CSci530: Computer Security Systems
Lecture 10 – 28 October 2011
Intrusion Detection

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Intrusion Types

- External attacks
  - Password cracks, port scans, packet spoofing, DOS attacks

- Internal attacks
  - Masqueraders, Misuse of privileges

Attack Stages

- Intelligence gathering
  - attacker observes the system to determine vulnerabilities (e.g., port scans)

- Planning
  - decide what resource to attack and how

- Attack execution
  - carry out the plan

- Hiding
  - cover traces of attack

- Preparation for future attacks
  - install backdoors for future entry points
Intrusion Detection

- Intrusion detection is the problem of identifying unauthorized use, misuse, and abuse of computer systems by both system insiders and external penetrators

- Why Is IDS Necessary?

IDS types

- Detection Method
  - Knowledge-based (signature-based) vs behavior-based (anomaly-based)
- Behavior on detection
  - passive vs. reactive
- Deployment
  - network-based, host-based and application-based
Components of ID systems

- Collectors
  - Gather raw data
- Director
  - Reduces incoming traffic and finds relationships
- Notifier
  - Accepts data from director and takes appropriate action

Advanced IDS models

- Distributed Detection
  - Combining host and network monitoring (DIDS)
  - Autonomous agents
    (Crosbie and Spafford)
Intrusion Response

• Intrusion Prevention
  – (marketing buzzword)
• Intrusion Response
  – How to react when an intrusion is detected

Possible Responses

– Notify administrator
– System or network lockdown
– Place attacker in controlled environment
– Slow the system for offending processes
– Kill the process
Phase of Response (Bishop)

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow up

PREPARATION

- Generate baseline for system
  - Checksums of binaries
    - For use by systems like tripwire
- Develop procedures to follow
- Maintain backups
IDENTIFICATION

- This is the role of the ID system
  - Detect attack
  - Characterize attack
  - Try to assess motives of attack
  - Determine what has been affected

CONTAINMENT

- Passive monitoring
  - To learn intent of attacker
  - Learn new attack modes so one can defend against them later
- Constraining access
  - Locking down system
  - Closing connections
  - Blocking at firewall, or closer to source
- Combination
  - Constrain activities, but don’t let attacker know one is doing so (Honeypots, Jail).
ERADICATION

• Prevent attack or effects of attack from recurring.
  – Locking down system (also in containment phase)
  – Blocking connections at firewall
  – Isolate potential targets

RECOVERY

• Restore system to safe state
  – Check all software for backdoors
  – Recover data from backup
  – Reinstall but don’t get re-infected before patches applied.
FOLLOWUP

- Take action against attacker.
  - Find origin of attack
- Notify other affected parties
  - Some of this occurs in earlier phases as well
- Assess what went wrong and correct procedures.
- Find buggy software that was exploited and fix

Limitations of Monolithic ID

- Single point of failure
- Limited access to data sources
- Only one perspective on transactions
- Some attacks are inherently distributed
  - Smurf
  - DDoS
- Conclusion: “Complete solutions” aren’t
Sharing Information

• Benefits
  – Increased robustness
  – More information for all components
  – Broader perspective on attacks
  – Capture distributed attacks
• Risks
  – Eavesdroppers, compromised components
  – In part – resolved cryptographically

Sharing Intrusion Information

• Defining appropriate level of expression
  – Efficiency
  – Expressivity
  – Specificity
CIDF

• Common Intrusion Detection Framework
  – Collaborative work of DARPA-funded projects in late 1990s
  – Task: Define language, protocols to exchange information about attacks and responses

CISL

• Common Intrusion Specification Language
  – Conveys information about attacks using ordinary English words
  – E.g., User joe obtains root access on demon.example.com at 2003 Jun 12 14:15 PDT
CISL

- Problem: Parsing English is hard
- S-expressions (Rivest)
  - Lisp-like grouping using parentheses
  - Simplest examples: (name value) pairs
    (Username ‘joe’)
    (Hostname ‘demon.example.com’)
    (Date ‘2003 Jun 12 14:15 PDT’)
    (Action obtainRootAccess)

CISL

- Problems with simple pairs
  - Confusion about roles played by entities
    - Is joe an attacker, an observer, or a victim?
    - Is demon.example.com the source or the target of the attack?
  - Inability to express compound events
    - Can’t distinguish attackers in multiple stages
- Group objects into GIDOs
CISL: Roles

- Clarifies roles identified by descriptors
  
  (Attacker
    (Username ‘joe’)
    (Hostname ‘carton.example.com’)
    (UserID 501)
  )

  (Target
    (Hostname ‘demon.example.com’)
  )

CISL: Verbs

- Permit generic description of actions
  
  (Compromise
    (Attacker ...)
    (Observer
      (Date ‘2003 Jun 12 14:15 PDT’)
      (ProgramName ‘GrIDSDetector’)
    )

    (Target ...)
  )

Lessons from CISL

• Lessons from testing, standardization efforts
  – Heavyweight
  – Not ambiguous, but too many ways to say the same thing
  – Mismatch between what CISL can say and what detectors/analyzers can reliably know

Worm and DDOS Detection

• Difficulty is distinguishing attacks from the background.
  – Zero Day Worms
  – DDoS
• Discussion of techniques
  – Honeynets, network telescopes
  – Look for correlation of activity
Reacting to Attacks

• How to Respond to Ongoing Attack
  – Disable attacks in one’s own space
  – Possibly observe activities
  – Beware of rules that protect the privacy of the attacker (yes, really)
• Do not retaliate
  – May be wrong about source of attack.
  – May cause more harm than attack itself.
  – Creates new way to mount attack
    ▪ Exploits the human element

Current event — How does this relate to our discussion

iPhone 4 Accelerometer Enables Device To Be Used For Spying
Scientific American - First Posted: 10/27/11 12:01 PM ET Updated: 10/27/11 12:01 PM ET By Christopher Intagliata

• Used to be if spies wanted to eavesdrop, they planted a bug. These days, it’s much easier. Because we all carry potential bugs in our pockets—smartphones. One team of researchers used an iPhone to track typing on a nearby computer keyboard with up to 80 percent accuracy. They presented the findings at a computer security conference in Chicago. [Philip Marquardt et al, (sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers, 18th ACM Conference on Computer and Communications Security]

• The researchers designed a malicious app for the iPhone 4. When you place the phone near a keyboard, it exploits accelerometer and gyroscope data to sense vibrations as the victim types—detecting whether keystrokes come from the left or right side of the keyboard, and how near or far subsequent keys are from each other. Then, using that seismic fingerprint, the app checks a pre-created “vibrational” dictionary for the most likely words—a technique that works reliably on words of three letters or more.

• Of course, you’d need to install the app to allow it to spy. But whereas most apps have to ask permission to access location data or the camera, that’s not so for the accelerometer. This kind of attack may offer good reason to limit accelerometer access too—and keep iPhones from becoming “spiPhones.”
The Human is the Weak Point

• Low bandwidth used between computer and human.
  – User can read, but unable to process crypto in head.
  – Needs system as its proxy
  – This creates vulnerability.
• Users don’t understand system
  – Often trust what is displayed
  – Basis for phishing
The Human is the Weak Point

- Humans make mistakes
  - Configure system incorrectly
- Humans can be compromised
  - Bribes
  - Social Engineering
- Programmers often don’t consider the limitations of users when designing systems.

Some Attacks

- Social Engineering
  - Phishing – in many forms
- Mis-configuration
- Carelessness
- Malicious insiders
- Bugs in software
Addressing the Limitations

- Personal Proxies
  - Smartcards or devices
- User interface improvements
  - Software can highlight things that it thinks are odd.
- Delegate management
  - Users can rely on better trained entities to manage their systems.
- Try not to get in the way of the users legitimate activities
  - Or they will disable security mechanisms.

Social Engineering

- Arun Viswanathan provided me with some slides on social engineering that we wrote based on the book “The Art of Deception” by Kevin Mitnik.
  - In the next 6 slides, I present material provided by Arun.
- Social Engineering attacks rely on human tendency to trust, fooling users that might otherwise follow good practices to do things that they would not otherwise do.
Total Security / not quite

- Consider the statement that the only secure computer is one that is turned off and/or disconnected from the network.
- The social engineering attack against such systems is to convince someone to turn it on and plug it back into the network.

Six Tendencies

- These tendencies are used in social engineering to obtain assistance from unsuspecting employees.
Six Tendencies

• People tend to comply with requests from those in authority.
  – Claims by attacker that they are from the IT department or the audit department.
• People tend to comply with requests from those who they like.
  – Attackers learn interests of employee and strikes up a discussion.

