

Computer and Network Security

Lecture 01: Overview & Mindset

COMP-5370/6370





Security is an **enormous** field with many specializations, sub-fields, and communities.

- This is an **intro course** focused on exposure to the topics and gaining experience applying security-centric ideas.
- If you want to see how far the rabbit hole goes, there are follow-on courses.

Security Vocabulary is HARD



Security

Privacy

Resilience

Information Assurance

Risk Management

C---r + *any of above*

- Everyone has a specific definition for every word
 - Not all definitions agree
- Definitions change frequently and new words are constantly added to vocabulary

CompSci Security Vocab



“Attack”

Intentional exploitation for attacker’s gain and victim’s loss

“Bug”

Something that fails in unintended ways

“Weakness”

Bug that may be able to harm S&P

“Vulnerability”

Weakness which can be intentionally triggered

“Exploit”

Way to leverage a vulnerability

Security Mindset



- A way of thinking about scenarios in order to identify and mitigate possible failures.
- Come in many form and applicable outside of computers/networks

Failures Come in Many Forms



- Tacoma Narrows
 - Design Failure
 - Natural Forces

Failures Come in Many Forms



- Tacoma Narrows
 - Design Failure
 - Natural Forces
- Hard Rock Hotel
 - Process Failure
 - Unintentional Actor

Failures Come in Many Forms



- Tacoma Narrows
 - Design Failure
 - Natural Forces
- Hard Rock Hotel
 - Process Failure
 - Unintentional Actor
- World Trade Center
 - Intentional Failure
 - Intentional Actor

Failures Come in Many Forms



- Tacoma Narrows
 - Design Failure
 - Natural Forces
- Hard Rock Hotel
 - Process Failure
 - Unintentional Actor
- World Trade Center
 - Intentional Failure
 - Intentional Actor
- Therac-25
 - Implementation Failure

Security Mindset



- A way of thinking about scenarios in order to identify and mitigate possible failures.
- Come in many form and applicable outside of computers/networks
 - Have to think like an attacker

Adversary



- Intelligent Actor
 - Person, Group, or Organization
- Have own:
 - Capabilities
 - Motivations
 - Intentions
- Are **NOT** restricted by expectations

Security Mindset



A way of thinking about scenarios in order to identify and mitigate possible failures.

- Come in many form and applicable outside of computers/networks
- Have to think like an attacker
 - Comprehend abilities and behavior patterns
 - Understand how search for/exploit weaknesses

Thinking Like an Attacker



- What is the **easiest/simplest** way to win?
 - “weakest link”, “low-hanging fruit”



Thinking Like an Attacker



- What is the **easiest/simplest** way to win?
 - “weakest link”, “low-hanging fruit”



Thinking Like an Attacker



- What is the **easiest/simplest** way to win?
 - “weakest link”, “low-hanging fruit”
- What are the **explicit assumptions** built into the system?
 - What are the creator’s expectations?
 - Who else does the creator rely on?

Thinking Like an Attacker



- What are the **explicit assumptions** built into the system?



Thinking Like an Attacker



- What is the **easiest/simplest** way to win?
 - “weakest link”, “low-hanging fruit”
- What are the **explicit assumptions** built into the system?
 - What are the creator’s expectations?
 - Who else does the creator rely on?
- What are the **implicit assumptions** which the aren’t always true/strong?
 - “outside the box” solutions

Thinking Like an Attacker



- What are the **implicit assumptions** which the aren't always true/strong?



Security Assumptions



2019 IEEE Symposium on Security and Privacy

Self-encrypting deception: weaknesses in the encryption of solid state drives

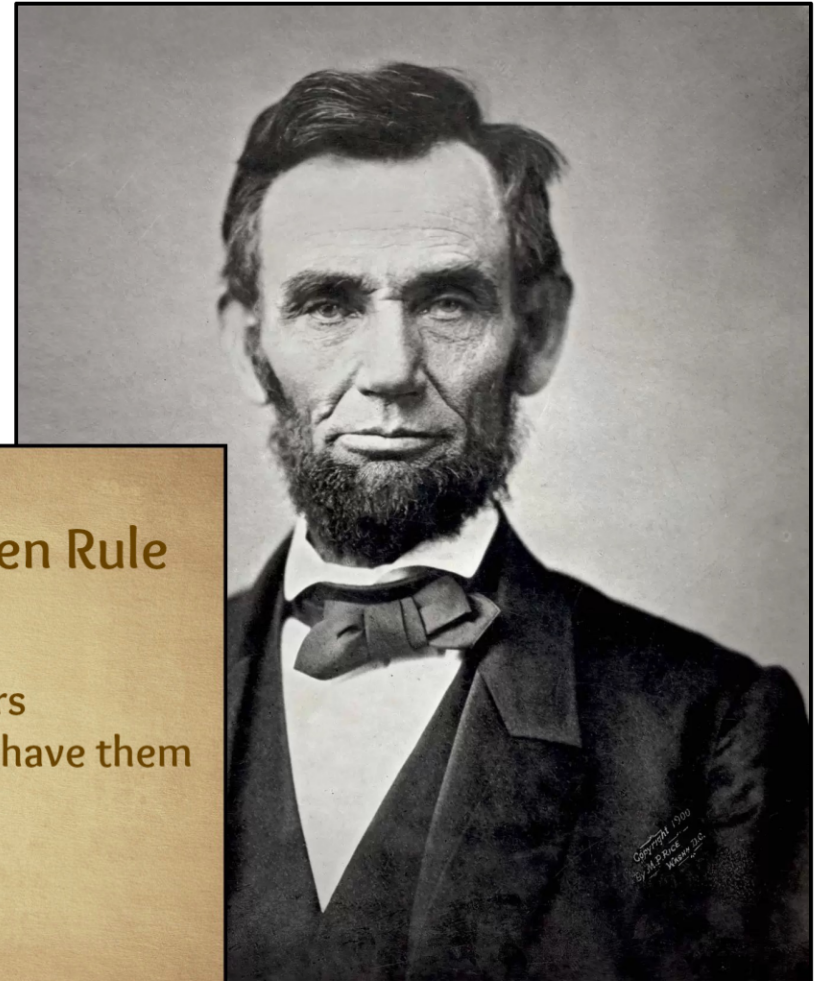
Carlo Meijer
Institute for Computing and Information Sciences
Radboud University Nijmegen
cmeijer@cs.ru.nl

Bernard van Gastel
School of Computer Science
Open University of the Netherlands
and
Institute for Computing and Information Sciences
Radboud University Nijmegen
Bernard.vanGastel@{ou.nl,ru.nl}

Support

Drive	1	2	3	4	5	6	7	8	9	Impact
Crucial MX100 (all)	✗	✗	✗		✗		✓	✓		Compromised
Crucial MX200 (all)	✗	✗	✗		✗		✓	✓		Compromised
Crucial MX300 (all)	✓	✓	✓		✗	✗	✓	✓		Compromised
Sandisk X600 (SATA)	✓	✓	✓		✗	✗	✓	✗		Probably compromised
Samsung 840 EVO (SATA)	✗	✓	✓		✓		✓		✓	Depends
Samsung 850 EVO (SATA)	✗	✓	✓		✓		✓	✓	✓	Depends
Samsung 950 PRO (NVMe)	✗	✓	✓		✓		✓	✓	✓	Probably safe
Samsung T3 (USB)				✗			✓	✓		Compromised
Samsung T5 (USB)				✗			✓	✓		Compromised

Role-Playing as "Bad Guys"



The Golden Rule

Do unto others
as you would have them
do unto you.

