Physical Security – the Good, the Bad, and the Ugly

Mark Seiden
MSB Associates
m@seiden.com

What is physical security, anyway?

- Access to tangible assets or artifacts that represent them or access to them.

Example of such assets include

people, computers, network plugs, the phone switch, a sysadmin's keyboard interface, unencrypted backup tapes, the encryption keys on a floppy disk, the list of code names for the deals in play, the personnel database, the access control computer on the enterprise net, the master key in the coffee cup, a clear view of the safe dial, the bearer bonds in the safe.

- Rather than attempt a rigorous definition, it's more fun to define it contextually… but as programmers, let's try to do it top-down.

Physical security on Planet Earth

- Perceptions about security has been elusive and highly distorted since 9/11.
- One can't economically "secure" anything large against a determined adversary with substantial resources.
- People are not rational when making risk vs. reward or investment decisions. Politicians (= sales people) use the "fear sell".
- Little evaluation of effectiveness of controls -- public perception and the ability to grab land are key.
- Rights to (and value of) "identity" and "privacy" are still in gray areas in many countries.

Physical security in the business environment

Some nasty trends reduce security (particularly control and auditability)

- Offshore development and operations (particularly customer service)
- Outsourcing to external entities
- Centralization of control and operations often = Making the wires much longer than ever

Physical Security in the Enterprise

- Fragmented responsibility and authority (split among facilities, sysadmin, networking, legal, HR, vendors), often multi-site.
- Shoestring budget, particularly for remediation of older facilities
- If there's "risk management" at all it's often got an insurance mindset
- Those with functional power are often low status, low skill, low training and quaity of their work is seldom measured or rewarded, so taking shortcuts is common.
- Decisionmakers have neither the time nor skills to verify vendor claims, and almost no solutions are "open source".
- …and they strongly believe in Security Through Obscurity.

...

- Common copouts, rationalizations, excuses:

"That's not my job" or "It's my vendor's problem".

"I don't consider that a *plausible* threat" or "We've never had that problem before".

We just have to raise the bar enough for them to go somewhere else.

Our controls are better than locks and keys.

You have to trust x or they won't get any work done.

But that database is *encrypted*!

Physical Security in a campus or building

- There's a lot of "legacy" to deal with in pre-existing buildings not specifically designed with security in mind

Existing partial-height walls, hung ceilings and raised floors, wiring rooms in the wrong places, wire runs through public areas, unsegmented networks, already installed doors and locks.

- Is there any perimeter? (At least we can still ask that question in physical security).
- Is there any protected area/vault which can serve as a basis for trust?
- Can one safely provide friendly facilities for joint venture partners or visitors?
- Required backdoors or key escrow (e.g. "Knox Box").
- Building control (Local Operating Networks) (e.g. LONworks).

Multi-tenant buildings weaken the defensible perimeter

- Shared infrastructure: telecom, datacomm, cleaning/janitorial facilities, common areas which are likely to be weak or unprotected.
- Probably master keyed
- Unknown visitors and deliveries to other tenants
- Independent access policies and controls
- It's ifficult to secure "the building" as a whole (on any level).

The weakest tenant's security policy could become your *de facto* security policy.

Colocation facilities are a very special case of multi-tenant buildings

- Some are like “gated communities”.
- Others are more like campgrounds with video.

Your co-tenant’s weakest visitor and vendor policy puts you at risk.

And finally we get down to the ground level components – nuts and bolts

Or, in this case, such elements as

Locks and electronic access controls (cards, readers, biometrics)

Sensors and alarms

Auditing facilities (to figure out what happened) such as

Video surveillance, backups, telephone detail billing, badge access logs.

These components have complex Real World interactions.

Doors

- Made of?
- Single or double?

Double glass doors usually have a gap between them. What's within reach?

- Where and of what construction are the hinges?

If doors are simple, how can they go this wrong?

...

Locks

- Tubular, Rim or mortise

  have different latch designs, different force-resistance, varying reliability, and weaken the door more or less.