Six Tendencies

• People tend to follow requests if they get something of value.
  – Subject asked to install software to get a free gift.
• People tend to follow requests to abide by public commitments.
  – Asked to abide by security policy and to demonstrate compliance by disclosing that their password is secure – and what it is.
Six Tendencies

• People tend to follow group norms.
  – Attacker mentions names of others who have “complied” with the request, and will the subject comply as well.

• People tend to follow requests under time commitment.
  – First 10 callers get some benefit.

Steps of Social Engineering

• Conduct research
  – Get information from public records, company phone books, company web site, checking the trash.

• Developing rapport with subject
  – Use information from research phase. Cite common acquaintances, why the subjects help is important.

• Exploiting trust
  – Asking subject to take an action. Manipulate subject to contact attacker (e.g. phishing).

• Utilize information obtained from attack
  – Repeating the cycle.
Context Sensitive Certificate Verification and Specific Password Warnings

• Work out of University of Pittsburgh
• Changes dialogue for accepting signatures by unknown CAs.
• Changes dialogue to prompt user about situation where password are sent unprotected.
• Does reduce man in the middle attacks
  – By preventing easy acceptance of CA certs
  – Requires specific action to retrieve cert
  – Would users find a way around this?

Current event – How does this relate to our discussion

Loose lips still sink corporate ships, social engineering as lethal as ever
Darlene Storm - Computer World – November 3, 2011

Last year at DefCon, contestants proved their social engineering schmooze was lethal to corporate America. Even after all the lessons learned from this summer's high profile hacks, made possible by social engineering attacks, the results from the 2nd annual social engineer Schmooze Strikes Back contest were the same. Loose lips still sink corporate ships; social engineering is no less lethal to companies. As the Social Engineering Capture the Flag report states "in the end, all of the companies would have received a failing mark in a real social engineering penetration test."

Intel was gathered from Google, security plans and procedures on corporate websites, LinkedIn, "miscellaneous,” and Facebook. Recon was also done via maps and job postings. Then there were things like personal blogs talking company dirt, the loose lips helping to sink corporate ships that required no manipulation or smooth talking for an attacker. And in real life, after determining targets and their social networking sites, an attacker could spoof emails from those sites or gather email addresses for phishing attempts.

The report concluded, "There is ample information floating out there that malicious social engineers can use to target the average company. This information can be put to use by the average, inexperienced social engineer to bear devastating results. This is consistent across all tested industries, with professional organizations appearing to be the most vulnerable.” Social engineering is still lethal to corporate America.
Trusted vs. Trustworthy

- We trust our computers
  - We depend upon them.
  - We are vulnerable to breaches of security.
- Our computer systems today are not worthy of trust.
  - We have buggy software
  - We configure the systems incorrectly
  - Our user interfaces are ambiguous regarding the parts of the system with which we communicate.
A Controversial Issue

• Many individuals distrust trusted computing.
• One view can be found at http://www.lafkon.net/tc/
  – An animated short film by Benjamin Stephan and Lutz Vogel

What is Trusted Computing

• Attestation
  – Includes Trusted path
• Separation
  – Secure storage (data/keys)
  – Protection of processes
• The rest is policy
  – That’s the hard part
  – And the controversial part
Separation of Security Domains

- Need to delineation between domains
  - Old Concept:
    - Rings in Multics
    - System vs. Privileged mode
  - But who decides what is trusted
    - User in some cases
    - Third parties in others
    - Trusted computing provides the basis for making the assessment.

Trusted Path

- We need a “trusted path”
  - For user to communicate with a domain that is trustworthy.
    - Usually initiated by escape sequence that application can not intercept: e.g. CTL-ALT-DEL
  - Could be direct interface to trusted device:
    - Display and keypad on smartcard
Communicated Assurance

• We need a “trusted path” across the network.
• Provides authentication of the software components with which one communicates.

The Landscape – Early Work

• Multics System in late 1960s.
  – Trusted path, isolation.
  – Described early need for remote attestation and how accomplished.
The Landscape – Industry

- Industry interest in the late 1990s.
- Consortia formed such as the Trusted Computing Group.
- Standards specifications, starting with specs for hardware with goal of eventual inclusion in all new computer systems.
  - Current results centered around attestation and secure storage.

The Landscape – Applications

- Digital Rights Management
- Network Admission Control
  - PC Health Monitoring
  - Malware detection
- Virtualization of world view
  - VPN Segregation
  - Process control / SCADA systems
- Many other users
Discussion - Risks

- Trusted computing is a tool that can be misused.
  - If one party has too much market power, it can dictate unreasonable terms and enforce them.
- Too much trust in trusted computing.
  - Attestation does not make a component trustworthy.
  - Some will rely too much on certifications.

Discussion - Benefits

- Allows systems to be developed that require trustworthy remote components.
  - Provides protection of data when out of the hands of its owner.
- Can provide isolation and virtualization beyond the local system.
  - Provides containment of compromise.
Discussion – What’s missing

• Tools to manage policy
  – Managing policy was limitation for TC support in Vista
• Applications that protect the end user
  – We need more than DRM and tools to limit what users run.
• New architectures and ways of thinking about security.

Trusted Baggage

• So why all the concerns in the open source community regarding trusted computing.
  – Does it really discriminate against open sources software.
  – Can it be used to spy on users.
Equal Opportunity for Discrimination

- Trusted computing means that the entities that interact with one another can be more certain about their counterparts.
- This gives all entities the ability to discriminate based on trust.
- Trust is not global – instead one is trusted “to act a certain way”.

Equal Opportunity for Discrimination(2)

- Parties can impose limits on what the software they trust will do.
- That can leave less trusted entities at a disadvantage.
- Open source has fewer opportunities to become “trusted”.

Covered Last Lecture
Is Trusted Computing Evil

- Trusted computing is not evil
  - It is the policies that companies use trusted computing to enforce that are in question.
  - Do some policies violate intrinsic rights or fair competition?
  - That is for the courts to decide.

What can we do with TC?

- Clearer delineation of security domains
  - We can run untrusted programs safely.
    - Run in domain with no access to sensitive resources
      - Such as most of your filesystem
      - Requests to resources require mediation by TCB, with possible queries user through trusted path.
Mediating Programs Today

• Why are we so vulnerable to malicious code today?
  – Running programs have full access to system files.
  – Why? NTFS and XP provide separation.
    ▪ But many applications won’t install, or even run, unless users have administrator access.
  – So we run in “System High”

Corporate IT Departments Solve this

• Users don’t have administrator access even on their own laptops.
  – This keeps end users from installing their own software, and keeps IT staff in control.
  – IT staff select only software for end users that will run without administrator privileges.
  – But systems still vulnerable to exploits in programs that cause access to private data.
  – Effects of “Plugins” can persist across sessions.
The next step

• But, what if programs were accompanied by third party certificates that said what they should be able access.
  – IT department can issues the certificates for new applications.
  – Access beyond what is expected results in system dialogue with user over the trusted path.

Red / Green Networks (1)

• Butler Lampson of Microsoft and MIT suggests we need two computers (or two domains within our computers).
  – Red network provides for open interaction with anyone, and low confidence in who we talk with.
  – We are prepared to reload from scratch and lose our state in the red system.
Red / Green Networks (2)

- The Green system is the one where we store our important information, and from which we communicate to our banks, and perform other sensitive functions.
  - The Green network provides high accountability, no anonymity, and we are safe because of the accountability.
  - But this green system requires professional administration.
  - My concern is that a breach anywhere destroys the accountability for all.

Somewhere over the Rainbow

- But what if we could define these systems on an application by application basis.
  - There must be a barrier to creating new virtual systems, so that users don’t become accustomed to clicking “OK”.
  - But once created, the TCB prevents the unauthorized retrieval of information from outside this virtual system, or the import of untrusted code into this system.
  - Question is who sets the rules for information flow, and do we allow overrides (to allow the creation of third party applications that do need access to the information so protected).
A Financial Virtual System

• I might have my financial virtual system. When asked for financially sensitive data, I hit CTRL-ALT-DEL to see which virtual system is asking for the data.
• I create a new virtual systems from trusted media provided by my bank.
• I can add applications, like quicken, and new participant’s, like my stock broker, to a virtual system only if they have credentials signed by a trusted third party.
  – Perhaps my bank, perhaps some other entity.

