Lecture 27: Review and Conclusion

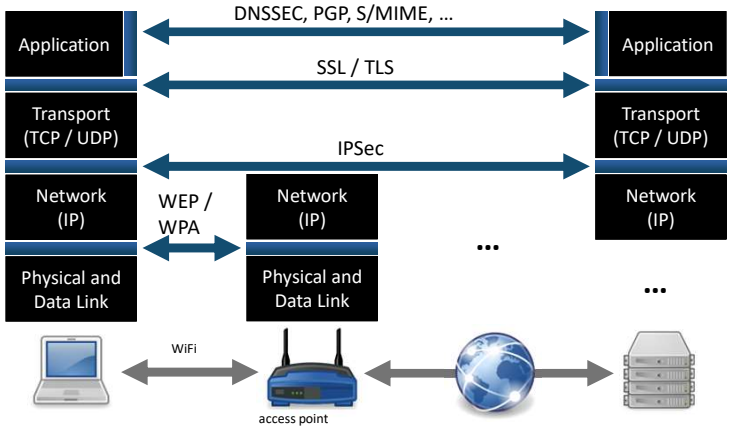
Stephen Huang

1. Review

Cryptographic Primitives

	Symmetric-key	Asymmetric-key	
Confidentiality	Block ciphers, Stream ciphers	Asymmetric-key encryption	
Integrity	Message authentication	Digital signatures	Hash functions

Security Protocols



WiFi Security

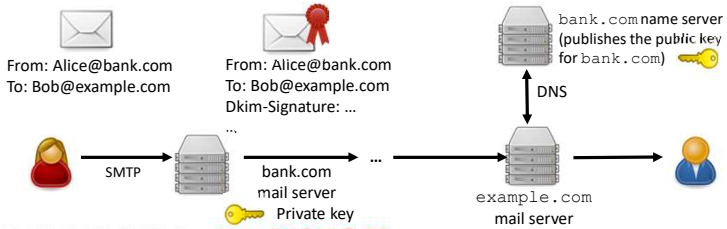
- Challenges: no inherent physical protection
- Simple "solutions" (which do not provide security)
  - hidden SSID, MAC filtering
- WEP (Wired Equivalent Privacy): serious flaws
- WPA 2 (WiFi Protected Access) = IEEE 802.11i
  1. discovery: station and AP agree on authentication and cipher suites
  2. authentication (includes key exchange): PSK or IEEE 802.1X
     - IEEE 802.1X: based on EAP, supports multiple authentication methods
  3. key management: derive / distribute transient pairwise / group keys
  4. protected data transfer: TKIP or CCMP (AES in CCM mode with 48-bit packet number to prevent replay)

IPSec and SSL/TLS

- IPSec
  - security between two hosts or networks (*e.g.*, VPN)
  - Authentication Header and Encapsulating Security Payload protocols in tunnel / transport mode
- SSL/TLS (Secure Socket Layer / Transport Layer Security)
  - security between client and server applications (i.e., two TCP ports), *e.g.*, HTTPS for secure web browsing
  - protocols: Record, Handshake (capabilities, key exchange, authentication), ChangeCipherSpec
    - session resume
- DNSSEC (Domain Name Security Extension), DNS over HTTPS (DoH), and DNS over TLS (DoT)
  - motivation: DNS cache poisoning (and privacy)

E-Mail Security

- PGP (Pretty Good Privacy) and S/MIME (Secure MIME)
  - provide end-to-end confidentiality and integrity between users
  - integrity: signature using the sender's private key
  - encryption: generate symmetric key and encrypt it with the recipients' public key
- DKIM (DomainKeys Identified Mail)
  - prevents e-mail spoofing using digital signatures
- SPF (Sender Policy Framework), DMARC



Authentication

- Authentication: confirming identity (*e.g.*, user or host)
- Authorization/access control: specifying access rights/privileges to resources

User Authentication and Access Control

- User authentication
  - factors: knowledge, inherence, ownership
  - multi-factor authentication
  - password-based authentication
    - attacks: online/offline guessing, precomputed hashes
    - countermeasures: hashing, salting
- Access control
  - subjects: entities that can perform actions on the system
  - objects: resources to which access must be controlled
  - types: DAC, MAC, ACL, RBAC
  - Unix access control: user and group IDs, permission bits

Software Vulnerabilities

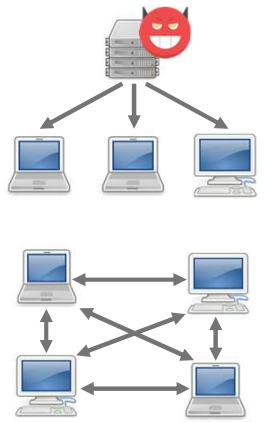
- Buffer overflow
  - when a process tries to store data beyond the boundaries of a fixed-length buffer
  - affects buffers on both the stack and the heap, may lead to arbitrary code execution
- Integer overflow
  - when an arithmetic operation leads to a value that is greater than the maximum value that can be stored
- Race condition
  - when results depend on the sequence or timing of uncontrollable events
  - no changes should be allowed between time of check and time of use
- …

