtarget.com/news/article/0,,sid183_gci1322169,00.html

Network Engineers As a Class Have Broad Access and Power, and Hence High Potential Riskiness

- Network engineers typically have **physical access** to a wide range of campus facilities, including access to high security facilities and after hour unsupervised site access.

  That sort of "all access" "backstage pass" means that engineers could easily introduce network equipment which only they know exists.

- Network engineers also commonly have the access and ability to **electronically monitor** any or all unencrypted network traffic.

- There may be a more security-sensitive "insider" position in a typical IT shop, but its hard for me to think of what job that might be.

When Hiring For Security-Critical Positions

- ***If Possible, Check:*** You need to be ***very*** careful to make sure you know and trust the people you hire for security-critical positions.

  -- Even if you don't normally do background checks, I would encourage you to consider checking the background of anyone who will be in a position that combines unlimited technical access with limited opportunity for effective oversight.

  -- Note that some states or institutions may limit use of background checks; seek the advice of your HR department and institutional legal counsel to make sure that requesting and using one is okay, and so you'll have all the necessary permissions.

- ***Get <u>More</u> Advice If You May Have "Found Something:"***
  If a background investigation does yield derogatory information, be sure to consult again with your HR department and institutional legal counsel for advice with respect to what (if any) impact that derogatory information can or should have on a potential hiring decision, and what if any procedural rights your candidate may have relating to the results of that investigation.

But Coming Back to the City of San Francisco's Password Problem…

- The city obviously still had physical access to all their network devices. **All geeks "know" (or should know) that if you have physical access to a device you should be able to use a serial console (or push the magic "reset button," etc.) to reset the device and regain control over that device, right?**

- That simple reality ("if I can touch it, I can 0wn it") is one reason why smart IT security folks tend to be so "paranoid" about physical security (as well as network and system security)…

- The reset process usually isn't hard. Cisco even has web pages conveniently describing the forgotten password recovery process, as do virtually all other popular network equipment vendors…

Example: Cisco Password Recovery

Password Recovery Procedure

Contents

Introduction

This document describes the procedure for recovering an **enable password** or **enable secret** passwords. These passwords are used to protect access to privileged EXEC and configuration modes. The **enable password** password can be recovered but the **enable secret** password is encrypted and can only be replaced with a new password using the procedure below.

Note: This password recovery procedure works for the following Cisco products:

- Cisco 806
- Cisco 827
- Cisco uBR900
- Cisco 1003
- Cisco 1004
- Cisco 1005
- Cisco 1400
- Cisco 1600
- Cisco 1700
- Cisco 2600
- Cisco 3600
- Cisco 4500
- Cisco 4700
- Cisco AS5x00
- Cisco 6x00
- Cisco 7000 (RSP7000)
- Cisco 7100
- Cisco 7200
- Cisco 7500
- Cisco uBR7100
- Cisco uBR7200
- Cisco uBR10000
- Cisco 12000
- Cisco LS1010
- Catalyst 2948G-L3
- Catalyst 4840G
- Catalyst 4908G-L3
- Catalyst 5500 (RSM)
- Catalyst 8510-CSR
- Catalyst 8510-MSR
- Catalyst 8540-CSR
- Catalyst 8540-MSR
- Cisco MC3810
- Cisco NI-2
- Cisco VG200 Analog Gateway
- Route Processor Module

Step-by-Step Procedure

1. Attach a terminal or PC with terminal emulation to the console port of the router. Use the following terminal settings:
   9600 baud rate
   No parity
   8 data bits
   1 stop bit
2. If you still have access to the router, type **show version** and record the setting of the configuration register; it is usually 0x2102 or 0x102.
3. If you don't have access to the router (because of a lost login or tacacs password), you can safely consider that your configuration register is set to 0x2102.
4. Using the power switch, turn off the router and then turn it back on.
   Important: To simulate step 4 on a Cisco 6400, pull out and then replace the Node Route Processor (NRP) or Node Switch Processor (NSP) card.
   Important: To simulate step 4 on a Cisco 6x00 using NI-2, pull out and then replace the NI-2 card.
5. Press Break on the terminal keyboard within 60 seconds of the power-up to put the router into ROMMON.
   If the break sequence doesn't work, see Possible Key Combinations for Break Sequence During Password Recovery for other key combinations.
6. Type **confreg 0x2142** at the `rommon 1>` prompt to boot from Flash without loading the configuration.
7. Type **reset** at the rommon 2> prompt.

Password Recovery On Many Devices

- In a large network, there might potentially be *many* devices with passwords needing to be reset. For example, in the city of San Francisco's case, there were reportedly some 1,100 discrete routers/switches/modems/ etc. which might need to be reset.

