Unauthorized Access

Fall 2015

Panos Papadimitatos
Networked Systems Security Group
www.kth.se/nss

Outline

- Introduction
- Firewalls
- Intrusion Detection Systems
- Authentication
  - Passwords
  - Kerberos
  - One time passwords
  - Biometrics
- Virtual Private Networks
- Previous Attacks

Unauthorized access

Broad definition

- When a person accesses resources, network infrastructure or computers and databases without legal permission
- American laws on unauthorized access: (link)

Unauthorized access (cont'd)

- *"Den som i annat fall än som sägs i 8 och 9 §§ olovligen bereder sig tillgång till en uppgift som är avsedd för automatiserad behandling eller olovligen ändrar, utplånar, blockerar eller i register för in en sådan uppgift döms för dataintrång till böter eller fängelse i högst två år. Detsamma gäller den som olovligen genom någon annan liknande åtgärd allvarligt stör eller hindrar användningen av en sådan uppgift."*
  - ***English summary:*** *Whoever unlawfully obtains access to a piece of information or unlawfully alter, destroy, obstruct registry in such a task is convicted of hacking (2 years max).*

Intruders

- Try gaining unauthorized access
- Outsiders or insiders
- Different attack motives and effects
- Examples
  - Guess-crack passwords
  - Access databases containing credit card data
  - View sensitive data like health records, payroll records
  - Compromise email accounts

Intruders (cont'd)

- **Misfeasor**
  - Otherwise legitimate user; accesses more than she/he is authorized to; misuses privileges
- **Masquerader**
  - Not authorized to use; penetrates; steals passwords
- **Clandestine user**
  - Seizes supervisory control; may evade auditing and access control mechanisms

[Stallings]

Intruder Patterns: The hacker

- Hacks for the thrill – because its fun!
  - Online hacking communities share 'results'
- Exploits weaknesses
- Maps a network for known security breaches
  - Port scanning
- Wide variety of open source tools (usually brute force tools)

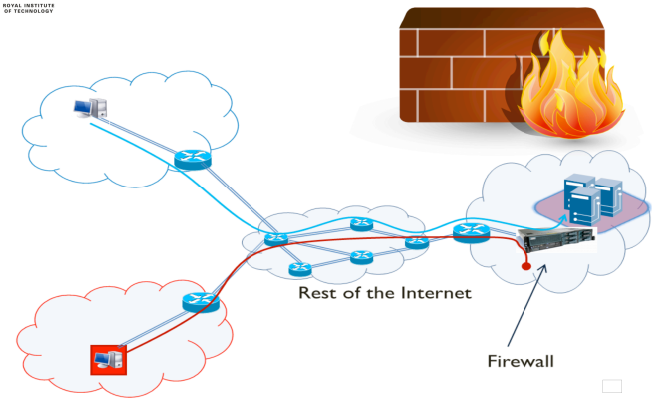

Intruder Patterns: The Insider

- Can be one of the system administrators
- Difficult to detect and prevent
- Common actions
  - Performing (large) copying and transferring of files
  - Accessing network off office hours

Intruder Patterns: The Criminal Enterprise

- Precise and organized attacks, sophisticated approaches
- Victims: Big corporations, country facilities & institutions
- Increasingly common nowadays
- Could be hired by governments or corporations
  - Marketing, industrial espionage
- Examples
  - Banking systems
  - Government facilities and institutions

Firewalls



Firewalls (cont'd)

- Hardware and/or software controlling network traffic flow
- Implemented in any networked environment
  - Internet
  - Private/corporate networks
- Several different firewall technologies

Packet Filters

- Core functionality for modern firewalls
- No state of data flow
- Operation at the network layer
- Not concerned with packet content (payload/data)
- They check the packet header(s)
  - Source and Destination IP addresses
  - Transport layer protocol used (e.g., UDP/TCP)
  - Transport layer attributes, e.g., source and destination ports

Packet Filters (cont'd)

- Weaknesses
  - Restricting access primarily based IP address
  - Cannot detect spoofed IP addresses (within the 'inner' network)
  - Cannot detect source routing problems
    - E.g., to redirect traffic
    - (Reminder for source routing: [link])
- No validation of data coming through

Stateful Inspection Firewalls

- Improvement over packet filters
- Packet filter **AND** tracking of the connection state
  - Examine sequences of packets
  - State tables for each connection
  - Block packets deviating from expected behavior
  - Check non-standard ports
  - Include Network Address Translation (NAT) information
  - Clean up old connections

Stateful Inspection Firewalls (cont'd)

- Check packet sequence numbers and block packets out of sequence

Table 2-1. State Table Example

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	192.0.2.71	80	Initiated
192.168.1.102	1031	10.12.18.74	80	Established
192.168.1.101	1033	10.66.32.122	25	Established
192.168.1.106	1035	10.231.32.12	79	Established

- As UDP is connectionless, only Source IP, Destination IP and ports can be checked
- Can catch more intrusion attempts