How Many Virtual Systems

• Some examples:
  – My open, untrusted, wild Internet.
  – My financial virtual system
  – My employer's virtual system.
  – Virtual systems for collaborations
    • Virtual Organizations
  – Virtual systems that protect others
    • Might run inside VM’s that protect me
      – Resolve conflicting policies
      – DRM vs. Privacy, etc
Digital Rights Management

- Strong DRM systems require trust in the systems that receive and process protected content.
  - Trust is decided by the provider of the content.
  - This requires that the system provides assurance that the software running on the accessing system is software trusted by the provider.

Privacy and Anti-Trust Concerns

- The provider decides its basis for trust.
  - Trusted software may have features that are counter to the interests of the customer.
    - Imposed limits on fair use.
    - Collection and transmission of data the customer considers private.
    - Inability to access the content on alternative platforms, or within an open source O/S.
Trusted Computing Cuts Both Ways

• The provider-trusted application might be running in a protected environment that doesn’t have access to the user’s private data.
  – Attempts to access the private data would thus be brought to the users attention and mediate through the trusted path.
  – The provider still has the right not to provide the content, but at least the surreptitious snooping on the user is exposed.

What do we need for TC

• Trust must be grounded
  – Hardware support
    ▪ How do we trust the hardware
    ▪ Tamper resistance
      – Embedded encryption key for signing next level certificates.
    ▪ Trusted HW generates signed checksum of the OS and provides new private key to the OS
Privacy of Trusted Hardware

• Consider the processor serial number debate over Intel chips.
  – Many considered it a violation of privacy for software to have ability to uniquely identify the process on which it runs, since this data could be embedded in protocols to track user’s movements and associations.
  – But Ethernet address is similar, although software allows one to use a different MAC address.
  – Ethernet addresses are often used in deriving unique identifiers.

The Key to your Trusted Hardware

• Does not have to be unique per machine, but uniqueness allows revocation if hardware is known to be compromised.
  – But what if a whole class of hardware is compromised, if the machine no longer useful for a whole class of applications. Who pays to replace it.
• A unique key identifies specific machine in use.
  – Can a signature use a series of unique keys that are not linkable, yet which can be revoked (research problem).
Non-Maskable Interrupts

- We must have hardware support for a non-maskable interrupt that will transfer program execution to the Trusted Computing Base (TCB).
  - This invokes the trusted path

The Hardware Basis

- Trusted computing is proof by induction
  - Each attestation stage says something about the next level
  - Just like PKI Certification hierarchy
- One needs a basis step
  - On which one relies
  - Hardware is that step
    - (well, second step anyway)
Hardware Topics

• Trusted Platform Module
• Discussion of Secure Storage
• Boot process

Trusted Platform Module

• Basically a Key Storage and Generation Device
• Capabilities:
  – Generation of new keys
  – Storage and management of keys
  ▪ Uses keys without releasing
Trusted Platform Module (TPM)?

Smartcard-like module on the motherboard that:

- Performs cryptographic functions
  - RSA, SHA-1, RNG
  - Meets encryption export requirements
- Can create, store and manage keys
  - Provides a unique Endorsement Key (EK)
  - Provides a unique Storage Root Key (SRK)
- Performs digital signature operations
- Holds Platform Measurements (hashes)
- Anchors chain of trust for keys and credentials
- Protects itself against attacks

TPM 1.2 spec: www.trustedcomputinggroup.org

Why Use A TPM?

- Trusted Platforms use Roots-of-Trust
  - A TPM is an implementation of a Root-of-Trust
- A hardware Root-of-Trust has distinct advantages
  - Software can be hacked by Software
    - Difficult to root trust in software that has to validate itself
  - Hardware can be made to be robust against attacks
    - Certified to be tamper resistant
  - Hardware and software combined can protect root secrets better than software alone
- A TPM can ensure that keys and secrets are only available for use when the environment is appropriate
  - Security can be tied to specific hardware and software configurations

Slide From Steve Lamb at Microsoft
Endorsement Key

- Every TPM has unique Endorsement key
  - Semi-root of trust for system
  - Generated and installed during manufacture
    - Issues
  - Real root is CA that signs public key associated with Endorsement key

Using Encryption for Atestation

- Extend
  - Add data to a PCR
  - 20 byte hash hashed into current PCR
  - As each module loaded its hash extends the PCR
- Quote
  - Sign current value of PCR
Secure Storage

- Full Disk Encryption
  - Key in register in disk
  - Or key in TPM and data encrypted/decrypted by TPM
- Seagate Drive uses register in Disk
  - Key must be loaded
  - User prompt at BIOS
  - Or managed by TPM
    - But OS image maybe on disk, how to get

OS Support for Trusted Computing (1)

- Separation of address space
  - So running processes don’t interfere with one another.
- Key and certificate management for processes
  - Process tables contain keys or key identifiers needed by application, and keys must be protected against access by others.
  - Processes need ability to use the keys.
OS Support for Trusted Computing (2)

- Fine grained access controls on persistent resources.
  - Protects such resources from untrusted applications.
- The system must protect against actions by the owner of the system.

Disk Layout & Key Storage

Windows Partition Contains:
- Encrypted OS
- Encrypted Page File
- Encrypted Temp Files
- Encrypted Data
- Encrypted Hibernation File

Where's the Encryption Key?
1. SRK (Storage Root Key) contained in TPM
2. SRK encrypts VEK (Volume Encryption Key) protected by TPM/PIN/Dongle
3. VEK stored (encrypted by SRK) on hard drive in Boot Partition

Boot Partition Contains: MBR, Loader, Boot Utilities (Unencrypted, small)
**BitLocker™ Architecture**

*Static Root of Trust Measurement of early boot components*

---

**Vista co-existence**

*Slide From Steve Lamb at Microsoft*

- BitLocker encrypts Windows *partition* only
- You won’t be able to dual-boot another OS on the same partition
- OSes on other partitions will work fine
- Attempts to modify the protected Windows partition will render it unbootable
  - Replacing MBR
  - Modifying even a single bit
No more running as root or administrator

• You may have full access within a virtual system, and to applications within the system it may look like root, but access to other virtual systems will be mediated.
• UserID’s will be the cross product of users and the virtual systems to which they are allowed access.
• All accessible resources must be associated with a virtual system.
Outline of Discussion

• Introduction – security vs privacy
• You are being tracked
• Aggregation of data
• Traffic analysis and onion routing
• P3P and Privacy Statements
• Protecting data on personal laptops/desktops
• Forensics
• Retention/Destruction Policies
• Who’s data is it anyway

What is Privacy?

• Privacy is about Personally Identifiable Information
• It is primarily a policy issue
  – Policy as a system issue
    ▪ Specifying what the system should allow
  – Policy as in public policy
    ▪ Same idea but less precise and must be mapped
• Privacy is an issue of user education
  ▪ Make sure users are aware of the potential use of the information they provide
  ▪ Give the user control
• Privacy is a Security Issue
  – Security is needed to implement the policy
Security v. Privacy

• Sometimes conflicting
  – Many security technologies depend on identification.
  – Many approaches to privacy depend on hiding one's identity.

• Sometime supportive
  – Privacy depends on protecting PII (personally identifiable information).
  – Poor security makes it more difficult to protect such information.

Major Debate on Attribution

• How much low level information should be kept to help track down cyber attacks.
  – Such information can be used to breach privacy assurances.
  – How long can such data be kept.
Privacy not Only About Privacy

• Business Concerns
  – Disclosing Information we think of as privacy related can divulge business plans.
    • Mergers
    • Product plans
    • Investigations
• Some “private” information is used for authentication.
  – SSN
  – Credit card numbers

You Are Being Tracked

• Location
  – From IP address
  – From Cell Phones
  – From RFID
• Interests, Purchase History, Political/Religious Affiliations
  – From RFID
  – From Transaction Details
  – From network and server traces
• Associates
  – From network, phone, email records
  – From location based information
• Health Information
  – From Purchases
  – From Location based information
  – From web history
More news - FOIA docs show feds can lojack mobiles without telco help –
Ars Technica - Julian Sanchez 10/16/2008

• Triggerfish, also known as cell-site simulators or digital analyzers, are nothing new: the technology was used in the 1990s to hunt down renowned hacker Kevin Mitnick. By posing as a cell tower, triggerfish trick nearby cell phones into transmitting their serial numbers, phone numbers, and other data to law enforcement.

Why Should you Care?

• Aren’t the only ones that need to be concerned about privacy the ones that are doing things that they shouldn’t?
• Consider the following:
  – Use of information outside original context
    • Certain information may be omitted
  – Implications may be mis-represented.
  – Inference of data that is sensitive.
  – Such data is often not protected.
  – Data can be used for manipulation.
Old News - Shopper’s Suit Thrown Out
Los Angeles Times – 2/11/1999

- Shopper’s Suit Thrown Out
- By Stuart Silverstein, Staff Reporter

February 11, 1999 in print edition C-2

A Vons shopper’s lawsuit that raised questions about the privacy of information that supermarkets collect on their customers’ purchases has been thrown out of court. Los Angeles Superior Court Judge David Horowitz tossed out the civil suit by plaintiff Robert Rivera of Los Angeles, declaring that the evidence never established that Vons was liable for damages.

