NETWORK SECURITY
THE BIG PICTURE

EN.600.444/644

Spring 2019

Dr. Seth James Nielson

WHAT HAVE WE LEARNED SO FAR?

- Network Stack
- Data Assets
- Psychology/Incentives
- Cryptography

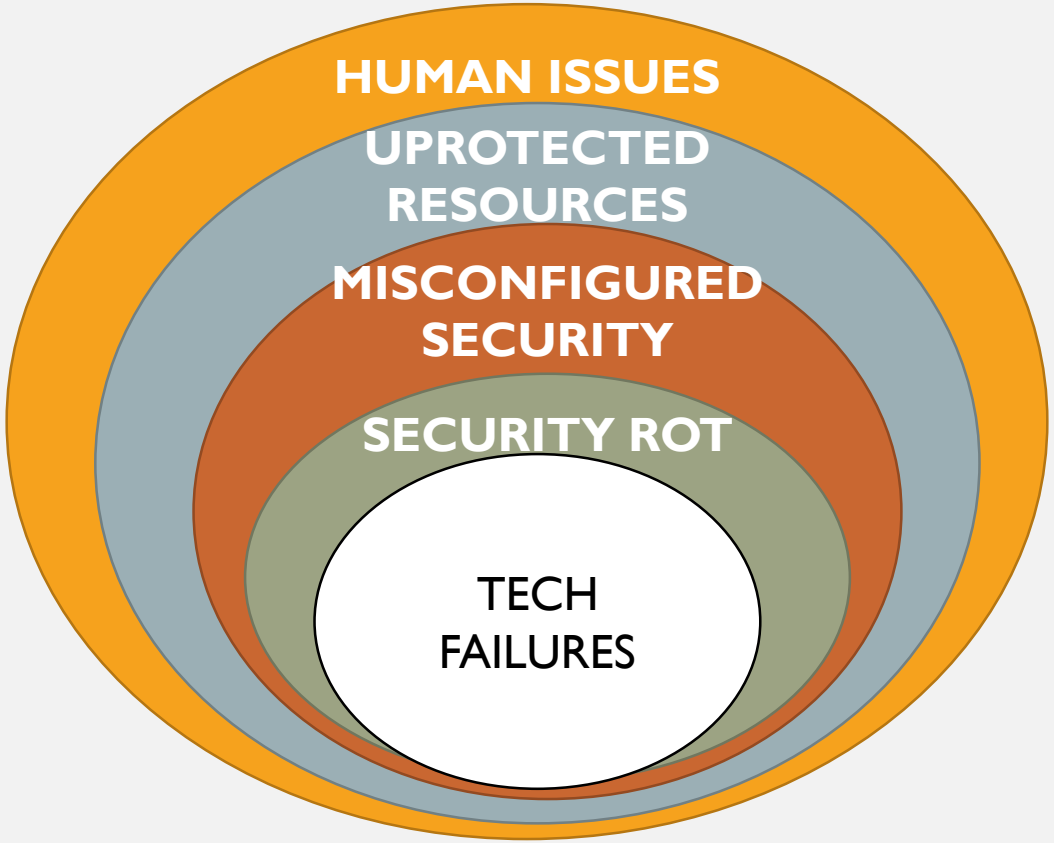
NETSEC TECHNOLOGIES

- Secure transport (e.g., TLS, Kerberos, VPNs)
- Firewalls (L4, L7)
- User and Entity Authentication
- Securing Infrastructure (DNSSec)