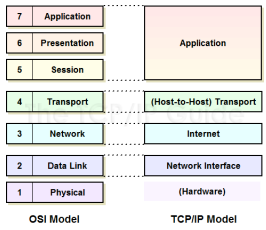
Image from NIST report "Guidelines on Firewalls and Firewall Policy"

Unauthorized Access

Panos Papadimitatos
Networked Systems Security Group
www.kth.se/nss

Application Firewalls

- Allow or deny access based on application behavior
- Add basic intrusion detection technology
- Create legitimate user profiles to discover deviations
  - E.g., emails containing an executable file (not permitted by the company's policy)
  - Using instant messenger through a port different than the expected one



Application-Proxy Gateways

- Transparent intermediary between two networks
- Mandatory to go through the gateway
- Host-to-host connection
  - Host to proxy connection (public IP)
  - Proxy to destination host (internal IP addresses)
- Per-application agents can inspect in detail packet content **and**
  - Implement classical firewalls rule sets
  - Authenticate individual users (require passwords, certificates etc
  - Be suitable for VPN implementations

Intrusion Detection Systems

Application-Proxy Gateways (cont'd)

- Higher level of security than application firewalls
- No two hosts in different networks communicate directly
- Encrypt/decrypt packets
- Authenticates users
- Inspect packets at application layer (check if behavior deviates from the expected actions)

Intrusion Detection Systems

- Software application to detect intrusion evidence
- Monitoring procedure and intrusion alarms
  - Real world analogy: smoke detector
- Possible issues
  - False negatives
  - False positives
- Two technologies
  - Anomaly detection
  - Signature detection

Anomaly Detection

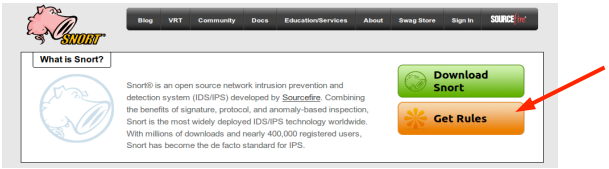
- **Abnormality is suspicious**
- Models of normal user behavior
  - Normal is correct
- Programmed
  - With normal behavior
  - Statistical models and experience
- Self-learning
  - Dynamic learning normal user behavior
  - Stochastic nature models
  - Detection of new attacks

Anomaly Detection (cont'd)

- **Abnormality is suspicious**
- Hard to have good all-encompassing normal behavior models
- Deviations can signal attacks while this is not the case
  - *False positive*
- The opposite is possible
  - Attackers pass as normal, i.e., *false negative*

Signature Detection

- The intruder behavior is specified
  - Definition of **what is** wrong behavior
  - Recall: Anomaly detection defines **what is not** intruder behavior
- Fewer false positives
- Example of open source IDS: http://www.snort.org/



Signature Detection (cont'd)

- Examples of suspicious behavior:
  - Unsuccessful login attempts within a short period of time (seconds)
  - Uncommon database queries
  - Attempts to log in with common root user names (admin, administrator, root etc)
- Hard to catch new, unknown attacks
  - Hard to create models for intruders
  - Hard to guess intruder profiles

Honeypots

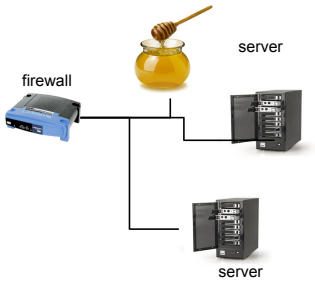
- Deception and trapping
- Distract adversaries
  - Early warnings of attacks
- Advertise vulnerabilities
  - Don't solve problems
- Discover adversarial trends and techniques

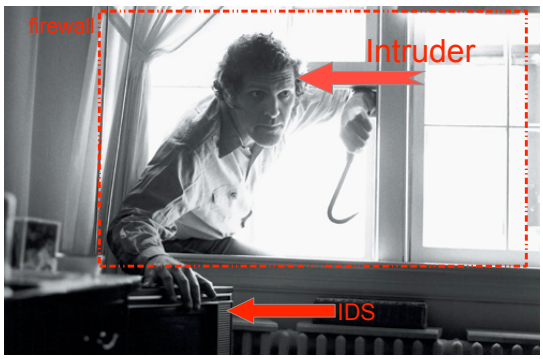
Honeypots (cont'd)

- Two basic types
  - Production honeypots
    - Trap the intruder
  - Research honeypots
    - Study intruder behavior
      - Collect large amounts of data
    - Hard to maintain

Honeypots (cont'd)

- As generic as possible
  - Unmodified systems
- Launch point of attacks
- Easy but not **too** easy
- The more time spent to hack honey pot, the more info gathered



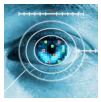


Authentication

- **Authentication**
  - Passwords
  - One time passwords
  - Digital signatures-certificates
- **On top of authentication**
  - Intrusion Detection Techniques
  - Firewalls
  - Software patches
  - Policies

Authentication (cont'd)