The central issue in the case was a negligence claim Rivera made against Vons. It stemmed from an accident at the Lincoln Heights’ Vons in 1996 in which Rivera slipped on spilled yogurt and smashed his kneecap.

Although that issue was a routine legal matter, the case drew attention because Rivera raised the privacy issue in the pretrial phase. Rivera claimed that he learned that Vons looked up computer records of alcohol purchases he made while using his club discount card and threatened to use the information against him at trial.

Vons, however, denied looking up Rivera’s purchase records and the issue never came up in the trial, which lasted two weeks before being thrown out by the judge Tuesday.

A Vons spokesman said the company was “gratified by the judge’s decision.” M. Edward Franklin, a Century City lawyer representing Rivera, said he would seek a new trial for his client.

---

2009 current event

- SAN FRANCISCO — There is a new common symptom of the flu, in addition to the usual aches, coughs, fevers and sore throats. Turns out a lot of ailing Americans enter phrases like “flu symptoms” into Google and other search engines before they call their doctors.

- link
Aggregation of Data

• Consider whether it is safe to release information in aggregate.
  – Such information is presumably no longer personally identifiable
  – But given partial information, it is sometimes possible to derive other information by combining it with the aggregated data.

Anonymization of Data

• Consider whether it is safe to release information that has been stripped of so called personal identifiers.
  – Such information is presumably no longer personally identifiable
  – But is it. Consider the release of AOL search data that had been stripped of information identifying the individual performing the search.
    ▪ What is important is not just anonymity, but likability.
    ▪ If I can link multiple queries, I might be able to infer the identity of the person issuing the query through one query, at which point, all anonymity is lost.
Traffic Analysis

• Even when specifics of communication are hidden, the mere knowledge of communication between parties provides useful information to an adversary.
  – E.g. pending mergers or acquisitions
  – Relationships between entities
  – Created visibility of the structure of an organizations.
  – Allows some inference about your interests.

Information Useful for TA

• Lists of the web sites you visit
• Email logs
• Phone records
• Perhaps you expose the linkages through web sites like linked in.
• Consider what information remains in the clear when you design security protocols.
Obama's cell phone records breached
Washington (CNN) 11/21/2008

• Records from a cell phone used by President-elect Obama were improperly breached, apparently by employees of the cell phone company, Verizon Wireless said Thursday.

• "This week we learned that a number of Verizon Wireless employees have, without authorization, accessed and viewed President-Elect Barack Obama's personal cell phone account," Lowell McAdam, Verizon Wireless president and CEO, said in a statement.

• McAdam said the device on the account was a simple voice flip-phone, not a BlackBerry or other smartphone designed for e-mail or other data services, so none of Obama's e-mail could have been accessed.

• Gibbs said that anyone viewing the records likely would have been able to see phone numbers and the frequency of calls Obama made, but that "nobody was monitoring voicemail or anything like that."

Linkages – The Trail We Leave

• Identifiers
  • IP Address
  • Cookies
  • Login IDs
  • MAC Address and other unique IDs
  • Document meta-data
  • Printer microdots

• Where saved
  • Log files

• Persistence
  • How often does IP address change
  • How can it be mapped to user identification
Unlinking the Trail

• **Blind Signatures**
  – Enable proof of some attribute without identifying the prover.
  – Application in anonymous currency.
  – Useful in 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 you activities are now visible at this single point of compromise.
  – Use of the anonymizer may highlight exactly 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 is applied.
  – With fixed probability, it is forwarded on to its destination.

• TA requires linking packets through the full chain of participants.
  – And may be different for each association.

P3P and Privacy Statements

• Most commercial web sites provide a privacy statement.
  – Most are not worth the paper they are printed on
    • You probably view it on your screen
    • Many actually are illustrative, as they are written to say that “we can’t control what happens to your data – so don’t blame us”.
    • Who reads them anyway.
    • How are they enforced
      – Some are certified by outside endorsers
P3P and Privacy Statements

- P3P was a protocol that was designed to allow users to specify their preferences, and to have these preferences negotiated by a browser when connecting to a site.
  - But it still doesn’t provide any enforcement that the site follows its stated policy.
  - It doesn’t ensure that the data held by the site is not compromised by outsiders.
  - You may still see support in some browsers, but it saw only brief adoption by web sites.

Protecting Data in Place

- Many compromises of privacy are due to security compromised on the machines holding private data.
  - Your personal computer or PDAs
  - Due to malware or physical device theft
- Countermeasures
  - For device theft, encryption is helpful
  - For malware, all the techniques for defending against malicious code are important.
  - Live malware has the same access to data as you do when running processes, so encryption might not be sufficient.
Forensics

• Forensics is the methods used to reconstruct data and/or collect and document evidence of actions that have occurred in the past.
• In computers, this usually involves:
  – Reconstruction of messages from logs, traces and recordings
  – Attribution of actions through log and trace analysis and other evidence such as identifiers that may remain.
  – Reconstruction of data that may have been deleted, erased, or destroyed.

Forensics

• Tools are available to recover supposedly deleted data from disks.
  – Similar tools can reconstruct network sessions.
  – Old computers must be disposed of properly to protect any data that was previously stored.
    ▪ Many levels of destruction
  – Tools like whole disk encryption are useful if applied properly and if the keys are suitably destroyed.
Privacy – Retention Policies

• PII (personally identifiable information)
  – Is like toxic waste
  – Don’t keep it if you can avoid it

• Regulations
  – Vary by Jurisdiction
  – But if you keep it, it is “discoverable”

The future of Privacy

• Who’s data is it anyway
  – Should PII carry tags that limit its use.
  – How do we enforce that such tagged policies are actually followed.
Current event – How does this relate to our discussion

US dismantles ‘massive’ cyber crime syndicate
BBC News 10 November 2011

Cyber criminals who are alleged to have made $14m (£9m) from advertising fraud have been arrested in Estonia.
The FBI alleged that the gang infected more than four million computers in 100 countries with code that redirected users to online ads.
The six arrested are Estonian nationals while the seventh member of the gang, a Russian, remains at large.
Security firms hailed the arrests as the “biggest cyber criminal take down in history”.

About 500,000 of the affected computers were in the US and many of the millions inadvertently enrolled in the fraud scheme were in
government offices, schools, and corporates.
Aiding the investigation into the scale of the scheme was US space agency Nasa which first discovered the malicious software on 130
of its computers. Security firm Trend Micro also provided key intelligence during the long investigation.

The FBI claimed that the “massive and sophisticated internet fraud scheme” revolved around servers set up to surreptitiously reroute
traffic to websites where the gang would get a cut of the advertising revenue.
Victims would start out trying to visit sites such as Amazon, Netflix and ESPN but instead end up on sites displaying adverts put
together by the gang, said the FBI in a statement.

“These defendants gave new meaning to the term, ‘false advertising’, said Manhattan US attorney Preet Bharara in a statement
detailing the take down which the FBI dubbed “Operation Ghost Click”.
Describing the gang as “cyber bandits”, Mr Bharara alleged they collected “millions in undeserved commissions for all the hijacked
computer clicks and internet ads they fraudulently engineered”.

FBI documents detail the scheme the gang is accused of running which employed rogue copies of the net’s address books to re-direct
people to the fraudulent sites.
The FBI has produced a software tool that people can download and run to see if they had been hit by the gang and were being re-
directed. The gang reportedly tricked people into installing the malicious code that hijacked their PC by disguising it as a codec
required to watch adult movies.

More than 100 computers were seized in raids conducted at the same time as the arrests. The rogue address books have now been
switched for servers that direct people to where they wanted to go.
Domestic ISPs are also being told about the people that were infected to give them a chance to clean up.
The defendants have been charged with five counts of wire fraud and computer intrusion crimes. If found guilty they face heavy jail
sentence.

Mid-Term Discussion

Cryptography

For each pair of methods for encryption or key management, list the major differences in their characteristics or strength, indicating for each difference, which of the two methods is stronger or more secure for the selected characteristic and why. Examples of characteristics that are different for some of the pairings include strength for confidentiality, strength for integrity, size of the key-space, support for non-repudiation, dependence on a third party, performance, and whether authentication is provided. Only some of the characteristics will be different for many of the pairings.

