Cops are from Mars, SysAdmins are from Pluto

Tom Perrine

tep@sdsc.edu

#include <disclaimer.h>

- I am not a lawyer
- I am not a cop
- I have opinions
- Your mileage (and experience) will vary

#include <locale.h>

- This is NOT the same talk I would have given before the "Carnivore experience"!
- I am not here to take heat for LE "problems"
- The security incident landscape is changing

“geeks” and “cops”

- two different cultures
- own language, traditions
- own “in-jokes”
- both are different from the “mainstream”
- can communicate, with effort

Secret Agenda

- Law Enforcement overview
- investigative processes
  - yours and theirs
- policy and laws
- evidence
- tips for testimony
- cases

Law Enforcement – overview

- Who is Law Enforcement (LE)?
- How are they like us?
- How are they different?

Who is LE?

- Local, state, federal flavors of sworn ("peace") officers - cops
- District Attorneys (DAs) and US Attorneys (USAs) - lawyers
  - ADAs and AUSAs actually do all the work

A Field Guide to Officers (US locale)

- K-12 school district, university campus
- city police, county sheriff, state patrol or troopers
- DA and USA investigators
- Secret Service, FBI, Customs
- DoD - AF OSI, NCIS, Army CID

LE is like us

- over-worked
- some have PHBs
- some have the "clue-nature", some do not
- some are trustworthy, some are not

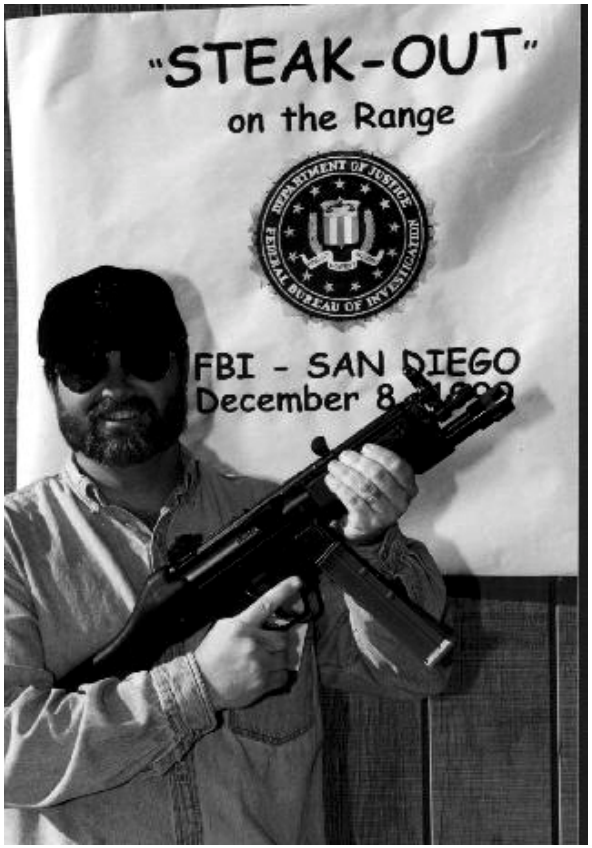
LE is changing

- "a badge, a gun and a laptop"
- better tech training available
- less macho

LE is your friend – but

- they have different goals
- they have different priorities
- they have different constraints on
  - what they can do
  - what they must do

...sometimes they share their toys :–)



But never forget…

- you can trust a person, but NEVER an organization

It's all about…

- personal relationships
- trust
- evidence and analysis
- policies
- law

Who calls who?

- If you are a system administrator, you will eventually have to deal with LE
- Sometimes you need them
- Sometimes they need you

Incident Response Process

- detect "something wrong"
- some basic analysis
- Decide
  - cover-up and move on (lather, rinse, repeat)
  - decide to trace back to perp

What do you really want?

- Make problem go away?
- "scare them off"?
- trace and inform source?
- prosecute - civil or criminal?
- track, kill, skin, eat, mount head on wall?

So, when do you call LE?

- Initial suspicions?
- After your own investigation?
- After analysis?
- After the civil trial?
- After midnight?

Do your own investigation first…

- "ISP exemptions" allow you to take "any steps needed to protect the communications system"
- sniff networks, interview users
- modify systems/networks
- save, process, archive logs

....but do it right!