- Normally, for a network of that size, authentication/authorization/ access control are scaleably handled by using centralized authentication technologies (such as radius).

- But if local passwords were used, password recovery may require visiting each and every one of those devices to do the password reset process and/or to load a known good config, a potentially long and tedious process -- particularly if devices are located in remote locations, or the networks in question have strict and strictly limited maintenance windows.

Add Potential Gotcha #2: Volatile Configuration

- Note that at least the Cisco lost password recovery procedure include a critical step, “reboot the router.”

- If a router’s configuration were to be stored *ONLY* in RAM, and NOT committed to flash memory or other persistent storage, rebooting the router (or any other event which resulted in a loss of power to the router) would trigger a complete loss of the router’s configuration and a network outage.

- **At the risk of stating the obvious, your network devices' configuration MUST always be saved to non-volatile storage to insure that systems CAN successfully survive a power outage or reboot.**

Worries About Scheduled Minor Power Outages

- Unusual levels of employee concern about short duration scheduled downtime may be a potential warning flag. Routers and other network devices should be able to easily survive a graceful shutdown and restart cycle.

- However, not having performed a forensic review of the City of San Francisco's network devices, we don't know for sure if the router configurations were committed to persistent storage or just lived in volatile memory. We do know, however, that the defendant was reportedly worried about an imminent scheduled power outage, potentially a sign that there may have been at least some network devices which wouldn't be coming back up after a reboot. See, for example, the prosecutor's motion in opposition to a reduction in bail at pages six and seven.

Add Gotcha #3: *no service password-recovery*

http://www.cisco.com/en/US/docs/ios/12_3/12_3y/12_3ya8/gtnsvpwd.html

Google

No Service Password-Recovery

The No Service Password-Recovery feature is a security enhancement that prevents anyone with console access from accessing the router configuration and clearing the password. It also prevents anyone from changing the configuration register values and accessing NVRAM.

Feature History for the No Service Password-Recovery Feature

Release	Modification
12.3(8)YA	This feature was introduced.
12.3(14)T	This feature was integrated into Cisco IOS Release 12.3(14)T.

Finding Support Information for Platforms and Cisco IOS Software Images

If the router has "no service password-recovery" enabled, you **can** still reset the router… but **only** to a default factory configuration. You'd then need to be prepared to reload the configuration from a backup copy of the configuration files to restore the router to service.

In General: ***Don't Use*** *no service password-recovery*

- I recognize that by merely mentioning the *no service password-recovery* command I run the risk of unintentionally "mis-inspiring" someone to enable this setting on their own devices, perhaps as part of an effort to harden their devices to better resist attempts at unauthorized physical access.

- Doing so, would, in my opinion, often be a big mistake.

- **I'd strongly urge you to RESIST the temptation to enable *no service password-recovery* on your own routers.**

Alternatives to *no service password-recovery*

- Physical access control measures will virtually always be needed to limit hands-on access to your routers since if someone can physically touch your router they can:

  -- cut data or power cables
  -- steal line cards, flash memory cards, GBICs, Xenpacks, removable power supplies, copper grounding wires, etc.
  -- vandalize the router's chassis
  -- etc.

- Physical access control measures necessary to prevent those sort of attacks can, simultaneously, ALSO preclude local serial console-based attempts at password recovery (unless you have networked or out-of-band access to the router's serial console port)

Add Gotcha #4: No Config File Backups

- This one's the *real* killer. If the router's as-configured state were to be lost (for whatever reason), having a usable backup copy of the device's configuration is critical to quickly bringing that device back up.
- The investigating officer's affidavit mentions (see the court filings mentioned on slide 10 of this presentation) that "[…] Child[s] was asked if he had implemented disaster recovery procedures, documented the network under his control and/or if he had made the required backups on devices, as is policy. His answers were '..no..'"
- That affidavit goes on to recount, "Mr. Maupin [an external consultant] and City staff were not able to […] locate any documentation, network maps or configuration files that would allow an authorized person to perform maintenance or rebuild the configuration on these devices."

[Some] Configuration File Recommendations

1. Configuration files should be periodically archived in digital and hardcopy forms (routinely retain any/all earlier versions)
2. One or more copies of the configuration files should ***not*** be under the control of the individuals who are responsible for running the network. For example, a copy of the configuration files might be routinely deposited with the chief information security officer (this is a basic "separation of duties" issue.)
3. Changes to network device configurations should be peer reviewed before actually being made, as part of implementing a general change management process.
4. Configuration files should be reviewed (or at least be made available for review) as part of an annual external IT audit.
5. Changes should be made in a transparent fashion, with appropriate tools used to document and disseminate copies of config file diffs to relevant technical and security staffs.

