02- Introduction to Security / Usable Encryption

Lorrie Cranor

January 23, 2017

05-436 / 05-836 / 08-534 / 08-734 / 19-534 / 19-734
Usable Privacy and Security
Outline

• Defining and motivating computer security
• Types of misuse
• Threats and attackers
• Basic security analysis
• (Un)usable encryption

Goals: To learn...
• about the breadth of things that one needs to worry about
• how an attacker might think
• how to reason about the security of a system
• why encryption poses usability challenges
What is computer security?

• Protecting information systems against misuse and interference

• “Building systems to remain dependable in the face of malice, error or mischance” (Ross Anderson)
Properties of a secure system

• Confidentiality: information is protected from unintended disclosure (secrecy, privacy, access control)

• Integrity: system and data are maintained in a correct and consistent condition

• Availability: systems and data are usable when needed (includes timeliness)
Secrecy, Confidentiality, Privacy, Anonymity

Not exactly the same thing

- **Secrecy**
  - Keep data hidden
  - E.g., Alice kept the incriminating information secret

- **Confidentiality**
  - Keep (someone else’s) data hidden from unauthorized entities
  - E.g., banks keep much account information confidential

- **Privacy**
  - Use/disclose a person’s data according to a set of rules
  - E.g., to protect Alice’s privacy, company XYZ removed her name before disclosing information about her purchases

- **Anonymity**
  - Keep identity of a protocol participant secret
  - E.g., to hide her identity from the web server, Alice uses The Onion Router (TOR) to communicate
Integrity, Authentication

*Not exactly the same thing*

- **Data integrity**
  - Ensure data is “correct” (i.e., correct syntax & unchanged)
  - Prevents unauthorized or improper changes
  - E.g., Trent always verifies the integrity of his database after restoring a backup, to ensure that no incorrect records exist

- **Entity authentication or identification**
  - Verify the identity of another protocol participant
  - E.g., Alice authenticates Bob each time they establish a secure connection

- **Data authentication**
  - Ensure that data originates from claimed sender
  - E.g., For every message Bob sends, Alice authenticates it to ensure that it originates from Bob
Attackers exploit bugs

- Software bugs
- Hardware bugs
- Humans (social engineering)
- Unintended characteristics (e.g., side channels, poor sources of randomness)
Modeling the attacker

• What type of action will they take?
  – Passive (look, but don’t touch)
  – Active (look and inject messages)

• How sophisticated are they?

• How much do they care? What resources do they have?
  – How much time/money will they spend?

• How much do they already know?
  – External / internal attacker?
Exploiting bugs as a nuisance

• Pranks, to be annoying
  – Newsday tech writer & hacker critic found …
    • Email box jammed with thousands of messages
    • Phone reprogrammed to an out of state number where caller’s heard an obscenity-loaded recorded message [Time Magazine, December 12, 1994]

• May be costly
  – MyDoom (2004) - $38.5 billion
  – SoBig (2003) - $37.1 billion
  – Code Red (2001) - $2 billion
Exploiting bugs for profit

• Credit card and financial account fraud
• Stealing intellectual property or confidential information
• Ransom
• Extortion
• Stealing computing resources to sell
The economics of botnets

[ Y. Namestnikov. The economics of botnets. Kaspersky Lab, 2009. ]
Pricelists

- $100-180 per 1000 installs (2011)
- $1-1,500 stolen bank account details (2009)
- $20-100+ US credit card (2013)
- $5-8 US citizen personal data (2009)
- $7-15 user accounts for paid online services (2009)
- $1000-2000 per month for botnet spam services (2009)
- $50-$$$ per day for botnet DDoS services (2009)
- $125,000 for zero-day browser exploit to private party (2012)
- $250,000 for zero-day iOS exploit to government (2012)

Sources:
- Stolen Target credit cards and the black market. Tripwire, 21 Dec 2013.
Types of Information System Misuse (1)
[Neumann and Parker 1989]

- External
  - Visual spying  
    Observing keystrokes or screens
  - Misrepresentation  
    Deceiving operators and users
  - Physical scavenging  
    “Dumpster diving” for printouts

- Hardware misuse
  - Logical scavenging  
    Examining discarded/stolen media
  - Eavesdropping  
    Intercepting electronic or other data
  - Interference  
    Jamming, electronic or otherwise
  - Physical attack  
    Damaging or modifying equipment
  - Physical removal  
    Removing equipment & storage media
Types of Information System Misuse (2)
[Neumann and Parker 1989]

• Masquerading
  – Impersonation  Using false identity external to computer
  – Piggybacking  Usurping workstations, communication
  – Spoofing  Using playback, creating bogus systems
  – Network weaving  Masking physical location or routing

• Pest programs
  – Trojan horses  Implanting malicious code
  – Logic bombs  Setting time or event bombs
  – Malevolent worms  Acquiring distributed resources
  – Viruses  Attaching to programs and replicating

• Bypasses
  – Trapdoor attacks  Utilizing existing flaws
  – Authorization attacks  Password cracking
Types of Information System Misuse (3)
[Neumann and Parker 1989]

- **Active misuse**
  - Basic
  - Denials of service
  
  Creating false data, modifying data
  Saturation attacks

- **Passive misuse**
  - Browsing
  - Inference, aggregation
  - Covert channels
  
  Making random or selective searches
  Exploiting traffic analysis
  Covert data leakage

- **Inactive misuse**
  
  Failing to perform expected duties

- **Indirect misuse**
  
  Breaking crypto keys
Basic security analysis

• How do you secure X? Is X secure?