Web Vulnerabilities

- File inclusion and file upload vulnerabilities
- Command injection
  - SQL injection (execute arbitrary SQL statements and queries) and its prevention
- XSS (Cross-Site Scripting)
  - enables an attacker to inject client-side script code into webpages generated by a webserver
  - main types: reflected and stored
- CSRF (Cross-Site Request Forgery)
  - enables an attacker to trick a user into sending malicious requests to a webserver
- …

Malware

- Types (propagation and functionality)
  - **backdoor** (or trapdoor): secret entry point into a system or program that circumvents the usual security access procedures
  - **trojan horse**: apparently benign application, which has some hidden malicious functionality
  - **worm**: independently running, self-replicating malware
  - **ransomware**: holds a computer system or data hostage
  - **botnet**: collection of "zombie" computers controlled through the Internet
  - …



Software Security and Adversarial Tactics

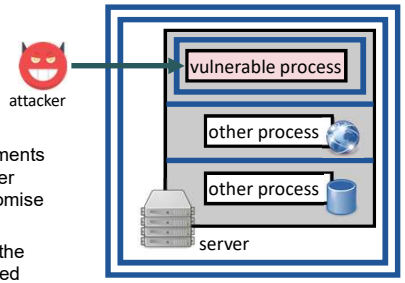
- Countermeasures against memory exploits
  - compile-time: languages/platforms/functions/libraries, stack canaries
  - run-time: executable space protection, ASLR
- Secure coding
  - input validation: blacklists vs. whitelists
  - code analysis: static vs. dynamic, *example*: taint analysis
- Attack phases
  - initial access
  - persistence
  - privilege escalation
  - …

Intrusion Detection Systems

- IDS (Intrusion Detection System): application or device that monitors a network or system for malicious activity
  - monitored activity
    - network-based: monitors network traffic
    - host-based: monitors activity on a host (*e.g.*, file accesses and processes)
  - detection method
    - signature-based: detect known attacks based on specific patterns
    - anomaly-based: detect "abnormal" behavior

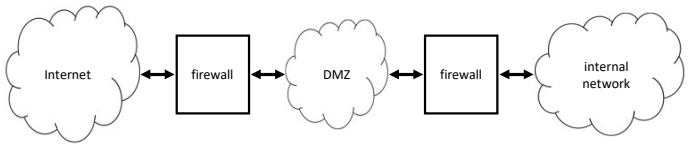
Principles of Secure Design

- Defense-in-depth: multiple-layers of security
  - attacker has to circumvent all of them to compromise its target
  - *examples*: multiple user authentication methods, firewalls, etc.
- Compartmentalization
  - divide the system into compartments and isolate them from each other → limit the impact of a compromise
  - principle of least privilege: each module should have only the minimum set of privileges needed to serve its purpose



Firewalls

- Firewall: software of device that filters network traffic based on a set of predefined rules
- Types: stateless (i.e., packet filtering) or stateful (i.e., session filtering)
- Application-layer firewalls: "understand" certain application-level protocols (e.g., FTP, DNS, HTTP)
- DMZ (Demilitarized Zone): separate publicly accessible servers from the internal network

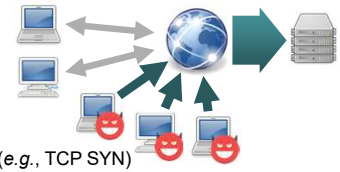


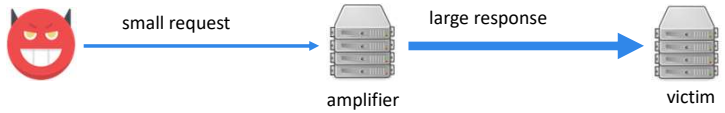
Sandboxing

- Sandbox: security mechanism for separating a running program (or one part of a running program) from the remainder of the system
  - typically for running untested or untrusted code (possibly from untrusted sources)
- Techniques
  - `chroot` jail
  - Linux seccomp (Secure Computing) mode
  - isolation based on Unix access control (*e.g.*, Android security)
  - virtual machines
  - …

Denial-of-Service Attacks

- DoS: attack against availability
  - DDoS: distributed DoS
- Common attack techniques
  - IP address spoofing
  - botnets and massive flooding attacks (*e.g.*, TCP SYN)
  - amplifiers (*e.g.*, DNS, NTP, memcached)





- Countermeasures
  - application front-end hardware, upstream filtering, (D)DoS-resistant hosting
  - ingress filtering against IP address spoofing

Thank you for your attention!

Log into AccessUH

Select Course Evaluation

Tell me …

- How do you like the slides, figures, animations, …
- The difficulty of the test: easy, challenging, ...
- Assignments: more? …