1. DES in CBC mode vs. DES in OFB mode.
2. RSA with a 512 bit key vs. AES with a 128 bit key.
3. Kerberos vs. Diffie Hellman Key exchange
4. One time pad vs. AES with a 128 bit key.
5. RSA as a block cipher with a 2056 bit key vs. DES in ECB mode.
6. Kerberos vs. Public Key Based certification infrastructure (PKI).
Mid-Term Discussion

Malicious Code

1. How are each of the three primary classes of malicious code propagated? In answering this, explain what steps and conditions that are necessary for the malicious code to start executing on a new computer. (15 points)

2. How far is the impact of an infection by malicious code of each type likely to propagate? What affects this propagation and what steps can be taken to partially contain or limit the spread of the malicious code. Consider iterative infection in answering this question (i.e. once one system or part of a system is infected, will the malicious code spread further, and how can we reduce the spread). [please answer on back of page] (15 points)

Mid-Term Discussion

Design problem

The Hacker group Anonymous has recently threatened to mount attacks on the New York Stock exchange and other financial and other organizations in sympathy with the actions of the Occupy Wall Street movement. You have been hired to stop them. Well... more precisely, you have been hired for a longer term job of redesigning the infrastructure supporting the markets (the NY Stock Exchange, NASDAQ, commodity exchanges, etc) to make these systems more resilient and secure. For now you are only going to focus on a single stock exchange, and within the next 40 minutes (roughly) you will answer questions about the problem, and your preliminary design.
Mid-Term Discussion

Design problem

1. Discuss in general terms requirements of the system and how they impact, or are impacted by security considerations. More specifically, i) describe the kinds of data in the system, and the implications for unauthorized disclosure of each kind of data, as well as for unauthorized modification of such data, and disruption of availability of such data; ii) describe the services provided by the system and the security implications for unavailability (e.g. denial of service) of such services, or delays in providing such services. (10 points)

2. Discuss in general terms the classes of users of the system, the data and services that each must access, and from where they need to be able to access the data and services. Discuss in general terms also the classes of adversaries that might want to attack the system, and the access that they must have (yes, this seems strange – the access they must have – keep in mind that attackers may be indistinguishable from some classes of legitimate users). For these adversaries, discuss their different motivations for attack, and what it would mean for their attacks to be successful. (10 points).

3. In the design of your system, how will you structure the protection domains – e.g. what will be the distinct regions of your system, and which data will be stored and which services provided from each of these regions (5 points).

4. For each class of authorized user, discuss techniques that should be used for authentication of the users. Be sure to consider the cost of each method you use, the “factor” that is checked. How will data be protected as it crosses the network, and how is this form of protection tied to (or not tied to) the authentication methods that you have chosen. (10 points)

Current event – How does this relate to our discussion

U.S. water utility reportedly hacked last week, expert says

CNET - by Elinor Mills November 17, 2011 7:40 PM PST

• Intruders compromised a water utility network last week and destroyed a pump, according to a state government report cited by a critical infrastructure security expert today.

• It appears that hackers breached the network of a company that makes SCADA (supervisory control and data acquisition) and stole customer usernames and passwords, said Joe Weiss, managing partner of Applied Control Solutions. “There was damage—the SCADA system was powered on and off, burning out a water pump,” he wrote in a brief blog post.

• The report did not identify the water utility attacked or the SCADA software vendor compromised, Weiss said in an interview with CNET. He declined to say where the utility is based because the report, released by a state terrorism information center, is marked “For Official Use Only.” However, a Department of Homeland Security representative indicated the facility was located in Springfield, Ill.
Announcements

- Paper due today
  - Accepted without penalty until Monday
- Final Exam on Monday December 12\textsuperscript{th}
  - 11AM-1PM in ZHS-159
  - Review during this lecture
- Course Evaluations at Break
Trends in Power Systems

- Evolution of the power distribution network
  - Local power systems
  - Interconnected
  - More centralized control
  - Automated reaction to events
  - Reaching into the neighborhoods
  - Encompassing the home

Federation in Power Systems

- Power systems span large geographic areas and multiple organizations.
  - Such systems are naturally federated
- Avoiding cascading blackouts requires increasingly faster response in distant regions.
  - Such response is dependent on network communication.
- Regulatory, oversight, and “operator” organizations exert control over what once were local management issues.
  - Staged power alerts and rolling blackouts
- Even more players as the network extends to the home.
  - Customers
  - Information Providers
What’s Different

- System requirements preclude certain defenses
  - Smart means harder to analyze
  - Infrastructure means harder to isolate
    - Access is part of service definition
  - Physical means domain-specific attack modes

Some Characteristics

- Federated model of the system
  - Components in field or at customers premises, etc.
  - Components managed by different entities
  - Means we need federated policy models
    - Not well understood
- Physical Attack Modes
  - Hidden control channels based on physical behavior
  - Domain specific knowledge needed to defend system.
  - Physical properties jump the “air-gap”
Understanding Smart Grid Security

- As a security problem, we need to model Smart Grid robustness expecting non statistical faults that cross the cyber-physical boundary.
  - Traditional security limits information and control flow within the cyber realm.
  - For the Smart Grid we must understand physical pathways.
    - We need to understand the coupled system of systems impact of faults within a single domain.
    - E.g. effects of tripping a breaker in one part of a system can effect other parts, independent of the cyber communication between them.
    - These causal physical relationships should be modeled as information and control channels.
  - Procedures and processes in the physical realm convert information channels into control channels.

Understanding Systemic Response

- The interesting questions about smart grid security relate to the response of the System of Systems.
  - We must identify the relevant domains.
    - Some domains are cyber, and each organization with ownership or control (including customers) represents one or more cyber domains.
    - Some domains are physical, and each separately controlled device or physical system might represent a domain.
    - We need to group similar domains, such as customer devices, to simplify our modeling
      - We are exploring how to do this
        - Perhaps drawing on DETER developed models for malware propagation
• Modeling can help us understand how threats propagate across domains.
  – There are several classes of propagation to be considered, based on the domains that are crossed.
    ▪ Cyber-Cyber
    ▪ Cyber-Physical
    ▪ Physical-Cyber
    ▪ Physical-Physical
    ▪ And transitive combinations.

Cyber-Threats

• Cyber-Cyber threats (traditional cyber security)
  – Easily scaled (scripts and programs)
  – Propagate freely in undefended domains
  – We understand basic defenses (best practices)

• Cyber-Physical threats (physical impact of cyber activity)
  – Implemented through PLC
    ▪ or by PHC (social engineering)
    ▪ or less direct means (computing power consumption)
  – Physical impact from programmed action
  – But which domain is affected (containment)
Physical-Threats

- Physical-Cyber threats (impact to computing)
  - For example, causing loss of power to or destruction of computing equipment.
    - A physical action impacts the computation or communication activities in a system.
  - Containment through redundancy or reconfiguration
- Physical-Physical threats (propagation of impact)
  - Traditionally how major blackouts occur
    - Cascading failure across domains
    - System follows physics, and effects propagate.
  - Containment is often unidirectional
    - A breaker keeps threat from propagating upward
    - But it explicitly imposes the impact downward

Transitive Threats (example)

- Dependence on unsecure web sites as control channels.
  - End customer smart devices (including hybrid vehicles) will make decisions based on power pricing data.
    - Or worse – based on an iPhone app
  - What if the this hidden control channel is not secure
    - Such as a third party web site or
    - Smart Phone viruses
  - An attack such control channels could, for example, set pricing data arbitrarily high or low, increase or decrease demand, or directly controlling end devices.
    - Effectively cycling large number of end devices almost simultaneously.
Transitive Threats

• More interesting real-world threats combine the binary threats for greater impact.
  – Cyber-Physical-Physical (CPP)
    • Multiple Nissan Leaf’s controlled from hacked smartphones.
  – Cyber-Physical-Cyber (CPC)
    • Controlling device on HAN that causes meter to generate alerts creating DOS on AMI network.
  – Physical-Cyber-Physical (PCP)
    • Leverage Cyber response, e.g. 3 Sensor Threshold for fire suppression system.

What we have shown

• We have demonstrated a way of classifying threat propagation to highlight threat propagation in Smart Grids
  – This is useful for design red-teams
  – This provides structure for modeling and simulation of threat propagation and response in such systems.
  – It helps us understand how to mitigate specific threats.
• Modeling smart grids requires understanding of the cyber and physical domains within the system of systems.
  – One must look at the transitive propagation of threats across those domains.
  – We need better ways to group similar domains to simplify modeling.
Traditional Security and the Smart Grid

- **Availability** used to be the critical service for power control networks.
  - The control network for interconnects was managed separately.
    - Sole purpose was to exchange commands and information needed to keep the system functional.
  - Integrity and confidentiality was provided through limited physical access.

