Threats – range and type

Ed Zaluska

COMP6230: Implementing Cybersecurity

Key issues

- potential threats
- potential attackers
- range of systems

Always remember…

- “A security system is only as strong as its weakest link”
- ‘perfect security’ does not exist
- to understand security vulnerabilities, you need to ***think like an attacker***
- many cybersecurity threats are simply traditional threats updated by adapting new technology
- *security in depth* is essential

Potential threats (non-exhaustive)

- eavesdropping (or visual surveillance)
- wiretapping (= keyboard logging)
- key interception
- impersonation (person, address, computer)
- data duplication
- cryptanalysis
- social engineering
- physical security
- malware
- exploiting software vulnerabilities
- *combinations* of different attacks

Potential attackers (non-exhaustive)

- criminal
- competitor
- hacker (or “cracker”)
- government
- terrorist
- ethical hacker
- (continues next slide…)

Potential attackers (continued)

- former employee
- employee
- customer
- contractor
- whistleblower
- everybody?

  (non-exhaustive list!)

Who represents the greatest threat to your security?

- **your staff!**
  - poor policies (often not followed)
  - poor training (needs regular refreshing)
  - complacency
  - incompetence (or stupidity)
- security products can be *dangerous* – they may appear to offer an *illusion* of security…

Range of systems (non-exhaustive)

Stand-alone computer (no network)

– possible attacks?

- physical security
- via computer terminal
- valid password
- removable data (with or without malware)
- system software upgrades

(Physical security detail…)

- Solid walls and doors (multiple?)
- (what about entry via roof?

  …or underground?)
- Solid locks, good key control
- CCTV cameras + alarms

  (UPS? Floodlights?)
- Guards (24 hour)

  (but *Quis custodiet ipsos custodes?*)
- …repeat for backup/other locations…

Distributed computer (private network)

– possible attacks?

- as before
- compromise of private network
- many cases where a (typically) control computer added to a system later
  – and with an Internet connection (for updating convenience)
- i.e. original security motivation for isolated network *forgotten*

Distributed computer (Internet)

(typically log-in from remote site)

– possible attacks?

- as before
- but now *much easier* for an attacker to launch an attack via the Internet
- also vulnerable to DOS/DDOS attacks

Server with website (Internet)

– possible attacks? (non-exhaustive)

- as before
- but now *much easier* for an attacker to exploit a vulnerability on the website software
- Open Web Application Security Project (OWASP)

  https://www.owasp.org/index.php/Main_Page

Conclusions

- overview of a complex topic
- many different threats possible
- many different potential attackers
  (on a wide range of systems)
- difficult or impossible to prevent attacks
  (but can make them much more difficult)