GREPSEC IV Workshop – 18 May 2019
Marines’ Memorial Club, San Francisco

What is this Thing called Security? The Puzzle Pieces of a Complex Subject

Paul Van Oorschot

Professor of Computer Science – Carleton University, Canada

What is Computer Security?

"Computer Security" aka ...

Too broad a question

- What would a supervisor like an incoming grad student to know
  what should be taught in a first course
  what concepts are important for a sound footing

- *"There is no ideal book ... "*

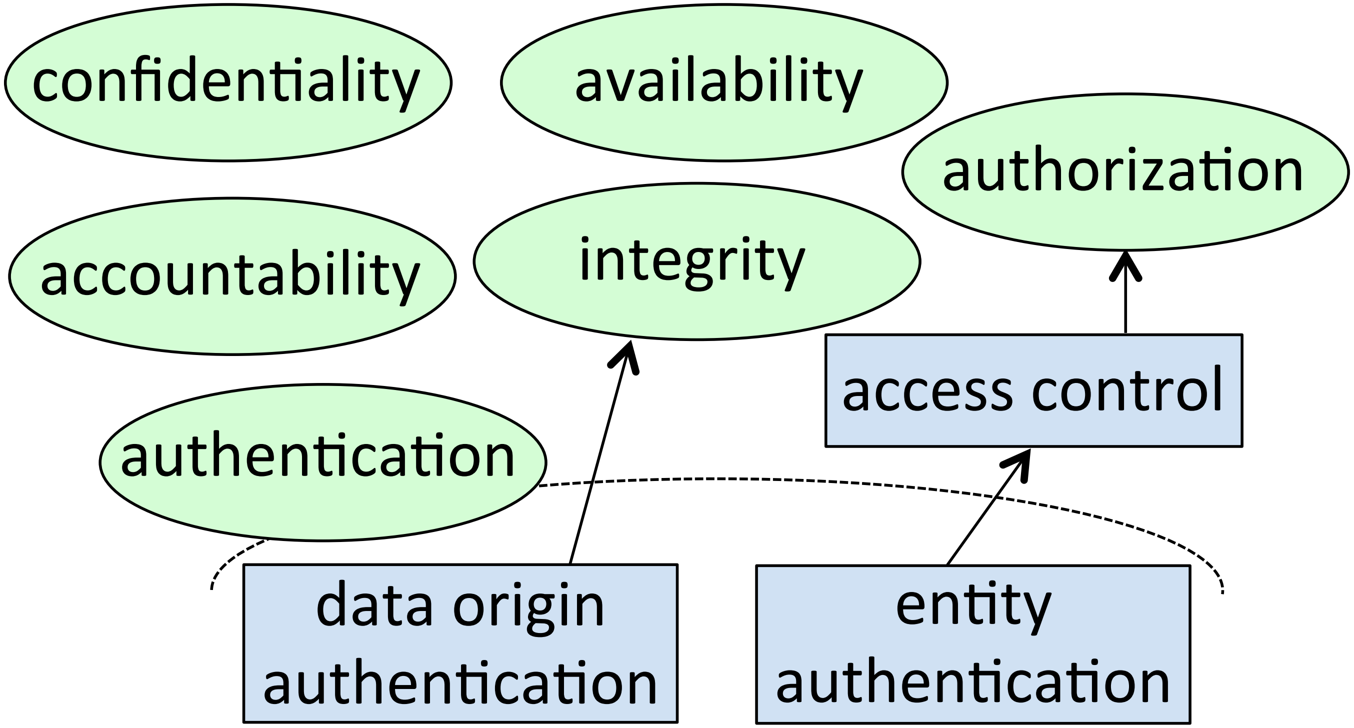
LOST
CONFUSED
UNSURE
UNCLEAR
PERPLEXED
DISORIENTED
BEWILDERED

Approaches (Teaching)

- theory
- programming, software tools
- case studies
- failure patterns
- open problems
- research papers

Oversimplified

- CIA triad ... plus AAA



- Confidentiality vs. traffic analysis, anonymity, privacy

Goals (Teaching)

- knowledge of risks
- awareness of enabling technologies
- conveying security concepts
- target audience:
  - end-users
  - software developers
  - R&D management
  - policy experts
  - research scientists

Characterization

- art
- science
- engineering practice

Quotes [Zalewski]

