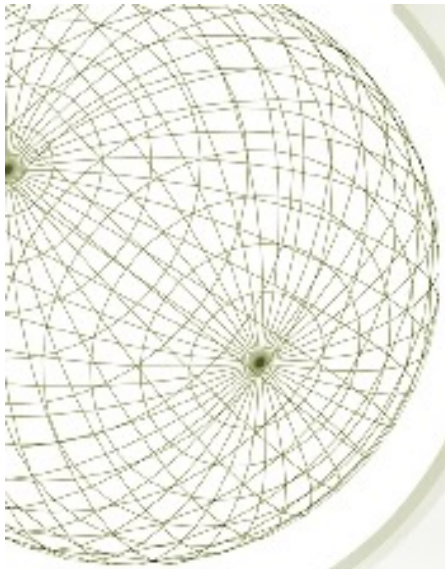
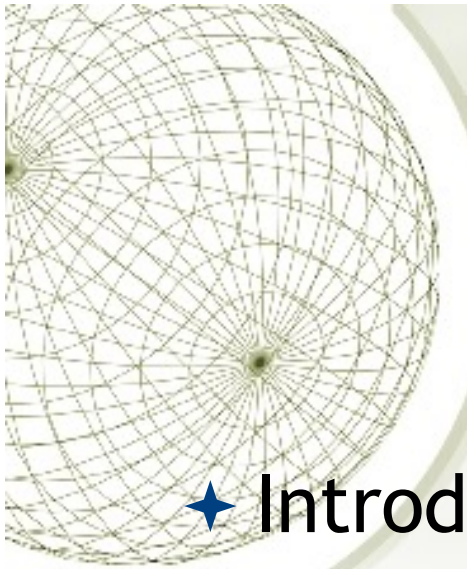


1DV700
Computer Security

Ola Flygt
Linnaeus University, Sweden
http://homepage.lnu.se/staff/oflmsi/
Ola.Flygt@lnu.se
+46 470 70 86 49

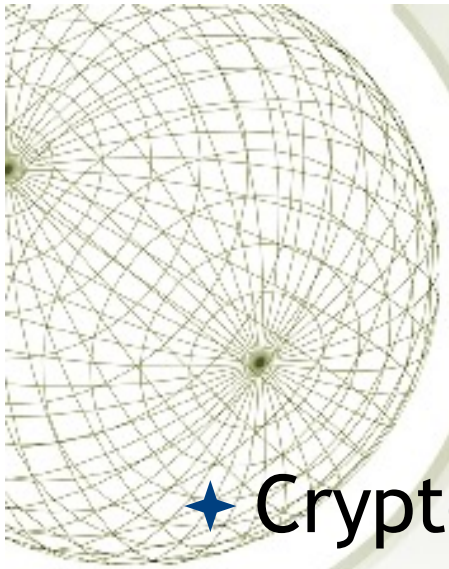
Introduction and overview

- What is computer (and network) security?
- Course philosophy and goals
- High-level overview of topics
- Course organization and information



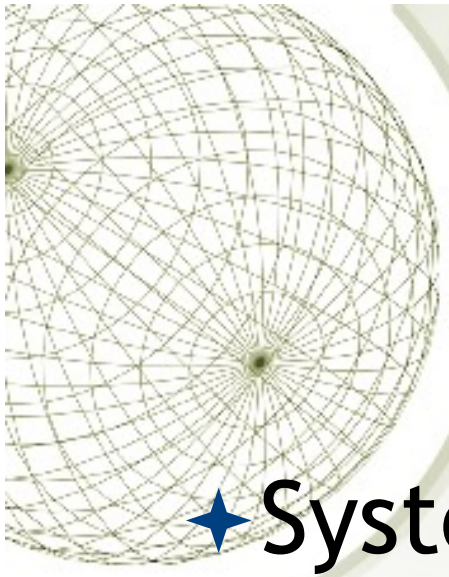
High-level overview

- Introduction…
  - What do we mean by security?
  - Is security achievable…?



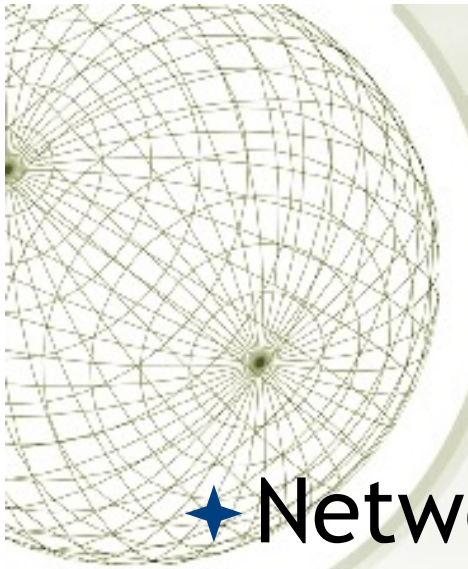
High-level overview

- Cryptography
  - Cryptography is not the (whole) solution…
  - …but is is an important part of the solution
  - Along the way, we will see why cryptography can't solve all security problems



High-level overview

- System security
  - General principles
  - Security policies
  - Access control; confidentiality/integrity
  - OS security

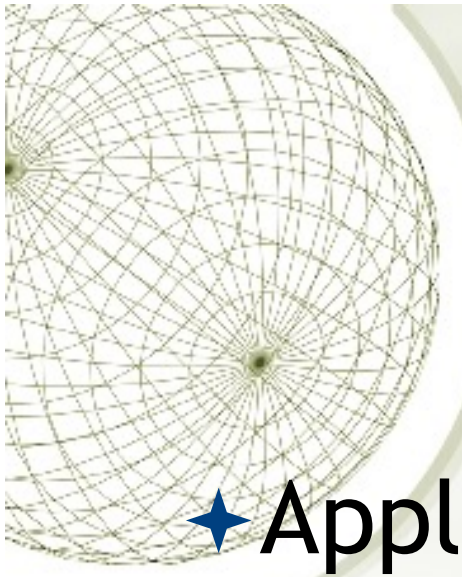


High-level overview

- Network security (only briefly covered)
  - Identity
  - Authentication and key exchange protocols
  - Anonymity and pseudonymity
  - Some real-world protocols

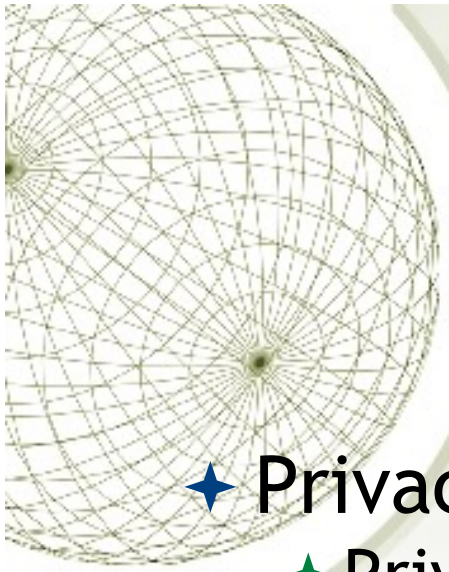
High-level overview

- Database security
  - Introduction to databases
  - Security requirements
  - Inference attacks
  - Protection for databases



