COMPUTER SECURITY

Security Principles

Topics for today

- Adopting good security principles

Users are a factor

- Usability is an important aspect in system design
- Neglecting to design and test for usability is likely to result in user error
  - Often usability is neglected during design time
  - Different people have different technical capabilities
    - Design for different users in mind

https://www.iconfinder.com/icons/329331/computer_group_laptop_people_team_user_users_icon

Why Johnny can’t encrypt

- Whitten and Tygar, 1999

https://www.smartdatacollective.com/5-advantages-using-encryption-technology-data-protection/

Research Question

- Suppose an average user of email feels the need for privacy and authentication
- Acquires PGP with that purpose in mind
- Will PGP's current design allow that person to realize what needs to be done?
- Can he figure out how to do it?
  - Avoiding dangerous errors?
  - Avoid becoming frustrated?
    - Such that he or she decides to give up on using PGP after all?

Research Observations

- Average people never acquired PGP with that intent
- Did not discover the encryption and authentication features baked into Outlook
- Users were never introduced to the underlying concepts
-

- https://www.wired.com/insights/2012/10/why-johnny-cant-syndicate/

PGP Usability Research

- Evaluate whether PGP 5.0v can be used successfully
  - by cryptography novices to achieve effective electronic mail security.
- Found a number of user interface design
  - may contribute to security failures,
- Test participants were given 90 minutes in which to sign and encrypt a message using PGP 5.0
  - the majority of them were unable to do so successfully

Conclusion

- Introducing PGP to average users may take a long time
- Require a lot of education
  - to add the concepts that underly privacy and authentication
-

- https://www.wired.com/insights/2012/10/why-johnny-cant-syndicate/

Why Johnny can’t encrypt

- Original paper written in 1999
- Many software updates were performed since then
- What is the current state?

Why Johnny can't encrypt

- Multiple papers followed
- "Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System" [Clark et. Al 2011]

Usability of PGP Client

Computer Science > Cryptography and Security

Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client

Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons

(Submitted on 29 Oct 2015 (v1), last revised 13 Jan 2016 (this version, v2))

This paper presents the results of a laboratory study involving Mailvelope, a modern PGP client that integrates tightly with existing webmail providers. In our study, we brought in pairs of participants and had them attempt to use Mailvelope to communicate with each other. Our results shown that more than a decade and a half after \textit{Why Johnny Can't Encrypt}, modern PGP tools are still unusable for the masses. We finish with a discussion of pain points encountered using Mailvelope, and discuss what might be done to address them in future PGP systems.

Usability of PGP Client

- Follow-up paper by Routi et a. [2015]
- Study participants asked to use Mailvelope to communicate with each other
- Main findings: modern PGP tools are still unusable for the masses
- Challenges encountered using Mailvelope
  - Paper proposes potential solutions address them in future PGP systems

SECURITY PRINCIPLES

Financial Considerations

- Cost/benefit analysis is part of risk management in security
  - Threat model first step in security analysis
- An attacker will allocate more resources against a valuable target

Prevention and Detection

- Prevention goal: stop a bad thing from happening
- Detection: see that something is going wrong
- Response: Do something about this
  - Response time critical for damage control

False Positives and False Negatives

- False positive:
  - An alert flag is raised without need
    - No risk, authorized user
- False negative:
  - No alert is raised even though an attack takes place
    - E.g., an unauthorized user is login into the system