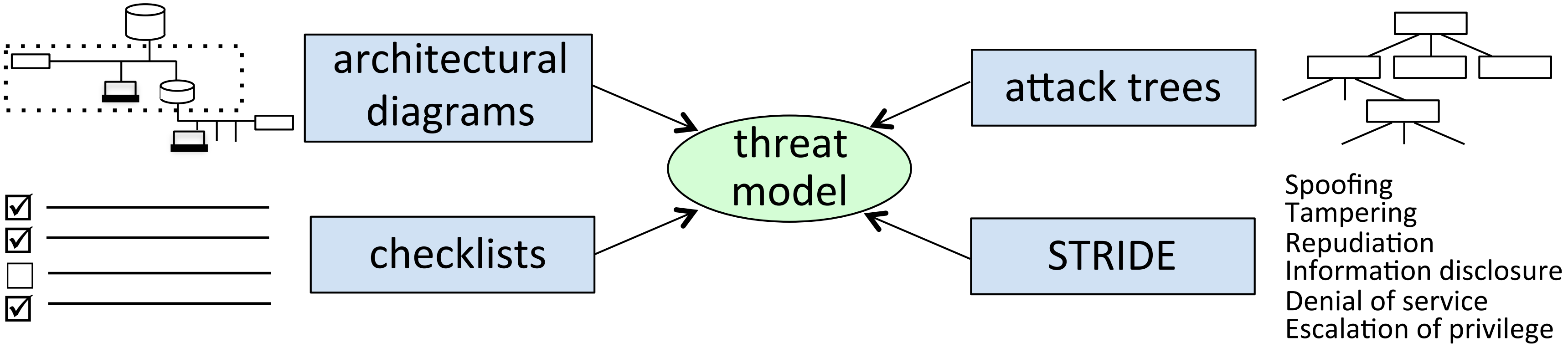
(re: usability of web browsers)

“Perhaps the most striking (and entirely nontechnical) property of web browsers is that most people using them are overwhelmingly unskilled... Web browsers... can be *successfully* used by people with virtually no computer training [but] can be operated *safely* only by [technically-savvy users]”

(re: HTML parsing, tag filtering, character encoding)

“an entire book has been written on this topic: inquisitive readers are advised to see *Web Application Obfuscation* (2011) ... and then weep about the fate of humanity. The bottom line is that [stopping dangerous patterns] is simply not feasible”

Which one of these is about security?