Copyright © 1999
by J.P. Price
www.tat.com

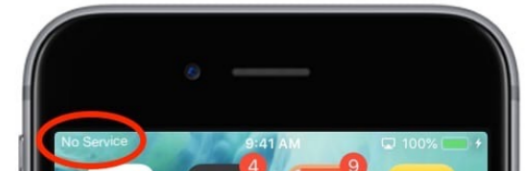
alphabetsalad.com

A central graphic element featuring a golden key with a heart-shaped head. The key is positioned vertically on the left side of a light brown rectangular background. To the right of the key, the text 'The Golden Rule' is written in a serif font. Below this, the Golden Rule is quoted in a smaller serif font. In the bottom right corner of the background, there is a small copyright notice. At the very bottom of the entire graphic, the website 'alphabetsalad.com' is listed.

Role-Playing as "Bad Guys"



Scenario



[Students](#) [Alumni](#) [Parents](#) [Employees](#) [Administration](#)

[Apply Now](#) [Give](#) [Libraries](#) [Map](#) [AU Access](#) [Search](#)



The Newsroom
The Official Source for Auburn University News

[OCM Home](#) [News Articles](#) [Campus Notices](#) [Expert Answers](#) [Calendar](#) [Submit News](#)

[Office of Communications & Marketing](#) / [The Newsroom](#) / [News Articles](#) / [2020](#) / [March](#) /

Search The Newsroom

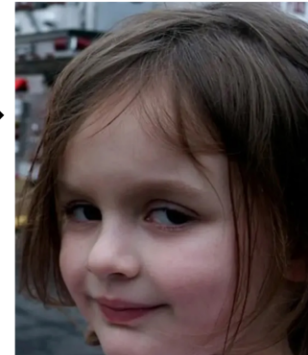
Auburn University to transition to remote instruction March 16-April 10

Published: March 12, 2020

Thinking Like an Attacker



Your Turn to be Her →



- What is the **easiest/simplest** way to win?
- What are the **explicit assumptions** built into the system?
- What are the **implicit assumptions** which the aren't always true/strong?

As an Attacker:



- What is the simplest way to gain access?

Attacker: Low-Hanging Fruit



- Lock-Picking
 - “high-skill manipulation”



Attacker: Low-Hanging Fruit



- Hammer beats door
 - “brute force attack”



Attacker: Low-Hanging Fruit



- Get-in and stay-in
 - “time of check, time of use vulnerability”



Attacker: Low-Hanging Fruit



- Trick someone into giving you access
 - “social engineering”



As an Attacker:



- What is the simplest way to gain access?
- What is assumed about the system?

Attacker: Breaking Assumptions



- Find an unlocked window
 - *Doors aren't the only way people enter and exit the building*



Attacker: Breaking Assumptions



minutekey



- Duplicate a key
 - *Only authorized people will ever possess keys*



Replication Prohibited: Attacking Restricted Keyways with 3D Printing

Ben Burgess
University of Michigan
baburges@umich.edu

Eric Wustrow
University of Michigan
ewust@umich.edu

J. Alex Halderman
University of Michigan
jhalderm@umich.edu

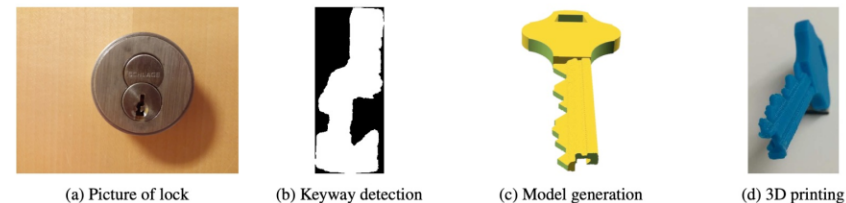
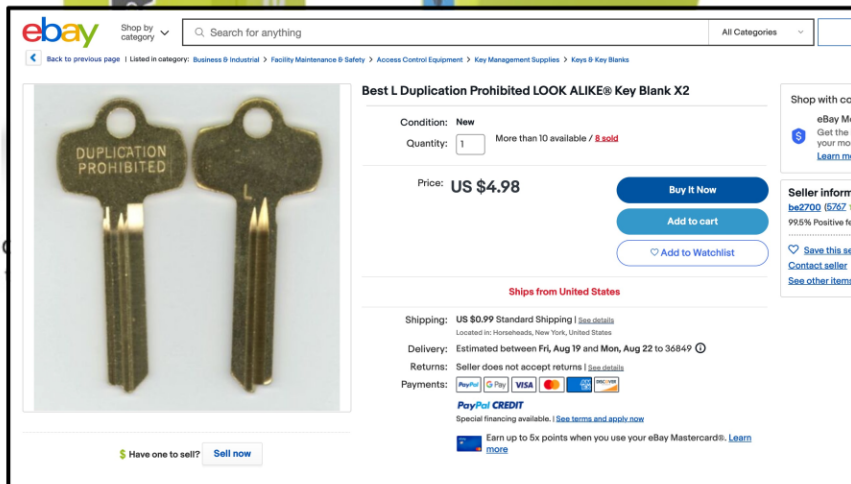


Figure 3: **Automatic key blank generation**—Our tool takes an image of a lock (a), automatically detects the outline shape of the keyway (b), and produces a 3D model of a blank (c) that fits in the keyway. A MakerBot Replicator 2 3D printed key (d) produced using the generated key blank model is illustrated.

As an Attacker:



- What is the simplest way to gain access?
- What is assumed about the system?
- What did defender not think about?

