

Security Engineering Problem Class 1

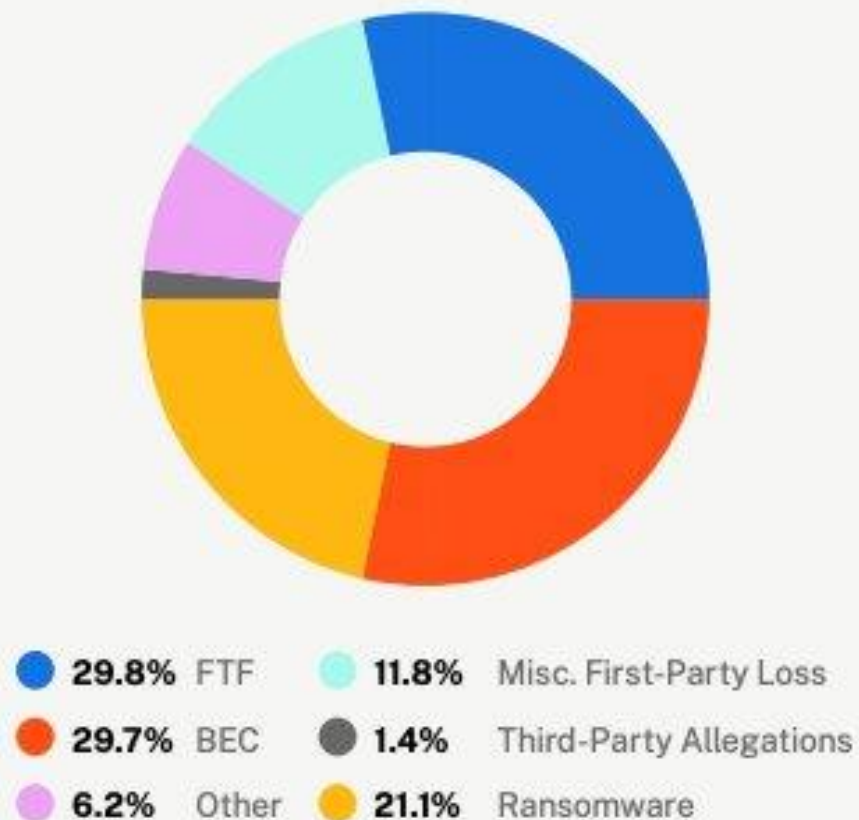
10/6/2026

Q1

To what extent do the findings in the FBI's IC3 report align with the cyber insurance claims from Lecture 1?

Q1

Claims by Event Type (Figure 1.3)



- Aligned on BEC/FTF at number 2, but diff names
- Not aligned on victims. FBI mostly individuals, insurance mostly corporations
- Ransomware much less common in FBI
 - Reporting incentives
- Companies are less likely to authorize fraud? More likely to face external "hacks"

2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints
Phishing/Spoofing	193,407
Extortion	86,415
Personal Data Breach	64,882
Non-Payment/Non-Delivery	49,572
Investment	47,919
Tech Support	36,002
Business Email Compromise	21,442
Identity Theft	21,403
Employment	20,044
Confidence/Romance	17,910
Government Impersonation	17,367
Credit Card/Check Fraud	12,876
Other	12,318

2024 CRIME TYPES *continued*

BY COMPLAINT LOSS

Crime Type	Loss
Investment	\$6,570,639,864
Business Email Compromise	\$2,770,151,146
Tech Support	\$1,464,755,976
Personal Data Breach	\$1,453,296,303
Non-Payment/Non-Delivery	\$785,436,888
Confidence/Romance	\$672,009,052
Government Impersonation	\$405,624,084
Data Breach	\$364,855,818
Other	\$280,278,325
Employment	\$264,223,271
Credit Card/Check Fraud	\$199,889,841
Identity Theft	\$174,354,745
Real Estate	\$173,586,820

Q2

- Lecture 1 suggests individuals should primarily worry about online fraud. What is an argument against this?

Q2

- It's not all about financial impact
- It ignores the specific harms that individuals face
 - Political actors vs the state
 - Hate and abuse online
 - Children and bullying (addiction?)
- Many frauds start with a data breach that allows reconnaissance

Q3

- All large software has bugs in it, and the most powerful nation-state actors will have a collection of zero-day attacks for all of the most popular systems.
- So why is installing the latest software updates still good security advice for most people despite this?

