Information Security in the Digital Era

Course URL:
http://pinformatics.org/phpm631

Agenda

- Concepts
- HIPAA
- https://www.youtube.com/watch?v=JKbn0xEePaw

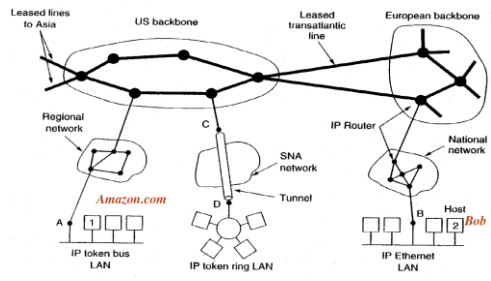
Medical Data Black Market

- The data for sale includes names, birth dates, policy numbers, diagnosis codes and billing information.
- Fraudsters use this data to create fake IDs to buy medical equipment or drugs that can be resold, or they combine a patient number with a false provider number and file made-up claims with insurers, according to experts who have investigated cyber attacks on healthcare organizations.
- Medical identity theft is often not immediately identified by a patient or their provider, giving criminals years to milk such credentials. That makes medical data more valuable than credit cards, which tend to be quickly canceled by banks once fraud is detected.
- Stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber crime protection company. He obtained the data by monitoring underground exchanges where hackers sell the information.
- Prices have come down recently.

What is Computer Security ?

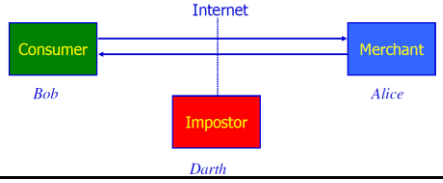
- Securing communications
  - Three steps:
    - Secrecy = prevent understanding of intercepted communication
    - Authentication = establish identity of sender
    - Integrity = establish that communication has not been tampered with
- Securing access to resources
  - Two steps:
    - Authenticate = establish identity of the requestor
    - Authorize = grant or deny access

A bird's eye view of the Internet



Communication security issues

- Encryption -How do I ensure the secrecy of my transactions?
- Authentication -How do I verify the true identity of my counterparts?
- Integrity -How can I be sure the message hasn't been altered?



Encryption

- Secret key cryptography: Based on a secret key
  - Same secret key used for encryption and decryption
  - Problem: How to transmit key securely on the Internet???
- Public key cryptography: Two keys used
  - Public key known to everybody. Used for encryption.
  - Private key known only to owner. Used for decryption.
  - Reliable public key distributed
    - This is the most difficult problem!

Encryption is not enough: Spoofs

- Pretending to be someone else
- Hard to login without someone's password
- But can send out communications with someone else's name on it
  - Email
    - 1993: Dartmouth sent a message saying midterm exam was cancelled
    - Message appeared to come from the Professor!

Needed: Message Authentication

- Make sure Bob gets the message unaltered
- Don't let Alice deny sending the message
  - Guarantee No Plausible Deniability
- Don't care about eavesdropper Darth, unless Darth changes the message
- How can cryptography help?

Digital Signatures

- Key property: Public and private keys can be applied in either order
- Alice has message M
  - She applies her private key to it
  - She sends encrypted message to Bob
- Bob decrypts it with Alice's public key
  - gets back original message
  - infers that Alice is indeed the sender (since only Alice has the private key that corresponds to her public key)
- In that way, encrypting a message with one's private key acts as a digital signature!

Public Key Management

- Public key cryptography works as long as
  - Private key is really kept secret
  - Hard to compute private key from public key
  - Get the correct public key from some trusted source
- Bob can send public key over insecure communication channel
- But how do you know Darth didn't send you his key instead?

Public Key Infrastructure (PKI)

- Certificate Authorities (CA) are Trusted Third Parties charged with the responsibility to generate trusted certificates for requesting individuals organizations
  - Certificates contain the requestors public key and are digitally signed by the CA
  - Before a certificate is issued, CA must verify the identity of the requestor
- These certificates can then facilitate automatic authentication of two parties without the need for out-of-band communication

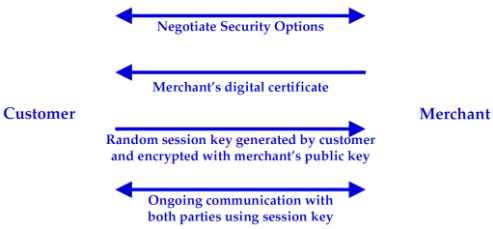
PKI Industry

- Main players: trusted third party CAs
  - Verisign
  - Entrust
  - Cybertrust
  - RSA
- Revenue from
  - products (PKI servers for intranets and extranets)
  - services (certificate services for individuals and organizations)

SSL/TLS

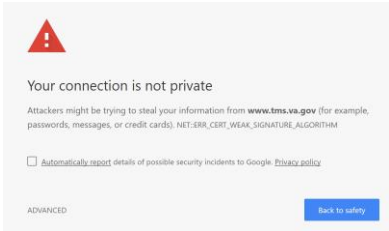
- Secure Sockets Layer / Transport Layer Security
- Provides reasonable level of security
- Often used for transactions between consumers and merchants

SSL/TLS

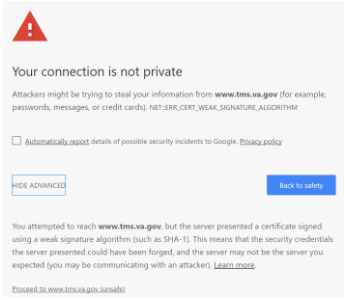


- https://hpbn.co/transport-layer-security-tls/

Firefox



Firefox



Application: Virtual Private Networks (VPNs)

- Secure, private networks that operate over a public network (like the Internet).
  - Messages are confidential
  - Only authorized users can access network
- "Tunneling"--encrypted messages from one protocol are packaged inside another protocol.