One Configuration File Mgmt Tool: RANCID

- RANCID == Really Awesome New Cisco confIg Differ, see www.shrubbery.net/rancid/ Quoting from that page:

  RANCID monitors a router's (or more generally a device's) configuration, including software and hardware (cards, serial numbers, etc) and uses CVS (Concurrent Version System) or Subversion to maintain history of changes.

  RANCID does this by the very simple process summarized here:

  ** login to each device in the router table (router.db),*
  ** run various commands to get the information that will be saved,*
  ** cook the output; re-format, remove oscillating or incrementing data,*
  ** email any differences […] from the previous collection to a mail list,*
  ** and finally commit those changes to the revision control system*

- RANCID is routinely used by large providers such as AOL, Global Crossing, etc. **YOUR network should be using it (or some other device configuration management program), too.**

Document Your Network Architecture/Design

- Beyond just watching device configuration files, you should also insure that your network's overall architecture/design has been fully documented.
- Sometimes there is a tendency to build or modify a network first, waiting to **document** the network until things "slow down a little." Of course, as we all know, things **never** really slow down, and hence many networks get built but never get documented the way they should be. Auditors should flag this when they notice it.
- Multiple factors may make careful network documentation particularly important, including:
  -- complex/uniquely innovative/advanced network designs
  -- large scale or high device count networks
  -- limited network engineering staff (or high staff turnover)
- It's unfortunate that Terry Child's apparent efforts to document the city's network in a three volume report may have been frustrated. See http://www.bluoz.com/blog/index.php?/archives/428-Terry-Childs-copyright-application.html [URL wrapped]

Also Document Your Processes & Procedures

- In addition to documenting your network's architecture and design, you should also be documenting the processes and procedures you use to operate your network.
- For example, document the steps involved in upgrading a router to a new version of IOS at your site. Similarly, document the procedure for resolving a circuit outage with each of your carriers -- and be sure to test the documented process to confirm that it actually works as described!
- By taking the time to document those processes and procedures, you create an institutional "knowledge base" that gives you further insurance against the accidental creation of human "single points of failure."
- Documenting processes and procedures also provides a good starting foundation for an outside IT auditor's annual review. If this documentation isn't available, auditors should note that

III. “Alternative” Network Access; Limitations on Access to the Network

So What Ever Happened WRT The Passwords?

- On July 21st, during a 15 minute meeting with the mayor of San Francisco, the defendant disclosed three usernames and one password. Those credentials allowed the city to regain access to its network -- but only from "one location," a connection in “room 125 of the Hall of Justice.” According to the motion offered by the DA in opposition to the request for a reduction in bail, “Surprisingly, the police department’s IT administrator was not aware of this access point installed by the Defendant.”
- Also on July 21st, “the Department of Park and Rec […] located another access point that the Defendant never revealed.”
- Childs also allegedly had dialup and DSL access paths into the city’s network.
- For the city, discovery of these alternative access points raised the uncomfortable possibility that **they might not be technically able to lock Childs out of their network:** Childs might have additional still-undiscovered access points he controlled, access points which might be difficult for the city to identify/eliminate.

So Which Was It?

- Were the defendant's various extra access points

  "undisclosed and unapproved surreptitious backdoors" meant to keep the city from being able to block he defendant's access to the city's network,

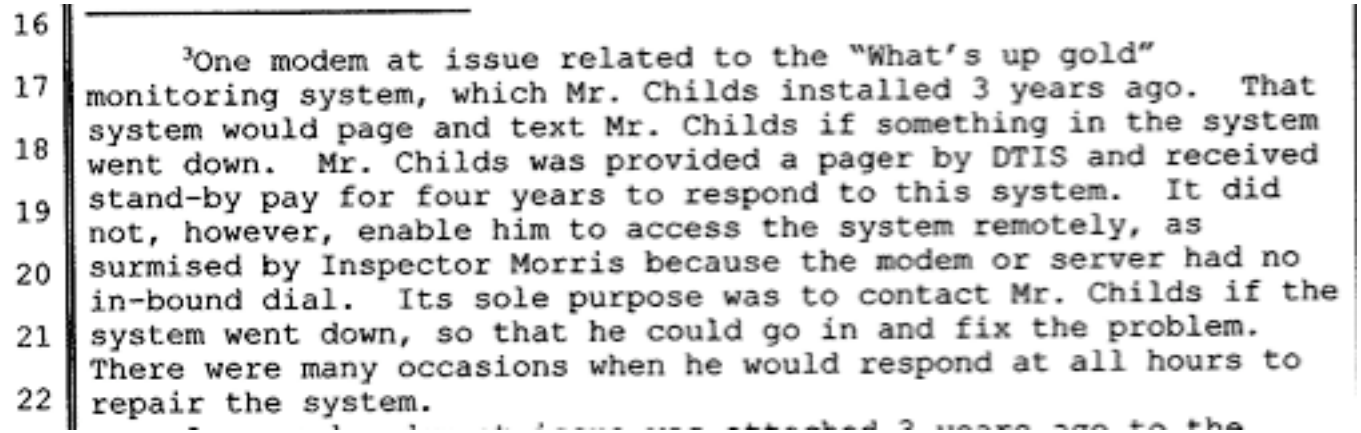
  or were they

  routine, reasonable and prudent "out of band emergency access" pathways meant to insure that Childs, as network manager, would alwayys have access to work on the network if it went down in an emergency?