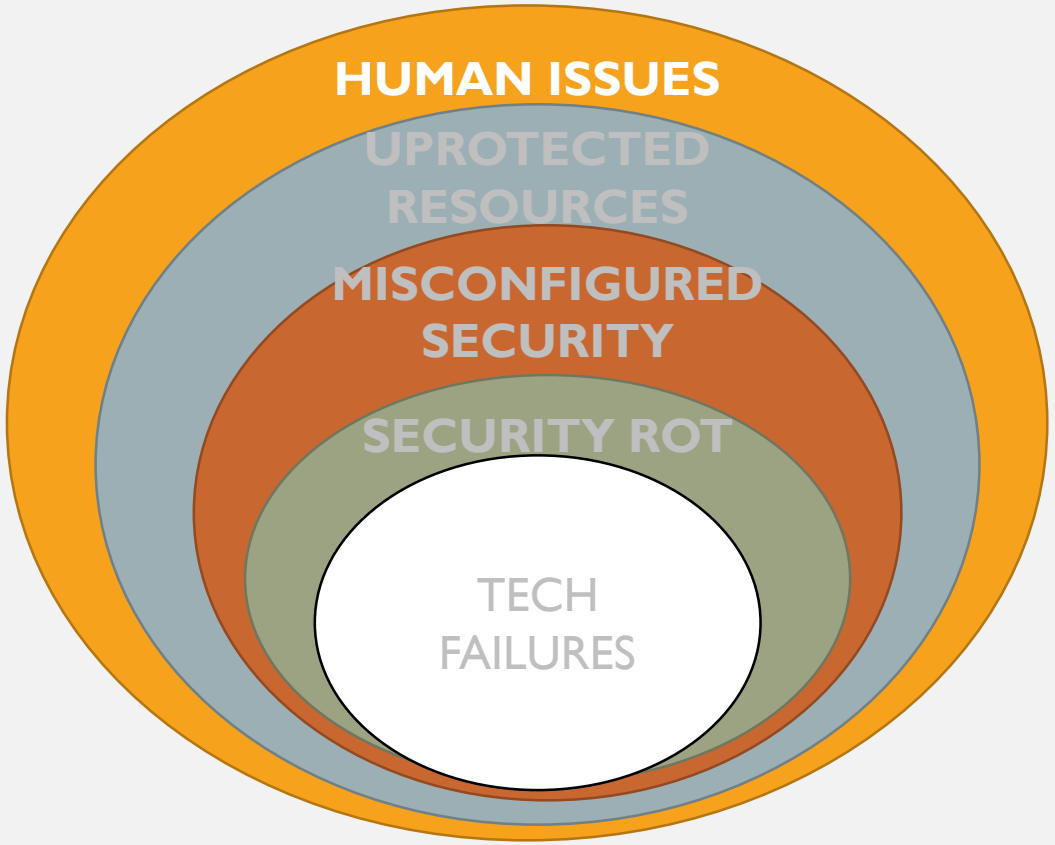
WHAT GOES WRONG?

- We have amazing technology.
- Why do the bad guys win?