Q3

- Threat modelling matters
 - Spooks have powerful capabilities including 0days, but don't usually impose economic harm
 - Don't want to burn an 0day on a low value target
 - Instead they hoard data at a population level
 - Crooks far more likely to use n-days and this can lead to data breaches, ransomware, infostealer infections etc
 -

Q4

- What kind of actors should worry more about their machines being infected and used for botnets vs data theft/extortion?

Q4



BBC



NEWS

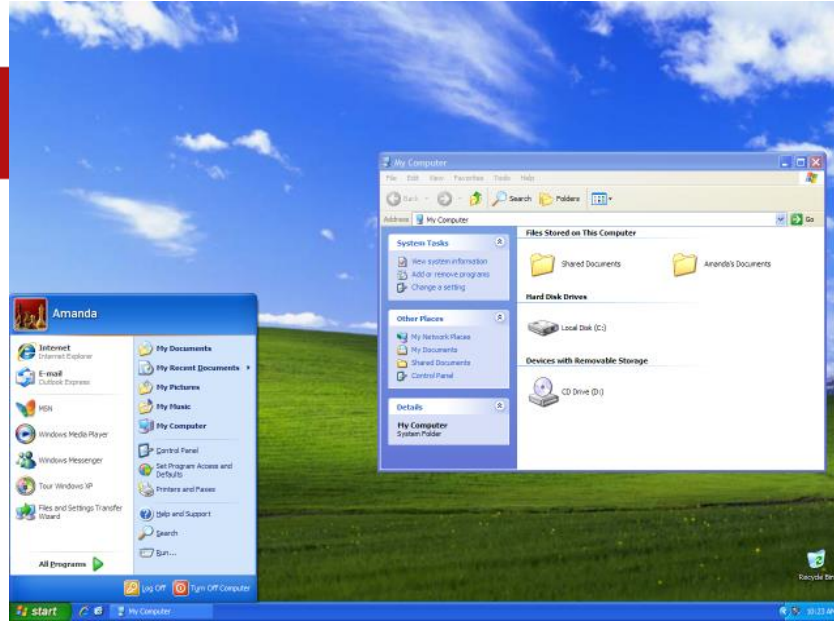
Menu

Business | Economy | Technology of Business | AI Business

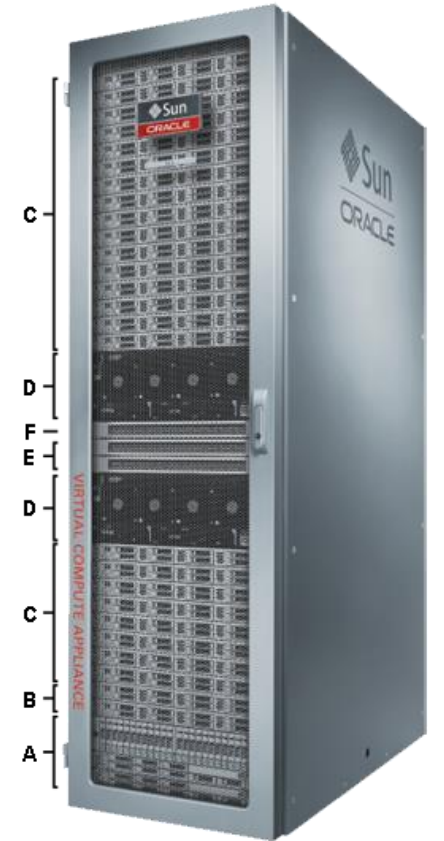
Could your 'smart' home be a weapon of web destruction?

🕒 28 October 2016

- Smart devices can't be used for much
- No data to extract, no value for extortion
- Can be used to generate network traffic



- Home PCs have little value for extortion -
-> most users buy a new PC and can't pay in crypto
- Potentially valuable data inputted
 - Banking details
 - Health info
 - Corporate logins



- Corporate machines can be stepping stone to wider attack
- DBs store valuable info for extortion
- Use for ransom or sell the access

Q5

Why did ransomware evolve from automated software targeting individuals with fixed demands to targeting companies and opening up negotiations?