- Remember, the connectivity needs of network engineers are different from those of average users…

There's a Lot That "Down" Networks Can't Do

- For example, if a network is down, it won't be able to deliver an email notifying you that it's down. Once the network comes back up, THEN that emergency notification will arrive, but that would be too late -- the network will have already been repaired.
- If you want to be notified when your network goes down, you'd typically use an alternative notification channel, such as pager alerts sent to an alphanumeric pager using a telephone modem.
- In the SFO case, they apparently used What's Up Gold for that purpose, and it would be perfectly reasonable for a notification product of that sort to have dial out (only) access via a modem:



[3]One modem at issue related to the "What's up gold" monitoring system, which Mr. Childs installed 3 years ago. That system would page and text Mr. Childs if something in the system went down. Mr. Childs was provided a pager by DTIS and received stand-by pay for four years to respond to this system. It did not, however, enable him to access the system remotely, as surmised by Inspector Morris because the modem or server had no in-bound dial. Its sole purpose was to contact Mr. Childs if the system went down, so that he could go in and fix the problem. There were many occasions when he would respond at all hours to repair the system.

Remote Dial-IN Access Can Be More Of An Issue

- It is also a tautological truism that you can't use a network that's down to fix itself -- you need access to a secondary "out-of-band" path that's still up.
- Because out-of-band connectivity is usually needed only rarely, common out-of-band connectivity options include inexpensive dial-in or broadband DSL connections, precisely the sort of connections discovered by the city in Terry's case.
- On the other hand, creating dial-in access and consumer-class broadband access connections into the city's network raises the possibility that those channels will be found and exploited by "war dialing" or "port scanning" hacker/crackers.
- As such, those out-of-band connections, unless very carefully secured, potentially represent a path which miscreants can use to circumvent traditional perimeter defenses such as firewalls and intrusion detection systems.

Discovering Unauthorized Modems (and Wireless!)

- When it comes to finding unauthorized modems attached to a network, there are several strategies that one could try, including:

  -- "war dialing" one's own network (however be aware that modems may not always be up/answering, they may be set to use a timer and only be up for a short/oddly scheduled period)

  -- auditing telecom payments to look for payment discrepancies: e.g., are there lines that are being paid for, but whose purpose and location and justification isn't understood/known?

- But these days, you also need to recognize that remote access might just as readily take place via a rogue WiFi wireless access point, a commercial WiMax connection, or a cellular modem paid for using non-institutional funds.

- It would be very difficult to conclusively exclude all possible potential backdoor connections into a large network.

Speaking of Problems "Finding Devices"

- **“San Francisco hunts for mystery device on city network”**
  http://www.infoworld.com/article/08/09/10/San_Francisco_hunts_for_mystery_device_on_city_network_1.html

  […]city officials say they are searching for a mysterious networking device hidden somewhere on the network.

  The device, referred to as a "terminal server" in court documents, appears to be a router that was installed to provide remote access to the city's Fiber WAN network, which connects municipal computer and telecommunication systems throughout the city. City officials haven't been able to log in to the device, however, because they do not have the username and password. In fact, the city's Department of Telecommunications and Information Services (DTIS) isn't even certain where the device is located, court filings state.

  The router was discovered on Aug. 28. When investigators attempted to log in to the device, they were greeted with what appears to be a router login prompt and a warning message saying "This system is the personal property of Terry S. Childs," according to a screenshot of the prompt filed by the prosecution.

"Mysterious" Terminal Servers?

- “Terminal servers” aren’t very “mysterious.” You're probably familiar with terminal servers from when they were routinely used to connect serial devices (such as modems) to IP networks.
- Terminal servers can, of course, also be used "in the other direction," allowing a user to connect over an IP network (like the Internet) to a serial port on a router or other network device. Given that this particular “mysterious device” shows a “router login prompt” when you connect to it, presumably this terminal server is, in fact, connected directly to a router serial port.
- What baffles me is this: the city was able to connect to the terminal server (even if they weren’t able to login), yet they reportedly haven't been able to re-find it and get it disconnected.
- Since they connected to the device at least once the terminal server MUST have an IP address or domain name associated with it, and given that information it should be a trivial exercise to localize that IP and unplug the device. I'd sure love to know more about why it is proving so hard to locate this device in practice.

