SCC.141 Professionalism in Practice

Week 11: Security in Systems

Protecting Software, Hardware, and People

15th January 2025
Dr Elmira Yadollahi, e.yadollahi@lancaster.ac.uk
School of Computing and Communications

*Inspired by Lecture by Dr Phil Benachour.

Term 1 Coursework marks

- The grades for your SCC.141 Term 1 coursework will be released on Friday **27th of January**.
- The grades should appear on your interactive transcript as soon as they are released.
  - We are in the process of completing the marking.
  - We will follow this with moderation.
  - Then send the final grades to the SCC Teaching Office.

Term 1 Coursework General Feedback

- A PDF on Moodle with detailed General Feedback for CW1

- It include the following sections
  - Key Points for Students to Improve Future Essays
  - Instances Where Students Did Not Fully Follow the Guidance
  - Recommendations for Future Submissions

- Read through the recommendation and implement them in your Term 2 Coursework.

Weekly Lecture topics in Term 2

Lancaster University

Week No	Topics focussed on ongoing challenges	Lecturer and Date
11	Security in Systems	Dr Elmira Yadollahi, 15th Jan
12	Privacy	Dr Elmira Yadollahi, 22nd Jan
13	Censorship/Surveillance/Section 230	Dr Elmira Yadollahi, 29th Jan
14	Malware	Dr Elmira Yadollahi, 5th Feb
15	Digital Exclusion	Dr Elmira Yadollahi, 12th Feb
16	Digital Inequalities	Dr Elisa Rubegni, 19th Feb
17	AI Ethics	Dr Elisa Rubegni, 26th Feb
18	Computing and Climate Change	Dr Elisa Rubegni, 5th March
19	Guest Lecture	Dr Elisa Rubegni, 12th March
20	Term 2 recap of topics	Dr Elisa Rubegni, 19th March

Learning Objectives

Lancaster University

- **Understand** the importance of system security
- **Define** key terms in the field
- **Describe** security design principles and guidelines
- **Look** at examples of security breaches
- **Learn** best practices and how they have changed over years

Agenda

Lancaster University

- Security in the Headlines
- Why System Security Matters?
- The CIA Triad: Foundations of Security
- Security Design Principles
- Immutable Laws of Security
- Key Takeaways & Future Outlook

Have you recently seen any significant security breach news in the media?

”Weak” Password Disaster – January 2024

COMEDY OF ERRORS —

A “ridiculously weak” password causes disaster for Spain’s No. 2 mobile carrier

BGP tampering caused by poor security hygiene causes major outage for Orange España.

DAN GOODIN - 1/5/2024, 12:01 AM

Getty Images

Enlarge

Dan Goodin (2024) A “ridiculously weak” password causes disaster for Spain’s No. 2 mobile carrier.

Available at: https://arstechnica.com/security/2024/01/a-ridiculously-weak-password-causes-disaster-for-spains-no-2-mobile-carrier/ .

[Accessed: January 6th , 2025].

Cyber-attack on NHS – May 2017

BBC (2017) NHS cyber-attack: GPs and hospitals hit by ransomware.

Available at: https://www.bbc.co.uk/news/health-39899646. [Accessed: January 6th , 2025].

WannaCry Ransomware

Cyberattack on NHS – May 2017

- Some 48 hospitals were understood to have been affected.
  - Figure shows the location of 37 hospitals revealed to have been attacked by the NHS at the time.
- Exploited a known Windows vulnerability—**EternalBlue**—to spread rapidly
- Caused serious disruptions, forcing hospitals to **cancel appointments**, **delay surgeries**, and **switch back to pen-and-paper systems**.

Express (2017). NHS cyber attack: Has my hospital been hacked? Latest list of affected hospitals.

Available at: https://www.express.co.uk/news/uk/803821/NHS-cyber-attack-hospital-trusts-hacked-cyber-security-hack-virus-patient-details.

[Accessed: January 6th , 2025].

Another Cyberattack on NHS - August 2022

- NHS IT supplier held to ransom by hackers

BBC (2023) NHS IT supplier held to ransom by hackers.

Available at: https://www.bbc.co.uk/news/technology-62506039

[Accessed: January 6th , 2025]

Another Cyberattack on NHS - August 2022

- NHS IT supplier held to ransom by hackers

BBC (2023) NHS IT supplier held to ransom by hackers.

