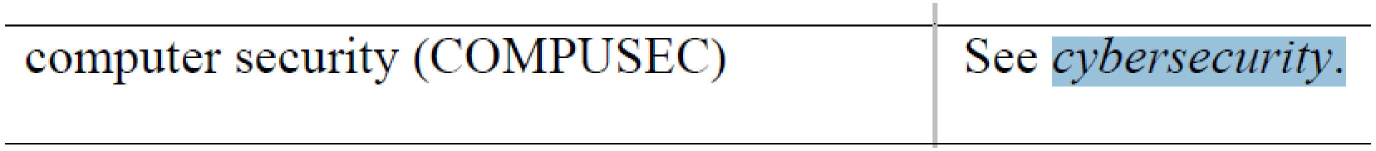
DEFINITIONS

CYBER VS COMPUTER VS INFORMATION SECURITY

- InfoSec
  - » *the most encompassing term – goes beyond digital (e.g., paper records)*
- Cyber vs Computer
  - » *CNNSI 4009:*



computer security (COMPUSEC)	See *cybersecurity*.

  - » *cyber ≈ computer + network*
- For our purposes, all three will be synonyms:
  - » *only interested in digital assets*
  - » *all systems of interest are networked → network security for computers is mandatory*

CNNSI 4009: CYBERSECURITY

- Prevention of damage to, protection of, and restoration of
  - » *computers, electronic communications systems, electronic communications services, wire communication, and electronic communication,*
  - » *including* ***information*** *contained therein, to ensure its*
  - » ***availability****,* ***integrity****,* ***authentication****,* ***confidentiality****, and* ***nonrepudiation****.*

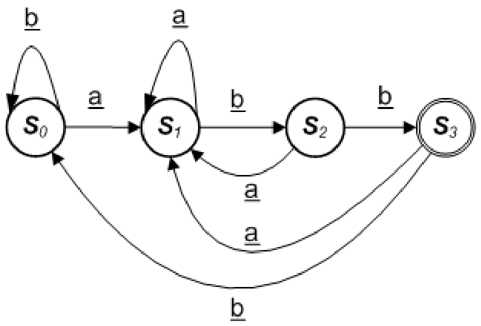
NISTIR 7298 R2

- Cybersecurity
  - *“The ability to protect or defend the use of cyberspace from cyber attacks.”*
- Cyberspace
  - *“A global domain within the information environment consisting of*
    - the interdependent network of information systems infrastructures including
      - the Internet,
      - telecommunications networks,
      - computer systems, and
      - embedded processors and controllers.”

STALLINGS: COMPUTER SECURITY

- "Measures and controls that ensure
  - *confidentiality, integrity, and availability of*
  - *information system assets including*
    - hardware,
    - software,
    - firmware, and
    - information being processed, stored, and communicated."

MORE DEFINITIONS



- A system is secure if it starts from a secure state, and

  is not allowed to transition to states that are deemed not secure.

- Security policy
  - *A statement that partitions the states of the system into secure states and non-secure states*

- A system is secure if it **starts** from a **secure** state, and

  is **not allowed** to transition to states that are deemed **not secure**,

  according to the security policies.

SECURITY IS ***ALWAYS*** RELATIVE TO

- A set of desired properties / policies
- An adversary with specific capabilities – ***THREAT MODEL***

SECURITY MECHANISMS

- Entities or procedures that are meant to ***enforce*** the security policies

- Breach of security:

