In-Class Presentations
- On the paper you read for a given report
  - I will email you which report you’re presenting on
  - Presentation is summary of your report
  - Send me PPT of your presentation at least 1h before
- DEN students use WebEx – I sent the link
- 10 minutes long, 5 slides:
  - Problem, why important, why difficult
  - Solution
  - Evaluation
  - Your opinion
  - Your ideas
- Graded: Slide appearance, content and delivery

Sanitization
- Remove or obscure (anonymize) sensitive data
  - Remove packet contents and application headers
  - Anonymize IP addresses
    - Positional – anonymize in order of appearance. Inconsistent and lose information about networks.
    - Cryptographic – anonymize by encrypting with a key. Consistent but still lose information about networks.
    - Prefix-preserving – cryptographic approach is applied to portions of IP separately to preserve network information.
  - Sanitization loses a lot of data – application headers, contents, IP addresses
    - This is acceptable for some research but not for all
  - Sanitized data still has sensitive information

Attack Classes
- Passive attacker
  - Observe publicly released trace
  - Use some public or private auxiliary information to infer private data
- Active attacker
  - Insert traffic during trace collection
  - Identify this traffic later in public trace
    - This creates an auxiliary information channel
    - Can learn what method was used to obscure private data
    - Can verify presence or absence of data items with same/similar values in other records
  - Provider cannot identify injected traffic
    - Covert channel problem

Privacy of Sanitized Data
- Attacks focus on breaking anonymization or discovering vulnerabilities to use in attacks
  - Web page attack – identify Web pages based on size and number of objects
  - Clock skew attack – infer clock skew from packet timing, link it to the one obtained by probing
  - Link layer, Clustering and Behavior attack – infer topology, cluster same prefix addresses, use behavior models of popular servers to pinpoint them in the trace
  - Scan attack – infer relationship between IPs in scans
  - Innumerable active attacks
    - Removing sensitive data for many of these attacks makes sanitized trace unusable

Drawbacks of Sanitization Approach
- Low utility
  - One-size-fits-all data is released
  - Any field sensitive in some context must be removed from all contexts
- Low privacy
  - Known attacks are not handled because that would seriously decrease utility
  - Active attacks cannot be handled
  - Data providers have no insight into trace usage
  - Users get access to entire trace, regardless of intent – future attacks can be launched by anyone

Our Proposal: Secure Queries
- Providers publish a query language
  - Interpreter allows certain queries on certain packet fields and in a given context
  - The restrictions are mined from a provider-specified privacy policy
- Users submit queries to an online portal, receive aggregate results: counts, distributions, histograms, etc.
Advantages of Secure Queries
- Higher utility
  - Fine-grain control over field processing and its context allows safe access to some fields that would be removed/obscured in sanitization – less data loss
  - Even application headers or contents could be processed
  - Easy coding in a high-level language
- Better privacy
  - Providers have insight into trace usage, can audit
  - Can precisely control what is allowed
  - Future attacks handled via policy/language changes – only those users that previously ran forbidden queries can launch attacks

Linkages – The Trail We Leave
- Identifiers
  - IP Address, cookies, login IDs
  - MAC Address and other unique IDs
- Where saved
  - Log files
- Persistence
  - How often does identifier change
  - How can it be mapped to user identification

Unlinking the Trail
- Blind Signatures
  - Content of the message is disguised before it is signed
  - Resulting signature can be verified against original content
  - Analogy: Enclosing a message in a write-through envelope which is signed and sealed. Signer doesn’t see the message.
  - Enable proof of some attribute without identifying the prover
  - Application in anonymous e-currency and e-voting

Anonymizers
- A remote web proxy
  - Hides originators IP address from sites that are visited
  - Usually strips off cookies and other identifying information
- Limitations
  - You are dependent on the privacy protections of the anonymizer itself
  - All your activities are now visible at this single point of compromise
  - Use of the anonymizer may highlight those activities that you want to go unnoticed

Onion Routing
- Layers of peer-to-peer anonymization
  - You contact some node in the onion routing network
  - Your traffic is forward to other nodes in the network
  - Random delays and reordering are applied.
  - With fixed probability, it is forwarded on to its destination
- Traffic analysis requires linking packets through the full chain of participants
  - And may be different for each association

Human Element
Social Engineering

- Organization invest into sophisticated security systems
  - Firewalls
  - Intrusion detection systems
  - Safes
  - Smart cards
- Humans repeatedly prove to be the weakest link
  - A skillful attacker will be able to obtain best guarded information by making a few phone calls ...


Robbing a Bank Without a Gun

- Stanley Rifkin worked for a contracting company to develop backup system for wire room of Security Pacific National Bank
  - People in wire room used one-day codes to authorize wire transfers
  - They wrote those on a paper each day and posted it inside the room
  - Stanley walked in a room one day to "take notes on operation procedures for the backup system" and memorized the code

Getting Credit History Information

- Grace was a PI who was following a trail of money that his client’s husband withdrew from their joint account
  - Grace knew that banks call a credit verification service CreditChex to verify new client information
  - Grace first called husband’s bank and got familiar with the lingo – what do they give to CreditChex when they ask for information, because he’s writing a book ...
  - Grace then called another bank employee presenting himself as CreditChex customer service representative and asked for employee’s MerchantID among other things
  - Grace called CreditChex next presenting himself as bank employee and got information about the husband’s new accounts

Robbing a Bank Without a Gun

- Stanley next walked to a phone in the bank’s lobby, gave a name and office number of an authorized employee, then gave daily code
  - He asked that $10M be transferred to his account in Switzerland
  - Wire-room employee asked for an interoffice settlement number
  - Stanley said he will check and call back
  - He called another department claiming to work in the wire room and asked for an interoffice settlement number then called back the wire-room and finalized the transaction