Available at: https://www.bbc.co.uk/news/technology-62506039

[Accessed: January 6th , 2025]

These NHS incidents underline a critical truth:
In healthcare—where stakes are life and death—**robust**, **proactive** **cyber-defense** is **non-negotiable**.

Outdated software, insufficient patching, and human error can all contribute to devastating attacks. Learning from these events helps us strengthen our own infrastructures, whether in healthcare or any other sector.

Robot Vacuums Hacks – October 2024

- Hacked robot vacuums are yelling racial slurs, chasing pets

Global News: Hacked U.S. robot vacuums are yelling racial slurs, chasing pets: report.

Available at: https://globalnews.ca/news/10807939/robot-vacuum-racial-slurs-ecovacs-hacked/

[Accessed: January 6th , 2025].

Robot Vacuums Hacks – October 2024

- “If you do it in a very silent way, [the victim] would never figure it out,” he says.

We hacked a robot vacuum — and could watch live through its camera

Available at: https://www.abc.net.au/news/2024-10-04/robot-vacuum-hacked-photos-camera-audio/104414020

[Accessed: January 13th , 2025].

Why System Security Matters

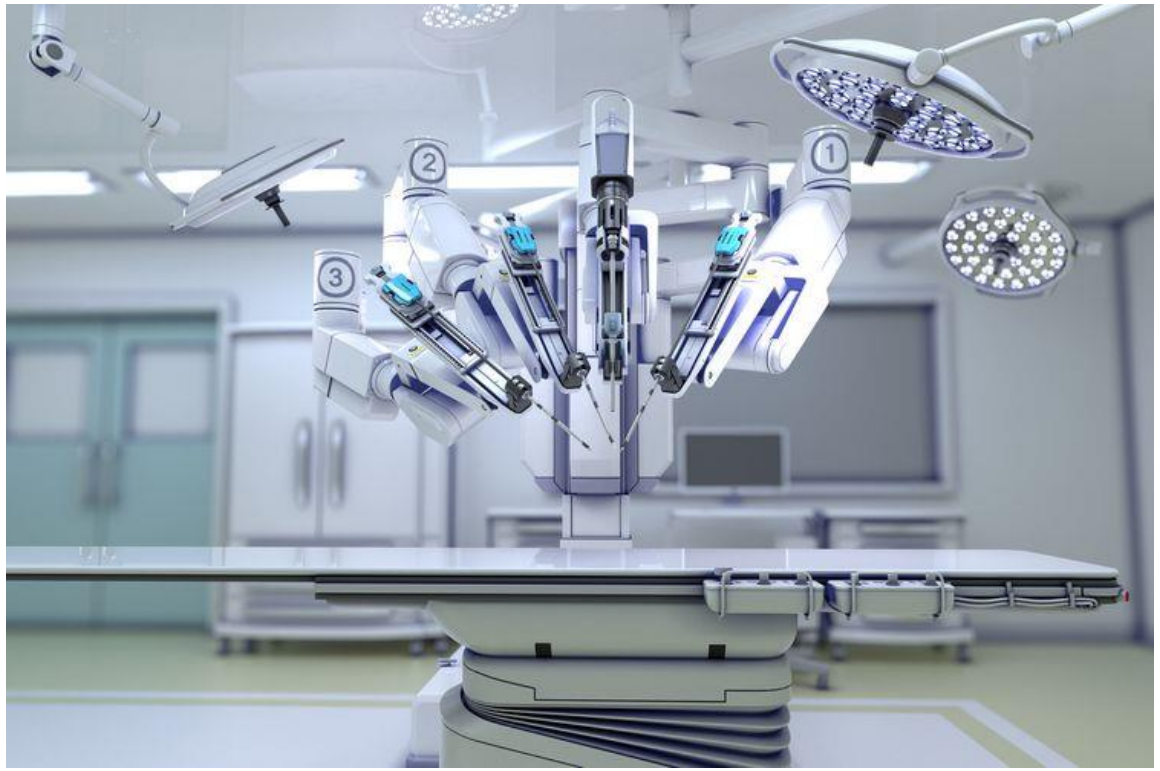
Lancaster University

"Trustworthy"?