- **Authentication methods categorization**
  - Something that you have
  - Something that you know
  - Something that you are



Check-point

- Firewalls can protect networked resources (first line of defense)
- IDS can detect additional, possibly more elaborate attacks that are not (proactively) prevented by the firewalls
- They can both operate without identifying the intruder
- Raising the bar: mandating **authentication** to a gateway
  - Such attackers are essentially insiders
  - All defenses (firewalls, IDS) apply on their traffic
- Consider deployment as per system needs, e.g.,
  - One or more firewalls
  - One or more IDS
  - IDS and firewall on the same or different machines
  - Gateway or not
  - Gateways at the source and/or destination network

Passwords

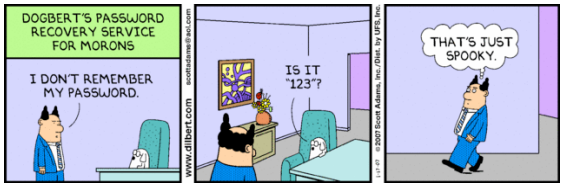
"System security is often as good as the weakest password"

Passwords

- Secret codes for authentication
- Simplest form of authentication
- Vulnerable against password attacks
  - Brute force attacks
    - Explore every possible combination in the worst case
  - Dictionary attacks
    - Tryout passwords from file, the dictionary

Passwords (cont'd)

- Secure password management and storage are crucial
- Hard to guess passwords
- Multiple ready-to-use cracking tools
  - Use brute force techniques
  - Target authentication protocols; unix, windows passwords

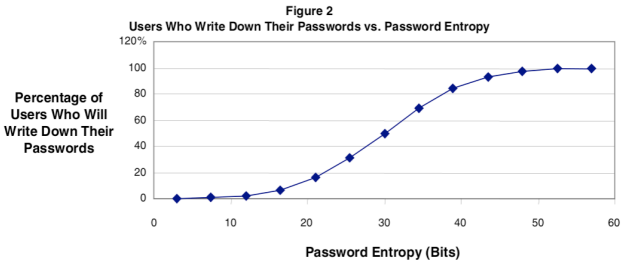


Password strength

- Password strength can be expressed in terms of entropy
- Entropy H is a measure of unpredictability
  - $H = L\log_2(N)$, where L is the password length and N is the size of the alphabet used
  - It takes approximately 2^H attempts to find the password

Character Pool	Available Characters (n)	Entropy Per Character
digits	10 (0-9)	3.32 bits
lower-case letters	26 (a-z)	4.7 bits
case sensitive letters and digits	62 (A-Z, a-z,0-9)	5.95 bits
all standard keyboard characters	94	6.55 bits

Password strength (cont'd)

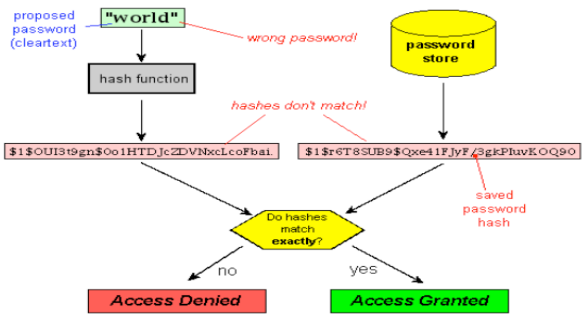


Source: Gartner Research (December 2004)

Password storage

- Hashes of passwords: store a value representing the user password
  - Intruders cannot obtain the original password
  - Extremely useful against Insiders
- Compare hashes instead of actual passwords
- Access control: restricting access to the password file
  - Policies (who, when, what, how)
  - Administrators

Password storage (cont'd)



Reasons to hate security engineers

- Change passwords
  - Fear for weakening of passwords
  - Protect against intruders (offline attacks)
- Strong passwords (entropy)
  - Hard to remember
- Don't write down your passwords

A famous password

- Bill Clinton used the password "Buddy" to protect the private key used to create digital signatures for his electronic mail

source: www.cryptosmith.com

One-time passwords

How do one-time passwords work?

- Valid for one session only or one transaction only
- Raise the bar for intruders
  - More difficult to capture passwords (limited validity time)
  - Created using a combination of trusted machine, given code and secret PIN
- Swedish online banking systems are an example

Difficult to attack

- Access to the card 
- Crypto devices block card after 3 failed attempts 
- Personal number (publicly available)
- Guess the four digit PIN 

An Actual Attack

- It is clear that brute-forcing a bank website is not a good idea
- Access to password generation algorithms is almost impossible
  - But not infeasible (check RSA breach)
- Alternative?
  - Phishing!