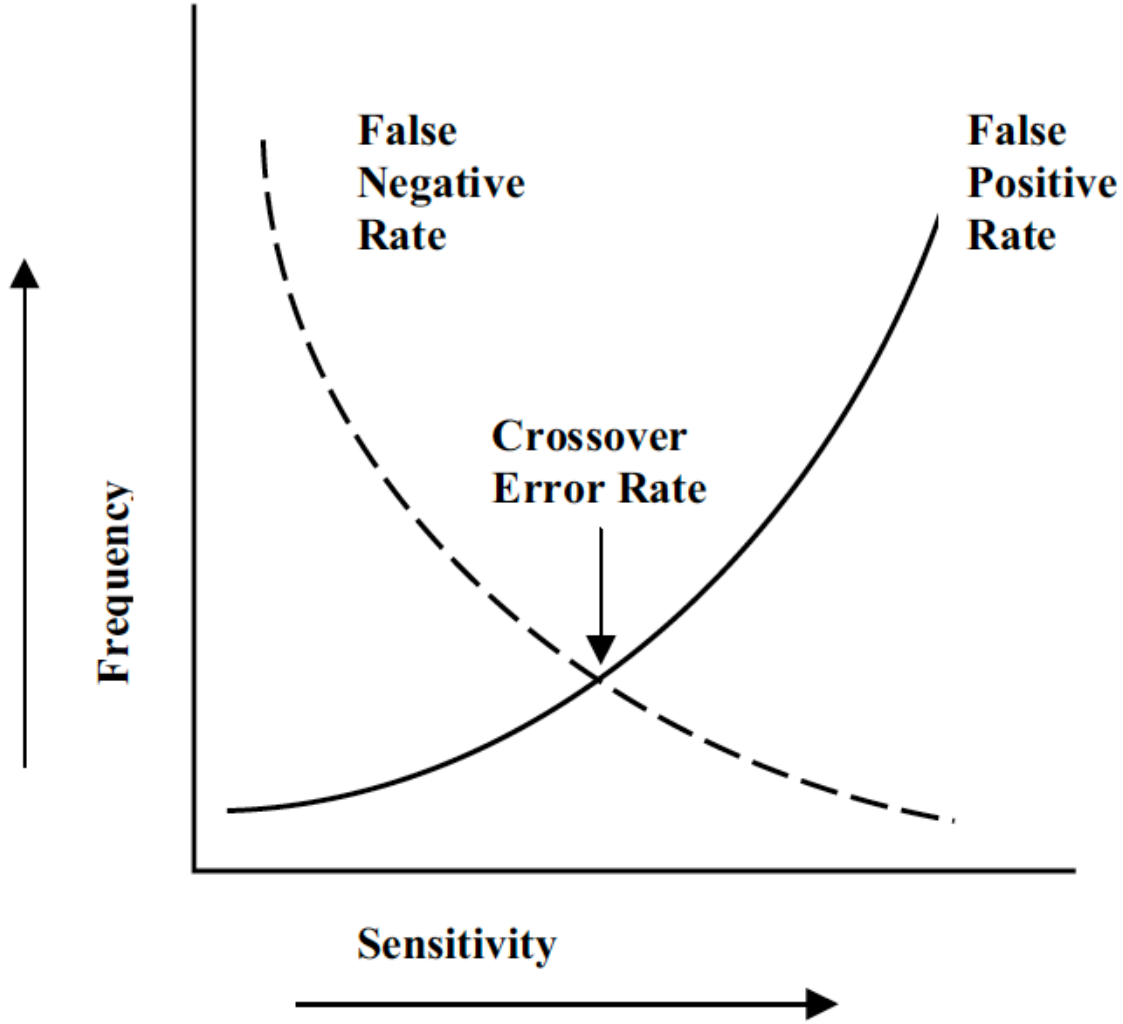
False Positives and False Negatives

- Trade-offs:
  - If too many false positives occur, usability is reduced
    - E.g., authorized user will fail login-in multiple times
  - False negative = security failure
    - Attacker not detected

False Positives and False Negatives

		Actual	
		Positive	Negative
Predicted	Positive	**True Positive**	**False Positive**
	Negative	**False Negative**	**True Negative**

Why is it a trade-off?



https://www.researchgate.net/publication/224386845_Optimal_combined_intrusion_detection_and_biometric-based_continuous_authentication_in_high_security_mobile_ad_hoc_networks/figures?lo=1

False Positives and False Negatives

- If system not sensitive enough:
  - False negatives occur
    - Threshold for raising a flag too high
- If system too sensitive:
  - False positive occur
    - Threshold for raising a flag too low
- How can we improve authentication

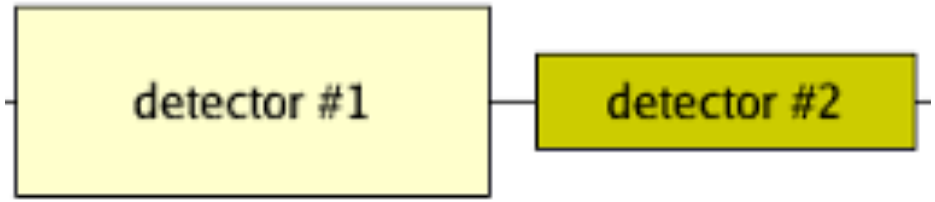
Multi-Layer Defense Approach

- Having multiple layers of defense
  - I.e., software, network defenses, etc.
- Advantages:
  - Different vulnerabilities require different defenses
  - Attacker will need to breach all defenses to mount a successful attack
- Disadvantages:
  - Most costly

Combining Multiple Detectors

- Detectors may be independent
  - In this case, analysis is easier
    - FP1 and FN1 false positive and negative for detector 1
    - FP2 and FN2 false positive and negative for detector 1