ATTACK VIEW


HUMAN ISSUES
UPROTECTED RESOURCES
MISCONFIGURED SECURITY
SECURITY ROT
TECH FAILURES

HUMAN ISSUES

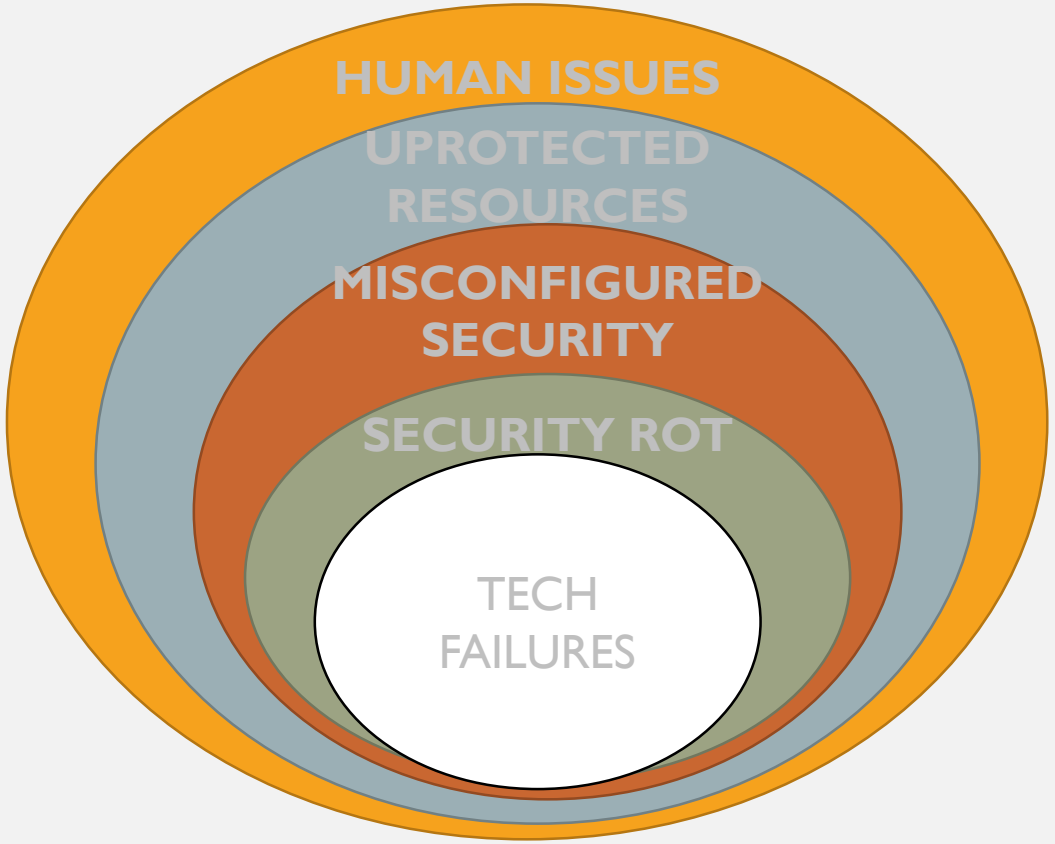


- Organizational
- Cultural
- Incentives
- Cyber-hygiene
- Risk management maturity

CONCRETE EXAMPLES

- Hygiene
  - Passwords still one of the most common ways in to a system
- Social Engineering
  - Stuxnet still started with a PDF in an email
- Incentives
  - Case Study: Major company that sidelined CISO from product security
  - Case Study: Major company used “security” to lock-in clients