An Actual Attack (cont'd)

- Users victims of phishing attack
- Email sent to customers, supposedly from Nordea
- Download an anti-spam tool
- Trojan included
- Error message when accessing Nordea's website
- Redirection to phishing site
- Users revealed passwords to intruders (link)

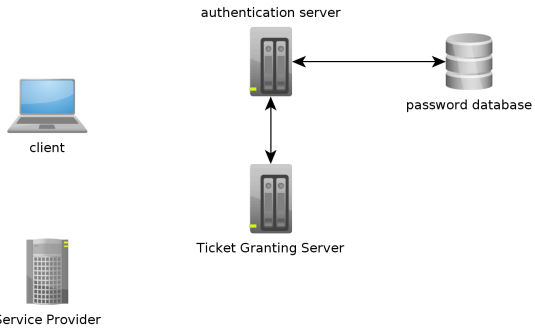
Kerberos

Authenticating users in local area networks without PKIs

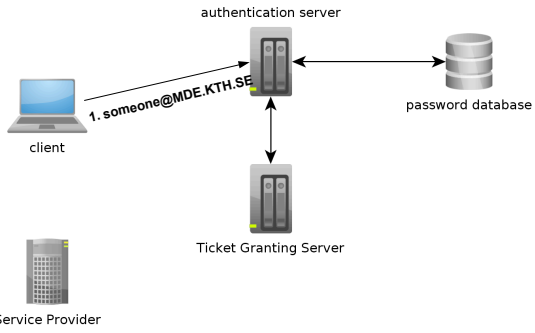
Kerberos (cont'd)

- Network authentication protocol for client/server applications
- Developed at MIT in the mid 1980s
- Untrusted network using trusted hosts
- Access to services
  - Email servers and file systems
- Kerberos 5 is the main version in use
- Why use Kerberos?
  - PKI complexity and cost

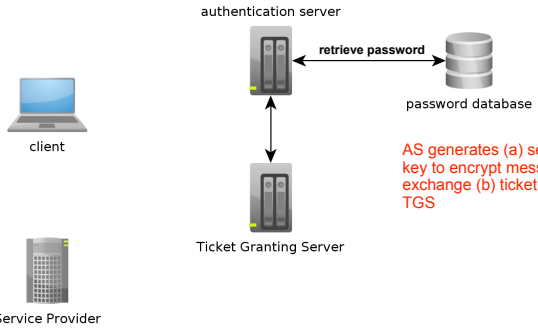
Kerberos (cont'd)



Kerberos (cont'd)

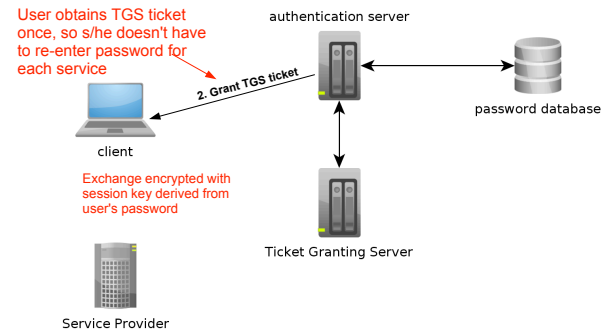


Kerberos (cont'd)

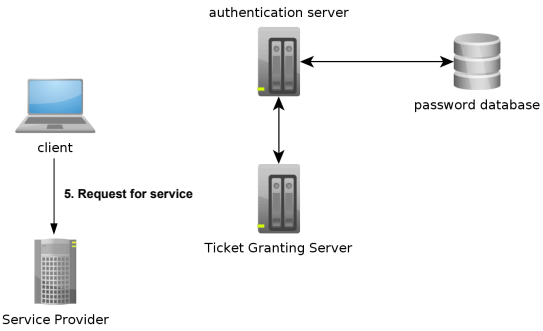


AS generates (a) session key to encrypt message exchange (b) ticket for TGS

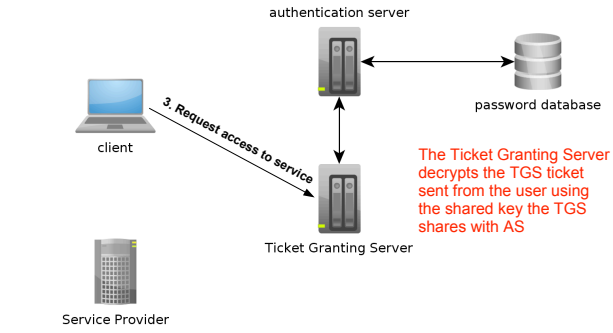
Kerberos (cont'd)



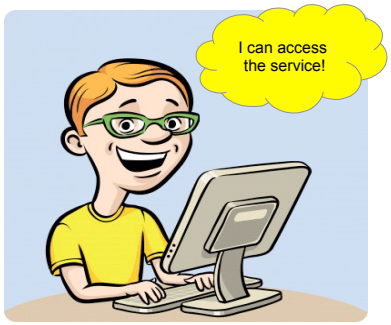
Kerberos (cont'd)