Attacker: Getting Creative



- Locate door with different properties
 - *Attackers can't fly but also aren't limited to the ground-floor*

Attacker: Getting Creative



- Obtain “unobtainium”

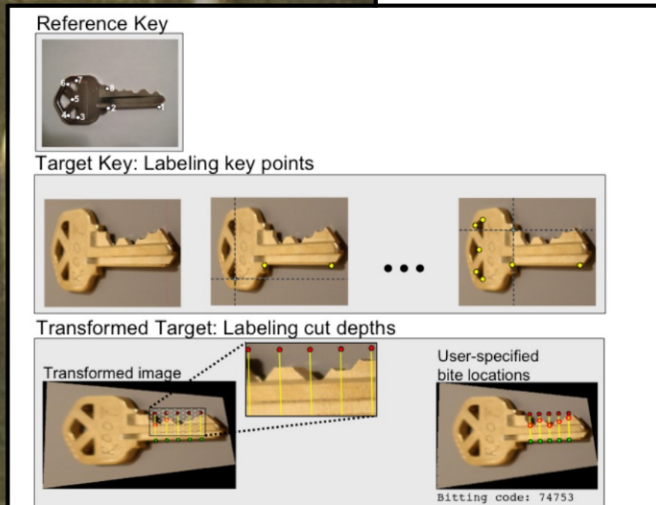
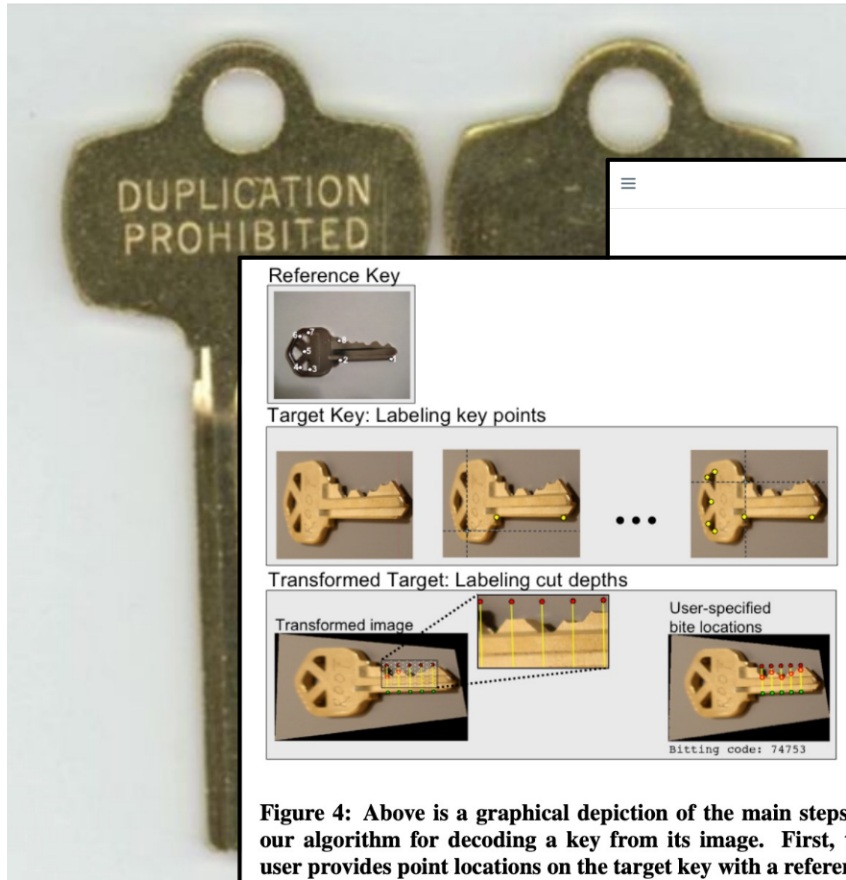


Figure 4: Above is a graphical depiction of the main steps in our algorithm for decoding a key from its image. First, the user provides point locations on the target key with a reference key as a guide. Next, the system warps the target image into the pose of the reference key and overlays markings of where the bite codes are to be found. Finally, the user specifies where the cut falls along each line and the bit depths are decoded by the system into a bitting code.

Reconsidering Physical Key Security: Teleduplication via Optical Decoding

Benjamin Laxton, Kai Wang and Stefan Savage
Department of Computer Science & Engineering
University of California, San Diego
La Jolla, California, USA



Figure 9: Our proof-of-concept telephoto experiment. The key image, captured at a distance of 195 feet, was correctly decoded as 74753.

Security Mindset



A way of thinking about scenarios in order to identify and mitigate possible failures.

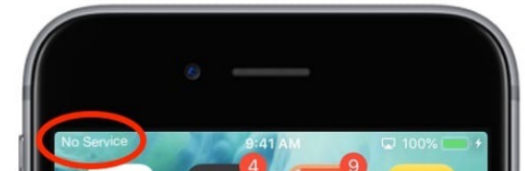
- Come in many form and applicable outside of computers/networks
- Have to think like an attacker
 - Comprehend abilities and behavior patterns
 - Understand how search for/exploit weaknesses
- Have to think like a defender
 - Identify what is being protected against who
 - Analyze/Evaluate cost-benefit trade-offs

Thinking Like a Defender



- What **assets** are you trying to protect?
 - What about those assets is important?
- Who are you trying to **defend against**?
Who are you willing to **let succeed**?
 - Nothing is ever 100% secure against all actors
- What will you **trade** for improved security?
 - Costs: time, energy, complexity, etc.

Scenario



[Students](#) [Alumni](#) [Parents](#) [Employees](#) [Administration](#)

[Apply Now](#) [Give](#) [Libraries](#) [Map](#) [AU Access](#) [Search](#)



The Newsroom
The Official Source for Auburn University News

[OCM Home](#) [News Articles](#) [Campus Notices](#) [Expert Answers](#) [Calendar](#) [Submit News](#)

[Office of Communications & Marketing](#) / [The Newsroom](#) / [News Articles](#) / [2020](#) / [March](#) /

Search The Newsroom

Auburn University to transition to remote instruction March 16-April 10

Published: March 12, 2020

Defender Complications



Your Turn



- What **assets** are you trying to protect?
 - What about those assets is important?
- Who are you trying to **defend against**?
Who are you willing to **let succeed**?
 - Nothing is ever 100% secure against all actors
- What will you **trade** for improved security?
 - Costs: time, energy, complexity, etc.

