CSci530: Security Systems
Lecture 1 – August 30, 2013
The Security Problem

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Administration

- Class home page
  http://ccss.usc.edu/530
  - Preliminary Syllabus
  - Assigned Readings
  - Lecture notes
  - Assignments
Who gets in

• If you wish to enroll and do not have D clearance yet, send an email to CSci530@usc.edu with:
  – Your name
  – If you meet the prerequisites
  – A phone number
  – Request to received D clearance

• I will assess and approve if appropriate.
Structure of lecture

- Classes from 9:00 AM – 11:50 AM
  - 10 minute break halfway through
  - Final 5 minutes for discussion of current events in security.
Administration

• Lab Component (see http://ccss.usc.edu/530L)
  – 1 of the 4 units
  – Instructor is David Morgan
  – Instruction 4:30-5:20 Fridays in OHE 122
    ▪ WebCast via DEN
    ▪ Today’s Lab instruction is only a 30 minute introduction
  – Hands on sections, choose from several sessions
    ▪ Provides an opportunity to do hands on work in OHE 406 lab.
    ▪ Some labs will be done remotely using DETER
    ▪ Must sign up for your preference of session.
    ▪ Details will be provided this afternoon.
Administration

- Class e-mail: csci530@usc.edu
- Instructor
  - Dr. Clifford Neuman
  - Office hours Friday 12:55-1:55 SAL 212
    (But today from 11:50AM to 12:30PM)
  - Contact info on class web page
- TA
  - Bailan Li
  - Hours and contact information will be posted
- Grader
  - To Be Determined
  - Hours and contact information will be posted
Administration

• Grading Base Grade
  – Reading reports: 5%, 5%, 5%
  – Exams: 25%, 30%
  – Research paper 30%

• Supplemental grade (can raise or lower base):
  – Lab exercises Pass(hi,lo)/Fail (adj 15%)
  – Class participation
    • up to 10% bonus
Blackboard

- Using the DEN Blackboard system
  - Read announcement http://mapp.usc.edu/
    - You must accept the terms of service
  - Follow the instructions to obtain access to the Blackboard website.
  - Contact webclass@usc.edu if you have difficulty gaining access to the system.
Class Participation

- Class participation is important.
  - Ask and answering questions in class.
  - Ask, answer, participate on-line
- Bonus for class participation
  - If I don’t remember you from class, I look in the web discussion forum to check participation.
    - Did you ask good questions.
    - Did you provide good answers.
    - Did you make good points in discussions.
Academic Integrity

• I take Academic Integrity Seriously
  – Every year I have too many cases of cheating
  – Last year I assigned multiple F’s for the class
  – On occasion, students have been dismissed from program

• What is and is not OK
  – I encourage you to work with others to learn the material
  – Do not to turn in the work of others
  – Do not give others your work to use as their own
  – Do not plagiarize from others (published or not)
  – Do not try to deceive the instructors

• See section on web site and assignments
  – More guidelines on academic integrity
  – Links to university resources
  – Don’t just assume you know what is acceptable.
The Three Aspects of Security

- Confidentiality
  - Keep data out of the wrong hand
- Integrity
  - Keep data from being modified
- Availability
  - Keep the system running and reachable
Policy v. Mechanism

• Security policy defines what is and is not allowed
  – What confidentiality, integrity, and availability mean

• Security mechanism is a method or tool for enforcing security policy
  – Prevention
  – Detection
  – Reaction
System Security Terminology

• A **vulnerability** is a weakness in the system that might be exploited to cause loss or harm.

• A **threat** is a potential violation of security and includes a capability to exploit a vulnerability.

• An **attack** is the actual attempt to violate security. It is the manifestation of the threat
  - Interception
  - Modification
  - Disruption
Orthogonal Aspects

- Policy
  - Deciding what the first three mean
- Mechanism
  - Implementing the policy
Important Considerations

• Risk analysis and Risk Management
  – How important to enforce a policy.
  – Legislation may play a role.
• The Role of Trust
  – Assumptions are necessary
• Human factors
  – The weakest link
In The Shoes of an Attacker

• Motivation
  – Bragging Rights
  – Revenge / to inflict damage
  – Terrorism and Extortion
  – Financial / Criminal enterprises

• Risk to the attacker
  – Can play a defensive role.
What is security

• System, Network, Data
  – What do we want to protect
  – From what perspective
• How to evaluate
  – Balance cost to protect against cost of compromise
  – Balance costs to compromise with risk and benefit to attacker.
• Security vs. Risk Management
  – Prevent successful attacks vs. mitigate the consequences.
• It’s not all technical
Security and Society

• Does society set incentives for security.
  – OK for criminal aspects of security.
  – Not good in assessing responsibility for allowing attacks.
  – Privacy rules are a mess.
  – Incentives do not capture gray area
    ▪ Spam and spyware
    ▪ Tragedy of the commons
Why we aren’t secure

• Buggy code
• Protocols design failures
• Weak crypto
• Social engineering
• Insider threats
• Poor configuration
• Incorrect policy specification
• Stolen keys or identities
• Denial of service
What do we want from security

• Confidentiality
  – Prevent unauthorized disclosure
• Integrity
  – Authenticity of document
  – That it hasn’t changed
• Availability
  – That the system continues to operate
  – That the system and data is reachable and readable.
• Enforcement of policies
  – Privacy
  – Accountability and audit
  – Payment
The role of policy in security architecture

Policy – Defines what is allowed and how the system and security mechanisms should act.

Enforced By

Mechanism – Provides protection interprets/evaluates (firewalls, ID, access control, confidentiality, integrity)

Implemented as:

Software: which must be implemented correctly and according to sound software engineering principles.
## Security Mechanisms

- Encryption
- Checksums
- Key management
- Authentication
- Authorization
- Accounting
- Firewalls
- Virtual Private Nets
- Intrusion detection
- Intrusion response
- Development tools
- Virus Scanners
- Policy managers
- Trusted hardware
Today’s security deployment

- Most deployment of security services today handles the easy stuff, implementing security at a single point in the network, or at a single layer in the protocol stack:
  - Firewalls, VPN’s
  - IPSec
  - SSL
  - Virus scanners
  - Intrusion detection
A more difficult problem

• Unfortunately, security isn’t that easy. It must be better integrated with the application.
  – At the level at which it must ultimately be specified, security policies pertain to application level objects, and identify application level entities (users).
Security Systems vs Systems Security

Integration of dynamic security services creates feedback path enabling effective response to attacks

GAA API

Authentication

Firewalls
Web Servers
Databases
IPSec
...

POLICY

EACL

SECURITY AUDIT RECORDS

INTRUSION DETECTION

UNDER ATTACK
Loosely Managed Systems

- Security is made even more difficult to implement since today’s systems lack a central point of control.
  - Home machines unmanaged
  - Networks managed by different organizations.
  - A single function touches machines managed by different parties.
    - Clouds
  - Who is in control?
Who is in Control

• The Intruder
• The Government
• Your employer
• The Merchant
• The credit card companies
• The credit bureaus
• Ultimately, it must be you who takes control, but today’s systems don’t take that view.
  – Balance conflicting interests and control.
The New York Times Web site was unavailable to readers on Tuesday afternoon after an online attack on the company’s domain name registrar. The attack also forced employees of The Times to take care in sending e-mails.

The hacking was just the latest of a major media organization, with The Financial Times and The Washington Post also having their operations disrupted within the last few months. It was also the second time this month that the Web site of The New York Times was unavailable for several hours. [The outage which] appeared to be affecting the Web site well into the evening — was “the result of a malicious external attack.” … carried out by a group known as “the Syrian Electronic Army, or someone trying very hard to be them.” The group attacked the company’s domain name registrar, Melbourne IT.

The attacks on Twitter and The New York Times required significantly more skill than the string of S.E.A. attacks on media outlets earlier this year, when the group attacked Twitter accounts for dozens of outlets including The Associated Press. Those attacks caused the stock market to plunge after the group planted false tales of explosions at the White House. “In terms of the sophistication of the attack, this is a big deal,” Mr. Frons said. “It’s sort of like breaking into the local savings and loan versus breaking into Fort Knox. A domain registrar should have extremely tight security because they are holding the security to hundreds if not thousands of Web sites.”
• End of Lecture 1

• Following slides are start of lecture 2
CSci530: Security Systems
Lecture 2 – September 6, 2013
Cryptography

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Administration

• Assignment 1 on course web page
  – http://ccss.usc.edu/530
  – Due 18 September 2013
Cryptography and Security

• Cryptography underlies many fundamental security services
  – Confidentiality
  – Data integrity
  – Authentication

• It is a basic foundation of much of security.
A Brief History

• Steganography: “covered writing”
  – Demaratus and wax tablets
  – German microdots (WWII).
  – Flaw: Discovery yields knowledge
    – Confidentiality through obscurity
• Cryptography: “secret writing”
  – TASOIINRNPSTO and TVCTUJUVUJPO
Encryption used to scramble data
The Basics of Cryptography

• Two basic types of cryptography
  – TASONO PINSTIR
    ▪ Message broken up into units
    ▪ Units permuted in a seemingly random but reversible manner
    ▪ Difficult to make it easily reversible only by intended receiver
    ▪ Exhibits same first-order statistics
The Basics of Cryptography

- Two basic types of cryptography
  - TRANSPOSITION (TASONOPINSTIR)
    - Message broken up into units
    - Units permuted in a seemingly random but reversible manner
    - Difficult to make it easily reversible only by intended receiver
    - Exhibits same first-order statistics
The Basics (continued)

• Two basic types of cryptography (cont)
  – TVCTUJUVUJPO
    ▪ Message broken up into units
    ▪ Units mapped into ciphertext
      – Ex: Caesar cipher
    ▪ First-order statistics are isomorphic in simplest cases
    ▪ Predominant form of encryption
The Basics (continued)

- Two basic types of cryptography (cont)
  - Substitution (TVCTUJUVUJPO)
    - Message broken up into units
    - Units mapped into ciphertext
      - Ex: Caesar cipher
    - First-order statistics are isomorphic in simplest cases
  - Predominant form of encryption
How Much Security?

• Mono-alphabetic substitution cipher
  – Permutation on message units—letters
    ▪ 26! different permutations
    ▪ Each permutation considered a key
  – Key space contains 26! = 4x10^{26} keys
    ▪ Equals number of atoms in gallon H_2O
    ▪ Equivalent to a 88-bit key
How Much Security?

• So why not use substitution ciphers?
  – Hard to remember 26-letter keys
    ▪ But we can restrict ourselves to shorter keys
    ▪ Ex: JULISCAERBDFGHKM, etc
  – Remember: first-order statistics are isomorphic
    ▪ Vulnerable to simple cryptanalysis
    ▪ Hard-to-read fonts for crypto?!
Crypto-analytic Attacks

• Classified as:
  – Cipher text only
    ▪ Adversary see only the ciphertext
  – Known plain text
    ▪ May know some corresponding plaintext (e.g. Login:)
  – Chosen plaintext
    ▪ Can ask to have text encrypted
Substitution Ciphers

• Two basic types
  – Symmetric-key (conventional)
    ▪ Single key used for both encryption and decryption
    ▪ Keys are typically short, because key space is densely filled
    ▪ Ex: AES, DES, 3DES, RC4, Blowfish, IDEA, etc
Substitution Ciphers

• Two basic types (cont)
  – Public-key (asymmetric)
    ▪ Two keys: one for encryption, one for decryption
    ▪ Keys are typically long, because key space is sparsely filled
    ▪ Ex: RSA, El Gamal, DSA, etc
One Time Pads

- For confidentiality, One Time Pad provably secure.
  - Generate truly random key stream size of data to be encrypted.
  - Encrypt: Xor plaintext with the keystream.
  - Decrypt: Xor again with keystream.