UNPROTECTED RESOURCES

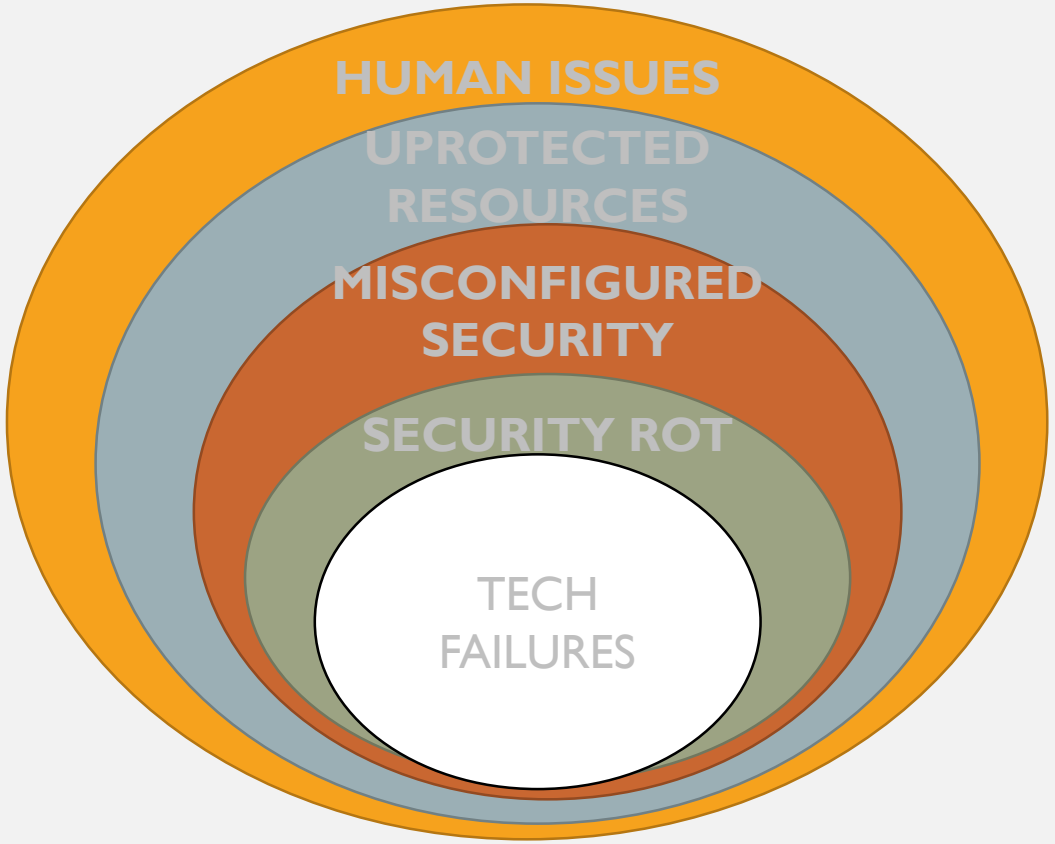


- “Forgotten” Resources
- “Unimportant” Resources
- Policy Failures
- Misunderstood threat modeling
- Misunderstood defenses
- Misunderstood cryptography

CONCRETE EXAMPLES

- Keys hardcoded in Github repos
- Software left on public FTP
- Voting security protocol that doesn't actually authenticate smart card

MISCONFIGURED SECURITY

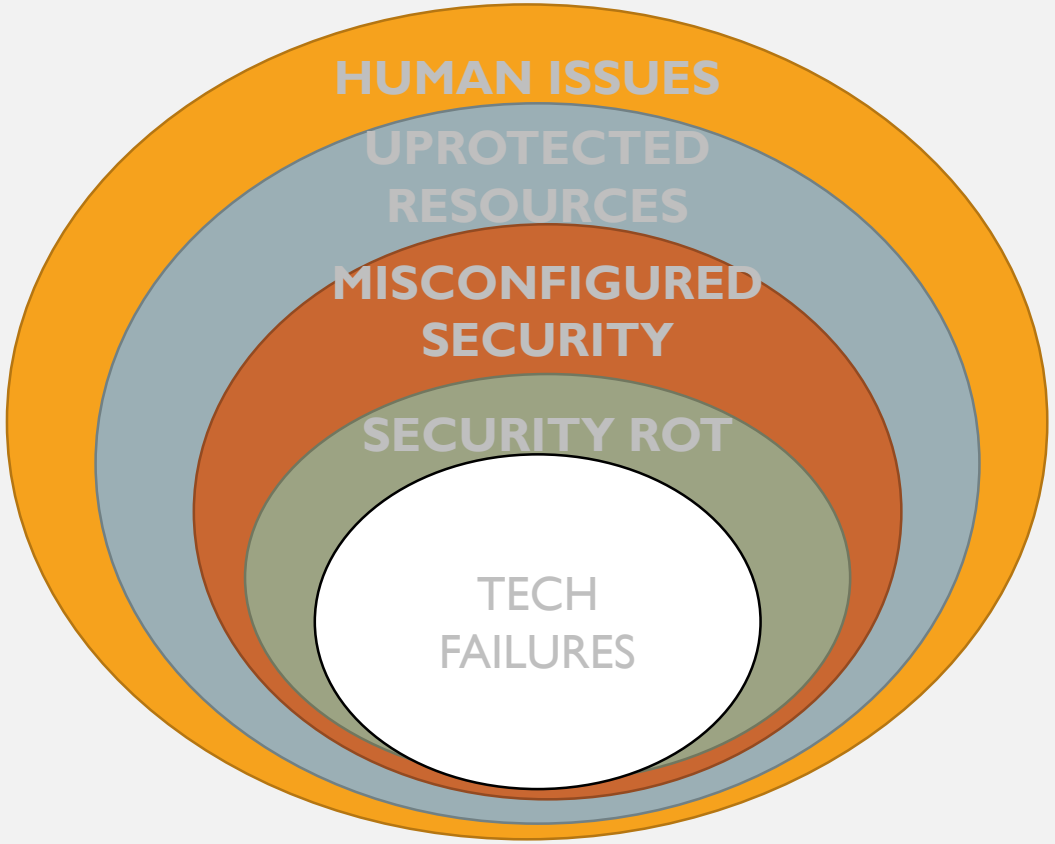


- Security boundaries
- Misunderstood defenses
- Misunderstood cryptography
- Misunderstood threat model
- Legacy support
- Out-of-the-box use of products