Detectors Mounted Serially



Combining Multiple Detectors

- Detectors may be independent
  - If we require alert from either detector to fail:
    - Detectors are mounted serially
    - Attacker has to pass both
    - $FN_{combined} = FN1 * FN2$

Combining Multiple Detectors – Parallel Detectors

- FN = Overall false negative
- TP = Overall true positive, attack failed

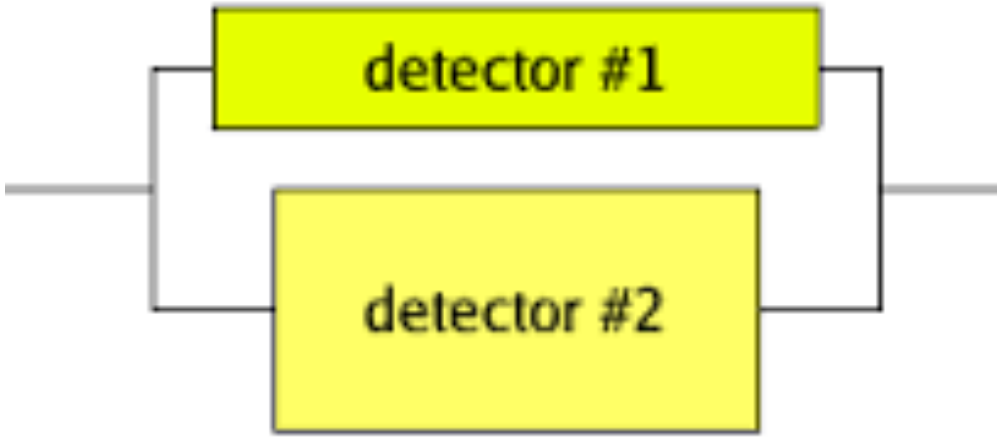
	#1 False N	#1 True P
#2 False N	?	?
#2 True P	?	?

Combining Multiple Detectors – Parallel Detectors

- FN = Overall false negative, attack succeeded
- TP = Overall true positive, attack failed

	#1 False N	#1 True P
#2 False N	FN	TP
#2 True P	TP	TP

Detectors Mounted in Parallel



Combining Multiple Detectors

- Detectors may be independent
  - If attacker needs to pass either detector, what is the combined false negative:
    - Detectors are mounted in parallel
    - Need alert from both detectors not to pass
    - $FN_{combined} = FN1 + (1 - FN1) * FN2$
      $= 1 - (1 - FN1) * (1 - FN2)$

Combining Multiple Detectors – Parallel Detectors

- FN = Overall false negative
- TP = Overall true positive, attack failed

	#1 False N	#1 True P
#2 False N	?	?
#2 True P	?	?

Combining Multiple Detectors – Parallel Detectors

- FN = Overall false negative
- TP = Overall true positive, attack failed

	#1 False N	#1 True P
#2 False N	FN	TN
#2 True P	TN	TP

Combining Multiple Detectors

- Detectors may be independent
  - If attacker needs to pass successfully either detector:
    - Detectors are mounted in parallel
    - $FN_{combined,parallel} = FN1 + FN2 * (1 - FN1)$
  - If we require alert from both detectors to fail:
    - Detectors are mounted serially
    - $FN_{combined,serial} = FN1 * FN2$

Combining Multiple Detectors

- Detectors may be independent
  - $FN_{combined,parallel} = FN1 + FN2 * (1 - FN1)$
  - $FN_{combined,serial} = FN1 * FN2$
  - Which False Negative probability is higher?
    - In parallel
      - Why?
        - Enough that one detector will fail
    - $FN_{combined,parallel} = FN_1 + FN_2 * (1 - FN_1) =$
      $= (FN_1 - FN_2)^2 + FN_1 * FN_2 >$
      $> FN_1 * FN_2 = FN_{combined,serial}$

PASSWORD AUTHENTICATION

Password Authentication

- Passwords have many inherent issues
- Stolen passwords lead to:
  - Identity theft
  - Financial damage to corporation
    - Cost of loosing business
    - Cost of resources to deal with clients
      - Hiring new employees, paying for free credit report for clients, etc.
    - Cost of restoring reputation

How hackers use your information for identity theft

August 20, 2017 • 6 min read

In a Nutshell

Hackers are getting more creative with how they use your information. From applying for credit cards in your name to stealing health insurance, the impact of identity theft has reached new heights.