- Weak for integrity
  - 1 bit changed in cipher text causes corresponding bit to flip in plaintext.

- Key size makes key management difficult
  - If key reused, the cipher is broken.
  - If key pseudorandom, no longer provably secure
  - Beware of claims of small keys but as secure as one time pad – such claims are wrong.
Block vs. Stream: Block

• Block ciphers encrypt message in units called blocks
  – E.g. DES: 8-byte key (56 key bits), 8-byte block
  – AES (discussed later) is also a block cipher.
  – Larger blocks make simple cryptanalysis useless (at least for short messages)
    ▪ Not enough samples for valid statistics
    ▪ 8 byte blocks common
    ▪ But can still tell if something is the same.
Key and Block Size

- Do larger keys make sense for an 8-byte block?
  - 3DES: Key is 112 or 168 bits, but block is still 8 bytes long (64 bits)
  - Key space is larger than block space
  - But how large is permutation space?
More on DES Internals

• More details on the internal operation of DES is covered in the Applied Cryptography class CSci531
• But we cover Modes of Operation in this lecture since these modes are important to apply DES, and the same modes can be used for other block ciphers.
Block vs. Stream: Stream

- Stream ciphers encrypt a bit, byte, or block at a time, but the transformation that is performed on a bit, byte, or block varies depending on position in the input stream and possibly the earlier blocks in the stream.
  - Identical plaintext block will yield a different cipher text block.
  - Makes cryptanalysis more difficult.
  - DES modes CBC, CFB, and OFB modes (discussed next) create stream ciphers from DES, which is a block cipher.
  - Similar modes available for AES.
DES Modes of Operation – Electronic Code Book (ECB)

Encrypt:
\[
x_1 \xrightarrow{e_K} y_1 \xrightarrow{e_K} y_2 \xrightarrow{e_K} \cdots \xrightarrow{e_K} y_n
\]

Decrypt:
\[
y_1 \xrightarrow{d_K} x_1 \xrightarrow{d_K} x_2 \xrightarrow{d_K} \cdots \xrightarrow{d_K} x_n
\]

- Each block encrypted in isolation
- Vulnerable to block replay

Copyright © 1995-2013 Clifford Neuman - UNIVERSITY OF SOUTHERN CALIFORNIA - INFORMATION SCIENCES INSTITUTE
DES Modes of Operation – Cipher Block Chaining (CBC)

- Each plaintext block XOR’d with previous ciphertext
- Easily incorporated into decryption
- What if prefix is always the same? IV!
DES Modes of Operation – Cipher Feedback Mode (CFB)

- For encrypting character-at-a-time (or less)
- Chains as in CBC
- Also needs an IV – Must be Unique – Why?
DES Modes of Operation – Output Feedback Mode (OFB)

Encrypt:

\[ IV \rightarrow e_K \rightarrow \text{output} \rightarrow e_K \rightarrow \text{output} \rightarrow \cdots \rightarrow e_K \rightarrow \text{output} \]

Decrypt:

\[ IV \rightarrow e_K \rightarrow \text{output} \rightarrow e_K \rightarrow \text{output} \rightarrow \cdots \rightarrow e_K \rightarrow \text{output} \]

–Like CFB, but neither ciphertext nor plaintext is fed back to the input of the block encryption.
Variants and Applications

• 3DES: Encrypt using DES 3x
  – Two and three-key types
  – Inner and outer-CBC modes
• Crypt: Unix hash function for passwords
  – Uses variable expansion permutations
• DES with key-dependent S-boxes
  – Harder to analyze
3DES Using Two Keys

3DES: Encrypt using DES 3x
⇒ two and three-key types

encryption:

\[ m \rightarrow E \rightarrow D \rightarrow E \rightarrow c \]

decryption:

\[ c \rightarrow D \rightarrow E \rightarrow D \rightarrow m \]

- Can use K₁,K₂,K₃, or K₁,K₂,K₁, or K₁,K₁,K₁

- Figure courtesy William Cheng
3DES Outer CBC

CBC on the outside:

- Figure courtesy William Cheng
3DES Inner CBC

- Inner is more efficient, but less secure
  - More efficient due to ability to pipeline implementation
  - Weaker for many kinds of attacks

Figure courtesy William Cheng
Why not Two Round

- Meet in middle attack makes it not much better than single DES.
  
  - Figure courtesy William Cheng

Copyright © 1995-2013 Clifford Neuman - UNIVERSITY OF SOUTHERN CALIFORNIA - INFORMATION SCIENCES INSTITUTE
Certification of DES

• Had to be recertified every ~5 years
  – 1983: Recertified routinely
  – 1987: Recertified after NSA tried to promote secret replacement algorithms
    ▪ Withdrawal would mean lack of protection
    ▪ Lots of systems then using DES
  – 1993: Recertified after continued lack of alternative
Enter AES

• 1998: NIST finally refuses to recertify DES
  – 1997: Call for candidates for Advanced Encryption Standard (AES)
  – Fifteen candidates whittled down to five
  – Criteria: Security, but also efficiency
    ▪ Compare Rijndael with Serpent
    ▪ 9/11/13 rounds vs 32 (breakable at 7)
  – 2000: Rijndael selected as AES
Structure of Rijndael

• Unlike DES, operates on whole bytes for efficiency of software implementations
• Key sizes: 128/192/256 bits
• Variable rounds: 9/11/13 rounds
• More details on structure in the applied cryptography class.
Security of Rijndael

• Key size is enough
• Immune to linear or differential analysis
• But Rijndael is a very structured cipher
• Attack on Rijndael’s algebraic structure
  – Breaking can be modeled as equations
Impact of Attacks on Rijndael

• Currently of theoretical interest only
  – Reduces complexity of attack to about $2^{100}$
  – Also applicable to Serpent

• Still, uncomfortably close to feasibility
  – DES is already insecure against brute force
  – Schneier (somewhat arbitrarily) sets limit at $2^{80}$

• Certainly usable pending further results
Public Key Cryptography

- aka asymmetric cryptography
- Based on some NP-complete problem
  - Unique factorization
  - Discrete logarithms
    - For any b, n, y: Find x such that \( b^x \mod n = y \)
- Modular arithmetic produces folding
A Short Note on Primes

- Why are public keys (and private keys) so large?
- What is the probability that some large number $p$ is prime?
  - About 1 in $1/\ln(p)$
  - When $p \sim 2^{512}$, equals about 1 in 355
    - About 1 in $355^2$ numbers $\sim 2^{1024}$ is product of two primes (and therefore valid RSA modulo)
RSA

- Rivest, Shamir, Adleman
- Generate two primes: p, q
  - Let n = pq
  - Choose e, a small number, relatively prime to \( (p-1)(q-1) \)
  - Choose d such that \( ed = 1 \mod (p-1)(q-1) \)
- Then, \( c = m^e \mod n \) and \( m = c^d \mod n \)
An Example

• Let $p = 5$, $q = 11$, $e = 3$
  – Then $n = 55$
  – $d = 27$, since $(3)(27) \mod 40 = 1$
• If $m = 7$, then $c = 7^3 \mod 55 = 343 \mod 55 = 13$
• Then $m$ should $= 13^{27} \mod 55$
An Example

- Computing $13^{27} \mod 55$
  - $13^1 \mod 55 = 13$, $13^2 \mod 55 = 4$, $13^4 \mod 55 = 16$, $13^8 \mod 55 = 36$, $13^{16} \mod 55 = 31$
  - $13^{27} \mod 55 = (13)(4)(36)(31) \mod 55 = (1872 \mod 55)(31) \mod 55 = 62 \mod 55 = 7$ (check)
CSci530: Security Systems
Lecture 3 – September 13, 2013
Public Key Cryptography Continued
(continued from last lecture)

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Administration

• Assignment 1 on course web page
  – http://ccss.usc.edu/530
  – Due 18 September 2013

• TA Office Hours
  – Bailan Li
  – Tuesday & Thursday 8:30-9:30AM
  – SAL 219
Other Public Cryptosystems

- **ElGamal** (signature, encryption)
  - Choose a prime $p$, a generator $< p$
  - Choose a random number $x < p$
  - Public key is $g$, $p$, and $y = g^x \mod p$
  - Private key is $x$; to obtain from public key requires extracting discrete log
  - Mostly used for signatures
Other Public Cryptosystems

• Elliptic curve cryptosystems
  – $y^2 = x^3 + ax^2 + bx + c$
  – Continuous elliptic curves used in FLT proof
  – Discrete elliptic curves used to implement existing public-key systems
    • Allow for shorter keys and greater efficiency
Importance of ECC

- There has been rapid progress in cryptanalysis of RSA and Diffie-Hellman public key systems.
  

- ECC is based on different mathematics, which has been shown to be NP complete.
Digital Signatures

• Provides data integrity
  – Can it be done with symmetric systems?
    ▪ Verification requires shared key
    ▪ Doesn’t provide non-repudiation

• Need proof of provenance
  – Hash the data, encrypt with private key
  – Verification uses public key to decrypt hash
  – Provides “non-repudiation”
    ▪ But what does non-repudiation really mean?
Digital Signatures

• RSA can be used
• DSA: Digital Signature Algorithm
  – Variant of ElGamal signature
  – Adopted as part of DSS by NIST in 1994
  – Slower than RSA (but likely unimportant)
  – NSA had a hand in its design (?!)
  – Key size ranges from 512 to 1024 bits
  – Royalty-free
Key Exchange

• Diffie-Hellman key exchange
  – Choose large prime $n$, and generator $g$
    ▪ For any $b$ in $(1, n-1)$, there exists an $a$ such that $g^a = b$
  – Alice, Bob select secret values $x$, $y$, resp
  – Alice sends $X = g^x \mod n$
  – Bob sends $Y = g^y \mod n$
  – Both compute $g^{xy} \mod n$, a shared secret
    ▪ Can be used as keying material
Hash Functions

• Given m, compute H(m)
• Should be...
  – Efficient: H() easy to compute
  – One-way: Given H(m), hard to find m’ such that H(m’) = H(m)
  – Collision-resistant: Hard to find m and m’ such that H(m’) = H(m)
Use of Hashes in Signatures

- Reduce input to fixed data size
  - MD5 produces 128 bits
  - SHA1 produces 160 bits
- Encrypt the output using private key
- Why do we need collision-resistance?
Current event – How does this relate to our discussion

N.S.A. Foils Much Internet Encryption

By NICOLE PERLROTH, JEFF LARSON and SCOTT SHANE Published: September 5, 2013

The National Security Agency is winning its long-running secret war on encryption, using supercomputers, technical trickery, court orders and behind-the-scenes persuasion to undermine the major tools protecting the privacy of everyday communications in the Internet age, according to newly disclosed documents.