- Mechanical, possibly with electric strike, or Electrified

And there's an access control, a "lock cylinder" in which you put a "key", (perhaps a reader for a badge, perhaps a biometric device or pin pad.)

Problems with Locks

- Sometimes you can't easily tell by looking if they're locked or unlocked
- Deadlockers are often mis-installed, broken, or ineffective
- Keyed locks often permit bypass on doors controlled by badge access control or a numerical code

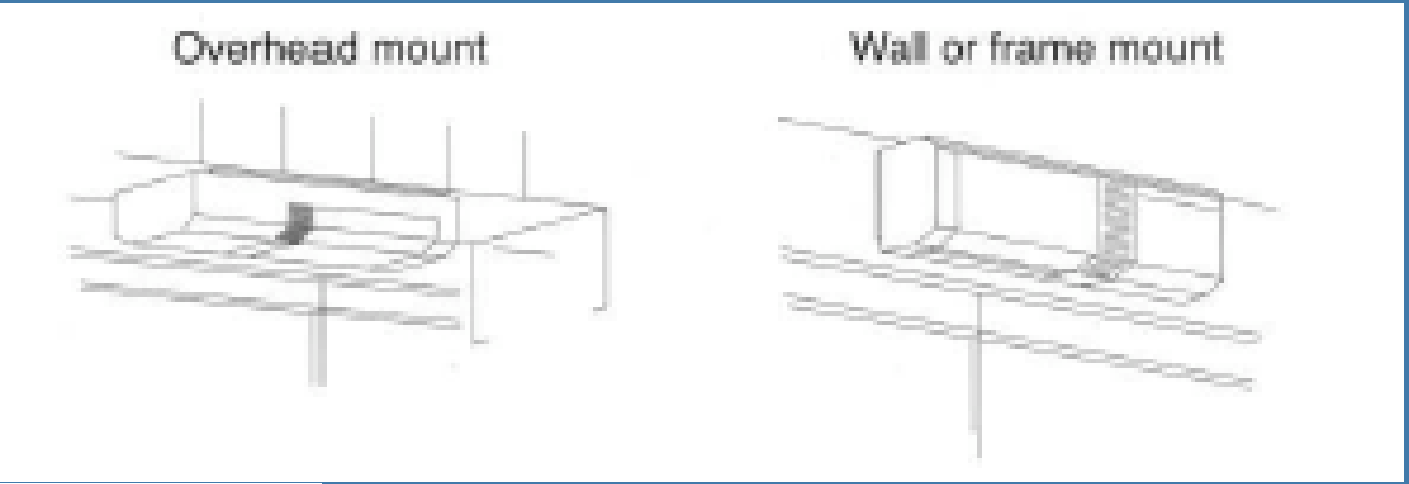
Request-to-exit switches

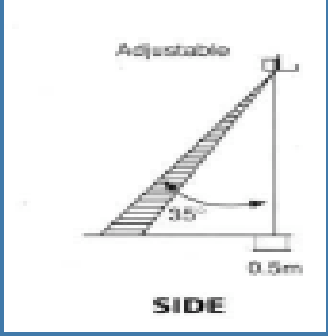
How do you get out, then?

Frameless glass doors are a problem

Request to exit sensors

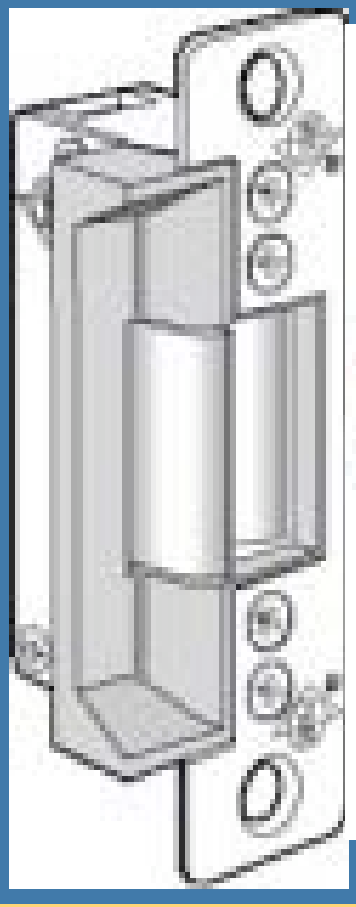
- Usually passive infrared (sense temperature differences between an object and the background)





Problems with Strikes (Electric or Magnetic)

- The biggest selling tubular locks have deadlockers rendered ineffective by the biggest selling electric strikes



...