Option 1: Do Nothing



Bama: 28 Notre Dame: 0

*“Maybe Alabama doesn’t
come back in the 2nd half”*

- Halftime Interview of 2012
national championship

- Give up
- Hope that attackers don’t notice your vulnerabilities
- Claim bad people shouldn’t be doing bad things

Option 2: Complete Overhaul



Option 2: Complete Overhaul



- Re-organize to limit the attack surface

Option 2: Complete Overhaul



- Re-organize to limit the attack surface
- Restrict entrance and exit to single location

Option 2: Complete Overhaul



- Re-organize to limit the attack surface
- Restrict entrance and exit to single location
- Increase attackers' risk of negative outcomes

Option 3: Intentionally Designed Defenses



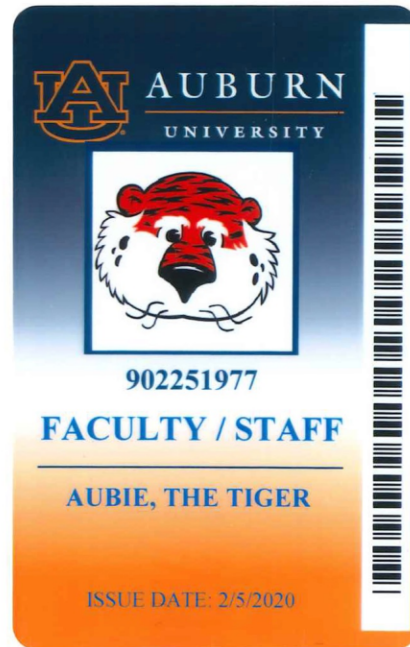
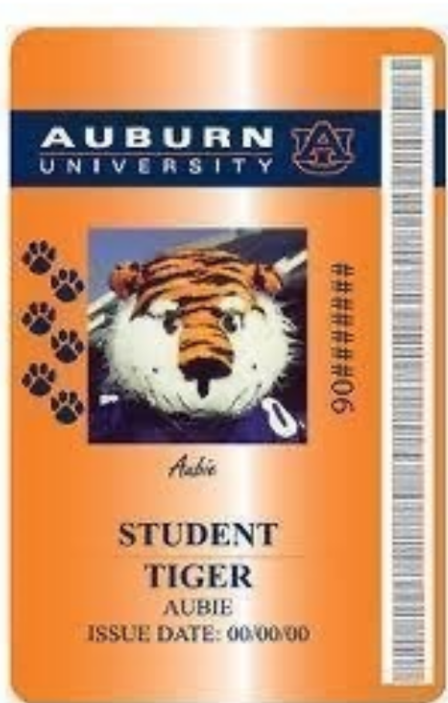
Option 3: Intentionally Designed Defenses



- Tiered physical boundaries



Option 3: Intentionally Designed Defenses



- Tiered physical boundaries
- Tiered access permissions

Option 3: Intentionally Designed Defenses



- Tiered physical boundaries
- Tiered access permissions
- Rely on non-experts to make rational decisions

Building Secure Solutions

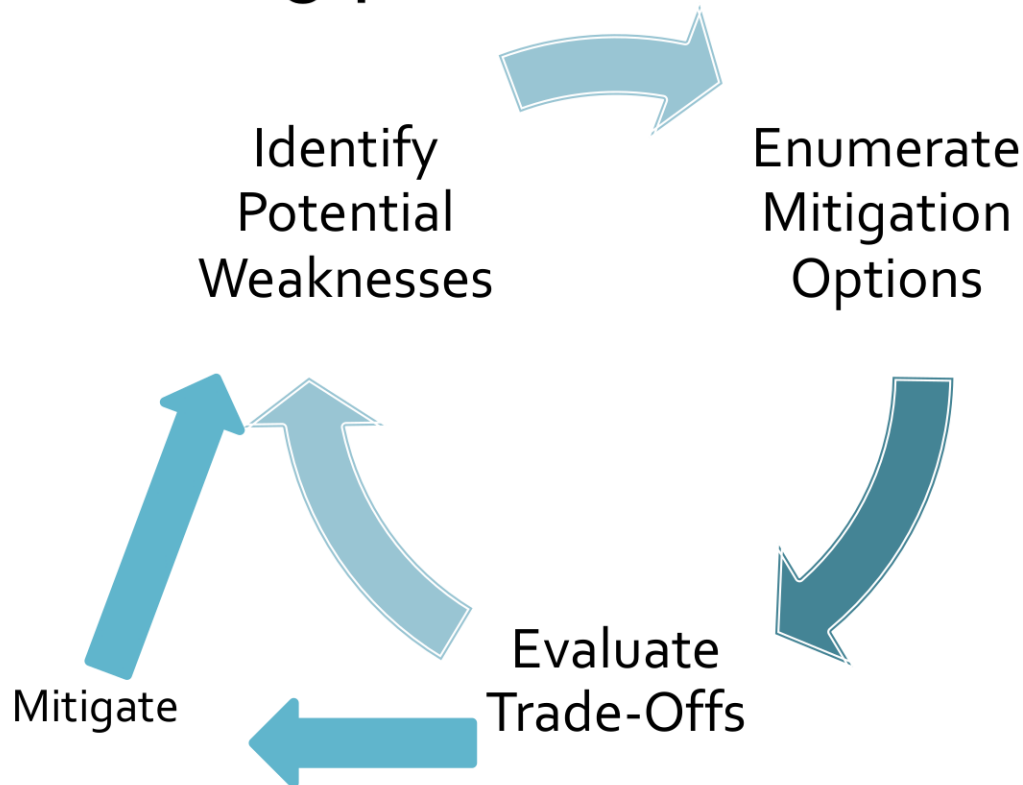


- Security is the outcome of a **process** and is not a *product* by itself
 - It is extremely hard to add-to design later
 - Is an on-going effort throughout the lifecycle

Threat Modeling



A systematic approach to analyzing and understanding potential weaknesses.



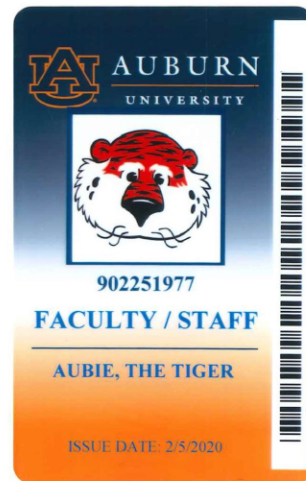
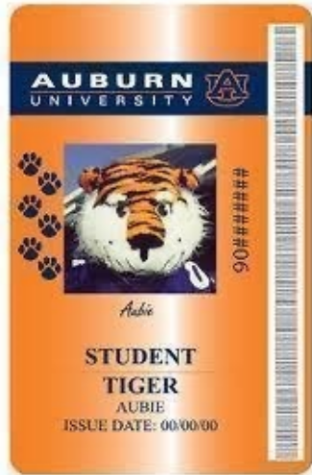
During Planning



- Create a system that is defensible



During Operation



- Create a system that is defensible
- Maintain the mechanisms for defending it

During Un-Wanted Events



REPORT YOUR LOST TIGER CARD

Students

If you cannot locate your student Tiger Card, you should immediately take one of the following actions to deactivate and protect your card. Once you have located your Tiger Card, you can easily reactivate your card the same way the card was deactivated:

1. Activate/deactivate your Tiger Card online.
 - You will need to login using your Auburn University student credentials (abc1234).
 - Once logged in, select "I Lost/Found My Card" under the "Quick Links" menu.
2. Activate/deactivate your cards through the mobile Tiger Card App.
3. Report your card as lost/found in person by coming by the Tiger Card office (Monday-Friday 7:30 a.m.- 4:30 p.m.)
4. Report your card as lost/found by phone at (334) 844-4507 (Monday-Friday 7:30 a.m.- 4:30 p.m.)