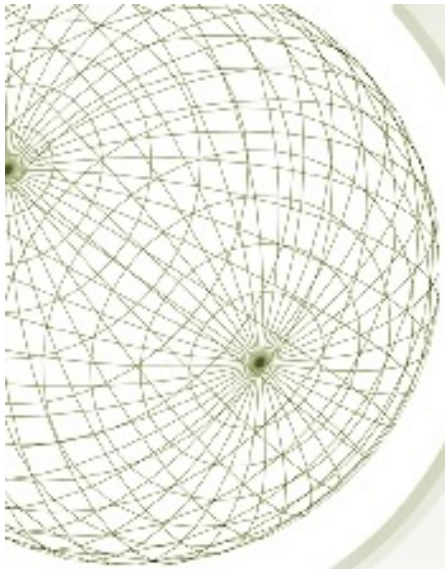
High-level overview

- Application-level security
  - Web-based security
  - Buffer overflows; secure programming and sandboxing
  - Viruses, worms, and malicious code

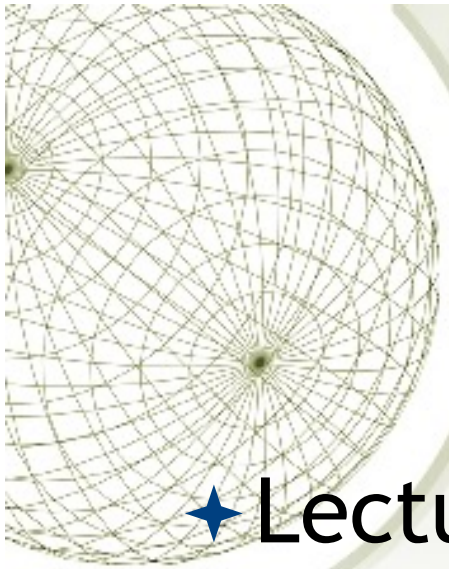


High-level overview

- Privacy
  - Privacy concerns and regulations
  - GDPR
- Managing security
  - Security standards
  - Risk analysis
  - Security planning
- Legal Issues and Ethics
  - Computer crime
  - Ethical Issues in Computer Science

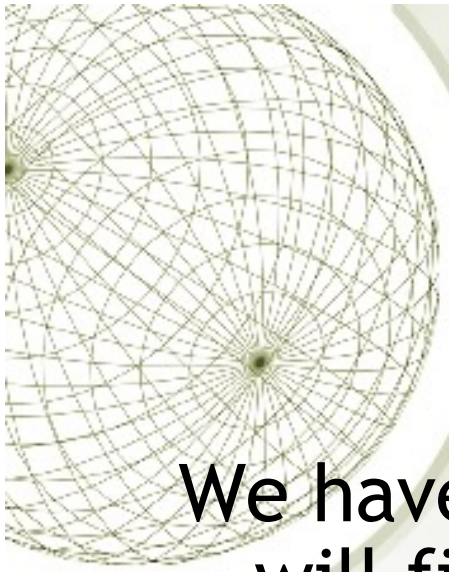


Course Organization



Staff

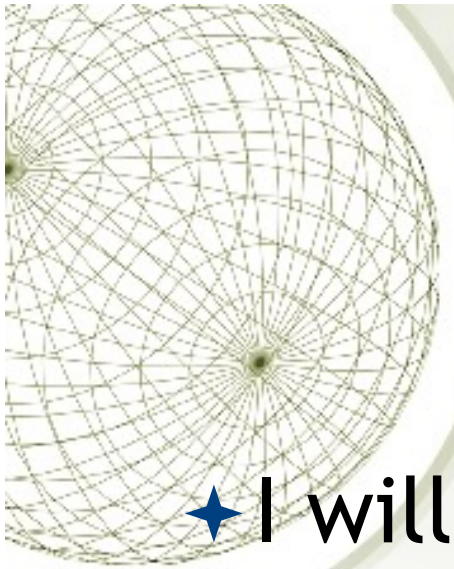
- Lectures
  - Ola Flygt
  - Hemant Ghayvat
  - Faiz Ul Muram
- Teaching assistants (several)
- Contact information found in Moodle



Course webpage

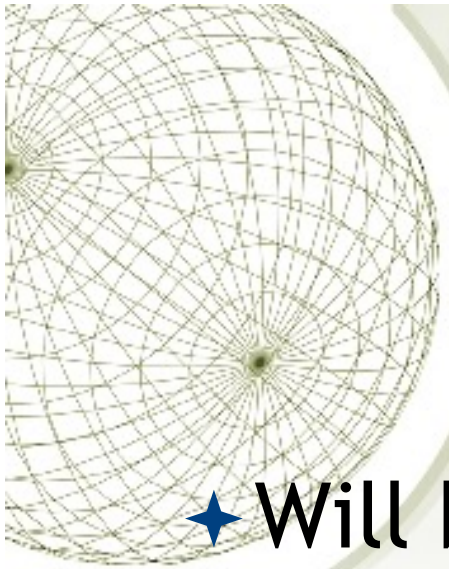
We have a course room in MyMoodle. Here you will find previous exams, assignments, links to the Time table etc.

- Slides will be posted for convenience, but no substitute for attending lecture and reading the textbook
- Practical assignments are distributed and submitted in Moodle
- Check often for announcements and changes in the time table and the MyMoodle room and on slack



Textbook

- I will primarily use one textbook:
  - "Security in Computing" by Pfleeger and Pfleeger 5th ed. but you can also use the 4th ed.
- Buy it!



Other readings

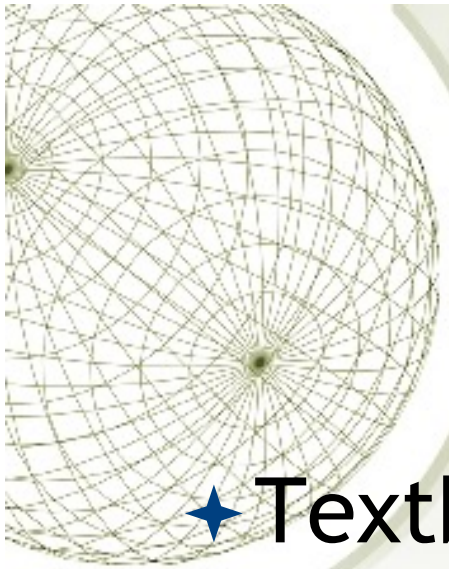
- Will be linked from Moodle or handed out
- Material from these readings is fair game for the exams, even if not covered in class (unless stated otherwise)
- Please suggest other readings or relevant news articles!

Course requirements

- Practical work
  - 3 assignments throughout the course period
  - Details about these to come
  - At the end of the course there will also be a written exam

Philosophy

- We are by no means going to be able to cover everything, the area is huge!
- Main goals
  - Exposure to different aspects of security; meant mainly to “pique” your interest
  - The “mindset” of security: a new way of thinking…
  - Become familiar with basic crypto, acronyms (RSA, SSL, PGP, etc.), and “buzzwords”
  - An emphasis on Computer Security



