Advanced Physical Security

Beyond Dumpster Diving and Social Engineering
or,
Screw the Firewall and the Secretary Too

Eric Schmiedl
security.ericschmiedl.com

“We Want Information… Information… Information… “
“You won’t get it.”
“By hook or by crook, we will…”

– The Prisoner (1967)

"Many of Russia's wealthiest banks and corporate tycoons have set up their own private security agencies, usually staffed with former KGB officers. Their task is to spy on their political and business enemies and to gather compromising material...

...the former KGB has fragmented into a multitude of private agencies that exploit their secret-police expertise for personal profit."

–Geoffrey York, *The Globe and Mail*, 7/8/00

"[US officials] say a record 108 nations were involved in trying to steal sensitive US technologies in 2005, the last year for which full data was available."

–James Kitfield, *Air Force Magazine*, March 2007

Blurring the line between industrial and government espionage

Hacking for exploration -> Hacking to steal money/information

Clever exploitation of technology -> Whatever gets the goods

Computer crime as a business

We've seen an explosion of computer crime in the past few years, and I'm not talking about people hacking the NSA so they listen in on Karl Rove's cell phone. I mean the flourishing industry in stolen credit card numbers. I mean people in Who-Knows-Where-istan using their botnets to wipe companies off the Web if they don't pay protection money. And above all, I mean identity theft -- people taking out lines of credit using stolen financial information. The thing is, Ivan P. Malwarovski doesn't care about how he gets the information he needs to take people to the cleaners. It doesn't matter to him whether he pulled off a great end-run around the IDS or whether he paid his buddy the ex-KGB agent to break into their office and plant a laptop in the dropped ceiling. Ivan makes his money no matter what. And what if he isn't in the identity theft business? Maybe he knows a Romanian commodities trader with a couple million left over from his last oil deal that he'd love to put towards some unorthodox market research. With modern financial networks subject to all sorts of monitoring, he might be better off with a microphone above the boardroom ceiling than a laptop.

You and everyone else are the weakest link

Elicitation
Recruitment
Infiltration

Elicitation...

"[the] subtle extraction of information during an apparently normal and innocent conversation."

– NASA

- **NEVER ask 'the question'**

Elicitation

- Play dumb-- make deliberately false statements. People love to correct errors.

- Get them involved in a game of one-upmanship.

- Ask for help.