The agency has circumvented or cracked much of the encryption, or digital scrambling, that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and automatically secures the e-mails, Web searches, Internet chats and phone calls of Americans and others around the world, the documents show.

Many users assume — or have been assured by Internet companies — that their data is safe from prying eyes, including those of the government, and the N.S.A. wants to keep it that way. The agency treats its recent successes in deciphering protected information as among its most closely guarded secrets, restricted to those cleared for a highly classified program code-named Bullrun, according to the documents, provided by Edward J. Snowden, the former N.S.A. contractor.

The agency, according to the documents and interviews with industry officials, deployed custom-built, superfast computers to break codes, and began collaborating with technology companies in the United States and abroad to build entry points into their products. The documents do not identify which companies have participated.

But some experts say the N.S.A.’s campaign to bypass and weaken communications security may have serious unintended consequences. They say the agency is working at cross-purposes with its other major mission, apart from eavesdropping: ensuring the security of American communications.

“The risk is that when you build a back door into systems, you’re not the only one to exploit it,” said Matthew D. Green, a cryptography researcher at Johns Hopkins University. “Those back doors could work against U.S. communications, too.”
• End of Lecture 2

• Following slides are start of lecture 3
CSci530: Security Systems
Lecture 3 – September 13, 2013
Key Management

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Administration

• Assignment 1 on course web page
  – http://ccss.usc.edu/530
  – Due 18 September 2013
Key Exchange

- Diffie-Hellman key exchange
  - Choose large prime \( n \), and generator \( g \)
    - For any \( b \) in (1, \( n-1 \)), there exists an \( a \) such that \( g^a = b \)
  - Alice, Bob select secret values \( x, y \), resp
  - Alice sends \( X = g^x \mod n \)
  - Bob sends \( Y = g^y \mod n \)
  - Both compute \( g^{xy} \mod n \), a shared secret
    - Can be used as keying material
Cryptography in Use

• Provides foundation for security services
  – Provides confidentiality
  – Validates integrity
  – Provides data origin authentication
  – If we know the key
• Where does the key come from
  – Straightforward plan
    ▪ One side generates key
    ▪ Transmits key to other side
    ▪ But how?
Key Management

- Key management is where much security weakness lies
  - Choosing keys
  - Storing keys
  - Communicating keys
What to do with keys

• Practical issues
  – How to carry them
    ▪ Passwords vs. disks vs. smartcards
  – Where do they stay, where do they go
  – How many do you have
  – How do you get them to begin with.
Bootstrapping Security

- Exchange the key in person
  - Can exchange key before it is needed.
  - Could be a password.

- Hide the key in something else
  - Steganography, fairly weak

- Armored courier
  - If all else fails

- Send key over the net encrypted
  - But, using what key (bootstrap)
Key Exchange

• Diffie-Hellman key exchange
  – Choose large prime $n$, and generator $g$
    ▪ For any $b$ in $(1, n-1)$, there exists an $a$ such that $g^a = b$
  – Alice, Bob select secret values $x$, $y$, resp
  – Alice sends $X = g^x \mod n$
  – Bob sends $Y = g^y \mod n$
  – Both compute $g^{xy} \mod n$, a shared secret
    ▪ Can be used as keying material
Diffie-Hellman Key Exchange (1)

- Choose large prime n, and generator g
  - For any b in (1, n-1), there exists an a such that $g^a = b$. This means that every number mod p can be written as a power of g (mod p).
    - To find such a g, pick the p such that $p = 2q + 1$ where q is also prime.
    - For such choices of p, half the numbers will be generators, and you can test if a candidate g is a generator by testing whether $g^q \pmod{n}$ is equal to n-1.
**Diffie-Hellman Key Exchange (2)**

- Alice, Bob select secret values \( x, y \)
- Alice sends \( X = g^x \mod n \)
- Bob sends \( Y = g^y \mod n \)
- Both compute \( g^{xy} \mod n \), a shared secret
  - Can be used as keying material
Man in the middle of DH

- DH provides key exchange, but not authentication
  - You don’t really know you have a secure channel
- Man in the middle
  - You exchange a key with eavesdropper, who exchanges key with the person you think you are talking to.
  - Eavesdropper relays all messages, but observes or changes them in transit.
- Solutions:
  - Published public values
  - Authenticated DH (Sign or encrypt DH value)
  - Encrypt the DH exchange
  - Subsequently send hash of DH value, with secret
Two Cases so Far

• Can exchange a key with anyone, but you don’t know who you are talking with.

• Can exchange keys with known parties in advance, but are limited to communication with just those parties.
Peer-to-Peer Key Distribution

- Technically easy
  - Distribute keys in person
- But it doesn’t scale
  - Hundreds of servers…
  - Times thousands of users…
  - Yields ~ million keys
Incremental Key Distribution

• Build toward Needham-Schroeder and Kerberos mechanisms
• Key-distribution tied to authentication.
  – If you know who you share a key with, authentication is easy.
  – You want to know who has the key, not just that anyone has it.
Encryption Based Authentication

• Proving knowledge of encryption key
  – Nonce = Non repeating value

{Nonce or timestamp}K_{CS}

But where does $K_{CS}$ come from?
KDC Based Key Distribution

Building up to Needham Schroeder/Kerberos

• User sends request to KDC: \( \{s\} \)
• KDC generates a random key: \( K_{c,s} \)
  – Encrypted twice: \( \{K_{c,s}\}K_c, \{K_{c,s}\}K_s \)
  – \( \{K_{c,s}\}K_s \) called ticket
  – Ticket plus \( K_{c,s} \) called credentials
  – Ticket is opaque and forwarded with application request
• No keys ever traverse net in the clear
Kerberos or Needham Schroeder

Third-party authentication service

- Distributes session keys for authentication, confidentiality, and integrity

1. $s, n$

2. $\{K_{c,s} S, n\}K_c, \{K_{c,s} C\}K_s$

3-5. $\{\text{Nonce or T}\}K_{cs}$
Problem

• User now trusts credentials
• But can server trust user?
• How can server tell this isn’t a replay?
• Legitimate user makes electronic payment to attacker; attacker replays message to get paid multiple times
  – Requires no knowledge of session key
Solution

• Add challenge-response
  – Server generates second random nonce
  – Sends to client, encrypted in session key
  – Client must decrypt, decrement, encrypt
• Effective, but adds second round of messages
• Can use timestamps as nonces
  – But must remember what seen
Problem

• What happens if attacker does get session key?
  – Answer: Can reuse old session key to answer challenge-response, generate new requests, etc
Solution

• Replace (or supplement) nonce in request/reply with timestamp [Denning, Sacco]
  – \{K_{c,s}, s, n, t\}K_c and \{K_{c,s}, c, t\}K_s, resp
  – Also send \{t\}K_{c,s} as authenticator
    ▪ Prevents replay without employing second round of messages as in challenge-response
    ▪ Lifetime of ticket
Problem #5

• Each client request yields new verifiable-plaintext pairs
• Attacker can sit on the network, harvest client request and KDC replies
Solution #5

- Introduce Ticket Granting Server (TGS)
  - Daily ticket plus session keys
- TGS+AS = KDC
  - This is modified Needham-Schroeder
  - Basis for Kerberos
- Pre-authentication
- Note: not a full solution
  - Makes it slightly harder for adversary.
Kerberos

Third-party authentication service

- Distributes session keys for authentication, confidentiality, and integrity
Public Key Distribution

• Public key can be public!
  – How does either side know who and what the key is for? Private agreement? (Not scalable.)
• Does this solve key distribution problem?
  – No – while confidentiality is not required, integrity is.
• Still need trusted third party
Key Distribution linked to Authentication

- It's all about knowing who has the keys.
- We will revisit Kerberos when we discuss authentication.
Key Management

• Key management is where much security weakness lies
  – Choosing keys
  – Storing keys
  – Communicating keys
Certification Infrastructures

- Public keys represented by certificates
- Certificates signed by other certificates
  - User delegates trust to trusted certificates
  - Certificate chains transfer trust up several links

Do you trust a certificate signed by Amazon?
Examples

- **PGP**
  - “Web of Trust”
  - Can model as connected digraph of signers

- **X.500**
  - Hierarchical model: tree (or DAG?)
  - (But X.509 certificates use ASN.1!)
Examples

- **SSH**
  - User keys out of band exchange.
  - Weak assurance of server keys.
    - Was the same host you spoke with last time.
  - Discussion of benefits

- **SET**
  - Hierarchical
  - Multiple roots
  - Key splitting
Key Distribution

- Conventional cryptography
  - Single key shared by both parties
- Public Key cryptography
  - Public key published to the world
  - Private key known only by owner
- Third party certifies or distributes keys
  - Certification infrastructure
  - Authentication
Practical use of keys

- Email (PEM or S/MIME or PGP)
  - Hashes and message keys to be distributed and signed.
- Conferencing
  - Group key management (discussed later)
- Authentication (next lecture)
- SSL
  - And other “real time” protocols
  - Key establishment
Recovery from exposed keys

• Revocation lists (CRL’s)
  – Long lists
  – Hard to propagate
• Lifetime / Expiration
  – Short life allows assurance of validity at time of issue.
• Realtime validation
  – Online Certificate Status Protocol (OCSP)
• What about existing messages?
Key Management Overview

- Key size vs. data size
  - Affects security and usability
- Reuse of keys
  - Multiple users, multiple messages
- Initial exchange
  - The bootstrap/registration problem
  - Confidentiality vs. authentication
Key Management Review

• KDC’s
  – Generate and distribute keys
  – Bind names to shared keys
Key Management Overview

• Who needs strong secrets anyway
  – Users?
  – Servers?
  – The Security System?
  – Software?
  – End Systems?

• Secret vs. Public
Security Architectures

• DSSA
  – Delegation is the important issue
    ▪ Workstation can act as user
    ▪ Software can act as workstation
      – if given key
    ▪ Software can act as developer
      – if checksum validated
  – Complete chain needed to assume authority
  – Roles provide limits on authority – new sub-principal
Group Key Management

- Group key vs. Individual key
  - Identifies member of groups vs. which member of group
  - PK slower but allows multiple verification of individuals
Group Key Management Issues

• Revoking access
  – Change messages, keys, redistribute

• Joining and leaving groups
  – Does one see old message on join
  – How to revoke access

• Performance issues
  – Hierarchy to reduce number of envelopes for very large systems
  – Hot research topic
Group Key Management Approaches

• Centralized
  – Single entity issues keys
  – Optimization to reduce traffic for large groups
  – May utilize application specific knowledges
• Decentralized
  – Employs sub managers
• Distributed
  – Members do key generation
  – May involve group contributions
**Current event – How does this relate to our discussion**

Fingerprint sensor in iPhone 5s is no silver bullet, researchers say
The technology would be most efficient if used as part of a two-factor authentication system, not alone
By Lucian Constantin – ComputerWorld - September 10, 2013 07:45 PM ET

- IDG News Service - The fingerprint sensor in Apple's new iPhone 5s has the potential to enhance the security of the device, but the devil will be in the details. Its effectiveness will depend on the strength of the implementation and whether it's used in conjunction with other security credentials, researchers said. Apple unveiled the iPhone 5s, which has a fingerprint sensor dubbed Touch ID built into the home button. The sensor will allow users to use their fingerprints instead of a password to unlock the device and make purchases on iTunes.