- The control network is increasingly dependent on other networks.
  - The phone network today is implemented on digital networks.
  - The network has connections to the open Internet.
    - Data for billing & monitoring made available to others.

- **Network Data Integrity** can be maintained through encryption, but **availability** requires dedicated and/or redundant links.
  - **Information Integrity** is affected by the number and nature of the parties involved
  - It becomes an issue of trust and confidence.
Traditional Security and the Smart Grid

- As the smart grid moves into the home, confidentiality becomes important.
  - Much inferred about customers by power consumption profile.
  - Economic value to consumption data
- Information integrity becomes critical
  - HAN components bridge the two networks.
  - Appliances managed based on information from the Internet.
    - Have an effect on power grid.

Modeling Security in the Smart Grid

- We need an accurate model for security in the smart grid in order to understand its vulnerabilities.
  - A model allows us to simulate and emulate
  - A model allows us to identify weaknesses.
- Today’s models are not accurate.
  - Separate models for cyber and physical.
  - Each model addresses only those threats we have already seen.
Understanding Smart Grid Security

- As a security problem, we need to model Smart Grid security using an adversarial model.
  - Traditional security limits information and control flow within the cyber realm.
  - For the Smart Grid we must model physical pathways.
    - E.g. effects of tripping a breaker in one part of a system will have effects in another part, independent of the cyber communication between them.
    - These causal relationships should be modeled as information and control channels.
  - Procedures and processes in the physical realm convert information channels into control channels.

Securing the Smart Grid

- Domain and security experts should identify all classes of sensors, actuators, and potential measurement points in the system.
  - Decide how each is associated with control and information channels.
  - Identify the other parties on the channel.
  - Identify security services needed for the channel.
    - Confidentiality
    - Integrity
    - Availability / Performance Isolation
    - Access Control
    - Anomaly Detection / Intrusion Detection
    - Trust Management
Some Examples

- Automated response to detected voltage changes.
  - We should model an associated control channel from those entities capable of causing voltage fluctuations.
- Home automation controller.
  - This creates a control channel from the customer.
    - The affect of such change in load must be considered and mitigated.
    - Control channels to the customers computer now become part of the smart grid, even if the intent was to avoid dependence on the Internet.

How We Might Get it Wrong

- Dependence on unsecure web sites as control channels.
  - End customer smart devices (including hybrid vehicles) will make decisions based on power pricing data.
  - What if the pricing channel is not secure
    - Such as a third party web site.
  - An attack on the third party web site could set pricing data arbitrarily high or low.
    - Effectively cycling large number of end devices almost simultaneously.
  - California's recent power crisis demonstrated that perceived pricing fluctuations form control channels.
    - Well the prices were real, though not the basis for them.
    - This led to rolling blackouts.
Securing The Smart Grid

- We must recognize that complete physical separation is no longer possible
  - Because the Smart Grid extends into physically unsecure areas.
- Thus we must provide isolation through technical means.
  - We must define protection domains
  - Improve support in the hardware, OS, and middleware to achieve isolation.
  - Design the system to identify policy on control flows so that Smart Grid components enforce it.

Cyber Isolation for the Smart Grid

- Both critical and non-critical functions may share physical infrastructure.
  - Control functions vs. billing functions.
  - The systems and network must, at their lowest levels, provide the separation needed by the critical functions.
    - To prevent compromise or denial of service by the less critical functions
    - To contain the effect of a compromise of a critical function from spreading to other parts of the system.
A Note on Simulation

- Simulations commonly used in power grid to evaluate scenario response.
  - Often using proprietary modeling tools.
- Cyber attack simulation and emulation capabilities available.
  - Testbeds like DETER (at USC-ISI) can be used to identify response to cyber attacks.
- These need to be combined
  - Support for federated experiments in DETER could allow separate emulation and simulation of multiple cyber and physical components.

Summary – C-P Security

- The Smart Grid extends to homes & businesses
  - New security implications for such connections.
  - Hidden control channels.
- Critical and non-critical functions will not be separate
  - Availability is critical
  - Performance isolation needed for critical communication.
- The federated nature of the smart grid demands:
  - Federated architectures to secure it.
  - Federated systems to model it
- Existing security for the power grid does not address the implications of the new architecture.
Defining The Cloud

- The cloud is many things to many people
  - Software as a service and hosted applications
  - Processing as a utility
  - Storage as a utility
  - Remotely hosted servers
  - Anything beyond the network card
- Clouds are hosted in different ways
  - Private Clouds
  - Public Clouds
  - Hosted Private Clouds
  - Hybrid Clouds
  - Clouds for federated enterprises
Risks of Cloud Computing

- Reliability
  - Must ensure provider’s ability to meet demand and to run reliably
- Confidentiality and Integrity
  - Service provider must have their own mechanisms in place to protect data.
  - The physical machines are not under your control.
- Back channel into own systems
  - Hybrid clouds provide a channel into one’s own enterprise
- Less control over software stack
  - Software on cloud may not be under your enterprise control
- Harder to enforce policy
  - Once data leaves your hands

Defining Policy

- Characterize Risk
  - What are the consequences of failure for different functions
- Characterize Data
  - What are the consequences of integrity and confidentiality breaches
- Mitigate Risks
  - Can the problem be recast so that some data is less critical.
    - Redundancy
    - De-identification
  - Control data migration within the cloud
### Controlling Migration

- Characterize Node Capabilities
  - Security Characteristics
    - Accreditation of the software for managing nodes and data
  - Legal and Geographic Characteristics
    - Includes data on managing organizations and contractors
  - Need language to characterize
  - Need endorsers to certify

- Define Migration Policies
  - Who is authorized to handle data
  - Any geographic constraints
  - Necessary accreditation for servers and software
    - Each node that accepts data must be capable for enforcing policy before data can be redistributed.
  - Languages needed to describe

### Enforcing Constraints

- With accredited participants
  - Tag data and service requests with constraints
  - Each component must apply constraints when selecting partners
    - Sort of inverting the typical access control model

- When not all participants are accredited
  - Callbacks for tracking compliance
  - Trusted computing to create safe containers within unaccredited systems.
Cloud Security Summary

• Great potential for cloud computing
  – Economies of scale for managing servers
  – Computation and storage can be distributed along lines of a virtual enterprise.
  – Ability to pay for normal capacity, with short term capacity purchases to handle peak needs.

• What needs to be addressed
  – Forces better assessment of security requirements for process and data.
  – Accreditation of providers and systems is a must.
  – Our models of the above must support automated resolution of the two.
Common Suggested Topics

- E-commerce, e-payment
- Security in routing
- IP Traceback
- Mobile Computing/Devices
- Bot-nets
- Middleware
- Honeypots
- System Assurance

Ecommerce Security

- Security of Trading Platform
  – Protecting the user
  – Protecting the company
  – The Untrusted Merchant
- Auctions
  – Fairness
- Payment Security
**Ecommerce: Trading Platform**

- Traditional platform security
  - Move critical data off server
- Use third parties to avoid need to collect critical customer data.

**Ecommerce: Fraud**

- Often external to system
  - Use of stolen credit cards
  - Drop locations for shipping
- Advertising fraud
  - Pay-per impression/click/action
  - Commission hijacking
Ecommerce: Auctions

- Typical real-world auction fraud techniques apply.
- Online issues
  - Denial of service
  - Visibility of proxy bids

Ecommerce: Payment

- Secure, reliable, flexible, scalable, efficient, and unobtrusive payment methods are required as a basic service of the Internet and must be integrated with existing and evolving applications.
Reliability

- Commerce will depend on the availability of the billing infrastructure.
- The infrastructure may be a target of attack for vandals.
- The infrastructure must be highly available and should not present a single point of failure.

Scalability

- The payment infrastructure should support multiple independent accounting servers and should avoid central bottlenecks.
- Users of different accounting servers must be able to transact business with one another and the funds must be automatically cleared between servers.
Efficiency

- Frequent payments for small amounts must be supported (micropayments).
- Performance must be acceptable, even when multiple payments are required.
- Merchants and payment servers must be able to handle the load.
- Per transaction cost must also allow small payment amounts.

Unobtrusiveness

- Users should not be constantly interrupted to provide payment information.
- However, users do want to control when, to whom, and how much is paid.
- Users must be able to monitor their spending.
Integration

- Payment systems must be tied to the existing financial infrastructure.
- Applications must be modified to use the payment infrastructure.
- Payments should be supported by common protocols that underlie applications.
- A common framework should support integration of multiple payment methods.