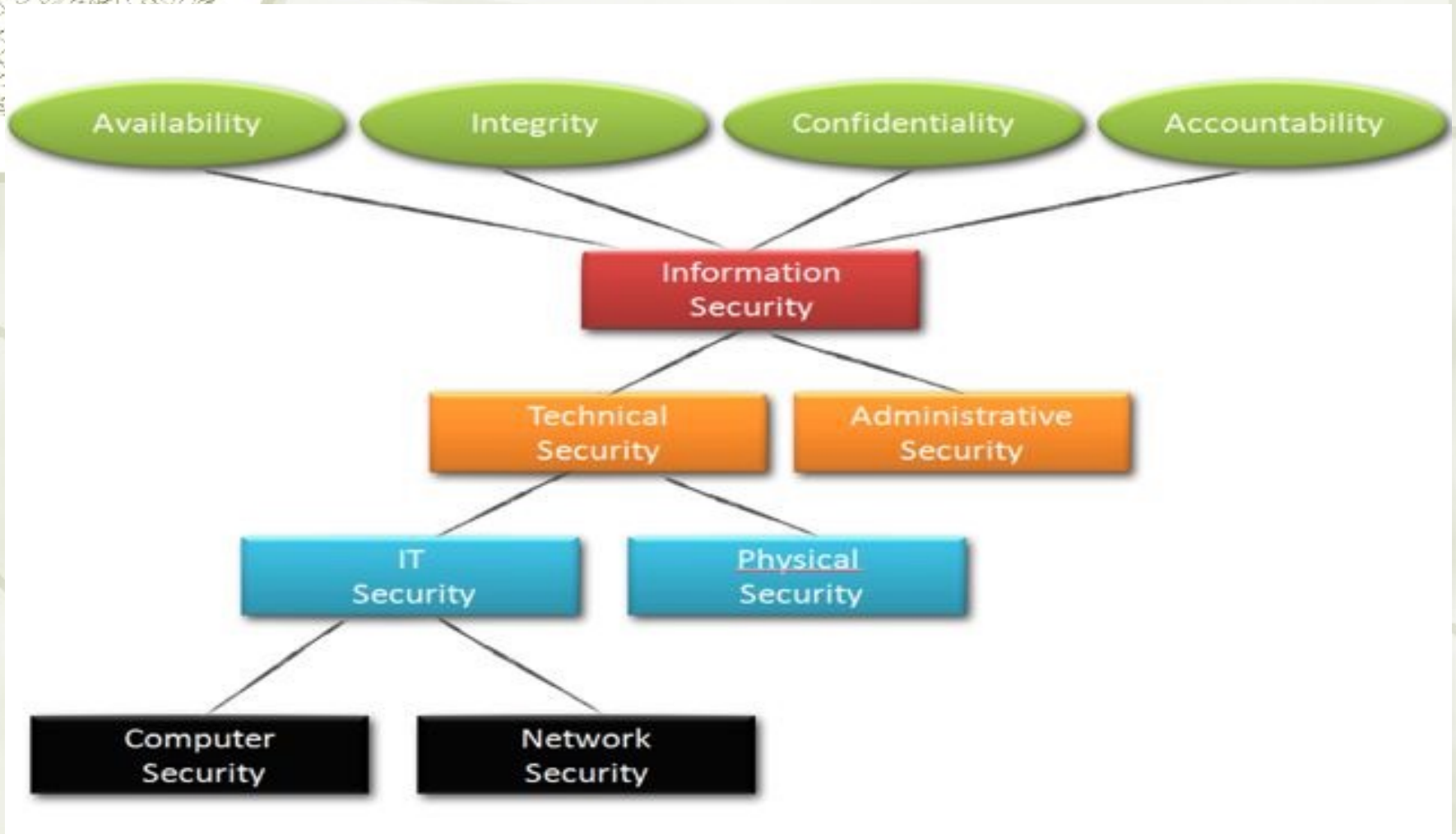
Student participation (I hope!)

- Textbook chapters and papers distributed
  - Read these before class and come prepared to discuss
- Monitor the media
  - Post relevant/interesting stories in the the slack channel
- Class participation counts!

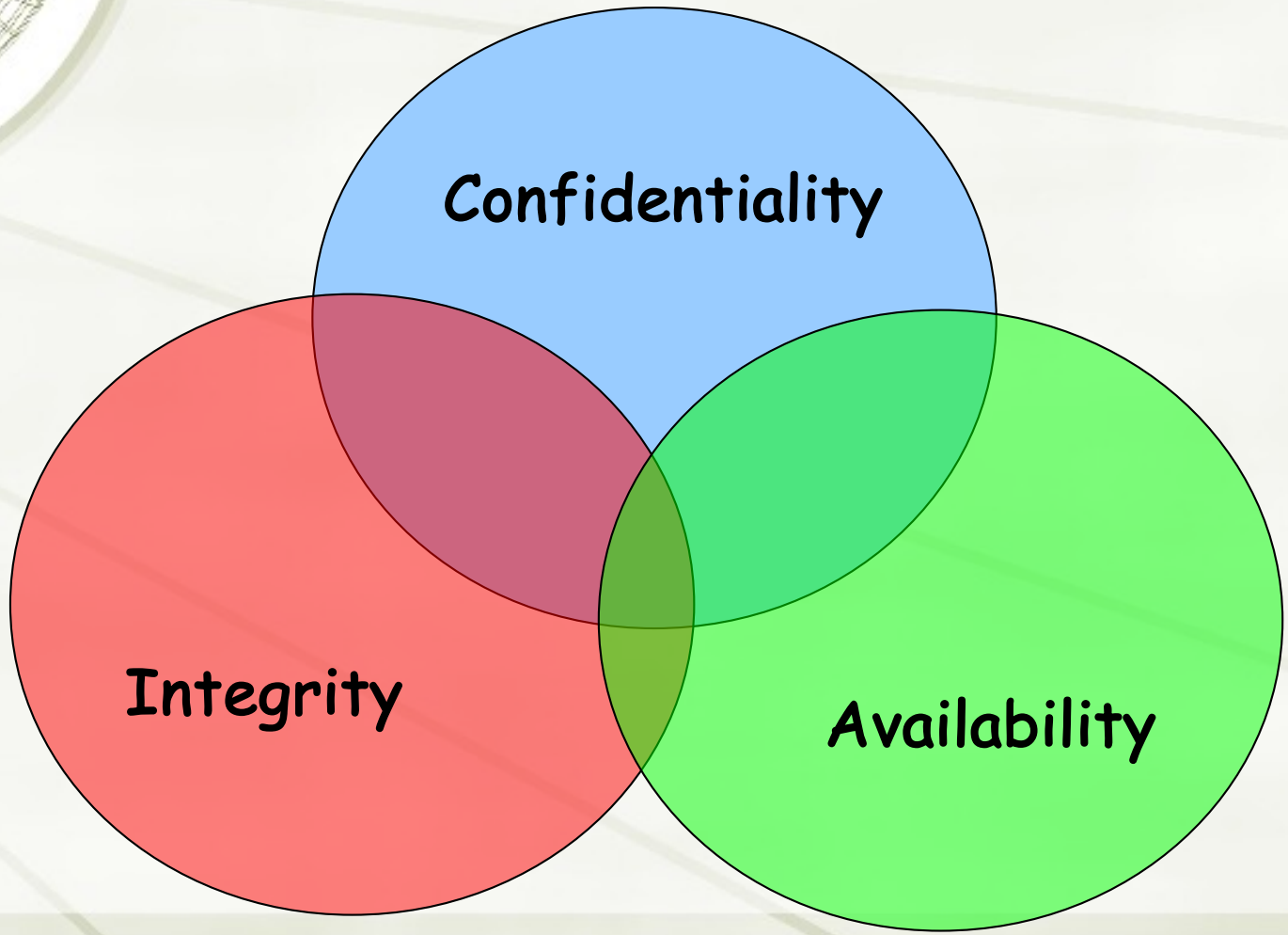
Introduction to Security

- Most of computer science is concerned with achieving desired behavior
- In some sense, security is concerned with preventing undesired behavior
  - Different way of thinking!
  - An enemy/opponent/hacker/adversary may be actively and maliciously trying to circumvent any protective measures you put in place
  - In other situations disasters or blunders create the undesired behaviour

The information security domain



Security Goals the CIA model



Some terminology

- CIA are the main goals
  - Confidentiality – keeping information secret
  - Integrity – making sure the information is correct
  - Availability – ensuring you can access the information when needed
- Other goals are often added
  - Authentication, authorization etc.
- Sometimes, the goals are conflicting …

"We are all Security Customers"

- Security is *always* a trade-off
- The goal should not be "to make the system as secure as possible"…
- …but instead, "to make the system as secure as possible *within certain constraints*" (cost, usability, convenience etc.)