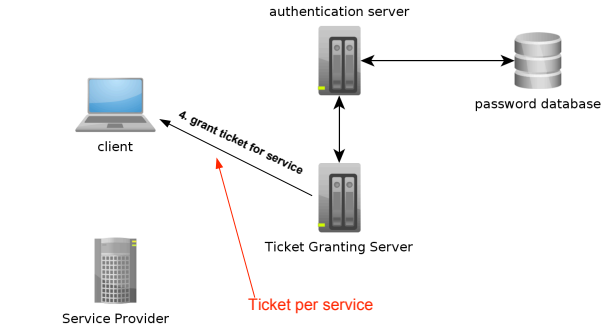
Kerberos (cont'd)



Kerberos (cont'd)



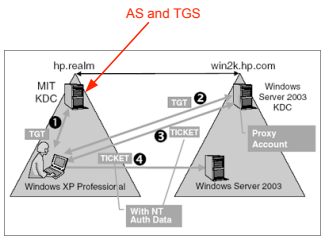
Kerberos (cont'd)



Kerberos (cont'd)

Multi-realm Kerberos

- Supports inter-realm Kerberos communication
- Requires trust between Kerberos servers
- Users authenticated in their realm
- Access services in neighboring realms



Kerberos (cont'd)

Summary

- Untrusted network but trusted hosts
  - How can hosts be reliable? Software running on hosts?
  - If hosts are compromised then Kerberos is compromised
- Kerberos 5 brings a lot of improvements over Kerberos 4
  - Stronger cryptography
- Password based security is a weakness point
- Suitable for local area or neighboring networks (Multiple Realm Kerberos)
- Alternative to certificates and PKIs

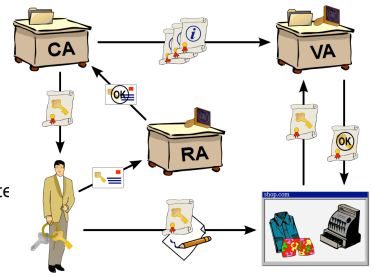
Public Key Infrastructure(s)

Why PKIs?

- To authenticate hosts across open networks
  - Beyond local area networks
- Passwords
  - Inconvenient
  - Insecure (stolen, storage, phishing)
- Use public key Cryptography for authentication
- Need to distribute public keys securely
  - Who is who?

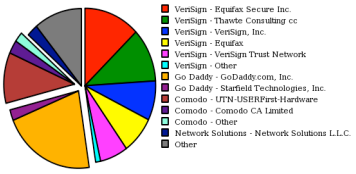
PKI overview

- Main elements
  - Hardware & Software
  - People & Policies
  - Procedures
- How are they used
  - Manage, Store, Distribute & Revoke keys
- Where are they used
  - E-commerce
  - E-banking



Certificates

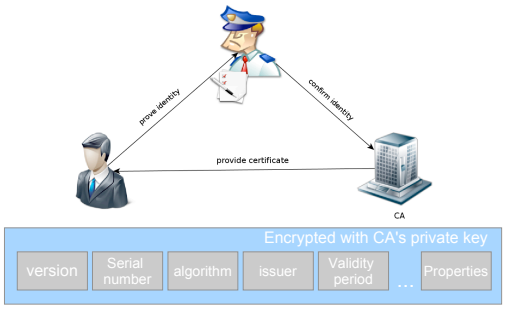
- Digital signatures of someone trusted
  - Trust in the signature (private-public key crypto)
  - Company, institution..
  - Hierarchical structure
  - Root certificates
- Bind public key with identity
- X.509 Standard for PKI certificates (PKIX)



Market share of certification authorities

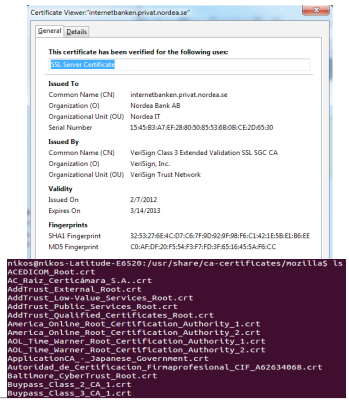
Source: netcraft.com

PKIX overview



SSL certificates

- Widely used in internet communications
- SSL/TLS for secure client/server applications
- Browsers have root certificates pre-stored
- Way to authenticate vendors, banks etc
- X.509 format



Smart card authentication

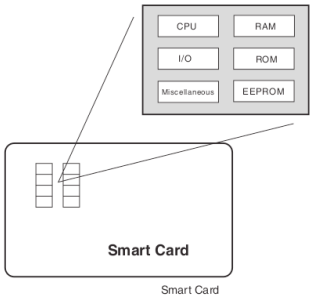
Some problems with PKIs

- Who do we trust & for what?
  - Who renders the CA trusted?
- Private Key protection
  - Who has access to our storage?
- Which "Erik Johansson" is he?
- Root certificate list exposure

Nice overview of PKI risks by Bruce Schneier: http://www.schneier.com/paper-pki.html

Smart cards

- "Intelligent" cards
- Minimized computer system
  - Ram/Rom
  - CPU
  - Slimmed down' OS in the ROM
  - EEPROM (storage of keys)
- Activated using
  - Biometrics
  - Password