- **Trustworthy** Systems Power Our Lives
  - We depend on them for daily life (smartphones, medical devices, industrial robots)
- **Frequent** & **Costly** Security Breaches
  - Attacks occur almost daily, costing time, money, and reputation
- **Complex Systems** => Inevitable Defects
  - Design flaws or coding bugs are common in large, interconnected systems
- **Natural** vs. **Malicious** Exposures
  - Some vulnerabilities appear by accident; others are exploited deliberately
- Why It Matters
  - Undermined trust leads to **downtime**, **data loss**, and potential **safety risks**

Why System Security Matters

Lancaster University

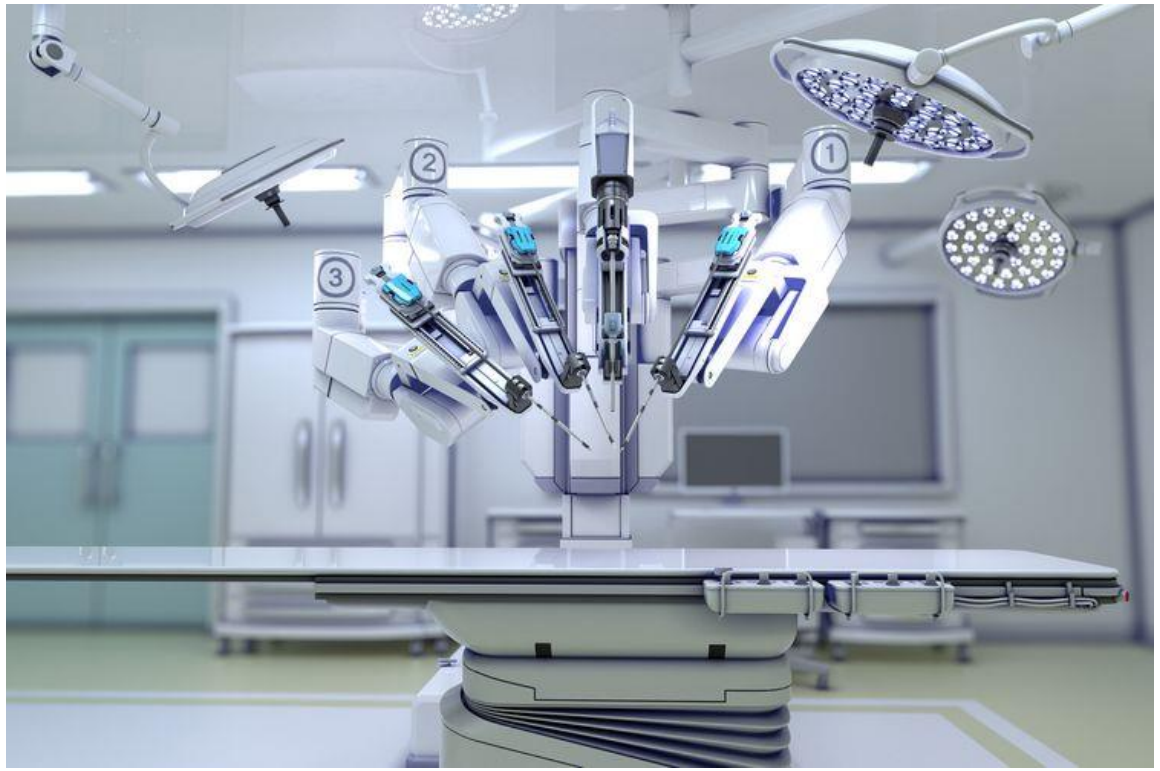


https://www.verywellhealth.com/robotic-surgery-4843262

https://www.carmagazine.co.uk/autonomous/waymo-google-self-driving-car/

Why System Security Matters

Lancaster University



https://www.verywellhealth.com/robotic-surgery-4843262

https://www.carmagazine.co.uk/autonomous/waymo-google-self-driving-car/

where there's software, there are bugs!!!