Faculty/Staff

For information on reporting a lost **Faculty/Staff** ID, please visit [ID Card Services \(Onboarding Center\)](#) or contact them at 334-844-1763. ID Card Services (Onboarding Center) is located at [1530 East Glenn Avenue](#).

Last updated: August 13, 2021



BACK TO TOP

- Create a system that is defensible
- Maintain the mechanisms for defending it
- Train and educate non-experts

Keeping Systems Defendable



REPORT YOUR LOST TIGER CARD

Students

If you cannot locate your student Tiger Card, you should immediately take one of the following actions to deactivate and protect your card. Once you have located your Tiger Card, you can easily reactivate your card the same way the card was deactivated:

1. Activate/deactivate your Tiger Card online.
 - You will need to login using your Auburn University student credentials (abc1234).
 - Once logged in, select "I Lost/Found My Card" under the "Quick Links" menu.
2. Activate/deactivate your cards through the mobile Tiger Card App.
3. Report your card as lost/found in person by coming by the Tiger Card office (Monday-Friday 7:30 a.m.- 4:30 p.m.)
4. Report your card as lost/found by phone at (334) 844-4507 (Monday-Friday 7:30 a.m.- 4:30 p.m.)

Faculty/Staff

For information on reporting a lost **Faculty/Staff** ID, please visit [ID Card Services \(Onboarding Center\)](#) or contact them at 334-844-1763. ID Card Services (Onboarding Center) is located at [1530 East Glenn Avenue](#).

Last updated: August 13, 2021



BACK TO TOP

- Create a system that is defendable
- Maintain the mechanisms for defending it
- Train and educate non-experts
- **Make safe easy and unsafe hard/obvious**

Building Secure Solutions



- Security is the outcome of a **process** and is not a *product* by itself
 - It is extremely hard to add-to design later
 - Is an on-going effort throughout the lifecycle
- Security is **not a checkbox** to hit on the way to releasing a product
 - “HIPAA Compliant” \neq safe/secure/private
 - “Used cipher X” \neq “Used cipher X correctly”

Certified != Secure



The screenshot shows the AWS Public Sector website. At the top left is the AWS logo. The top right navigation bar includes links for 'Contact Us', 'Support', 'English', 'My Account', and a prominent orange 'Create an AWS Account' button. Below this is a secondary navigation bar with categories like 'Products', 'Solutions', 'Pricing', 'Documentation', 'Learn', 'Partner Network', 'AWS Marketplace', 'Customer Enablement', 'Events', and 'Explore More'. The main content area is titled 'Public Sector' and features a sub-header 'Address security and compliance requirements'. A paragraph explains that AWS GovCloud (US) is available to government customers, highly regulated industries, and other commercial entities meeting requirements. Below this are ten icons representing various regulatory frameworks: FedRAMP, FISMA, Department of Defense Security Requirements Guide (SRG), U.S. International Traffic in Arms Regulations (ITAR), Criminal Justice Information Services (CJIS), National Institute of Standards and Technology (NIST), Federal Information Processing Standard (FIPS) Publication, Defense Federal Acquisition Regulation Supplement (DFARS), Department of Commerce Export Administration Regulations (EAR), and IRS-1075 Encryption Standards.

aws Contact Us Support English My Account [Create an AWS Account](#)

[Products](#) [Solutions](#) [Pricing](#) [Documentation](#) [Learn](#) [Partner Network](#) [AWS Marketplace](#) [Customer Enablement](#) [Events](#) [Explore More](#)

Public Sector [Industries](#) [Programs](#) [Security & Compliance](#) [Partners](#) [Resources](#) [Countries](#) [Events](#)

Address security and compliance requirements

AWS GovCloud (US) is available to government customers, organizations in highly regulated industries, and other commercial entities that meet AWS GovCloud (US) requirements.

- FedRAMP**
Federal Risk and Authorization Management Program (FedRAMP)
- FISMA**
Federal Information Security Management Act (FISMA)
- Department of Defense Security Requirements Guide (SRG)**
- U.S. International Traffic in Arms Regulations (ITAR)**
- Criminal Justice Information Services (CJIS)**
- National Institute of Standards and Technology (NIST)**
- Federal Information Processing Standard (FIPS) Publication**
- Defense Federal Acquisition Regulation Supplement (DFARS)**
- Department of Commerce Export Administration Regulations (EAR)**
- IRS-1075 Encryption Standards**

Security Mindset



A way of thinking about scenarios in order to identify and mitigate possible failures.

- Come in many form and applicable outside of computers/networks
- Have to think like an attacker
 - Comprehend abilities and behavior patterns
 - Understand how search for/exploit weaknesses
- Have to think like a defender
 - Identify what is being protected against who
 - Analyze/Evaluate cost-benefit trade-offs

Things to Look Forward To



- Concepts & Ideas
 - “Security Mindset”
 - Randomness
- Applied Crypto
 - Encryption/Hashing
 - Key Exchanges
 - Real-World Application
 - Privacy Protections
 - C---r Issues
- Network Security
 - Good/Bad Protocols
 - Web attacks/defenses
- Host/App Security
 - Malware, botnets, etc
 - Binary exploitation