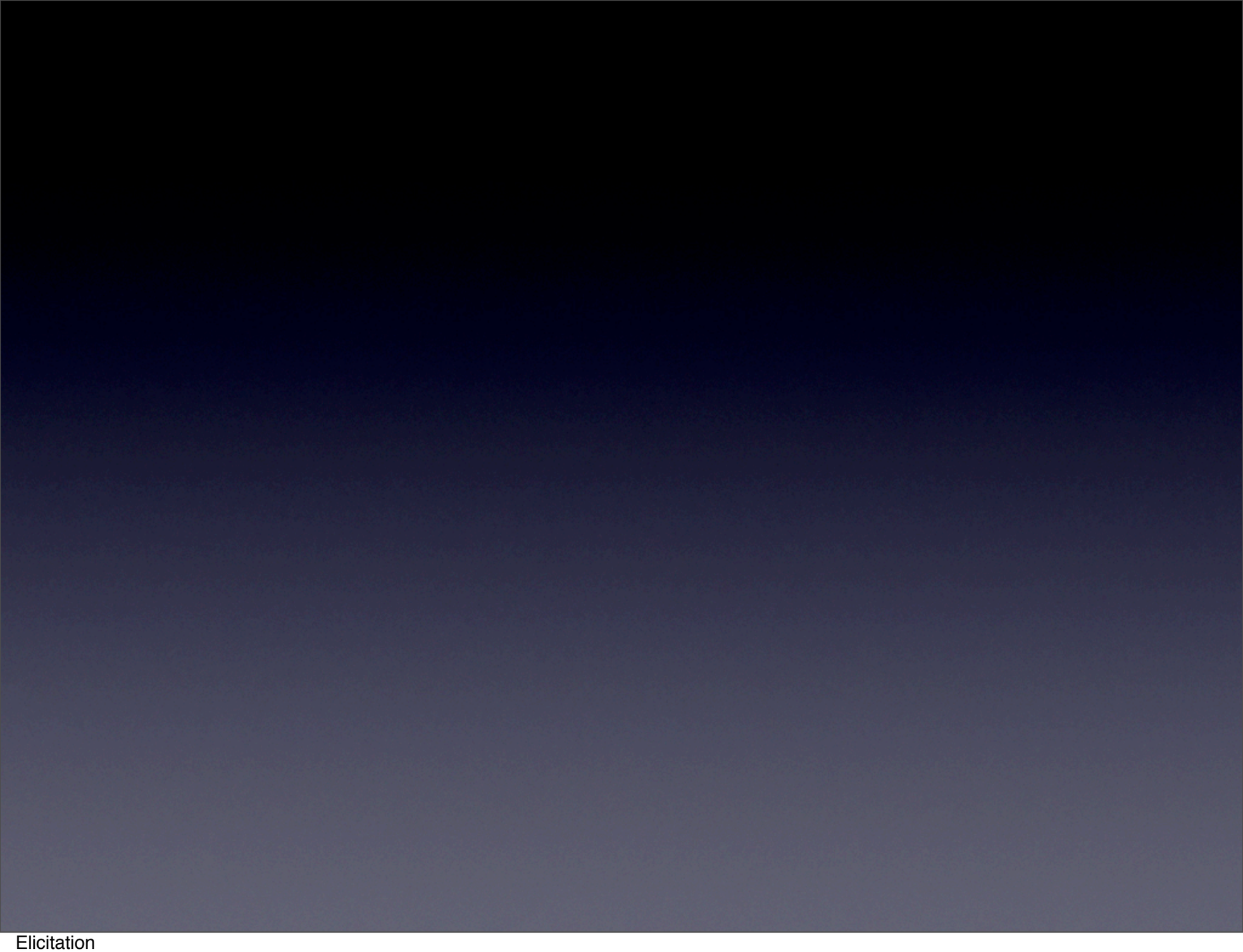
- Flattery!
  - "The greater the expert, the more he appreciates praise." – Christopher Nolan

- Ask sensitive questions in the middle of a conversation.

Elicitation
People usually only remember the beginning and the end of a conversation. You'll probably only remember the beginning and end of the presentation

- It's all about putting together little pieces of information.
  - Speak with many different people to fill in different parts of the picture.
    - In each division of the company (technical, sales, etc.) a few people will know about the target project
  - Outside the company, too:
    - Customers
    - Suppliers
    - Trade journalists
    - Professional societies
    - Consultants