Why Robotic Security Matters

Lancaster University

- **Potential Harassment:**
  - Hacked robots (even household ones) can be turned into tools for offensive or harmful behaviour
- **Safety & Liability:**
  - Compromised functionality (e.g., sensors, movement) can cause accidents or damage
- **User Trust:**
  - Adoption stalls if people fear privacy invasions or physical harm

Why Robotic Security Matters

Lancaster University

Robots add a physical dimension

- **Potential Harassment:**
  - Hacked robots (even household ones) can be turned into tools for offensive or harmful behaviour
- **Safety & Liability:**
  - Compromised functionality (e.g., sensors, movement) can cause accidents or damage
- **User Trust:**
  - Adoption stalls if people fear privacy invasions or physical harm

Lancaster University

The CIA Triad:
Foundations of Security

Core Goals of Secure Systems: The CIA Triad

Lancaster University

- The CIA Triad (Confidentiality, Integrity, Availability) is a **foundational model** for understanding security requirements

- Organizations use it to shape policies, controls, and strategies that **minimize threats**

Confidentiality

Lancaster University

Definition:

- Computing resources and data (raw) and information (processed) should be **accessible only** to authorised users

Two Related Concepts:

- **Data Confidentiality:** Ensures that information is not disclosed to unauthorized parties.
- **Privacy:** Gives the owner control over what data is collected, how it's stored, and how it's used.

Practical Methods:

- Encryption (in transit and at rest), access controls, authentication.

Example:

- Protecting patient data in a medical system so only registered nurses/doctors can view or update it.

Integrity

Lancaster University

Definition:

- Resources should **only be modified or removed** by authorized users.

Two Related Concepts:

- **Data Integrity:** Ensures data (files, databases) isn't tampered with—accidentally or maliciously.
- **System Integrity:** The system should function as intended, free of unauthorized modifications.

Key Takeaways:

- Even small changes can break critical processes or mislead decision-making.
- Modifications can be malicious (attacks) or accidental (bugs, errors).

Practical Methods:

- Checksums, hashing, digital signatures, version control.

Example:

- A drone's flight controller firmware must remain unaltered. An injected change could crash the drone or redirect it illegally.

Availability

Lancaster University

Definition:

- Resources need to be **accessible** when needed by the **authorised users**.

Key Aspects:

- **Performance:** Slow or overloaded systems hurt availability.
- **Single Point of Failure:** Avoid designs where one failing component takes down the entire system.
- **Redundancy & Backups:** Provide fallback options (e.g., mirrored servers, spare hardware).

Types of Failures:

- **Malicious:** Denial-of-Service attacks or ransomware.
- **Accidental:** Network outage, hardware crash, misconfiguration.
- **Environmental:** Natural disasters, power failures.

Example:

- A hospital's patient-monitoring system must remain up 24/7—any downtime could endanger lives.

Bringing It All Together

Lancaster University

Why CIA Matters:

- Security **fails** if any one of these pillars (C, I, or A) is compromised.
- Comprehensive security strategies must **balance** all three.

Real-World Example:

- In a **smart factory**, robots rely on data confidentiality (blueprints, trade secrets), integrity (correct assembly instructions), and availability (uninterrupted operation).
- A breach in any pillar can disrupt production, cause safety hazards, or leak IP.

Action Points:

- Align **policies** and **technical controls** with CIA goals (e.g., encryption policies, authentication, redundancy).
- Regularly **review** and **audit** to ensure these controls remain effective as the environment evolves.

Lancaster University

Security Design Principles

Security Design Principles

Lancaster University

Foundations for Building Trustworthy Systems:

- Saltzer J. and Schroeder M. (1974), **The Protection of Information in Computer Systems**

Key Insight:

- These eight timeless principles guide secure software and system design, bridging the gap from 1974 to modern-day challenges.

Eight Security Design Principles

In Lecture Activity

Lancaster University

- Review the security principles
- Mark the ones you are already familiar with
- Take **3 minutes** to chat with a person next to you about:
  - The principles you are already using
  - The principles you are not familiar with
  - Your experience with using one of the principle (positive and negative)

In Lecture Activity

- Review the security principles
- Mark the ones you are already familiar with
- Take **3 minutes** to chat with a person next to you about:
  - The principles you are already using
  - The principles you are not familiar with
  - Your experience with using one of the principle (positive and negative)

Economy of Mechanism

Lancaster University

Economy of Mechanism

- **Core Idea**: Keep designs as simple and small as possible, reducing the chance of errors
- Reuse simple good quality components/libraries
- **Example**:
  - ***Robotics*:** A manipulator with minimal firmware complexity is easier to audit. Overly complex code could hide vulnerabilities that allow an attacker to seize control