CONCRETE EXAMPLES

- Poorly chosen cryptography algorithms and protocols
- Air-gapped servers not air-gapped
- Out-of-box devices with default passwords

SECURITY ROT

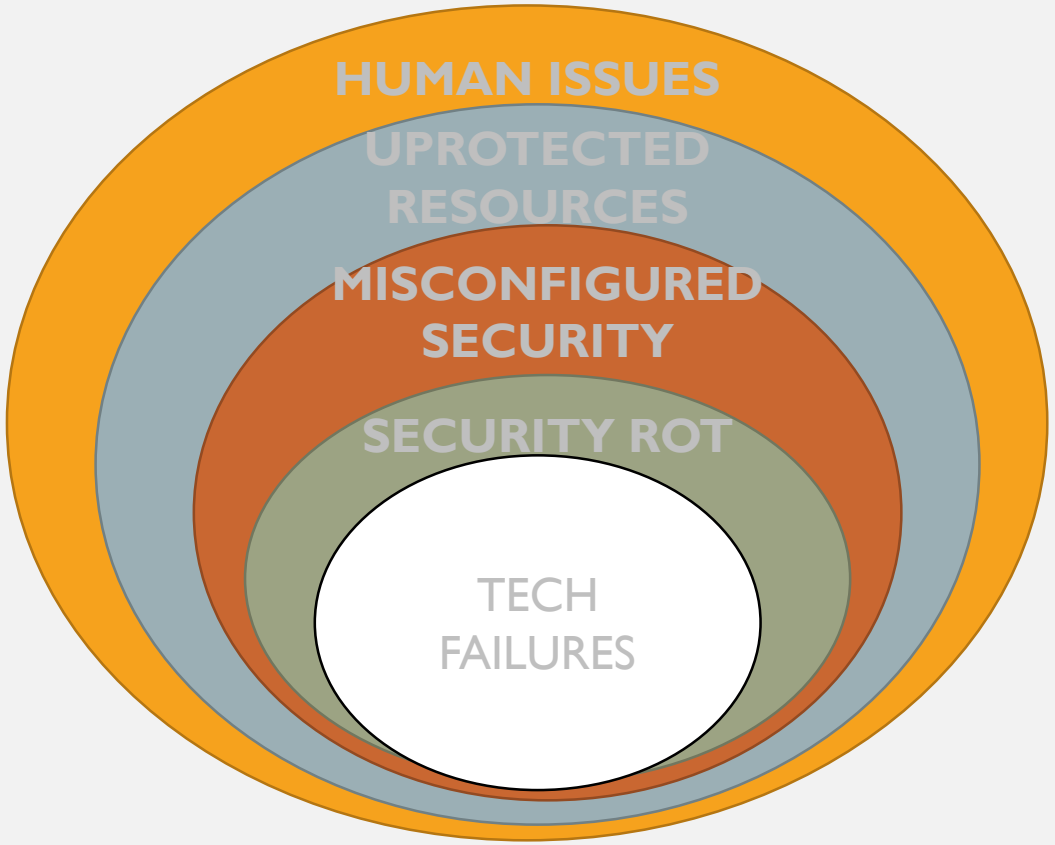


- Access controls not maintained
- Data rot
- Lack of monitoring, alerts, ID
- Complacency

CONCRETE EXAMPLES

- Equifax was an unpatched server
- Case Study: major company couldn't detect malware spreading from inside
- Employees leave but access not rescinded

TECH FAILURES



- Cryptography failures
- Bugs/Vulnerabilities

CONCRETE EXAMPLES

- Zero-day vulnerabilities
- Heartbleed
- Quantum computing (in the future)