Introduction

Network Security
mod-net-sec
University of Birmingham
Network Security

Introduction

• Networked computing in the presence of an adversary

• Adversary
  – an entity that *attacks*, or is a threat to, a networked system

• Attack
  – An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. [source: RFC 2828]
More definitions

• Security Services
  – Prevent **bad** things from happening
  – Mechanism

• Security Policies
  – Define what is **bad**
  – Define what is **good**
<table>
<thead>
<tr>
<th>Area</th>
<th>Usual perspective</th>
<th>Security perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reliability</td>
<td>Random failures</td>
<td>Deliberate failures</td>
</tr>
<tr>
<td>Usability</td>
<td>User confusion</td>
<td>User deception</td>
</tr>
<tr>
<td>Programming languages (memory safety)</td>
<td>Crashes</td>
<td>Entrance vector</td>
</tr>
<tr>
<td>Software engineering (bugs)</td>
<td>Software quality</td>
<td>Attack vectors</td>
</tr>
</tbody>
</table>
Holistic perspective

• Security is only as good as the **weakest link**
• Therefore, we must understand all the parts of the system
  – OS
  – Networking
  – Devices
  – Physical security
  – People
• We will mostly cover networking
Exercise

Task: log into online bank account to transfer funds
What are the vulnerabilities?
Channel Security concepts

• Channel security
  – Confidentiality
    • Keeping data and resources hidden
  – Integrity
    • Data integrity (integrity)
    • Origin integrity (authentication)
  – Availability
    • Efficient transfer of information in the communication channel
Network Security concepts

• Network properties
  – Anonymity
    • Untraceability
    • Unlinkability
    • Unobservability

  – Availability
    • Enabling access to data and resources
Additional concepts

• Authenticity
  – Property of being genuine. Can be verified and trusted

• Accountability
  – Actions of an entity can be traced uniquely to that entity
  – Nonrepudiation or “you can’t escape your past”.

Additional concepts

• **Threat** – Set of circumstances that has the potential to cause loss or harm. Or a potential violation of security.

• **Vulnerability** – Weakness in the system that could be exploited to cause loss or harm.

• **Attack** – When an entity exploits a vulnerability on system. Strategic noise; not random error.

• **Control or Countermeasure** – A means to prevent a vulnerability from being exploited.
Graph example

- Graph budget: 6 nodes with 2 edges each.
- Possible designs:
  - Consider a star graph topology.
  - Consider a constant-degree graph.
- Functionality: transfer information from one node to another within a finite number of steps.
- Attacks: remove one node
- Comment on error tolerance (reliability).
- Comment on attack tolerance (security).
- Can you design for better security?
Concept diagram

Security entails:
- Identifying assets
- Identifying vulnerabilities
- Designing countermeasures
- Assessing risk

[Figure 1.2 from Stallings & Brown]
Exercise

• List the threats, vulnerabilities, attacks, and defenses
Classes of threats:

• Disclosure
  – Snooping

• Deception
  – Modification, spoofing, repudiation of origin, denial of receipt

• Disruption
  – Modification

• Usurpation
  – Modification, spoofing, delay, denial of service
Common threats

• Snooping or interception
  – Unauthorised interception of information on via a network

• Falsification
  – Unauthorised change of information

• Masquerading or spoofing
  – An impersonation of one entity by another

• Repudiation
  – A false denial that an entity received some information
Examples: trust and assumptions

• Locks prevent unauthorised access
  – What assumptions does this statement build on?

• What threats does the Internet pose?
Examples

• Computer security on desktop big problem
  – Unpatched system compromised in 5min - 2 hours
Examples: Software Update

• Stem the flow of worms / viruses
  – Upgrade software to address vulnerabilities
• Many systems unpatched
  – Most organizations take 2+ weeks to patch
  – Unmanaged PCs take years to upgrade
• Automated updates
  – Trustworthiness of update source
  – Non-disruptive patches
Examples:
Zero-day Exploits

• Worms that exploit previously unknown vulnerability
  – Potentially disastrous results
• Identify unknown worms
  – Scanning detection
  – Honeypots
• Automated signature generation
• Recovery
Defining security

• Security Policy
  – A statement of what is allowed in a networked system and what is not allowed
  – Divides the world into secure and non-secure states
  – A secure system starts in a secure state. All transitions keep it in a secure state.