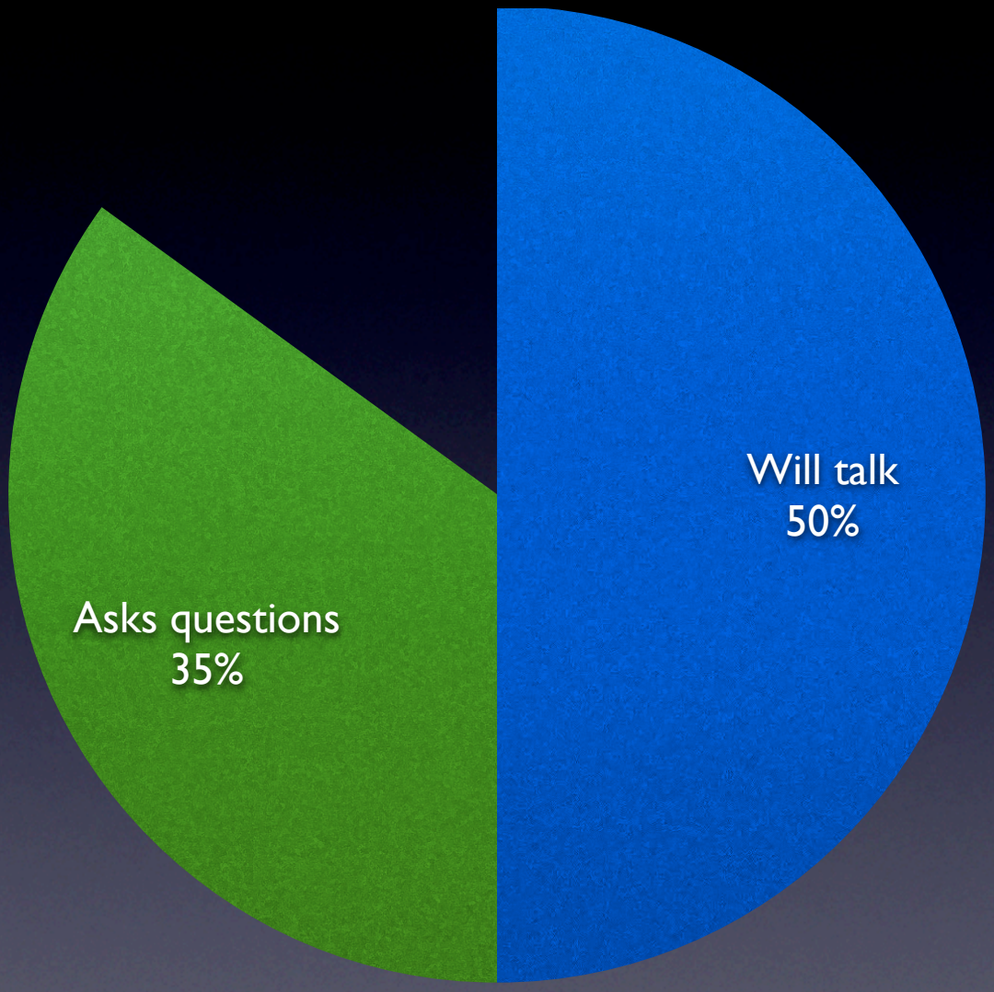
- **Know when to stop.**



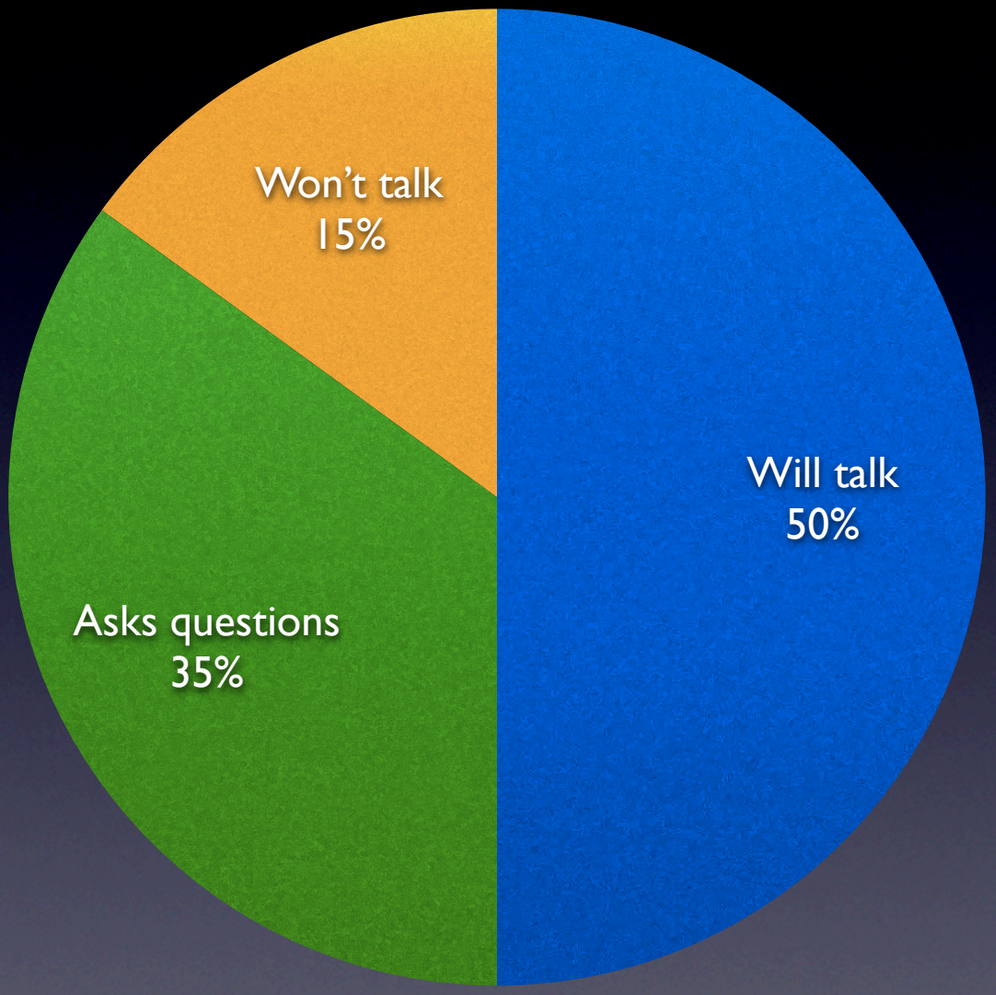
Elicitation
50% will talk to an anonymous stranger immediately
35% will ask who the stranger is working for, but talk happily after being told that the stranger can’t say who he’s working for
15% won’t talk