https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information/

Password Authentication

- Passwords are hard to remember
  - Especially strong passwords
- Users have many accounts
- Users tend to reuse passwords
  - Consequence: security breach of one site causes account compromise on other sites

Password Authentication

- Some solutions:
  - Password managers
  - Two-factor authentication
    - What is the probability of failure?
      - Both factors need to fail to succeed
      - If independent:
        - $FN_{combined} = FN1 * FN2$
  - Combining both may results in stronger protection

ASSESSING SECURITY

Offline Security

- What is an off-line parallel to online security?
  - Safe
- What are the requirements from a safe?
  - Contents should be be inaccessible to an attacker

Safe Security Rating

- How do we rate security?
  - For safe = security rating
    - E.g., UL rating
  - Examples:
    - **TL-15:** The safe has been tested for a NET working time of 15 minutes to break into
      - using “common hand tools, drills, punches hammers, and pressure applying devices.”
    - **TL-30**: The same expert and tools now takes 30 minutes

1. B-RATED SAFES

B-rated safes (aka class b safes) include any safe which has walls that are at least a ¼-inch thick, and a door that is ½-inch thick. Additionally, b-rated safes must have some sort of locking device, such as a key lock or a wheel combination lock.

Class b safes are some of the cheapest options available on the market, and are most frequently used by businesses to protect small amounts of cash, or by individuals who are looking for an added layer of protection for their personal documents.

It's important to remember that any box with a lock on it that meets the thickness requirements stated above can be labeled a b-rated safe, and safes within this category are not required to undergo testing to receive this valuation. So, it is always advised that customers consider the type of locking device they will be getting, whether or not a relocker is present, and if the safe comes with a drill/ballistic resistant hard plate— all of which offer added protection.

HOTEL SAFE BEIGE-GREY MATT & SILVER

2. C-RATED SAFES

Class c safes, or c-rated safes, must have walls that are at least ½-inch thick and doors that are 1-inch thick— making them twice as heavy as their class b counterparts. They are similar, however, in the sense that they can come with a range of locking devices, from digital number pads to wheel combination locks and time locks.

Additionally, like b-rated safes, class c safes aren't subjected to formal written standards, meaning there are no specific criteria that manufactures must adhere to when building them.

This means that the quality and safety levels of class b safes and class c safes can vary, making it crucial for customers to do their research before making a purchase decision.

https://www.stockinger.com/en/blog/a-complete-guide-to-safe-ratings

Safe Ratings

B-Rate Safes

This is a catchall rating for essentially any box with a lock on it. The safe industry had an unwritten standard of 0.25 inch body, 0.5 inch door. No tests are given to provide this rating. When buying a B-rate safe, look at things such as lock work, hard plates, and relocks.

C-Rate Safes

This is defined as a 0.5 inch thick steel box with a 1-inch thick door and a lock. As before No tests are given to provide this rating. Look at the lock work, relocks and other features when making your decision.

TL-15

Safes given a U.L. TL-15 rating have all passed standardized tests defined in UL Standard 687 using the same tools and usually the same group of testing engineers. The label requires that the safe be constructed of 1-inch solid steel or equivalent. The label means that the safe has been tested for a NET working time of 15 minutes using “common hand tools, drills, punches hammers, and pressure applying devices.” Net working time means simply “when the tool comes off the safe the clock stops”. There are over fifty different types of attacks that can be used to gain entrance into the safe.

TL-30

These tests are essentially the same as the TL-15 tests except for, the net working time. They get 30 minutes and a few more tools to help them gain entrance.

Net Working Time

This is the UL term for testing time which is spent trying to break into a safe using tools such as diamond grinding wheels, high-speed drills with pressure applying devices, or common hand tools such as hammers, chisels, saws, and carbide-tip drills. If a safe has been rated with a 30-minute net working time, (TL30), the rating certifies that the safe successfully withstood a full 30 minutes of attack time with a range of tools.