architectural diagrams

checklists

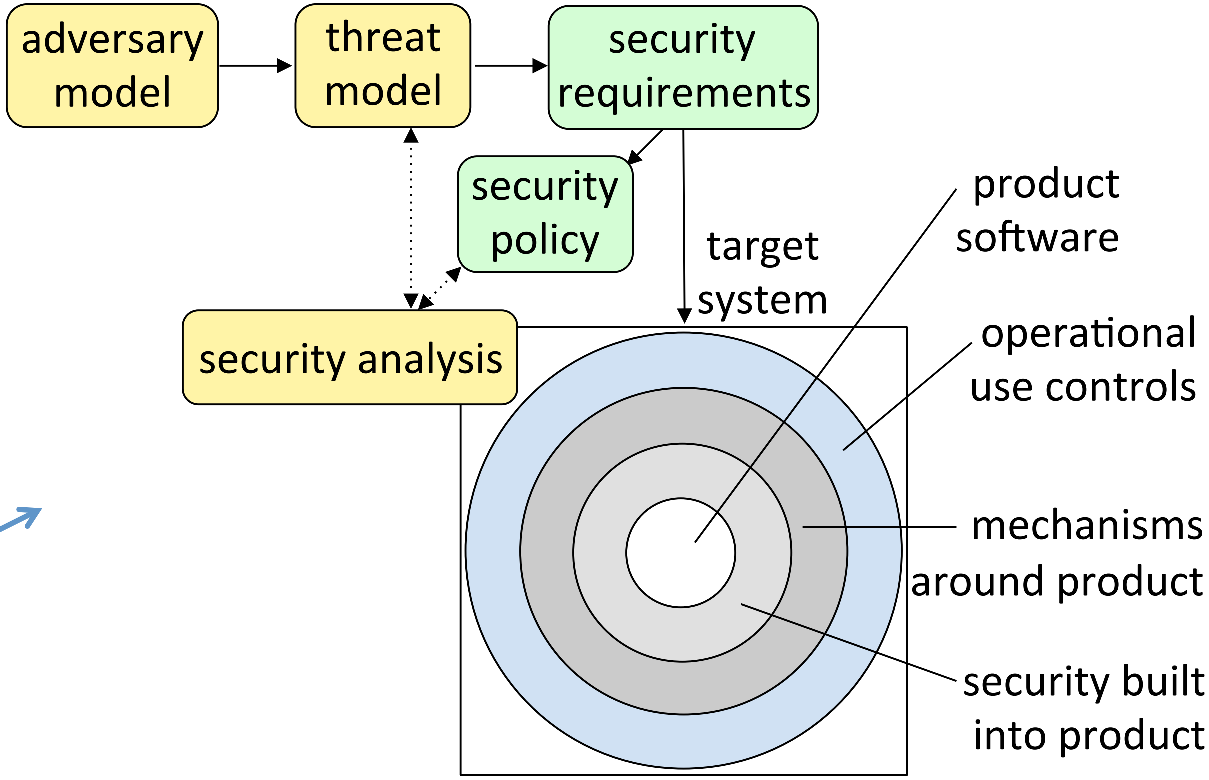
threat model

attack trees

STRIDE

Spoofing
Tampering
Repudiation
Information disclosure
Denial of service
Escalation of privilege

Is this part of computer security?