1. What are we protecting?
2. Who is the adversary?
3. What are the security requirements?
4. What security approaches are effective?
1. What are we protecting?

- Enumerate assets and their value
- Understand architecture of system
- Useful questions to ask
  - What is the operating value, i.e., how much would we lose per day/hour/minute if the resource stopped?
  - What is the replacement cost? How long would it take to replace it?
2. Who is the adversary?

• Identify potential attackers
  – How motivated are they?

• Estimate attacker resources
  – Time and money

• Estimate number of attackers, probability of attack
Common (abstract) adversaries

• Attacker action
  – Passive attacker: eavesdropping
  – Active attacker: eavesdropping + data injection

• Attacker sophistication
  – Ranges from script kiddies to government-funded group of professionals

• Attacker access
  – External attacker: no knowledge of cryptographic information, no access to resources
  – Internal attacker: complete knowledge of all cryptographic information, complete access
  • Result of system compromise
3. What are the security requirements?

- Enumerate security requirements
  - Confidentiality
  - Integrity
  - Authenticity
  - Availability
  - Auditability
  - Access control
  - Privacy
  - ...

Temporal properties

- **Age**
  - Prove that data exists before a certain time
  - Lower bound on the duration of existence

- **Freshness**
  - Prove that data was created after an event
  - Upper bound on the duration of existence

- **Temporal order**
  - Verify ordering of a sequence of events
Other properties

- **Auditability**
  - Enable forensic activities after intrusions
  - Prevent attacker from erasing or altering logging information

- **Availability**
  - Provide access to resource despite attacks
  - Denial-of-Service (DoS) attacks attempt to prevent availability
4. Approaches to achieve security

- No security
  - Legal protection (deterrence)
  - Innovative: patent attack, get protection through patent law

- Build strong security defense
  - Use cryptographic mechanisms
  - Perimeter defense (firewall), VPN

- Resilience to attack
  - Multiple redundant systems (“hot spares”)

- Detection and recovery (& offense ?)
  - Intrusion detection system
  - Redundancy, backups, etc.
  - Counterstrike? (Legal issues?)
Threat models

• Can’t protect against everything
  – Too expensive
  – Too inconvenient
  – Not worth the effort

• Identify most likely ways system will be attacked
  – Identify likely attackers and their resources
    • Dumpster diving or rogue nation?
  – Identify consequences of possible attacks
    • Mild embarrassment or bankruptcy?
  – Design security measures accordingly
    • Accept that they will not defend against all attacks
Think like an attacker

• Adversary is targeting assets, not defenses
• Will try to exploit the weakest part of the defenses
  – E.g., bribe human operator, social engineering, steal (physically) server with data
Case study

• Class discussion on security of a house
  – What are we protecting?
  – Who is the adversary?
  – What are the security requirements?
  – What security approaches are effective?
Takeaways

• Security: important but difficult
• Security is not absolute
  – Attacker
  – Properties
  – Cost
• Security is about managing risk in the presence of an adversary
Encryption basics

• Putting a message in code so that other people can’t read it

• Two main approaches:
  – Symmetric encryption (same key used for encryption and decryption)
  – Asymmetric encryption (keypair: public key and private key)
What might you want to encrypt?

- Hard drive (or some part of it), disks, USB sticks
- Emails you send
- Messages you send (text messages)
- “Everything” you’re sending when you’re browsing the web
Properties of encryption

• Secrecy
  – Is Lorrie the only person who can decrypt my message?

• Authenticity
  – Did this message really come from Lorrie?

• Integrity
  – Has someone tampered with Lorrie’s message?
Usability problems

• Encryption is rarely configured by default
• You need a good password
  – …and you can’t lose it or forget it
• Public/private key encryption
  – How to get someone’s public key?
  – How do I make it work on my phone?
• “Only paranoid people use encryption”
Why Johnny can’t encrypt

• Questions about the reading?
• How did the experimenters motivate the tasks and get participants to care about security?
• Why was it so hard for participants to complete the tasks?
• What role did attackers play in this user study?
Why Glenn couldn’t encrypt

• Imagine that Ed wants to send a message to Glenn and worries that others might want to intercept his messages

• Ed asked Glenn for his PGP key

• “And yet, Greenwald still didn't bother learning security protocols. ‘The more he sent me, the more difficult it seemed,’ he says. ‘I mean, now I had to watch a f***ing video…?’”

• [http://vimeo.com/56881481](http://vimeo.com/56881481)

• Snowden ended up reaching out to Laura Poitras instead


Can you do better?

In small teams, spend 5 minutes trying to develop a succinct introduction to email encryption (similar to what you just saw) for someone who knows nothing, but fears an attacker. This should be the first thing that is explained when they open an email encryption program the first time.