- Preserve evidence
- Document everything!
- CYA - morally, legally, ethically
- follow your policies
- follow the law(s)

Once LE is involved

- must avoid becoming "agent of the government"
- their goals are not always your goals, remember?

If you are an "agent"

- All LE constraints would apply to you!
- Evidence you gather or handle would come under all LE constraints
- Improper wiretaps are a Federal Felony - no saving throw!

Start with your policies

- company HR policies
- non-disclosure agreements
- "personal information", "student records"
- who may authorize disclosure?
- who owns/controls hosts?
- who talks to LE and/or the press?

Then go to the justice system

- relevant (Fed) laws are scattered through US code
- overview of relevant Federal law at
  - http://www.sdriw.org/Presentations

Title 18 – criminal code

- wiretap laws - all over
- sec 1030 - cyber-crime ($5K bar)
- sec 2701- ECPA (freebie)
- secs 2510, 2517, 2511, 2703, 2705- exceptions
- sec 2707 - ISP liability

Title 47

- sec 223 - cyber-harassment

Oh, by the way…

- State laws vary widely
- Some states have good coverage, others have none
- Non-US laws is sometimes strange and wonderful

California, for example…

- Personal privacy is a constitutional right
- student records have excellent protection
- Penal Code 502
  - good for "us", bad for minors

Who you gonna call?

- Campus cops?
- local (state, county)?
- FBI?
- Secret Service?
- Customs?
- Mounties? AFP?

What are they gonna do?

- Ask lots of questions
- Go through their process…

LE Investigative Process

- initial complaint to LE
- initial contact from LE
- Interviews -give evidence and analysis to LE
- wait
- wait some more
- maybe a trial or plea

initial complaint

- you guess who you should call
  - FBI Cybersquad, if you've got one
- describe crime as you see it
- provide your contact info
- "leave a message"

initial contact

- call back from "the right person"
- will take some details (again)
- will do some research and make an appointment for interviews

interviews

- two suits show up at your door
- plan on at least 60-90 minutes
- provide "first-round" of information

Plan to provide

- organization's background
- possibly a tour
- network maps
- your security policies
- all the incident data

kinds of evidence

- images of disk drives
- logs and backups
  - remember to suspend log and backup overwrites!
- email

Please…

- Be patient
- be willing to answer questions, sometime over and over
- if you are a manager, let LE talk to the tech people ASAP
- try to respond quickly to requests for info
- be patient

Handing over evidence

- How do you balance the desire to disclose with
  - internal policies
  - ECPA
  - ISP liability
  - personal liability

Internal policies

- get cooperation from "higher powers"
- involve your legal folks
- the only good lawyer, is *your* lawyer :-)

CYA

- hardcopy documentation of approvals
- can be very informal, such as a signature on a notebook page
- identify your people, get them educated before you need them

two cases

- you are the victim
- you are a 3rd party that has evidence of a crime against someone else

If you are the victim

- generally, liability shelter in providing evidence
- check your policies
- check your lawyers

If you are a 3rd party

- in all cases, get some form of court order!
- could be a
  - search warrant
  - subpoena
  - "2703" order
- some liability shelter in responding to a court order in "good faith"

Asking for a court order

- usually not seen as an "adversarial issue" by LE
- is "business as usual"
- it is the proper CYA
- should be sent to you via your legal folks

OK, now what?

- Mostly, you wait
- The wheels grind slowly, but eventually they *do* grind
- your case may not be high priority, but you may have the key to a big case
- Don't discuss details of pending cases

Trial or plea...

- In general, cases will plea
- lower stakes for perp, only $$$
- quality of evidence

Tips for testimony

- It's nothing like TV/movies
- be prepared, have hardcopy in-hand for everything you expect to be asked about
- discuss questions with prosecutor
- "just the facts, ma'am", unless ASKED for an opinion

"Reasonable Doubt"

- as technical folks, we tend to be more aware of "possibilities"
- "Is it possible that…"
- "It is not impossible, but I've never heard of it, or seen it, nor have any other experts I consulted"

Sometimes, "they" call you…

- And how do you know who they really are?
- "social engineering"
- are they "poaching"?

Authentication

- "Who is this, really?"
- Why are you calling me?
- What do you want?
- How can I prove who you are?

In general...