Elicitation
50% will talk to an anonymous stranger immediately
35% will ask who the stranger is working for, but talk happily after being told that the stranger can't say who he's working for
15% won't talk



Elicitation
50% will talk to an anonymous stranger immediately
35% will ask who the stranger is working for, but talk happily after being told that the stranger can't say who he's working for
15% won't talk



Elicitation
50% will talk to an anonymous stranger immediately
35% will ask who the stranger is working for, but talk happily after being told that the stranger can't say who he's working for
15% won't talk

What will people tell a complete stranger?

Enemy Within: Recruiting Spies

"[Recruitment requires] incremental entrapment in a subtle web of irresistible compromises." – James Angleton, CIA counter-spook

Recruitment
Gradual escalation

1. Spot the potential recruit
2. Do your homework
3. Get access to them
4. Develop them as a recruit
5. Recruit them
6. Profit!!!

Recruitment
Steps of recruitment

- People with access to:
  - The information
  - Other people (access agents)
- Make sure they aren't counter-spies

What to look for in a potential agent

- Their potential motivations
- Their habits/vices

Background work-- what do you want to know about someone in order to recruit them?

- Money
- Revenge (on a person)
- Revenge (on a government or system-- disaffection)
- Blackmail or hostage situation
- National pride
- Emotional involvement
- Naivete
- Sex
- Ideology

Why would they work for you?

- People who can get you in touch with the target.
  - Ideally they have connections in the target group or community, but prostitutes will do in a pinch.

- Find recruits
- Make introductions
- Fuck

What do access agents do?

(I had a feeling that would get your attention.)

- People trust people they have sex with
  - KGB swallows and ravens
  - the "secretaries offensive" / Romeo spies
    - "Love, or a plausible semblance of it, was capable of generating more intelligence over a longer period than brief sexual encounters [and blackmail." –Mitrokhin / Andrew

Development, the nice way

1. Establish friendship
2. Ask for innocent or insignificant favor, and reward it generously
3. Wash, rinse, repeat. They become dependent on your money
4. Get them on the path to betrayal
    - ask for the internal phonebook
5. Ask for something more sensitive, with a good excuse

Development, the mean way

- Make their life hell
- Offer to fix it– for a (small but significant) price.
- Escalate.

- Make the pitch.
- Be ready to blackmail.

KPMG / Guy Enright / Diligence, Inc

Story time.

- A fake resume and good interview skills will get you far.
  - ...ditto with protest or political groups
    - Heathrow Airport & C2i vs. Plane Stupid
- Temporary employees
  - Construction worker + lunchbox full of radio transmitters and microphones = a night shift full of fun

What if you can't spot a likely agent? Infiltrate!