adversary model

threat model

security requirements

security policy

security analysis

target system

product software

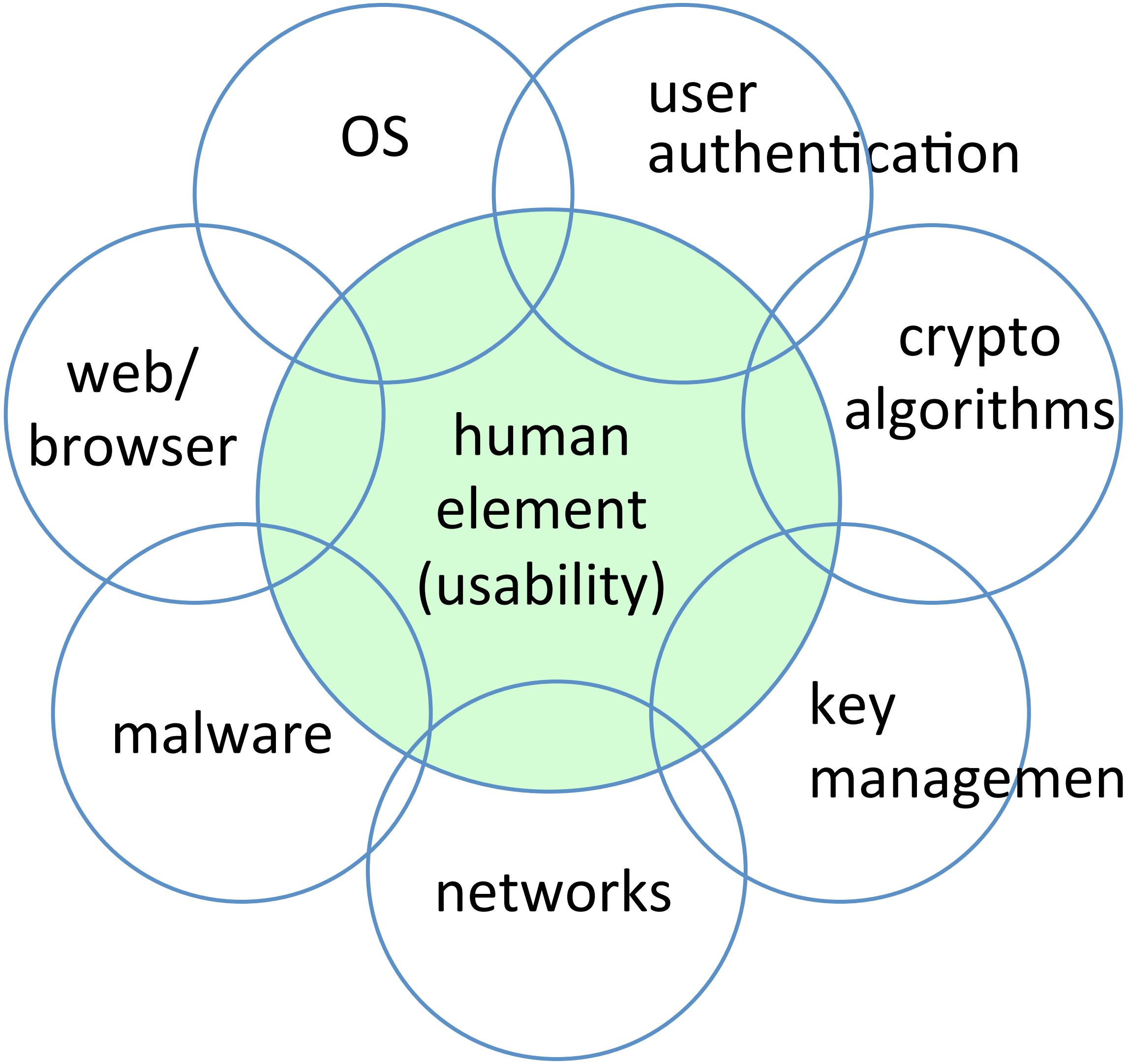
operational use controls

mechanisms around product

security built into product

How about this?