  A system enters an unauthorized (non-secure) state

  - *It is a failure of the security mechanism(s)*

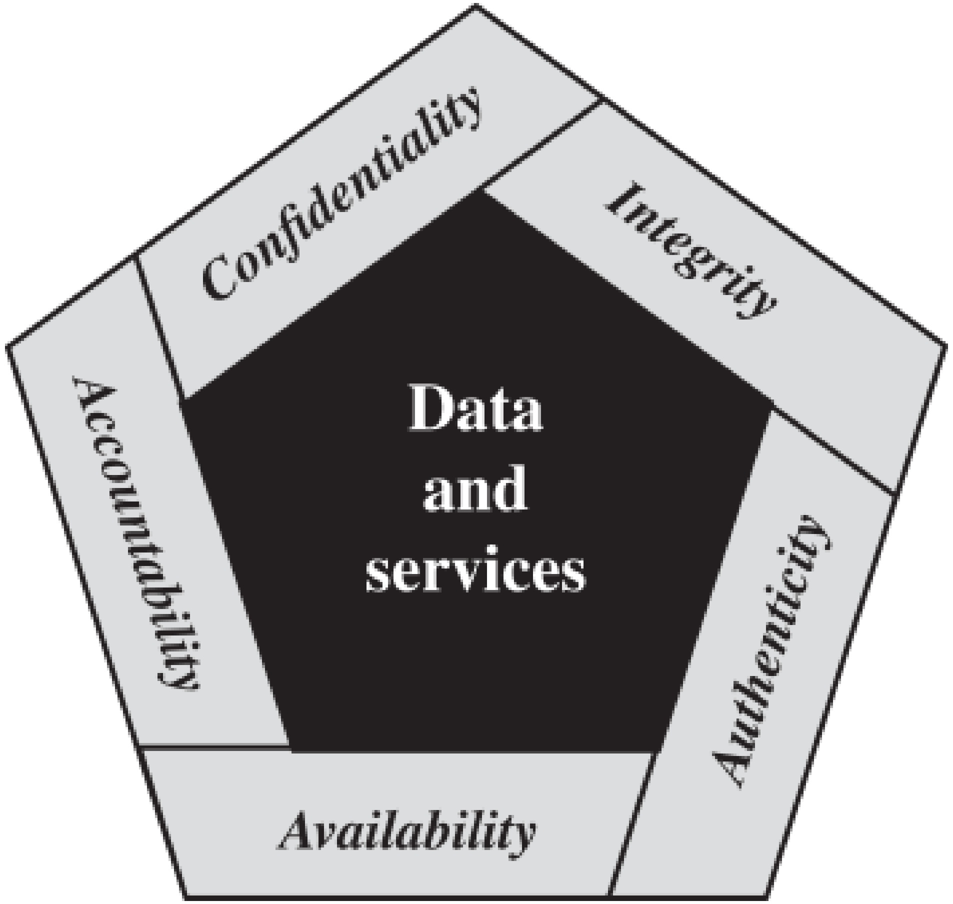
EXAMPLE: MULTI-USER COMPUTER SYSTEM

- Security policy:
  - » *a user **U** shall not be allowed to delete or modify files belonging to other users, unless the owners of a file explicitly grants such permission to **U**.*
- Security mechanism:
  - » *OS file-system access control mechanisms*
- Breach of security example:
  - » *Alice exploits a vulnerability in the OS file-system that allows her to delete other people's files*

  ➔ *The exploit causes the system to transition from a secure state to a non-secure state*

SECURITY REQUIREMENTS/GOALS

A CONCISE VERSION



CONFIDENTIALITY PROPERTY

- Information must remain accessible only to authorized parties, whether stored (at rest) or in transit (in motion)

- Mechanisms
  - *access control*
  - *data encryption + protocols*
  - *steganography*

Integrity

- Data, software or hardware must remain unaltered, except by authorized parties.
- Mechanisms
  - *error detection/correction codes*
  - *cryptographic digests*

AVAILABILITY

- Information, services and computing resources must remain accessible for authorized use.

- Mechanisms
  - *fault tolerance/resilience*
  - *detection and protection against denial-of-service attacks*

AUTHORIZATION

- Computing resources must accessible only by authorized entities.
  - *e.g., those approved by the resource owner or domain administrator.*

- Mechanism
  - *access control*

AUTHENTICATION

- Principal (definition):
  - *An agent representing a user, communicating entity, or system process.*
- A principal has ***priviliges*** specifying the resources it is authorized to access
  - *identity of a principal is critical → asserted identities must be verified*
- Authentication
  - *assurance that a principal, data, or software is genuine relative to expectations arising from appearances or context*
  - ***DATA (ORIGIN) AUTHENTICATION***
    - implies integrity
  - ***ATTRIBUTION***

Accountability

- The ability to identify principals responsible for past actions

- Mechanism
  - *(secure) transaction logs*

- Implies ***non-repudiation***
  - *principals cannot later credibly deny previous commitments or actions*

TRUSTED VS TRUSTWORTHY

- Trusted
  - *something that **has** our confidence*
- Trustworthy
  - *something **deserves** our confidence*
    - i.e., will reliably meet expectations

CONFIDENTIALITY VS PRIVACY & ANONYMITY

- Confidentiality
  - *information protection to prevent unauthorized disclosure*

- Information privacy
  - *protection of and sharing control of personally sensitive information*

- Anonymity
  - *one's actions or involvement are not linkable to a public identity*

ASSETS & POLICY

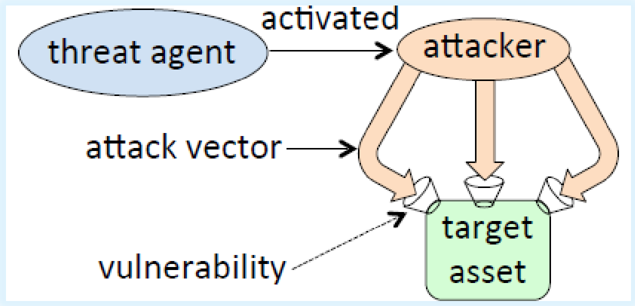
- Digital
  - *information, software, hardware, computing & communications services*
- Physical
  - *cyber-physical systems (e.g., ICS/SCADA) control*
  - *… physical property, hardware, financils, etc.*
- Policy
  - *defines what protection each assets needs*

POLICIES: THEORY VS. PRACTICE

- Theory
  - *formal security policy precisely defines each possible system state as either*
    - **authorized** (**secure**) or
    - **unauthorized** (**non-secure**).
  - *security policy is violated if the system moves into an unauthorized state*
- Practice
  - *security policies are often **informal** documents including guidelines and expectations*
  - *formulating precise policies is more difficult and time-consuming*
    - formal policies that are mathematically verifiable are something of a holy grail