- It's not clear if the feature will also be used in other scenarios that have yet to be revealed or if third-party applications will also be able to use it to authenticate users. In presenting the technology Tuesday, Apple said the fingerprint data is encrypted and locked in the device's new A7 chip, that it's never directly accessible to software and that it's not stored on Apple's servers or backed up to iCloud.

- "Common attacks against fingerprint readers include using photos of fingers or creating fingerprint molds based on captured prints," said Dirk Sigurdson, director of engineering for the Mobilisafe mobile risk management technology at security firm Rapid7, via email. "Hopefully the iPhone sensor will have strong protections against using copied fingers." Fingerprint technology is not a high-security feature, said Marc Rogers, principal security researcher at mobile security firm Lookout. That's why most military installations, for example, use hand geometry or retina scanners instead, he said.

- The best single factor of authentication is a strong password stored only in the user's brain, but it's inherently difficult for people to create and remember strong passwords, Sigurdson said. This often results in bad passwords being used, so a good fingerprint reader and matching algorithm will likely improve the security of iOS devices, he said. Rogers believes fingerprints could add great security if they're used in conjunction with other security credentials as part of two-factor authentication.

- For example, Apple could allow users to set a strong, complex password that's used to encrypt the file system and which would need to be entered only when the device is switched on. The user's fingerprint could then be used as a medium-strength access credential to unlock the device when it's on and needs to be used. This would provide both security and convenience for users, Rogers said.
• End of Lecture 3

• Following slides are start of lecture 4
CSci530: Security Systems
Lectures 4&5 – September 20&27, 2013
Authentication

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Identification vs. Authentication

Identification

Associating an identity with an individual, process, or request

Authentication

– Verifying a claimed identity
Basis for Authentication

Ideally

Who you are

Practically

Something you know

Something you have

Something about you

(Sometimes mistakenly called things you are)
Something you know

Password or Algorithm
e.g. encryption key derived from password

Issues

Someone else may learn it
Find it, sniff it, trick you into providing it
Other party must know how to check
You must remember it
How stored and checked by verifier
Examples of Password Systems

Verifier knows password

Encrypted Password

One way encryption

Third Party Validation
Attacks on Password

Brute force

Dictionary

Pre-computed Dictionary

Guessing

Finding elsewhere
What makes for a good password

How some systems define good passwords:
MickeyMinniePlutoHueyLouieDeweyDonaldGoofyWashington

When asked why one might have such a long password, they were told the password should be at least 8 characters and include at least one capital.
Something you Have

Cards

- Mag stripe (= password)
- Smart card, USB key
- Time varying password

Issues

- How to validate
- How to read (i.e. infrastructure)
Case Study – RSA SecureID

Claimed - Something You Have
Reduced to something they know

How it works:
Seed
Synchronization

Compromises:
RSA Break-in
Or man in the middle
Something about you

Biometrics
  Measures some physical attribute
    Iris scan
    Fingerprint
    Picture
    Voice

Issues
  How to prevent spoofing
    Suited when biometric device is trusted, not suited otherwise
Other forms of authentication

IP Address

Caller ID (or call back)

Now “phone factor” (probably tm)

Past transaction information

(second example of something you know)
“Enrollment”

How to initially exchange the secret.

In person enrollment
Information known in advance
Third party verification
Mail or email verification
Multi-factor authentication

Require at least two of the classes above.
  e.g. Smart card plus PIN
  RSA SecurID plus password (AOL)
  Biometric and password

Issues
  Better than one factor
  Be careful about how the second factor is validated. E.g. on card, or on remote system.
General Problems with Password

Space from which passwords Chosen
Too many passwords
And what it leads to
Single Sign On

“Users should log in once
And have access to everything”

Many systems store password lists
Which are easily stolen

Better is encryption based credentials
Usable with multiple verifiers

Interoperability is complicating factor.
Encryption Based Authentication

- Proving knowledge of encryption key
  - Nonce = Non repeating value

\[ \{\text{Nonce or timestamp}\}K_{cs} \]

C ➔ S
Authentication w/ Conventional Crypto

- Kerberos or Needham Schroeder

Diagram:

- KDC
- C
- S

1. KDC to C
2. C to S
3. C to S
4. S to C
5. S to C
Current event – How does this relate to our discussion

Snowden disclosures prompt warning on widely used computer security formula
The Courant – September 20, 2013 - Joseph Menn - Reuters

SAN FRANCISCO (Reuters) - In the latest fallout from Edward Snowden's intelligence disclosures, a major U.S. computer security company warned customers on Thursday to stop using software that relies on a weak mathematical formula developed by the National Security Agency.

RSA, the security arm of storage company EMC Corp, told current customers in an email that a toolkit for developers had a default random-number generator using the weak formula, and that customers should switch to one of several other formulas in the product.

Last week, the New York Times reported that Snowden's cache of documents from his time working for an NSA contractor showed that the agency used its public participation in the process for setting voluntary cryptography standards, run by the government's National Institute of Standards and Technology, to push for a formula that it knew it could break.

NIST, which accepted the NSA proposal in 2006 as one of four systems acceptable for government use, this week said it would reconsider that inclusion in the wake of questions about its security.

Developers who used RSA's "BSAFE" kit wrote code for Web browsers, other software, and hardware components to increase their security. Random numbers are a core part of much modern cryptography, and the ability to guess what they are renders those formulas vulnerable.

The NSA-promoted formula was odd enough that some experts speculated for years that it was flawed by design. A person familiar with the process told Reuters that NIST accepted it in part because many government agencies were already using it.
Authentication w/ PK Crypto

• Based on public key certificates
Public Key Cryptography (revisited)

- Key Distribution
  - Confidentiality not needed for public key
  - Solves $n^2$ problem
- Performance
  - Slower than conventional cryptography
  - Implementations use for key distribution, then use conventional crypto for data encryption
- Trusted third party still needed
  - To certify public key
  - To manage revocation
  - In some cases, third party may be off-line
Certificate-Based Authentication

Certification authorities issue signed certificates

- Banks, companies, & organizations like Verisign act as CA’s
- Certificates bind a public key to the name of a user
- Public key of CA certified by higher-level CA’s
- Root CA public keys configured in browsers & other software
- Certificates provide key distribution
Certificate-Based Authentication (2)

Authentication steps

- Verifier provides nonce, or a timestamp is used instead.
- Principal selects session key and sends it to verifier with nonce, encrypted with principal’s private key and verifier’s public key, and possibly with principal’s certificate.
- Verifier checks signature on nonce, and validates certificate.
Secure Sockets Layer (and TLS)

Encryption support provided between Browser and web server - below HTTP layer

Client checks server certificate
   Works as long as client starts with the correct URL

Key distribution supported through cert steps
Authentication provided by verify steps
Trust models for certification

• X.509 Hierarchical
  – Single root (original plan)
  – Multi-root (better accepted)
  – SET has banks as CA’s and common SET root
• PGP Model
  – “Friends and Family approach” - S. Kent
• Other representations for certifications
• No certificates at all
  – Out of band key distribution
  – SSH
Federated Identity
Passport v Liberty Alliance

• Two versions of Passport
  – Current deployed version has lots of weaknesses and is centralized
  – Version under development is “federated” and based on Kerberos

Liberty Alliance
  – Loosely federated with framework to describe authentication provided by others.
Passport v1

- Goal is single sign on
- Implemented via redirections

Assigned reading: http://avirubin.com/passport.html
Federated Passport

- Announced September 2001
- Multiple registrars
  - E.g. ISPs register own users
- Kerberos credentials
  - Embedded authorization data to pass other info to merchants.
- Federated Passport is predominantly vaporware today, but .net authentication may be where their federated model went.
Liberty Alliance

- Answer to MS federated Passport
- Design criteria was most of the issues addressed by Federated Passport, i.e. no central authority.
- Got off to slow start, but to date has produced more than passport has.
- Use SAML (Security Association Markup Language) to describe trust across authorities, and what assertions means from particular authorities.
- These are hard problems, and comes to the core of what has kept PKI from being as dominant as orginally envisioned.
- Phased approach: Single sign on, Web service, Federated Services Infrastructure.
Federated Identity - Shibboleth

• Internet 2 Project
  – Federated Administration
  – Attribute Based Access Control
  – Active Management of Privacy
  – Based on Open SAML
  – Framework for Federation
Shibboleth - Architecture

• Service Provider
  – Browser goes to Resource Manager who users WAYF, and users Attribute Requester, and decides whether to grant access.

• Where are you from service
  – Redirects to correct servers

• Federation
The Shibboleth Protocol

1. User requests resource

2. I don’t know you, or where you are from

3. Where are you from?

4. Redirect to IdP for your org

5. I don’t know you. Authenticate using your org’s web login

6. I know you now. Redirect to SP, with a handle for user

7. I don’t know your attributes. Ask the IdP (peer to peer)

8. Based on attribute values, allow access to resource

Source: Kathryn Huxtable khuxtable@ku.edu 10 June 2005
Generic Security Services API
Moving up the Stack

Standard interface for choosing among authentication methods

Once an application uses GSS-API, it can be changed to use a different authentication method easily.

Calls

- Acquire and release cred
- Manage security context
  - Init, accept, and process tokens
- Wrap and unwrap
Authentication in Applications

Unix login
Telnet
RSH
SSH
HTTP (Web browsing)
FTP
Windows login
SMTP (Email)
NFS
Network Access
Unix Login

One way encryption of password
Salted as defense against pre-computed dictionary attacks
To validate, encrypt and compare with stored encrypted password
May use shadow password file
Telnet

A remote login application

Normally just an unencrypted channel over which plaintext password sent.

Supports encryption option and authentication options using protocols like Kerberos.
RSH (Remote Shell/Remote Login)

Usually IP address and asserted account name.

Privileged port means accept asserted identity.

If not trusted, request unix password in clear.

Kerberos based options available

Kerberos based authentication and optional encryption
Secure Shell (SSH)

Encrypted channel with Unix login
  Establish encrypted channel, using public key presented by server
  Send password of user over channel
  Unix login to validate password.

Public key stored on target machine
  User generate Public Private key pair, and uploads the public key to directory on target host.
  Target host validates that corresponding private key is known.
Web Browsing (HTTP)

Connect in the clear, Unix Password
Connect through SSL, Unix password
Digest authentication (RFC 2617)
Server sends nonce
Response is MD5 checksum of
  Username, password, nonce URI
User certificate, strong authentication
File Transfer Protocol

Password based authentication or GSS-API based authentication

Including use of Kerberos

Authentication occurs and then stream is encrypted
Windows Network Login

In Win2K and later uses Kerberos
In Win NT
  Challenge response
  Server generates 8 byte nonce
  Prompts for password and hashes it
  Uses hash to DES encrypt nonce 3 times
Email

SMTP – To send mail
- Usually network address based
- Can use password
- Can be SSL protected
- SMTP after POP
Email

Post Office Protocol
Plaintext Password
Can be SSL protected
Eudora supports Kerberos authentication

IMAP
Password authentication
Can also support Kerberos
Email – Message Authentication

PGP and S/MIME

Digital Signature on messages

Message encrypted in session key

Optional

Hash of message encrypted in private key

Validation using sender’s public key
Email – Message Authentication

SPF and SenderID

– Authenticate domain of sender
– SPF record for domain in DNS
  ▪ Specifies what hosts (i.e. mail server host) can send mail originating from that address.
  ▪ Receivers may validate authorized sender based on record
  ▪ Can falsely reject for forwarded messages
Email – Message Authentication

Domain Keys

- Public key associated with domain in DNS
- Originators MTA attaches signature
  - Authenticated sender domain
  - Not individual sender
  - Signature covers specific header fields and possibly part of message.
- Messages may be forwarded
File System Authentication

Sun’s Network File System

Typically address based

Athena Kerberized version

Maps authenticated UID’s to addresses

NFS built on ONC RPC

ONC RPC has stronger Kerberos/GSSAPI support
File System Authentication

Andrew File System
Based on Andrew RPC
Uses Kerberos authentication

OSF’s DCE File System (DFS)
Based on DCE RPC
Uses Kerberos authentication
Network Access Servers

Radius

Problem: Not connected to network until connection established
Need for indirect authentication

Network access server must validate login with radius server.