Candidate Categories (Topics) re: Security



Crypto

block cipher

EKE

modes of operation

hash functions

symmetric-key

ChaCha20 Poly1305

RSA DH ECDSA

ciphertext

PAKE

public-key

signatures

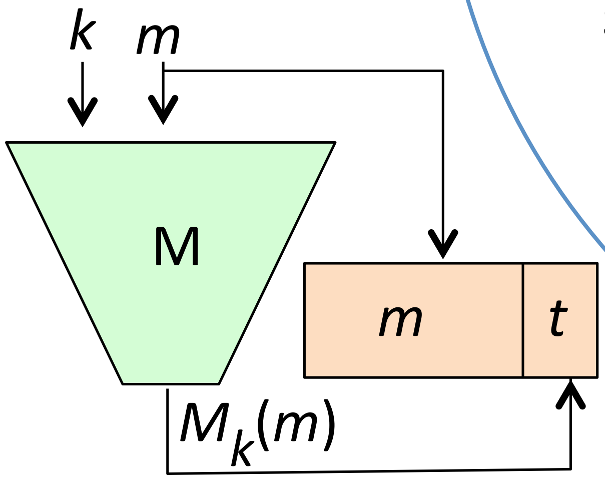
cryptographic key

asymmetric

SHA-3

AES-MAC

AEAD



User Authentication

dictionary attack

online guessing

offline guessing

salt & pepper

CAPTCHAs

passphrases

rate-limiting

one-time passwords

passcode generators

two-factor authentication

biometrics

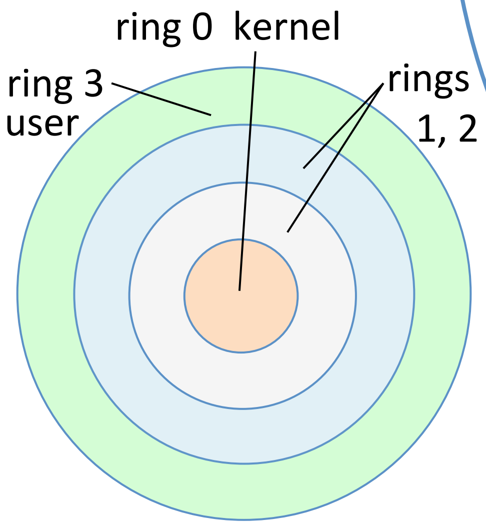
false accept rate

graphical passwords

password managers

what you know	what you have
where you are	what you are/do

Operating Systems



access control

segment descriptors

privileged bit

ACL

reference monitor

capabilities

RBAC