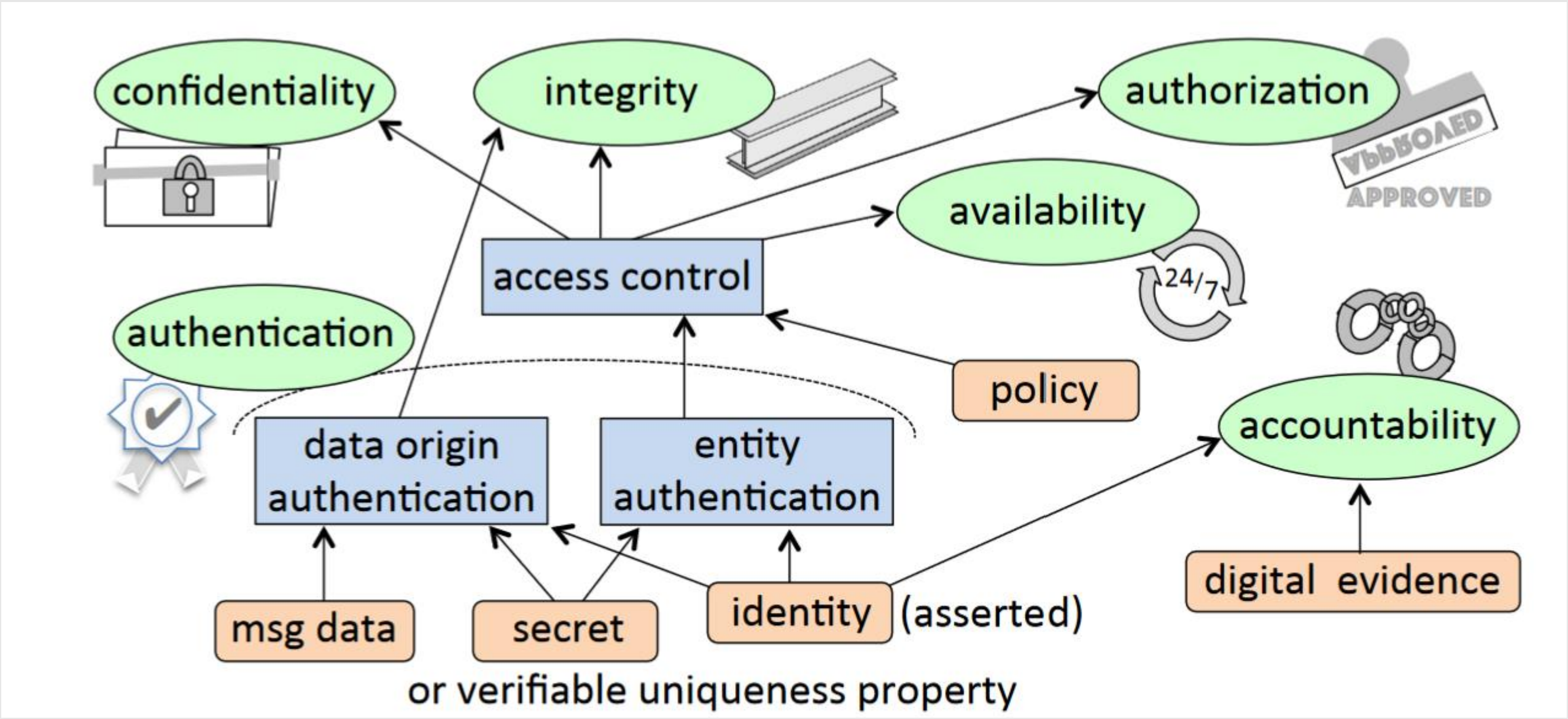
ATTACKS & AGENTS

- Attack
  - » *deliberate execution of one or more steps intended to cause a security violation*
    - e.g., unauthorized access
  - » *exploits specific vulnerabilities*
- Vulnerability
  - » *specific system characteristics that enable (directly, or indirectly) policy violations*
    - design flaws, implementation flaws, configuration errors, etc.
- Thread agent/actor
  - » *the source of an attack, aka* ***adversary/attacker***



[CREDIT: Oorschot]

A MORE COMPLETE PICTURE

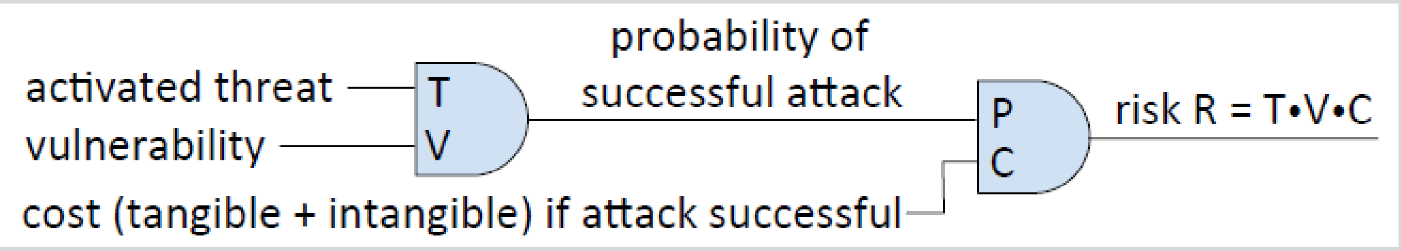


[CREDIT: Oorschot]

RISK

RISK

- Motivation
  - » *need to understand the losses that might result from security violations*
- Risk
  - » *the expected loss due to harmful future events, relative to an implied set of assets and over a fixed time period*
  - » *depends on*
    - threat agents, probability of attack & expected losses
- Risk equation
  - » $R = T \times V \times C$


activated threat
vulnerability
T
V
probability of successful attack
P
C
risk R = T•V•C
cost (tangible + intangible) if attack successful

[CREDIT: Oorschot]