- Exposed/accessible strike placement or wiring
- Magnetic strikes not on uninterruptable power
- Magnetic strikes are frequently on the wrong side of the door
- Adhesive tape on magnetic strike reduces holding strength dramatically (according to an inverse cube law!)
- Magnetic strikes need a request-to-exit sensor or switch

And problems with lock cylinders…

- Picking
- Making a key, or even better a master key.
- On Interchangeable Core cylinders, making a Control Key, which allows easy removal of the lock cylinder and replacement with one of your preference.

Very few lock instances are necessary for a brief time to make a master or control key by disassembly. Locks in public areas, old doors in basement storage, and padlocks frequently/easily sprout legs.

Revocation of rights is unacceptably difficult and expensive with mechanical locks.

Electronic access controls

- There's a computer and a database involved (oh oh).
- It's wired (somehow) to microcomputer-based "panels" with local authority to unlock doors (containing caches of access rights and access events.)
- Panels are connected on local wiring (a loop or point-to-point) to badge readers, electrically-controlled locks, door state sensors and "request to exit" sensors or switches. Lots of components which can be manipulated along long wires!
- A refreshing number of ad-hoc proprietary protocols to look at. Any bets how frequently these components mutually authenticate their counterparties in a authentication or auditing transaction?
- Back doors for installers and maintainers (and maybe others).

And what about those cards?

- Proximity cards are an early example of RFID tags.
- Typically have a short facility ID and a card number (think of a subnetted 32-bit IP address).
- Most can be read remotely by an attacker (no challenge'/response0 -- imagine a card emulator that will replay the bit sequence just read.
- Some are "field programmable"
- Low card numbers are often more senior = more privileged.
- Brute force attacks are typically logged but there are no countermeasures
- So are these more or less secure than keys? Instant revocability and fine-grained access control are their big advantages, but a class attack makes them risky.

A case study (Mark Seiden/Mark Chen)

- Receptors GP3 access control system.
- SCO Unix on a PC on the enterprise network but with nonstandard addresses. Serial wiring to “guard stations” running terminal emulation, TCP to ethernet-attached panels.
- Root password (“r00t”) published in the user manual.
- Dialup modem (which tech support recommended be always left on).
- So I logged on as root, and started poking around.
- Netstat –na said it was listening for tcp connections on 21 ports including rexec, rpc, and sqlexec.
- All the source was on the machine and features were compiled in with #defines. (e.g. #ifdef JETWAY, #ifdef US_HOUSE)

…

- customers mentioned in the source code (with #ifdefs) included

LDS CHURCH, AMD, GE King of Prussia and Camden, University of Washington, Corning, US House of Representatives, US Senate, USC, Yale, and 5 airports by name.

(Turns out their customers included >50 airports, prisons, courthouses, and even a spook agency.)

Looking at the database schema and tables was instructive!

The system has a concept of “passkey”, a magic word typed at a guard terminal which conveys various privileges. (all in database table psky.dat, lightly obfuscated).

Looking at the passkey validation code, we noticed that there was a special undocumented passkey, a magic function of the date, which conveyed system manager privilege to anyone knowing the magic spell.

So, what could an attacker do?

An outsider on a dialup line, or an insider on the LAN, could

permanently or temporarily enable badges with bogus access or deny access to legitimate users.

cause immediate diagnostic events to occur (e.g. unlocking doors or areas),

schedule timed events to occur (e.g. unlock all doors 2am-3am on Sunday)

create stealth badges (which then had unlogged access).

alter unsigned code downloaded to badge controllers (stored on the UNIX host).

Disable the logging/history mechanism, remove or alter log records in the database.