Password sent to radius server encrypted using key between agent and radius server.
Old tricks help German hackers bypass iPhone 5s Touch ID security
Jeremy Kirk, IDG News Service  - Sep 23, 2013 6:16 AM

Apple's Touch ID authentication system can be defeated using a well-honed technique for creating a latex copy of someone's fingerprint, according to a German hacking group.

The Chaos Computer Club (CCC), which hosts an annual hacking conference and publishes computer security research, wrote on its blog that their experiment shows that fingerprint authentication "should be avoided."

Apple introduced Touch ID with its latest high-end iPhone 5S on Sept. 10. A person's "fingerprint is one of the best passcodes in the world. It's always with you, and no two are exactly alike," according to the company's website.

A hacker who goes by the name Starbug found that while Touch ID scans at a higher resolution, it can be beaten by increasing the resolution of the victim's fingerprint.

The CCC posted a video of what it wrote is a successful attack. Faking the print involves photographing the victim's fingerprint at 2400 DPI. The image is inverted and laser printed at 1200 DPI onto a transparent sheet using a "thick toner setting," according to the CCC.
• End of Lecture 5

• Following slides are start of lecture 6
CSci530: Computer Security Systems
Lecture 6 – 4 October 2013
Authorization and Policy

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Authorization: Two Meanings

- Determining permission
  - Is principal P permitted to perform action A on object U?
- Adding permission
  - P is now permitted to perform action A on object U
- In this course, we use the first sense
Access Control

• Who is permitted to perform which actions on what objects?

• Access Control Matrix (ACM)
  – Columns indexed by principal
  – Rows indexed by objects
  – Elements are arrays of permissions indexed by action

• In practice, ACMs are abstract objects
  – Huge and sparse
  – Possibly distributed
Delegated Authentication

Usually an authorization problem
How to allow an intermediary to perform operations on your behalf.
Pass credentials needed to authenticate yourself
Apply restrictions on what they may be used for.
Proxies

• A proxy allows a second principal to operate with the rights and privileges of the principal that issued the proxy
  – Existing authentication credentials
  – Too much privilege and too easily propagated

• Restricted Proxies
  – By placing conditions on the use of proxies, they form the basis of a flexible authorization mechanism
Restricted Proxies

- Two Kinds of proxies
  - Proxy key needed to exercise bearer proxy
  - Restrictions limit use of a delegate proxy
- Restrictions limit authorized operations
  - Individual objects
  - Additional conditions
Authenticating Hardware and Software

• DSSA
  – Delegation is the important issue
    ▪ Workstation can act as user
    ▪ Software can act as workstation
      – if given key
    ▪ Software can act as developer
      – if checksum validated
Next Generation Secure Computing Base (Longhorn)

• Secure booting provides known hardware and OS software base.

• Security Kernel in OS provides assurance about the application.

• Security Kernel in application manages credentials granted to application.

• Security servers enforce rules on what software they will interact with.
Instantiations of ACMs

- **Access Control Lists (ACLs)**
  - For each object, list principals and actions permitted on that object
  - Corresponds to rows of ACM
  - Example: Kerberos admin system
Instantiations of ACMs

• Capabilities
  – For each principal, list objects and actions permitted for that principal
  – Corresponds to columns of ACM
  – Example: Kerberos restricted proxies
• The Unix file system is an example of…?
Problems

- Permissions may need to be determined dynamically
  - Time
  - System load
  - Relationship with other objects
  - Security status of host
Problems

• Distributed nature of systems may aggravate this
  – ACLs need to be replicated or centralized
  – Capabilities don’t, but they’re harder to revoke

• Approaches
  – GAA
Authorization

• Final goal of security
  – Determine whether to allow an operation.
• Depends upon
  ▪ Policy
  ▪ Possibly authentication
  ▪ Other characteristics
The role of policy in security architecture

Policy – Defines what is allowed and how the system and security mechanisms should act.

Enforced By

Mechanism – Provides protection interprets/evaluates (firewalls, ID, access control, confidentiality, integrity)

Implemented as:

Software: which must be implemented correctly and according to sound software engineering principles.
Policy: The Access Matrix

- Policy represented by an Access Matrix
  - Also called Access Control Matrix
  - One row per object
  - One column per subject
  - Tabulates permissions
  - But implemented by:
    - Row – Access Control List
    - Column – Capability List
Policy models: Bell-LaPadula

- Discretionary Policy
  - Based on Access Matrix
- Mandatory Policy
  - Top Secret, Secret, Confidential, Unclassified
  - * Property: S can write O if and only if Level S <= Level O
    - Write UP, Read DOWN
  - Categories treated as levels
    - Form a matrix

(more models later in the course)
Other Policy Models

- Mandatory Access Control
  - Bell-Lepadula is an example
- Discretionary Access Control
  - Many examples
- Role Based Access Control
- Integrity Policies
  - Biba Model – Like BellLepadula but inverted
  - Clark Wilson
    - Constrained Data, IVP and TPs
Role Based Access Control

• Similar to groups in ACLs, but more general.
• Multiple phases
  – Administration
  – Session management
  – Access Control
• Roles of a user can change
  – Restrictions may limit holding multiple roles simultaneously or within a session, or over longer periods.
  – Supports separation of roles
• Maps to Organization Structure
Integrity Policies

• Biba Model – Like BellLepadula but inverted
• Clark Wilson
  – Constrained Data, IVP and TPs
Authorization Examples

• Access Matrix
• Access Control Lists
  – .htaccess (web servers)
  – Unix file access (in a limited sense)
    ▪ On login lookup groups
  – SSH Authorized Keys
• Capabilities
  – Unix file descriptors
  – Proxies mix ACLs and capabilities
Security is more than mix of point solutions

• Today’s security tools work with no coordinated policy
  – Firewalls and Virtual Private Networks
  – Authentication and Public Key Infrastructure
  – Intrusion Detection and limited response

• We need better coordination
  – Intrusion response affected at firewalls, VPN’s and Applications
  – Not just who can access what, but policy says what kind of encryption to use, when to notify ID systems.

• Tools should implement coordinated policies
  – Policies originate from multiple sources
  – Policies should adapt to dynamic threat conditions
  – Policies should adapt to dynamic policy changes triggered by activities like September 11th response.
GAA-API: Integration through Authorization

- Focus integration efforts on authorization and the management of policies used in the authorization decision.
  - Not really new - this is a reference monitor.
  - Applications shouldn’t care about authentication or identity.
    - Separate policy from mechanism
  - Authorization may be easier to integrate with applications.
  - Hide the calls to individual security services
    - E.g. key management, authentication, encryption, audit
Generic Authorization and Access-control API

Allows applications to use the security infrastructure to implement security policies.

gaa_get_object_policy_info function called before other GAA API routines which require a handle to object EACL to identify EACLs on which to operate. Can interpret existing policy databases.

gaa_check_authorization function tells application whether requested operation is authorized, or if additional application specific checks are required.
Three Phases of Condition Evaluation

GAA-API

- `gaa_get_object_policy_info()`
- `gaa_check_authorization()` \( T/F/U \)
- `gaa_execution_control()` \( T/F/U \)
- `gaa_post_execution_actions()` \( T/F/U \)

EACL

a.isi.edu, connect, Tom

System State
GAA-API Policies originate from multiple sources

- Discretionary policies associated with objects
  - Read from existing applications or EACLs
- Local system policies merged with object policies
  - Broadening or narrowing allowed access
- Policies imported from policy/state issuers
  - ID system issues state credentials, These credentials may embed policy as well.
- Policies embedded in credentials
  - These policies attach to user/process credentials and apply to access by only specific processes.
- Policies evaluated remotely
  - Credential issuers (e.g. authentication and authorization servers) evaluate policies to decide which credentials to issue.
Communicating threat conditions

Threat Conditions and New Policies carried in signed certificates
- Added info in authentication credentials
- Threat condition credential signed by ID system

Base conditions require presentation or availability of credential
- Matching the condition brings in additional policy elements.
Integrating security services

The API calls must be made by applications.
- This is a major undertaking, but one which must be done no matter how one chooses to do authorization.

These calls are at the control points in the app
- They occur at auditable events, and this is where records should be generated for ID systems
- They occur at the places where one needs to consider dynamic network threat conditions.
- Adaptive policies use such information from ID systems.
- They occur at the right point for billable events.
Advances Needed in Policy

- Ability to merge & apply policies from many sources
  - Legislated policies
  - Organizational policies
  - Agreed upon constraints
- Integration of Policy Evaluation with Applications
  - So that policies can be uniformly enforced
- Support for Adaptive Policies is Critical
  - Allows response to attack or suspicion
- Policies must manage use of security services
  - What to encrypt, when to sign, what to audit.
  - Hide these details from the application developer.
GAA - Applications and other integration

- Web servers - apache
- Grid services - globus
- Network control – IPsec and firewalls
- Remote login applications – ssh
- Trust management
  - Can call BYU code to negotiate credentials
  - Will eventually guide the negotiation steps
What dynamic policies enable

- Dynamic policy evaluation enables response to attacks:
  - Lockdown system if attack is detected
  - Establish quarantines by changing policy to establish isolated virtual networks dynamically.
  - Allow increased access between coalition members as new coalitions are formed or membership changes to respond to unexpected events.
Demo Scenario - LockDown

- You have an isolated local area network with mixed access to web services (some clients authenticated, some not).
Demo Scenario - LockDown

- You have an isolated local area network with mixed access to web services (some clients authenticated, some not).
- You need to allow incoming authenticated SSH or IPSec connections.
Demo Scenario - LockDown

- You have an isolated local area network with mixed access to web services (some clients authenticated, some not).
- You need to allow incoming authenticated SSH or IPSec connections.
- When such connections are active, you want to lock down your servers and require stronger authentication and confidentiality protection on all accesses within the network.
Policies

- HIPAA, other legislation
- Privacy statements
- Discretionary policies
- Mandatory policies (e.g. classification)
- Business policies
Mechanisms

• Access Matrix
  – Access Control List
  – Capability list
• Unix file system
• Andrew file system
• SSH authorized key files
• Restricted proxies, extended certificates
• Group membership
• Payment
Summary