**KILL IT
WITH FIRE**



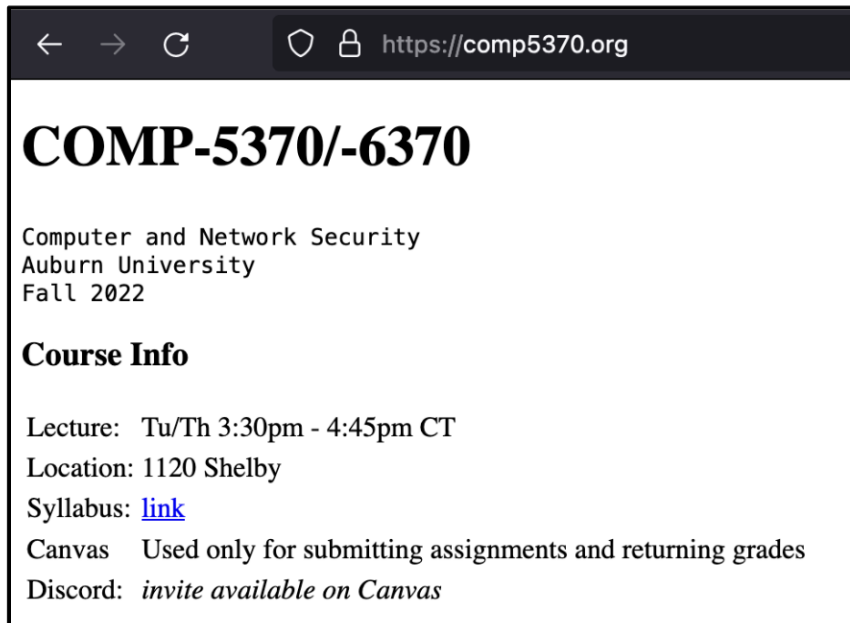
canvas

LET IT BURN

- Canvas is *the DEVIL*
 - Only for submitting and getting grades



Course Website

A screenshot of a web browser showing the course website. The address bar displays 'https://comp5370.org'. The main content area has a large heading 'COMP-5370/-6370' followed by the text 'Computer and Network Security', 'Auburn University', and 'Fall 2022'. Below this is a section titled 'Course Info' containing details about lecture times, location, a syllabus link, and information about Canvas and Discord.

← → ↻ 🔒 https://comp5370.org

COMP-5370/-6370

Computer and Network Security
Auburn University
Fall 2022

Course Info

Lecture: Tu/Th 3:30pm - 4:45pm CT
Location: 1120 Shelby
Syllabus: [link](#)
Canvas Used only for submitting assignments and returning grades
Discord: *invite available on Canvas*

- Canvas is *the DEVIL*
 - Only for submitting and getting grades
- <https://comp5370.org>
 - Syllabus
 - Slides
 - Assignments
 - ...

Grading Overview



- **Projects (3x)**
 - Project 1 is 2 parts for a total of 10%
- **In-Class Exams (2x)**
- **Midterm (1x)**
- **Final (1x)**

Grading

- **3x Course Projects (each)** — 10%
- **Final Exam** — 25%
- **2x In-Class Exams (each)** — 12.5%
- **Midterm Exam** — 20%

Calculating Your Course Grade With your returned scores as a percentile value (i.e. 0% – 100%), fill-in the below formula:

$$0.10 \times project_1 + 0.10 \times project_2 + 0.10 \times project_3 + 0.125 \times exam_1 + 0.125 \times exam_2 + 0.20 \times midterm + 0.25 \times final$$

Course Textbook



- There is **no textbook** for this course b/c...

The Internet is *OUR* Textbook



The Internet is *OUR* Textbook



A screenshot of the Wikipedia article for Matt Blaze. The article text includes: "Matt Blaze is an American researcher who focuses on the areas of secure systems, cryptography, and trust management. He is currently the McDevitt Chair of Computer Science and Law at Georgetown University. FRN and is on the board of directors of the Tor Project." It also lists his work on the Escrowed Encryption Standard and his role at the University of Colorado Boulder.

A screenshot of the Wikipedia article for Amie Stepanovich. The article text includes: "Amie Stepanovich is a lawyer and drone surveillance. She is a research center at the Electronic Frontier Foundation. She is a former in-chief of the New York Law Resource Center, and she served as a law professor at the New York State Bar Association." It also lists her education at Florida State University and her career at the New York State Bar Association.

A screenshot of the Electronic Frontier Foundation (EFF) website. The page features the EFF logo, navigation links, and a profile for Kurt Opsahl. The profile text reads: "Kurt Opsahl is the Deputy Executive Director and General Counsel of the Electronic Frontier Foundation. In addition to representing clients on civil liberties, free speech and privacy law, Opsahl counsels on EFF".

A screenshot of a Twitter post by Kurt Opsahl (@kurtopsahl). The tweet text reads: "PSA: Crypto means Cryptography. #usesec18 cc @mattblaze @astepanovich". The tweet includes a photo of three people (Matt Blaze, Amie Stepanovich, and Kurt Opsahl) wearing "CRYPTO IT MEANS CRYPTOGRAPHY" t-shirts. The tweet is dated August 15, 2018, and has 72 likes and 4 quote tweets.

The Internet is *OUR* Textbook



Theorem 19.18. *The AND protocol (P, V) is a Sigma protocol for the relation \mathcal{R}_{AND} defined in (19.22). If (P_0, V_0) and (P_1, V_1) provide knowledge soundness, then so does (P, V) . If (P_0, V_0) and (P_1, V_1) are special HVZK, then so is (P, V) .*

Proof sketch. Correctness is clear.

For knowledge soundness, if (P_0, V_0) has extractor Ext_0 and (P_1, V_1) has extractor Ext_1 , then the extractor for (P, V) is

$$Ext\left((y_0, y_1), ((t_0, t_1), c, (z_0, z_1)), ((t_0, t_1), c', (z'_0, z'_1)) \right) := \\ \left(Ext_0(y_0, (t_0, c, z_0), (t_0, c', z'_0)), Ext_1(y_1, (t_1, c, z_1), (t_1, c', z'_1)) \right).$$

For special HVZK, if (P_0, V_0) has simulator Sim_0 and (P_1, V_1) has simulator Sim_1 , then the simulator for (P, V) is

$$Sim((y_0, y_1), c) := ((t_0, t_1), (z_0, z_1)),$$

where

$$(t_0, z_0) \stackrel{R}{\leftarrow} Sim_0(y_0, c) \quad \text{and} \quad (t_1, z_1) \stackrel{R}{\leftarrow} Sim_1(y_1, c).$$

The Internet is *OUR* Textbook



Theorem 19.18. *The AND protocol (P, V) is a Sigma protocol for the relation \mathcal{R}_{AND} defined in (19.22). If (P_0, V_0) and (P_1, V_1) provide knowledge soundness, then so does (P, V) . If (P_0, V_0) and (P_1, V_1) are special HVZK, then so is (P, V) .*

Proof sketch. Correctness is clear.