Sensors and alarms

- When is sensed movement in a protected area an alarm event? One solution is forcing everybody to badge in and out, and reference-counting the occupants. When the count is 0, nothing should be moving.

But alarms are usually dis-integrated from badge systems, which makes this difficult to impossible.

- Sensors can sometimes be activated from outside the protected area. This can be used to cause false “request to exit” events or nuisance alarm conditions. (False alarms are a social engineering opportunity).
- Sensors are wired to their control elements in primitive ways (usually a closed loop).
- Battery-powered Wireless sensors. Think “garage door opener” technology. Battery consumption has traditionally been more important than security.

Video

- Cheap USB- or net-connected digital motion-detect video compensates for a wide variety of sins, (or the temptation to sin by unknown third parties).
- Video can go almost anywhere these days, in things that look like or started life as floodlights, smoke detectors, clocks, pagers, or eyeglasses.

But…

You need to provide adequate coverage of asset areas (image size, illumination, numbers of cameras) and in the time domain, too.

You need random access and adequate retention to be able to follow up..

You need to carefully control access to the stored video.

Bad guys can make use of video also!

A colocation case study

- Very large facility with “vaults”, cages, and cabinets on a raised floor.
- Common data wiring is in conduits overhead. Raised floor is plenum for cool air and power. (Heat is not your friend.)
- Facility issued their own anonymous looking prox card credential.
- Cabinets with wafer locks in common areas (not even in cages)
- Cages had 5’ coarse mesh walls, video in some of the aisles, masterkeyed sliding doors, could be easily opened using several methods.
- “Vaults” had video pointed at the door, hand geometry readers for entry, electrified lock, a “door open” magnetic switch, a motion detector just inside the door.

Need some concept of Identity for most controls to work effectively

- Perhaps they need to know who you *really* are
- Or more likely just that you are the same person as registered before.
- Or, best of all, that you have particular roles or rights (the right to drive, or to drink, or to go into vault 203 unaccompanied.)

We have been conflating these aspects of identity, devaluing our identity documents by leaking stronger authenticators to counterparties even for low value transactions.

Is it better for your colo to accept your driver's license, to issue you their own credential containing a shared secret or to check your face in a database?

Events of a single month pointing to identity theft as a growth area

- Brooklyn, New York: busboy targets Fortune “400 richest”.

- Verisign issues two Class 3 code signing certificates in the name of Microsoft Corporation (perhaps to a Brooklyn busboy.)
- US General Accounting Office reports assault weapons and ammunition easily obtainable using phony driver’s licenses (GAO Report 01-427)

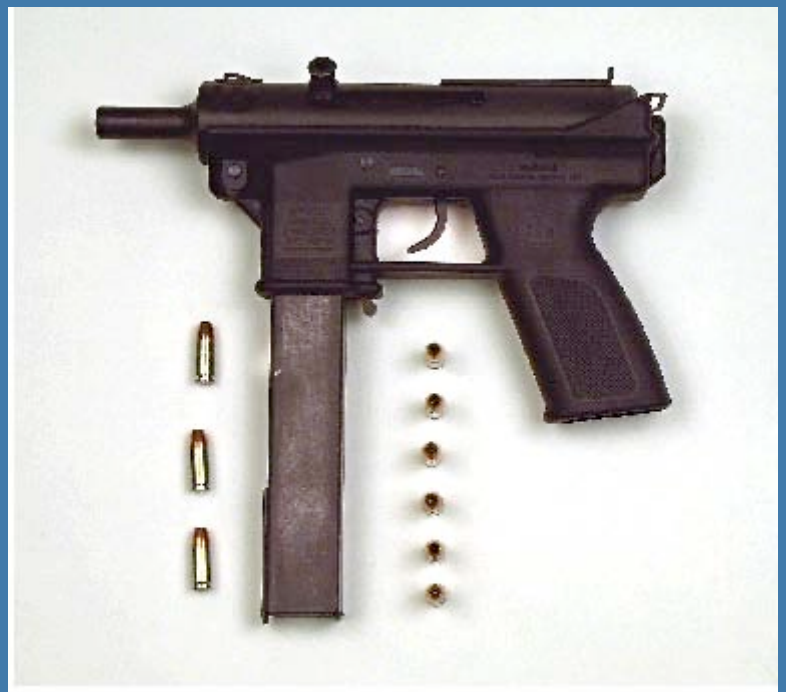
A system that keeps honest people honest?