Other City of San Francisco Access Related Concerns

- Quoting Paul Venezia once more:

> *There are also statements in the filing that point out that the* ***network devices were only accessible from certain places within the network. They claim this as another example of malfeasance on the part of Childs, saying "Thus, even possessing the passwords were [sic] not enough to regain control of the network, but one had to know where to go to communicate with the network's core devices."*** *Using ACLs to protect against intrusion is standard operating procedure. This is what access-classes on VTYs are for.*

http://weblog.infoworld.com/venezia/archives/cat_terry_childs.html?source=Terry%20Childs
[URL split due to length; emphasis added]

ACLs to Control Admin Access? ==> Dandy! Not Disclosing Those ACLs? ==> *NOT* Okay!

- It's fine for devices to be configured to use restrictive access control lists to limit access, particularly when we're talking about privileged access to sensitive devices. A person using free hotel wireless in the Ukraine should not be able to login to your router. Preventing that's good and entirely okay.

- Where things begin to go sour is when restrictions don't get documented or disclosed, or when only arcane or obscure locations are granted access.

- Understanding limits on the locations which will work for access to a given device is as much part of an access "recipe" for that device as a username or password, and failure to disclose that critical information can be as much or more of a barrier to access as refusing to disclose a username or password.

IV. The "Traffic Sniffing" Allegation
(Or "Here We Go, Back To Passwords, Again!")

From The Motion Opposing A Reduction in Bail

B. The Defendant had Access to confidential files and data belonging to the City

According to the experts working on the network, the Defendant could have access to files and data of different departments. First, data travels on the network unencrypted and can be read and captured by anyone monitoring the network. The defendant could have captured and saved this information while he was monitoring the system. Secondly, the Defendant had usernames and passwords of employees of different departments, including his supervisor Herb Tong. The Defendant would be able to access this information by logging directly into those networks using those employees' password and see data files that that specific user was entitled to see.

The Defendant had programs on the network referred to as "sniffing programs" that were designed to identify certain types of data that was moving on the network's traffic. These programs could be directed to look for certain types of data on the network and download them to his hard drive for later uses.

Why *Wasn't* Traffic Encrypted End-to-End?

- If the City of San Francisco's had been encrypting traffic end-to-end, it wouldn't matter if Terry (or anyone else) tried to sniff it: there wouldn't be much to see. If the city of San Francisco wasn't routinely encrypting all their network traffic, they **should have been**, and **so should you!**
- Once network traffic is encrypted, all an eavesdropper would see would be each traffic flow's source/destination, protocols and port numbers in use, etc. The traffic's content would all be scrambled and thus unreadable by someone intercepting those packets.
- The city's failure to aggressively work to encrypt virtually all traffic, including *particularly* all sensitive traffic containing (a) passwords, (b) personally identifiable information or (c) law-enforcement sensitive public safety information, is something that's very hard for me to understand.

Terry's List of Employee Usernames and Passwords

- The extract from the prosecutor's motion in opposition to a reduction in bail also refers to a list of "usernames and passwords of employees." From the context (e.g., a discussion of monitoring/sniffing network traffic), one is lead to believe that these usernames and passwords may be ones which the defendant captured from the network.
- However, could it also be possible that these were usernames and passwords which the defendant was authorized to see and which in fact he was expected to administer? For example, if the city uses radius for authentication to its wireless network access points or its VPN, who creates those radius accounts? Could it have been Childs?
- What are we to make, then, of the fact that those accounts and passwords could potentially have been used to login and look at sensitive files on those users' accounts?

Putting Terry's List of Passwords In Context

- I think we forget (or maybe many users just never knew) that privileged system administrators could and can:
  -- **access any user's files**, including things like sensitive email messages, confidential documents, or the shadow password file itself (and with a copy of the shadow password file, one could use rainbow tables or brute force methods to crack passwords)
  -- he/she could **resurrect "deleted" files** from backup tapes or disk snapshots, potentially doing so into a third party's account
  -- he/she could **create new accounts** (including potentially creating accounts for phantom people who don't actually exist)
  -- he/she could **cache a user's current password, change it to something new, login and use it, and then change it back**
  -- he/she can install **untrustworthy executables**, including trojaned login daemons which might capture passwords
- So… a list of usernames and passwords is by no means essential for a former administrator who still has full privileges himself.