- **Why It Matters**: Less code → fewer paths → fewer bugs → simpler verification

Fail-Safe Defaults

Lancaster University

Fail-Safe Defaults

- **Core Idea**: Deny by default; only grant access if explicitly allowed
- A conservative design must be based on arguments **why objects should be accessible**, rather than **why they should not**
- **Example**:
  - ***IoT Door Locks*:** Default state is “locked” unless credentials are valid. Minimizes the chance of accidental unlock or unauthorized access

- **Why It Matters**: Mistakes or overlooked details tend to revert the system to *safe* behaviour instead of wide-open

Complete Mediation

Lancaster University

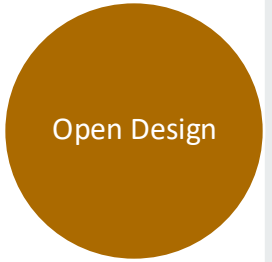
Complete Mediation

- **Core Idea**: Every request for a resource must be checked for authorization—no cached “shortcuts”
- It forces a system-wide view of access control, which in addition to normal operation includes **initialization**, **recovery**, **shutdown**, and **maintenance**
- **Example**:
  - ***Autonomous Vehicles*:** Each sensor reading or software module request is re-validated to avoid stale permissions. Prevents attackers from gaining indefinite access by forging a single token

- **Why It Matters**: Eliminates “once you’re in, you’re in forever” scenarios

Open Design

Lancaster University



- **Core Idea**: Open Design stresses transparency in security. Don't rely on "security by obscurity"
- Mechanisms can be public; **keys** or **passwords** remain secret
- **Example**:
  - ***Cryptography Standards*:** AES and RSA are openly published, peer-reviewed. Security is in the *keys*, not the hidden algorithm

- **Why It Matters**: Encourages robust, peer-reviewed designs that stand up to public scrutiny

Separation of Privilege

Lancaster University

- **Core Idea**: Divide power so no single entity alone has enough authority to compromise the system
- **Example**:
  - ***Banking or Industrial Controls*:** Transactions or equipment changes require approvals from multiple roles
  - ***Drone Fleet Management*:** Launch or route changes need both a pilot credential and a system admin credential
- **Why It Matters**: Reduces insider threats and accidental misuse

Defence in Depth (linked to Separation of Privilege)

Lancaster University

Separation of Privilege

- As a strategy, it involves multiple layers of security controls to protect assets
- If **one layer of security fails**, the other layers will still be able to protect the asset
  - Physical security, network security, application security, and data security
- **Goal:** to create a secure environment that is resilient to attack and can quickly detect and respond to any security incidents

- Multiple layers of security can:
  - Reduce the risk of a successful attack
  - Minimize the damage caused

Least Privilege

Lancaster University

- **Core Idea**: A subject (user or process) should have the minimal privileges necessary for its task
- **Example**:
  - ***Robotics as a Service*:** Each robot or AI microservice gets only the permissions needed (e.g., read sensor data, can't write to system logs or databases unnecessarily)

- **Why It Matters**: Limits damage if an account is compromised—attackers can't escalate to full control

Least Common Mechanism

Lancaster University

- **Core Idea**: Minimize shared resources/mechanisms used by multiple components
- **Example**:
  - ***Cloud Microservices*:** Each microservice has its own database credentials rather than a single, universal “DB admin” credential

- **Why It Matters**: One compromised shared mechanism can become a single point of failure for the entire system

Psychological Acceptability

Lancaster University

- **Core Idea**: Security must be user-friendly to be adopted.
- Usability and security are sometimes overlooked.
- **Example**:
  - ***MFA (Multi-Factor Authentication)*:** If it's too cumbersome or slow, users find workarounds. Balanced design leads to strong adoption.

- **Why It Matters**: The best security fails if users avoid or bypass it due to complexity.