- Tailgating
- Forged IDs
- Request to Exit Sensors
- Attack the mechanism
- Dropped ceilings

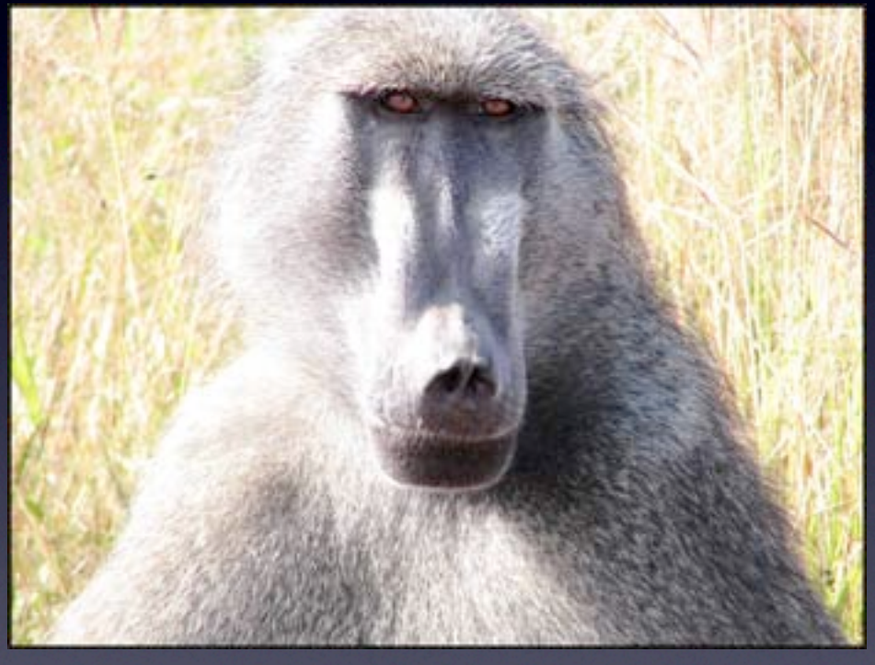
Maybe you just want to break in, Watergate style...

People are polite. Take advantage of them!

Tailgating: the fine art of following legit users through a door



The man in charge of security at an unnamed military base wanted to check the security at his installation. He called up two of his drinking buddies who worked as staff in one of the more sensitive areas in the base, and proposed a little game... using his authority, he had passes made up for them that replaced the faces on their cards with those of African baboons, and offered them each a night of drinks if they could get in undetected for a solid week. They were only found out three months later when one of the staffers dropped his card in front of the guard -- the guard finally looked at the picture when he was picking it off the floor. Photo IDs suck.