Getting a List of Employees

- Didi was a head-hunter who wanted to steal a few employees for her client from his competition
  - Didi first called a reception desk at the competition, presenting as branch employee and got connected to Accounting
  - She called Accounting and got cost center – charge code for billing each department’s needs
  - Didi then called a random other department, pretending to be a branch employee and asked how to get a printed phonebook for a contractor – call Publications
  - She called Publications and asked for phonebook to be mailed to branch contractor – a rented mailbox; she sweet talked the guy there to skip formal procedure for paperwork filing and just bill this to the cost center
The attacker dials private phone company’s number for Mechanized Line Assignment Center
- Presents himself as cable splicer in the field
- Gives a few convincing statements
- Asks for help to rewire the terminal and gets all phone numbers assigned to the wires

The attacker calls utility company “from some company branch and he has a vice president’s office on the phone”
- He says his computer is down and could he get some help
- The attacker then gives victim’s name and asks for account number, phone number and address

Frank Parsons has been running from the FBI
- He moved to a new state and was looking for a job
- He found a good job but they wanted a background criminal check
- The form asked for a fingerprint to check state criminal record (which Frank didn’t have)
- Frank wanted to find out if this will be transmitted to the FBI
- He called the state patrol and asked, said he worked with State Department of Justice and they were doing a research ...

Doyle Lonnegan is a collection man for gambling debts and he needs to collect a debt from X
- Doyle finds out X’s frequented video rental store
- Doyle calls another branch pretending to be a satisfied customer and asks for store number, manager’s name, etc.
- Doyle then calls X’s store, presents himself as fellow employee from a different store – says X is there and wants to rent and wants to use his credit card number on file but computers are down ...
- He can now charge the debt to the credit card

Company CLPhone advertised 1–cent cell phone with a contract subscription
- Mark wants the phone but not the subscription
- He calls a local CLPhone branch and presents himself as a customer who talked to a sales person the other night and would like to sign up – Mark gets sales person’s name
- Mark calls another CLPhone branch presenting himself as a sales person who has a customer waiting – customer already signed up but branch is out of cell phones

Bobby wants to break into company’s network
- He first calls an employee, Ted, presenting himself as Eddie from the Help Desk
- Eddie asks Ted how has his network service been because they have been having problems – supplies his cell phone for when the problem arises (reverse social engineering).
- Eddie also obtains Ted’s port number from Ted Bobby then calls IT, presenting himself as Eddie from the Help Desk and asks that the port be disabled
- Frustrated Ted calls and Eddie “fixes the problem”
- Eddie asks Ted to install a piece of software so “this doesn’t happen again”
Breaking into the Network – 2
- Attacker wants to get an inside access
  - He first calls HR and asks for the list of new employees
  - Attacker then calls one new employee and gives her security briefing - he also gets her username and gets her to change her password with his help

Breaking into the Network – 3
- Attacker wants to get confidential files for project X
  - He calls company switchboard and gets phone number of any employee – Sam
  - Attacker calls Sam, saying he is from FedEx and there is a package for project X – gets project lead’s name (Jerry) and number
  - Calls Jerry’s office and learns he’s on vacation but gets his secretary’s number – Michelle
  - Calls Michelle and asks for project X people E-mails “because Jerry asked me for a favor”
  - Calls IT and claims he is employee who just bought a laptop - gets dial-in access

Breaking into the Network – 3
- Attacker then finds a computer with a guest account and breaks in – this computer runs Unix system
- He examines a shadow file and figures out that one of the project people (Steve) has password Janice
  - But password doesn’t work
  - Attacker waits for the weekend and calls Steve pretending to be from IT and repairing crashed network
  - He asks for Steve’s password, providing the old one

Breaking into the Network – 4
- Attacker calls the switchboard asking for employee Jones – learns his first name Jo
  - Speaks to Jo and claims to be from payroll – Joe’s paycheck has been deposited to Credit Union account
  - Jo provides his employee number to clear up the mess
  - Attacker calls another branch and asks to be given a temporary username and password while on business trip – gives Joe’s name and employee number for verification

Breaking into the Network – 5
- Danny wants to break into company’s network and steal some confidential files on product X but they use two-factor authentication
  - Secure ID – a time based token that changes every 60 seconds
  - Username and password
- Danny learns some employee’s name (Bob), number, his manager’s number, username, password, etc.
  - Waits for a stormy day
  - Calls IT and claims to be Bob who left his secure ID at his desk and could someone fetch it and read the info

Breaking into the Network – 5
- IT refuses but offers a temporary secure ID that will work just the same
  - A guy in IT even calls his manager to check that this is OK and vouches for “Bob”
- Danny searches newsgroups for postings on product X – gets the name of the guy working on it (Scott)
  - Scott happens to be in the office and happily provides server name to “IT guy”
  - Danny can’t connect to server from dial-up and he calls IT again and asks for a temporary account in IT
  - From IT computers he finds a vulnerability on the development server and grabs files on product X
What are the Key Steps?
- Knowing the lingo
- Being familiar, relaxed and friendly
- Playing on people's feelings
  - People want to help
  - Especially if you work for their boss
  - Or they can be easily intimidated
- Pretending to be an insider
- Asking for "insignificant" pieces of information

How to Protect from Social Engineering?
- Limit the number of people who know key information
- Educate employees about security
- Establish authentication procedures going through a single site
- Ask employees to call back when providing sensitive information, and to use the number on file