University of Illinois at Urbana-Champaign
Dept. of Electrical and Computer Engineering

ECE 101: Exploring Digital Information Technologies

Authentication and Physical Security

Online Security: Authentication

Reliably Identifying an Entity

Authentication: the process or action of verifying the identity of a user or process.

By extension, the process to associate a computer program with a person or a company (an entity)

Example: Usernames and Passwords

When authenticating a user, a machine or a website compares the password entered by the user with the one that it already knows.

Problems with Password Storage

- Many early systems (and, unfortunately, some to this day) kept the passwords for all of their accounts in a "password file" that contained the passwords in clear text.
- Normally, by design, the password storage would only be accessed by an administrator user (root, admin, superuser) and operating system utilities.
- But under unusual circumstances, caused by software implementation errors or deliberate misuse, the contents of the password storage file almost inevitably can become available to adversaries.

Encryption

- **Encryption** is the process of encoding information.
- Encryption is part of the broader field of **Cryptography**, which is the **practice and study of techniques for secure communication** i.e. communication in the presence of an adversary.
- Today, cryptography is used as a tool for informatics, business, finance, politics, human rights—any sector that deals with **personal information** or requires communication.

Encrypted Passwords

Since storing passwords in the clear has clearly proven itself to be a bad idea, one option was to store passwords in an encrypted form instead—store them in a coded form.

Encryption beyond Passwords

There is always someone malicious to listen in on your conversation …

- Modern communications, especially the Internet, operate under the assumption that the world is hostile and for anything you say there is always someone malicious to listen
- Same reason why people would put handwritten letters in an envelope before sending, but scaled for billions of people and devices.
- Cryptography, in turn, is one of the major instruments in the arsenal o information security, a digital protective envelope for communications.

Secure Communication

- Today people are used to most of their connections to the web being secure, but that was not always the case.
- HTTP (Hypertext Transfer Protocol), the foundation of data communication over the World Wide Web (WWW), is plaintext.
- All of the data in HTTP requests and responses is sent in the clear, under a risk of all sorts of intrusions and fraud.
- Providing security of communication over computer networks is the continuing challenge.
- Cryptography influences all sorts of daily business.

How can Cryptography Help?

Cryptography has grown to be not only about encryption anymore, but includes a group of special-purpose algorithms to sustain the wider infrastructure of information security, such as:

- user and message authentication,
- protection from illegitimate changes to messages,
- protection from eavesdropping, etc.

Beyond the Algorithms: Something to Note

Security of communications **cannot be achieved solely by developing mathematical algorithms and protocols**. Strong cryptography is necessary for secure communications, but not sufficient. Reliable security of information goes beyond cryptography alone. It also requires **carefully planned procedures, operation and establishment of laws**.

Cryptography is a powerful tool that needs to be utilized properly. A tough bank vault will not protect the gold inside if the lock combination is written on a sticky note next to it. Like seat belts, cryptography will not completely protect us, but is indispensable nevertheless. **Many systems fail because they were designed to protect the wrong things—or the right things, but in the wrong way**.

Physical Security

Humans: When Do You Need Help?

When these images appear on your home camera, do you call the police?



Never?

That's not my cat! Always?

Security: Determining Whether Our Property is in Danger

(physical) security:
How can I **decide whether my home** (for example) **is in danger?**

Role of Computing in Security

- improves and coordinates sensors
- learns habits and preferences
- mimics human presence
- integrates with personal computing
- preserves data

The Security Company Business Model

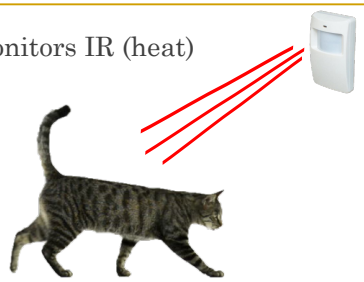
In return for purchase and installation costs and a monthly service fee, **home security firms offered**…

- an **array of sensors** to detect intrusion,
- **centralized control** with a PIN to turn the alarm system on and off,
- **remote 24/7 human oversight** to minimize false positives
- **automatic notification** of both emergency services (police/fire) as well as the homeowner

They could also help with timer-based **control of lights and sounds** within the home to trick an observer into thinking that someone was in the home.

Historical Motion Sensing

Passive sensor monitors IR (heat) in field of view.



Rapid changes register as "motion."

Historical Sensing of Perimeter State

When doors are closed, electrical current flows across connection made between edges of doors (red line).

When a door opens, the circuit breaks (black line), detecting the change.

Historical Sensing of Broken Glass

A similar approach, involving a thin strip of foil, was used to detect broken windows.

When a window is broken, the foil tears, breaking the circuit.

Historical Signage to Discourage Intrusion

Companies provided signs to warn potential intruders that a building was under 24/7 surveillance.

Generally, they didn't explain why such tactics can be effective.

Sensing and Processing Have Advanced Dramatically

How does ubiquitous computing change this business?

Let's start with sensors.

Semiconductor optics technology has enabled **high-resolution, low-power cameras**.