Cost-benefit analysis

- Important to evaluate what level of security is necessary/appropriate
  - Cost of mounting a particular attack vs. value of attack to an adversary
  - Cost of damages from an attack vs. cost of defending against the attack
  - Likelihood of a particular attack

Assets

Hardware:

- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:

- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)
- Individual applications

Data:

- Documents
- Photos
- Music, videos
- Email
- Class projects

Values of Assets

Off the shelf;
easily replaceable

Hardware:
- Computer
- Devices (disk drives, memory, printer)
- Network gear

Software:
- Operating system
- Utilities (antivirus)
- Commercial applications (word processing, photo editing)

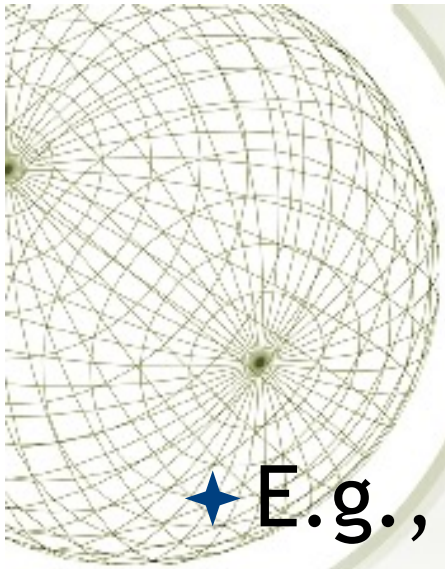
Data:
- Documents
- Photos
- Music, videos
- Email
- Class projects

- Individual applications

Unique; irreplaceable

"More" security not always better

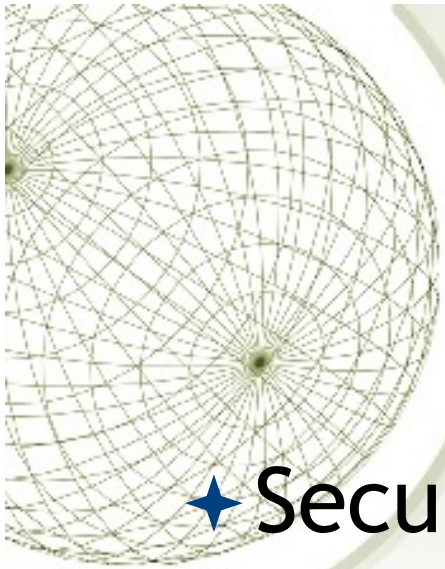
- "No point in putting a higher post in the ground when the enemy can go around it"
  - Need to identify the *weakest link*
  - Security of a system is only as good as the security at its weakest point…
- Security is not a "magic bullet"
- Security is a process, not a product



Human factors

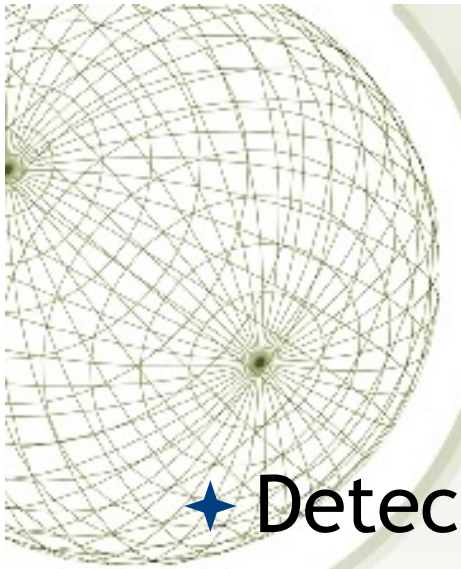
- E.g., passwords…
- Outsider vs. insider attacks
- Software misconfiguration
- Not applying security patches
- Social engineering
- Physical security

Movie time!



Importance of precise specification

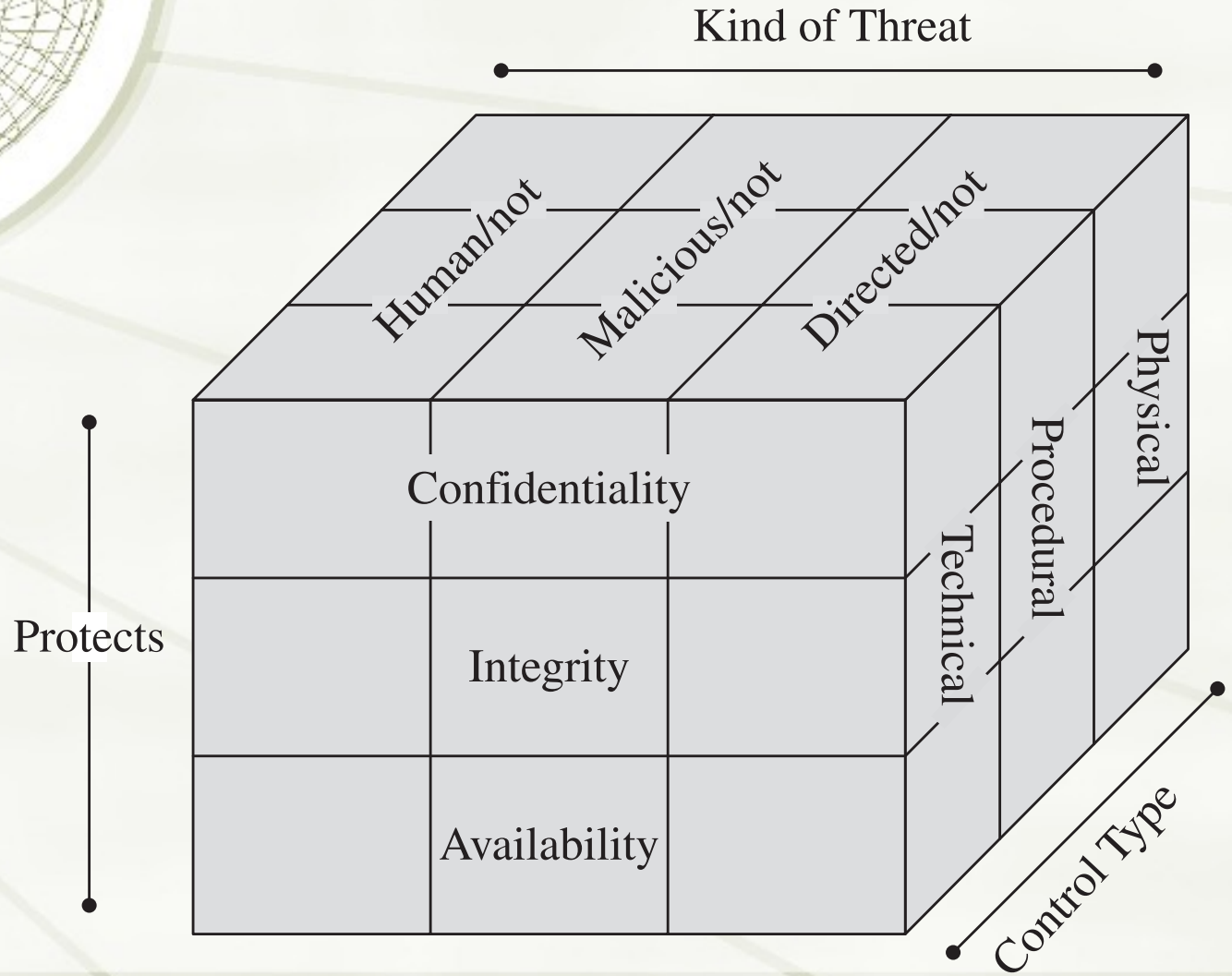
- Security policy
  - Statement of what is and is not allowed
- Security services
  - General methods for enforcing a security policy
- Security mechanism
  - Specific tools that implement the services
- One is meaningless without the other…