security kernel

audit trails

file permissions

chroot jail

SELinux

setuid

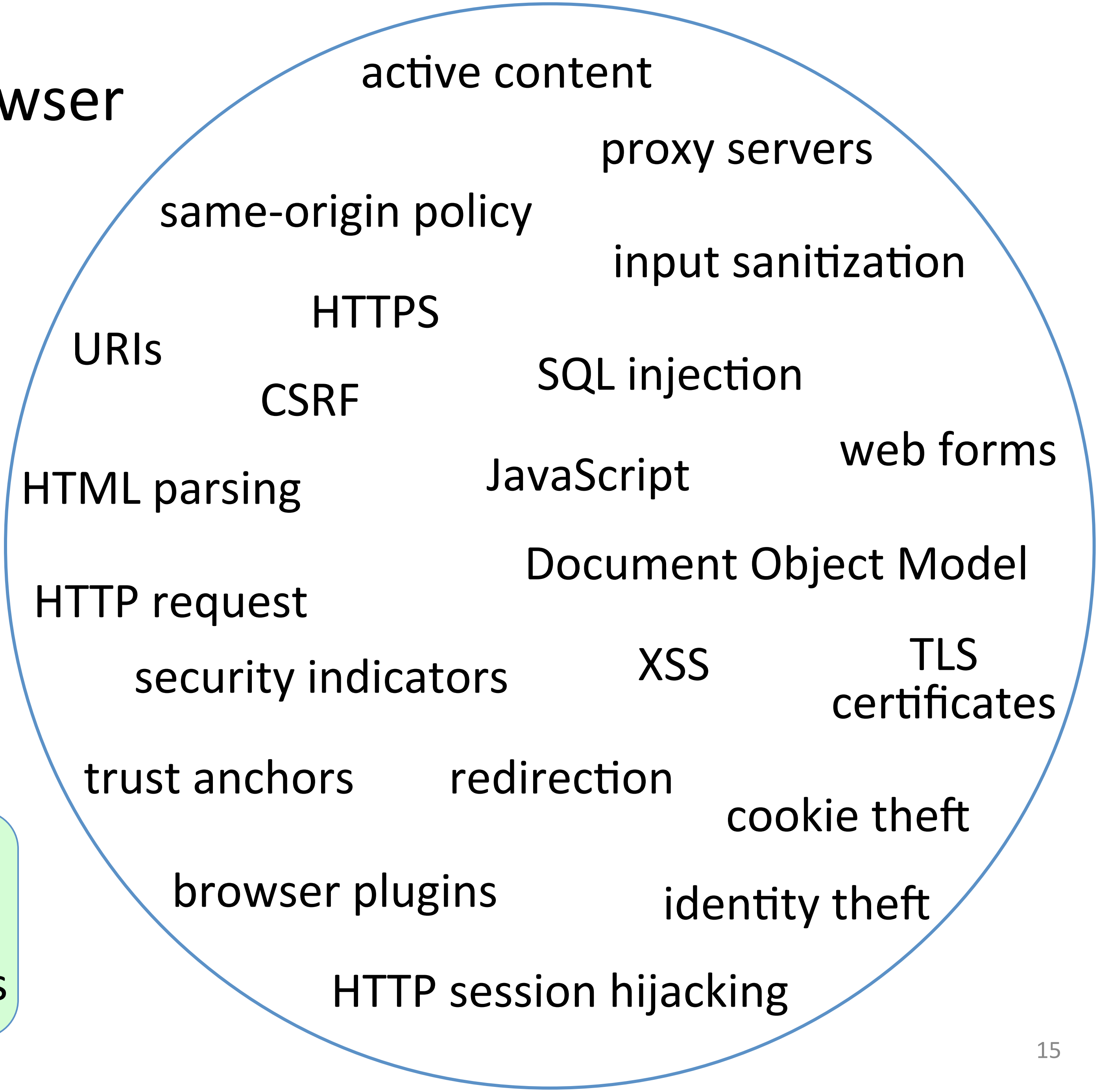
privilege escalation

race conditions

symbolic links

world-writable files

Web/Browser



active content

proxy servers

same-origin policy

input sanitization

HTTPS

URIs

SQL injection

CSRF

web forms

HTML parsing

JavaScript

Document Object Model

HTTP request

security indicators

XSS

TLS certificates

trust anchors

redirection

cookie theft

browser plugins

identity theft

HTTP session hijacking

usable security

mental models

Networks

stateless packet filters

sockets

perimeter network

anomaly-based IDS

ingress filtering

proxy firewalls

IPv6

encrypted tunnels

NAT

screening routers

host-based firewalls

SSH

circuit-level proxy