Powerful **image processing**
- can now be applied to sensor output
- in conjunction with other sensor data (called **sensor fusion**).

Audio and Other Sensing Technologies Also Useful

Audio processing
- can also be **much more sophisticated**,
- thanks to improvements in computation power (per dollar).
- Now we **can "hear" glass breaking** instead of checking every pane in the house.

Other **sensing media**
- useful for **identify**ing and differentiating **human occupants and pets** from intruders,
- including radio, IR, and visible light.

Not my cat!

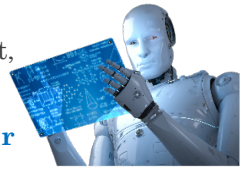
Also not my cat!

(I don't own a cat.)

Many More Advances as Well

Computation has also enabled other improvements:

- **automated mapping** of home environment,
- **understanding habits** and personal preferences
- control systems to **mimic normal behavior**
- **integration with personal computing** (wifi, mobile phones)
- **preservation of data** (protected in tamperproof storage and in the cloud)



Let's Imagine a Future Scenario…

Imagine a future scenario. Here's the security log:

2022-02-14 10:32:04 UPS van stopped in front of house.

2022-02-14 10:32:05 No UPS delivery expected from transaction history.

2022-02-14 10:32:05 Entering threat level yellow.

2022-02-14 10:32:13 UPS driver does not match usual UPS delivery person.

2022-02-14 10:32:16 UPS driver not found in UPS driver database. Suspect visual recorded.

2022-02-14 10:32:16 Entering threat level orange.

Log from Future Security Incident (continued)

2022-02-14 10:32:33 Suspect is carrying envelope.

2022-02-14 10:32:42 Suspect deposited envelope in own pocket.

2022-02-14 10:32:55 Suspect moving to back of house.

2022-02-14 10:33:07 Suspect peering into windows.

[[PRIVATE LOG: 2022-02-14 10:33:10 Suspect identified as Danny Ocean. Initiating framing. Breaking window.]]

2022-02-14 10:33:12 Broken glass detected near suspect.

2022-02-14 10:33:12 Entering threat level red. Notifying local police.

Your luck is up, Ocean!

Where's the Computing?

Imagine a scenario. Here's the security log

2022-02-14 10:32:04 UPS van stopped in front of house.

2022-02-14 10:32:05 No UPS delivery expected from transaction history.

2022-02-14 10:32:05 Entering threat level yellow.

2022-02-14 10:32:13 UPS driver does not match usual UPS delivery person.

2022-02-14 10:32:16 UPS driver not found in UPS driver database. Suspect visual recorded.

2022-02-14 10:32:16 Entering threat level oran

video analysis detects and recognizes delivery vehicle

integration with email and browser action analysis

local history recorded by security devices

future service provided by UPS

And More Computation…

2022-02-14 10:32:33 Suspect is carrying envelope.

2022-02-14 10:32:42 Suspect deposited envelope in own pocket.

2022-02-14 10:32:55 Suspect moving to back of house.

2022-02-14 10:33:07 Suspect peering into windows.

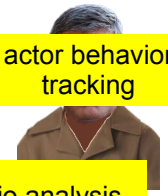
[[PRIVATE LOG: 2022-02-14 10:33:10 Suspect identified as Danny Ocean. Initiating framing. Breaking window.]]

2022-02-14 10:33:12 Bre glass detected near susp

2022-02-14 10:33:12 Ente g threat level red. Notify local police

Your luck is up, Ocean!

additional, advanced video analysis [extra cost!]



actor behavior tracking

audio analysis

personalized hacking (optional)

But Do We Still Need Security Companies?

But **detection technologies**—
- even whole "home security" packages—
- **are readily available in stores**.

Given the ubiquity
- of sensors, wifi, mobile phones,
- why do companies like ADT still exist?

Can't you just put a system together yourself?

Don't many people already do so?

Evolution of the Sales Pitch

A home security system
- also monitors your home
- when you're at home.

What if someone breaks in and attacks you?

What if a stray / wild animal gets in?

Not Everyone Wants to Do It Themselves

Being able
- to **differentiate** these situations
- **from your throwing a party** may be difficult.

Security companies
- **have the most data**
- as well as humans online 24/7
- to make the right call.

That may be nicer than having your security system call the cops to bust up your party…

Evolution of the Sales Pitch

So the pitch is still relevant.

These companies provide

- **expert integrators**—avoid human error in integrating devices and software, and
- **expert overseers**—humans (or ML systems, or both) monitor actual events before reporting, without involving the homeowner.

And of course there's still the **signage**…

Added Bonus: New Markets!

Modern **infrastructure**

- also **extends easily** to home monitoring
- **when residents themselves need monitoring**.

So what?

Senior citizens living alone may benefit from monitoring!

Added Bonus: New Markets!

Support for senior citizens:

- **portable button and voice-controlled access** to children and/or local caregivers,
- automatic **detection of emergency** health **situations**,
- **continuous monitoring of health** indicators
- **integration with medical device** measurements (ex: blood sugar for diabetic patients)