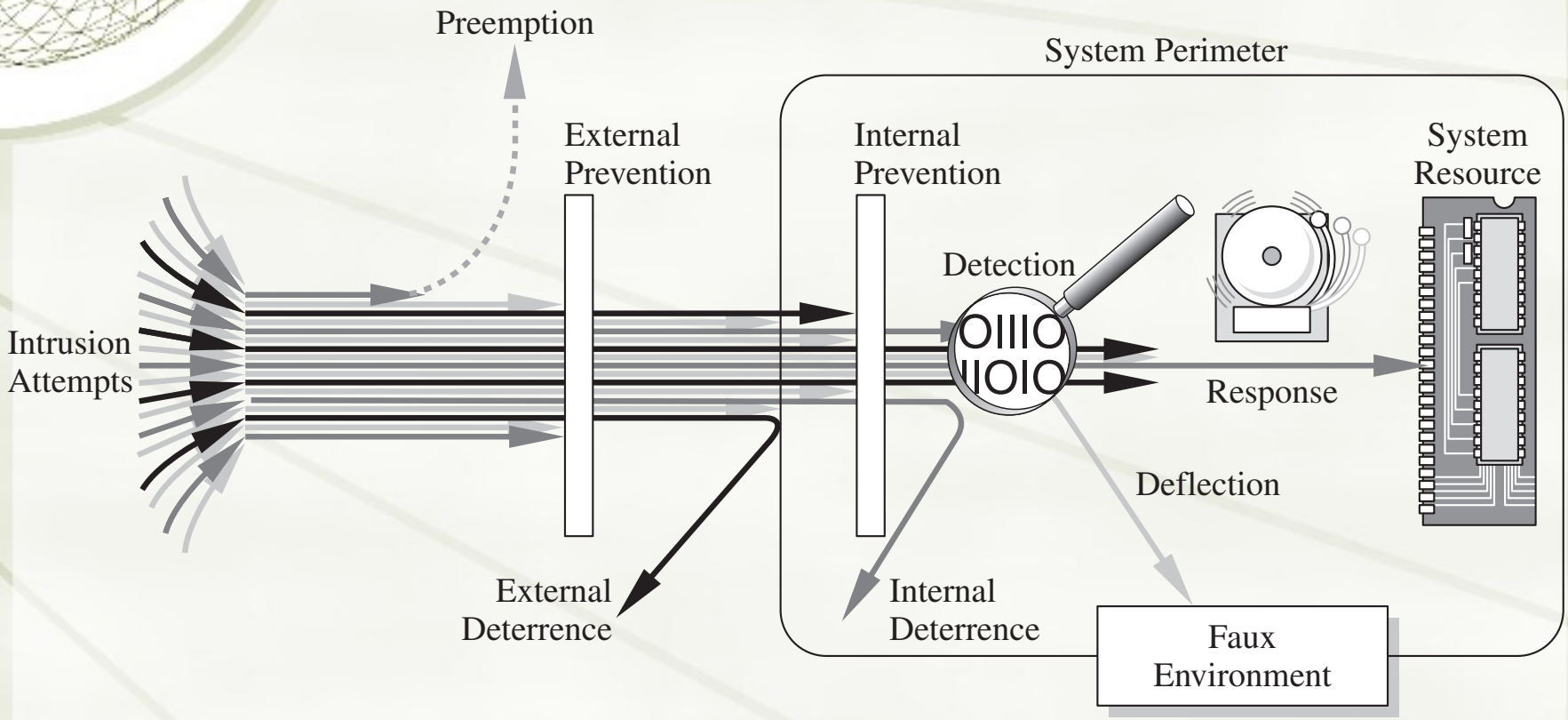
Prevention - not the only concern

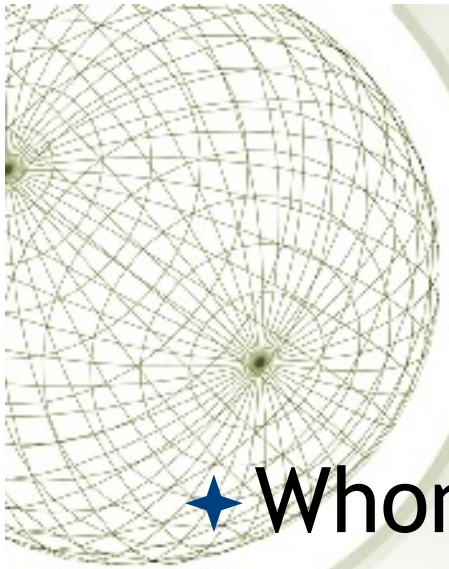
- Detection and response
  - How do you know when you are being attacked?
  - How quickly can you stop the attack?
  - Can you prevent the attack from recurring?
- Recovery
  - Can be much more important than prevention
- Legal issues?

