Module 2
Security Threats & Countermeasures

Submodule 1: Security Threats

Attack Vector

- An attack vector is a path or means by which a hacker (or cracker) can gain unauthorized access to a computing device or a network for malicious purposes.
  - The gained access could allow the delivering of payload
  - Attack vectors enable the hackers to exploit system and/or network vulnerabilities.
  - Programming is often heavily involved in the attack vectors.
  - Human ignorance or weakness can be exploited to engineer attack vectors.

Typical Attack Vectors-I

- Denial of service
- Insider and privilege misuse
    - Unapproved or malicious use of organizational resources
- Crimeware
    - Ransomware
    - Other malware
- Web application attacks
    - Repurposing of systems followed by actions such as stealing credentials, theft of personal information etc.
- Physical theft and loss

Typical Attack Vectors-II

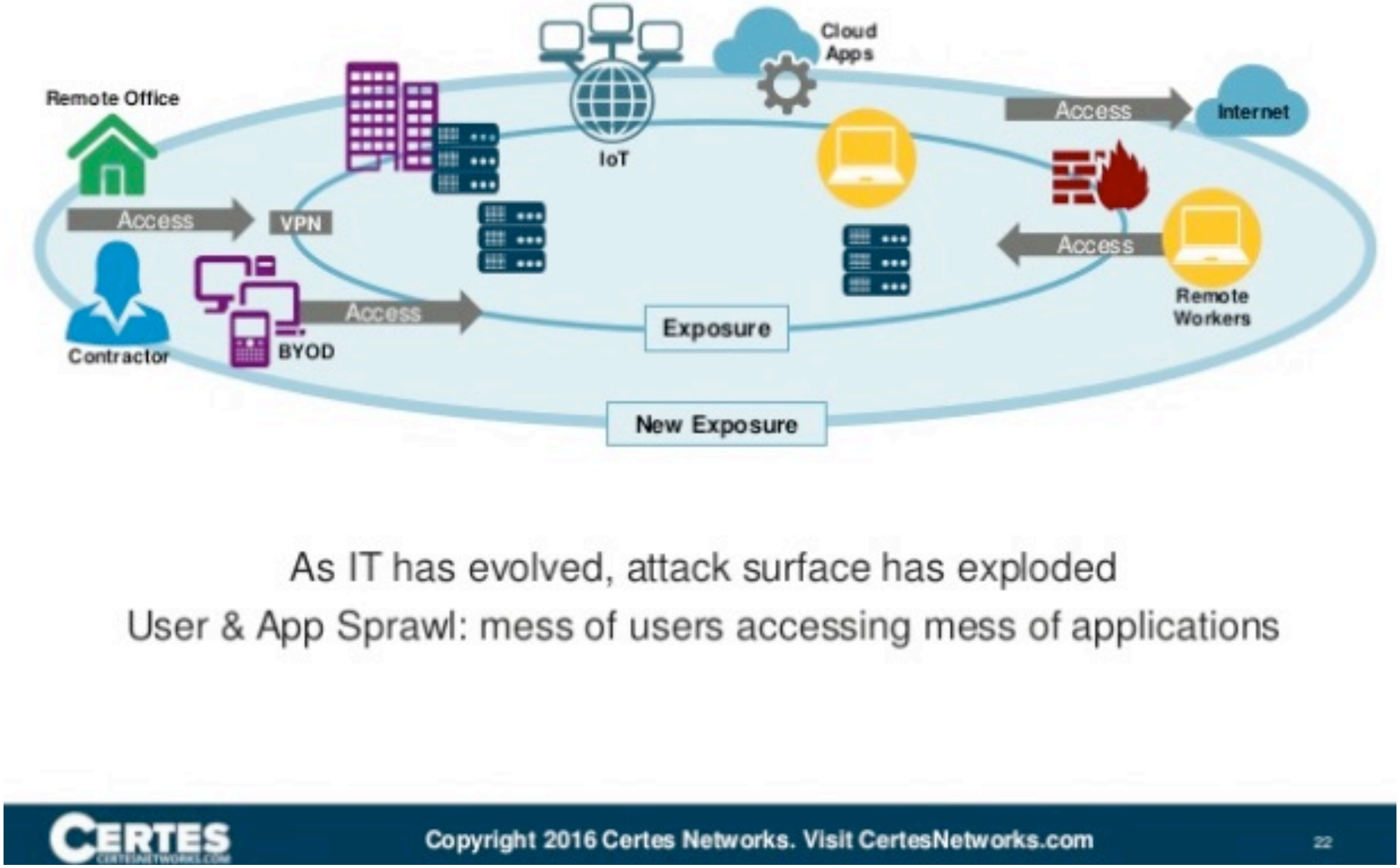
- Cyber-espionage
  - State-affiliated groups target industries such as manufacturing and public sectors.
- Point of sale intrusions
  - Mostly impacting retail and food services
- Payment card skimmers
- Miscellaneous errors
  - Mis-delivery of information in either electronic or paper format
- Hybrid of many vectors

Attack Surface

- Attack surface is the exposure, the reachable and exploitable vulnerabilities that exist.
- Examples of attack surface:
  - Open ports on outward facing web and other servers, code listening on those ports
  - Services available on the inside of the firewall
  - Code that processes incoming data, email, XML, office documents, industry-specific custom data exchange formats (EDI)
  - Interfaces, SQL, web forms
  - An employee with access to sensitive information is socially engineered

Attack Surface by Category

- Network attack surface
  - The attack will often be delivered via a network
- Software attack surface
  - With a primary focus on web applications
- Human attack surface
  - Social engineering, errors, trusted insider etc.



As IT has evolved, attack surface has exploded

User & App Sprawl: mess of users accessing mess of applications

In-Class Exercise

Go to: https://www.hacksplaining.com/

Create an account and go to lessons.

Take the following lessons:

- Broken access control
- Password mismanagement
- Email spoofing
- Malvertising