Access Control

- Something you have
  - Smart Cards:
    - Store user's digital certificate and/or private key
- Something you know
  - Login Procedures
  - Password leaks
  - Passwords are inconvenient
  - Two-factor authentication
- Something you are
  - Biometrics: fingerprint, face & voice recognition

Sneaking through the backdoor

- Strategies whose goal is to gain control by bypassing access control defenses
- Exploit "holes" in applications that connect our machine to the network
  - Viruses and worms: programs that run on machines where they're not wanted
  - Spyware, adware, malware: programs that are (usually) added to your computer without your knowledge and that do things you don't want
  - Buffer overflow attacks
  - Denial of Service attacks: flood the server with fake message so that no legitimate message can get through

Defensive Measures

- Virus scanners and removers
- Malware scanners and removers
- Firewalls
  - Put up around a network for more security
  - Hide structure of network
  - Only allow traffic from "legitimate users"
  - Screens data packets for checks
- Intrusion Detection Systems
  - Data mining techniques to detect and report suspicious activities
  - Main strategies
    - Pattern recognition
    - Anomaly detection
- Other Preventive Measures
  - Stay Current on patches
    - Zero day attack: Never seen before

Despite all that … security breaches are on the rise

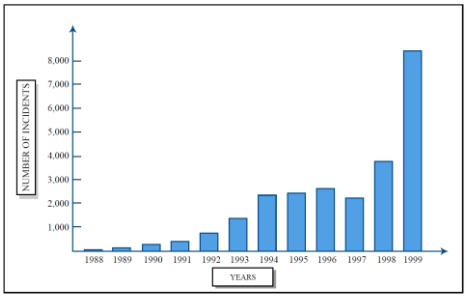


Figure by MIT OCW.

… and requires far less technical expertise

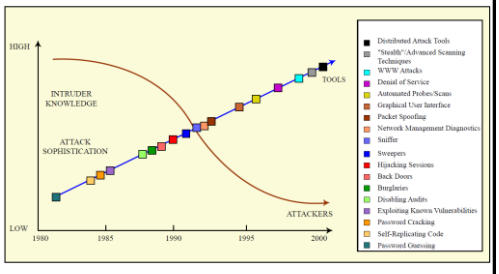


Figure by MIT OCW.

Agenda

- Concepts
- HIPAA

HIPAA Security
Hye-Chung Kum's Opinion

- NOT security expert
- Security vs Compliance
- Main threat
  - Identity theft
  - Medical fraud ?
- Due Diligence
  - Risk Analysis and Management
    - Security Risk Assessment : Tools
  - Physical Safeguards
  - Technical Safeguards
  - Training
  - Reasonable documentation
- When breach occurs
  - Reporting requirements
  - Penalties and noncompliance
  - Extenuating circumstances

HIPAA Security
Hye-Chung Kum's Opinion Summary

- The art of balancing
  - Security is costly BUT very important
  - Security costs can take away from services
  - Each health system MUST have someone who knows enough about security to do the balancing act
    - Management have to know enough to recognize them, keep them, and listen to their advice
  - Dynamic: Stay just above the curve
    - At least now – lots of systems have lots of holes
    - So relatively easy to stay ahead of the curve

Take Away I
What is Computer Security ?

- Securing communications
  - Three steps:
    - Secrecy = prevent understanding of intercepted communication
    - Authentication = establish identity of sender
    - Integrity = establish that communication has not been tampered with
- Securing access to resources
  - Two steps:
    - Authenticate = establish identity of the requestor
    - Authorize = grant or deny access

Take Away II
Encryption

- Secret key cryptography: Based on a secret key
  - Same secret key used for encryption and decryption
  - Problem: How to transmit key securely on the Internet???
- Public key cryptography: Two keys used
  - Public key known to everybody. Used for encryption.
  - Private key known only to owner. Used for decryption.
  - Reliable public key distributed
    - This is the most difficult problem!
    - Public Key Infrastructure (PKI): certification services (trusted site)

Take Away III
Defensive Measures

- Virus scanners and removers
- Malware scanners and removers
- Firewalls
  - Put up around a network for more security
  - Hide structure of network
  - Only allow traffic from "legitimate users"
  - Screens data packets for checks
- Intrusion Detection Systems
  - Data mining techniques to detect and report suspicious activities
  - Main strategies
    - Pattern recognition
    - Anomaly detection
- Other Preventive Measures
  - Stay Current on patches
    - Zero day attack: Never seen before