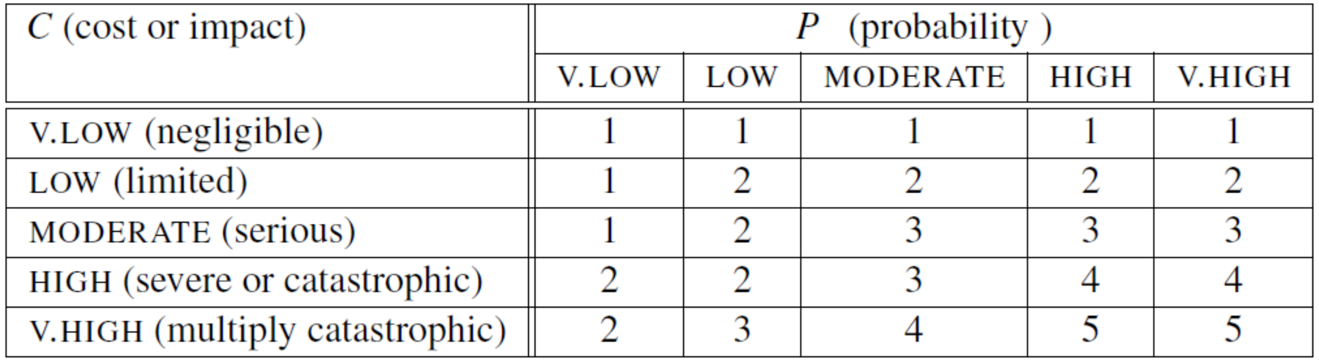
Risk modeling

- Estimating unknowns
  - *it is often difficult to put credible numbers in the equation*
- Modeling expected losses—***annual expected losses*** (*ALE*)
  - $ALE = \sum_{i=1}^{n} F_i \, C_i$
- Risk
  - *the expected loss due to harmful future events, relative to an implied set of assets and over a fixed time period*
  - *depends on*
    - threat agents, probability of attack & expected losses
- Risk equation
  - $R = T \times V \times C$

RISK ASSESSMENT

- Questions
  - *What assets are most valuable, and what are their values?*
  - *What system vulnerabilities exist?*
  - *What are the relevant threat agents and attack vectors?*
  - *What are the associated estimates of attack probabilities, or frequencies?*
- Cost-benefits analysis
  - *given limited resources ($, hardware, worktime)—what is the best way to deploy them?*
- Risk assessment challenges
  - *incomplete knowledge of vulnerabilities, worsened by rapid technology evolution;*
  - *difficult to quantifying the value of intangible assets*
    - strategic information, corporate reputation
  - *incomplete knowledge of threat agents and their adversary classes*

QUALITATIVE RISK ASSESSMENT



C (cost or impact)	*P* (probability)				
	V.LOW	LOW	MODERATE	HIGH	V.HIGH
V.LOW (negligible)	1	1	1	1	1
LOW (limited)	1	2	2	2	2
MODERATE (serious)	1	2	3	3	3
HIGH (severe or catastrophic)	2	2	3	4	4
V.HIGH (multiply catastrophic)	2	3	4	5	5

[CREDIT: Oorschot]

- Risk management vs. mitigation
  - *not all threats can/should be mitigated by technical means*
  - *other means*
    - transfer risk to third parties—e.g., cloud provider, insurance, etc.
    - accept risk—either by choice, or necessity

ADVERSARY MODELING

Adversary attributes

- Objectives
  - *these often suggest target assets requiring special protection*
- Methods
  - *e.g., the anticipated attack techniques, or types of attacks*
- Capabilities
  - *computing resources (CPU, storage, bandwidth), skills, knowledge, personnel, opportunity (e.g., physical access to target machines)*
- Funding level
  - *this influences attacker determination, methods and capabilities*
- Outsider vs. insider
  - ***outsider attacks** are launched w/o any prior special access to the target network is an*
  - ***insider attacks** originate from parties having some starting advantage*
    - e.g., an employee (current/former)

NAMED GROUPS OF ADVERSARIES

1. Foreign intelligence
   - *including government-funded agencies*
2. Cyber-terrorists or politically-motivated adversaries
3. Industrial espionage agents
   - *perhaps funded by competitors*
4. Organized crime (groups)
5. Lesser criminals and crackers/hackers
   - *i.e., **individuals** who break into computers*
6. Malicious insiders
   - *e.g., disgruntled employees*
7. Non-malicious employees
   - *often security-unaware*

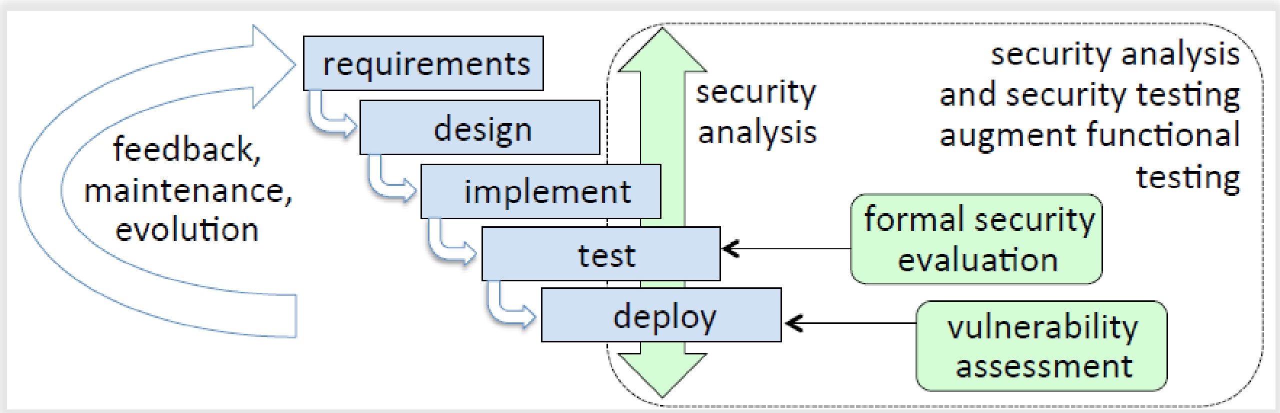
THREATS & CONTROLS

- Threat
  - *any combination of circumstances and entities that might harm assets, or cause security violations*
    - a **credible** threat has both the means and intent
- Attack vectors
  - *specific methods, or sequences of steps, by which attacks are carried out*
- Controls & countermeasures
  - *used to enforce policies aiming to*
    - prevent violations, or
    - (quickly) detect violations in order to react to limit damage, and
    - recover from violations.
- Schemas
  - *for attackers: categorical, capability-based*
  - *for attacks: targeted, opportunistic, generic*

