SCHOOL OF LECT

Security Engineering - Lecture

E:SX6VMP6XE3-00001

- Friday, 20 November 2026
- 13:10 - 14:00

Seminar Room 2

Scan to check-in



Expires at 20/11/2026 14:10

Problem Class 3

Security Engineering

Network Security

Security Engineering

Q1: “De-perimeterization is great. I don’t have to worry anymore about malicious or out-of-date devices on my network anymore.”

To what extent is this statement true?

I don’t have to worry anymore about malicious or out-of-date devices on my network anymore

Truth

- If device on network infected by malware, they still have to auth for sensitive services
- Access refused if device is known infected (device trust)

False

- Big problem if your ZTNA device is out-of-date or compromised
- Infected devices may still create problems
  - Ransomware
  - Data exfil
  - Stolen session tokens
  - Etc

Q2: Which threat actors and attack techniques are most/least impacted by zero trust network access?

Which threat actors and attack techniques are most/least impacted by zero trust network access?

Most

- Unsophisticated attackers relying on stolen credentials
  - If MFA + device trust
- Techniques that use VPN to pivot laterally
- …

Least

- Insider threat
- Social engineering
- Token theft
- Identity provider/help desk attacks
- …

Q3: Why does spoofing an email require the social engineering to succeed right away? How might attackers get around this limitation and conduct back-and-forth social engineering?

Q3

Why does spoofing an email require the social engineering to succeed right away?

- Any replies go to the real owner, so you can't respond

How might attackers get around this limitation and conduct back-and-forth social engineering?

- Switch to another communications channel that attacker owns
  - "Reply to" field pointing to address attacker owns
  - Click on a link
  - Switch to teams/whatsapp/....

Q4: How comfortable would you be logging into your bank account on a public airport WiFi? Would a VPN offer you additional protection in this scenario?

Bank account on a public airport WiFi

Mostly comfortable.

- TLS largely solves man-in-the-middle
  - Packets are encrypted so no easy passive attacks
  - Impersonation blocked by attacker not being able to sign digital certificate
    - … unless DigiNotar
    - Just don't click through browser warnings
- VPN protects meta data and moves trust away from local wifi

Q4: What kinds of web attacks would be made more difficult by domain registrars enforcing Know Your Customer whenever a new domain is registered?

What kinds of web attacks would likely increase as a result?

Registrars enforcing Know Your Customer

Reduction

- Lookalike phishing + typosquatting harder to register
- Consumer fraud
  - Fake shops, investment scams, tech-support scmas
- Evasion of blocklists
- Attackers using DGA to control botnets
- …

Increase

- Registering domains from dodgey registrars
  - Forum shopping!!
- Compromise of existing websites
- Phishing via URL shortening
- Registration fraud
- Domain-less attacks
  - Direct IP command and control etc
- ….

Detection & Response

Security Engineering

Q1: A detection system flags 99% of attacks and wrongly flags 1% of benign logins. Only 1 in 10,000 logins is malicious. What fraction of alerts are real attacks, and what does this mean for a SOC?

A detection system flags 99% of attacks and wrongly flags 1% of benign logins. Only 1 in 10,000 logins is malicious.

Across say 1 million logins:

- 100 malicious logins and 99 are flagged as malicious
- 999,900 benign logins and 9,999 are flagged as malicious

Precision of ~0.98% = 99/(99+9,999)

SOC implications:

- Alert fatigue + habituation
- Vendor marketing about catching 99% of attacks is misleading
  - Solution with higher precision but lower recall may be better in practice

Q2: “Our threat intel provider flags 50,000 malicious IP addresses a day, so we automatically block all.”

Give three reasons this could be a bad policy, and say what evidence would tell you whether it is.

“Our threat intel provider flags 50,000 malicious IP addresses a day, so we automatically block all.”

- Delay from malicious activity to being added to block list
- Many attackers rotate network addresses
- False positives from shared infra create problems
  - CDNs, cloud providers, Tor/VPN exit nodes etc

How you know

- Employees complain
- Check network activity
  - Do blocked IPs ever touch network
  - What critical services are involved
- Compare overlap with a third party list

Q3: Allowlisting is the most effective blocking control and the least popular. Why?

Would you recommend it for a 50-person firm, a hospital, and a bank, and how would your answer differ?

Allow listing as a blocking control

- Efficacy and pain depend on where it's applied
  - Network allow-listing prevents
- Depends on the threat landscape + resources
  - Need an IT team to manage exceptions/requests (likely not 50 person firm)
  - Banks perhaps have more to lose, so recommend it there
  - Hospitals value operational freedom
    - No-one wants to own an allowlist harming a patient

Q4: After a breach, a firm routes its forensic investigation through its lawyers so the findings are privileged.

Who benefits and who loses? What happens to the “learn and improve” stage of incident response?