BUT Those Usernames & Passwords *Could Have Been* A "Godsend" for The Defendant If/When His Normal Access Ever Got Truncated

- By maintaining a list of other users' usernames and passwords:

  -- **he could have been trying to insure that he'd have continuing connectivity to "his" network "no matter what"**
  -- or he could have been looking for a way to **frame someone else**
  -- or he might have been **curious** about what was being said about him in email, and by whom; with username/password pairs, he could readily check
  -- or he might have had some **perfectly innocent reason** for allegedly keeping that list of employee usernames/passwords, such as wanting to be able to help users if/when they forgot their passwords (**but keeping a list of passwords is a bad idea**)

An Example of Why Lists of Passwords Are A Bad Idea…

San Francisco Network Passwords Spilled by Prosecutors

By Chris Preimesberger
2008-07-28

Article Views: 17287
Article Rating: ★★★★☆ / 10

UPDATED: San Francisco prosecutors accidentally leaked user names and passwords to the city's network, but officials say the network is safe. The District Attorney's office revealed 150 user names and passwords when they entered them as evidence in the case against Terry Childs, the network admin who locked the city out of its own network for nine days in July.

The tale of the rogue network admin at the city and county of San Francisco continues to roll on with the IT world watching incredulously.

In the latest update to the 15-day-long caper, prosecutors from District Attorney Kamala Harris' office submitted personal-access passwords and user names in an exhibit for court reference last week as evidence in their case against Terry Childs, the network architect and administrator who held the city's WLAN hostage for nine days in a professional disagreement with his manager.

A listing of about 150 user names and passwords of city officials for access into the system was submitted as evidence as part of the public record of the trial. After the passwords were discovered by the press earlier today, they were "redacted" from the record, DA spokeswoman Erica Derryck explained to me.

"The codes were always going to be used as evidence against Mr. Childs, and these [active] passwords have been changed as part of the process of undoing a situation that began with Mr. Childs' alleged criminal conduct," Derryck told me.

http://www.eweek.com/c/a/Data-Storage/New-Twist-in-Rogue-SF-Admin-Caper/

A Random Observation About The Abuse of Special Administrative Access

- While one would hope that system administrators would be ethical enough to respect the privacy of their users' mail and files, at least one recent survey indicated that **up to a third of IT staff** admitted to

  […] snooping around the network, looking at highly confidential information, such as salary details, M & A plans, people's personal emails, board meeting minutes and other personal information that they were not privy to. They did this by using their privileged rights and administrative passwords […]

  http://www.net-security.org/secworld.php?id=6459

- **<u>Your</u> site has a policy (with serious sanctions) prohibiting admins from trolling through confidential user files, right?**

And What About Those "*Sniffing Programs?*"

- The way they were mentioned in the extract from the "Motion Opposing A Reduction in Bail" shown on page 48, the "sniffing programs" sure were made to sound, well, rather suspicious…

But We All Know That It *Isn't* Unusual for Engineers To Have Tools to Sniff Traffic

- For example, many sites routinely run **Snort, Bro or another passive intrusion detection system** to detect compromised hosts, external attacks and other network security issues. (**If your site isn't currently doing this, get that project on your to-do list ASAP**). In order to be able to do that work, high capacity fiber networks will be commonly be instrumented with fiber splitters. 10baseT or 100baseT ethernet networks may use ethernet taps and/or switches capable of mirroring traffic to a span port.
- Network administrator may also capture network traffic using a laptop with Wireshark (or a similar protocol analyzer product) on an *ad hoc* basis for things like diagnosing network performance problems or resolving network configuration issues.
- Nothing about any of this "sniffing" by an authorized network engineer is particularly noteworthy or a cause for concern per se.

Encrypted Files Aren't *Ipso Facto* Criminal, Either

Based on the analysis of the Defendant's work computers, hard drives, flash drives, laptop, and work servers, he had saved most of his files on these devices that were encrypted. These drives cannot be unlocked but without the Defendant's password and thus much of the data remains unknown. According to the forensics done thus far on the drives, there is over a terabyte of data stored, which is over a thousand gigabytes of information. These files were downloaded and saved on city computers during the defendant's employment. The Defendant has never volunteered this information or provided the encryption codes so law enforcement could identify what the Defendant was storing. This information could be configurations and backup files that the Defendant told the police that he did not maintain or even possibly confidential and privileged data and email of city employees.

Aarguably, those encrypted files could also be completely innocent files holding only the Defendant's personal information. If the Defendant asserts his 5th Amendment rights, we may never know.

V. The General Problem of Disgruntled Employees In Security-Critical Positions

One of the Trickiest Issues in the IT World: Safely Dealing With a Disgruntled Employee Who Happens to Hold a Security-Critical Job

- Imagine that you're an information technology manager, and one of your employees -- who just happens to holds a security-critical job -- has become "disgruntled"/"problematic." What do you do? Leave them in place? Suspend/discharge them? Something else?
- On the one hand, **if the employee is left in place**, they might never act out in any harmful way (but then again the employee might take actions that could prove to be profoundly destructive)
- On the other hand, **if the employee is suspended or discharged**, management's disciplinary measures **might** resolve a problematic situation, but equally that action **might** serve to trigger the very sort of destructive behavior that no one wants to see happen.
- This is a situation which you need to handle *just right* if you want to avoid an utter disaster.

