Fourth week tutorial

Yuvraj Patel

Question 1

“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 I don’t have to worry anymore about malicious or out-of-date devices on my network anymore.”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? Does the Mirai Botnet tell us anything about de-perimeterization?

Question 1

“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 I don’t have to worry anymore about malicious or out-of-date devices on my network anymore.”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? Does the Mirai Botnet tell us anything about de-perimeterization?

- It only really works if you have a good inventory of devices so you can check they’re all up to date
- You may also want to have a perimeter with DDoS defenses even if all authentication is per device

Question 2

Can we trust anything we do online, given the known weakness of protocols such as BGP, and the various limitations of Certification Authorities?

Question 2

Can we trust anything we do online, given the known weakness of protocols such as BGP, and the various limitations of Certification Authorities?

- The known limitations have multiple ‘patches’
- BGP attacks are limited by rules on how many routes you accept from whom
- CA subversion is limited by certificate pinning
- It’s a large and complex ecosystem with powerful players having an incentive to keep it running...

Question 3

The default settings used in VPNs are probably intentionally weak. So, do VPNs have any value in any setting?

Question 3

The default settings used in VPNs are probably intentionally weak. So, do VPNs have any value in any setting?

- In an ideal world you might de-perimeterize
- In the real world you may have the most critical machines running on ancient software that cannot be patched, e.g., MRI scanners on Windows 7
- Your customers may have policies that require secure networks for certain functions
- And then there’s the Operational Technology

Question 4

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?

Question 4

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?

- Suppose the ‘free wifi’ hub is a malicious device operated by another person in the airport
- The main threats are
  - Bad DNS
  - A phishing site
  - MITM attack
- What’s the appropriate defense against that?

Question 5

What's the point of locks, if they can be so easily bumped? Why even bother breaking a lock if you can just smash a window?

Question 5

What's the point of locks, if they can be so easily bumped? Why even bother breaking a lock if you can just smash a window?

- Some locks are not bad. Lever locks must be drilled or impressioned; multipoint locks broken
- Locks generally deter Derek and Charlie, nudging them to pick other targets
- They remove legal excuses
- They're a condition of insurance

Question 6

Why is MiFare Classic such a weak protocol? If you have a building using it, what steps might you take to improve assurance?

Question 6

Why is MiFare Classic such a weak protocol? If you have a building using it, what steps might you take to improve assurance?

Question 6

Why is MiFare Classic such a weak protocol? If you have a building using it, what steps might you take to improve assurance?

- 48-bit keys were needed in the 1990s for export
- Keys are easy to copy, even if you just touch them
- So, you can copy the master key used by the guard, or the cleaner
- You eventually must replace them, but if the university card is now used in 100 buildings...

Question 7

Explain how Deter-detect-alarm-delay-respond might be relevant in a home security environment.

Question 7

Explain how Deter-detect-alarm-delay-respond might be relevant in a home security environment.

- Deter using design of street and garden, visible alarms, and locks
- Detect using PIR, CCTV
- Alarm to your phone or an alarm company
- Delay might mean hiding your jewelry
- Response may mean the alarm company checking your CCTV and calling the police

Question 8

Might an IoT device need some forms of tamper resistance? What about a video games console?

Question 8

Might an IoT device need some forms of tamper resistance? What about a video games console?

- Many examples, most of them protecting a business model from circumvention by the user!
- Started with printer cartridges
- Rights-management chips are now everywhere from tractors to water filters and insulin pumps
- Video games consoles use them so they can subsidize the console from sales of games and accessories

Question 9

Differential Power and Fault analysis are really complicated. You are a CISO trying to explain to your CEO the possible attacks that may occur on your new IoT device, of which you have produced 3 million units. How far up the list of risks should these attacks be, and how would you explain their potential for damage and the circumstances under which this damage could occur?

Question 9

Differential Power and Fault analysis are really complicated. You are a CISO trying to explain to your CEO the possible attacks that may occur on your new IoT device, of which you have produced 3 million units. How far up the list of risks should these attacks be, and how would you explain their potential for damage and the circumstances under which this damage could occur?

Question 9

Differential Power and Fault analysis are really complicated. You are a CISO trying to explain to your CEO the possible attacks that may occur on your new IoT device, of which you have produced 3 million units. How far up the list of risks should these attacks be, and how would you explain their potential for damage and the circumstances under which this damage could occur?

- Could someone extract a key and then undermine your business model with compatible spare parts?