For knowledge soundness, if (P_0, V_0) has extractor Ext_0 and (P_1, V_1) has extractor Ext_1 , then the extractor for (P, V) is

$$Ext\left((y_0, y_1), ((t_0, t_1), c, (z_0, z_1)), ((t_0, t_1), c', (z'_0, z'_1)) \right) := \\ \left(Ext_0(y_0, (t_0, c, z_0), (t_0, c', z'_0)), Ext_1(y_1, (t_1, c, z_1), (t_1, c', z'_1)) \right).$$

For special HVZK, if (P_0, V_0) has simulator Sim_0 and (P_1, V_1) has simulator Sim_1 , then the simulator for (P, V) is

$$Sim((y_0, y_1), c) := ((t_0, t_1), (z_0, z_1)),$$

where

$$(t_0, z_0) \stackrel{R}{\leftarrow} Sim_0(y_0, c) \quad \text{and} \quad (t_1, z_1) \stackrel{R}{\leftarrow} Sim_1(y_1, c).$$

A Graduate Course in Applied Cryptography
Dan Boneh and Victor Shoup
<https://toc.cryptobook.us/>

Attacker: Getting Creative



- Obtain “unobtainium”

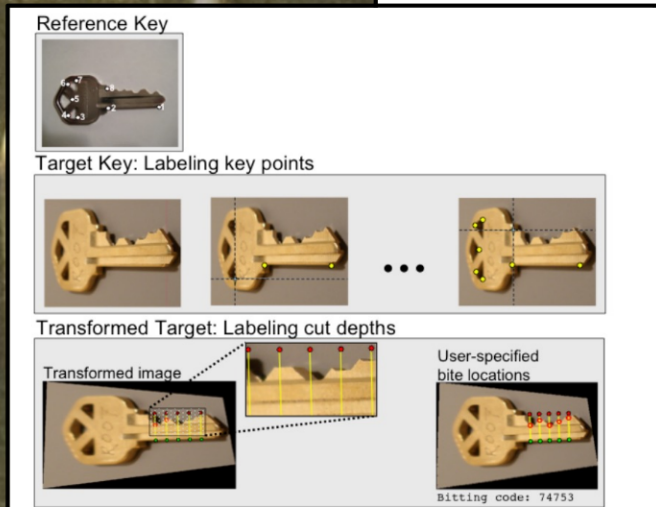
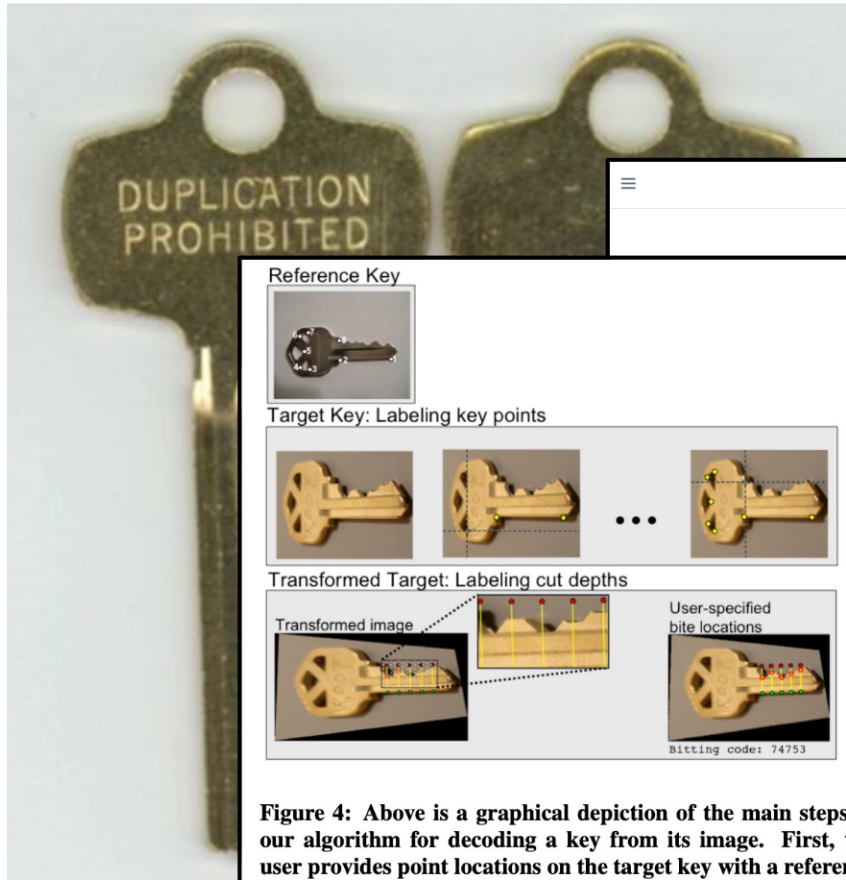


Figure 4: Above is a graphical depiction of the main steps in our algorithm for decoding a key from its image. First, the user provides point locations on the target key with a reference key as a guide. Next, the system warps the target image into the pose of the reference key and overlays markings of where the bite codes are to be found. Finally, the user specifies where the cut falls along each line and the bit depths are decoded by the system into a bitting code.

Reconsidering Physical Key Security: Teleduplication via Optical Decoding

Benjamin Laxton, Kai Wang and Stefan Savage
Department of Computer Science & Engineering
University of California, San Diego
La Jolla, California, USA



Figure 9: Our proof-of-concept telephoto experiment. The key image, captured at a distance of 195 feet, was correctly decoded as 74753.

Attacker: Getting Creative



- Obtain “unobtainium”

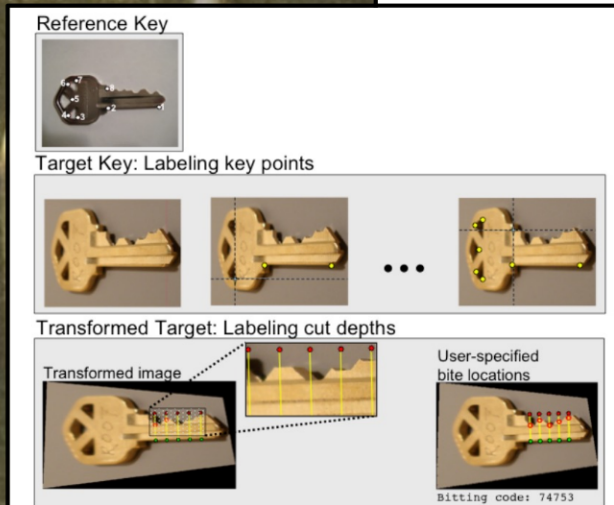
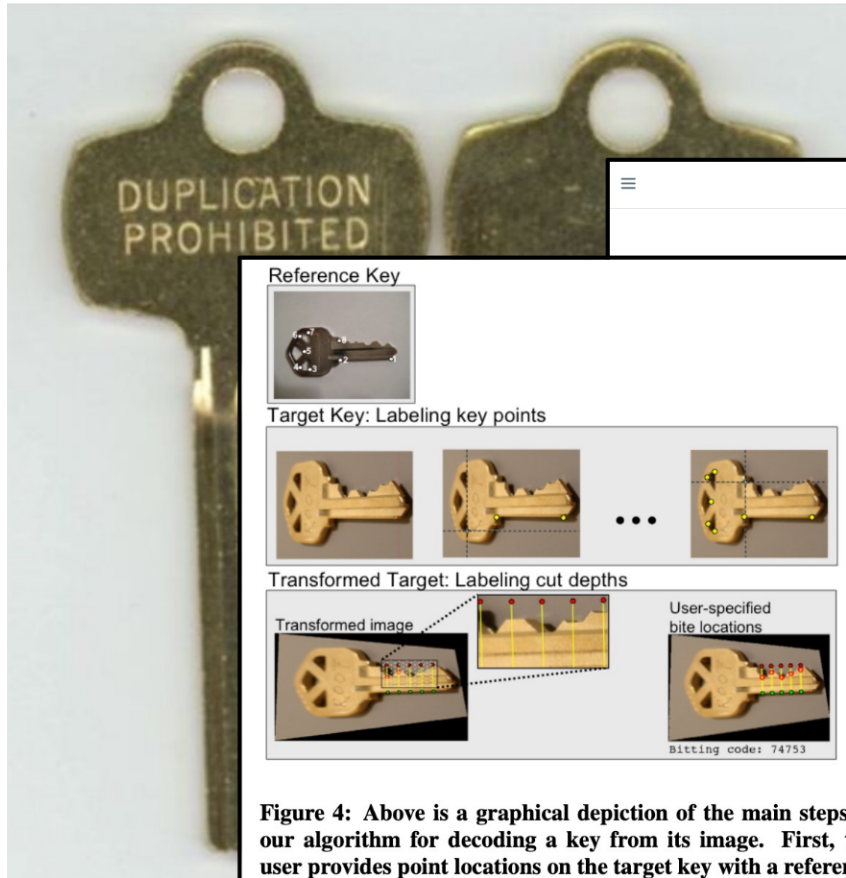