This Is The Part of the Talk That Will Particularly Disappoint Tech Folks in the Audience (Sorry!)

- I don't have some magical technical solutions that will somehow reach out and keep employees from "going rogue" or "becoming disgruntled." Wish I did; unfortunately, I don't. Employees, as human beings, are a lot trickier than "just" computers or networks.

- I believe that ultimately keeping employees from become "going rogue" requires what some refer to as "soft skills," not the execution of a "technical" agenda.

- In a nutshell, what's required is what I call the "two ells:"

  -- **leadership** and
  -- **loyalty.**

Meat and Potatoes Leadership

- The sort of "leadership" I have in mind is pretty basic "meat and potatoes" stuff such as:
  -- making the right hires & compensating them as well as possible
  -- **letting people know what needs to be done, then giving them the authority and discretion to figure out how to do it (and backing them up if/when they end up needing your support)**
  -- keeping your people in the loop about what's going on and listening to what they're trying to tell you
  -- making timely decisions, and accepting responsibility for them
  -- knowing what to pay attention to, and what to let slide
  -- **recognizing and appreciating what your folks do for you** and
  -- **accomplishing the mission.**
- But there's nothing magic about that particular list -- you could just as easily adopt the "Leadership Secrets of the Rogue Warrior," Dick Marcinko instead. The key is to **start doing <u>something!</u>**

Leadership Inspires Loyalty

- Because there are limits to anyone's ability to technically control the actions of employees in security critical jobs, at root, when you get right down to it, we all basically rely on the loyalty of our co-workers. **If you're truly a leader, you'll get that loyalty.**
- As a working proposition, I think there are six types of loyalty:
  1. loyalty to the organization as a whole
  2. loyalty to the employee's immediate manager
  3. loyalty to the customers
  4. loyalty to the employee's work friends and colleagues,
  5. loyalty to one's work
  6. loyalty to one's self.
- **Employees who have even *ANY* one of those types of loyalty will not "go rogue."** They may not choose to stay with the organization for their entire career, but if/when they leave, they'll leave cleanly and in a professional way.

1. Loyalty to The Organization

- It would be great if every employee was a true-blue "corporate man" or "corporate woman," passionate about their employment and fiercely loyal to their organization.
- In reality, that isn't always the case.
- Sometimes organizations may be at least partially dysfunctional, and when that happens, employees may not feel a "connection" to the organization and its goals and objectives. They may have a **job,** but they're **not on a mission.**
- While cartoons such as Dilbert (or the movie "Office Space") do a good job of satirizing dysfunctional organizations, in real life dysfunctional organizations may lead to disgruntled employees -- which isn't very funny if it happens in an IT security context.
- So how can one inspire loyalty to the organization? Will handing out motivational posters do the job? **Uh, no.** Effectively building organizational loyalty is really a "whole talk in itself."

2. Loyalty to The Immediate Manager

- There are legions of folks who, while they aren't "corporate cheerleaders," are still trustworthy because they at least have respect for, and personal loyalty to, their immediate manager.
- But there can be "organizational risk points," particularly where senior technical staff are overseen by non-technical managers.
- If loyalty to the employee's immediate manager is present, even if the employee is somewhat cynical about the value/role of the larger organization, it is very unlikely that an employee will become disgruntled and thus a problem.
- This is an example of: "I thought about doing <insert something bad here>, but doing that would have ended up screwing over Bob, my supervisor. He's pretty decent as bosses go, so I'd never do <bad thing>."
- Sometimes, however, there may be employees who have neither organizational loyalty nor loyalty to their immediate manager.[64]

3. Loyalty to The Customer

- If both of those types of loyalty are absent, maybe the defendant will at least be **professionally loyal to the innocent customers they ultimately serve.**

- For example, City of San Francisco staff would hopefully not be willing to act in a way which might ultimately harm city residents. But, in order for that sort of loyalty to "kick in," staff need to have opportunities for routine and actual contact with customers.

- Some staff, particularly senior technical staff at some organizations, may be intentionally "sheltered" from customer contact, and that "protection" from customer contact can result in customers being depersonalized or made less "real." If you want to encourage loyalty to customers, make **sure** that all staff members have an opportunity to interact with customers.

4. Loyalty to Work Friends and Colleagues

- Do not take this type of loyalty lightly. This type of loyalty is the sort of thing whihc in war time motivates soldiers to perform heroic acts such as taking grave personal risks to save a buddy.