Smart Card

Source: Smart Cards: The Authentication Solution For the E- Business User, Norbert Pohlmann

The Comodo breach

- Questioned PKI security
- RA intrusion attack
  - Stolen administrative password
- Request for domain certificates
  - login.yahoo.com
  - mail.google.com
- Certificates discovered and revoked

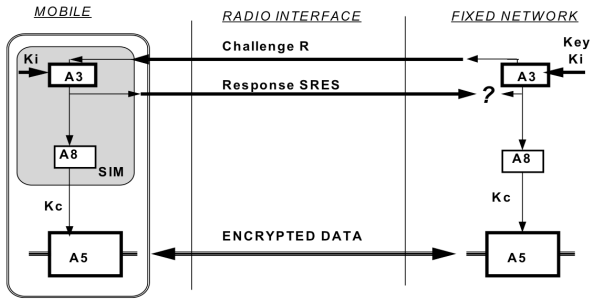
COMODO
Creating Trust Online™

http://www.crn.com/news/security/229400197/bogus-comodo-ssl-certs-targeted-google-yahoo-in-attack-linked-to-iran.htm?itc=refresh

Advantages of smart cards

- Store multiple keys
- Single sign-on
- Secure storage of keys
- Cryptographic applications
- Passwords not lost

GSM authentication



Biometrics

Biometrics	Single-node cost (includes hardware)	Strengths	Weaknesses	Opportunities	Threats
Face recognition	Low	Easy; fast; one of the least expensive methods	Subject to spoofing attempts; awkward lighting in the image can affect authentication	General	Reliability (changes in lighting and photo angles affect the reliability of data)
Fingerprint	Low	Inexpensive, very secure, uniqueness, ease of capture	Latent prints, cuts and dirt can mar image	Law enforcement corporate databases; long standing reputation	Validity of matching accuracy (masking the finger to avoid the match; ability to force a false match)
Palm scanning/hand geometry	Moderate	Tiny storage requirement; intuitive operation	Slow, less accurate than finger scanning	Manufacturing/shop floors	Confidentiality (hijacking of contour data that are simple could affect privacy)
Iris/retina scanning	High	Extremely difficult to fool	Intrusive and inconvenient	Nuclear facilities, medical services, correctional institutions	Ability to presenting a photo of the target's iris. (lack of liveliness testing), printing iris pattern on contact lenses
Thermal image	Extremely high	Extremely difficult to fool	Requires expensive infrared cameras	Sites requiring ultra high security	User acceptance (involves infrared imaging that could be seen intrusive)
Voice print	Low	Inexpensive; good for remote access	Slow; can be affected by physical condition or emotional state	Remote banking, remote database access	Reliability (vulnerable to replay attacks)
Signature recognition	Low	Inexpensive	Can be affected by physical condition or emotional state	Industrial	Data accuracy and reliability (variable trait data; vulnerable to replay attacks)

Table I. A SWOT analysis of the biometric techniques used commercially

http://www.emeraldinsight.com/journals.htm?articleid=1747892&show=html

Biometrics Authentication

Biometrics

Biometrics	Single-node cost (includes hardware)	Strengths	Weaknesses	Opportunities	Threats
Face recognition	Low	Easy; fast; one of the least expensive methods	Subject to spoofing attempts; awkward lighting in the image can affect authentication	General	Reliability (changes in lighting and photo angles affect the reliability of data)
Fingerprint	Low	Inexpensive, very secure, uniqueness, ease of capture	Latent prints, cuts and dirt can mar image	Law enforcement corporate databases; long standing reputation	Validity of matching accuracy (masking the finger to avoid the match; ability to force a false match)
Palm scanning/hand geometry	Moderate	Tiny storage requirement; intuitive operation	Slow, less accurate than finger scanning	Manufacturing/shop floors	Confidentiality (hijacking of contour data that are simple could affect privacy)
Iris/retina scanning	High	Extremely difficult to fool	Intrusive and inconvenient	Nuclear facilities, medical services, correctional institutions	Ability to presenting a photo of the target's iris. (lack of liveliness testing), printing iris pattern on contact lenses
Thermal image	Extremely high	Extremely difficult to fool	Requires expensive infrared cameras	Sites requiring ultra high security	User acceptance (involves infrared imaging that could be seen intrusive)
Voice print	Low	Inexpensive; good for remote access	Slow; can be affected by physical condition or emotional state	Remote banking, remote database access	Reliability (vulnerable to replay attacks)
Signature recognition	Low	Inexpensive	Can be affected by physical condition or emotional state	Industrial	Data accuracy and reliability (variable trait data; vulnerable to replay attacks)

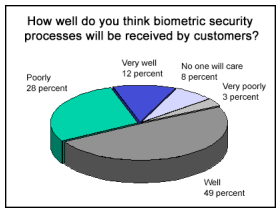
Table I. A SWOT analysis of the biometric techniques used commercially