Routing DFIR through lawyer

Benefits

- The lawyers!!!
- Breached organization may be able to defend lawsuit better
- Maybe the CISO?
- Those with financial interest
  - Insurers, shareholders, …

Loses

- Customers whose data is lost face barriers to litigation
  - Shareholders too!
- Internal team can't document the failure
- The wider community can't learn from the incident
  - Maybe attackers benefit?

Q5: Automated response can isolate a laptop or revoke a session token in seconds, but a human analyst takes hours.

When should a firm let the tool act without approval? Give one example where automation is clearly right and one where it is clearly wrong.

Automated Containment

- Generally a question of risk of compromise vs cost of friction
- Clearly right --> Rare + high impact signals and/or low cost action
  - Mass encryption of files
  - Revoking authentication token
  - Killing a process
  - …
- Clearly wrong --> Common signals and/or high cost action
  - Login from foreign country
  - Credential reset
  - Containing critical machine (e.g. ICS or hospital setting)
  - …

Q6: “Backups mean we don’t need to worry about ransomware.” Discuss.

Backups

Helps recovery if data is encrypted but two problems:

1. Backups may not work
   - Corrupted by attacker
   - Not updated recently enough
   - Shadow IT not backed up
   - Time to restore
   - …
2. Alternative ransom threats like leaking data, DDoS etc



Assurance

Security Engineering

Q1: Why do military and safety critical software buyers maintain requirements for high-assurance, whereas B2C software builders have dropped this requirement? What is lost as a result?

Q1

- Why is persists
  - Higher cost of failures is the obvious answer
    - Even then, it's not clear this "kind of assurance" helps
    - User failure can be just as costly in medicine
  - Legacy cultural issues, concentration in defense market
  - War is infrequent so agile may be lacking user feedback?
- What is lost
  - Shared evidence of security (e.g. certifications)

Q2: How can formal methods as a route to assurance be reconciled with a focus on user testing?

Q2

- Obvious answer is no.
  - It's hard to build a formal specification of users and test the properties of it
- More subtle answer is you can build light-weight formal methods into development process
  - AI might help?
- An even deeper answer is that we can formalise some aspects, but not others
  - TLS protocol was formally tested, but browsers can play around with how it's visualised to users

Q3: What is the relationship between prices in a bug bounty program and assurance over software security?

Q3

- General intuition is that higher prices = more assurance
  - Increases cost of compromise
  - Researchers sell to vendor instead of criminal
- Economic PoV is more complex
  - High prices could just be a sign there's lots of demand
  - There's many reasons supply curve is steeper, not just quality of software

Q4: Discuss the defensibility of the four patch strategies introduced in the lecture for a CISO facing allegations they were negligent.

1. **PCI DSS:** Update high and critical vulnerabilities (according to CVSS) within one month of release
2. **EPSS:** Patch what ML says is most likely to be exploited.
3. **KEV:** Patch what has already been exploited.
4. **Cloud infra:** Rely on professionals.

Q4: Discuss the defensibility of the four patch strategies introduced in the lecture for a CISO facing allegations they were negligent.

1. **PCI DSS:** Update high and critical vulnerabilities (according to CVSS) within one month of release
   - This is industry standard, baked into many standards. You have a clear defence
2. **EPSS:** Patch what ML says is most likely to be exploited.
   - This is new and untested, you don't get credit for the proactive vulns you avoided. But you will be blamed if you didn't patch a critical vuln or one that's been actively exploited
3. **KEV:** Patch what has already been exploited.
   - Reasonably defensible. You might be blamed if a "critical" vuln has been left unpatched for months because it hadn't been exploited
4. **Cloud infra:** Rely on professionals.
   - Highly defensible

Q5: If a vendor goes bankrupt, what are the security benefits and risks associated with "open-sourcing" their code bases?

Q5

- Benefits
  - In theory, customers or a 3rd party could fork the code and release a patch if a vulnerability is discovered
  - OSS is a good thing, maybe a community actively supports the project
- Risks
  - Source code helps attackers find vulnerabilities
    - But also LLMs appear to be very good at building source code
  - "Patched" forked codebase might include a backdoor
  - Is the eventual vendor less likely to maintain if it's OSS?

Q6: Name three traditional security assumptions that are no longer true due to advances in AI systems.

Q6

- Fraudulent emails tend to have lots of errors
- Hearing a voice/seeing a video of a person is a form of authentication
- Traditional CAPTCHAs block bots
- Attackers don't have time/capacity for reconnaisance to understand procedures
- Exploits of CVEs are hard to create
- ...

Q7: How can a defender avoid forum shopping when it comes to assessing their vendors' security posture?

Q7

You have to do it via:

- Choose a security scanning rating yourself
- Direct verification via integrations
- Ask your own questions