Figure 4: Above is a graphical depiction of the main steps in our algorithm for decoding a key from its image. First, the user provides point locations on the target key with a reference key as a guide. Next, the system warps the target image into the pose of the reference key and overlays markings of where the bite codes are to be found. Finally, the user specifies where the cut falls along each line and the bit depths are decoded by the system into a bitting code.

Reconsidering Physical Key Security: Teleduplication via Optical Decoding

Benjamin Laxton, Kai Wang and Stefan Savage
Department of Computer Science & Engineering
University of California, San Diego
La Jolla, California, USA



Figure 9: Our proof-of-concept telephoto experiment. The key image, captured at a distance of 195 feet, was correctly decoded as 74753.

Law/Ethics/University Policy



Law/Ethics/University Policy



- In-Scope systems will be explicitly stated
- Everything else is out-of-scope
- When in doubt, stop and ask

Law/Ethics/University Policy



- In-Scope systems will be explicitly stated
- Everything else is out-of-scope
- When in doubt, stop and ask

1) DO NOT COMMIT CRIMES

Law/Ethics/University Policy



- In-Scope systems will be explicitly stated
- Everything else is out-of-scope
- When in doubt, stop and ask

1) DO NOT COMMIT CRIMES

2) Respect others' security & privacy

Have Questions?



- In-person interaction usually solves problems immediately
 - Office hours in syllabus and on website
 - After-class, open-door, etc. (instructor-only)
 - If the office-phone rings, I pick it up
- Email is a valid but highly-latent channel
 - Might answer in next lecture
 - Might take couple of days to get to your email

Course TA



- Ginny Genge
- Office Hours:
 - Mo 1-2
 - We 4-5
 - 2168 Brown-Koppel

Code Counts in CS



Errors in Submission Students should be aware that all projects will be graded in an auto-grader style workflow (i.e. automated and/or mechanical actions to test submission). If a compilation/interpretation error is encountered (i.e. syntax error, tabs vs. spaces in Python, etc.) the submitted source code **will not** be examined nor debugged and **a grade of zero (0) will be given**. The environment in which your projects will be graded will be clearly defined in each assignment and non-running projects will be eligible for a regrade as discussed below.

Regrade Requests While obvious grading errors* can be handled immediately by bringing them the instructor's attention, students are welcome to request an assignment/project/exam be regraded in its entirety by contacting the TA. All regrade requests must follow the requirements of:

1. Clearly state that a regrade is being requested.
2. Clearly state the fundamental misunderstanding that caused the original submission to be deducted points.
3. Clearly state the changes that were made to remediate that fundamental misunderstanding.
4. Contain no extraneous changes that are not related to that fundamental misunderstanding.
5. Be made within seven (7) days of the assignment being returned.
6. Be requested over email.

Students should be aware that points will be deducted based on the original submission's fundamental misunderstanding and depending on the circumstances, this may result in a grade of zero (0). The instructor has the final authority on A) whether a regrade will be conducted based on the request and B) to what degree the fundamental misunderstanding will be penalized.

Late Assignments Hurt



Late Assignments Any assignment submitted after the deadline must be sent via e-mail to the TA. Late assignments will lose 10 percentage points per hour[†] based on the timestamp in the email received. **“Late-days” are not available to students in the Fall 2024 iteration of this course.** In the case of extenuating circumstances, the student *must* contact the instructor at the earliest reasonable opportunity. The Excused Absence policy will be applied but exceptions may be made at the instructor’s discretion.

- 10% deduction per hour
 - 1 Day = 24 hours
 - $100\% - 240\% = -140\%$

**You do not
have late days**

Grading Overview



- **Projects (3x)**
 - Project 1 is 2 parts for a total of 10%
- **In-Class Exams (2x)**
- **Midterm (1x)**
- **Final (1x)**

Grading

- **3x Course Projects (each)** — 10%
- **Final Exam** — 25%
- **2x In-Class Exams (each)** — 12.5%
- **Midterm Exam** — 20%

Calculating Your Course Grade With your returned scores as a percentile value (i.e. 0% – 100%), fill-in the below formula:

$$0.10 \times project_1 + 0.10 \times project_2 + 0.10 \times project_3 + 0.125 \times exam_1 + 0.125 \times exam_2 + 0.20 \times midterm + 0.25 \times final$$

Project 1-A



- Released tomorrow and due in 2 weeks
- Use the Security Mindset while building a straight-forward, custom data format parser
- Does **not** require large amount of code but **does** require a large amount of thinking



CTF This Weekend



The Auburn University
Ethical Hacking Club
and
Auburn Cyber Research
Center present



CyberFire Puzzles

By Los Alamos National Laboratory

August 23rd - 25th, 2024
Brown-Kopel Engineering Student Center
23rd: Kick-Off Event 6pm-8pm
24th: Competition 10am - End of Day
25th: Competition 10am - 5pm

Admission \$30
EHC Members \$25
(Due by noon on 8/21)
Late Admission \$35
(Available at the Door)



Visit
aub.ie/cyberfire2024
for more information



- “Capture the Flag” challenges
- Register via link in your email
 - \$30 registration but meals + snacks/drinks provided

Computer and Network Security

Lecture 01: Overview & Mindset

COMP-5370/6370