• Policies naturally originate in multiple places.
• Deployment of secure systems requires coordination of policy across countermeasures.
• Effective response requires support for dynamic policy evaluation.
• Such policies can coordinated the collection of data used as input for subsequent attack analysis.
Current event – How does this relate to our discussion

October kicks off cybersecurity awareness month - USA Today September 30th

- SEATTLE – October is National Cyber Security Awareness month.
- This laudable public awareness initiative was launched 10 years ago by the U.S. Department of Homeland Security and the National Cyber Security Alliance, an organization of private companies that sponsor StaySafeOnline.org.
- Oct. 1-6, General online safety. Aims to raise online safety awareness among all Americans and reinforce the simple measures everyone should take to be safer and more secure online and their understanding that cybersecurity is a shared responsibility.
- Oct. 7-13, Mobile online safety & security. Highlights the need to maintain a focus on safety and security wherever and whenever we use the Internet.
- Oct. 14-20, Cyber education. Highlights the importance of cyber education and workforce development, including the advancement and opportunities in Science, Technology, Engineering, and Math (STEM) education.
- Oct. 21-27, Cybercrime. Highlights how people can protect themselves against cybercrime and how to get help.
- Oct. 28-31, Cybersecurity and critical infrastructure. Highlights the need to take every step necessary to protect our critical infrastructure.
Review for Mid-term

- Cryptography
  - Basic building blocks
  - Conventional
    - DES, AES, others
  - Public key
    - RSA
  - Hash Functions
  - Modes of operation
    - Stream vs. Block
Review for Mid-term

• Key Management
  – Pairwise key management
  – Key storage
  – Key generation
  – Group key management
  – Public key management
  – Certification
Review for Mid-term

• Authentication: Know, Have, About you
  – Unix passwords
  – Kerberos and NS
  – Public Key
  – Single Sign On
  – Applications and how they do it
  – Weaknesses
Review for Mid-term

• Authorization and Policy:
  – Access Matrix
    ▪ ACL
    ▪ Capability
  – Bell Lapadula
  – Dynamic Policy Management
  – Delegation
  – Importance of getting policy right
• End of Lecture 6

• End of Material to be Covered on MID-Term Exam

• Following slides are to be covered in lecture 7, and lecture 8 (the short lecture following the mid-term)
CSci530: Security Systems
Lecture 7,8 October 11, 18, 2013
Untrusted Computing and Mailicious Code

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Announcements

Mid-term exam
- Friday 18 October 2013
- 9:00 AM through 10:40AM
- Short Lecture to follow at 11:AM
- At present, location for mid-term will be our usual meeting room. If they change this I will post a messages to the class
Classes of Malicious Code

How propagated

• Trojan Horses
  – Embedded in useful program that others will want to run.
  – Covert secondary effect.

• Viruses
  – When program started will try to propagate itself.

• Worms
  – Exploits bugs to infect running programs.
  – Infection is immediate.
Classes of Malicious Code

The perceived effect

• Viruses
  – Propagation and payload

• Worms
  – Propagation and payload

• Spyware
  – Reports back to others

• Zombies
  – Controllable from elsewhere
Activities of Malicious Code

- Modification of data
  - Propagation and payload
- Spying
  - Propagation and payload
- Advertising
  - Reports back to others or uses locally
- Propagation
  - Controllable from elsewhere
- Self Preservation
  - Covering their tracks
Defenses to Malicious Code

• Detection
  – Virus scanning
  – Intrusion Detection
• Least Privilege
  – Don’t run as root
  – Separate users ID’s
• Sandboxing
  – Limit what the program can do
• Backup
  – Keep something stable to recover
Trojan Horses

• A desirable documented effect
  – Is why people run a program
• A malicious payload
  – An “undocumented” activity that might be counter to the interests of the user.
• Examples: Some viruses, much spyware.
• Issues: how to get user to run program.
Trojan Horses

- Software that doesn’t come from a reputable source may embed trojans.
- Program with same name as one commonly used inserted in search path.
- Depending on settings, visiting a web site or reading email may cause program to execute.
Viruses

- Resides within another program
  - Propagates itself to infect new programs (or new instances)
- May be an instance of Trojan Horse
  - Email requiring manual execution
  - Infected program becomes trojan
Viruses

• Early viruses used boot sector
  – Instruction for booting system
  – Modified to start virus then system.
  – Virus writes itself to boot sector of all media.
  – Propagates by shared disks.
Viruses

• Some viruses infect program
  – Same concept, on start program jumps to code for the virus.
  – Virus may propagate to other programs then jump back to host.
  – Virus may deliver payload.
Recent Viruses Spread by Email

• Self propagating programs
  – Use mailbox and address book for likely targets.
  – Mail program to targeted addresses.
  – Forge sender to trick recipient to open program.
  – Exploit bugs to cause auto execution on remote site.
  – Trick users into opening attachments.
Viruses Phases

• Insertion Phase
  – How the virus propagates
• Execution phase
  – Virus performs other malicious action
• Virus returns to host program
Analogy to Real Viruses

• Self propagating
• Requires a host program to replicate.
• Similar strategies
  – If deadly to start won’t spread very far – it kills the host.
  – If infects and propagates before causing damage, can go unnoticed until it is too late to react.
How Viruses Hide

• Encrypted in random key to hide signature.
• Polymorphic viruses changes the code on each infection.
• Some viruses cloak themselves by trapping system calls.
Macro Viruses

- Code is interpreted by common application such as word, excel, postscript interpreter, etc.
- May be virulent across architectures.
Worms

- Propagate across systems by exploiting vulnerabilities in programs already running.
  - Buffer overruns on network ports
  - Does not require user to “run” the worm, instead it seeks out vulnerable machines.
  - Often propagates server to server.
  - Can have very fast spread times.
Delayed Effect

- Malicious code may go undetected if effect is delayed until some external event.
  - A particular time
  - Some occurrence
  - An unlikely event used to trigger the logic.
Zombies/Bots

- Machines controlled remotely
  - Infected by virus, worm, or trojan
  - Can be contacted by master
  - May make calls out so control is possible even through firewall.
  - Often uses IRC for control.
Spyware

- Infected machine collect data
  - Keystroke monitoring
  - Screen scraping
  - History of URL’s visited
  - Scans disk for credit cards and password.
  - Allows remote access to data.
  - Sends data to third party.
Some Spyware Local

• Might not ship data, but just uses it
  – To pop up targeted ads
  – Spyware writer gets revenue for referring victim to merchant.
  – Might rewrite URL’s to steal commissions.
Theory of Malicious Code

• Can not detect a virus by determining whether a program performs a particular activity.
  – Reduction from the Halting Problem
• But can apply heuristics
Defenses to Malicious Code

• Detection
  – Signature based
  – Activity based

• Prevention
  – Prevent most instances of memory used as both data and code
Defenses to Malicious Code

• Sandbox
  – Limits access of running program
  – So doesn’t have full access or even users access.

• Detection of modification
  – Signed executables
  – Tripwire or similar

• Statistical detection
Root Kits

• Hide traces of infection or control
  – Intercept systems calls
  – Return false information that hides the malicious code.
  – Returns fall information to hide effect of malicious code.
  – Some root kits have countermeasures to attempts to detect the root kits.
  – Blue pill makes itself hyper-root
Best Detection is from the Outside

• Platform that is not infected
  – Look at network packets using external device.
  – Mount disks on safe machine and run detection on the safe machine.
  – Trusted computing can help, but still requires outside perspective
Economics of Malicious Code

• Controlled machines for sale
• “Protection” for sale
• Attack software for sale
• Stolen data for sale
• Intermediaries used to convert online balances to cash.
  – These are the pawns and the ones that are most easily caught
Economics of Adware and Spam

- Might not ship data, but just uses it
  - To pop up targeted ads
  - Spyware writer gets revenue for referring victim to merchant.
  - Might rewrite URL’s to steal commissions.
Current event – How does this relate to our discussion

Adobe cyber attack a wake-up call - security firm
2013-10-10 12:05 - Duncan Alfreds- News24.com

Cape Town - The hacker attack on Adobe Systems may increase the vulnerability of all computers running the company's software, a security firm has said. Hackers hit Adobe a week ago and made off with source code along with credit card numbers relating to three million of its customers.

"The risk is elevated because the attackers can now analyse the stolen source code and identify vulnerabilities that were not known so far. They can then develop exploits for these vulnerabilities (zero days)," Ziv Mador director of Security Research at SpiderLabs told News24. Adobe moved quickly to reset customer passwords, but the risk of compromising a system running the software could dent the company's reputation.

Common malware - Mador said that the hack illustrated the risk that large corporations faced in terms of a growing cyber attack. "It shows that even resourceful companies may be successfully targeted and breached. It emphasizes the need to take the necessary precautions and apply a comprehensive security policy to minimise the risk for such breaches."

According to Kaspersky Lab, malware that spreads via infected flash drives are designed to steal personal and financial information. "The Worm.Win32.Mabezat, a file infecting worm which spreads to new computers when accessing an infected drive (including USB thumbs) or file share from a computer that supports the auto-run feature," said Mohammad-Amin Hasbini, GreAt experts at Kaspersky. It emerged recently that some hacker groups were hiring out their services to target companies for specific purposes that may include intellectual property theft.
Review for Mid-Term – 2012 MT Q1

• (30 points) Cryptography - Cryptography - For each of the following methods for encryption or key management methods, match the method with the major characteristics discussed in class. This is not a one-to-one mapping. Some more than one method may match a characteristics, and a single method may also match more than one characteristic. We are looking for specific characteristics, for which you will receive credit. If you list what is a minor characteristic (for example, that DES by itself does not provide authentication), while you will not lose credit, you will not get credit either. You will lose a point if you associated a method with a characteristic that does not apply to the method. There are more blanks in the page below than actual correct answers, so you do not need to fill in all the blanks.