• Security Mechanism
  – A method, tool, or policy for enforcing a security policy.
  – Prevent, detect, respond, or recover.
Policy assumptions

- The security policy correctly divides the world into secure and insecure states.
- Mechanisms prevent transition from secure to insecure states

- Example: Bank officers may move money between accounts. Any flawed assumptions here?
Evidence of how much to trust a system

Forms of evidence
  – System specifications
  – Design
  – Implementation
  – Attack/Penetration tests
  – Field tests or Hackathons
Example of assurance

• Why do you trust a car from a major manufacturer?
  – Testing and certifications
  – Standards
  – Seals

• Analogy to software assurance
Human Factors

• Users specify security policy
  – Difference between a secure and insecure action is user intent

• Users can only make good decisions about something they understand

• Research in security turning to HCI: Humans are the last (and often weakest) link
Keypoints

• You must look at the big picture when securing a system
• Pay attention to key network security concepts
  – Anonymity and privacy
  – Availability
  – Auditing
  – Channel security requirements (C,I,A)
  – Traffic analysis/surveillance
  – Deception (human factors)
  – Redundancy (against targeted errors not random errors)
Keypoints continued...

• Differentiating Threats, Vulnerabilities, Attacks, and Defenses.
• Policy vs Mechanism
• Assurance
Security is all around you

• Subscribe to the Cryptogram newsletter
• Join Slashdot!
Tying it together

Threats → Policy → Specification → Design → Implementation → Operation
FBI Publishes Top Email Terms Used By Corporate Fraudsters

Qedward writes

"Software developed by the FBI and Ernst & Young has revealed the most common words used in email conversations among employees engaged in corporate fraud. The software, which was developed using the knowledge gained from real life corporate fraud investigations, pinpoints and tracks common fraud phrases like 'cover up,' 'write off,' 'failed investment,' 'off the books,' 'nobody will find out' and 'grey area'. Expressions such as 'special fees' and 'friendly payments' are most common in bribery cases, while fears of getting caught are shown in phrases such as 'no inspection' and 'do not volunteer information.'"

Read the 54 comments

Hiding Secret Messages In Skype Silences

Posted by samzenpus on Monday January 07, @02:47PM
from the sound-of-silence dept.

Orome1 writes

"A group of researchers from the Institute of Telecommunications of the Warsaw University of Technology have devised a way to send and receive messages hidden in the data packets used to represent silences during a Skype call. After learning that Skype transmits voice data in 130-byte packets and the silences in 70-byte packets, the researchers came upon the idea of using the latter to conceal the sending and receiving of additional messages."

Read the 79 comments

US Nuclear Lab Removes Chinese Tech

Posted by samzenpus on Monday January 07, @12:32PM
from the get-it-out-of-here dept.

Rambo Tribble writes

"Reuters reports that Los Almos National Laboratory has removed switches produced by Chinese firm H3C, which once had ties to Huawei. This appears to be a step taken to placate a nervous Congress, rather in response to any detected security issues. From the article: 'Switches are used to manage data traffic on computer networks.' The exact number of"
Case study: Critical Infrastructure Protection
Examples of Systems

- Transportation
- Financial
- Energy
- Human health
- Agricultural health
- Communication
- Cities and fixed infrastructure
Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.

Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked.

These same advances have created new vulnerabilities to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.
In early 2000, NHS decided to aggregate disparate databases into a single centrally accessible database. What are the threats caused by aggregation of data?
McDonnell Douglas Aircrash example

• DC10 – a wide-bodied triple jet-engined plane capable of carrying 340 passengers manufactured in USA

• Incidents:
  – 56 crashes and 1262 fatalities
  – Cargo door (outward design); needs heavier locks than inward design
  – Hull-board design
  – Blackbox design (audit)
  – Culture of ignoring safety concerns.
Interdependency of Systems

[Diagram showing interdependencies between various systems such as Banking and Finance, Government, Emergency Response, Transportation, Oil and Natural Gas, Potable and Waste Water, Electricity, and Telecom. Each system is connected by arrows indicating dependencies and interrelations.]
For want of a nail the shoe was lost.
For want of a shoe the horse was lost.
For want of a horse the rider was lost.
For want of a rider the battle was lost.
For want of a battle the kingdom was lost.
And all for the want of a horseshoe nail.
Case Study: 2003 Blackout

• Provides an excellent example of failure of a critical infrastructure system involving computer control

• Not caused by a malicious attack but influential in advancing concerns about cyber security for critical infrastructure
Basic Structure of the Electric Grid

Color Key:
- **Blue**: Transmission
- **Green**: Distribution
- **Black**: Generation

- Transmission Lines: 765, 500, 345, 230, and 138 kV
- Substation Step-Down Transformer
- Customer:
  - Subtransmission: 26 kV and 69 kV
  - Primary Customer: 13 kV and 4 kV
  - Secondary Customer: 120 V and 240 V

Generating Station
- Generator Step Up Transformer
- Transmission Customer: 138 kV or 230 kV
Objectives of an Energy Management System (EMS)