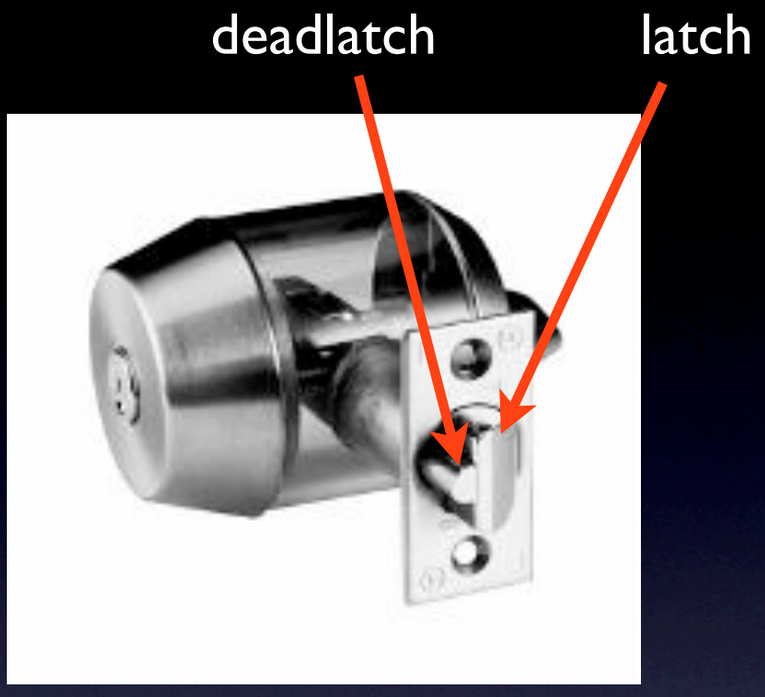
Source: www.african-safari-pictures.com

The man in charge of security at an unnamed military base wanted to check the security at his installation. He called up two of his drinking buddies who worked as staff in one of the more sensitive areas in the base, and proposed a little game... using his authority, he had passes made up for them that replaced the faces on their cards with those of African baboons, and offered them each a night of drinks if they could get in undetected for a solid week. They were only found out three months later when one of the staffers dropped his card in front of the guard -- the guard finally looked at the picture when he was picking it off the floor. Photo IDs suck.

Request to Exit Sensor (n):

Motion detector conveniently placed to save an attacker the trouble of picking the lock—by allowing him to use a helium balloon instead

- Sliding/carding/loiding
- Lockset vulnerabilities
- Breathe on the fingerprint sensor
- ...a whole lot more

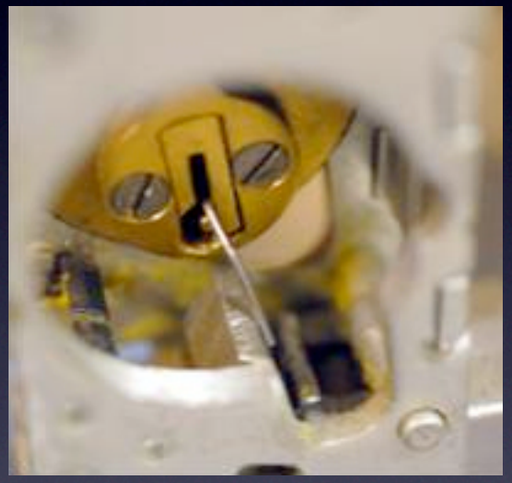


- aka 'sliding' or 'carding'
  - aka 'using a credit card'
    - (don't actually do that)

The card pushes or pulls the latch back when you slip it between the door and doorjamb. Sometimes even modern locks with deadlatches designed to prevent this are vulnerable -- either the locksmith installed the strikeplate in the door such that it doesn't push back the little nub, or the door is using an electric strikeplate that doesn't even try to engage the deadlatch.