Security evaluations & pen testing

- Security audit
  - *verify adherence to policies*
- Penetration test
  - *adversary simulation*
  - *black-box vs. white-box*
  - *planned vs. unannounced*

SECURITY ANALYSIS

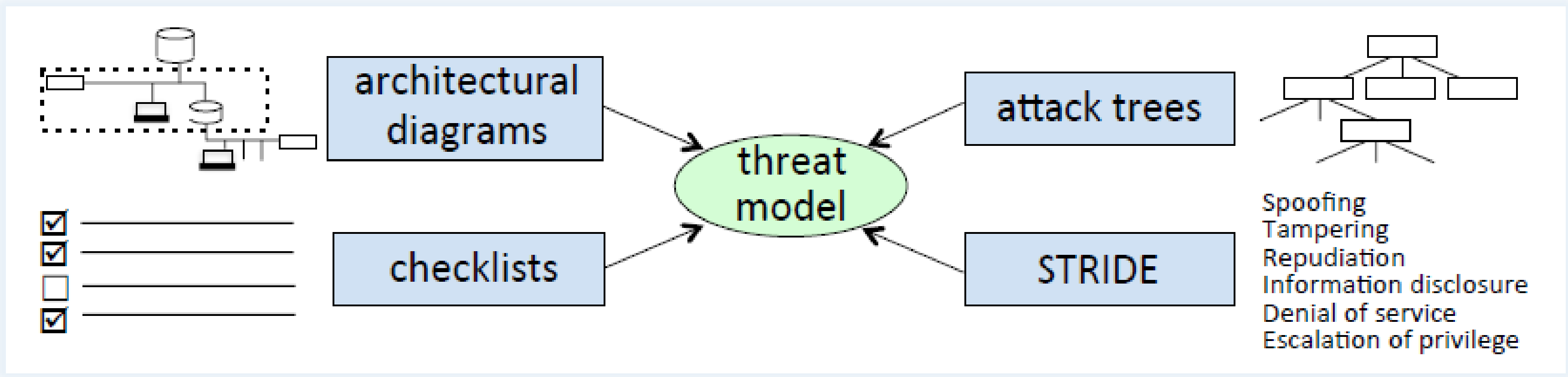

requirements
design
implement
test
deploy
feedback, maintenance, evolution
security analysis
security analysis and security testing augment functional testing
formal security evaluation
vulnerability assessment

[CREDIT: Oorschot]

- Aims to identify vulnerabilities (primarily design-related) and overlooked threats
  - *ideally, it takes place throughout the lifecycle of the product*
- Main focus
  - *security architecture*
- Security model
  - *relates system components to parts of the security policy to be enforced*

Threat modeling

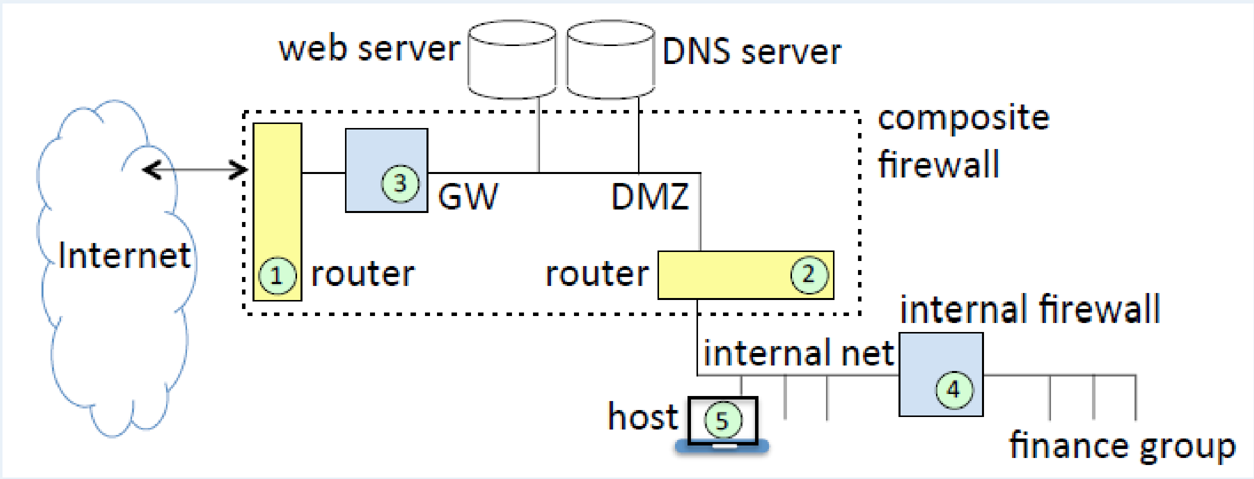
- Threat model
  - *identifies threats, threat agents, and attack vectors that the target system considers in scope to defend against—known from the past, or anticipated*
- Different approaches are used:



[CREDIT: Oorschot]