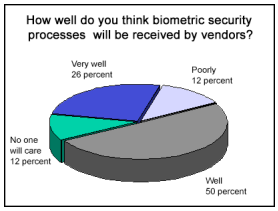
http://www.emeraldinsight.com/journals.htm?articleid=1747892&show=html

Biometrics

- Something that the user *is*
- Analysis of biological observations
- Intention of authentication without active user enrollment
  - Passwords
- Check whether identity matches template in database
- Architecture
  - Data capture
  - Signal processing
  - Matching
  - Data storage
  - Decision

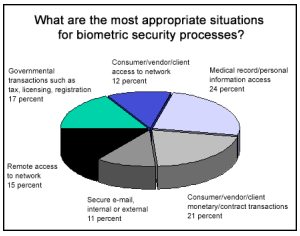
Is biometric authentication the future?

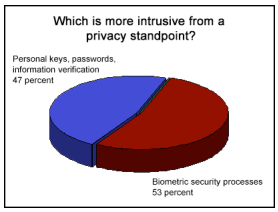




Source: http://www.techrepublic.com/article/survey-results-bring-on-the-biometrics/5032095

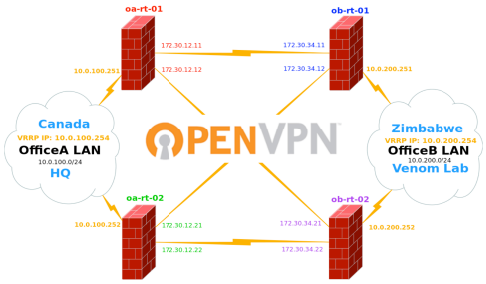
Is biometric authentication the future?





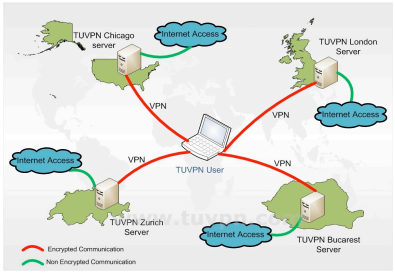
Source: http://www.techrepublic.com/article/survey-results-bring-on-the-biometrics/5032095

Virtual Private Networks



Virtual Private Networks (cont'd)

- **Broad definition:** a network that provides a secure link between two or more private networks



http://blog.tuvpn.com/wp-content/uploads/servicio_vpn_english(1).jpg

Virtual Private Networks (cont'd)

- **Virtual:** data are channeled through a public network (Internet) emulating a point-to-point connection
- **Private:** secure *tunneling* of data provides confidentiality, integrity, authentication and access control
- **Why:** To connect businesses, employees working from different locations but using the same resources
- **Main advantage:** They are inexpensive and efficient to implement compared to other options

Types of VPNs

- Access VPNs
  - Access to mobile and remote users
- Intranet VPNs
  - Link office branches to central headquarters
- Extranet VPNs
  - Combination of the two above
- Each type of VPN has slightly different security requirements

Security Requirements for VPNs

- **Confidentiality:** Encryption of data
- **Integrity:** (Keyed) hash functions
- **Authentication:** Digital Signatures
- **Binding of identities to keys:** Digital Certificates
- **Access Control:** Firewalls and filtering mechanisms

Against Intruders

- **Authentication & Certification**
  - Only authenticated-legitimate users have access to the VPN
  - Secure tunneling
- **Access Control**
  - Firewalls
  - Intrusion Detection Systems (IDS)
  - Sensitive data-resources protected

IPSec features

- Operation at the network layer, to encrypt/authenticate IP packets
  - AH for authentication
  - ESP for encryption and optional authentication
- Security Association
  - Shared security attributes
  - AH or ESP
  - Destination address
- Internet Key Exchange (IKE) to set up SAs

Secure Tunneling

- Encapsulation of datagram when entering the "tunnel"
- De-capsulation when reaching the other end-point

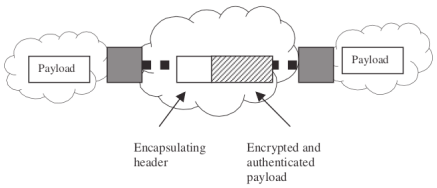
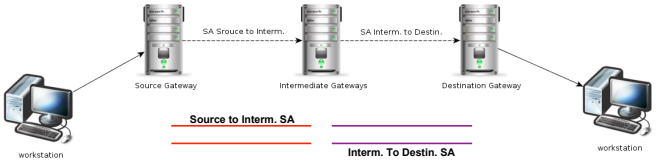
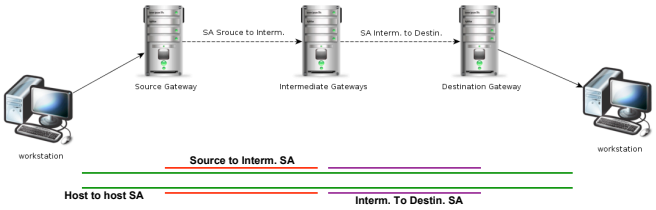