Modern Applications of the 8 Principles

Lancaster University

- **Robotics:** Secure firmware updates (Fail-Safe Defaults + Complete Mediation)
- **Autonomous Vehicles:** Separation of safety-critical code from infotainment (Least Privilege + Separation of Privilege)
- **AI Pipelines:** Training data integrity checks, digital signatures on ML models (Integrity + Complete Mediation)
- **IoT & Edge Devices:** Minimizing firmware complexity (Economy of Mechanism)
- **Human Factors:** Easy-to-use password managers (Psychological Acceptability)

Lancaster University

Immutable Laws of Security

Immutable Laws of Security

- **Brief History**: Originally published by Microsoft in 2001 (updated in 2009), aimed at common-sense truths in security.
- **New Version (2023)**: Reflects shifts in threat actors, cloud computing, IoT, AI, and zero-trust approaches.
- **Why These Laws Matter**: They capture foundational patterns—both technical and human—that continue to shape security best practices.

The 2009 Immutable Laws of Security

Lancaster University

- Law #1: If a bad guy can persuade you to run his program, it's not your computer anymore.
- Law #2: If a bad guy can alter the OS, it's not your computer anymore.
- Law #3: If a bad guy has unrestricted physical access, it's not your computer anymore.
- Law #4: If you let a bad guy upload programs to your website, it's not your website anymore.
- Law #5: Weak passwords trump strong security.
- Law #6: A computer is only as secure as the administrator is trustworthy.
- Law #7: Encrypted data is only as secure as the decryption key.
- Law #8: An out-of-date virus scanner is only marginally better than none.
- Law #9: Absolute anonymity isn't practical (online or offline).
- Law #10: Technology is not a panacea.

Law #1: If a bad guy can persuade you to run his program, it's not your computer anymore.

Law #2: If a bad guy can alter the OS, it's not your computer anymore.

Law #3: If a bad guy has unrestricted physical access, it's not your computer anymore.

Law #4: If you let a bad guy upload programs to your website, it's not your website anymore.

Law #5: Weak passwords trump strong security.

Law #6: A computer is only as secure as the administrator is trustworthy.

Law #7: Encrypted data is only as secure as the decryption key.

Law #8: An out-of-date virus scanner is only marginally better than none.

Law #9: Absolute anonymity isn't practical (online or offline).

Law #10: Technology is not a panacea.

Why Revisit the Laws in 2023?

Lancaster University

- **Changing Threat Landscape:** Rise of ransomware, cloud-based services, IoT, AI-driven attacks
- **Business & Productivity Pressures:** The push to move fast often outruns security measures
- **Shared Responsibilities:** From “individual PC admin” to “team sport,” zero-trust, and collaborative defences
- **ROI of Attacks:** Cybercrime is more organized and profit-driven than ever

The (New) Immutable Laws of Security (2023)

Lancaster University

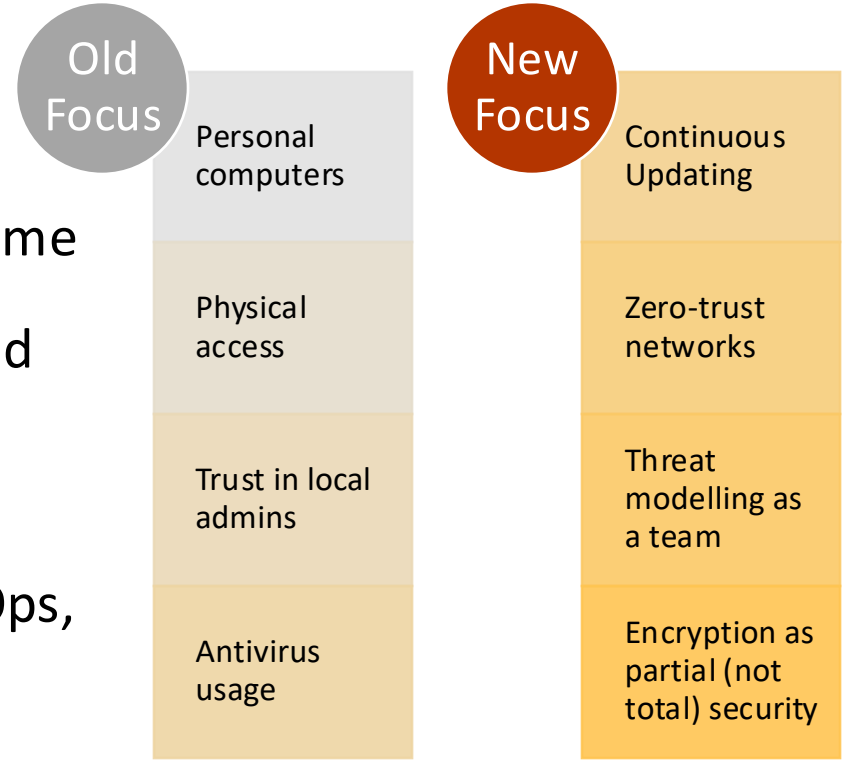
- Law #1: Security success is ruining the attacker's return on investment (ROI).
- Law #2: Not keeping up is falling behind.
- Law #3: Productivity always wins.
- Law #4: Attackers don't care.
- Law #5: Ruthless prioritization is a survival skill.
- Law #6: Cybersecurity is a team sport.
- Law #7: Your network isn't as trustworthy as you think it is.
- Law #8: Isolated networks aren't automatically secure.
- Law #9: Encryption alone isn't a data protection solution.
- Law #10: Technology doesn't solve people and process problems.

