

---

# Protecting the Client

- Clients of networked applications
- Smart cards
- DRM

---

## Network Clients

- Thus far, we've focused on servers — network apps and privilege programs
- Do clients have the same risks?
- Yes — in some ways, more...

---

## Clients at Less Risk

- You can send arbitrary text to a web server
- To attack a web browser, you have to lure them there
- Email can be sent to anyone — and it can contain links to web servers
- Other apps are harder to attack

---

## Email and the Web

- Most mailers do not do their own HTML processing (at least not for full HTML)
- They have some way of invoking the standard browser's rendering engine
- Example: the Eudora mailer suffered from an Internet Explorer flaw (`http://email.about.com/cs/eudoratips/qt/et122001.htm`)
- Mozilla provides the *Gecko* rendering engine
- Active content — Java, Javascript, ActiveX, Flash, and the like — make life *much* harder (but we'll cover that later in the semester)

---

## Other Applications

- *Any* program, including network clients, can have security flaws
- Buffer overflows and the like abound
- If someone using the application connects to your server — or if you can trick someone into connecting to your server — you can compromise their machine
- Client software is often updated *less* frequently
- Rarely run on dedicated machines

---

## The Enemy Has Your Device

- Normally, you own your machine
- What if the enemy owns it?
- What if your enemy is *supposed* to own it?
- Who'd do that? Lots of people. . .

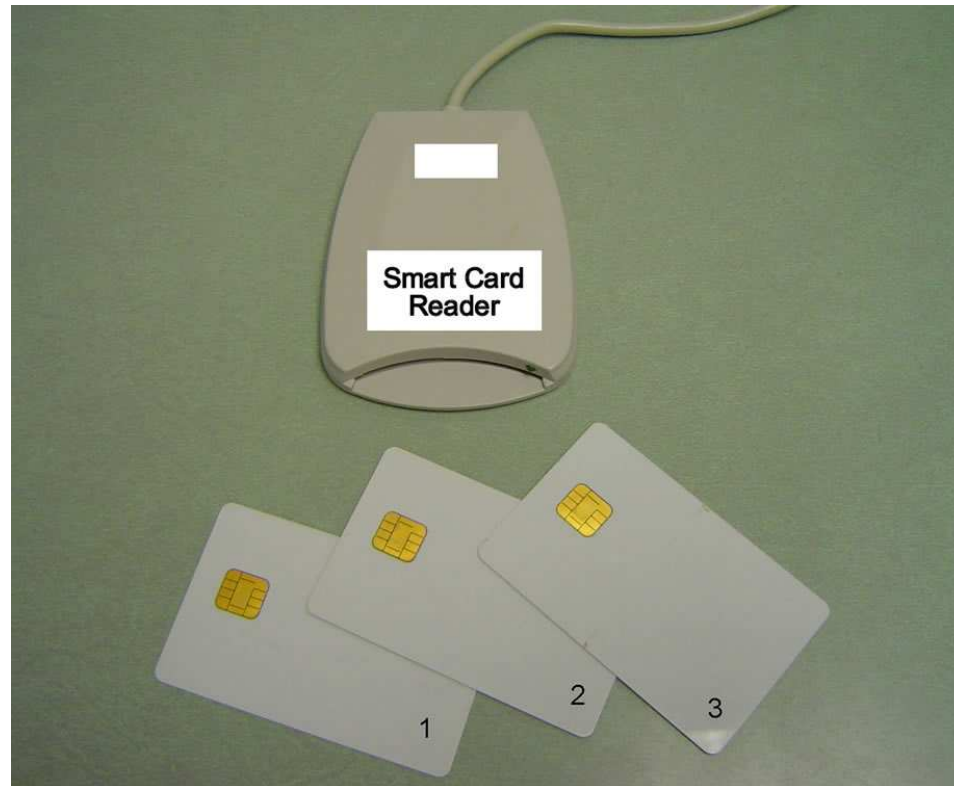
---

# Smart Cards

- Often in credit card form factor
- Contains small CPU and non-volatile storage (some contain RSA accelerator chip)
- Used for many purposes

---

## Reader and Smart Cards



These cards use contacts for power and I/O. Other types use inductive coupling or radio.



---

## Uses of Smart Cards

- Money or equivalent (transit fares, parking meters, vending machines, etc.)
- Counterfeit resistance (credit cards, especially in Europe)
- “Something you have” for authentication
- Pay TV or satellite/cable box

---

## The Enemy's Goals

- In stored value systems, the attacker wants to add more money to the card
- Alternatively, the attacker wants to extract the secret, to permit counterfeiting of more cards
- If an authentication token is locked by a PIN, the attacker wants to discover or replace the PIN

---

# Attack Techniques

- Software
- Physical

---

## Software Attacks on Smart Cards

- The card is running software and talking to the outside world
- Can you launch a buffer overflow attack?
- Is that software vulnerable to the usual attacks?
- In principle, any attack that works against other systems can work here

---

# Physical Attacks

- An attacker can manipulate the physical environment
- An attacker can monitor the physical behavior
- An attacker can try to reverse-engineer the chip

---

## Differential Power Analysis

- When a transistor switches on, it allows current flow
- The power difference between “on” and “off” can be measured
- Measure the instantaneous power consumption of the smart card
- Repeat this for a moderately large number of operations
- Statistical analysis will reveal the value of the cryptographic key at different points