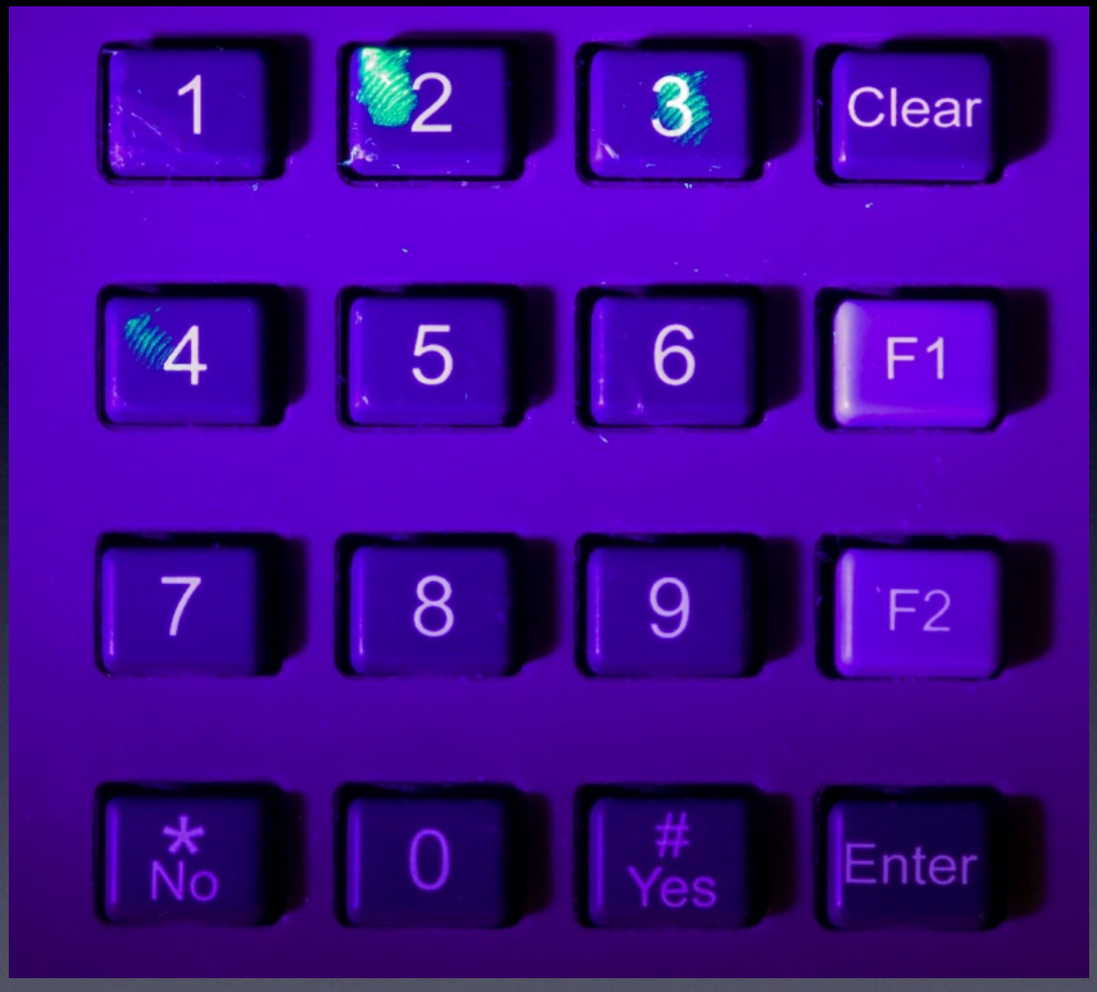
Photos from the Institute of Certified Locksmiths, http://theinstituteofcertifiedlocksmiths.org

- Lockset vulnerabilities:
- Don't involve picking the lock– they're often fast and easy
- Vary from model to model
- e.g the Adams-Rite Bypass:

Electronic Locks



Some electronic systems are really well designed and secure



Others aren't. You can bypass a lot of keypads with the strategic use of yellow highlighter ink. It blends in great with the keys but fluoresces under UV light, and fingers track it from key to key so you can see what order the keys are pushed.

Sometimes, just your breath is enough.

If you breathe on some older fingerprint locks, the lock will open-- your breath doesn't condense where the last user's fingerprint left skin-oils.

(I’m not Deviant Ollam)

Lock picking leaves no visible evidence of entry, and most mechanical locks can be picked

A priest, a rabbi, and a spy walk into an office building.
The spy says to the receptionist,
"Mind if I use your restroom?"

Matt Blaze independently discovered and published a vulnerability in master-keyed pin tumbler locks that allows someone with a single key that fits a single lock in the system to figure out the master key for the system. In short, they cut a series of six or seven keys (one for each pin in the lock). Each key is identical to the source (change) key, except for one pin position which is left uncut. To find the master key, they try each key in the lock, and record which one(s) work. They repeat this again, cutting down each uncut position by one cut-depth, until they've reached the bottom cut depth. They now have at least two key-cut codes for the lock: one of which is the key they started with, one of which is the master key for the building, and maybe a few others whose purpose can be figured out with a little more work.

How the Watergate burglars were caught

Former CIA official and Watergate burglary-team member James McCord used duct tape on the stairwell door locks to prevent them from locking. While making his rounds, Watergate security guard Frank Willis noticed the duct tape and pulled it off, then continued on his rounds. But McCord was stupid and put more duct tape on—when the security guard saw that it had been replaced, he called the cops.

One more thing we can learn from Watergate

Dropped ceilings are really convenient. When they were caught, the Washington DC police found two ceiling panels had been taken down from the ceiling of the DNC secretary's office. Since the secretary's office was adjacent to that of the chairman's, it was possible to place a bug above those panels that would listen to everything being said in the office. It didn't matter how well the office was secured—the DNC chairman could have had the best lock in the world on his door, but the dropped ceiling panels that most people assume are the real ceiling were a wonderful backdoor.