9. CERTIFICATION OF TRANSFEREE *(Buyer)* - Questions a. through l. must be answered with a "yes" or a "no" in the box at the right of the question.

a. Are you the actual buyer of the firearm indicated on this form? If you answer "no" to this question the dealer cannot transfer the firearm to you. *(See Important Notice 1.)*		g. Have you been discharged from the Armed Forces under **dishonorable** conditions?	
b. Are you under indictment or information in any court for a crime for which the judge could imprison you for more than one year? An information is a formal accusation of a crime made by a prosecuting attorney.		h. Are you an alien **illegally** in the United States?	
c. Have you been convicted in any court of a crime for which the judge could have imprisoned you for more than one year, even if the judge actually gave you a shorter sentence? *(See Important Notice 5 and EXCEPTION.)*		i. Have you ever renounced your United States citizenship?	
d. Are you a **fugitive** from justice?		j. Are you subject to a court order restraining you from , harassing, stalking, or threatening an intimate partner or child of such partner? *(See Important Notice 6 and Definition 4.)*	
e. Are you an unlawful user of, or addicted to, marijuana, or any depressant, stimulant, or narcotic drug, or any other controlled substance?		k. Have you been convicted in any court of a misdemeanor crime of domestic violence? This includes any misdemeanor conviction involving the use or attempted use of physical force committed by a current or former spouse, parent, or guardian of the victim or by a person with a similar relationship with the victim. *(See Definition 5.)*	
f. Have you ever been adjudicated mentally defective or have you been committed to a mental institution?		l. Are you a citizen of the United States?	

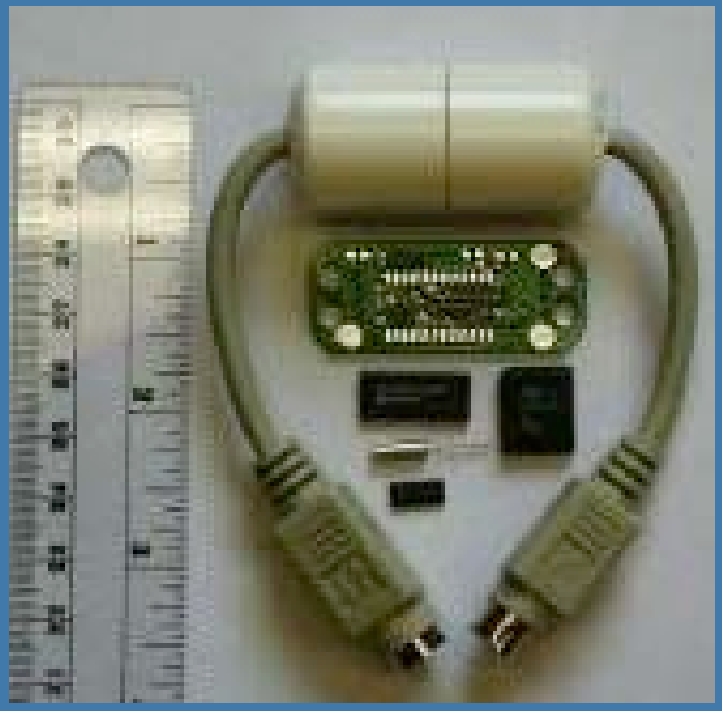
Everything you need to create identity is available on Ebay!

Santa Fe, New Mexico Purchase



Model AB-10 Intratec 9mm Semiautomatic Pistol With 32-Shot Magazine and 9mm 124-Grain Hydra-Shok Jacketed Hollow-Point Ammunition

While we're showing scary devices



We knew about electromagnetic emanations

But what about acoustic emanations?