Image taken from book "Network security: current status and future directions", Christos Douligeris, Dimitrios N. Serpanos

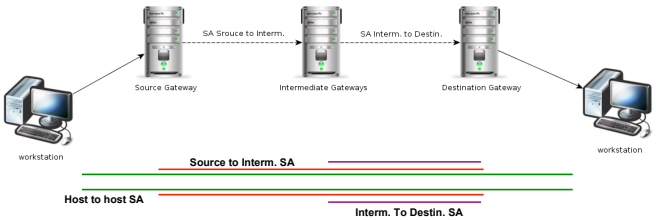
Single Tunneling in VPNs



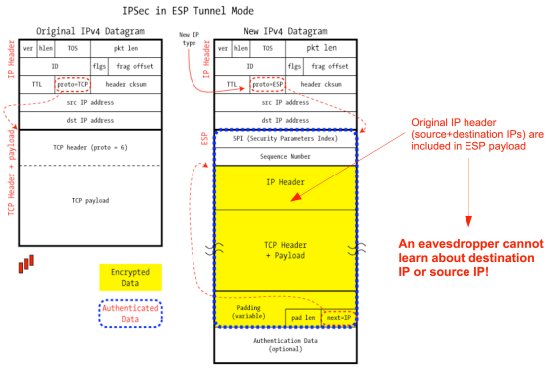
Multi-layered tunneling



Multi-layered tunneling



ESP Tunnel Mode



VPN firewall example

- Cisco RV120W Wireless-N VPN Firewall features:
- **Stateful packet inspection (SPI)** firewall

  (and wireless security)
- **IP Security (IPsec) VPN support**

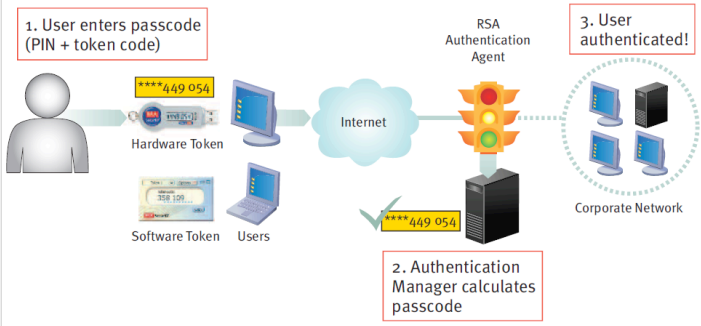
  (with hardware acceleration)

Examples of reported attacks

The RSA Breach (2011)

- Two factor authentication:something you know + something you have (link)
- User enters id & pass code= PIN + token code
- Token code produced according to secret key (seed) of token and internal clock
- Intruders breached into RSA's networks and stole information related to its SecurID two-factor authentication

How Does RSA SecurID Work?



The RSA Breach (2011)

- Typical example of criminal enterprise
- Advanced Persistent Threats
- RSA's open letter to its customers
  - "Recently, our security systems identified an extremely sophisticated cyber-attack in progress being mounted against RSA."
- *"No additional details about what the RSA attackers did steal...both the seeds that link every token to a specific account and the algorithm that calculates the numeric sequence generated by the token have been compromised"* (link)

APT attacks

- First phase: Social engineering attack
  - Find, study weakest links
  - Phishing emails (2011 Recruitment plan.xsl)
  - A **single** employee retrieved the email from **junk folder**
- Second phase: Inside the network
  - Seek for admin rights
- Third phase: extract what you can
  - Take the money and run!

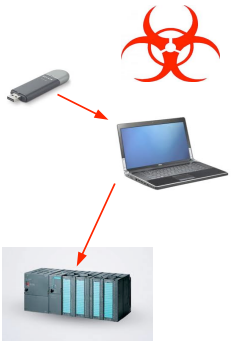
APT attacks (cont'd)

- Information stolen was used against Lockheed Martin (the exact attack parameters remain unknown)
- Lockheed Martin is one of the world's largest military constructors
- Attackers exploited Lockheed Martin's VPN network
- Lockheed-Martin detected the attack and acted quickly to thwart it
- Report about the attack (link)

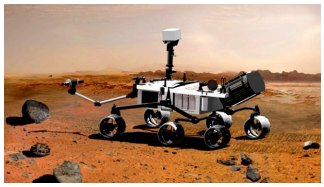
LOCKHEED MARTIN

Stuxnet

- Infiltrating-controlling Iranian nuclear plants
- Suspected (not proven) western super powers (USA & Israel)
- video from Synmatec
- Importance: physically overtaking-controlling infrastructure
- Duqu: next generation stuxnet
  - Gather intelligence for future cyber-attacks



NASA hacking attack (Nov 2011)



- Seized control of networks at NASA's Jet Propulsion Laboratory
- Installed malware, delete or steal sensitive data
- Hijacked the accounts of users in order to gain their privileged access
- Chinese-based IP addresses
- The attackers had full functional control over the networks