- Balance generation and demand
- Maintain scheduled voltages
- Ensure that thermal limits are not exceeded
- Keep the system in a stable condition
- Maintain the “N-1 criterion”
- Plan, design, and maintain the system to operate reliably
- Prepare for emergencies
SCADA for EMS

• EMSs are increasingly exploiting computers and data networking

• Supervisory Control and Data-Acquisition (SCADA):
  – Data acquisition: collection, processing, monitoring
  – Supervisory control: manual overrides, alarm inhibit/enable
  – Alarm display and control
SCADA System General Layout

[Diagram showing control center, data historian, control server, communications routers, engineering workstations, switched telephone, leased line or power line based communications, radio microwave or cellular, satellite, wide area network, field site 1, field site 2, field site 3, modem, PLC, WAN CARD, IED, RTU]
Documented Security Incidents for Industrial Control Systems

- Salt River Project (1994): breach of a water and electricity provider’s computers by modem
- Worchester Air Traffic Communications (1997): teenager disables public switching network for an airport
- Maroochy Shire Sewage Spill (2000): attacker accesses system releasing 264,000 gallons of raw sewage
- Uranium enrichment centrifuge-overspinning attack (2008-2010) by malware attack mounted by US/Israel on Iranian nuclear-power program.
First Scenario

• Using war dialers, an adversary finds modems connected to the programmable breakers of the electric power transmission control system, cracks the passwords that control access to the breakers, and changes the control settings to cause local power outages and damage equipment.

• The adversary lowers the settings from 500 Ampere (A) to 200 A on some circuit breakers, taking those lines out of service and diverting power to neighboring lines. At the same time, the adversary raises the settings on neighboring lines to 900 A, preventing the circuit breakers from tripping and overloading the lines.

• This causes significant damage to transformers and other critical equipment, resulting in lengthy repair outages.

Second Scenario

• A power plant serving a large metropolitan district has successfully isolated the control system from the corporate network of the plant, installed state-of-the-art firewalls, and implemented intrusion detection and prevention technology.

• An engineer innocently downloads information on a continuing education seminar at a local college, inadvertently introducing a virus into the control network. Just before the morning peak, the operator screens go blank and the system is shut down.
The 2003 Blackout

• Started August 14 around 4pm and lasted about 4 days.
• 50 million people were affected.
• Total costs were estimated at more than 5 billion US dollars.
• – run video --
Cascading Failure

- **Phase 5:** Unplanned shifts of power across the region
- **Phase 6:** Full cascade
- **Phase 7:** Formation of islands
- Why the blackout stopped where it did
Root Causes

• Causality can be described at multiple levels
  – Management
  – Technology

• There is rarely a single cause for a major event
  – “The vessel Baltic Star, registered in Panama, ran aground at full speed on the shore of an island in the Stockholm waters on account of thick fog. One of the boilers had broken down, the steering system reacted only slowly, the compass was maladjusted, the captain had gone down into the ship to telephone, the outlook man on the prow took a coffee break and the pilot had given an erroneous order in English to the sailor who was tending the rudder. The latter was hard of hearing and understood only Greek.”
The Tree that Did $5,000,000,000 in Damage

All for the want of a horseshoe nail?
What Caused the Blackout?

• Limited reserves and un-trimmed trees in the Cleveland control area
• More failures than expected
• Insufficient understanding of system state through networked computer control
  – Multiple failed systems: MISO state estimator and alarms at First Energy
• System integration that enabled the blackout to spread broadly without supporting adequate information exchange
Effects on Other Infrastructure

• Water supply
  – Example: Cleveland lost water pressure and issued a boil advisory

• Transportation
  – Example: Amtrak NE Corridor down above Philadelphia
  – Example: 7 hour wait for trucks because of loss of electronic border checks at the Canada/US border

• Communication
  – Wired telephones continued but cellular service was disrupted

• Industry
  – Many factory closings in affected area

• Fixed infrastructure
  – Looting in Ottowa and Brooklyn (but limited compared to the 1977 NY blackout)
**Cyber-Security Dimension**

- Blackout was influential for cyber-security.
- **Why?** The report asserts that there is no evidence that a cyber-attack contributed to the blackout. Yet, the computer control difficulties **did** contribute.
- Increasing interdependency of the system and increased reliance on computer monitoring and control open the path to **deliberately-caused** failures like the 2003 blackout based on cyber-attacks.
Reading

- London Ambulance failure from cascading effects: http://erichmusick.com/writings/06/lsas_failure.html
Example: Card security failure

- Additional examples
  - Card security (0x20 success)
Example: Challenger disaster (O-rings; 6 stage)
Conclusions

• The biggest impediment to a more secure online world is the ignorance of common security failures.

• Understanding the history of security failures is one of the excellent ways of learning about network security.