AES as a block cipher
One time pad
Diffie-Hellman-Key exchange
RSA with a 256 bit key
DES in cipher feedback mode (CFB)
DES in Electronic Code Book in (ECB) mode

• Suitable as the basis for providing authentication
• Provides strong integrity
• Dense key space
• Provable / perfect confidentiality protection
• Uses an initialization vector
• Stream cipher
• Uses a single key shared by sender and receiver
2. (30 points) Identity Management

Answer the following questions regarding identity management:

• The three “factors” for authentication may be described as “something that is known”, “something that one has”, and “something about an individual”. Explain how effective implementation of the second and third factors are each dependent on “something that is known”. (10 points)

• What is the goal of federated identity management (what advantages does it provide)? Be sure to consider both kinds of federated identity management systems: those that use a common implementation and are federated only administratively, as well as those that support federation across different implementations for authentication (such as web-based federated identity management systems). (10 points)

• What are the difficulties of effectively implementing federated identity management system? For any difficulties you identify, indicate which kind of system (from the kinds in part b) the difficulty applies to. (10 points) [answer on back of page]
You have been asked to design the key management system for a smart meter system to be used by power companies (utilities) across the world. In this system, utility owned smart meters will be installed on customer's houses. These meters will communicate in a wireless mesh (meaning that one meter will send packets to another meter, which will forward the packets until they reach a “concentrator” on a power pole, which will then send the packets back to the utility over a fiber optic link or a long haul radio link). Important security goals for the communication are that the integrity and privacy of customer data be maintained, and that the system should be resistant to denial of service attacks. Certain functions of the meters may be controllable remotely by utilities, and there might be a capability to update the software on the meters by the utility over the network. The meters are also capable of communicating with certain devices in each customer's home. (40 points)

• List the entities that need encryption keys in such a system. Entities may be specific devices, certain people, etc, but list the different kinds of devices and the different roles of people, etc)? (5 points)

• For each of the entities your listed in part a, list the keys that need to be provided up front (the term is “provisioned”) and the kind of each key (e.g. a secret key, a private key, a public key). (10 points)

• For each of the KEYS listed in part b, indicate who else shares the key. If they key is a private key, then indicate that the key is PRIVATE, and tell me who knows the corresponding public key. (10 points)

• Describe briefly the purpose of each key and indicate the reason that you chose a secret, private, or public key for that purpose, and the reason for sharing the key (or the corresponding key) or for not sharing the key (or the corresponding key) with other entities in the system. (15 points)
Intrusion Everything

• Intrusion Prevention
  – Marketing buzzword
  – Good practices fall in this category
    ▪ We will discuss network architectures
    ▪ We will discuss Firewalls
  – Intrusion detection (next week)
    ▪ Term used for networks
    ▪ But applies to host as well
      – Tripwire
      – Virus checkers
  – Intrusion response (part now, part next week)
    ▪ Evolving area
      – Anti-virus tools have a response component
      – Can be tied to policy tools
Architecture: A first step

• Understand your application
  – What is to be protected
  – Against which threats
  – Who needs to access which apps
  – From where must the access it

• Do all this before you invest in the latest products that salespeople will say will solve your problems.
What is to be protected

• Is it the service or the data?
  – Data is protected by making it less available
  – Services are protected by making them more available (redundancy)
  – The hardest cases are when one needs both.
Classes of Data

• Decide on multiple data classes
  – Public data
  – Customer data
  – Corporate data
  – Highly sensitive data
    (not total ordering)

• These will appear in different parts of the network
Classes of Users

• Decide on classes of users
  – Based on the access needed to the different classes of data.

• You will architect your system and network to enforce policies at the boundaries of these classes.
  – You will place data to make the mapping as clean as possible.

• You will manage the flow of data
Example

• Where will you place your company's public web server, so that you can be sure an attacker doesn't hack your site and modify your front page?

• Where will you place your customer's account records so that they can view them through the web?
  – How will you get updates to these servers?
Other Practices

• Run Minimal Systems
  – Don’t run services you don’t need
• Patch Management
  – Keep your systems up to date on the current patches
  – But don’t blindly install all patches right away either.
• Account management
  – Strong passwords, delete accounts when employees leave, etc.
• Don’t rely on passwords alone
How to think of Firewalled Network

Crunchy on the outside.
Soft and chewy on the inside.
– Bellovin and Merrit
Firewalls

- Packet filters
  - Stateful packet filters
    - Common configuration
- Application level gateways or Proxies
  - Common for corporate intranets
- Host based software firewalls
  - Manage connection policy
- Virtual Private Networks
  - Tunnels between networks
  - Relationship to IPsec
Packet Filter

• Most common form of firewall and what one normally thinks of
• Rules define what packets allowed through
  – Static rules allow packets on particular ports and to and from outside pairs of addresses.
  – Dynamic rules track destinations based on connections originating from inside.
  – Some just block inbound TCP SYN packets
Network Address Translation

• Many home firewalls today are NAT boxes
  – Single address visible on the outside
  – Private address space (net 10, 192.168) on the inside.
• Hides network structure, hosts on inside are not addressable.
  – Box maps external connections established from inside back to the private address space.
• Servers require persistent mapping and manual configuration.
  – Many protocols, including attacks, are designed to work through NAT boxes.
Application FW or Proxies

- No direct flow of packets
  - Instead, connect to proxy with application protocol.
  - Proxy makes similar request to the server on the outside.
- Advantage
  - Can’t hide attacks by disguising as different protocol.
  - But can still encapsulate attack.
- Disadvantage
  - Can’t do end to end encryption or security since packets must be interpreted by the proxy and recreated.
Host Based Firewalls

• Each host has its own firewall.
  – Closer to the data to be protected
  – Avoids the chewy on the inside problem in that you still have a boundary between each machine and even the local network.

• Problems
  – Harder to manage
  – Can be manipulated by malicious applications.
Virtual Private Networks

- Extend perimeter of firewalled networks
  - Two networks connected
  - Encrypted channel between them
  - Packets in one zone tunneled to other and treated as originating within same perimeter.

- Extended network can be a single machine
  - VPN client tunnels packets
  - Gets address from VPN range
  - Packets encrypted in transit over open network
IPSec

• IP Security (IPsec) and the security features in IPv6 essentially move VPN support into the operating system and lower layers of the protocol stack.

• Security is host to host, or host to network, or network to network as with VPN’s
  – Actually, VPN’s are rarely used host to host, but if the network had a single host, then it is equivalent.
Attack Paths

• Many attacks today are staged from compromised machines.
  – Consider what this means for network perimeters, firewalls, and VPN’s.
• A host connected to your network via a VPN is an unsecured perimeter
  – So, you must manage the endpoint even if it is your employees home machine.
Defense in Depth

• One should apply multiple firewalls at different parts of a system.
  – These should be of different types.

• Consider also end to end approaches
  – Data architecture
  – Encryption
  – Authentication
  – Intrusion detection and response
Protecting the Inside

• Firewalls are better at protecting inward threats.
  – But they can prevent connections to restricted outside locations.
  – Application proxies can do filtering for allowed outside destinations.
  – Still need to protect against malicious code.
• Standalone (i.e. not host based) firewalls provide stronger self protection.
Virus Checking

• Signature based
  – Looks for known indicators in files
  – Real-time checking causes files to be scanned as they are brought over to computer (web pages, email messages) or before execution.
  – On server and client

• Activity based
  – Related to firewalls, if look for communication
  – Alert before writing to boot sector, etc.

• Defenses beyond just checking
  – Don’t run as root or admin
Current event – How does this relate to our discussion

Your refrigerator may cause a cyber attack

Picture being at the grocery store, trying to remember how much milk you have at home.

You can take the chance of buying some and having too much. Or you can own a “smart” refrigerator that can tell you whether you’re already stocked up. Convenient, right?

But it’s also a hacker’s delight.

I got on the topic of the danger of smart fridges with Scott Montgomery, the public sector vice president at McAfee Inc., a California cyber security company. He said such fridges are connected to the Internet. And if a hacker wanted to, he could actually hack into the fridge and bypass the firewalls in someone’s computer network.
CSci530: Computer Security Systems
Lecture 10 – 1 November 2013
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
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 ‘GrIIDS Detector’)
    )
  )
  (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 elementW
Current event – How does this relate to our discussion

Cyber-Squatters' Set Up Fake Obamacare Websites
Thursday, 24 Oct 2013 01:12 PM - By Sandy Fitzgerald – Newsmax.com

More than 700 fake or misleading websites playing off of the new federal Healthcare.gov site and the word Obamacare have been created on the Internet by so-called cyber-squatters looking to steal personal information from individuals trying to get healthcare coverage.

One website, the Examiner noted, has even branded itself as part of the "Obamacare enrollment team" and directs people to enter their name, address, Social Security number, and more on an enrollment form. But the site — www.obama-care.us — doesn't enroll anybody in anything. It just takes the information.

Earlier this month, McAfee Antivirus founder John McAfee described the Obamacare website as a hacker's dream because millions of Americans could have their identities stolen. He warned that anyone could put up a fake page and claim to be a healthcare insurance broker affiliated with the federal program.

"Any hacker can put a website up, make it look extremely competitive, and because of the nature of the system, this is healthcare after all, they can ask you the most intimate questions, and you're freely going to answer them," McAfee said.
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 (2)

• 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

• Robert B. Cialdini summarized six tendencies of human nature in the February 2001 issue of Scientific American.

• 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 learns 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?
CSci530: Security Systems
Lecture 12 – November 15 2013
Trusted Computing

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute

Copyright © 1995-2013 Clifford Neuman - UNIVERSITY OF SOUTHERN CALIFORNIA - INFORMATION SCIENCES INSTITUTE
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 provides isolation and virtualization beyond 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”.

Copyright © 1995-2013 Clifford Neuman - UNIVERSITY OF SOUTHERN CALIFORNIA - INFORMATION SCIENCES INSTITUTE
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”.

Copyright © 1995-2013 Clifford Neuman - UNIVERSITY OF SOUTHERN CALIFORNIA - INFORMATION SCIENCES INSTITUTE
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 CTL-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

Slide From Steve Lamb at Microsoft
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)

Slide From Steve Lamb at Microsoft
BitLocker™ Architecture
Static Root of Trust Measurement of early boot components

Slide From Steve Lamb at Microsoft
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
Russian nuclear power plant infected by Stuxnet malware says cyber-security expert

The Independent – Friday 15 November

Stuxnet, a malware program widely believed to have been created by the US and Israel, has infected a Russian nuclear power plant, according to cybersecurity expert Eugene Kaspersky.

Speaking at the Canberra Press Club 2013 in Australia, Kasperksy recounted a story from “the Stuxnet time” when a friend of his working in an unnamed nuclear power plant reported that the plant’s computers were “badly infected by Stuxnet”.

Kaspersky criticized government departments responsible for engineering cyber-attacks, saying: “They don’t understand that in cyberspace, everything you do - it’s a boomerang: it will get back to you.”

The Stuxnet virus was first discovered in June 2010 and was found to specifically target industrial control systems manufactured by Siemens.
Mid-term Q1

• Policy Management - For each of the following methods of representing policy, match the method with the major characteristics or relevant terms discussed in class.

• Bell La Padula
  • Associated with object
  • Separation of roles
  • Identity based
  • Star Property
  • Integrity
  • Mandatory Access Control
  • Associated with user
  • Often Sparsely Filled

• Biba

• Role-Based Access Control

• Access Control List

• Capability List

• Access Matrix
Mid-term Q2

• Explain why a typical public key (asymmetric) cryptosystem under a brute force attack is weaker than a typical conventional (symmetric) cryptosystem with the same size encryption key? (15 points)

• Why is it that modes of operation based on Xor in the final step (i.e. after any encryption operations) are typically weak with respect to integrity. Consider both the one-time pad, and the output-feedback mode-of-operation. (10 points)

• Identify and explain the role of the trusted third party in incremental key distribution systems using both public key and conventional cryptography. What data is created by such third parties that will be used for authentication? (15 points)
Mid-term Q3 (preamble)

- You have been hired by a smartphone maker to add biometric authentication to their smartphone, in answer to customer demand caused by the fingerprint reader on the new iPhone. Your new employer is insisting that this integration be done right, not simply as a gimmick that can be readily defeated. Because you have taken a security course at USC, you understand some of the issues surrounding policy and multi-factor-authentication, and you are ready to design a solution. In answering the questions that follow, put yourself in the shoes of an adversary, and think about how they get access to a phone, and what kinds of things they might be capable of doing, then design your approach to mitigate the impact of such attacks.
Mid-term Q3a

• List the kinds of functions performed by a phone that will require authentication. By functions, I mean either access to specific data, or certain specific events that might be initiated by a user. (It is ok to group similar functions together, but to understand what is meant by similar functions, you should read the remaining questions, as those that are similar are the ones that would be treated the same way in the questions that follow). (10 points)
Mid-term Q3b and c

• How will you protect data on the device from being accessed by someone that gains access to the phone? Such an attacker is also likely to power down the phone initially after stealing it, so that his or her location isn’t tracked. Consider that such an attacker might want to read data off the embedded memory directly, not just access it by logging in. What kind of authentication will you require for access to data on the phone, and when will this authentication be required. (10 points – answer on back of page)

• How will you support authentication by the user to basic services on the internet, and will the user need to authenticate each time. Your answer to this described your solution to single-sign-on. (5 points)
Mid-term Q3d

- For internet services requiring stronger authentication, describe some approaches that support multi-factor authentication. In your design, which factors are used, and at what point in the users experience are each factor checked? (15 points – answer on back of page)
CSci530: Security Systems
Lecture 13 – November 15, 2013
Privacy

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
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 ones 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
• 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.
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.
Unlinking the Trail

• 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 it 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.
CSci530: Security Systems
Lecture 13 – December 6th, 2013
Security for Critical Infrastructure
and Cyber-Physical systems

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Critical Infrastructure

- **Critical**
  - Compromise can be catastrophic
  - Existing approaches to protection often based on isolation.