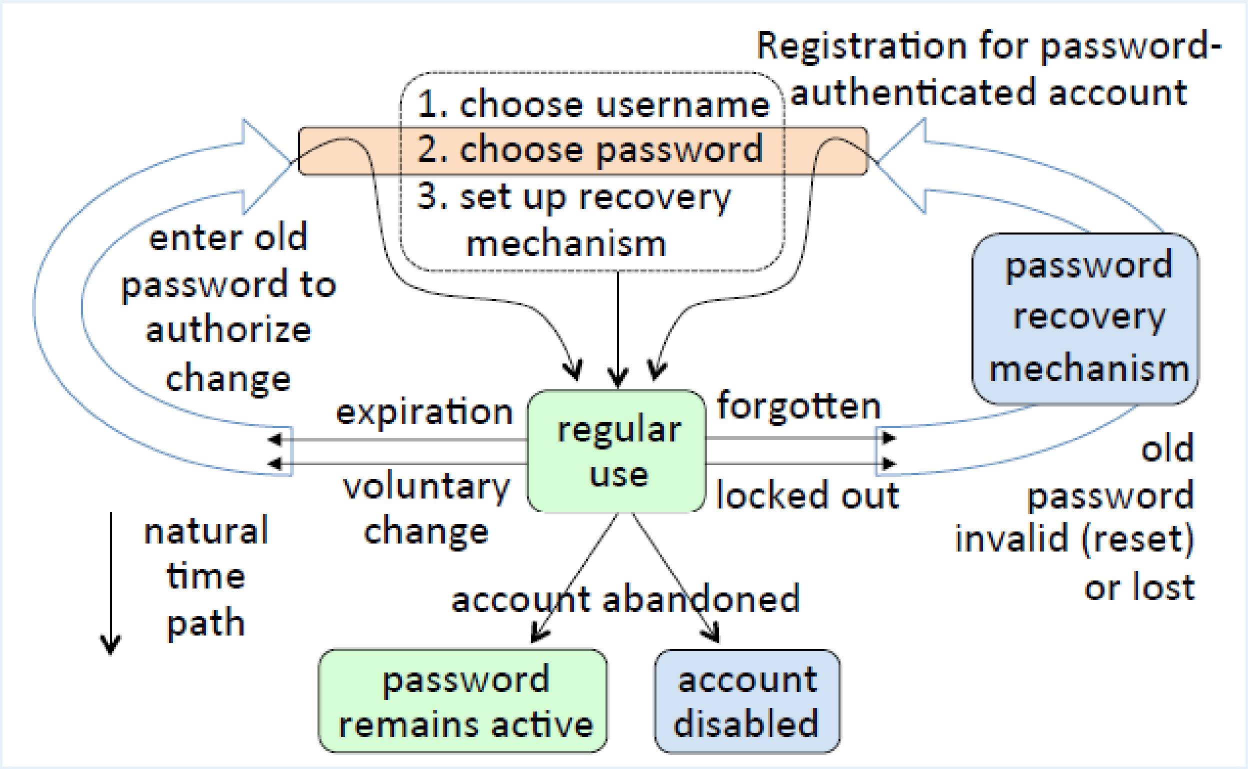
DIAGRAM-DRIVEN THREAD MODELING

- Starting point an architectural diagram, i.e.:
  - » *architectural*
  - » *data flow*
  - » *user workflow*
  - » *lifecycle*



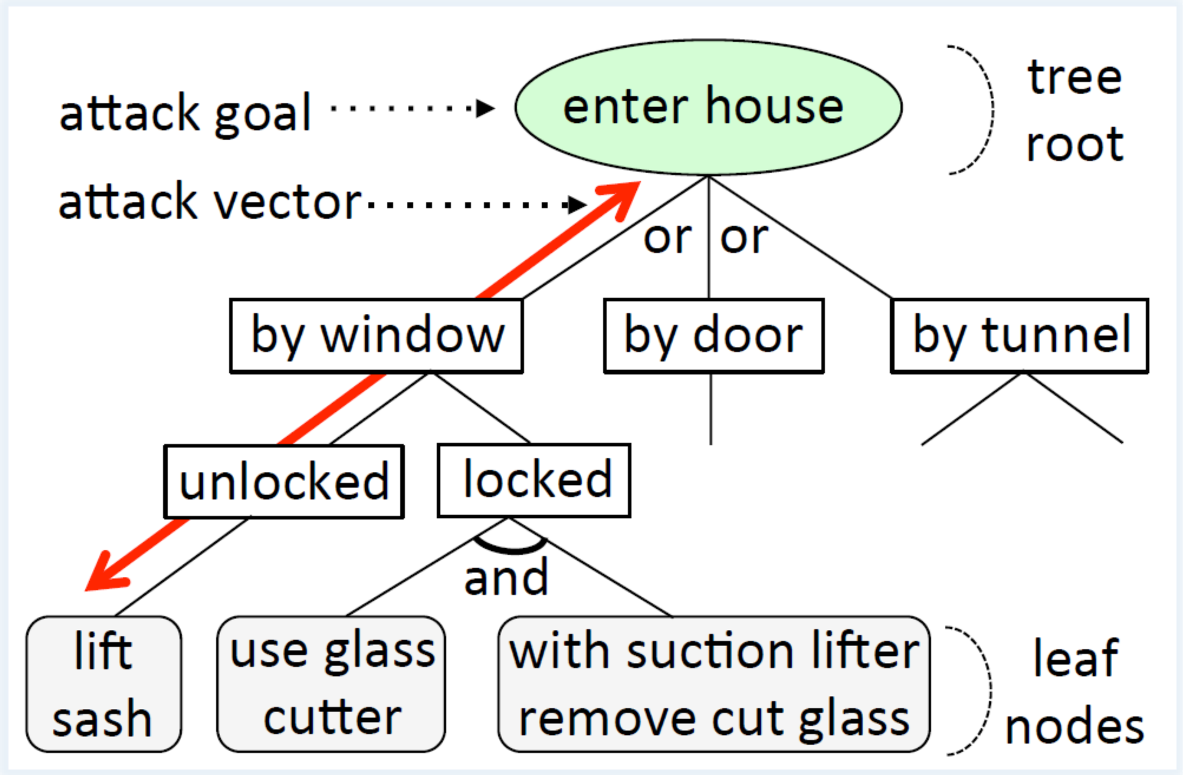
[CREDIT: Oorschot]