Controls/Countermeasures



Multiple Controls

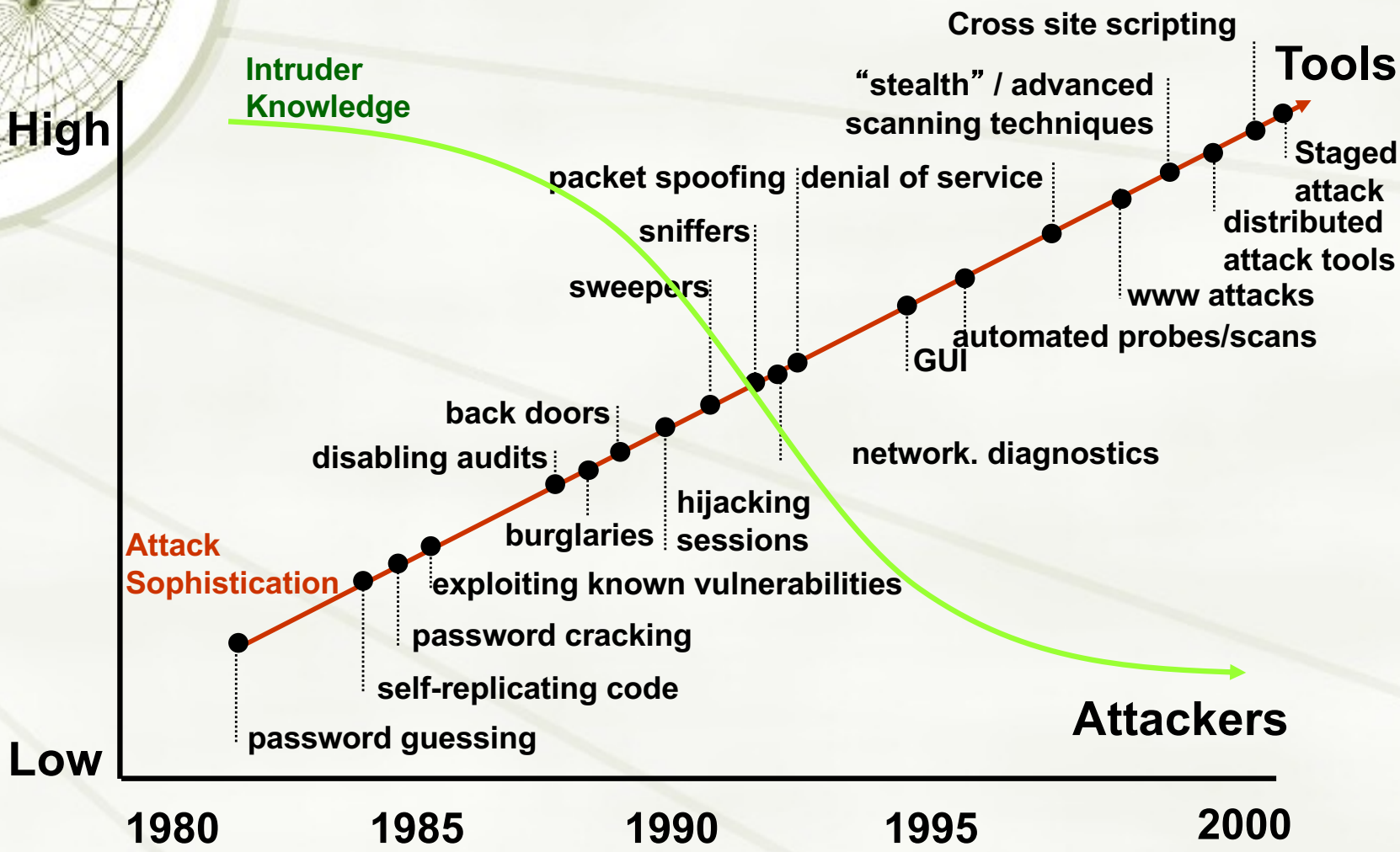




"Trusting trust"

- Whom do you trust?
- Does one really need to be this paranoid??
  - Probably not
  - Sometimes, yes….
- Shows that security is complex…and essentially impossible
- Comes back to risk/benefit trade-off

What are we up against?



What is the threat?

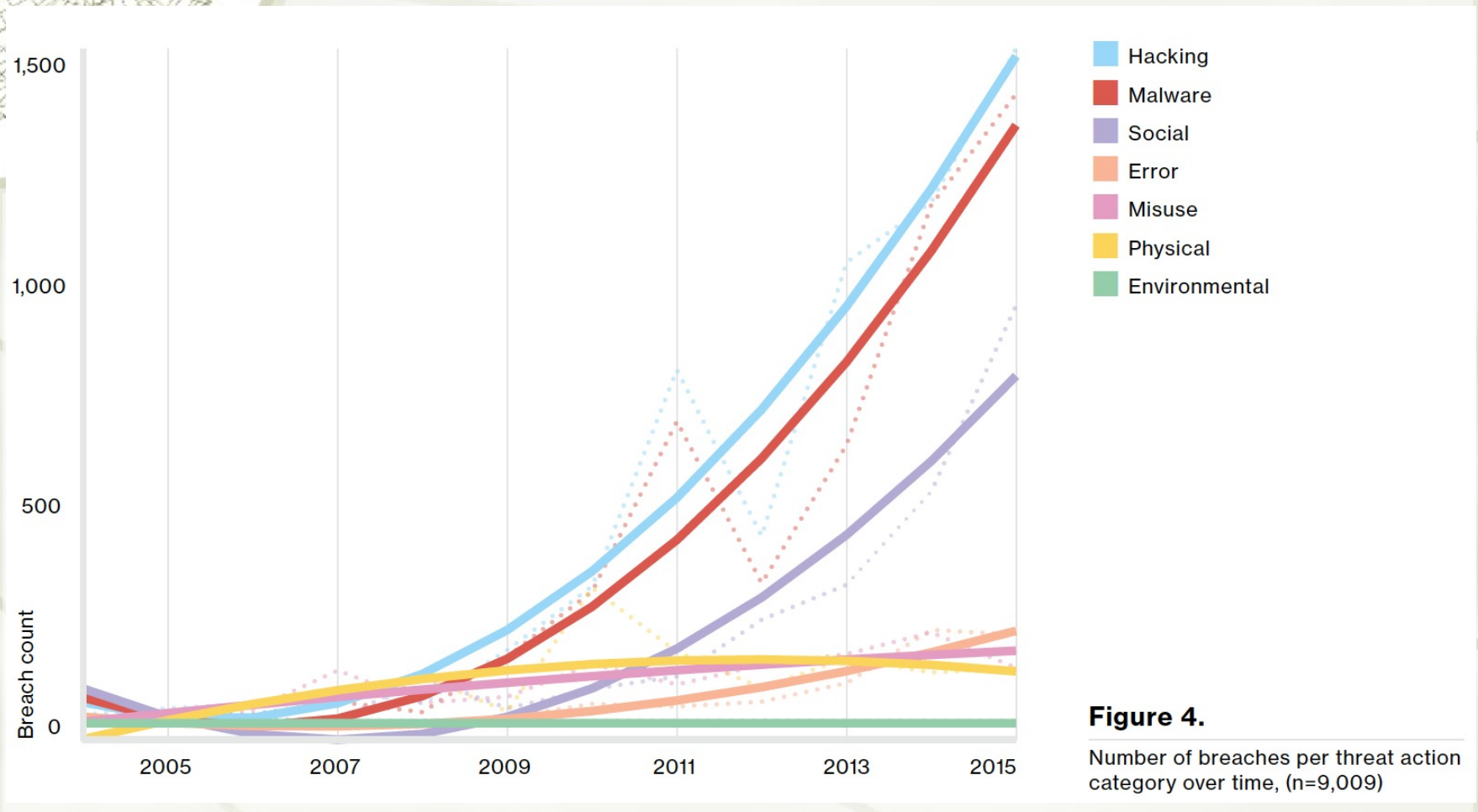


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

Figure from Verizon 2016 Data Breach Investigations Report

What is attacked?