https://www.nashvillesafehouse.com/faq/terminology/

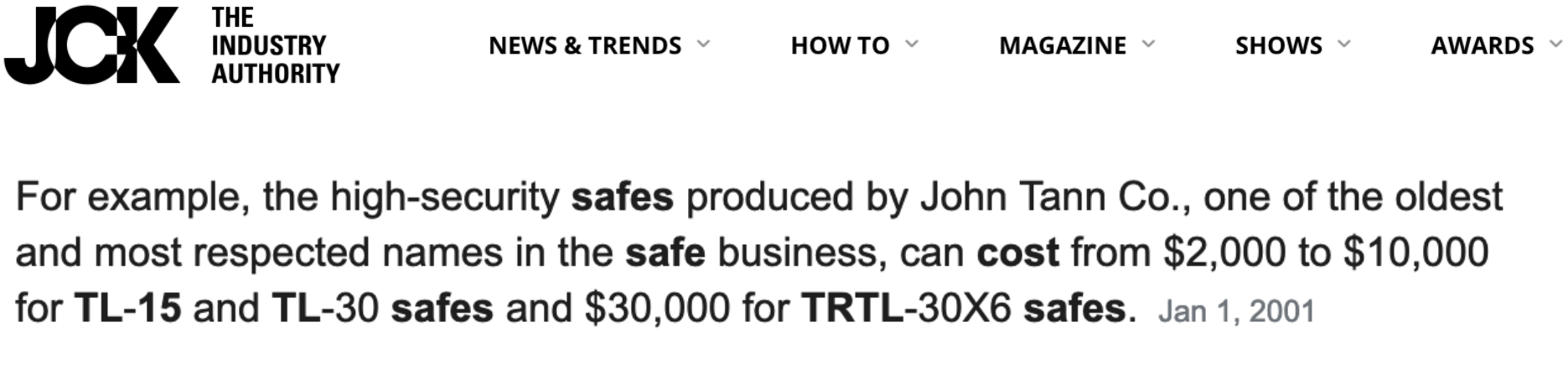
Safe Security Rating

- How do we rate security?
  - For safe = security rating
    - E.g., UL rating
  - Examples:
    - **TL-15:** The safe has been tested for a NET working time of 15 minutes to break into
      - using “common hand tools, drills, punches hammers, and pressure applying devices.”
    - **TL-30**: The same expert and tools now takes 30 minutes
  - What if we need a stronger guarantee?

Safe Security Rating

- How do we improve security?
  - Provide protection against stronger attackers
  - Examples:
    - **TRTL-15**: safe has been tested for a NET working time of 15 minutes
      - “with a torch and a range of tools which might include high speed drills and saws with carbide bits, pry bars, and other impact devices”
    - Provides stronger guarantees

Security Costs



https://www.jckonline.com/magazine-article/how-safe-is-your-safe/

Security Cost

- Security is about financial trade-offs
  - More security often means higher costs
  - Need to analyze and balance
    - Cost of security defenses vs. cost and probability of successful attack

Computer Security

- How do we rate security?
  - For safe = Rating of safe
  - How do we assess risk for computer system?
    - Harder to analyze
    - Create a good threat model
      - Who is the attacker, how many resources/time does he have?

DATA PRIVACY AND USABILITY

Privacy and Security

- Privacy is part of confidentiality
- How do we distinguish between privacy and security?

Privacy and Security

- ***Privacy*** relates to any rights you have to control your personal information and how it's used
  - For example, you're asked to read and agree to privacy policies when you download new smartphone apps.
- ***Information Security***, on the other hand, refers to how information is protected
- Your data may exist in a lot of places
  - That can challenge both your privacy and your security

Data Privacy and Usability

- License agreements are frequently written in legal language
  - Long and hard to understand
  - Users tend to accept
- Users do care about their privacy
- Privacy breaches may result in damage to users
- How do we improve programs?
  - To increase usability/privacy guarantees?

Data Privacy and Usability

- Many applications request a lot of privileges
  - Even without needing them for the explicit goal they are trying to achieve
    - May or may not use these privileges
- Principles of least privilege should be follows
  - E.g., why would an application request your location at all times?
    - Instead of just when using the application

ACCESS CONTROL

Least Privilege Principle

- When designing a new system, consider the needs of the system
  - Identify a Trusted Computing Base (TCB)

Trusted Computing Base (TCB)

- Every system has a TCB
- TCB requirements:
  - Needs to be correct
    - Implementation should achieve stated goals
  - Needs to be complete
    - Cannot be passed by an attacker
  - Can’t be tampered with
    - Attacker can not change it

TCB Design

- Principles:
  - Keep It Simple
    - Many times, Simple = Small
  - Follow privilege separation
    - Privileged operations should be implemented in small separate components

Operating System

- Operating system provides security guarantees to the system
  - Prevents processes against accessing memory of other processes
  - Responsible for access control
    - E.g., a process can change files only if he has the right permissions
    - Typically process permissions are the same as the user permissions
      - But it can be set to be different than the user permission

Operating System

- OS has a TCB
  - In an operating system, TCB would include the system files and processes in the underlying kernel

Complete Mediation

- To secure access, construct a ***Reference Monitor***
  - Monitors all access to system resources
  - Correct, tamper-proof, cannot be bypassed

Questions?