Ex: Password-authenticated account lifecycle


Registration for password-authenticated account
1. choose username
2. choose password
3. set up recovery mechanism
enter old password to authorize change
password recovery mechanism
expiration
regular use
forgotten
voluntary change
locked out
old password invalid (reset) or lost
natural time path
account abandoned
password remains active
account disabled

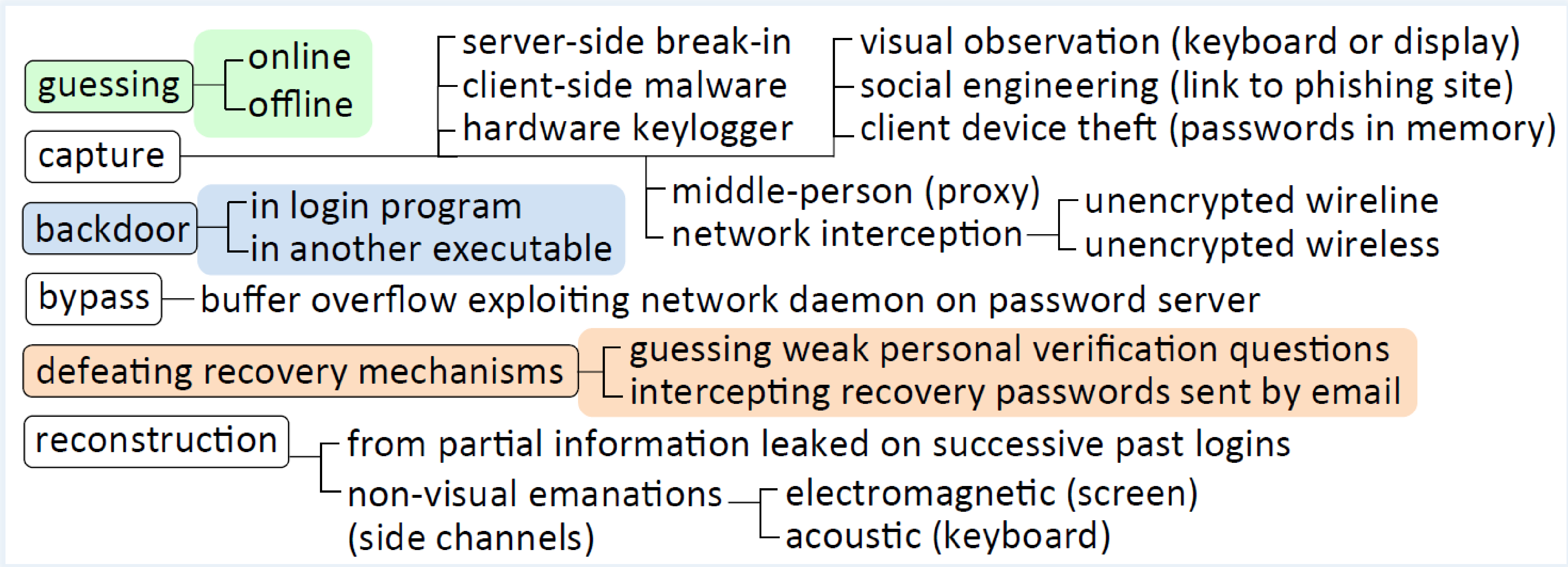
[CREDIT: Oorschot]

Ex: Attack tree



[CREDIT: Oorschot]

Ex: Attack list



- guessing
  - online
  - offline
- capture
  - server-side break-in
  - client-side malware
  - hardware keylogger
  - visual observation (keyboard or display)
  - social engineering (link to phishing site)
  - client device theft (passwords in memory)
  - middle-person (proxy)
  - network interception
    - unencrypted wireline
    - unencrypted wireless
- backdoor
  - in login program
  - in another executable
- bypass
  - buffer overflow exploiting network daemon on password server
- defeating recovery mechanisms
  - guessing weak personal verification questions
  - intercepting recovery passwords sent by email
- reconstruction
  - from partial information leaked on successive past logins
  - non-visual emanations (side channels)
    - electromagnetic (screen)
    - acoustic (keyboard)