Multiple forms of payment

- Secure presentation
- Customer registration
- Credit-debit instruments
- Electronic currency
- Server scrip
- Direct transfer
- Collection agent
Secure presentation (and non-secure variant)

Uses traditional credit card numbers
  – As safe as the phone (cordless?)
  – Potentially huge customer base
  – Little need for infrastructure

Examples - products based on:
  – Secure Sockets Layer
  – SHTTP

Issues
  – No customer signature
  – Legitimacy of merchant
  – Real time authorization
  – Transaction cost

Customer registration

• Customers register and receive passwords, keys, or new account identifiers
  – Transactions clear through financial service provider who gateways to existing financial system (credit cards or checking accounts)
  – Protects external account information

• Examples: First Virtual, CyberCash, SET

• Issues:
  – Security of system specific credentials
  – Real time authorization
  – Transaction cost
Credit-debit instruments

Financial service provider maintains accounts for customers
- Authorized individuals spend from account.
- Payment instrument authorizes transfer.
- Modes: credit like credit card, debit like checks
- Requires new infrastructure

Examples:
- USC’s NetCheque
- FSTC Electronic Check Project

Issues
- Security of system specific credentials and instruments
- Aggregation and tie to financial system
- Durability of account information and of provider

Electronic currency

Users purchase currency from currency servers. Currency is presented to merchant who turns it in to currency server.
- Potential for anonymity
- Possible off line operation

Examples:
- Mondex
- DigiCash
- NetCash
- Various stored value cards

Issues
- Backing of the currency
- Level of anonymity
- Tamper resistance of hardware
- On-line vs. off-line
- Who’s at fault for counterfeiting
- Storage requirements
- Extensive matching capabilities required
Server scrip

- Payment instrument spendable with individual merchants.
  - Verification of scrip is a local issue
  - Requires a market and other forms of payment to enable purchase of merchant script.

- Examples:
  - Millicent
  - Payword

- Issues:
  - Aggregation of purchases improves performance
  - But must manage many kinds of currency

Direct transfer

- Customer initiates transfer of funds to account of merchant
  - May result in instrument sent externally

- Examples:
  - Most on-line bill payment mechanisms

- Issues
  - Matching of payment to customer or transaction
  - Account management similar to credit-debit model
Collection agent

- Merchant refers customer to third party who collects payment and provides receipt.
  - Receipt is presented to merchant who then provides the goods or services.
- Examples:
  - OpenMarket payment switch
- Issues
  - Third party implements the payment methods
  - Issues are the same as for methods supported

Some representative systems

Available today
- Secure Socket Layer
- CyberCash
- SET
- Open Market

Trials
- Mondex

Demonstrated, Research
- FSTC Electronic Check
- NetCheque
- NetCash
- NetBill

No longer with us
- First Virtual
- DigiCash
Secure socket layer (secure presentation)

- Merchant has certified public key
- Client submits form with credit card information to merchant encrypted
- Merchant obtains authorization for credit card in same manner as for phone order
- Availability: NetScape Commerce Server, IE, Apache, OpenMarket, Others, (Verifone)

First Virtual (customer registration)

- Customer establishes First Virtual account
  - Customer sends account ID to merchant
  - Merchant forwards to FV server
  - FV server verifies through e-mail to customer
    ▪ Customer can refuse payment to merchant
    ▪ If too frequent, customer loses account
- Issues:
  - Does not use encryption
    ▪ No changes to client software
    ▪ Minimal changes needed for merchant
    ▪ Known compromise scenario, but of limited use
  - Exposure limited by delaying payment to merchant (waived for vetted merchants)
- Availability: FV (now MAIL) no longer does payments, Customer base sent to CyberCash
CyberCash (customer registration)

- Customer registers credit card with CyberCash and selects signature key
  - Special software running on client encrypts and signs credit card number and transaction amount and sends to merchant.
  - Merchant forwards to CyberCash server which obtains authorization and responds to merchant
- Issues:
  - Credit card number not exposed to merchant
  - Payment clears through credit card system
  - Will adopt SET for credit card payment
  - CyberCoin for "micropayments"
- Availability: http://www.cybercash.com
  Core commercial product is different than described here; does credit card authorizations for merchants.

DigiCash (electronic currency)

- Software implementation of electronic currency providing unconditional anonymity
  - Special software on client implements electronic wallet to store and retrieve currency.
  - On-line detection of double spending
  - Post-fact tracking of double spending
- Availability: http://WWW.DigiCash.COM
  - In Chapter 11 reorganization (11/4/98)
Secure Electronic Transactions (SET)

- Customer obtains signature key from card issuer
  - Special software running on client encrypts and signs credit card number and transaction amount and sends to merchant
  - Merchant forwards to acquirer which processes transaction through credit card system and responds to merchant with authorization

- Advantages
  - Certification of customer and merchant
  - Credit card number not exposed to merchant

- Disadvantages
  - Slow encryption
  - In practice, many are dropping the customer registration requirement

- Availability: Part of product offerings by others

Open Market (collection agent)

Provides multi-mechanism collection services for web browsers.
- Payment is made to Open Market payment switch.
- Switch authorizes delivery of goods.
- Added value provided to customer through “smart statement”.

Availability: http://www.openmarket.com
Mondex (electronic currency)

- Provides smart-card based electronic currency for point of sale and card to card transactions
  - Currency can be accepted off-line
  - Uses a tamper resistant smart card
  - Card signs transactions, so no anonymity
  - Card-to-card transactions using “wallet”
  - Smartcard reader needed to use on network
- Availability: several pilots underway, not available yet for Internet transactions

Electronic Check (Credit-debit)

- Electronic check provides credit-debit payment instruments that can be sent across the Internet, but which clear through existing banking networks (e.g., ACH)
  - Instrument authenticated using public key cryptography and digital signatures
  - PCMCIA “electronic checkbook” protects keys
  - Trial expected in 1997.
USC/ISI NetCheque® (credit-debit)

• Implements on-line “checking-account” against which payments are authorized.
  – No prior arrangement between customer and merchant.
  – A check authorizes the payee to transfer funds from the payor’s account.
  – Multiple currencies per account.
  – Payments clear through multiple payment servers.

• Availability as research prototype: http://www.netcheque.org

Flow of NetCheque Payment Instrument
NetCheque representation

- Internal representation is opaque
- Important fields:
  - Account and accounting server: Amount, payee, expires
  - Customer and merchant info: Signatures and endorsements
- MIME encoded for use by applications
- Applications display checks according to their own requirements.
  - Display check makes it look like check
  - Statement displays one line per check
- Statement API returns entire check with endorsement
  - Allows easy import of information from check into users' financial applications.

NetCheque Payment Instrument

--NetCheque(SM) V1.0
Content-Type: APPLICATION/X-NETCHEQUE
Content-Transfer-Encoding: BASE64
Content-Description: Pay 10.00 NCU to marketplace@NETCHEQUE.ISI.EDU

AAAAAQAAAA5OZXRDaGVxuWVFyjEn8AAAAAAITT0ZUV0FRV9WMS4wAAAAAQED
NTE4AzI2N2GCAQcwgDGDoAMCAQWxExsXTKUQ0hFUVFLk1TSS5FRFWIKTAn
oAMCAQchIDAEwGw1OZXRDaGVxuWUbEW51dGNoZEFlZ5pc2kuZWR1o4G7MIC4
oAMCAQchAwIBAaKBgqSpEILdnGj8taheciceub3DK+0qYb+ayEtyZudV5yC
RVFVRS5Ju0kuRURVAAABQAAAAAAIBM05DQExATEAAAAEAJU5AAAC4w4MDAw
M2Q4NzkJODAyMTk0Nzk4AAAACQIxxNUNsaWZmb3JkX05lW1hbgAAAAEBMQEx
AAAAhIhcmtdHhBeYWN1Q25FVENIRVFR5JU0kuRURVAAAAAA==

--NetCheque(SM) V1.0--
NetCheque security

- Check has plaintext part and signature
- Endorsements are separately signed and linked to a particular check
- Signature component is modular
  - Current implementation is Kerberos proxy
    - Signature verifiable by customer's bank
  - Can accommodate RSA or DSS signatures

Clearing funds through multiple servers

AS: Accounting Server  U: User  S: Service Provider
USC/ISI’s NetCash

- Users purchase currency from currency server using NetCheque - deposits to currency server’s account back the currency
- Supports weakly anonymous payment
  - Cash can be exchanged for new cash anonymously
  - Customer chooses the currency server
- Multiple currency servers, the NetCheque system is used to clear cross-server payments