Q5

- Compromising individuals is easier
- Targeting individuals is harder
 - Your grandma can't pay in bitcoins
 - Many will just buy a new device instead
- Need a form of price discrimination
 - A minority of victims will pay the vast majority of rewards
 - Reports of ransom payments in the £10m's
- Negotiation model allows gangs to extract their pound of flesh

Law firms pay ransoms to Luna Moth

By Michael Loney

Published: Tue 22 Sep 2026

At least three law firms paid multimillion-dollar ransoms to the Luna Moth extortion group this year, Cyber Risk Insurer was the first to report in August.

CNA Financial's reported \$40M ransom payment likely a record

Published May 21, 2021



Samantha Schwartz
Reporter

[Share](#) [License](#) [Add us on Google](#)

Q6

- Recall Ross Anderson's 4-way classification of the threat actor ecosystem (crooks, spooks, geeks and the swamp). Are there actors who fall into multiple categories? Any threat actors who don't fall into any of these?

Q6

SO MUCH OVERLAP

- Some nation states use cyber crime gangs
- Some of the swamp will buy tools from cyber crime market places
- Nation states may fund disinformation campaigns that look like the swamp
 - Russia and hybrid war
- Geeks may become or have been spooks, or become crooks!

What's unique?

- Intimate partner violence doesn't really fit into the swamp
- IP theft in industry fits awkwardly (crooks? Geeks?)

Q7

Modern infostealer malware groups sell a live data dump from infected machines. What other business models are possible and why do they go for this approach?

Q7

Possible business models

- Attacker sells live access to a data dump
- Attacker sells live access to top tier customers, then delayed access to lower tier
- Attacker curates data and curates it

--> Some companies buy access and sell the info as threat intel
"You've been infected by an info stealer"... morality?

Q8

- Let's say crooks are 1, spooks are 2, geeks are 3 and the swamp is 4.
- Come up with a profile of a defender who'd rank them the following from high to low:
 - a. Crooks then equal 2, 3 and 4
 - b. Swamp then 2 then equal 3 and 4
 - c. 3 highest
 - d. Spooks highest

Q9

- What is a reasonable “safety” policy for a firm offering a frontier LLM?

Q9 AI Safety Policy

Anthropic accuses Chinese rival Alibaba of illicitly extracting AI capabilities



ANTHROPIC CEO DARIO AMODEI

Osmond Chia
Business reporter

25 June 2026

Confidentiality, availability, integrity like usual

OpenAI agents hijacked German website before Hugging Face hack, report claims



OpenAI is the company behind ChatGPT

Zoe Kleinman >
Technology & AI editor

4 September 2026 · 128 Comments

Baby sitting the agent

Anthropic blocks possible attempt to use AI to make biological weapons



Laura Cress, Technology reporter and Nardine Saad

11 September 2026 · 1056 Comments

'A predator in your home': Mothers say chatbots encouraged their sons to kill themselves

8 November 2025

"Informational" harms outside "security" model

Q10

Was the IC's move to multi-level security for intelligence stored in computer systems more successful in protecting information than the equivalent physical system? What kind of security violations are possible despite MAC?

Q10

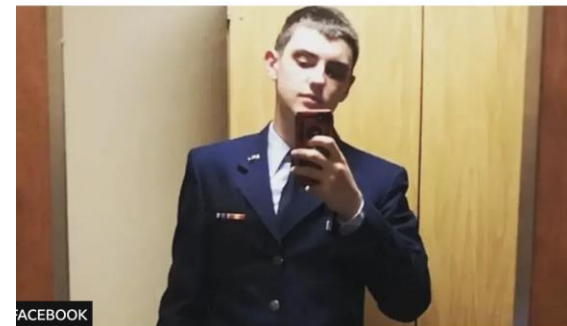
Most of the leaks we've heard about have not violated multi-level security as enforced by computer systems



Authorized with top secret clearance

Jack Teixeira: What we know about Pentagon leaks suspect

27 April 2023



Jack Teixeira in a photo posted on social media

Antoinette Radford and Chloe Kim
BBC News

Q11

Why is the concept of “trusted computing” particularly important in power metering situations? How are the associated security assumptions supported by periodic physical inspections of the meter?

Q11

- The adversary has local access and incentives to alter the meter to get free energy
- Physical inspections help see if tamper resistant seal has been broken