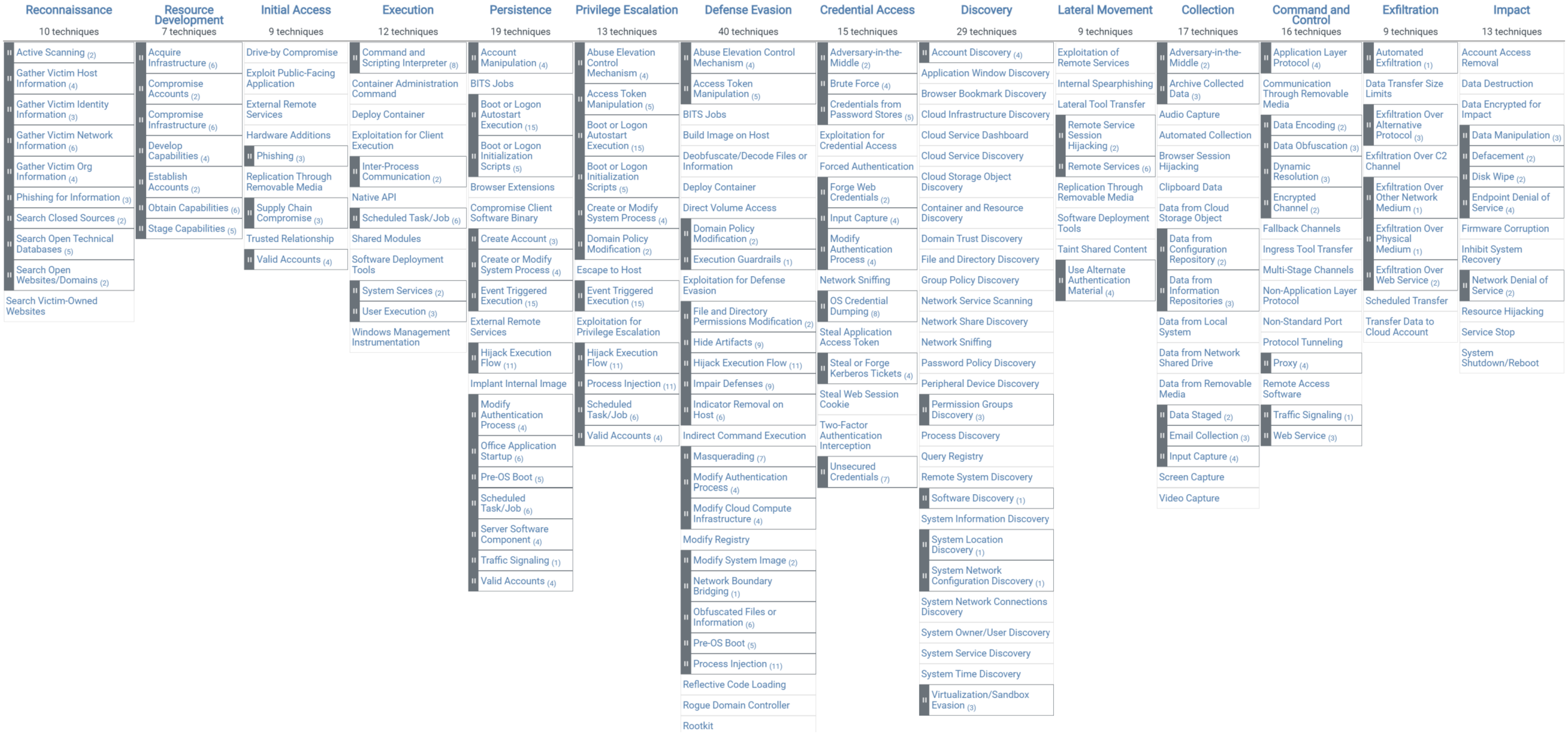
[CREDIT: Oorschot]

STRIDE

- **S**poofing
  - *attempts to impersonate a thing (e.g., web site), or an entity (e.g., user).*
- **T**ampering
  - *unauthorized altering, e.g., of code, stored data, transmitted packets.*
- **R**epudiation
  - *denial of responsibility for past actions*
- **I**nformation disclosure
  - *unauthorized release of data.*
- **D**enial of service
  - *impacting availability of services, or the quality of services, through malicious actions that consume resources or induce errors in systems*
- **E**scalation of privilege
  - *obtaining privileges to access resources*
    - typically referring to malware that gains a base level of access as a foothold and then exploits vulnerabilities to extend this to gain greater access

MITRE ATT&CK

a taxonomy of adversarial tactics and techniques attack.mitre.org



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (2)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (8)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	BITS Jobs	Credentials from Password Stores (5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (3)	Obtain Capabilities (6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (5)	Supply Chain Compromise (3)	Scheduled Task/Job (6)	Create Account (3)	Escape to Host	Direct Volume Access	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Web Service (2)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)		Trusted Relationship	Shared Modules	Create or Modify System Process (4)	Event Triggered Execution (15)	Domain Policy Modification (2)	Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Event Triggered Execution (15)	Exploitation for Privilege Escalation	Execution Guardrails (1)	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	External Remote Services	Hijack Execution Flow (11)	Exploitation for Defense Evasion	OS Credential Dumping (8)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (2)
			User Execution (3)	Hijack Execution Flow (11)	Process Injection (11)	File and Directory Permissions Modification (2)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			Windows Management Instrumentation	Implant Internal Image	Scheduled Task/Job (6)	Hide Artifacts (9)	Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
				Modify Authentication Process (4)	Valid Accounts (4)	Hijack Execution Flow (11)	Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Office Application Startup (6)		Impair Defenses (9)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (3)	Remote Access Software		
				Pre-OS Boot (5)		Indicator Removal on Host (6)	Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)		
				Scheduled Task/Job (6)		Indirect Command Execution		Peripheral Device Discovery		Screen Capture	Web Service (3)		
				Server Software Component (4)		Masquerading (7)		Permission Groups Discovery (3)		Video Capture			
				Traffic Signaling (1)		Modify Authentication Process (4)		Process Discovery					
				Valid Accounts (4)		Modify Cloud Compute Infrastructure (4)		Query Registry					
						Modify Registry		Remote System Discovery					
						Modify System Image (2)		Software Discovery (1)					
						Network Boundary Bridging (1)		System Information Discovery					
						Obfuscated Files or Information (6)		System Location Discovery (1)					
						Pre-OS Boot (5)		System Network Configuration Discovery (1)					
						Process Injection (11)		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
								Virtualization/Sandbox Evasion (3)					