Dot matrix printers

Keyboards, telephone keypads, ATM Pin Pads

Dmitri Asonov, Rakesh Agrawal:

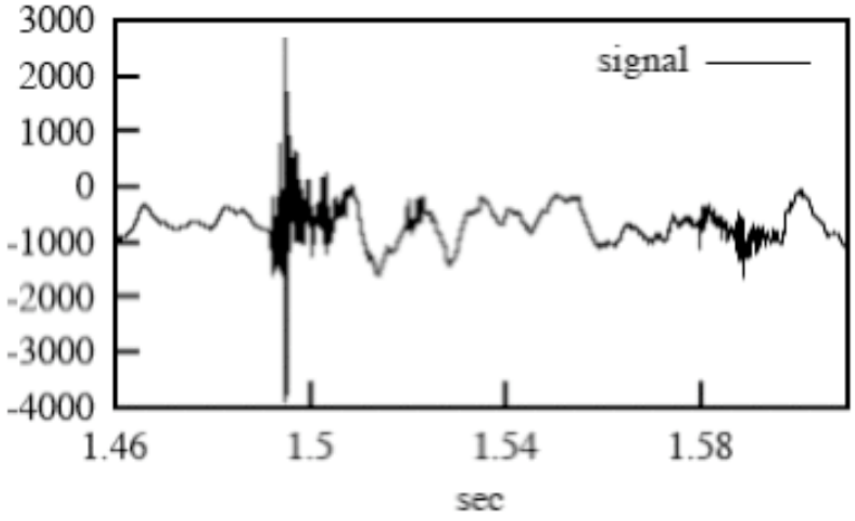


Figure 1. The acoustic signal of one click.

Feature extraction from the acoustic signal

Trained a neural network…

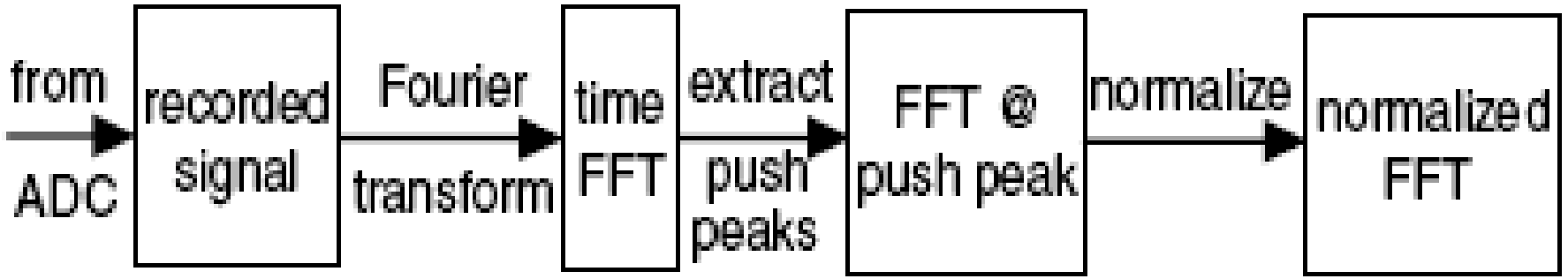


Figure 4. Feature extraction.

Asonov and Agrawal's interesting findings

- Average Depth of Correct Symbol (for 30 keys) is 1.99. (9,0,0) means neural network output this key 9 times as first choice, 0 times as second choice, 0 times as third choice. The same keyboard was used for training and testing.

Keyboard A, ADCS: 1.99						
key pressed	q	w	e	r	t	y
recognized	9,0,0	9,1,0	1,1,1	8,1,0	10,0,0	7,1,0
key pressed	u	i	o	p	a	s
recognized	7,0,2	8,1,0	4,4,1	9,1,0	6,0,0	9,0,0
key pressed	d	f	g	h	j	k
recognized	8,1,0	2,1,1	9,1,0	8,1,0	8,0,0	8,0,0
key pressed	l	;	z	x	c	v
recognized	9,1,0	10,0,0	9,1,0	10,0,0	10,0,0	9,0,1
key pressed	b	n	m	,	.	/
recognized	10,0,0	9,1,0	9,1,0	6,1,0	8,1,0	8,1,0

Table 2. The neural network is tested with 300 clicks, 10 clicks per key.