dual-homed host

IPsec

Bro

ICMP

Snort

TCP sequence numbers

IPS

port forwarding

pen-testing

DMZ

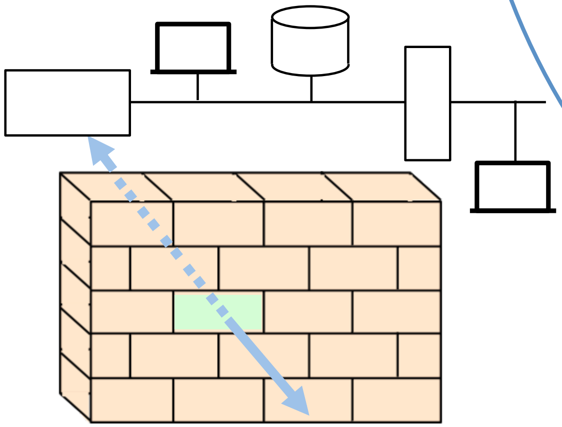
vulnerability scanners

encapsulation

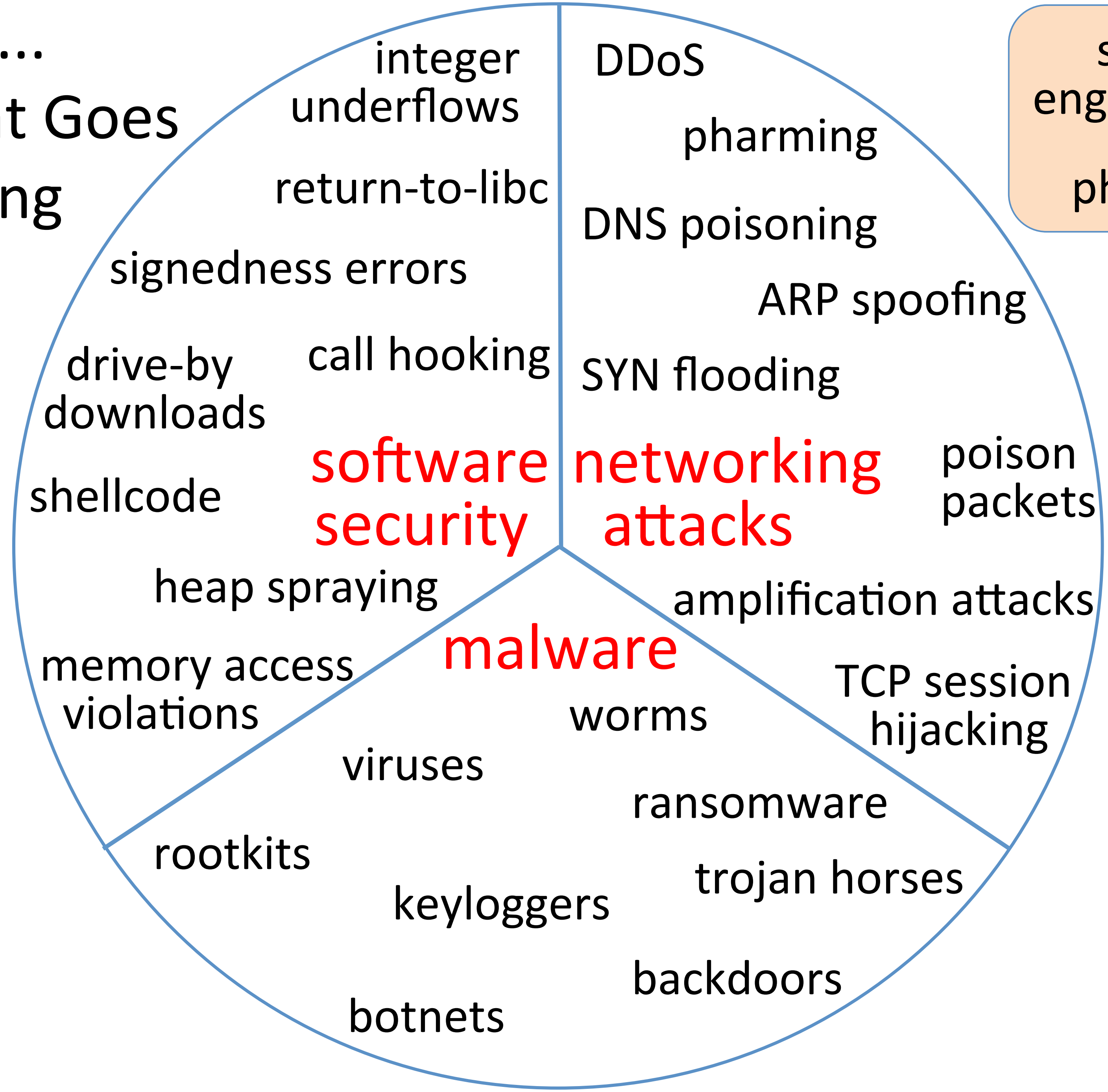
exploitation toolkits

VPNs

IP datagrams



and ... What Goes Wrong



software security

integer underflows

return-to-libc

signedness errors

drive-by downloads

call hooking

shellcode

heap spraying

memory access violations

networking attacks

DDoS

pharming

DNS poisoning

ARP spoofing

SYN flooding

poison packets

amplification attacks

TCP session hijacking

malware

worms

viruses

ransomware

rootkits

trojan horses

keyloggers

backdoors

botnets

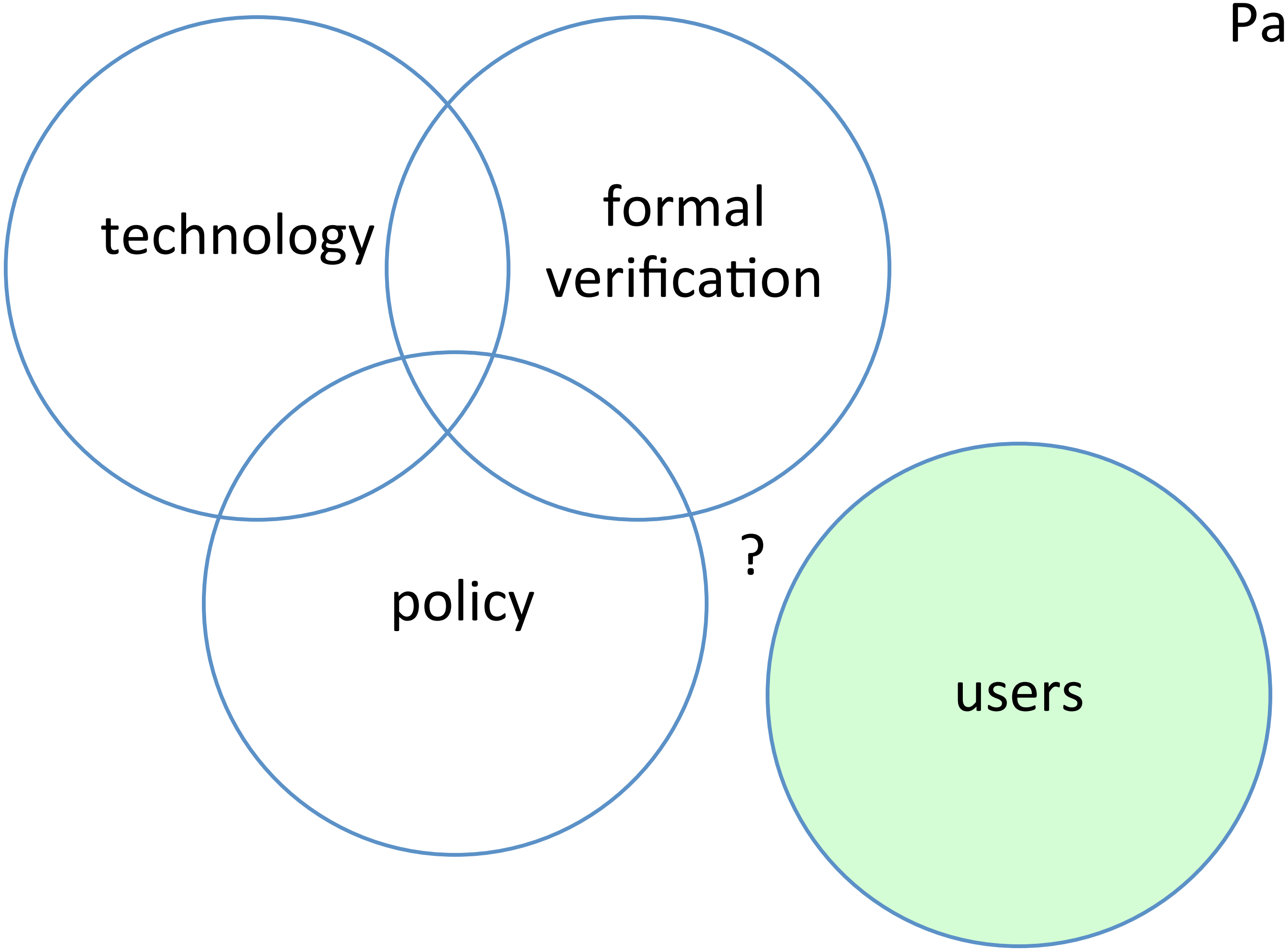
social engineering

phishing

... and lots more ....