“Gentlemen do not read each other’s mail.”

–Henry L. Stimson, US Secretary of State, 1931

I guess that means all you gentlemanly types can safely skip over to that other awesome talk you were thinking of going to, because I’m going to talk about just those things Mr. Stimson hated.



Who's expecting this guy?

Visual surveillance is the easiest and probably the most legal way of seeing what a target is up to. All it demands is access to a good vantage point, and modern optics will reveal a lot. Who expects someone to be looking in through a skyscraper's window?

Not Boston's MBTA, anyway.

As part of their research into the security of Boston's MBTA subway system, my friends Zack Anderson, RJ Ryan, and Alessandro Chiesa realized that the main operations building was visible from publicly-accessible areas of a nearby office building. Through the magic of modern technology, they didn't even need to get past the front desk in order to see what was going on inside.

flexispy.com
world-tracker.com

Flexispy.com will sell you software for 100-150 Euro (depending on OS) that allows any Symbian, Windows Mobile, or Blackberry-based phone to be used as a bug.



—*Die Welt*, 4/26/2008

Security staff at the Ritz-Carlton hotel in Wolfsburg, Germany found a “babyphone” intercom concealed under the sofa in Porsche boss Wendelin Wideking’s room. According to hotel records, no family had stayed in the room for several weeks prior.

...regular intercoms, too

Digital Voice Recorders:
They're even advertised as perfect for recording meetings!

What does your voice mail say about you?

Voice mail boxes are easy to password-guess

Why not just put a bug on the CEO?
Heck, why not get him to bug his *own* meeting,
and save us the trouble...

Wireless microphones are designed to provide crystal-clear audio at a decent range, consistently and reliably. Even to the guy with the radio in the parking lot.

...getting a little more advanced:
Bluetooth!
Keyloggers!
the PBX! VOIP!

That van has been parked there for an *awfully* long time: Advanced Techniques

TEMPEST

Wim Van Eck discovered the fine art of Van Eck Phreaking back in the 80s, even though the NSA had known about the trick since the 1950s–they called it TEMPEST. In short, TEMPEST attacks involve using the radiation emitted by electronics in the course of normal operation to figure out what those electronics are doing. The original Van Eck research used the signal emitted by CRTs to reconstruct the picture on the screen at a distance. Nowdays, LCDs make that a whole lot tougher—so get your boss to buy you that 30" Cinema Display already....

But forget the wireless keyboard. Turns out some are pretty easy to intercept.

Phone taps

If you're going to go great lengths to read someone's email, you might as well listen to their phone calls too. If you're Wal-Mart trying to hunt down people talking with the New York Times, pesky details like warrants aren't a big obstacle to your investigation. [Bruce Gabbard story]

They should have hired Anthony Pellicano.

You can hide a transmitter just about anywhere.

You can hide a transmitter anywhere. No, seriously. Tell your paranoid boss he may want to go in for a proctologic examination.

Heck, you can even hide the bug outside the room.

Google ‘laser bounce window listener’

Ceiling camera is watching you

Sandridge Elementary School case. But cameras don’t just provide compromising footage of office trysts

Using hidden cameras to discover alarm system codes or safe combinations

Other useful information: reconstructing keystrokes from audio

How to Find a Bug: the fine art of TSCM

Spy shop ‘bug finders’ suck.

No, really, don’t even bother.

Spotting signals: the spectrum analyzer.

What's the difference?
OSCOR and other spectrum comparators, the WinRADIO cheap option

Even when the bugs are turned off:
the Non-Linear Junction Detector

Voice Over Just About Anything:
the HF receiver and carrier-current bugs

Can’t Beat the Heat:
Thermal Imaging

...most important of all:
physical search!

Check the car, and the home.

Case examples: Equitable Life CEO and Tommy Sheridan

Want to hire a pro?
It'll cost you.

When TSCM goes wrong

Kid Rock nightclub story

Wireless networks are outside the scope of this talk.
Not that it matters, since they're all 100% secure these days anyway.
Go attack something easier. Like a printer.