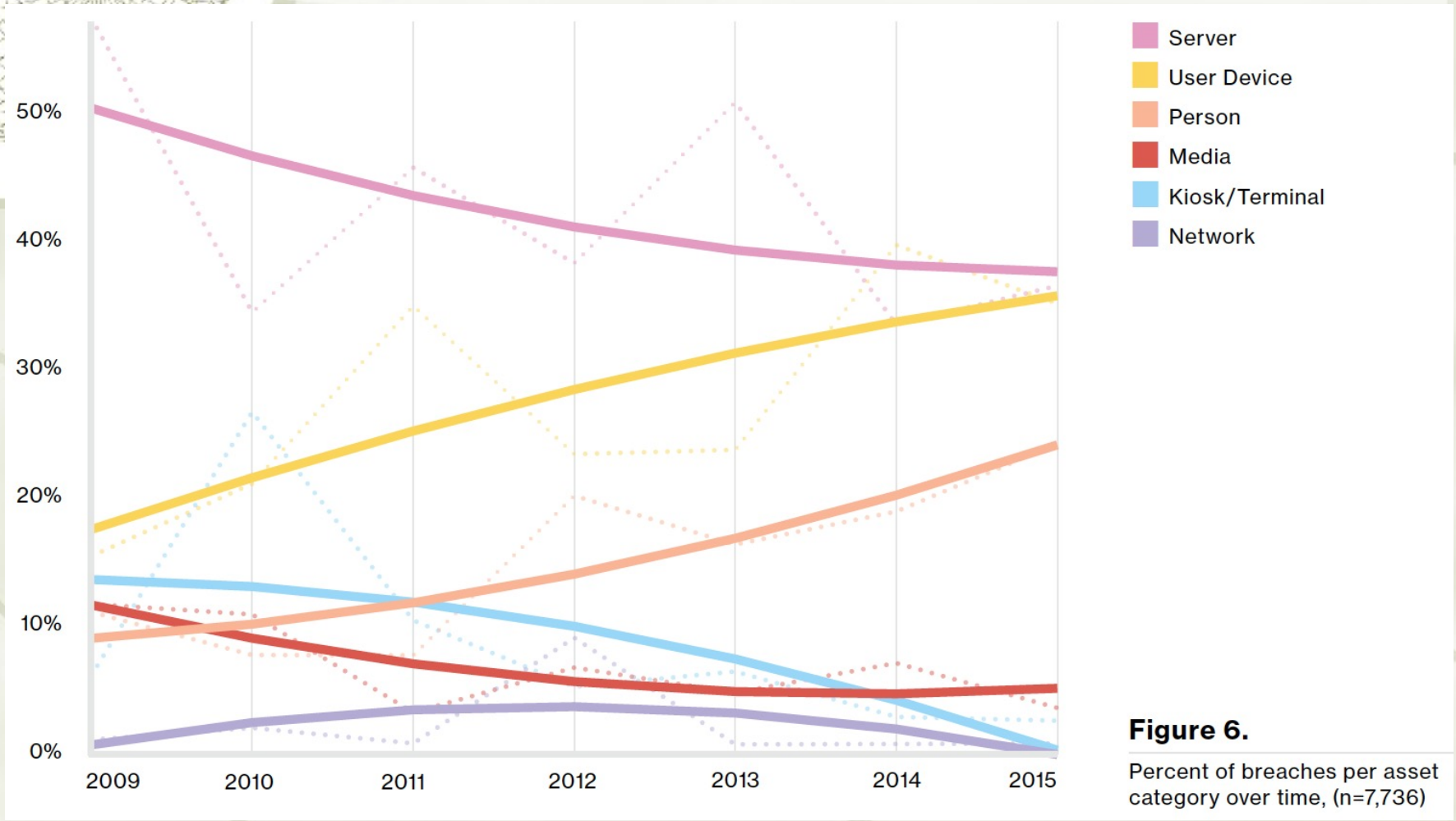


Figure 6.

Percent of breaches per asset category over time, (n=7,736)

Figure from Verizon 2016 Data Breach Investigations Report

Changes of incidents over time

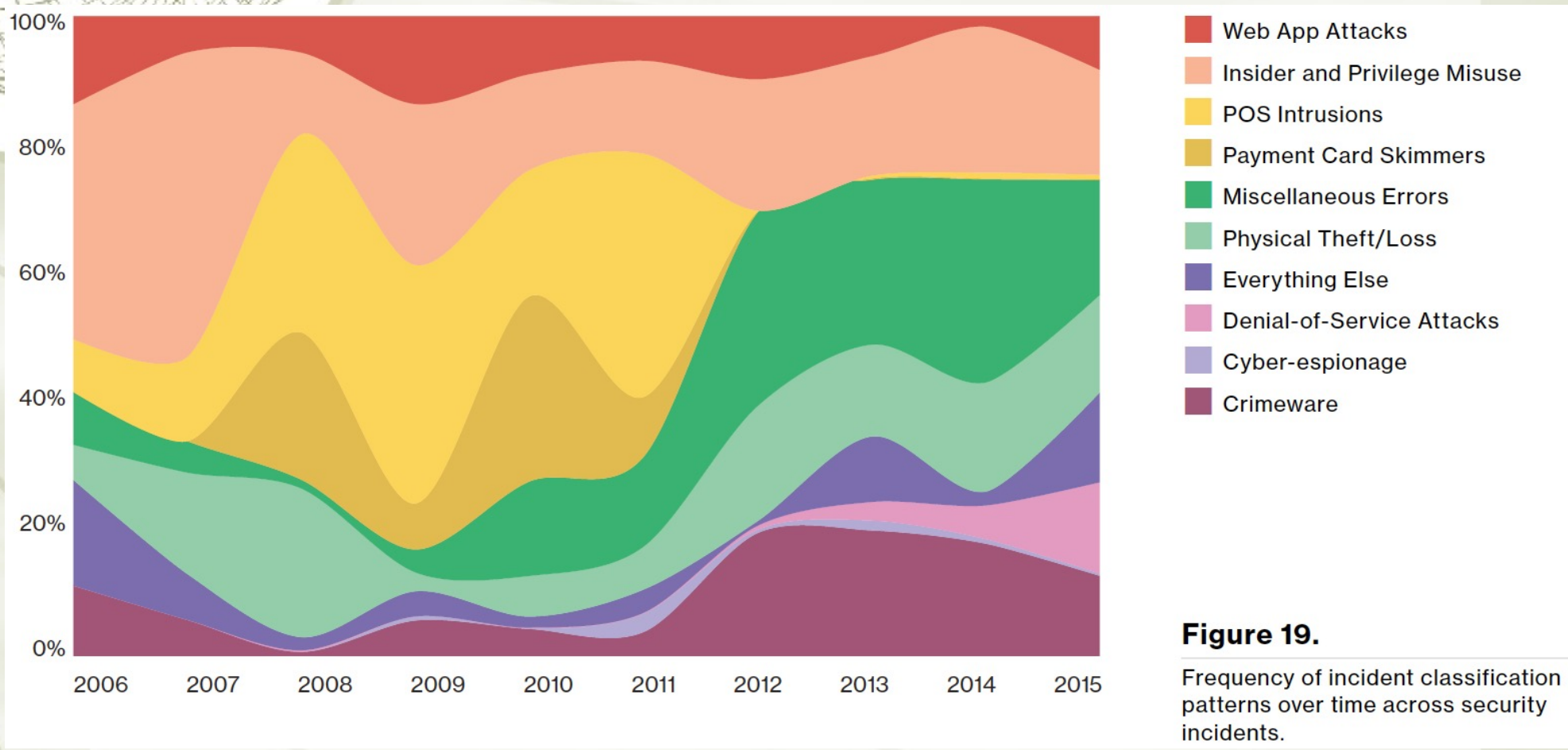


Figure 19.

Frequency of incident classification patterns over time across security incidents.