- [ ] Law #1: Security success is ruining the attacker’s return on investment (ROI).
- [ ] Law #2: Not keeping up is falling behind.
- [ ] Law #3: Productivity always wins.
- [ ] Law #4: Attackers don’t care.
- [ ] Law #5: Ruthless prioritization is a survival skill.
- [ ] Law #6: Cybersecurity is a team sport.
- [ ] Law #7: Your network isn’t as trustworthy as you think it is.
- [ ] Law #8: Isolated networks aren’t automatically secure.
- [ ] Law #9: Encryption alone isn’t a data protection solution.
- [ ] Law #10: Technology doesn’t solve people and process problems.

What's Changed & What's the Same?

Lancaster University

- **Physical vs. Virtual**:
  - Then: If an attacker physically touches your machine, game over
  - Now: Attackers might never be physically present—cloud breaches, remote exploits, supply chain intrusions
- **Local Admin** vs. **Team Sport**:
  - Then: One admin could make or break security
  - Now: Security requires cross-team collaboration—DevOps, cloud architects, compliance officers, etc
- **Antivirus** vs. **Ongoing Patch & Monitor**:
  - Then: Keeping AV updated was big
  - Now: Ongoing patching, threat intelligence, and real-time monitoring are crucial



Bringing the Laws into Your Daily Security Practice

Lancaster University

- **Raise the Cost for Attackers:** (Law #1) Use multi-factor authentication, frequent patching, network segmentation
- **Stay Current:** (Law #2) Ongoing training, threat intelligence, and adopting latest security frameworks (e.g., zero-trust)
- **Balance Security & Productivity:** (Law #3) Implement user-friendly solutions or they'll be bypassed
- **Attackers Don't Care:** (Law #4) They'll exploit any gap—human, process, or technical
- **Prioritize Ruthlessly:** (Law #5) Tackle highest-impact risks first.
- …and so on for each new law

Key Takeaways

Lancaster University

- **Security is Holistic**
  - Encompasses **people**, **processes**, and **technology**—no single tool or policy stands alone
- **CIA Triad Remains Foundational**
  - Ensuring Confidentiality, Integrity, and Availability applies across software, hardware, and cloud/IoT environments
- **Timeless Principles Still Matter**
  - Saltzer & Schroeder's guidelines and the (new) Immutable Laws of Security continue to guide robust system design
- **Preventive & Adaptive**
  - Security is not a "set-and-forget" effort—it needs **continuous monitoring**, **patching**, and **evolution**

Future Outlook

- **AI & Robotics:**
  - As automation and machine learning advances, **adversarial AI attacks** and **robotic system vulnerabilities** demand stronger safeguards
- **Zero-Trust & Beyond**
  - Shifting from perimeter-focused security to **zero-trust architectures**, emphasizing **continuous verification**
- **Quantum-Ready Security**
  - Preparing for a future where **quantum computing** may break current cryptographic standards
- **Collaboration is Key**
  - **Cross-disciplinary teamwork** (security experts, developers, operations, legal) is essential for proactive defence
- **Ongoing Education & Awareness**
  - Threat landscapes evolve daily—regular **training**, **threat intelligence**, and **best-practice sharing** keep defences resilient

Lancaster University

Thank you for listening, any questions?