…

- Asonov and Agrawal also have less dramatically demonstrated successful acoustic recognition of ATM PIN pads and telephone keypads.

What solutions?

Don’t use keyboards with acoustic outputs during PIN or password entry (one patent they cite suggests eyetracking is a good solution).

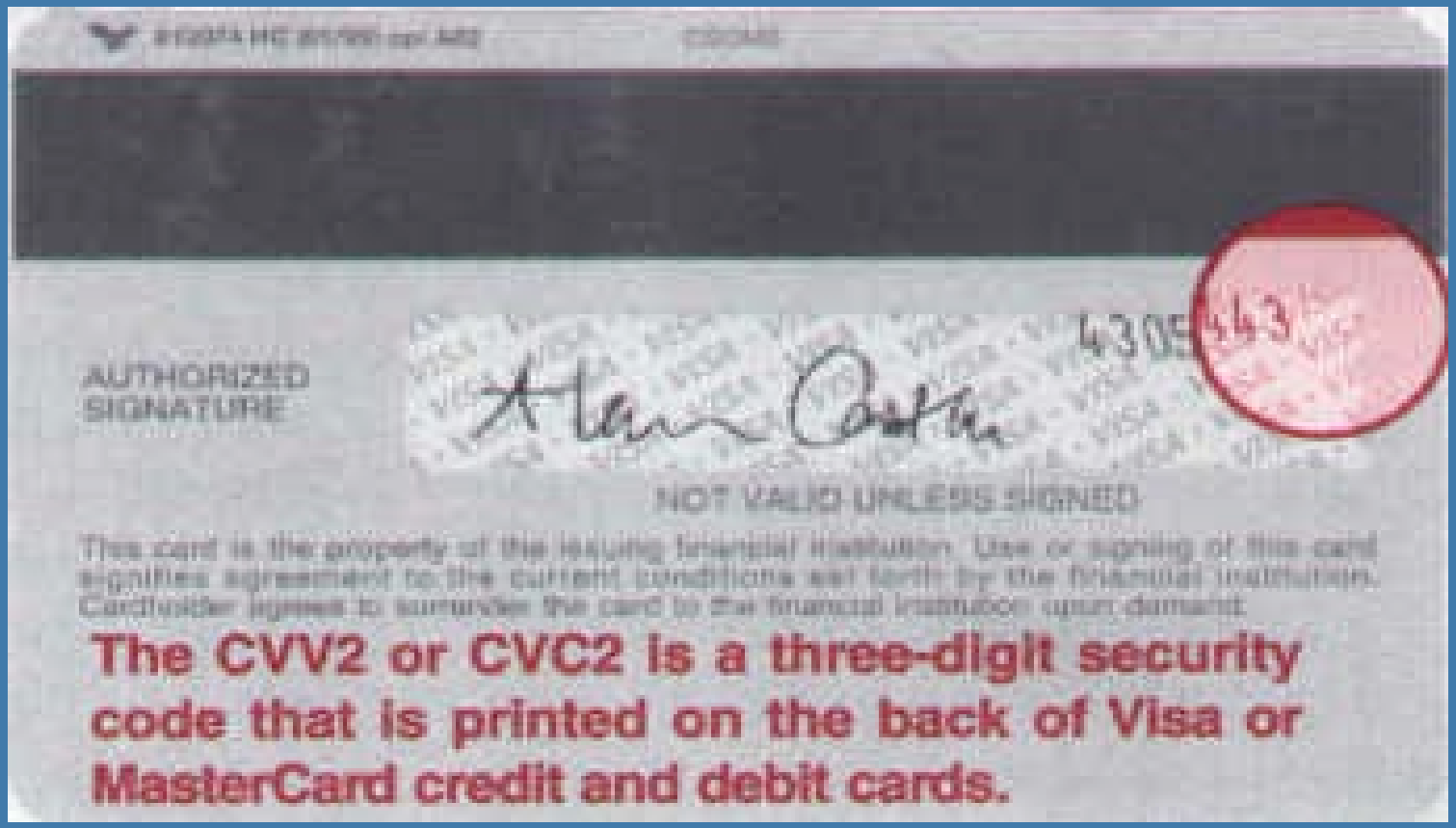
Mute telephone microphones during such entry.