---

# Fault Injection

- Certain stresses can cause erroneous computations
- It's practical to use heat or radiation to confuse a CPU or memory
- It has been demonstrated, theoretically and practically, that this can be used to break security
- Other techniques: controlling power

---

# Reverse Engineering

- With suitable tools, it's possible to reverse-engineer a CPU and read the memory
- Techniques include microtomes, scanning electron microscopes, and the like
- Separate set of physical-layer defenses



---

## Chipworks.com's Self-Description

“Chipworks provides microprobing, a type of reverse engineering, as part of our complete portfolio of patent and competitive intelligence services. Microprobing is an analytical technique used to achieve electrical contact with, or access to, a point in the active circuitry of a die using a special piece of equipment called a “microprobing station”. Microprobing lets us selectively inject probes into a device’s internal nodes and measure real time waveforms, currents and voltages which is critical for identifying specific functions that occur under specific conditions.”

---

## Protecting Chips

- Use of “non-metallic links” for device programming
- Ghost logic — fake logic elements to complicate the analysis
- False heat dissipation
- Extra metal layers

---

## Satellite and Premium Cable TV

- *Very* sophisticated enemies
- General attack
  - Sell counterfeit descrambler boxes
  - Buy legitimate access card
  - Extract key from card
  - Distribute keys over the Internet

---

## Where is the Value?

- Is the value on the card or in some database?
- If the value is in the card, must take precautions against counterfeiting
- If the value is in the database, the card is a just a pointer; security features in the card protect against theft, not value loss

---

## MTA Metrocard



Primarily an online system; central database has authoritative card value. Some offline use for buses. No protection against theft.

---

## Washington, D.C., Farecard



Note that the card itself knows its value. No protection against theft or counterfeiting.

---

## The CU ID Card

- The mag stripe and bar code are primarily database indices
- (The mag stripe actually contains more data)
- If the card is reissued, a new database index is assigned

---

## Mag Stripe Cards

- Two or three tracks; standardized format
- CUID has social security number plus other fields:

track 1: error: e5

track 2: <2118713710312940>

track 3: error: e5

- My Amtrak card:

track 1: <AGR^STEVEN^BELLOVIN^PLUS>

track 2: <20070228=5081653010>

track 3: error: e5



---

# Digital Rights Management

- Allow publisher to control use of content
- Prevent arbitrary redistribution of copyrighted materials
- Change sales terms from *physical purchase* to *license*

---

## General Approaches

- Restrict consumer's ability to use the material
- Trace usage (often via “watermarking”)

---

## Restricting Use

- Preferred approach of content providers
- Used by most (legitimate) vendors of digital music and films
- Many different types, implementing many different policies

---

## Apple's iTunes

- “personal, noncommercial use”
- “five Apple-authorized devices at any time”
- “shall not be entitled to burn Video Products”
- “burn an audio playlist up to seven times”
- (`http://www.apple.com/support/itunes/legal/terms.html`)

---

## Microsoft's Media DRM

- Media files are encrypted, and contain pointer to license source
- User obtains license from clearing house
- License includes terms and conditions as well as decryption key
- “Licenses can have different rights, such as start times and dates, duration, and counted operations.”
- “may allow the consumer to . . . copy the file to a portable device”
- “Licenses, however, are not transferable.”
- (<http://www.microsoft.com/windows/windowsmedia/howto/articles/drmarchitecture.aspx>)

---

## How Does It Work?

- Operating system mediates access to files
- Operating system enforces rules imposed by the content provider
- Ordinary OS protection mechanisms isolate the unprotected content from the user
- Or do they?

---

## The User Versus the OS

- If you own the computer, you're the administrator; you have root privileges
- The vendors' challenge: protecting content against the superuser
- Several different approaches

---

# Approaches

- Obscurity — make it hard to find the plaintext
- Obfuscation — confuse the code to make reverse-engineering harder
- End-to-end crypto — do decryption on the sound card or video card.  
(But what about the “analog hole”?)
- Trusted hardware



---

## Trusted Hardware

- Ultimately, all software-only schemes are futile
- You can always trace the code, patch modules, etc
- But — other software can attempt to detect such “attacks”, and disable playback
- See above
- The *only* reliable solution is trusted hardware
- Manage the keys and the decryption outside of the OS
- As needed, use tamper-resistance techniques for such hardware

---

# Watermarking

- Tag files with owner and/or licensee information
- Tags should be invisible in normal use of the file
- Tags should resist detection and deletion
- In practice, this has proved to be extremely difficult to accomplish

---

## Defeating Watermarking

- Pictures: scaling, clipping, color balance, rotation, geometric distortion, printing/scanning
- Sound: Fourier transforms
- Thus far, the attackers are winning

---

## Legal Issues

- The law in the US and other countries outlaws “circumvention technology”
- Lawsuits and threats of lawsuits have blocked some work
- A lot of other stuff is out there, including both academic research and practical tools (i.e., dcss)
- Crucial philosophical issue: do DRM schemes give content owners more power than copyright law would?

---

## Current State of Affairs

- Technical measures are good enough that they're not the weak point
- CD/DVD ripping plus redistribution is easier than cracking DRM schemes
- That said, many DRM schemes have been cracked
- Two-fold attack by content owners: technical measures and lawsuits