- LE does not make cold calls after hours
- cyber-crime (white collar) investigation is a M-F 9-5 job
- there is no "hot pursuit" in cyberspace
- asking for proof of ID is "normal"

Also, for all Federal LE

- you should never be cold-called by someone non-local
- all initial contacts will be done via their local office, or via the local police

"Poachers"

- working out of jurisdiction or assigned area
- working "out of scope"
- the "midnight avenger"
  - hanging out on IRC baiting pedophiles, hackers, warez d00ds

Some real examples…

- Operation SunDevil
- Secret Service Agent Stevens from Denver
- "Stryder"
- Local .com
- child porn

Operation SunDevil – 1990

- Secret Service seized all computers at Steve Jackson Games
- classic "bag and tag"
- almost put SJ Games out of business
- bad (no) evidence
- no charges, ever
- EFF formed soon after :-)

Secret Service Agent Stevens – 1996

- 3 am call to NOCs at SDSC, Netcom, CISCO
- In "hot pursuit" of "one of Kevin's friends"
- wanted home phone number of Tsutomu Shimomura
- gave Denver cell phone for call-back

Hmmm...

- cold call, during DEFCON
- had office phone number for Secret Service office in Denver (closed)
- unable to verify name via watch office in D.C. (useless)
- turned out to be DEFCON practical joke

STRYDER.SDSC.EDU – 1998

- Solaris host, compromised in September 1998
- intruders used Stryder to go to other already-hacked sites
- detected intrusion, set up sniffer, watched for several days
- intruders were connected to well-known hacking group

After our own investigation

- turned whole thing over to local FBI
  - asked for subpoena
  - provided 4 Gbytes of data
  - case went to NY office
- started waiting…
- forgot the whole thing, until…

October 1999

- get cold call from FBI in New York
- ask him to go through local office
- get authentication from known SA in SD
- assist with analysis
- still waiting…

November 2000

- still waiting
- case is making progress

July 2001

- stll waiting
- case is making progress

Local .com – 1999

- get 3am call from friend at local .COM
- handling large intrusion
- looking for LE contact

.com did the investigation

- had handled all internal stuff - up to company President and Counsel
- had worked with ISPs to trace to an IP at a large university
- just needed FBI to contact LE at university and take over

good outcome

- able to connect two groups
- FBI interviewed suspect several days later
- suspect was arrested several months later, charged in 3 Fed jurisdictions
- personal contact and trust are the key

Child porn case – 2000

- invited to serve as expert witness in child porn case
- part of international child porn case
- suspect had 40,000 child porn images on his home hard drive
- had text files of "pliable caregivers" in 3rd world orphanages
- he said that "evil hackers did it"

Evidence

- on his system - W98
  - FTP logs, images on his system
- on his friend's system in Ohio
  - IRC chat logs bragging about collection
- daughter changed sides during trial
  - he had pictures of her mixed in his collection!

Trial

- many questions of digital evidence
- lots of "is it even remotely possible..." from defense - creating doubt
- had physical evidence to complement digital evidence
- longest 4 hours of my life

Good Outcome

- convicted on all counts charged
- sentencing guidelines said 30 years
- judge wussed out and gave only 9 years
- perp is sitting in jail, with a BFR (Big Friendly Roommate)

Ways to cooperate

- might as well, you will need each other at some point
- better if you lay groundwork in advance
- person to person is best
- NEVER trust an organization

SDSC's experiences

- started with SDRIW in 1995
- expanded to HTCIA in 1998
- last bridges in place with "CATCH TEAM" in 2000

SDRIW – 1995

- San Diego Regional Information Watch
- regional "CERT"
- partnership between academia, government and private sectors
- 80% technical, 20% law enforcement
- face to face contacts

HTCIA – 1998

- High Tech Crime Investigation Association
- 80% law enforcement, 20% technical
- emphasis on training, communications

"C.A.T.C.H. Team" – 2000

- the acronym came first - don't ask
- multi-agency high-tech crime task force
- full-service - investigation through prosecution
- has its own assigned ADA and AUSA

Remember

- LE is another sub-culture, just like us
- they come in many flavors, just like us
- sometime you need them , sometimes they need you
- build personal contacts with them, NOW, before you need them

Finally

- know the laws and your own policies
- you have more flexibility than LE
- court orders are your friends
- there are lots of ways to cooperate

Trust, but verify

- trust PEOPLE, never organizations
- build personal relationships
- be careful, be patient