- trusted computing & hardware
- privacy & ethics
- virtualization security
- cloud computing
- wireless access
- formal verification
- side channel attacks
- platform hardening, security assessment, fuzzing
- IoT ...

Opportunities


technology

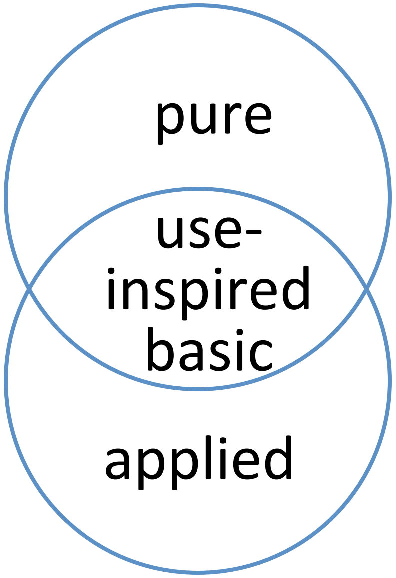
formal verification

policy

?

users

Pasteur's Quadrant


pure

use-inspired basic

applied

20 Design Principles for Security

- P1: Simplicity-and-necessity
- P2: Safe-defaults
- P3: Open-design
- P4: Complete-mediation
- P5: Isolated-compartments
- P6: Least-privilege
- P7: Modular-design
- P8: Small-trusted-bases
- P9: Time-tested-tools
- P10: Least-surprise
- P11: User-buy-in
- P12: Sufficient-work-factor
- P13: Defense-in-depth
- P14: Evidence-production
- P15: Data-type-verification
- P16: Remnant-removal
- P17: Trust-anchor-justification
- P18: Independent-confirmation
- P19: Request-response-integrity
- P20: Reluctant-allocation

HP1: Security-by-design

HP2: Design-for-evolution

Books?

Welchman. *The Hut Six Story* (1982, 1/e)

Martin. *Everyday Cryptography* (2017, 2/e)

Menezes, vanO, Vanstone. *Handbook of Applied Cryptography* (1996)

Hankerson, Menezes, Vanstone. *Guide to EC Cryptography* (2004)

Boyd, Mathuria. *Protocols for Auth. & Key Establishment* (2003, 2019)

Garfinkel, Lipford. *Usable Security: History, Themes, Challenges* (2014)

Gasser. *Building a Secure Computer System* (1988)

Jaeger. *Operating System Security* (2008) [Tanenbaum: *Modern OS*]

Curry. *Unix System Security* (1992)

Dowd, McDonald, Schuh. *Art of S/W Security Assessment* (2006)

Books [2/2]

Szor. *Art of Computer Virus Research and Defense* (2005)

Aycock. *Computer Viruses and Malware* (2006)

P. Denning. *Computers Under Attack: Intruders, Worms, Viruses* (1990)

Housley, Polk. *Planning for PKI: Best Practices for Deploying PKI* (2001)

Orman. *Encrypted Email: History & Technology of Msg Privacy* (2015)

Zalewski. *Tangled Web: Guide to Securing Modern Web Apps* (2011)

Snader. *VPNs Illustrated: Tunnels, VPNs, IPsec* (2005)

Zwicky, Cooper, Chapman. *Building Internet Firewalls* (2000, 2/e)

Bace. *Intrusion Detection* (2000).

Skoudis, Liston. *Counter Hack Reloaded: Attacks & Defenses* (2006, 2/e)

Harper et al. Gray Hat Hacking: *Ethical Hacker’s Handbook* (2011, 3/e)

Concluding Remarks re: Security

Whether planning a research program, or how to teach, think:

- framework
- pigeonholes
- context

Thank you ... Questions?