- **Infrastructure**
  - It touches everything
  - It can’t be isolated by definition
    - But the cyber components have been isolated in the past

- **Smart (or i- or e-)**
  - We can’t understand it
  - And we can’t even isolate the cyber components.
Critical Infrastructure is a Federated

• Characteristics of Federated Systems
  – Parts of the system managed by different parties.
  – No single entity with physical control of all components
  – Lack of a common set of security policies

• Today’s Systems are Naturally Federated
  – We can’t impose central structure
  – Among these systems
    ▪ The Power grid and the smart grid
    ▪ The Financial System
    ▪ Cloud Computing
    ▪ The Internet in general
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
Understanding Securability

• Security is About Boundaries
  – We must understand the boundaries
  – Containment of compromise is based on those boundaries

• Federated Systems Cross Boundaries
  – Federation is about control
    ▪ And the lack of central coordinated control
    ▪ By definition, we can’t control parts of the system.
  – Protecting such systems requires constraints at the boundaries.
Securing the Federation

• Traditional Security
  – It’s about protecting the perimeter.
  – Imposing policy on ability to access protected resources.

• In Federated Systems
  – The adversary is within the perimeter.
  – There are conflicting policies.

• The failure lies in not defining the perimeter
  – Or more precisely, in choosing the wrong one
  – Allowing the boundaries to change
  – Not implementing correct containment at the boundary
Meaning of Security for C-P Systems

• In traditional cyber systems, emphasis on:
  – Confidentiality and Integrity

• In Cyber-Physical systems much greater emphasis on:
  – Resiliency (one example of “availability”)
  – The consequences of failure are greater.

• Interrelation of Integrity with Resilience
Trends in Power Systems

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

• System requirements preclude certain defenses
  – Smart means harder to analyze
  – Infrastructure means hard to isolate
    • Access part of service definition
  – Physical means domain-specific attack modes
Tradition Security and the Smart Grid

- 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 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.
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.

Copyright © 1995-2013 Clifford Neuman - UNIVERSITY OF SOUTHERN CALIFORNIA - INFORMATION SCIENCES INSTITUTE
November 18th, 2012:
Your utility meter just churns away at the side of your home, but the information it's cranking out has computer science graduate students at USC talking. "At least they're not widely deployed so we wanted to study what type of utility meters are deployed now," said Wenyuan Xu with the USC Department of Computer Science. "Are they secure?"

The Correct Perimeters

• Systems can be secure for a particular function
  – We need to define perimeters for particular functions

• In the Power Grid
  – Billing and Business operations are one function
  – SCADA and infrastructure control are another.
  – In the smart grid, customer access and HAN control a third

• In the Banking System
  – Each bank has its own perimeter
  – Inter-bank and transaction systems have their own
  – Interactions with customers are all in individual protection domains
Federated systems change over time

- They evolve with new kinds of participants
  - E.g. Power grid → Smart Grid
  - Now the customer is part of the control loop
- New peers join the federation
  - Not all may be as trusted
  - An adversary could acquire an existing participant
- Mis-guided public policy could require expansion of protection domains.
- This is why a monolithic security domain will not work.
Interesting questions about security in federated systems 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 (or otherwise domain specific), and each separately controlled device, or physical or functional 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
Containment

Containment techniques must be appropriate to the boundary and the function to be protected.

- Firewalls, Application Proxies, Tunnels (VPN’s) suitable in the Cyber Domain.
- Cyber-Physical boundaries require different techniques.
  - We must understand cyber and physical paths
  - We must understand the coupled systems of systems impact of faults originating in single domain.
  - We must understand the C-P impact of attack automation
- Financial systems require yet another set of techniques
- We need to group similar, yet distinct protection domains.
• **Operational Resilience** is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures.

  – The definition also usually includes the ability of the system to restore such capability, once it has been interrupted.

  – A system performs many functions and operational resilience is a function of functional resilience of different aspects of the system.

  – The function depends on domain understanding (especially time-scales)
Functional Resilience

- In the Smart Grid functions include:
  - SCADA
    - Impact of failure in seconds
  - Demand Response
    - Impact of failure depends on reserves, but order of minutes to hours
  - Billing and administrative
    - Impact of failure on order of months.
  - Home automation, customer “features”
    - Little impact of failure
Basis for Functional Resilience

• Functional System Architecture
  – Structure of Fault Containment Regions
    ▪ Mapped to protection domains
  – Functional Redundancy
    ▪ And how redundant components are organized
  – Failure/Fault Models
    ▪ Independence of failure or common mode
    ▪ Intelligent adversaries
How resilience used to be achieved

• *Availability* has always been a critical service for power control networks and C-P systems
  – 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.
Threat 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-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

- 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-Cyber 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

- 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
    - Breaker keeps threat from propagating upward
    - Explicitly imposes the impact downward
  - Reserves often necessary for containment
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
    ▪ Multiple Chevy Volts’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.
Physical-Cyber Threats

- Physical-Cyber threats (impact to computing)
  - For example, causing loss of power to or destruction of computing or communication equipment.
    - A physical action impacts the computation or communication activities in a system.
  - Containment through redundancy or reconfiguration
    - Standard disaster recovery techniques including off-site backup, and even cloud computing.
  - Still need to expect
    - Computing supply chain issues and hardware provenance (counterfeit products, or changes during fabrication).
Physical-Physical Threats

• 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
    ▪ Firewalls and circuit breakers have analogies in many problem domains (including the financial sector)
  – Such containment in problem specific areas often protects against only known threats.
Improving 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
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.
Securing the Smart Grid

• 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
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.
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”
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.
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.
2011 Final Design Problem

• (40 points) – Security in a Cloud Based File Store

You have been hired to redesign the security mechanisms for a cloud based file service (similar to DropBox). Your main concern is ensuring the confidentiality and integrity of data stored in the cloud. Ideally, files stored in the cloud will only be readable to authorized users, and not accessible to others including employees of the cloud storage company itself.

Files stored in the cloud will be accessed by their owner on various devices, including desktop and laptop computers, smartphones, and from the web. Certain “shared” directories (and the files they contain) may be accessible to selected other users with whom the owner has chosen to share a directory. Files should remain accessible to authorized users on their devices even when the users are disconnected from the network. The owner of a shared file or directory must be able to revoke access to other users that were previously authorized.
CSci530: Security Systems
Lecture 14 – December 6, 2013
Security in the Cloud

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
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 ones 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.
Break – 10 Minutes - Evaluations

20 minutes Total
CSci530: Security Systems
Lecture 14.2
Misc Topics

Dr. Clifford Neuman
University of Southern California
Information Sciences Institute
Common Suggested Topics

- Security in routing
- IP Traceback
- Mobile Computing/Devices
- Bot-nets
- Middleware
- Honeypots
- System Assurance
- E-commerce, e-payment
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.
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:  • Issues:
  – First Virtual  – Security of system specific credentials
  – CyberCash  – Real time authorization
  – SET  – 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  
- CMU’s NetBill  
- 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 into 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
  – Customer and merchant info
• 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

AAAAAQAAAA5OZXRDaGVxdWVfVjEuMAAAAA1TT0ZUV0FSRV9WMS4xAAAAAQED
NTE4AzI2N2GCAQcwgEDoAMCAQWhExsRTkVUQ0hFUUUVFLk1TSS5FRFWiTAn
oAMCAQGhIDAeGw1OZXRDaGVxdWUuEW5ldGNoZXF1ZS5pc2kuZWRl04G7MIG4
oAMCAQGhAwIBaKBqwSBqEILdnGDj8taheicu2b3DK+0qYB+ayEtyZUdVsyC
RVFVRS5JU0kuRURVAAAAABQAAAAIBM05DVQExATEAAAAEAjU5AAAACwk4MDAw
MzQ4NzkJODAyMTk0Nzk4AAACQIxNUNsaWZmb3JkX05ldW1hcmtldHBsYWNlQE5FVENIRVFVRS5JU0kuRURVAAAAA==
--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

AS1
accounts: AS3, S1, CS1

AS2
accounts: AS3, U2, CS2

AS3
accounts: AS1, AS2

S1

U2

<check>
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
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
Glossary of Attacks

This is not a complete list

• 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)
  - 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)?
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 mis-use 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)
CURRENT EVENTS
The Quantum Algorithm That Could Break the Internet
From the New Scientist – Slate 11/30/13

• When does a quantum computer start to get scary? - By Celeste Biever

• Peter Shor, a computer scientist at the Massachusetts Institute of Technology, explains why he devised an algorithm for a quantum computer that could unravel our online data encryption.

• Celeste Biever: Internet security relies on the fact that our computers can't break its cryptosystems. But the quantum algorithm you devised has the potential to do just that. Why create it?
  Peter Shor: My motivation was to see what you can do with a quantum computer. An earlier quantum algorithm worked by using periodicity—the tendency of some number sequences to regularly repeat. This is related to factoring, or finding which smaller numbers big numbers are divisible by, so I thought a quantum computer might be able to factor large numbers. As Internet cryptosystems rely on the fact that current computers cannot factor big numbers, I figured a powerful enough quantum computer could break these systems.

• CB: Did you worry about the implications when you finished Shor's algorithm in 1994?
  PS: I felt great having discovered something nobody else knew. If I hadn't done it, someone else would have, eventually. At that time quantum computers were completely hypothetical and I didn't really think one could be built. Now the only ones that are built are toy ones, so they can't yet come close to factoring numbers large enough to pose a risk.

• CB: Twenty-one is the biggest number a quantum computer has factored. When do we worry?
  PS: If you start factoring 10-digit numbers, then it's going to start getting scary. I think we are pretty safe for five or 10 years, probably more.

• CB: Quantum cryptography can't be broken by factoring. Could it one day replace standard cryptosystems?
  PS: For short distances it wouldn't be too hard to build a quantum key distribution network to encrypt data. Over longer distances, you would need quantum repeaters every 50 kilometers or so on the fiber-optic network, as it's difficult to maintain a quantum state over long distances. Even if they are cheap by then, it's a lot of investment.