Don’t use passwords at all (although replay attacks are still problem with tokens.

Unauthorized 802.11 bridges are pretty scary also.

- They can (lightly) encrypt and leak your traffic outside your building
- They're cheap
- They require only brief access for bad guys to install them

Problems with Credit and Debit Cards



Systems of all sorts are decreasingly

- Designed
- Built by people who truly understand their behavior
- Deployed by such people
- Tested

This is as true for security systems as for the buggy applications we are in such a hurry to expose to our customers.

Scary trends

- All your secrets on your laptop
- Or maybe: all your secrets on your Palm Pilot
- Or maybe: all your secrets on your converged wireless phone/palm pilot/remote control/electronic wallet (“trust us, it works”)

Vendors are often in league with the devil

"In memory of Ellen Shannon Aged 26 Years

Who was fatally burned March 21st 1870

By the explosion of a lamp filled with R.E. Danforth's

Non Explosive Burning Fluid"

-- tombstone epitaph, Girard PA.

Contractually require audits, independent design and code reviews, employee security as rigorous as your own, and prompt disclosure of all flaws in products and services.

“She blinded me with science”

But do you really think science will protect you?

The “people problems” are most difficult:

- Social engineering
- Passwords
- Trust of insiders
- The building master hidden in the coffee cup of the facility manager who was too low status to have a locked office
- People resist heavy-handed authority
- People will cover up even the most severe incidents. For example, the loss of a complete set of keys.

Some rules of thumb to avoid "physical security hell"

Just as in information security:

- You need to understand your business assets and plausible threats to them
- The risks are yours, and (no matter what) it's your reputation on the line, even if you can shift the formal liability elsewhere
- It's usually cheaper to create compensating controls to *detect* problems than to *prevent* them in the first place. This is where a bit of obscurity can add value.
- You need to put some policy and process in place and verify that the policies are dynamic, culturally appropriate, and reasonable.

…

- Design and architecture are very important, and you can't do them economically late in the game, even less so when bricks and mortar are involved.
- "God is in the details" – put someone on your side who really understands them and who can help you keep things clean.
- Audit your vendors. Test the locks. Test the manual procedures. If you want to be considered a good guy by your vendors, hire a consultant to act like a bad guy and to provide plausible deniability.

...

- A healthy level of paranoia can be a good thing.

For many things “trust but verify” is a good practice. This means *independent* verification rather than relying on vendor representations or self-certification.

Use secret-sharing or other multiple-custody protocols for key installation.

- Know who you’re trusting.

Pre-employment background and credit checks for sensitive employees including those at your vendors.

"Knowing is not enough; we must apply.

Willing is not enough; we must do."

-- Goethe (1749-1832)

References

- "I can copy a proximity card at least as easily as I can take an impression of a key." -- Jonathan Westhues http://cryolite.ath.cx/perl/skin/prox
- Keyboard Acoustic Emanations (Dmitri Asonov, Rakesh Agrawal)

www.almaden.ibm.com/software/quest/Publications/papers/ssp04.pdf

Matt Blaze on makins Masterkeys: www.crypto.com/masterkey.html

And on safe cracking: www.crypto.com/papers/safelocks.pdf

Securitech Gallery of {illegal, badly locked doors} off www.securitech.com

Questions: Now or later to m@seiden.com

(and thanks for listening)

Barry Wels references

- Opening locks by bumping paper:

Wwwtoool.nl/bumping.pdf

Winkhaus press release responding to vulnerability disclosure

www.winkhaus.de/presseframe/files/041014_Statement_Presse_BlueChip.doc