System Administration

Week 11, Segment 1
System Security I: Assessing Risk

Department of Computer Science
Stevens Institute of Technology

Jan Schaumann
jschauma@stevens.edu
https://stevens.netmeister.org/615/

Photo by Casey Horner on Unsplash
This Week

What I won’t tell you:
• How to make your system ”secure”.
• How to break into other systems.
• Everything you need to know.

What I will tell you:
• What you need to know to start looking.
• What concepts are critical to understand.
• What conceptual pitfalls you are likely to encounter.
• A few always and nevers.
Security is not an end-goal.

Security is a *trade-off* property to help you increase resilience against *specific* risks.
System Security

You are Here

Political
Financial
Application
Presentation
Session
Transport
Network
Link
Physical
Where/how does ‘security’ come into play?

Disks, Storage:
- storage model (DAS, NAS, SAN, Cloud)
- partitions / mount options

Filesystem Basics / Software Types:
- firmware compromise on hard drives
- DoS on disk space
- filesystem features (permissions, access control lists)

Software Installation & Multi-user basics:
- software package management and updates
- VMs, containers, etc.
- patch management
- package integrity checking
- privileges and trust models
- authentication methods, multi-factor authentication
- raising privileges
Where/how does ‘security’ come into play?

Networking:
- protocols and visibility of data on different layers
- tcpdump can read all packets
- location of attacker on network implies capabilities
- physical networks
- network censorship
- plain text protocols

DNS; HTTP:
- If you control the DNS, you control the domain
- DNS registrars as attack points
- use of DNS as a second channel for other protocols
- trustworthiness of DNS (DNSSEC, DoT, DoH)
- HTTP as the universal entry into any network
- code execution context (CGI vs. server-side vs. client-side)
- content control and inspection capabilities of e.g. CDNs
Where/how does 'security' come into play?

HTTPS; SMTP:
- observation of packets via tcpdump(1)
- TLS authentication
- PKI, Certificate Authorities
- protocol downgrade and MitM attacks
- email as attack methods (spam, phishing)
- recipient and sender authentication, open relays
- SMTP plain text vs. opportunistic encryption

Writing System Tool:
- automation as a defensive weapon
- using the wrong tool for the job => writing insecure code
- understanding language / framework pitfalls
- simplicity reduces attack surface
- all code has bugs
Where/how does ‘security’ come into play?

Backup and Disaster Recovery, Monitoring:
• disasters include security breaches
• data loss as a risk
• safety of backups (encrypted backups?)
• incident detection via events, metrics, and context
• sensitive data in logs
• outsourcing monitoring services

Configuration Management:
• role based access control
• inherent trust, full control
• CAP theorem may impact security controls

Security touches everything.
herself for the performance of another's contract. See 3 Blackf. R. 431.

From U.S. Gazetteer Places (2000) [gaz2k-places]:

Security-Widefield, CO -- U.S. Census Designated Place in Colorado
  Population (2000):    29845
  Housing Units (2000): 10177
  Water area (2000):   .040374 sq. miles (0.105391 sq. km)
  Total area (2000):   14.562629 sq. miles (37.617857 sq. km)
  FIPS code:
  Located within:     Colorado (CO), FIPS 08
  Location:             38.744731 N, 104.723226 W
  ZIP Codes (1990):
  Note: some ZIP codes may be omitted esp. for suburbs.
  Headwords:
    Security-Widefield, CO
    Security-Widefield
    Security, CO
    Security

Freedom from risk.
himself for the performance of another's contract. See 3 Blackf. R. 431.

From U.S. Gazetteer Places (2000) [gaz2k-places]:

Security-Widefield, CO — U.S. Census Designated Place in Colorado
Population (2000): 29845
Housing Units (2000): 10177
Water area (2000): 0.493456 sq. miles (1.278046 sq. km)
Total area (2000): 15.015711 sq. miles (38.890512 sq. km)
FIPS code: 68847
Located within: Colorado (CO), FIPS 08
Location: 38.744731 N, 104.723226 W
ZIP Codes (1990):
Note: some ZIP codes may be omitted esp. for suburbs.
Headwords:
  Security-Widefield, CO
  Security-Widefield
  Security, CO
  Security
Suffering harm or loss of what?

- access to data
- integrity of data
- availability of services
- reputation
- monetary loss due to any of the above
- monetary loss due to physical items of actual value
- ...
How to determine risk

“Risk Assessment”

• identify assets (that which you wish to protect, what you value)
How to determine risk

“Risk Assessment”

• identify assets

• identify threats (possible dangers to your assets, bad things that might happen)
How to determine risk

“Risk Assessment”

• identify assets
• identify threats
• identify vulnerabilities (weaknesses in a system, component, protocol, …)
How to determine risk

“Risk Assessment”

• identify assets
• identify threats
• identify vulnerabilities
• determine likelihood of damage (considering mitigating or exacerbating factors)
How to determine risk

“Risk Assessment”

• identify assets
• identify threats
• identify vulnerabilities
• determine likelihood of damage
• estimate cost of recovery (including recovery of data, immediate revenue loss, replacing physical items, ...)

CS615 - System Administration
How to determine risk

“Risk Assessment”

• identify assets
• identify threats
• identify vulnerabilities
• determine likelihood of damage
• estimate cost of recovery
• estimate cost of defense (objectively, without consideration of your budget; include partial defense or mitigating strategies)
How to determine risk

“Risk Assessment”

- identify assets
- identify threats
- identify vulnerabilities
- determine likelihood of damage
- estimate cost of recovery
- estimate cost of defense

A risk is the likelihood of a threat successfully exploiting a vulnerability and the estimated cost (or potential damage) both in the short and long term you may incur as a result.
Never waste resources on unspecified, vague risks or FUD.

Always remember that risks are scoped and specific.
How do we secure a system?

You can’t “secure” a system.

You can *minimize specific risks* by e.g.:

• closing an attack vector
• eliminating a vulnerability
• reducing the attack surface
• changing the economics of the adversary

..but for that, you need a *threat model*.