Offloading the risks

- Limiting exposure to risk
  - Credit vs. debit model for accounts
  - Deferring payment to merchants
- Shifting risk to other parties
  - Agreements shifting risk to merchant
  - Regulations protecting the consumer
  - Insurance - perhaps as higher transaction fees
Technical solutions

- Protecting payment credentials
  - Token cards
  - Smart cards

- On-line authorization
  - Detects double spending
  - Checks for sufficient funds
  - Enables checks for spending patterns

- Tagging documents

Common Suggested Topics

- E-commerce, e-payment
- Security in routing
- IP Traceback
- Mobile Computing/Devices
- Bot-nets
- Middleware
- Honeypots
- System Assurance
Security in Routing

- Routing is a peer to peer system
- Topology is dynamic
  - (otherwise we would not need routing protocols)
- Routing is Transitive
- Security through Signing updates
- Policy is the hard part
- Systems SIDR, SBGP, etc

IP Traceback

- IP Addresses are spoofable
  - Difficulty depends on next level protocol
- How can we mitigate this effect
  - Ingress filtering
  - IP Traceback techniques
  - Only effects certain address spoofing, not relays
Mobile Devices

- Characteristics
  - Resource limited
  - Intermittent connectivity
    - Offline operation

Battling Bot-nets

- Detection
  - Finding the control panel
  - Learning what they do

- Response
  - Isolation/quarantine
Security For Middleware

- DCOM, CORBA, RPC, etc
- Issues
  - Authentication in underlying protocols
  - Confidentiality and integrity
  - Delegation
  - Management

Honey

- Honeypots
  - Looks like interesting system
- Honeynets
  - Dynamic Virtualization
- Honeytokens
  - Setting a trap
Outside Looking In

- How do we get out from an infected system.
  - Boot off CD
  - Mount drive on analyzer, etc.

REVIEW
Review - Topics

- Cryptography
- Key Management
- Identity Management (and Authentication)
- Policy (and Authorization)
- Attacks
  - Classic
  - The human element
- Defenses
  - Firewalls, Intrusion Detection and Response, Encryption, Tunnels, Defenses to Malware
- Architectures and Trusted Computing
- Cyber-Physical and Cloud Computing

Glossary of Attacks

This is not a complete list
- Availability
  - Denial of Service (DoS AND DDoS)
    - Over consumption of resources
      - Network, ports, etc
      - Take down name servers, other critical components
    - Exploits to crash system
    - Cache poisoning
Glossary of Attacks

This is not a complete list

- **Confidentiality**
  - Eavesdropping
  - Key Cracking
  - Exploiting Key Mismanagement
  - Impersonation
    - Exploiting protocol weakness
    - Discovered passwords
    - Social Engineering
  - Exploiting mis-configurations

- **Integrity**
  - Breaking Hash Algorithms
  - Exploiting Key Mismanagement
  - Impersonation
    - Exploiting protocol weakness
    - Discovered passwords
    - Social Engineering
  - Exploiting mis-configurations
  - Cache Poisoning
Glossary of Attacks

This is not a complete list

- **Miscellaneous**
  - Spam
  - Phishing
  - Malware attacks
    - Spyware
    - Viruses
    - Worms
    - Trojan Horse
  - Man in the middle
  - SQL Injection
  - Cross Site Scripting

Hypothetical Case Studies

- **Past exams**
  - Electronic voting (Fall 2004)
  - Medical records (Fall 2003)
  - Intrusion Detection and Response (Fall 2005)
  - Security for the DMV (Fall 2008)
Electronic Voting

You have been asked to design a system to support the collection and counting of votes for the next election. In particular, you have been asked to design a system that will accurately tabulate votes entered by voters at polling places throughout the state and to transmit those votes to the county clerk of each county where the totals will be tabulated.

(a) Threats. What are the threats in such a system? What can go wrong?
(b) Requirements. What are the requirements for authentication, authorization, assurance, audit, and privacy? Explain who and what must be authenticated, what authorizations are required, what assurance is needed for the software, and what kind of records must be maintained (as well as what kinds of records should not be maintained).
(c) Considering the requirements listed above, and how they relate to the assurance problem, i.e. how can steps taken for authentication, authorization and audit be used to ensure that the software has not been modified to improperly record or transmit votes?
(d) What technologies proposed for digital rights management be used to provide stronger assurance that the system’s integrity has not been compromised. What is similar about the two problems, and how would such technologies be applied to the voting problem.

Medical Records

• You have been hired as a consultant to advise on the design of a security mechanism that will be used to protect patient data in a new medical records system. This system will manage and support the transmission of patient records, including very large images files for X-rays, MRI, CAT-scans and other procedures. The system must provide appropriate levels of protection to meet HIPAA privacy regulations, and it must allow the access to records needed by physicians and specialists to which patients are referred.

(a) Describe appropriate requirements for confidentiality, integrity, accountability, and reliability/availability in such a system.

(b) In what part(s) of the system (e.g., where in the protocol stack would you include support for each of the requirements identified in (a)? Why would you place mechanisms where you suggested; what were the issues you considered?

(c) What security mechanisms and approaches to implement those mechanisms would you use to meet the requirements in (a) as implemented in the parts of the system you identified in (b)?
Intrusion Detection and Response

- You have been asked to design a system that will provide effective response to new attacks. The system you design will have two components, an intrusion detection component designed to detect attacks, and a dynamic policy enforcement mechanisms that will dynamically adjust policies based on what is learned about attacks from the intrusion detection component. Your system is supposed to provide an effective defense against viruses, worms, as well as attacker targeted penetration attempts to the systems in your organization.
Security for the DMV - 2008

- (30 points) Design Question – You have been hired by the state of California to improve the security of the computer systems at the department of motor vehicles. Much if the information in the system is sensitive and it will be important to limit access to this data, not just by the general public, but also to maintain strict accountability for access by DMV and law enforcement employees themselves. Given the large number of terminals throughout the state (including those in patrol cars) from which such data is accessible, you have been asked to consider approaches that will prevent data from being downloaded and then transferred to other computer systems outside of the states network.

- a) Describe the data to be protected in such a system and suggest the policy that should be applied for each class of data i.e. who can view it and who can modify it. (10 points)

- b) Suggest techniques that can be applied to prevent misuse of the data by insiders, i.e. those that might have authorization to access the data according to the policies implemented by the computer systems, but who might not have legitimate need to access the data. (5 points)

- c) Suggest techniques that could prevent the data from being accessed by malicious code that might end up installed on, and having infected, terminals in the system. (10 points)

- d) Suggest techniques that would prevent data from being downloaded from the system and then transferred to other external systems over which the access controls to the data might not be enforced. (10 points)

Copyright © 1995-2009 Clifford Neuman - UNIVERSITY OF SOUTHERN CALIFORNIA - INFORMATION SCIENCES INSTITUTE

CURRENT EVENTS

Copyright © 1995-2009 Clifford Neuman - UNIVERSITY OF SOUTHERN CALIFORNIA - INFORMATION SCIENCES INSTITUTE
Current event – How does this relate to our discussion
Can hackers really set fire to your printer? HP says no way
Los Angeles Times – November 29th - Deborah Netburn

Talk about a hot story: On Tuesday an article on MSNBC.com suggested the possibility of hackers from across the world hacking into a printer and giving it instructions so crazed that the printer would overheat and catch fire. Kapow!

The piece was based on interviews with Salvatore Stolfo, of the Computer Science Department of Columbia University’s School of Engineering and Applied Science and his team of researchers who had spent months investigating the hackability of Hewlett Packard printers with the help of various research and security grants. “The research on this is crystal clear,” Stolfo told MSNBC. “The impact of this is very large. These devices are completely open and available to be exploited.”

Stolfo and his team illuminated many ways that hackers could exploit the printers they hacked — using them to steal personal information, or attack otherwise secure networks, for example. But the piece of the story that suggested flaming printers is the part that quickly caught fire on the Internet.

By the middle of the day, however, HP had issued a lengthy refutation that its printers can catch fire. “Today there has been sensational and inaccurate reporting regarding a potential security vulnerability with some HP LaserJet printers,” the company said in a news release. “Speculation regarding potential for devices to catch fire due to a firmware change is false.”

The company concedes that there is a potential security vulnerability with some of its LaserJet printers, but says no customer has ever reported unauthorized access. As for the fire potential, the company had this to say: “HP LaserJet printers have a hardware element called a ‘thermal breaker’ that is designed to prevent the fuser from overheating causing a fire. It cannot be overcome by a firmware change or this proposed vulnerability.”