- In the workplace, loyalty to one's friends can be the saving quality that deters an employee from "going rogue," thereby protecting those friends and colleague as well as the organization itself, the employee's manager, and the organization's customers.

- This is another reason to beware of "single person shops" -- if you have employees who are personally and professionally isolated, and if that occurs, an important potential deterrent to abuse may be missing.

5. Loyalty to "One's Own Work"

- If you've spent a lot of time carefully building a system and making it work, you naturally feed a sense of pride and accomplishment.

- Protecting that work may be another factor motivating you to keep your temper under control and your tongue civil, but concern that one's meister work may be at risk due to careless or unknowing actions may actually sometimes by the catalyst for actions that may be inconsistent, or which may seem inconsistent with the "other loyalties" I've already mentioned.

- I think the defendant quite clearly believed he was acting in a way that was "loyal to his own work," protecting the FiberWAN.

6. Loyalty to "One's Self"

- Finally, before you can "go rogue," you even need to overcome a sense of loyalty to one's own values.

- For example, maybe you've promised to uphold professional standards of conduct, or you come from a religious background and have a strong sense of morals, or you just have a well developed conscience and know right from wrong. Before you can "go rogue," you need to decide that you no longer care about being "true to yourself." That's a pretty radical break.

- In this case, I suspect that the defendant had convinced himself that he ***was*** being true to his own principles (particularly to a strong mission orientation)

From The Defendant's Point of View, What Triggered This Incident?

9. Around June of 2007 Mr. Tong acted unilaterally with respect to some issue on the fiberWAN system with which Mr. Childs strongly disagreed. Mr. Childs felt that after that time, Mr. Tong began to undermine his work[4]. Mr. Tong also began to make emergency decisions on the network, without consulting Mr. Childs. As a result of these actions, the network would get damaged, putting the entire system at risk. Mr. Childs made a number of complaints via e-mail to Herb Tong's superiors, and

---

The server at issue was installed in the data center before Mr. Childs became employed at DTIS.

[4]For example, in March 2008, 311 was having DNS problems. Mr. Childs instructed the contractor to assist and the contractor refused. Mr. Childs subsequently learned that Herb Tong had instructed the contractor not to do any work at Mr. Child's request. As a result, it took 311 an additional month to get the issue resolved. Mr. Childs sent an e-mail to Mr. Tong chastising him for this.

From The Defendant's Point of View, What Triggered This Incident? (continued)

filed a formal complaint against Mr. Tong around early June, 2008. Given this hostile environment, it became clear to Mr. Childs that persons without the ability to properly run the fiberWAN system wanted to run him out of the office.

See the Defense's motion to reduce bail, available at http://weblog.infoworld.com/venezia/childs/tcreduce_bail.pdf

One wonders: should there have been a different manager supervising Mr. Childs while he had a formal complaint on file against his supervisor, thereby potentially avoiding this whole incident?

VI. Summary of Recommendations

Summary of Recommendations

- Take the "insider threat" problem seriously -- it's important.
- Avoid running a large networks with only a single engineer
- Where allowed, conduct background checks and take the result of those inquiries into account when hiring for sensitive positions
- Use scalable AAA practices for large networks, not local passwords on each box
- Insure device configurations have been written to flash or other non-volatile storage so the device can successfully reboot
- Avoid the *no service password-recovery* command
- Provide adequate physical security for each networked device
- Make backups of configuration files, and routinely store at least one copy with your information security officer
- Subject proposed changes to peer review

Summary of Recommendations (2)

- Periodically do an external audit of all systems and networks
- Use RANCID to track changes to network device configurations
- Document your network architecture and design, as well as common policies and procedures relating to it.
- Monitor your network, including providing an out-of-band channel for delivering alerts
- Limit dial-in (or other out-of-band) network access; consider using dial-back modems as an option where access is needed.
- Carefully document locations from which access-limited access is permitted.
- Monitor network traffic with Snort, Bro or a comparable intrusion detection system, and clarify (via policy) who will do this
- Encrypt network traffic end-to-end

Summary of Recommendations (3)

- Forbid creation of written lists of user passwords
- Forbid privileged access to user files by administrators except for specific permitted purposes, and establish serious sanctions for violations
- Develop institutional policies for dealing with disgruntled/ problematic employees in security-critical roles
- Cultivate leadership skills among IT management
- Cultivate loyalty among IT employees
- Be on the lookout for the development of confrontational situations which may involve security-critical employees
- If a supervisor is the subject of a formal complaint by a subordinate, consider temporarily transferring responsibility for management of that employee to someone else (to avoid a conflict of interest, or the perception of such a conflict)

Thanks For The Chance To Talk Today!

- Are there any questions?