Figure from Verizon 2016 Data Breach Investigations Report

Confirmed data breaches over time

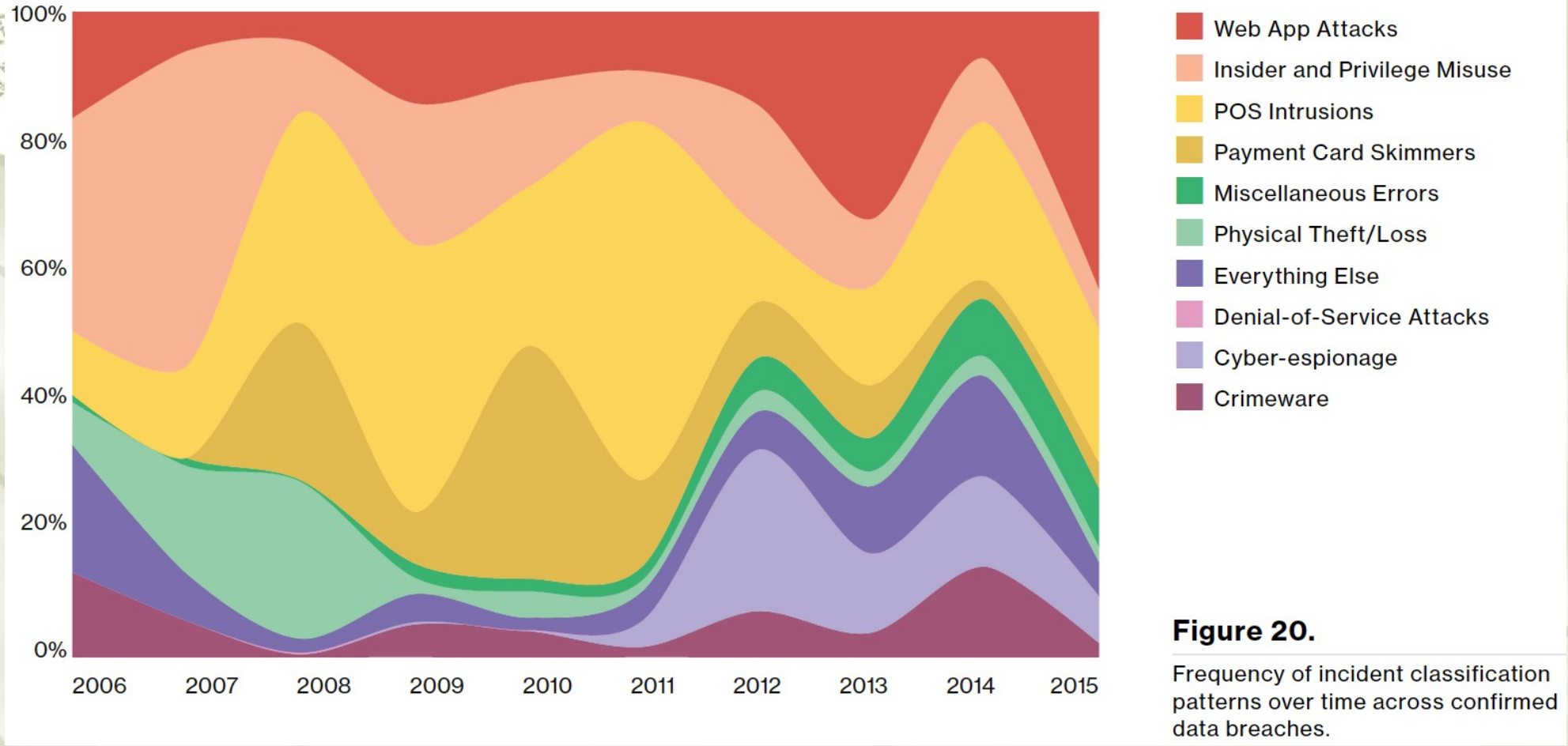


Figure 20.

Frequency of incident classification patterns over time across confirmed data breaches.

Figure from Verizon 2016 Data Breach Investigations Report

What is motivating the insider attacker?

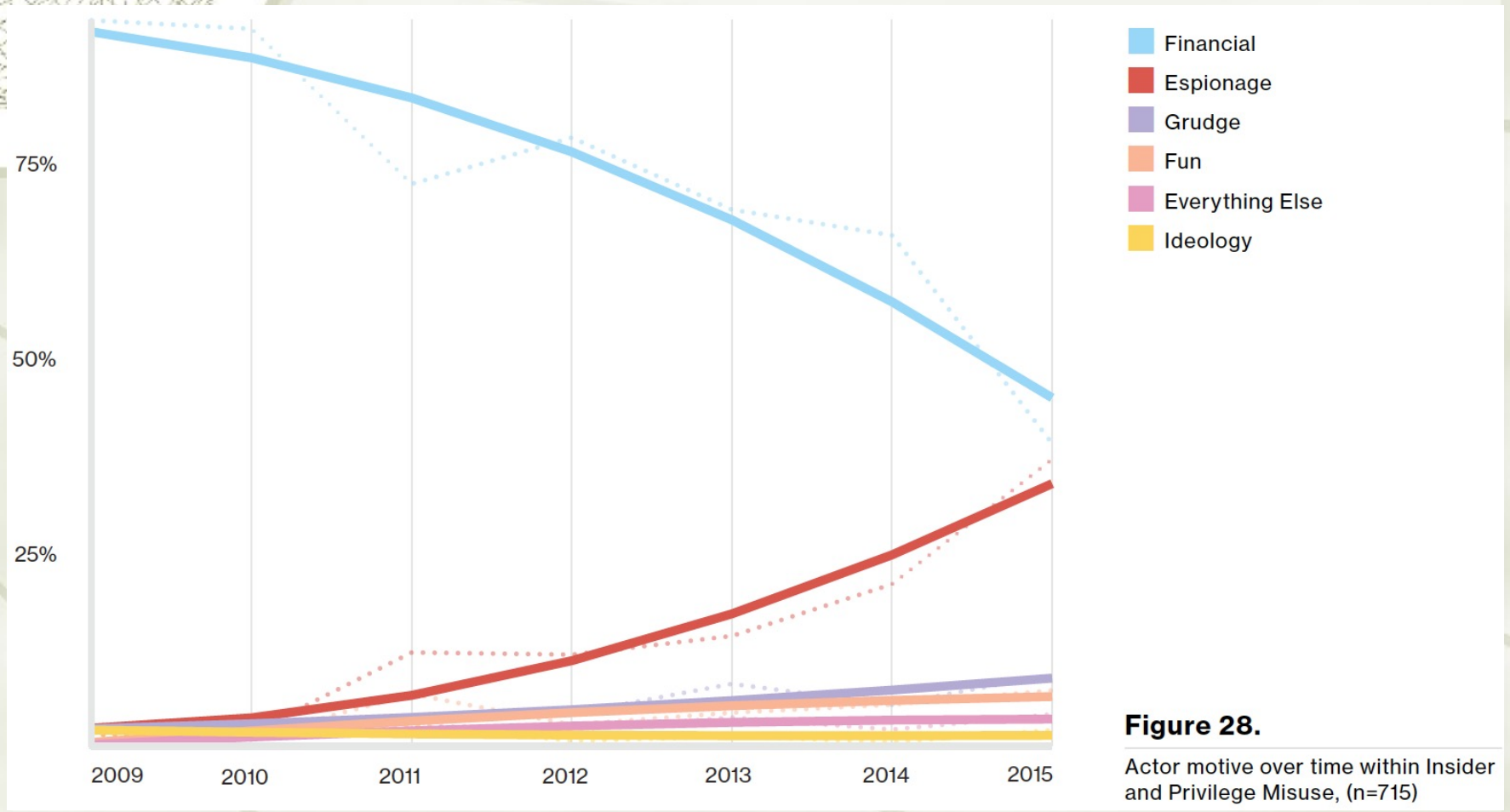


Figure 28.

Actor motive over time within Insider and Privilege Misuse, (n=715)

Figure from Verizon 2016 Data Breach Investigations Report

Conclusion

- In this course, we will focus on security in stand alone computer systems
- But important to keep in the back of your mind the previous discussion…

  …and if you decide to enter the security field, learn more about it!